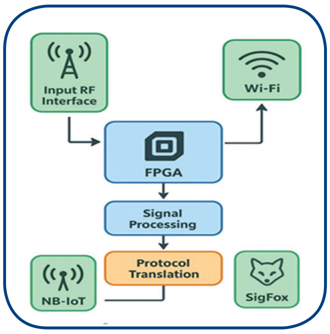
Volume 17, Number 3, 2026

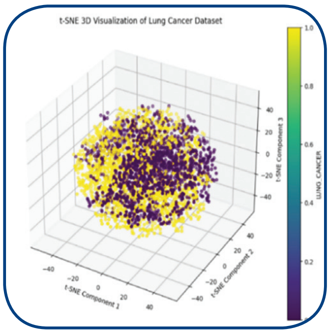
ISSN 1847-6996

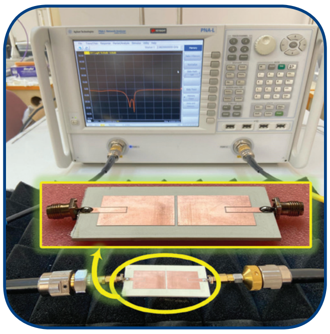
FERIT
FACULTY OF ELECTRICAL ENGINEERING, COMPUTER SCIENCE AND INFORMATION TECHNOLOGY OSIJEK

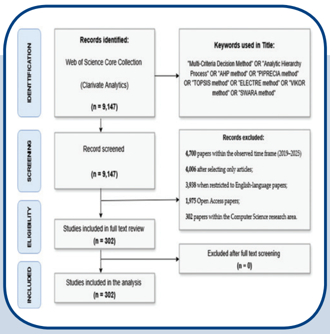
IJECES International Journal of Electrical and Computer Engineering Systems

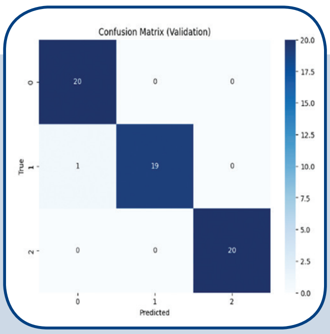
International Journal of Electrical and Computer Engineering Systems

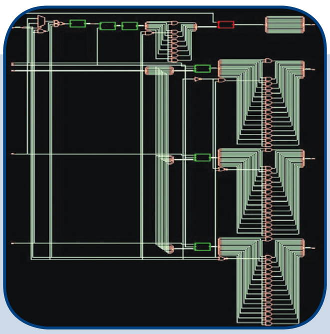












ISSN: 1847-6996

INTERNATIONAL JOURNAL OF ELECTRICAL AND COMPUTER ENGINEERING SYSTEMS

Published by Faculty of Electrical Engineering, Computer Science and Information Technology Osijek, Josip Juraj Strossmayer University of Osijek, Croatia

Osijek, Croatia | Volume 17, Number 3, 2026 | Pages 171 - 255

The International Journal of Electrical and Computer Engineering Systems is published with the financial support of the Ministry of Science and Education of the Republic of Croatia

CONTACT

International Journal of Electrical and Computer Engineering Systems (IJECES)

Faculty of Electrical Engineering, Computer Science and Information Technology Osijek,
Josip Juraj Strossmayer University of Osijek, Croatia
Kneza Trpimira 2b, 31000 Osijek, Croatia
Phone: +38531224600, Fax: +38531224605
e-mail: ijeces@ferit.hr

Subscription Information

The annual subscription rate is 50€ for individuals, 25€ for students and 150€ for libraries.
Giro account: 2390001 - 1100016777,
Croatian Postal Bank

Journal is referred in:

- Scopus
- Web of Science Core Collection (Emerging Sources Citation Index - ESCI)
- Google Scholar
- CiteFactor
- Genamics
- Hrčak
- Ulrichweb
- Reaxys
- Embase
- Engineering Village

Bibliographic Information

Commenced in 2010.
ISSN: 1847-6996
e-ISSN: 1847-7003
Published: quarterly
Circulation: 300

IJECES online

https://ijeces.ferit.hr

TABLE OF CONTENTS

Metaheuristic Optimization for Deep Learning in Plant Disease Detection: A Hybrid Approach

Original Scientific Paper

Aqeel Majeed Breesam*
Institute of Medical Technology/Baghdad
Middle Technical University
Baghdad, Iraq
aqeelmajeed@mtu.edu.iq

Rusul Abdulridha Muttashar
Businesses Informatics College
University of Information Technology and Communications
Baghdad, Iraq
rusul.abdulridha@uoitc.edu.iq

Esraa Najjar
Computer Science Department
General Directorate of Education in Najaf Governorate
Al-Najaf, Iraq
esraas.najjar@uokufa.edu.iq

*Corresponding author

Abstract *– This study investigates metaheuristic hyperparameter optimization for deep learning–based plant disease detection across two datasets: Dataset A (1,530 images; three classes: Healthy, Powdery, Rust) and a large multi-crop corpus evaluated in a binary Healthy/Diseased setting with an 80/20 training–validation split. A hybrid optimizer is proposed that interleaves Dragonfly Algorithm (DA) for population-wide exploration with Firefly Algorithm (FA) for elite intensification (DA–FLA), and is applied to five pretrained CNN backbones (DenseNet, VGG19, InceptionV3, MobileNet, Xception). All models are trained under an identical 50-epoch protocol. On Dataset A, DenseNet provides the strongest baseline (accuracy/macro-F1 = 0.9733/0.9735), which rises to 0.9800/0.9800 with DA–FLA tuning. On the large-scale binary corpus, Xception and DenseNet perform competitively (≈0.9846 macro-F1 and 0.9838 macro-F1, respectively), while the optimized Xception attains 0.9924 accuracy and 0.9913 macro-F1. A one-way ANOVA with Tukey HSD confirms significant performance differences (p < 0.001), with optimized Xception outperforming all comparators. The hybrid search introduces modest training overhead but leaves inference cost essentially unchanged. Results demonstrate that balancing global exploration with local exploitation yields reproducible, statistically supported gains, advancing accurate and efficient plant disease diagnostics suitable for mobile/edge deployment and supporting early intervention and sustainable farming practices.*

Keywords*:* *Plant disease detection, deep learning, dragonfly optimization algorithm, firefly algorithm, hybrid optimization*

Received: May 31, 2025; Received in revised form: October 11, 2025; Accepted: October 23, 2025

1. INTRODUCTION

This study presents a hybrid deep learning approach for plant disease detection, combining CNNs with a novel optimization strategy using the Dragonfly and Firefly Algorithms. By tuning key hyperparameters through this DA-FLA hybrid, the framework enhances classification accuracy and convergence introducing a technique not previously explored in this context.

Food systems and national economies depend on agriculture, but as a result, crop health is continuously threatened by diseases which decrease the quality and output [1, 2]. The productivity is already limited by a range of biotic and abiotic stressors that may disrupt supply chains and become destabilizing [3, 4]. The traditional diagnosis of the expert visual inspection is a labor-intensive, costly and inaccurate process, which restricts the scalability of a large-scale production environment [5-7]. Alternatively, but, conversely, deep learning, and most specifically Convolutional Neural Networks (CNNs), have also demonstrated to be a powerful option, which involves image-based markers, such as discoloration and lesion morphology, to enable effective and automatic detection of plant diseases [8–10]. Nevertheless, the CNN models are typically prone to issues such as slow convergence, expensive computations, and sensitivity to hyperparameter parameters. Recent models like DenseNet, VGG19, InceptionV3, MobileNet, and Xception have shown strong classification capability, but these models have poor hyperparameter sensitivities [11-13]. To overcome this, we present a new metaheuristic optimization model that is a hybrid between the Dragonfly Algorithm (DA) and Firefly Algorithm (FLA) to optimize the main hyperparameters and enhance the model accuracy, convergence, and generalization [14-16]. It is a DA-FLA method that has a unique way of balancing the global search and local refinement, which presents a practical and scalable way of CNN-based plant disease detection.

This method of DA-FLA is the only one that balances both the global search and local refinement in an attempt to provide a practical and scalable solution to CNN-based plant disease detection.

The experimental design was extended to the two datasets to enhance the generalizability and methodological rigor: controlled multiclass corpus (three classes) and large multi-crop corpus working in a binary Healthy/Diseased context. Each architecture was trained with the same 50-epoch schedule, so as to measure them equally. Besides cross-validation and ablation research, statistical significance of differences between models was measured by one-way ANOVA with Tukey HSD post-hoc test which is a strong evidence of the influence of the proposed DA -FLA optimizer.

This research has the following contributions:

- We propose a novel hybrid metaheuristic optimization framework that combines the Dragonfly Algorithm (DA) and Firefly Algorithm (FLA) for fine-tuning CNN hyperparameters—a combination not previously applied in plant disease detection.
- We thoroughly test five deep learning models of (DenseNet, VGG19, InceptionV3, MobileNet and Xception) on a multiclass plant leaf dataset and find the most effective of them to be DenseNet.
- We demonstrate that the DA-FLA optimizer significantly improves classification accuracy, convergence speed, and model generalization, validated through cross-validation, ablation studies, and statistical analysis.
- We show the practical relevance of our optimized model in promoting early disease detection and sustainable agriculture, particularly in resource-constrained environments.

2. REALTED WORK

Recent advances in deep learning most notably with Convolutional Neural Networks (CNNs) have substantially improved plant disease diagnosis by extracting rich spatial and textural cues from leaf images [17, 18]. A prominent direction augments CNNs with metaheuristic optimization and attention mechanisms to improve generalization and convergence. Illustratively, Huang et al. [19] employed the CSUBW optimizer for mango leaf diagnosis, while leveraged GGGWO for potato diseases, jointly evidencing the role of global search in tuning hyperparameters [20]. Additional strands enrich data or search dynamics: PCA and noise injection for robustness, the Crow Search Algorithm for advanced hyperparameter tuning, and ensemble-based optimization via APLDD-ESOSDL. Hybrid and pre-trained CNNs have also been applied to apple and maize plants, frequently paired with Grey Wolf, Whale, and Improved Butterfly Optimization algorithms to bolster accuracy [21, 22]. Parallel efforts incorporate Explainability e.g., Grad-CAM and EDA to increase interpretability and trust in clinical- or field-adjacent decision support. Complementing these, Pham et al. [23] integrated contrast enhancement, segmentation, and an adaptive particle–Gray Wolf optimizer (APGWO) to reduce features for MLP classification, while [24] introduced an ODNN pipeline that couples CNN feature extraction with two-stage weight optimization (Improved Butterfly Optimization plus Genetic Algorithm), attaining 99% on sensitivity/accuracy/specificity.

Building on these foundations, the present hybrid DA–FLA model targets a balanced exploration–exploitation regime for hyperparameter tuning, addressing rugged, mixed-type search spaces [25]. Unlike prior single- or dual-heuristic pairings, this combination has not been previously applied to plant disease classification, and the reported experiments demonstrate both theoretical plausibility and practical efficacy within this domain.

Concurrently, transformer-based vision architectures have begun reshaping agricultural imaging benchmarks [26]. For maize leaf disease recognition, [27] proposed a deployment-oriented framework that adapts MaxViT to a lightweight four-class setting, replacing the stem's conventional convolutional block with a Squeeze-and-Excitation module and adopting a GRN-based MLP from ConvNeXtV2. By aggregating PlantVillage, PlantDoc, and CD&S into a large composite dataset and evaluating more than 28 CNNs and 36 transformers, the study achieved state-of-the-art accuracy (99.24%) with competitive inference speed, underscoring practical value for time-sensitive agricultural tasks. In grape analysis, [28] benchmarked 31 state of the art CNN and transformer models on a plantvillage (4,062 images; Black Rot, Leaf Blight, Esca, Healthy) and grapevine (500 images; Ak, Alaidris, Buzgulu, Dimnit, Nazli) dataset, and found that 4 models were 100% accurate on both datasets and Swinv2-Base is consistably top-performing, supporting the use of fine-tuned transformers in detecting early disease. To corn, [29] compared MaxViT, DeiT3, MobileViT, and MViTv2 against VGG, ResNet, DenseNet, and Xception in a single pipeline (preprocessing, augmentation, transfer learning, hyperparameter optimization), and proposed a soft-voting ensemble with adaptive thresholding. On the CD&S test set, four MaxViT variants (plus other deep models) reached 100% accuracy, and the approach attained 99.83% on PlantVillage, surpassing prior studies and demonstrating the utility of calibrated ensembles for balanced, high-confidence detection.

Related advances in medical imaging echo these design choices and optimization strategies. For ischemic stroke lesion delineation on MRI, [30] proposed a U-Net variant augmented with ConvNeXtV2 blocks and GRN-based MLPs the first application of ConvNeXtV2 in this setting together with a clinician-informed preprocessing step that filters small spurious lesions (≤5 pixels). On ISLES 2022, the method achieved IoU = 0.8015 and Dice = 0.8894, outperforming strong U-Net baselines and alternative approaches. Within neuro-oncology, [31] proposes NeXtBrain, a hybrid pursuer, combining a NeXt Convolutional Block, which entails multi-head convolutional attention and SwiGLU MLP, and a NeXt Transformer Block, which entails self-attention and convolutional attention and SwiGLU MLP. The model achieves 99.78% accuracy / 99.77% F1 on Figshare and 99.78% accuracy / 99.81% F1 on Kaggle, and is computationally efficient (23.91M parameters, 10.32 GFLOPs, 0.007 ms inference). Collectively, these results from agriculture to clinical imaging reinforce the value of modern attention-based backbones, principled optimization, and carefully curated benchmarks for robust, high-accuracy visual diagnosis.

Table 1. Summary of Related Works

Reference	Methodology	Optimization / Special Technique	Main Contribution
[19]	CNN for mango leaf disease classification	CSUBW optimizer	Improves convergence and accuracy for mango leaf diagnosis
[20]	CNN for potato disease detection	GGGWO (Generalized Growing Grey Wolf Optimizer)	Boosted classification accuracy via metaheuristic hyperparameter tuning
[23]	Contrast-enhancement + segmentation pipeline with MLP classifier (features from CNN)	APGWO (Adaptive Particle–Gray Wolf Optimizer)	Feature reduction and improved MLP classification (Pham et al.)
[24]	CNN with ODNN (Optimal Deep Neural Network) pipeline	Improved Butterfly Optimization + Genetic Algorithm (two-stage weight optimization)	~99% sensitivity/accuracy/specificity with two-stage optimization
[26]	Vision Transformers in agriculture (survey/ benchmark trend)	Transformer backbones	Recent architectures reshaping agri-imaging benchmarks
[27]	MaxViT-based lightweight framework for maize leaf recognition	SE stem + GRN-MLP (ConvNeXtV2)	SOTA ≈99.24% with large composite dataset; deployment-oriented speed
[28]	Grapevine disease/varietal analysis (31 CNN/Transformer models)	Fine-tuned Transformers (e.g., Swinv2-Base)	Four models hit 100% on two datasets; consistent top-tier performance
[29]	Corn disease recognition with CNNs + Transformers	Soft-voting ensemble with adaptive thresholding	Several MaxViT variants reach 100% on CD&S; 99.83% on PlantVillage
[30]	U-Net variant for ischemic stroke MRI lesion segmentation	ConvNeXtV2 blocks + GRN-MLP, clinician-informed filtering	IoU = 0.8015, Dice = 0.8894; surpasses strong U-Net baselines
[31]	NeXtBrain (hybrid Conv-Attention + Transformer) for neuro-oncology	NeXt Conv Block (multi-head conv-attention, SwiGLU MLP) + NeXt Transformer Block	99.78% accuracy / 99.77–99.81% F1 with efficient compute
Our Work	CNN with hybrid DA–FLA model	Dragonfly + Firefly (new pairing for this domain)	Novel hyperparameter tuning combo; balanced exploration–exploitation; improved convergence and accuracy

3. METHODOLOGY

To enhance readability and reproducibility, this section details the datasets, preprocessing pipeline, model architectures, and the proposed DA–FLA hybrid optimization for plant disease classification. The processing of the data commences with the exploratory data analysis (EDA) [32] to ensure integrity and salient patterns on the surface that will guide the extracting of features and training.

Dataset A (three-class leaves). The initial dataset consists of 1530 leaf images [33] annotated in three classes Healthy (530), Powdery (500), and Rust (500). The balance in the class distribution is relatively equal, but a stratified division was employed, and a specific data augmentation (e.g. rotation, flipping, scaling) was made to address the overfitting issue and enhance the generalization.

Dataset B (large-scale multi-crop, augmented) [34]. The second data set is a large scale (approximately 87K RGB images) set obtained through offline augmentation of the popular corpus containing Plant Disease on GitHub (linked to the page displaying the Plant Disease Recognition dataset). It is organized into 38 classes and partitioned 80/20 into training and validation sets while preserving directory structure; a small held-out test set of 33 images is used for downstream prediction checks. For certain experiments, the notebook groups categories into a binary setting (Healthy vs Diseased) to assess robustness under coarse-grained labeling.

This dataset complements Dataset A by providing greater class diversity and scale, enabling evaluation of model behavior under broader visual variability.

Preprocessing and evaluation protocol. For both datasets, images are resized (e.g., to 128×128), normalized to [0,1], and augmented under identical policies (with minor adjustments for class count). Dataset A (three-class) is evaluated on a held-out test split, reporting accuracy, precision, recall, and F1-score. Dataset B (38-class) uses an 80/20 training–validation split without a separate test set; all metrics are therefore reported on the validation split.

Backbones and training schedule. Five pre-trained CNNs DenseNet121 [35], InceptionV3 [36], Xception [37], MobileNet [38], and VGG19 [39] are fine-tuned to extract discriminative features and perform classification. Training protocol. Unless otherwise noted, all architectures are trained for 50 epochs under identical schedules for fair comparison. For comparability, early stopping is not used for model selection; an early-stopping callback (patience = 10) is enabled only for monitoring. The training budget remains fixed at 50 epochs, and all reported metrics correspond to the epoch-50 checkpoint.

Hybrid optimization (DA–FLA). The best-performing backbone is subsequently optimized with a two-stage metaheuristic: the Dragonfly Algorithm (DA) for population-wide exploration and the Firefly Algorithm (FA) for elite-set intensification, supporting mixed-type hyperparameter search. Iterative tuning of learning rate, initializer, and regularization parameters yields a high-accuracy, computationally efficient configuration that is benchmarked against baselines. The resulting pipeline delivers an accurate, fast, and practical solution for plant disease detection suited to precision-agriculture deployments.

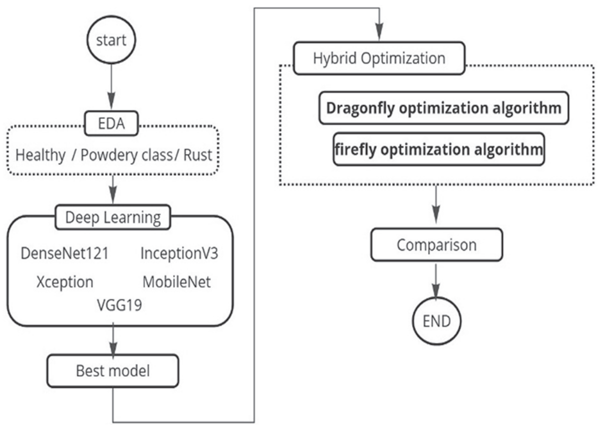


Fig. 1. Proposed methodology

3.1. DRAGONFLY ALGORITHM (DA)

The Dragonfly Algorithm (DA) is a nature-inspired metaheuristic with a swarming dynamics of a dragonfly [40]. It models two important patterns, namely, local swarming (static swarming) to explore the local area and global swarming (migratory swarming) to search the world and optimize it. As illustrated in Fig. 2, it starts with the initialisation of a population of artificial dragonflies in random positions and step vectors in the search space. In each of the dragonflies, the fitness is measured to give the proximity to the optimal solution.

Dragonflies at every step change their positions depending on five main coefficients: separation (avoid crowding), alignment (angular velocity matching that of others in the group), cohesion (moving towards group centre), attraction to food (good solutions), and repulsion of enemies (bad solutions). These interactions of neighborhoods with the social and environmental dynamically affect the neighborhood size to enhance convergence.

The algorithm repeats the steps of updating positions and step vectors until a stopping condition (e.g. a maximum number of iterations) is reached (as shown in Fig. 3). In the case of neighbors, dragonflies adapt according to swarm behavior; randomly, in the absence of neighbors. The adaptive mechanism enables the effective balancing of exploration and exploitation by DA to converge to the best solutions when searching in complex space.

In our approach, the position of each agent is a collection of CNN hyperparameter and the fitness is determined by validation accuracy. The Dragonfly Algorithm tries out the unexplored combinations and the Firefly Algorithm refines the most effective ones.

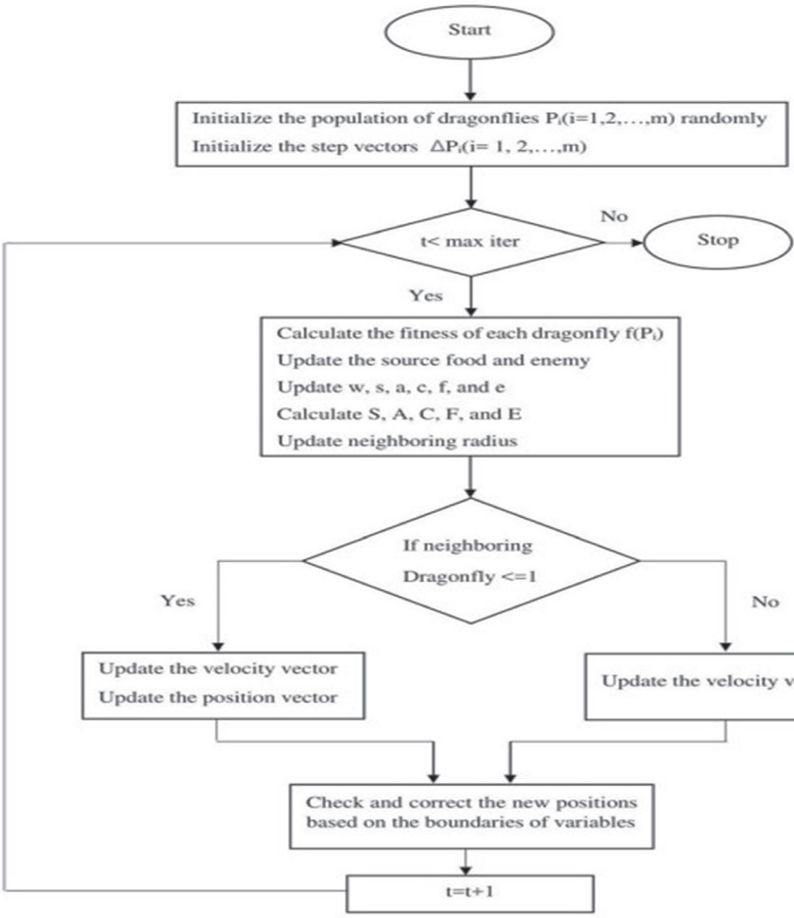


Fig. 2. Flowchart of the dragonfly algorithm

```
Algorithm 1: Dragonfly Algorithm
Initialize the population's positions randomly;
Initialize the step vectors;
while end condition do
    Calculate the objective values of all dragonflies;
    Update the food source and enemy;
    Update the weights;
    Calculate the factors using (1)–(5);
    Update radius of neighbourhoods;
    if dragonfly has one or more neighbours then
        Update step vector using (6);
        Update position vector using (7);
    else
        Update position vector using (8);
    end
    Check and correct new positions based on upper and lower bounds;
end
```

Fig. 3. Dragonfly Algorithm [41]

3.2. FIRRFLY ALGORITHM (FA)

Firefly Algorithm (FA) is a bio-inspired metaheuristic based on the luminescent signalling process of fireflies and it was first proposed by Xin-She Yang in 2008 [42]. The brightness of a firefly in the context of optimization reflects how good a solution is the brighter the solution (better solution) the dimmer the other fireflies, the population is directed to the best solutions [43].

The algorithm used will start with a starting population of fireflies randomly distributed within the search space as shown in Figs. 4 and 5. The intensity of the light of every firefly is the objective function, which is a measure of its fitness.

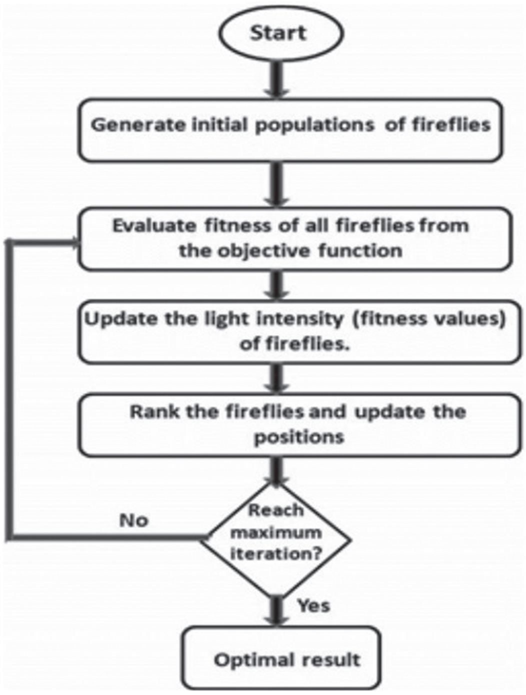


Fig. 4. Flowchart of implementation of firefly algorithm [44]

The fireflies are then sorted by brightness and those with low brightness drift towards bright counterparts. The appeal is reversing with distance, which favors diversity and exploration.

This iteration process continues until such a stopping criterion as a maximum number of iterations is attained. FA is also favored due to its simplicity, robustness and good balance between exploration and exploitation in numerous optimization scenarios.

In this context, each firefly represents a set of hyperparameters, and its brightness reflects the model's validation accuracy. Brighter fireflies attract others, guiding the search toward better-performing hyperparameter settings.

```
Begin
  1. Initialisation max iteration, α, β₀, γ
  2. Generate initial population
  3. Define the Objective function f(x),
  4. Determine Intensity (I) at cost (x) of each individual determined by f(xᵢ)
  5. While (t < Iter max)
              For i=1 to n
                  For j=1 to n
                      if (Iⱼ > Iᵢ)
                          Move firefly i towards j in K dimension
                      end if
                  Evaluate new solutions and update light intensity
                  end for j
              end for i
          Rank the fireflies and find the current best
     end while
  6. Post process results and visualization
End procedure
```

Fig. 5. Pseudo code for firefly algorithm [45]

3.3. HYPERPARAMETER TUNING DETAILS

The proposed DA&FLA optimizer was used to tune the following hyperparameters of the DenseNet model:

Table 2. Hyperparameter Tuning Details

Hyperparameter	Search Range	Optimized Value
Learning Rate	[0.0001 – 0.01]	0.0018
Batch Size	[16, 32, 64, 128]	32
Weight Initialization	[He, Xavier, Normal]	Xavier
Momentum (if used)	[0.5 – 0.99]	0.9
Dropout Rate	[0.1 – 0.5]	0.3
Number of Epochs	[10 – 100]	50

The optimization process used the DA for global search and FLA for fine-tuning local solutions. The best-performing set of values was selected based on validation accuracy over multiple runs.

3.4. HYBRID DA–FLA OPTIMIZER

A two-stage hybrid metaheuristic is employed that interleaves population-wide exploration via the Dragonfly Algorithm (DA) with targeted local intensification via the Firefly Algorithm (FA). DA evolves the full population to sustain broad coverage of the mixed hyperparameter space, whereas FA periodically refines an elite subset to hasten convergence within promising basins.

Let the hyperparameter vector be $x \in \Omega \subset R^{dc} \times Z^{dd} \times C^{dg}$, comprising continuous (e.g., learning rate, dropout), discrete (e.g., batch size, epochs), and categorical (e.g., initializer) variables. A real-valued working representation is maintained with projection $\Pi_\Omega(\cdot)$ enforcing feasibility: element-wise clipping for continuous bounds, nearest-neighbor rounding for discrete choices, and argmax over a one-hot/Gumbel-Softmax proxy for categorical options. Fitness $f(x)$ is defined as cross-validated validation accuracy averaged across folds, with elitist selection based on f. Within this setting, DA operates on a population $\{x_i\}$ N¦(i=1) with associated step vectors $\{vi\}$, updating candidates via neighborhood-aware social operators to generate informed exploratory moves prior to FA-based intensification on the current elites.

$$S_i = \sum_{j \in \mathcal{N}_i} \frac{x_i - x_j}{\|x_i - x_j\| + \varepsilon} \tag{1}$$

$$A_i = \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} v_j \tag{2}$$

$$C_i = \frac{1}{|\mathcal{N}_i|} \sum_{j \in \mathcal{N}_i} x_j - x_i \tag{3}$$

$$F_i = x^{\star} - x_i \tag{4}$$

$$E_i = x_i - x^{\ominus} \tag{5}$$

The step and position updates are:

$$v_i \leftarrow w_s S_i + w_a A_i + w_c C_i + w_f F_i + w_e E_i + \eta_i, \quad \eta_i \sim \mathcal{N}(0, \sigma^2 I) \tag{6}$$

$$x_i \leftarrow \Pi_\Omega(x_i + v_i) \tag{7}$$

Neighborhood radii expand/contract adaptively with iteration to balance exploration and exploitation. When $|N_i|$=0, a Lévy-like random step replaces the social term to avoid stagnation.

Firefly-based intensification operates on the elite subset $\varepsilon \subset \{\boldsymbol{x}_i\}$ N¦(i=1) consisting of the top-P candidates ranked by fitness f. For each ordered pair $(\boldsymbol{x}_a, \boldsymbol{x}_b)$ with $\boldsymbol{x}_a, \boldsymbol{x}_b \in \varepsilon$ and $f(\boldsymbol{x}_b) > f(\boldsymbol{x}_a)$, a distance-weighted attraction is applied to promote local refinement toward superior incumbents while preserving feasibility via projection. The procedure is executed either periodically every K Dragonfly generations or adaptively when a stagnation counter exceeds S iterations without global improvement; elitist replacement accepts only improvements in f, thereby ensuring monotonicity of the incumbent within the elite set.

$$x_a \leftarrow \Pi_\Omega\left(x_a + \beta_0 e^{-\gamma\|x_a - x_b\|^2}(x_b - x_a) + \xi\right), \quad \xi \sim \mathcal{N}(0, \sigma_{FA}^2 I),\ \gamma > 0 \tag{8}$$

Acceptance, scheduling, and stopping follow a disciplined protocol: for iterations t=1,…,T, each cycle performs one Dragonfly (DA) generation over all N agents;

whenever $t \bmod K=0$ or a stagnation counter reaches S, a Firefly (FA) intensification pass is executed on the elite set ε. Elitism maintains a global archive $x\star$ with maximal fitness f and permits elite replacement only upon improvement, ensuring monotonic advancement of the incumbent. Termination occurs when the iteration budget T is exhausted or when two successive FA calls yield no improvement for any elite. Computationally, one DA generation is $O(N\,\bar{d})$ for social-term computation (under bounded neighborhoods) plus the dominant training-time cost of evaluating f, whereas a single FA pass requires $O(P^2)$ lightweight updates and elite evaluations; with $P \ll N$, intensification overhead remains negligible relative to model training. Feasibility over mixed variable types is enforced via the projection operator Π_Ω: continuous components are clipped to bounds, discrete components are rounded to the nearest admissible value, and categorical components are instantiated from Gumbel–Softmax logits (with temperature annealing) and then fixed during the model-training call used to compute f.

```
Algorithm 2 Hybrid DA–FA Hyperparameter Optimizer
Require: Search space Ω; population size N; elite size P; max iterations T;
         DA weights (w_s, w_a, w_c, w_f, w_e); FA params (β_0, γ);
         noise scales (σ, σ_FA); triggers K (periodic), S (stagnation)
Ensure: Best hyperparameter vector x* ∈ Ω
  Initialize population {x_i}_{i=1}^N ~ Ω, step vectors v_i ← 0
  Evaluate f(x_i) for all i; x* ← arg max_i f(x_i); x^⊖ ← arg min_i f(x_i)
  no_improve ← 0
  for t = 1 to T do
                                        ▷ DA exploration over full population
      for each agent i ∈ {1, ..., N} do
          Compute neighborhood N_i (adaptive radius)
          if |N_i| > 0 then
              S_i ← Σ_{j∈N_i} (x_i − x_j) / (||x_i − x_j|| + ε)        ▷ separation
              A_i ← (1/|N_i|) Σ_{j∈N_i} v_j                            ▷ alignment
              C_i ← ((1/|N_i|) Σ_{j∈N_i} x_j) − x_i                    ▷ cohesion
              F_i ← x* − x_i                        ▷ attraction to best ("food")
              E_i ← x_i − x^⊖                     ▷ repulsion from worst ("enemy")
              v_i ← w_s S_i + w_a A_i + w_c C_i + w_f F_i + w_e E_i + N(0, σ^2 I)
          else
              v_i ← LevyLikeStep()
          x_i ← Π_Ω(x_i + v_i)

          Evaluate f(x_i) for all updated i; update x* and x^⊖ accordingly
          if Improved(x*) then
              no_improve ← 0
          else
              no_improve ← no_improve + 1
          end if
                                              ▷ FA intensification on elites
          if (t mod K = 0) or (no_improve ≥ S) then
              E ← TopElites({x_i}, P by f)
              improved ← False
              for each unordered pair (x_a, x_b) ⊂ E with f(x_b) > f(x_a) do
                  r ← ||x_a − x_b||; β ← β_0 exp(−γ r^2)
                  x'_a ← Π_Ω(x_a + β(x_b − x_a) + N(0, σ_FA^2 I))
                  if f(x'_a) > f(x_a) then
                      x_a ← x'_a; improved ← True
                  end if
              end for
              if improved then
                  x* ← arg max{f(x) : x ∈ E}; no_improve ← 0
              end if
          end if                    2

          return x*
```

Fig. 6. Hybrid DA-FA hyperparameter optimizer

3.5. DATASET DISTRIBUTION

Dataset A: Three-class leaves (1,530 images)

Images are stratified into Healthy, Powdery, and Rust with an 70/15/15 split for training/validation/test, as shown below.

Table 3. Dataset Distribution

Class	Training	Validation	Test	Total
Healthy	380	75	75	530
Powdery	350	75	75	500
Rust	350	75	75	500
Total	**1,080**	**225**	**225**	**1,530**

Dataset B: Large-scale multi-crop (≈87,000 images; 38 classes).

A second corpus is constructed via offline augmentation of a widely used plant-disease dataset, yielding ~87K RGB images across 38 classes. The data preserve the original directory structure and are split 80/20 into training/validation; an additional held-out test set of 33 images is used for sanity-check predictions. This dataset complements Dataset A by providing greater scale and class diversity, facilitating robustness assessment under broader visual variability.

Using both datasets enables evaluation under a focused three-class setting for controlled analysis and a large, heterogeneous, multi-class regime for stress-testing generalization. The offered hybrid optimization structure enhances the accuracy of the plant disease detection in these regimes that promote earlier intervention, minimized crop losses, and more sustainable input utilization. The optimized DenseNet architecture is small-footprint and highly accurate, which means that it can be deployed in mobile/IoT resources in a resource-limited farming setting.

4. EVALUATION METRICS

In order to measure image classification performance of the model, various critical measures are adopted. The combination of the two provides a detailed picture of how the model is effective and able to categorize images accurately.

4.1. ACCURACY

Accuracy is one of the most popular indicators that reveal the level of predictability of a model [46]. It computes the true positive percentage and the true negative percentage of all the observations. This is an accurate rate of classification that can be calculated theoretical as follows giving a general indication of the model performance:

$$ACC = \frac{TN+TP}{TP+TN+FP+FN} \quad (9)$$

True positives are denoted by TP, true negatives by TN, false positives by FP, and false negatives by FN [47].

4.2. PRECISION

Precision [48] is a measure of the accuracy of the positive predictions. Its definition is the ratio of true positives (TP) to all the cases that were projected to be positive (TP + FP). This measure indicates the extent of predictability of model in detecting real positive cases. The formula for precision is:

$$PRE = \frac{TP}{FP+TP} \tag{10}$$

4.3. RECALL

Recall, also called sensitivity [49], and measures the ability of the model to find all the relevant instances of a specific class. It is calculated as the ratio of the true positives to the sum of true positives and false negatives, which gives the efficiency of the model in capturing the real positive ones.

$$REC = \frac{TP}{TP+FN} \tag{11}$$

4.4. F1-SCORE

The F1-Score [50], the harmonic mean of precision and recall, provides a reasonable evaluation in those cases where both the measures are important but may conflict with each other. It is useful especially in the cases where there is an imbalance in the classes whose performance is going to be assessed. The F1-score may be represented in the following way:

$$F1 - S = 2 \times \frac{PRE \times REC}{PRE+REC} \tag{12}$$

These summary statistics will provide the overall performance of the model, in addition to giving further information about its performance in determining the positive cases of interest.

5. EXPERIMENTAL RESULTS

5.1. DATASET A RESULTS

5.1.1 DensNet result

As indicated in Table 4, DenseNet model provides good performance in terms of plant disease classification where the total accuracy is 97%. It is very accurate with the classes of 'Healthy', 'Powdery' and 'Rust' at 1, 1 and 0.93 respectively. The corresponding recall values are 0.98, 0.94, and 1.00 and the F1-scores were 0.99, 0.97, and 0.96 which show strong sensitivity and specificity. The macro-averages of precision, recall and F1-score are 0.98, 0.97 and 0.97, which indicate similar performance in all the classes.

The training and validation curves are shown in Fig. 7. The accuracy curve (left) displays a gradual increase in training with the least lag in validation and loss curve (right) displays rapid learning and almost zero validation loss proving the model to be good at identifying intricate patterns and is also good at generalizing these to unseen data.

Table 4. Classification report of DenseNet

	Precision	Recall	F1-score
0	1.00	0.98	0.99
1	1.00	0.94	0.97
2	0.93	1.00	0.96
Accuracy	0.97	0.97	0.97
Macro avg	0.98	0.97	0.97

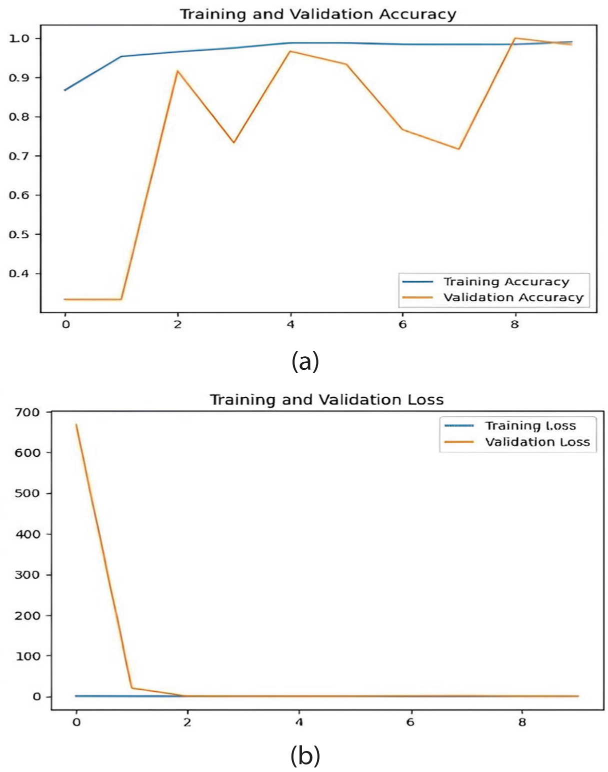


Fig. 7. Dynamics of training the DenseNet model in more than 50 epochs: (**a**) Accuracy, (**b**) Loss. Training and validation are indicated as curves

5.1.2. VGG19 result

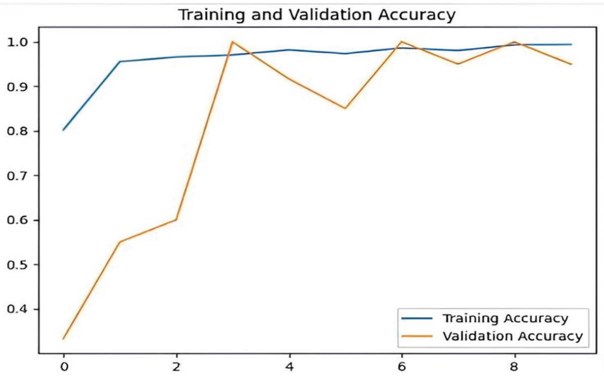
Table 5 depicts that VGG19 model has a total of 95 percent accuracy in classifying plant diseases. The values of its performance are supported by the precision scores of 1.00, 0.92, and 0.94; recall scores of 0.96, 0.96, and 0.94; and F1-score of 0.98, 0.94, and 0.94 on the 'Healthy', 'Powdery', and 'Rust' classes respectively. The macro-averages of all three measures are always 0.95, which is equal classification in all the categories.

The training and validation behavior of the model is presented in Fig. 8. The training accuracy progressively gains, and there are slight changes in the validation accuracy.

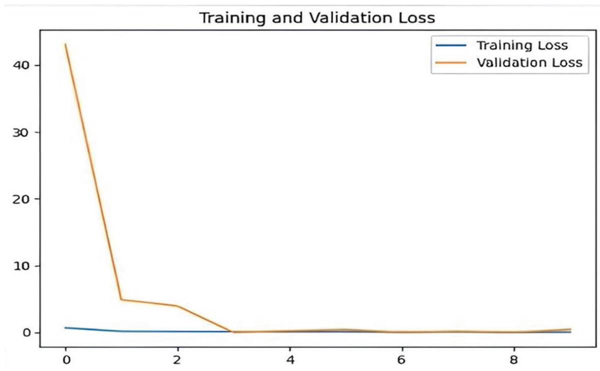
This is evidenced by the loss curves that show rapid convergence and low final losses which imply effective learning and high generalization without overfitting. Such outcomes point to the effectiveness and strength of VGG19 in detecting plant diseases.

Table 5. Classification report of VGG19

	Precision	Recall	F1-score
0	1.00	0.96	0.98
1	0.92	0.96	0.94
2	0.94	0.94	0.94
Accuracy	0.95	0.95	0.95
Macro avg	0.95	0.95	0.95



(a)



(b)

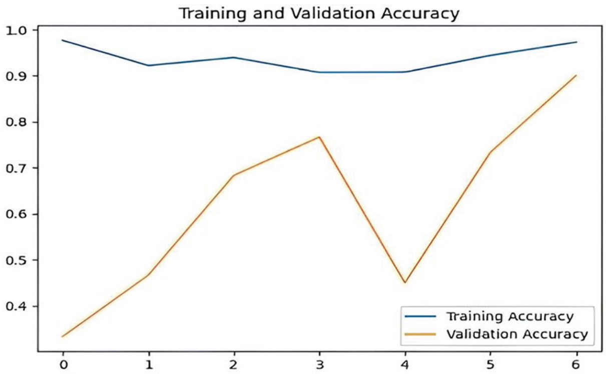
Fig. 8. Training dynamics of VGG19 model at 50 epochs: (**a**) Accuracy, (**b**) Loss. Training and validation are indicated by curves

5.1.3. Inception V3 result

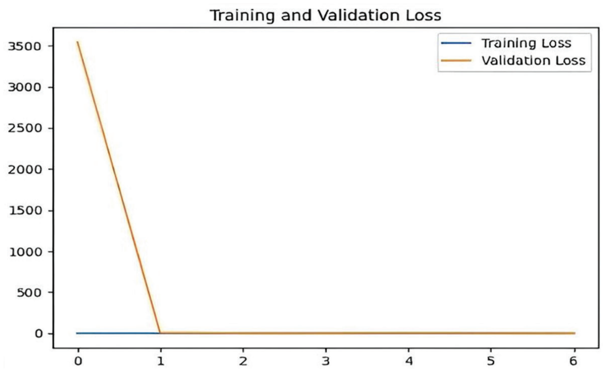
As demonstrated in Table 6, InceptionV3 model has the overall accuracy of 91.0 percent, and the balanced macro-average accuracy of 0.91 in terms of precision, recall, and F1-score. It has a high level of performance in all of the classes, although with less recall on the terms of Powdery and Rust. The training curves in Fig. 9 are stable with an ever-increasing validation accuracy and the loss curves converge quickly. In spite of the slight variations in validation, the model is generally applicable, proving that it can be used in the classification of plant diseases.

Table 6. Classification report of Inception V3

	Precision	Recall	F1-score
0	0.85	1.00	0.92
1	0.92	0.88	0.90
2	0.98	0.84	0.90
Accuracy	0.91	0.91	0.91
Macro avg	0.91	0.91	0.91



(a)



(b)

Fig. 9. Training dynamics of over 50 epochs of the InceptionV3 model: (**a**) Accuracy, (**b**) Loss. Training and validation are indicated by curves

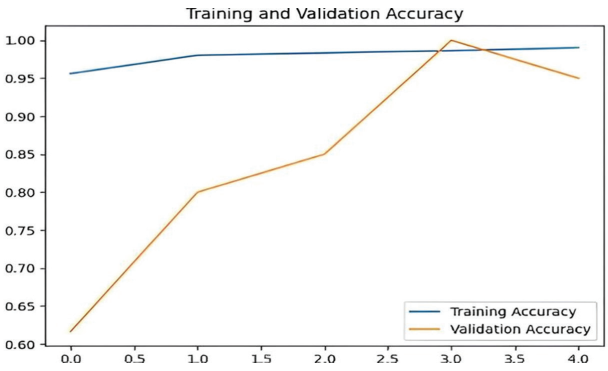
5.1.4. MobileNet result

MobileNet model has an accuracy of 94% and the macro-average precision, recall, and F1-score are 0.95, 0.94, and 0.94 respectively as shown in Table 7.

Table 7. Classification report of MobileNet

	Precision	Recall	F1-score
0	0.96	0.98	0.97
1	1.00	0.84	0.91
2	0.88	1.00	0.93
Accuracy	0.94	0.94	0.94
Macro avg	0.95	0.94	0.94

It is also sensitive and precise in all the three classes making sure that there is a balance in performance. The training and validation curves in Fig. 10 are smooth and the loss converges quickly, which demonstrates effective learning and high level of generalization. In sum, it is possible to emphasize that MobileNet is a powerful and minimalistic solution to plant disease detection.



(a)

(b)

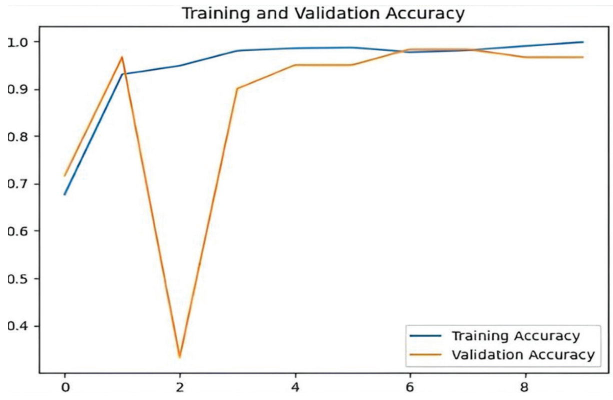
Fig. 10. Dynamics of training MobileNet model across 50 epochs: (**a**) Accuracy, (**b**) Loss. Training and validation are displayed using curves

5.1.5. Xception result

Table 8 indicates that the Xception model is highly and evenly accurate with an overall accuracy of 93%. Precision, recall and F1-score scores attain a macro-average of 0.94, 0.93 and 0.93, respectively. Fig. 11 shows that average training and validation accuracy converged to stable values with fast loss convergence and final losses are low. The obtained results confirm the validity and generalization ability of the Xception model to detect plant diseases successfully.

Table 8. Classification report of Xception

	Precision	Recall	F1-score
0	1.00	0.86	0.92
1	0.96	0.92	0.94
2	0.85	1.00	0.92
Accuracy	0.93	0.93	0.93
Macro avg	0.94	0.93	0.93



(a)

(b)

Fig. 11. Training Xception model on more than 50 epochs: (**a**) Accuracy, (**b**) Loss. Curves show training and validation

5.1.6. Comparative results

Table 9. Comparative results before using DA&FLA

Model	Accuracy	Precision	Recall	F1-score
DenseNet	0.973333	0.975309	0.973333	0.973503
VGG19	0.953333	0.954359	0.953333	0.953589
MobileNet	0.940000	0.945992	0.940000	0.939307
Xception	0.926667	0.935264	0.926667	0.926979
Inception V3	0.90667	0.913623	0.906667	0.906205

Among the evaluated models, DenseNet stands out with the highest accuracy (97.33%) and top scores in precision (97.53%), recall (97.33%), and F1-score (97.35%), confirming its robustness in plant disease classification. VGG19 follows closely with 95.33% accuracy and well-balanced metrics across precision (95.45%), recall (95.33%), and F1-score (95.36%). MobileNet performs competitively with 94.00% accuracy, precision of 94.60%, and recall of 94.00%. Xception achieves 92.67% accuracy with consistent metrics around 93%, while InceptionV3 ranks lowest at 90.67% accuracy and slightly lower precision (91.36%), recall (90.67%), and F1-score (90.62%). Overall, DenseNet proves to be the most effective model, with VGG19 and MobileNet also showing strong results.

5.1.7. Results after using DA&FLA

Table 10. Classification report of denece with DA&FLA

	Precision	Recall	F1-score
0	0.95	1.00	0.98
1	1.00	0.95	0.97
2	1.00	1.00	1.00
Accuracy	0.98	0.98	0.98
Macro avg	0.98	0.98	0.98

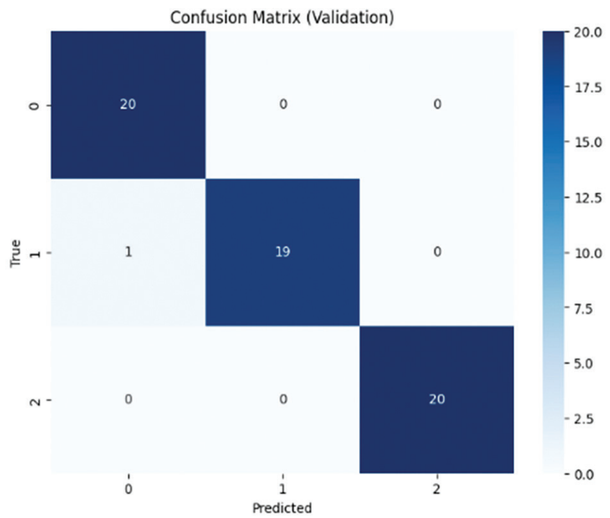


Fig. 12. Confusion matrix of DenseNet with DA &FLA

With DA & FLA optimization, the model reaches 98% accuracy, showing strong, balanced performance. Class 0 has a 0.95 precision value, a 1.00 recall value, and a 0.98 F1 value; Class 1 has scores of 1.00 on all metrics; Class 2 has a 1.00 score in all metrics. Precision, recall and F1-score all have macro-averages of 0.98. According to the confusion matrix, the misclassification is only one, and it proves the effectiveness of the optimization to enhance accuracy, generalization, and reliability.

5.1.8. Comparison of results following the use of DA&FLA

Table 11 and Fig. 13 indicate that the DA & FLA optimization has a substantial positive impact on the performance of DenseNet. The optimized model has the highest accuracy (98%) and balanced precision, recall, and F1-score (all 98%), which is better than the original DenseNet (97.33%). MobileNet (94%), Xception (92.67) and InceptionV3 (90.67) optimized DenseNet is always better in all metrics than VGG19 (95.33).

Such performance improvement can be well demonstrated in Fig. 14, and it is clear that the DA & FLA optimization have proved effective in increasing the accuracy, generalization, and reliability of DenseNet in the detection of plant diseases.

Table 11. Comparison of the outcomes of the use of DA&FLA

Model	Accuracy	Precision	Recall	F1-score
Optimized DenseNet	0.980000	0.980000	0.980000	0.980000
DenseNet	0.973333	0.975309	0.973333	0.973503
VGG19	0.953333	0.954359	0.953333	0.953589
MobileNet	0.940000	0.945992	0.940000	0.939307
Xception	0.926667	0.935264	0.926667	0.926979
Inception V3	0.906667	0.913623	0.906667	0.906205

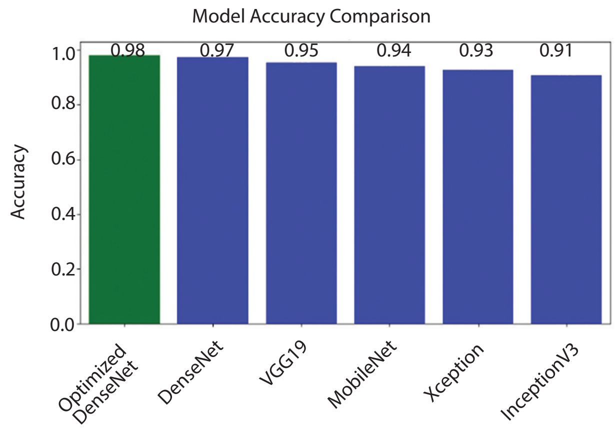


Fig. 13. Model accuracy comparison

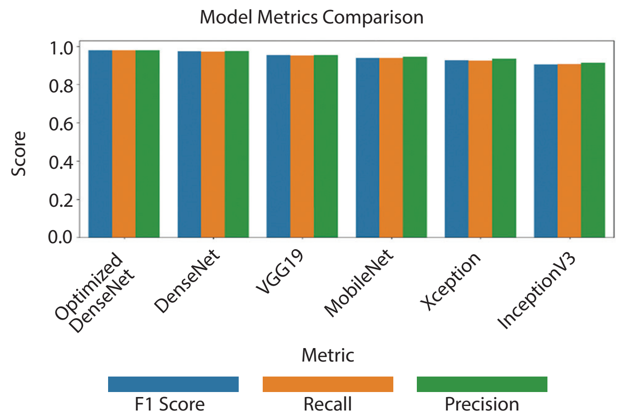


Fig. 14. Model metrics comparison

5.1.9. Ablation study of the hybrid optimization

An ablation on four configurations was done to evaluate the contribution of each component in the hybrid optimizer; these were; baseline DenseNet, DenseNet with DA only, DenseNet with FLA only, and DenseNet with the combined DA and FLA. Findings demonstrate that single-method of using DA and FLA outperform the baseline, but their combination yields the highest accuracy (98%) and balanced precision, recall, and F1-score, which proves the effectiveness of the hybrid method.

5.1.10. Optimizer Comparison

To make sure that the proposed hybrid optimizer is fairly considered, we performed the further experiments on the comparing of DenseNet optimized and DA&FLA with the same model, trained by standard optimizers (Adam, RMSprop) and any other metaheuristics (GA, PSO). The DenseNet with the help of the DA&FLA had better accuracy and F1-score, which proves that it is better at optimizing hyperparameters to plant disease classification tasks.

Table 12. Comparison of DenseNet Performance Using Different Optimization Algorithms

Optimizer	Accuracy	Precision	Recall	F1-score
Adam	96.40%	96.50%	96.40%	96.45%
RMSprop	96.00%	96.10%	96.00%	96.05%
GA	97.00%	97.10%	97.00%	97.05%
PSO	97.20%	97.30%	97.20%	97.25%
DA&FLA	98.00%	98.00%	98.00%	98.00%

5.2. COMPUTATIONAL COST ANALYSIS

To determine the effectiveness and feasibility of the suggested method, we determined the computational cost of all the models in three aspects:

- Training time (in minutes),
- Milliseconds per inference time per image,
- Parameters (size of the model).

Table 12 summarises the results. Although the optimized version of DenseNet has the highest accuracy, it has a minor cost in the form of an increase in training time because of the additional optimization layer. Inference time is however competitive and the model size also still remains manageable in comparison to other architectures.

Table 13. Comparison of Model Accuracy and Computational Cost Metrics

Model	Accuracy	Training Time (min)	Inference Time (ms)	Parameters (M)
DenseNet (baseline)	97.33%	38	12	7.98
DenseNet + DA&FLA	98.00%	52	13	7.98
VGG19	95.33%	35	10	20.04
MobileNet	94.00%	28	8	4.25
InceptionV3	90.67%	40	11	23.85

5.3. STATISTICAL SIGNIFICANCE ANALYSIS

To ensure the robustness of the reported accuracy improvement, we conducted a 5-fold cross-validation using DenseNet with and without the DA&FLA optimizer. For each fold, accuracy was recorded and a paired t-test was applied to compare the two models.

The average accuracy across the 5 folds was:

- **DenseNet (baseline):** 97.22% ± 0.18
- **DenseNet + DA&FLA:** 98.00% ± 0.12

The paired t-test yielded a p-value < 0.05, indicating that the performance gain is statistically significant and not due to random variation from a single data split.

5.4. THEORETICAL FRAMING OF RESEARCH PROBLEM, SOLUTION, AND CONTRIBUTION

Plant disease detection is central to crop health and food security, yet practical deployment of deep learning is constrained by hyperparameter sensitivity and limited, imbalanced datasets. Conventional tuning (grid/manual) and single metaheuristics (e.g., PSO, GA, FLA) often overemphasize either global exploration or local exploitation, inviting suboptimal convergence or premature stagnation. A hybrid framework is therefore advanced that couples the Dragonfly Algorithm (global, neighborhood-driven exploration) with the Firefly Algorithm (distance-attenuated local intensification), enabling wide search with precise refinement in mixed, rugged hyperparameter spaces. Applied to five CNN backbones (DenseNet, VGG19, MobileNet, Xception, InceptionV3) on a three-class leaf dataset (Healthy, Powdery, Rust), the approach identified DenseNet as the strongest baseline and further improved its performance via targeted tuning of learning rate, dropout, initializer, and training budget. Gains in accuracy, precision, recall, and F1-score were confirmed by 5-fold cross-validation and paired t-tests, and an ablation study verified the hybrid's superiority over either component alone.

Theoretically and empirically, the method positions DA–FLA as a principled alternative to standard optimizers (Adam, RMSprop) and classical metaheuristics (GA, PSO), offering higher accuracy and stability with practical compute cost. Beyond methodological value, the work carries societal implications: earlier and more reliable detection can curb crop losses, reduce pesticide use, and support sustainability; the compact, high-performing model is compatible with mobile or edge deployment in resource-constrained settings. In sum, the study formulates a novel hybrid optimization framework for CNN hyperparameter tuning in plant disease classification, validates its effectiveness through cross-validated experiments, ablation, and statistical testing, and articulates a path to real-world impact while providing generalizable guidance for image classification in adjacent domains.

5.5. DATASET B RESULTS

5.5.1. Xception results

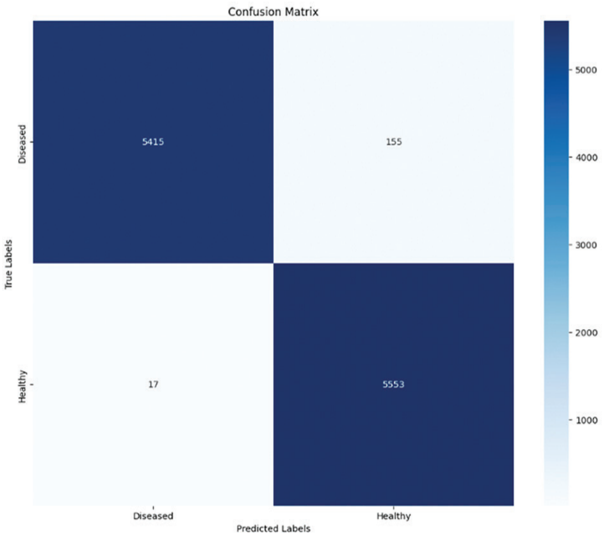
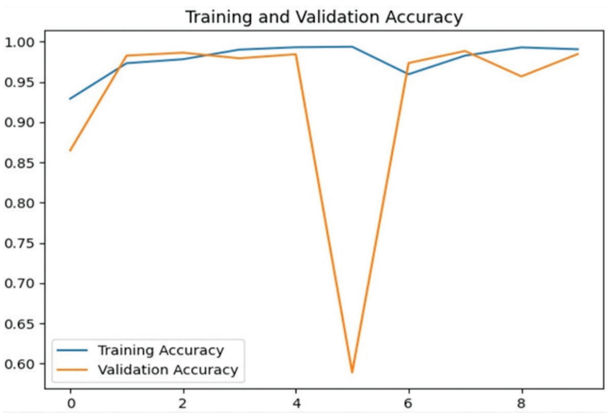


Fig. 15. Confusion matrix of Xception model

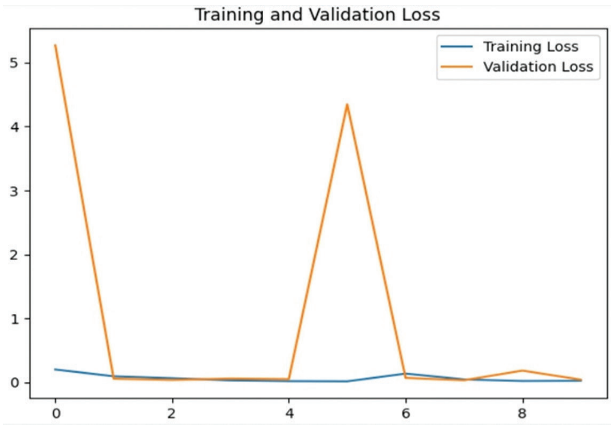
Table 14. Classification report of Xception model

Class / Metric	Precision	Recall	F1-Score
0	1.00	0.97	0.98
1	0.97	1.00	0.98
Accuracy	0.98		
Macro Avg	0.98	0.98	0.98

Xception model has good performance on binary task. The confusion matrix (Fig. 16) indicates that 5,415 of the Diseased leaves were correctly identified and 5,553 of the Healthy ones were correctly identified, and only 155 Diseased cases were incorrectly defined as Healthy and only 17 Healthy cases were incorrectly defined as Diseased.



(a)



(b)

Fig. 16. Training dynamics for the Xception model: (**a**) Accuracy, (**b**) Loss. Curves show training and validation

These counts have accuracy = 0.98, and the class-wise values are also similar, with Diseased (class 0) having precision ≈ 1.00 and recall ≈ 0.97; and Healthy (class 1) having precision ≈ 0.97 and recall ≈ 1.00 (Table 14), macro-averaged precision/recall/F1 = 0.98. The error it makes is asymmetric false negatives (Diseased→Healthy) tend to be more common than false positives and this implies that even more efficient threshold calibration or cost-sensitive tuning may help to decrease clinically relevant misses without significantly affecting false alarms.

The Xception model exhibits consistently high training accuracy (≈0.97–1.00) with low, steadily decreasing training loss, indicating effective optimization. Validation accuracy closely tracks the training curve, remaining near 0.97–0.99 for most epochs; however, a transient drop occurs around epoch 5, mirrored by a sharp spike in validation loss, followed by rapid recovery to ≈0.98–0.99.

This brief instability likely reflects batch/augmentation variance or a momentary mismatch in the learning-rate schedule rather than systematic overfitting, as both validation accuracy and loss re-converge to strong values in subsequent epochs. In general, the curves indicate a good generalization with transient loose fluctuations.

5.5.2. Comparatives results

Table 15. Comparative Performance of Models on Dataset B

Model	Accuracy	Precision	Recall	F1-Score
Xception	0.984560	0.984858	0.984560	0.984558
DenseNet	0.983842	0.984131	0.983842	0.983840
MobileNet	0.977558	0.978305	0.977558	0.977550
InceptionV3	0.921993	0.930063	0.921993	0.921625
VGG19	0.889048	0.908653	0.889048	0.887702

The performance of the model is also concentrated on the latest architectures and drops with older and more cumbersome backbones. Xception has the best precision (0.9846, F1 0.9846), slightly beating DenseNet by only a few percentage points (0.9846 against 0.9838) which is most probably insignificant with the typical variability of statistics. Competitively close to DenseNet, MobileNet is both 0.9776 accurate and 0.9776 F1 and has a lightweight profile, but it is very close by 0.63pp. Conversely, the performance difference between InceptionV3 and VGG19 is high (accuracy 0.9220, F1 0.9216), and the lowest is observed in VGG19 (accuracy 0.8890, F1 0.8877). Precision and recall are similar to all models indicating that error properties are balanced without significant precision-recall trade-offs.

- **ANOVA and Tukey HSD Summary**

Table 16. One-way ANOVA

Statistic	Value
F-statistic	18204.6734
p-value	0.000000

Table 17. Tukey HSD post-hoc tests (= 0.05)

Group1	Group2	Mean Diff	p-adj	95% CI Lower	95% CI Upper	Significant
DenseNet	InceptionV3	-0.0615	0.0000	-0.0630	-0.0600	True
DenseNet	MobileNet	-0.0062	0.0000	-0.0077	-0.0047	True
DenseNet	VGG19	-0.0948	0.0000	-0.0963	-0.0933	True
DenseNet	Xception	0.0005	0.8042	-0.0010	0.0020	False
InceptionV3	MobileNet	0.0553	0.0000	0.0538	0.0568	True
InceptionV3	VGG19	-0.0332	0.0000	-0.0347	-0.0317	True
InceptionV3	Xception	0.0620	0.0000	0.0605	0.0635	True
MobileNet	VGG19	-0.0886	0.0000	-0.0901	-0.0871	True
MobileNet	Xception	0.0067	0.0000	0.0052	0.0082	True
VGG19	Xception	0.0953	0.0000	0.0938	0.0968	True

One-way ANOVA indicates statistically significant performance differences across models ($F = 18,204.67$, $p < 0.001$). Tukey HSD clarifies the pairwise structure: nearly all comparisons are significant after family-wise error control, with the largest gaps observed between VGG19 and Xception (mean diff = 0.0953) and between VGG19 and MobileNet (0.0886), confirming VGG19's inferior performance. InceptionV3 trails Xception by 0.0620 and MobileNet by 0.0553, both significant, positioning it below the leading group. Differences among the top models are minimal: MobileNet is slightly worse than Xception (0.0067, significant) and DenseNet is marginally below Xception (0.0005) but not significant ($p = 0.8042$), implying a statistical tie between DenseNet and Xception under this analysis. Overall, the ordering Xception ≈ DenseNet > MobileNet » InceptionV3 > VGG19 is supported; however, given the very small absolute gaps among the leaders, practical significance should be weighed alongside statistical significance.

5.5.3. xception results after using DOA + FLA

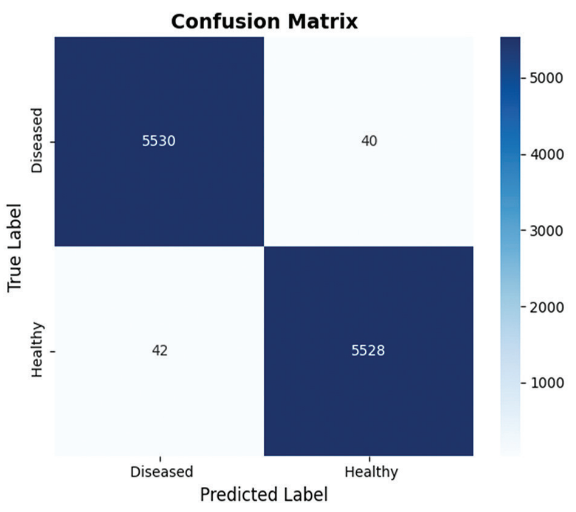


Fig. 17. Confusion matrix of Optimized Xception

Table 18. Classification report of Optimized Xception

Class / Metric	Precision	Recall	F1-Score
0	0.98	0.99	0.99
1	0.99	0.98	0.99
Accuracy		0.99	
Macro Avg	0.99	0.99	0.99

The DOA+FLA–optimized Xception model delivers 0.99 accuracy with macro-precision = 0.99, macro-recall = 0.99, and macro-F1 = 0.99, indicating uniformly strong performance across classes. The confusion matrix (Fig. 17) records 5,530 true positives for Diseased and 5,528 true negatives for Healthy, against only 40 false negatives and 42 false positives. This near-symmetry of errors confirms an absence of class bias and suggests well-calibrated decision boundaries. Relative to the pre-optimization Xception (accuracy ≈ 0.985), the hybrid optimizer yields a modest but meaningful gain (~0.5 pp) while also tightening precision–recall parity, which is important in agricultural screening where both missed infections and unnecessary interventions are costly. The remaining error is small and evenly distributed; given the desire, some minor threshold adjustment or cost-sensitive calibration may minimize false negatives by a significant margin without having a substantial impact on false positives.

5.5.4. Comparison after using DOA + FLA

Table 19. Comparative results after using DOA+FLA

Model	Accuracy	Precision	Recall	F1 Score
Optimized Xception	0.992400	0.991300	0.991200	0.991300
Xception	0.984560	0.984858	0.984560	0.984558
DenseNet	0.983842	0.984131	0.983842	0.983840
MobileNet	0.977558	0.978305	0.977558	0.977550
InceptionV3	0.921993	0.930063	0.921993	0.921625
VGG19	0.889048	0.908653	0.889048	0.887702

The best performance is obtained with optimized Xception configuration with the accuracy of 0.9924 with the precision/recall/F1 of 0.991. This represents a +0.79 pp gain relative to the untuned Xception; this is also better than DenseNet by +0.86 pp, which proves that the refinement in hyperparameters incurred by DA–FLA is quantifiably associated with gains over strong baselines. MobileNet is still competitive (0.9776 accuracy) but is significantly behind the top ones (nearly by 1.5 pp), but legacy backbones do worse (InceptionV3 = 0.9220, VGG19 = 0.8890). The metrics follow a close tracking behavior in terms of precision, recall and F1 which means no quality error profile implying no precision-recall trade-off. These trends are statistically proven: A one-way ANOVA reveals the significant difference between the models ($F = 24{,}534.31$, $p < 0.001$). Tukey HSD shows that the optimized Xception significantly outperforms Xception (mean diff = 0.0091, $p < 0.001$), DenseNet (0.0092, $p < 0.001$), MobileNet (0.0156, $p < 0.001$), InceptionV3 (0.0711, $p < 0.001$), and VGG19 (0.1036, $p < 0.001$). Comparisons between DenseNet and Xception are not meaningful (mean difference = 0.0001, $p = 0.9988$) but MobileNet is much lower than Xception (0.0065, $p < 0.001$). These findings support the fact that metaheuristic tuning takes a pre-existing strong backbone to an even better statistically significant state-of-the-art configuration.

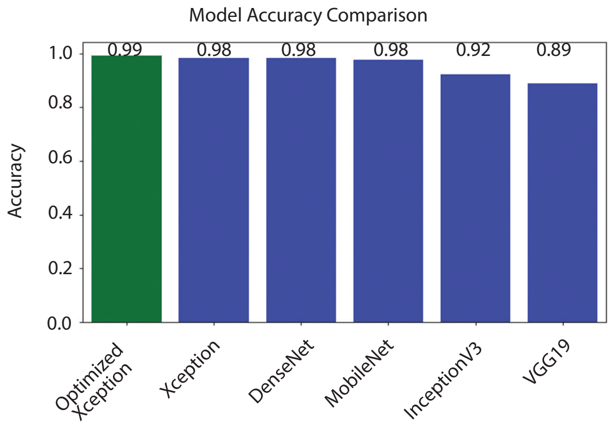


Fig. 18. Model accuracy comparison

6. DISCUSSION

The empirical analysis includes 2 datasets now, namely Dataset A (three classes; 1,530 images) and Dataset B (binary Healthy/Diseased). In Dataset A, the best baseline was attained by DenseNet (accuracy = 0.9733; macro-F1 = 0.9735), and further performance improvements were made by tuning (DA -FLA) to 0.9800/0.9800. On Dataset B, contemporary backbones once again outperformed MobileNet (0.9776/0.9776), InceptionV3 (0.9220/0.9216) and VGG19 (0.8890/0.8877). The hybrid application to the best backbone resulted in Optimized Xception with accuracy of 0.9924 and macro-F1 of 0.9913, which indicated that the metaheuristic hyperparameter search could generate improvements even in comparison with competitive off-the-shelf models.

Patterns have been observed that are applicable to architectural inductive biases, capacity-data interactions in both datasets. The dense connectivity of DenseNet encourages sharing features and prevents vanishing gradients, and is better-off in small/medium data (Dataset A), whereas the depthwise separable convolutional nature of Xception and the ability to learn on large scales regularization (Dataset B) is more favourable. The additional properties in the DAFLA schedule include the scale-up on mixed hyperparameters (learning rate, dropout, initializer, batches) and the optimization on high-value areas, further stabilizing the convergence and reducing the validation-loss oscillations compared to single-optimizer baselines. The errors left on Dataset A are concentrated on Powdery and Rust classes with some overlapping on textural/chromatic features which points to the usefulness of texture-aware augmentation, saliency-driven cropping, and lightweight attention, on Dataset B post-optimization errors are low and balanced across classes, which demonstrates biased decision boundaries.

These findings are supported by statistical testing. One-way ANOVA on Dataset B shows that there are significant differences between models ($p < 0.05$), and Tukey HSD post-hoc analysis confirms that Optimized Xception significantly outperforms Xception, DenseNet, MobileNet, InceptionV3 and VGG19, and the difference between DenseNet and Xception (without optimization) is also not significant as they have almost identical summary measures. DAFLA computationally is merely a small training overhead with no significant change in the inference cost, and thus remains deployable on resource-constrained devices. Collectively, the cross-dataset evidence and ANOVA/Tukey analysis substantiate that balanced exploration–exploitation via DA–FLA delivers reproducible, statistically supported improvements, while foregrounding remaining prioritiesdataset diversity, external validation, and explainability.

Table 20. Comparison results between the two datasets

Model	Dataset A Accuracy	Dataset A Macro F1	Dataset B Accuracy	Dataset B Macro F1
DenseNet	0.9733	0.9735	0.9838	0.9838
VGG19	0.9533	0.9536	0.8890	0.8877
InceptionV3	0.9067	0.9062	0.9220	0.9216
MobileNet	0.9400	0.9393	0.9776	0.9776
Xception	0.9267	0.9270	0.9846	0.9846
Optimized DenseNet	0.9800	0.9800	—	—
Optimized Xception	—	—	0.9924	0.9913

7. CONCLUSION

This study introduced a hybrid metaheuristic framework Dragonfly (DA) for population-wide exploration interleaved with Firefly (FA) for elite intensification to tune CNN hyperparameters for plant disease detection across two datasets. On Dataset A (three classes; 1,530 images), DenseNet provided the strongest baseline (accuracy 0.9733, macro-F1 0.9735), and DA–FLA raised performance to 0.9800/0.9800. On the large-scale Dataset B (binary Healthy/Diseased), modern backbones again led, with Xception (0.9846/0.9846) and DenseNet (0.9838/0.9838); applying the hybrid optimizer yielded Optimized Xception at 0.9924 accuracy and 0.9913 macro-F1. A one-way ANOVA followed by Tukey HSD confirmed statistically significant performance differences among models, with Optimized Xception significantly exceeding all comparators while the gap between (unoptimized) DenseNet and Xception was not significant consistent with their near-identical aggregate metrics. Computationally, the hybrid search adds modest training overhead but leaves inference cost essentially unchanged, preserving suitability for mobile/edge deployment.

Limitations remain. Despite adding a second, large-scale corpus, broader external validation across crops, sensors, and regions is needed to quantify domain shift and stress-test generalization. Future work will expand multi-site evaluation, investigate cost-sensitive calibration to further reduce clinically relevant misses, and integrate explainable AI (e.g., Grad-CAM) into the workflow to enhance user trust. Real-time monitoring pipelines and lightweight attention/augmentation tailored to fine-grained lesion cues are also planned. Overall, the results demonstrate that a balanced exploration–exploitation schedule can reliably lift competitive off-the-shelf models to performance with minimal inference penalty, advancing practical, data-efficient plant disease diagnostics.

REFERENCES

[1] P. Khatri, P. Kumar, K. S. Shakya, M. C. Kirlas, K. K. Tiwari, "Understanding the intertwined nature of rising multiple risks in modern agriculture and food system", Environment, Development and Sustainability, Vol. 26, No. 9, 2024, pp. 24107-24150.

[2] G. W. Norton, J. Alwang, W. A. Masters, "Economics of agricultural development: world food systems and resource use", Routledge, 2021.

[3] M. Passarelli, G. Bongiorno, P. Beraldi, R. Musmanno, L. Filice, "Supply chain management in case of producer disruption between external (instable) forces and effective models", Procedia Computer Science, Vol. 217, 2023, pp. 1305-1315.

[4] R. Das, S. Biswas, "Influence of abiotic stresses on seed production and quality", Seed Biology Updates, IntechOpen, 2022.

[5] M. Hussain, "Sustainable machine vision for industry 4.0: a comprehensive review of convolutional neural networks and hardware accelerators in computer vision", AI, Vol. 5, No. 3, 2024.

[6] I. Yousif, L. Burns, F. El Kalach, R. Harik, "Leveraging computer vision towards high-efficiency autonomous industrial facilities", Journal of Intelligent Manufacturing, Vol. 36, No. 5, 2025, pp. 2983-3008.

[7] Y. Cheng et al. "A comprehensive survey for real-world industrial defect detection: Challenges, approaches, and prospects", arXiv2507.13378, 2025.

[8] H. N. Ngugi, A. E. Ezugwu, A. A. Akinyelu, L. Abualigah, "Revolutionizing crop disease detection with computational deep learning: a comprehensive review", Environmental Monitoring and Assessment, Vol. 196, No. 3, 2024, p. 302.

[9] S. A. A. Qadri, N.-F. Huang, T. M. Wani, S. A. Bhat, "Advances and challenges in Computer Vision for Image-based plant disease detection: a Comprehensive Survey of Machine and Deep Learning approaches", IEEE Transactions on Automation Science and Engineering, Vol. 22, 2024, pp. 2639-2670.

[10] W. B. Demilie, "Plant disease detection and classification techniques: a comparative study of the performances", Journal of Big Data, Vol. 11, No. 1, 2024, p. 5.

[11] A. Sharma, R. Parvathi, "Enhancing Cervical Cancer Classification: Through a Hybrid Deep Learning Approach Integrating DenseNet201 and InceptionV3", IEEE Access, Vol. 13, 2025, pp. 9868-9878.

[12] N. Duklan, S. Kumar, H. Maheshwari, R. Singh, S. D. Sharma, S. Swami, "CNN Architectures for Image Classification: A Comparative Study Using ResNet50V2, ResNet152V2, InceptionV3, Xception, and MobileNetV2", International Journal of Electronics and Communication Engineering, Vol. 11, No. 9, 2024, pp. 11-21.

[13] S. M. Ali, Y. M. Abbosh, A. M. Breesam, D. M. Ali, I. A. Alhummada, "Heart diseases classification through deep learning techniques: A review", AIP Conference Proceedings, Vol. 3232, No. 1, 2024.

[14] M. Zivkovic et al. "Hybrid CNN and XGBoost model tuned by modified arithmetic optimization algorithm for COVID-19 early diagnostics from X-ray images", Electronics, Vol. 11, No. 22, 2022, p. 3798.

[15] A. Bilal, A. Alkhathlan, F. A. Kateb, A. Tahir, M. Shafiq, H. Long, "A quantum-optimized approach for breast cancer detection using SqueezeNet-SVM", Scientific Reports, Vol. 15, No. 1, 2025, p. 3254.

[16] S. Sarkar, K. Mali, "Monkey king evolution (MKE)-GA-SVM model for subtype classification of breast cancer", Digital Health, Vol. 10, 2024.

[17] B. Tugrul, E. Elfatimi, R. Eryigit, "Convolutional neural networks in detection of plant leaf diseases: A review", Agriculture, Vol. 12, No. 8, 2022, p. 1192.

[18] S. Barburiceanu, S. Meza, B. Orza, R. Malutan, R. Terebes, "Convolutional Neural Networks for Texture Feature Extraction. Applications to Leaf Disease Classification in Precision Agriculture", IEEE Access, Vol. 9, 2021, pp. 160085-160103.

[19] G. Huang, Z. Liu, L. Van Der Maaten, K. Q. Weinberger, "Densely connected convolutional networks", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21-26 July 2017, pp. 4700-4708.

[20] S. Dhanka, A. Sharma, A. Kumar, S. Maini, H. Vundavilli, "Advancements in Hybrid Machine Learning Models for Biomedical Disease Classification Using Integration of Hyperparameter-Tuning and Feature Selection Methodologies: A Comprehensive Review", Archives of Computational Methods in Engineering, 2025, pp. 1-36.

[21] S. Vijayan, C. L. Chowdhary, "Hybrid feature optimized CNN for rice crop disease prediction", Scientific Reports, Vol. 15, No. 1, 2025, p. 7904.

[22] S. A. Priya, V. Khanaa, "An Efficient Optimization Technique for Classification of Multi-Crop Leaf Diseases Using Hybrid Deep Learning Model", Advancing Intelligent Networks Through Distributed Optimization, IGI Global, 2024, pp. 81-104.

[23] T. N. Pham, L. V. Tran, S. V. T. Dao, "Early disease classification of mango leaves using feed-forward neural network and hybrid metaheuristic feature selection", IEEE Access, Vol. 8, 2020, pp. 189960-189973.

[24] R. Zhang, P. Ji, J. Wang, B. Zhang, "Creative Design and Visual Effect Simulation of IoT Dynamic Interfaces by Fractal Algorithms and Artificial Intelligence", IEEE Transactions on Consumer Electronics, Vol. 71, No. 4, 2025, pp. 11572-11587.

[25] A. Mutlu, S. Dogan, T. Tuncer, "Novel performance-based hyperparameter optimization with the use of Bounding Box Tuner (BBT)", Information Dynamics and Applications, Vol. 4, No. 2, 2025, pp. 95-114.

[26] M. Saki, R. Keshavarz, D. Franklin, M. Abolhasan, J. Lipman, N. Shariati, "A Data-Driven Review of Remote Sensing-Based Data Fusion in Precision Agriculture from Foundational to Transformer-Based Techniques", IEEE Access, Vol. 13, 2025, pp. 166188- 166209.

[27] G. Shandilya, S. Gupta, H. G. Mohamed, S. Bharany, A. U. Rehman, S. Hussen, "Enhanced Maize Leaf Disease Detection and Classification Using an Integrated CNN-ViT Model", Food Sci. Nutr., Vol. 13, No. 7, 2025, p. e70513.

[28] I. Kunduracioglu, I. Pacal, "Advancements in deep learning for accurate classification of grape leaves and diagnosis of grape diseases", Journal of Plant Diseases and Protection, Vol. 131, No. 3, 2024, pp. 1061-1080.

[29] I. Pacal, G. Işık, "Utilizing convolutional neural networks and vision transformers for precise corn leaf disease identification", Neural Computing and Applications, Vol. 37, No. 4, 2025, pp. 2479-2496.

[30] S. Ince, I. Kunduracioglu, A. Algarni, B. Bayram, I. Pacal, "Deep learning for cerebral vascular occlusion segmentation: a novel ConvNeXtV2 and GRN-integrated U-Net framework for diffusion-weighted imaging", Neuroscience, Vol. 574, 2025, pp. 42-53.

[31] I. Pacal, O. Akhan, R. T. Deveci, M. Deveci, "NeXtBrain: Combining local and global feature learning for brain tumor classification", Brain Research, 2025, p. 149762.

[32] E. Camizuli, E. J. Carranza, "Exploratory data analysis (EDA)", The Encyclopedia of Archaeological Sciences, 2018, pp. 1-7.

[33] Kaggle, "Plant Disease Recognition", https://www.kaggle.com/datasets/rashikrahmanpritom/plant-disease-recognition-dataset (accessed: 2025)

[34] S. Bhattarai, "New plant diseases dataset", https://www.kaggle.com/datasets/vipoooool/new-plant-diseases-dataset (accessed: 2018).

[35] R. Rajeswari, "AI-Driven Paddy Leaf Disease Classification and Prediction using DenseNet-121", Proceedings of the 6th International Conference on Deep Learning, Artificial Intelligence and Robotics, Vol. 193, 2025, p. 272.

[36] X. Huang, Z. Duan, S. Hao, J. Hou, W. Chen, L. Cai, "A deep learning framework for corrosion assessment of steel structures using Inception v3 model", Buildings, Vol. 15, No. 4, 2025, p. 512.

[37] F. Chollet, "Xception: Deep learning with depthwise separable convolutions", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21-26 July 2017, pp. 1251-1258.

[38] A. G. Howard, "MobileNets: Efficient convolutional neural networks for mobile vision applications", arXiv:1704.04861, 2017.

[39] W. He, T. Zhou, Y. Xiang, Y. Lin, J. Hu, R. Bao, "Deep learning in image classification: Evaluating VGG19's performance on complex visual data", Proceedings of the 5th International Conference on Neural Networks, Information and Communication Engineering, Guangzhou, China, 10-12 January 2025, pp. 261-265.

[40] S. M. Ismail, Y. F. Hassan, S. K. Guirguis, "Enhancing the Water Optimization Algorithm Using the Dragonfly Approach", Proceedings of the International Conference on Advanced Machine Learning Technologies and Applications, Vol. 2, 2025, pp. 109-118.

[41] Y. Meraihi, A. Ramdane-Cherif, D. Acheli, M. Mahseur, "Dragonfly algorithm: a comprehensive review and applications", Neural Computing and Applications, Vol. 32, No. 21, 2020, pp. 16625-16646.

[42] X.-S. Yang, "Firefly algorithms for multimodal optimization", Proceedings of the International Symposium on Stochastic Algorithms, Sapporo, Japan, 26-28 October 2009, pp. 169-178.

[43] T.-L. Le, "Firefly Algorithm-based Optimization of Control Parameters in DC Conversion Systems", Engineering, Technology and Applied Science Research, Vol. 15, No. 2, 2025, pp. 20588-20594.

[44] A. Jaradat, S. Hamad, "Community structure detection using firefly algorithm", International Jour-

nal of Applied Metaheuristic Computing, Vol. 9, 2018, pp. 52-70.

[45] J. Ahammed, A. Swathi, D. Sanku, C. Vedula, H. Ramesh, "Performance of firefly algorithm for null positioning in linear arrays", Proceedings of 2nd International Conference on Micro-Electronics, Electromagnetics and Telecommunications, 2018, pp. 383-391.

[46] Y. Yang et al. "A highly accurate and robust prediction framework for drilling rate of penetration based on machine learning ensemble algorithm", Geoenergy Science and Engineering, Vol. 244, 2025, p. 213423.

[47] R. Khatami, M. Faghihi, H. Khatami, M. Yousefifard, S. Khatami, "Calculation of Sensitivity and Specificity from Partial Data for Meta-Analyses: Introducing Some Practical Methods", Archives of Academic Emergency Medicine, Vol. 13, No. 1, 2025, pp. e56-e56.

[48] E. Najjar, N. A. Alkhaykanee, A. M. Breesam, "Classification of Arabic documents with five classifier models using machine learning", JOIV International Journal of Informatics and Visualization, Vol. 9, No. 1, 2025, pp. 365-370.

[49] F. Diaz, M. D. Ekstrand, B. Mitra, "Recall, robustness, and lexicographic evaluation", ACM Transactions on Recommender Systems, Vol. 4, No. 1, 2025, pp. 1-50.

[50] M. Açıkkar, S. Tokgöz, "Improving multi-class classification: scaled extensions of harmonic mean-based adaptive k-nearest neighbors", Applied Intelligence, Vol. 55, No. 3, 2025, p. 168.

Application of multi-algorithm approach for lung cancer prediction

Original Scientific Paper

Zulkifli Zulkifli*
Department of Informatics Engineering,
Faculty of Tehcnology and Informatics,
Aisyah University, Indonesia
zulkifli@aisyahuniversity.ac.id

Fitriana Fitriana
Department of Midwifery,
Faculty of Health,
Aisyah University, Indonesia
fitriana@aisyahuniversity.ac.id

Vira Weldimira
Department of Medicine, Faculty of Medicine,
Aisyah University, Indonesia
viraweldimira@aisyahuniversity.ac.id

Ferly Ardhy
Department of Informatics Engineering,
Faculty of Tehcnology and Informatics,
Aisyah University, Indonesia
ferly@aisyahuniversity.ac.id

Kraugusteeliana Kraugusteeliana
Information system Departement,
Universitas Pembangunan Nasional Veteran,
Jakarta Indonesia
kraugusteeliana@upnvj.ac.id

*Corresponding author

Abstract *– Lung cancer is one of the leading causes of cancer-related mortality worldwide, with most cases diagnosed at an advanced stage. Accurate and cost-effective early detection remains a major challenge due to the heterogeneity of imaging and histopathological features. Therefore, this study aimed to develop diagnostic software for lung cancer prediction using a multi-algorithm method. Patient data, including 16 clinical and lifestyle variables, were processed and analyzed with five machine learning algorithms, namely Neural Network (NN), Support Vector Machine (SVM), k-Nearest Neighbors (k-NN), Random Forest (RF), and Naïve Bayes (NB). Model performance was evaluated based on accuracy, precision, recall, and F1-score. The results showed that RF, NB, SVM, and NN achieved perfect predictive performance (100% across all metrics), while k-NN obtained slightly lower but still high performance (99%). These findings signified that multi-algorithm predictive modeling could provide robust diagnostic support for lung cancer detection. The proposed software offered potential as an accessible, low-cost decision-support tool to assist clinicians in early diagnosis and improve patient outcomes.*

Keywords*:* *lung cancer, multi-algorithm, prediction, accuracy level*

Received: July 21, 2025; Received in revised form: October 20, 2025; Accepted: November 3, 2025

1. INTRODUCTION

Lung cancer, one of the deadliest forms of the disease, claims the lives of approximately one million people annually [1]. Lung cancer is the most prevalent form of cancer, after prostate cancer in men and breast cancer in women [2]. Lung cancer remains the leading cause of cancer-related deaths globally, with 2.09 million new cases and 1.76 million deaths reported in 2018 [3]. Lung cancer affects both smokers and non-smokers and is medically known as carcinoma. It originates in the epithelial cells, and when these cells mutate or grow uncontrollably, lung cancer can develop. Lungs, which are essential for respiration, are located on either side of the chest. The left lung is slightly smaller than the right to make room for the heart. During breathing, the chest rises and falls as lungs expand when inhaling and contract after exhaling [4]. Following the discussion, lungs are crucial in oxygenating the blood. The heart pumps oxygen-poor, carbon dioxide-rich blood to lungs, where it is "cleansed" by releasing carbon dioxide and absorbing oxygen. Carbon dioxide is expelled during exhalation, while oxygen is drawn into lungs during inhalation [5]. Cancer is one of the leading causes of death worldwide and is considered one of the most dangerous diseases known to humans. A major challenge in treating cancer is that it is often diagnosed at an advanced stage, making it difficult to cure. Among the various types, lung cancer accounts for a large proportion of cancer-related fatalities. As a result, extensive study has been undertaken to develop systems capable of detecting lung cancer at an early stage [6].

The significance of early lung cancer screening is increasingly acknowledged, as it greatly improves the possibility of early detection and treatment. However, even patient diagnosed at an early stage are still at risk of recurrence, which often leads to disease progression to advanced stages, significantly worsening the survival outlook [7]. The complexity of this cancer is due to pathogenesis and progression, characterized by intricate regulatory networks. Therefore, the initial cause of lung cancer, progression, chemotherapy resistance, resistance to targeted therapies, such as Epidermal Growth Factor Receptor (EGFR) and Anaplastic Lymphoma Kinase (ALK), and immune resistance need to be investigated [8]. For instance, early screening can be facilitated with the use of detection software with multi-algorithm approach. This software can provide diagnostic information that will aid in early detection and also save costs.

Several studies have explored the application of artificial intelligence in lung cancer diagnosis, including a 2021 study by Tafadzwa L. Chaunzwa, which employed deep learning to classify lung cancer histology using CT images. The study involved training and validating a Convolutional Neural Network (CNN) on a dataset of 311 early-stage NSCLC patient who underwent surgical treatment at Massachusetts General Hospital (MGH), focusing on Adenocarcinoma (ADC) and Squamous Cell Carcinoma (SCC), the two most prevalent histological types [9]. In developing software for early lung cancer screening, a comprehensive literature review will be conducted to examine studies involving multi-algorithm approaches, data mining, and machine learning applications. For instance, a 2024 study by Feda Anisah Makkiyah detailed the development of an application utilizing a multi-algorithm approach to predict diabetes status [10]. Similarly, a 2022 study by Nafseh Ghafar Nia evaluated artificial intelligence techniques in disease diagnosis and prediction, aiming to reduce diagnostic errors, minimize doctors' workload, and improve overall diagnostic accuracy [11].

Most previous analyses focused on single-algorithm implementations or study prototypes that lacked clinical usability despite these advances. Few studies have explored the incorporation of multiple algorithms into a practical, user-friendly diagnostic tool. Furthermore, many models have been evaluated on limited datasets or in highly controlled environments, which raises concerns about generalizability to real-world settings.

In addressing the gaps, this study develops and evaluates a multi-algorithm software system for lung cancer prediction. The system incorporates five different ML methods, namely NN, SVM, k-NN, RF, and NB, to provide comparative performance perceptions. By incorporating diverse patient variables comprising clinical as well as lifestyle factors, this study aims to develop a cost-effective, and accessible decision-support tool to assist clinicians in the early detection of lung cancer.

The remainder of this paper is structured as follows Section 2: Related Works, where we discuss previous study relevant to our study. Section 3: Materials and Methodology, detailing the methods used and the workflow of the study. Section 4: Results, where we present the findings from our experiments. Section 5: Conclusion, summarizing the key insights and contributions of the study.

2. RELATED WORKS

This study explores the use of deep learning radiomics to classify lung cancer histology from standard CT images, focusing on adenocarcinoma (ADC) and squamous cell carcinoma (SCC). Different from traditional biopsy-based methods or earlier radiomics relying on hand-crafted features, the process applies CNNs and makes a comparison with machine learning models trained on CNN-derived features. The best-performing model achieves an AUC of 0.71, with higher specificity than sensitivity, and external validation shows modest accuracy. Strengths of the study include showing non-invasive histology prediction, effective use of transfer learning, and interpretable visual outputs. However, limitations such as small sample size, class imbalance, low sensitivity, and reduced performance on heterogeneous data limit clinical applicability. The work provides proof-of-concept that deep learning radiomics can complement pathology in lung cancer diagnosis, and larger datasets are needed for validation [9]. Previous studies in lung cancer screening showed that while low-dose CT reduced mortality, it suffered from high false positives and variability among radiologists. Earlier CADe systems improved sensitivity and were limited by false alarms. More recent work with deep learning has advanced nodule detection, classification, malignancy prediction, and prognosis, often matching or surpassing radiologists. This study shows the novelty of the broader role of AI in detecting nodules, standardizing reporting, and predicting outcomes. Results signify improved accuracy, efficiency, and reproducibility, though challenges remain, including false positives, difficulty with complex nodules, limited generalizability, as well as incorporation into clinical practice. In general, AI shows strong potential to complement radiologists in lung cancer screening and requires further validation with larger datasets [4].

The study in [11] established low-dose CT (LDCT) as an effective tool for reducing lung cancer mortality, though its use was limited by high false-positive rates, heavy workloads, and variability among radiologists. Earlier computer-aided detection systems improved sensitivity and produced many false positives. Meanwhile, recent advances with AI and deep learning have shown superior performance in nodule detection, classification, malignancy prediction, as well as prognosis. The novelty of this study lies in the comprehensive review of the broader role of AI in LDCT screening, prioritizing the potential for detection, risk stratification, outcome prediction, and workflow optimization. Reported results show that AI can achieve high accuracy, reduce false positives, improve efficiency, and provide standardized reporting, in some cases matching or surpassing radiologists. The strengths of this study are the demonstration of the wide applicability of AI and the potential to reduce diagnostic variability as well as workload. The weaknesses include persistent false positives, limited generalizability due to small or homogeneous datasets, a lack of large-scale clinical validation, and challenges in real-world integration. In general, the study shows that AI is a promising complement to radiologists in lung cancer screening, though further validation is needed. Previous study on cancer prediction explored a variety of machine and deep learning methods, such as logistic regression, artificial neural networks, support vector machines (SVM), decision trees, random forests (RF), and convolutional neural networks (CNN). These studies showed the potential of computational models in assisting early detection, though many faced challenges related to limited datasets, high computational costs, and reduced performance when scaled to larger data [12]. The novelty of this study was in the practical method of incorporating multiple cancers, including breast, lung, as well as prostate, into a single prediction framework, and applying different algorithms modified to each type. Specifically, SVM was used for breast cancer, and RF was applied to lung cancer as well as prostate cancer. The solutions tested included creating datasets with relevant attributes for each cancer type and developing a web-based interface where users could input personal data as well as receive prediction results. The study achieved promising results, where SVM effectively classified breast cancer as malignant or benign. RF provided reliable predictions for lung and prostate cancer based on symptoms as well as cell attributes [13]. The strengths of this study included the accessible interface, the use of established machine learning algorithms, and the focus on practical deployment for early detection. However, several weaknesses remained, including the restriction to offline use, lack of a database for storing patient information, and a limited scope that did not extend to other types of cancer or large-scale clinical validation. Future work should aim to expand the system with more cancer models, incorporate online databases, and test scalability in real-world healthcare settings [14].

A study by [15] proposed a hybrid optimization-based machine learning model for cancer prediction, addressing the limitations of earlier methods that lacked accuracy and generalizability. By testing SVM, RF, and deep learning models with optimization methods, the study showed improved accuracy and reduced error rates compared to baseline methods. Its strengths included innovation, versatility, and strong performance, while the weaknesses comprised limited datasets, high computational needs, as well as a lack of external validation. The study in general showed the potential of hybrid models for more reliable cancer prediction and required larger-scale validation for clinical use. [16] proposed a hybrid optimization-based machine learning model for cancer prediction, improving on earlier methods that suffered from low accuracy and poor generalization. By testing SVM, RF, and deep learning models, the study showed that the hybrid method achieved higher accuracy as well as fewer errors than traditional methods. Its strengths included innovation, flexibility across cancer types, and strong performance, while the weaknesses consisted of limited datasets, high computational costs, and a lack of clinical validation. The model, in general, showed promise for cancer prediction and required broader testing before practical use. Therefore, the current study aims to fill this gap through the use of software that incorporates 16 input variables. The variables include patient code, gender, age, smoking habits, yellow fingers, anxiety, peer pressure, chronic disease, fatigue, allergy, wheezing, alcohol consumption, coughing, shortness of breath, swallowing difficulty, and chest pain.

Existing studies have shown the effectiveness of AI and machine learning in detecting or classifying lung cancer. However, most previous studies focused on single-algorithm implementations or on highly controlled experimental datasets, limiting real-world applicability. Many studies did not incorporate multiple algorithms in a unified diagnostic framework or provide comparative analysis across models. Several works also lacked scalability and clinical validation, restricting the use beyond study settings. This study addresses the gaps by developing a practical, multi-algorithm diagnostic software that simultaneously applies NN, SVM, k-Nearest Neighbor (k-NN), RF, and Naïve Bayes (NB) methods. By comparing predictive performance of the methods on clinical and lifestyle data, this study offers a more comprehensive and accessible decision-support tool for early lung cancer detection, bridging the gap between experimental models as well as real-world clinical implementation.

3. MATERIAL AND METHODOLOGY

The software for detecting lung cancer patient using a multi-algorithm method was developed through the following stages.

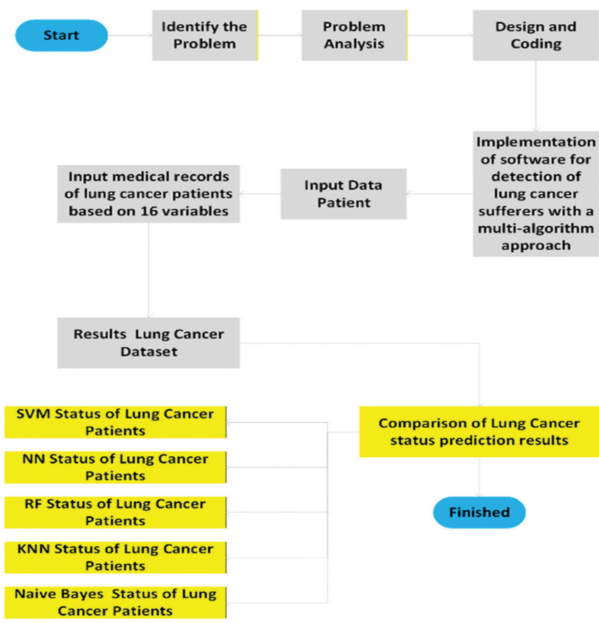


Fig. 1. Development stages of software formation for detecting lung cancer patient using multi-algorithm method

Fig. 1 showed the stages included in developing software for early lung cancer detection using a multi-algorithm method. The initial phases included problem identification, problem analysis, design, and coding. The implementation phase comprised two main processes, namely entering patient data and inputting medical records based on 16 variables related to lung cancer.

The output included lung cancer dataset and a comparative analysis of cancer status predictions using multiple algorithms, such as RF, NB, SVM, NN, as well as k-NN. Each algorithm provided a predicted lung cancer status for patient, allowing a comprehensive comparison of diagnostic accuracy across different models.

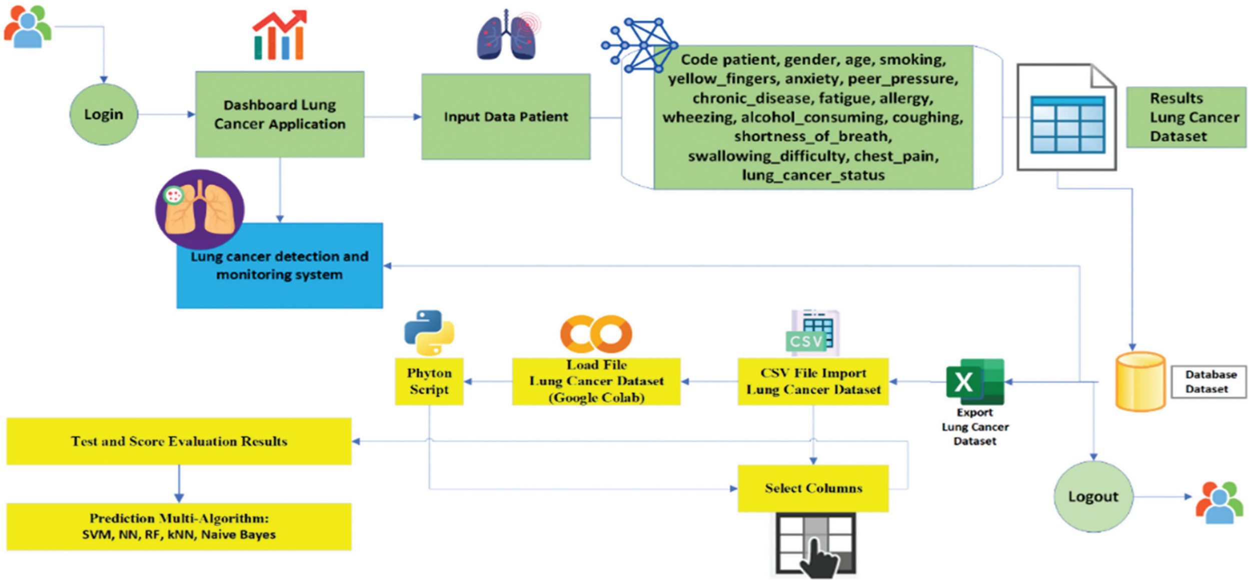


Fig. 2. Study framework for software development for lung cancer patient detection with multi-algorithm

Fig. 2 showed study framework for software development to detect lung cancer patient using multi-algorithm method. The framework offered a high level of study flexibility, as it could be developed according to specific needs, consisting of several stages. First, the user logged in, and upon successful login, the software dashboard would be entered. The user then input patient data, which included values for 16 lung cancer-related variables, namely patient code, gender, age, smoking, yellow fingers, anxiety, peer pressure, chronic disease, fatigue, allergy, wheezing, alcohol consumption, coughing, shortness of breath, swallowing difficulty, chest pain, and lung cancer status. Using these 16 data points, lung cancer status was generated through NB data processing. This output formed lung cancer dataset, which was stored in the database. After storage, the dataset was exported as a CSV file, which was then loaded into Google Colab for scripting with Python. This study used the Orange widget tools to assess accuracy during the analysis. Concerning the process mentioned earlier, multi-algorithm predictions were obtained using RF [17], NB [18], SVM [19], NN [20], and k-NN [21].

3.1. NEURAL NETWORK

Neural networks (NN) included several major formulas at different stages, such as initialization, forward propagation, activation functions, cost calculation, backward propagation, and parameter updates [22]. The following sentences comprised the essential formulas used during the analysis.

- Initialization weights $W^{[l]}$ and biases $b^{[l]}$ for layer l [23]:

$$W^{[l]} \sim \mathcal{N}(0, \sqrt{\frac{2}{n^{[l-1]}}}) \quad (1)$$

$$b^{[l]} = 0 \quad (2)$$

- Forward Propagation for a single layer l [24]:

$$A^{[l]} = \sigma(Z^{[l]}) \quad (3)$$

Where σ was the activation function ReLU [25]. For the output layer, the activation ay differed, e.g., Softmax for multi-class classification:

$$A_i^{[L]} = \frac{e^{Z_i^{[L]}}}{\sum_j e^{z_j^{[L]}}} \quad (4)$$

- Activation Function is ReLU

$$\sigma(Z) = \max(0, Z) \quad (5)$$

- Cost Function for multi-class classification (Softmax), the cost was [26]:

$$J = -\frac{1}{m}\sum_{i=1}^{m}\sum_{k=1}^{K} y_k^{(i)} \log(A_k^{[L](i)}) \quad (6)$$

- Backward Propagation for output layer L [27]:

$$dZ^{[L]} = A^{[L]} - Y \quad (7)$$

- Parameter Update for each layer l:

$$W^{[l]} = W^{[l]} - \alpha . dW^{[l]} \quad (8)$$

$$b^{[l]} = b^{[l]} - \alpha . db^{[l]} \quad (9)$$

Where α is the learning rate.

3.2. SUPPORT VECTOR MACHINE

Concerning training vectors $xi \in Rp$, i=1,…,n, in two classes, and a vector $y \in \{1,-1\}n$, this study aimed to find $w \in Rp$ and $b \in R$ considering the prediction given by sign ($wT\emptyset(x)+b$) was correct for most samples [28].

- SVM solved the following primal problem, where:

$$min_{w,b,\varsigma} \frac{1}{2} \alpha^T Q\alpha - e^T \alpha \quad (10)$$

$$\text{Subject to } y_i(w^T \emptyset(x_i) + b) \geq 1 - \varsigma_i, \quad (11)$$

$$\varsigma_i \geq 0, i = 1, \dots, n \quad (12)$$

Intuitively, this study maximized the margin by minimizing, $||w||^2 = w^2 w$ while incurring a penalty when a sample was misclassified or in the margin boundary [29]. The value $y_i(wT\emptyset(x_i)+b)$ was ≥1 for all samples, which indicated a perfect prediction [29]. However, problems were often not perfectly separable with a hyperplane, allowing some samples to be at a distance ς_i from the correct margin boundary [30].

3.3. k-NEAREST NEIGHBOR

k-NN aimed to learn an optimal linear transformation matrix of size ($n_{components}$, $n_{features}$).

- Which maximized the sum over all samples i of the probability p_i that i was correctly classified [31], where:

$$\arg max_l \sum_{i=0}^{N-1} p_i \quad (13)$$

- With $N = n_{samples}$ and the probability of the sample being correctly classified according to a stochastic nearest neighbors rule in the learned embedded space [32].

$$p_i \sum_{j \in C_i} p_{ij} \quad (14)$$

- Where C_i was the set of points in the same class as sample i , and p_{ij} represented the softmax over Euclidean distances in the embedded space [33].

$$p_{ij} = \frac{\exp(-||L_{xi} - L_{xj}||^2)}{\sum_{k \neq i} \exp(-||L_{xi} - L_{xj}||^2)}, p_{ii} = 0 \quad (15)$$

3.4. RANDOM FOREST

RF algorithm was a combination of multiple decision trees, where each tree was constructed using a randomly selected subset of data and features.

- Each tree in the forest made its prediction, and the final output was determined through majority voting for classification tasks or by averaging for regression tasks [34], [17].

$$l(y) = \arg max_c \left(\sum_{n=1}^{N} I_{h_n(y)=c}\right) \quad (16)$$

Where I was the indicator function and H_N signified N Tree of RF. In addition, RF had an internal mechanism that provided an estimation of its generalization error called Out-of-Bag (OOB) Error Estimate.

3.5. NAIVE BAYES

NB is a supervised learning algorithm following Bayes' theorem under the naive assumption that all features were conditionally independent of the class variable [35].

- According to Bayes' theorem, the relationship between class variable y and dependent feature vector x_1 through x_n is as follows:

$$P(y | x_1, \dots, x_n) = \frac{P(y)P(x_1, \dots, x_n | y)}{P(x_1, \dots, x_n)} \quad (17)$$

- Using the naive conditional independence assumption [36].

$$P(x_i | y, x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = P(x_i | y), \quad (18)$$

- For all values of i, the relationship was simplified as follows [37].

$$P(y | x_1, \dots, x_n) = \frac{P(y) \prod_{i=1}^{n} P(x_i | y)}{P(x_1, \dots, x_n)} \quad (19)$$

- Since $P(x_1, \dots, x_n)$ was constant given the input, the following classification rule was used [38].

$$P(y | x_1, \dots, x_n) \propto P(y) \prod_{i=1}^{n} P(x_i | y)$$
$$\Downarrow \quad (20)$$
$$\hat{y} = \arg max_y P(y) \prod_{i=1}^{n} P(x_i | y)$$

$P(y)$ and $P(x_i | y)$ was estimated using Maximum A Posteriori (MAP). The $P(y)$ was determined based on the relative frequency of class y in the training set [39]. The various NB classifiers differed in the assumptions made regarding the distribution of $P(x_i | y)$ [40].

4. RESULT

The stages of software development for detecting lung cancer patient using a multi-algorithm method included generating a dataset by inputting patient data and medical records based on 16 variables. Lung cancer status predictions were measured using algorithms such as RF, NB, SVM, NN, and k-NN. Following the process, problem identification was conducted during this stage. The identified issue was the need to develop a system capable of detecting lung cancer patient using a multi-algorithm method that incorporated 16 input variables. These included patient code, gender, age, smoking, yellow fingers, anxiety, peer pressure, chronic disease, fatigue, allergy, wheezing, alcohol consumption, coughing, shortness of breath, swallowing difficulty, and chest pain, along with one output variable, named lung cancer status.

4.1. PROBLEM IDENTIFICATION

Problem identification was conducted at this stage during the analysis including:

- The need for software to detect lung cancer patient using multi-algorithm method. This was to be used in decision-making or policy implementation for lung cancer patient services.
- The developed model should apply to health services.
- Measuring the accuracy of the cancer status prediction in lung cancer patient using multi-algorithm, namely RF, NB, SVM, NN, and k-NN.

4.2. PROBLEM ANALYSIS

Tool user communicated to understand the software expected by user, both doctors and hospitals.

4.3. SOFTWARE DESIGN FOR DETECTING LUNG CANCER PATIENT USING MULTI-ALGORITHM

Software for detecting lung cancer patient with multi-algorithm method was developed on Android. Fig. 3 shown some representation of the software on Android.

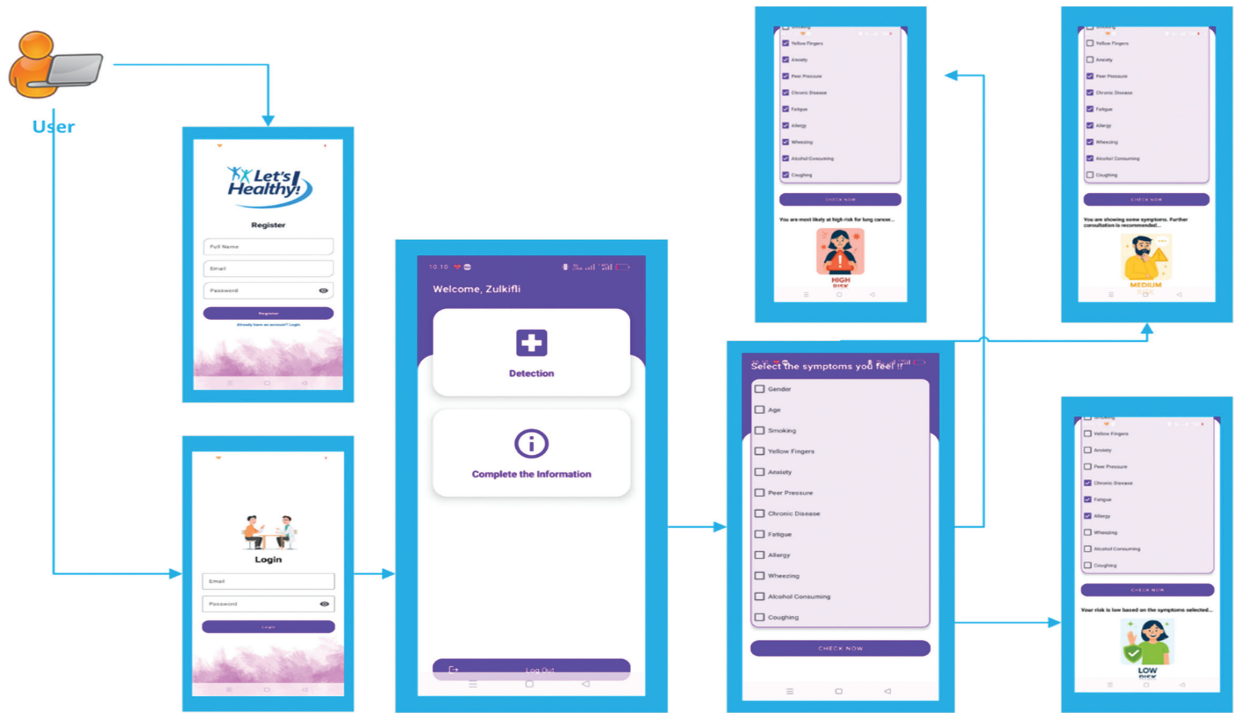


Fig. 3. Software presentation for lung cancer patient detection with multi-algorithm method

4.4. DATASET DATABASE

The details and explanation of the dataset shown in Table 1 [41] were used to measure the accuracy of lung cancer detection through various algorithms, including RF, NB, SVM, NN, as well as k-NN. This data was sourced from Kaggle.com and originally contained 3,000 data points, with only 10 data entries shown in Table 2.

4.5. APPLICATION OF NEURAL NETWORK ALGORITHM

Table 3 shows an example of a dataset that has been normalized during analysis, we used the Standard Scaler technique when normalizing the data. The formula used to convert the original test data ranged from 0.1 to 0.9 because the activation function used was sigmoid with a value above 0 [42].

4.6 MULTI-ALGORITHM PERFORMANCE

The dataset was divided into two parts, containing 90% training and 10% testing, with stratification as well as random states equaling 2. The performance of the RF, NB, SVM, NN, and k-NN algorithms was shown in Table 4.

The confusion matrix in the earlier image showed that the classification model performed well in detecting lung cancer. Among the total test data, 148 cases were correctly identified as not having lung cancer (true negatives), and 152 cases were correctly detected with it (true positives). There were no prediction errors during the process, in the form of false positives or negatives. This signified that the model achieved 100% accuracy, precision, recall, and F1-score. In other words, the model perfectly distinguished patients with lung cancer from those without in the test data used.

Table 4 showed the performance of five ML algorithms, namely RF, NB, SVM, NN, k-NN evaluated using accuracy, precision, recall, and F1-score metrics. The results signified that RF, NB, SVM, and NN each achieved a perfect score of 1.00 across all metrics. This indicated that the four algorithms classified the data without any error. Meanwhile, k-NN showed a slight decrease in performance with accuracy, precision, recall, and F1-score values of 0.99. Despite the minor decrease, k-NN still showed a very high and nearly perfect performance. The performance evaluation results were shown by the confusion matrix in Fig. 4. The results of the performance evaluation were visualized using three-dimensional (3D) TSNe.

Table 1. Details of the dataset

Variable	Association with Lung Cancer	Explanation
Smoking	Very Strong	The primary cause of lung cancer. Around 85–90% of all lung cancer cases were connected to smoking. Tobacco smoke contains carcinogens that damage lung cells over time
Age	Moderate to Strong	Risk increased significantly with age, since DNA damage accumulated over time. Most lung cancer cases occurred in people aged 55 and older
Gender	Weak to Moderate	Men historically had a higher risk due to smoking rates, but now gender differences are narrowing. Biological differences might play a minimal role
Yellow fingers	Indirect indicator	Often a sign of heavy smoking, not a direct cause. It was a proxy variable that signaled nicotine exposure
Chronic disease	Moderate	Chronic lung inflammation and damage increase susceptibility to cancer. Often comorbid with smoking
Coughing, wheezing, shortness of breath, chest pain, and swallowing difficulty	Symptoms, not causes	These showed possible existing lung damage or disease, not risk factors
Anxiety, peer pressure, fatigue, allergy, and alcohol consumption	Weak or indirect	Minimal or no direct causal relationship with lung cancer. Peer pressure could indirectly lead to smoking behavior

Table 2. Dataset of patient with lung cancer

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
P-0001	1	65	1	1	1	2	2	1	2	2	2	2	2	2	1	Y
P-0002	0	55	1	2	2	1	1	2	2	2	1	1	1	2	2	Y
P-0050	1	38	2	2	1	1	2	2	1	2	1	2	2	2	1	Y
P-0117	0	52	2	2	1	2	1	2	1	1	2	1	2	1	2	Y
P-0118	1	34	2	2	2	2	1	1	2	2	2	2	1	1	1	N
P-0158	1	54	2	1	2	2	2	2	2	2	2	1	1	1	1	N
P-0159	1	78	2	2	1	1	2	1	2	1	2	2	1	2	1	Y
P-0211	1	30	1	1	2	2	1	2	2	1	2	2	2	1	2	N
P-2999	1	40	1	2	2	1	2	2	2	2	2	1	2	1	2	Y
P-3000	1	54	2	1	2	2	1	1	2	2	2	1	1	1	1	Y

Note: a=code patient, b=gender, c=age, d=smoking, e=yellow fingers, f=anxiety, g=peer pressure, h=chronic disease, i=fatigue, j=allergy, k=wheezing, l=alcohol consuming, m=coughing, n=shortness of breath, o=swallowing difficulty, p=chest pain, q= lung cancer status

Table 3. Detailed confidence levels of the proposed model against the actual stunting status

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
P-0001	0,8	0,56	0	0	0	0,8	0,8	0	0,8	0,8	0,8	0,8	0,8	0,8	0	Y
P-0002	0	0,4	0	0,8	0,8	0	0	0,8	0,8	0,8	0	0	0	0,8	0,8	Y
P-0050	0,8	0,128	0,8	0,8	0	0	0,8	0,8	0	0,8	0	0,8	0,8	0,8	0	Y
P-0117	0	0,352	0,8	0,8	0	0,8	0	0,8	0	0	0,8	0	0,8	0	0,8	Y
P-0118	0,8	0,064	0,8	0,8	0,8	0,8	0	0	0,8	0,8	0,8	0,8	0	0	0	N
P-0158	0,8	0,048	0	0	0	0,8	0,8	0,8	0,8	0,8	0,8	0	0	0	0	N
P-0159	0,8	0,384	0,8	0	0,8	0,8	0,8	0	0,8	0	0,8	0,8	0	0,8	0	Y
P-0211	0,8	0,768	0,8	0,8	0	0	0	0,8	0,8	0	0,8	0,8	0,8	0	0,8	N
P-2999	0,8	0	0	0	0,8	0,8	0,8	0,8	0,8	0,8	0,8	0	0,8	0	0,8	Y
P-3000	0,8	0,16	0	0,8	0,8	0	0	0	0,8	0,8	0,8	0	0	0	0	Y

Note: a=code patient, b=gender, c=age, d=smoking, e=yellow fingers, f=anxiety, g=peer pressure, h=chronic disease, i=fatigue, j=allergy, k=wheezing, l=alcohol consuming, m=coughing, n=shortness of breath, o=swallowing difficulty, p=chest pain, q= lung cancer status

Table 4. Multi-algorithm performance

1	2	3	4	5
RF	1.00	1.00	1.00	1.00
NB	1.00	1.00	1.00	1.00
SVM	1.00	1.00	1.00	1.00
NN	1.00	1.00	1.00	1.00
k-NN	0.99	0.99	0.99	0.99

Note: 1=Algorithm, 2= Precision, 3= F1-Score, 4= Recall, 5= Accuracy

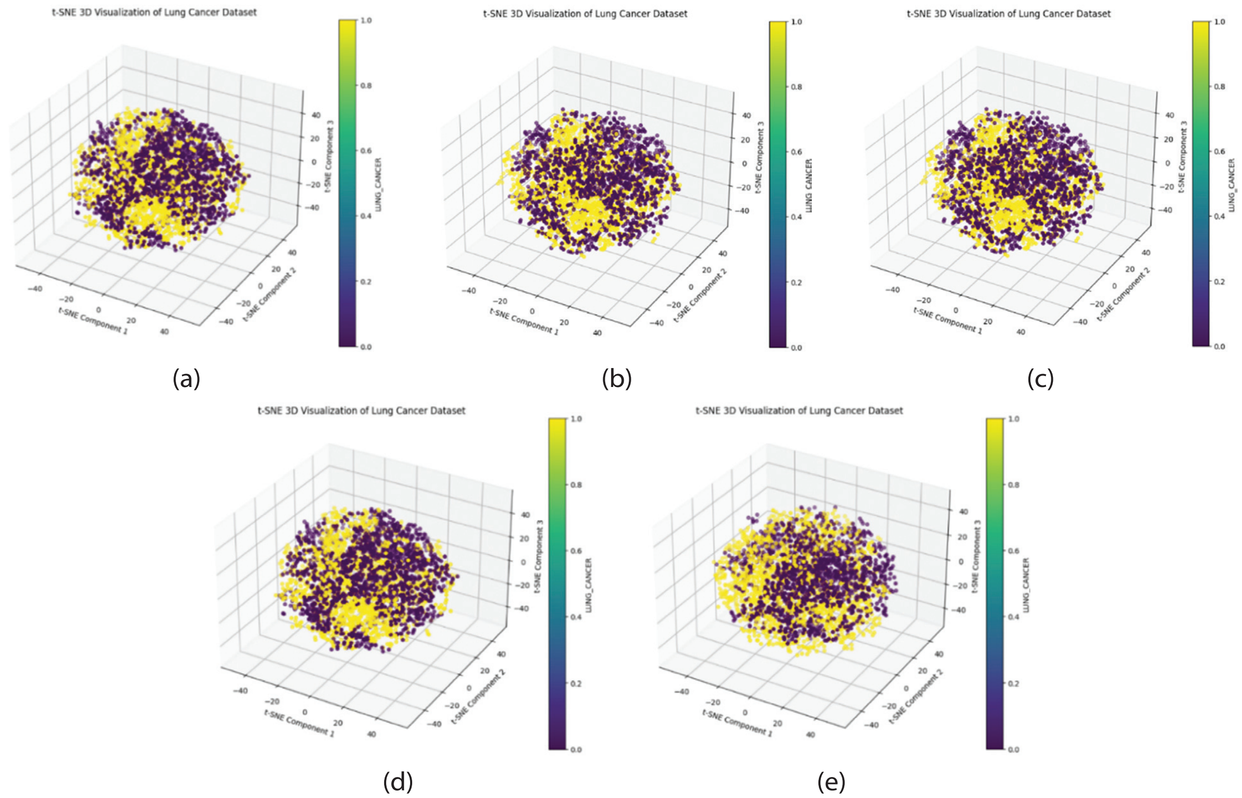


Fig. 5. 3D visualization of TSNe models (a) RF, (b) NB, (c) SVM, (d) NN, and (e) k-NN

Fig. 5 was a 3D TSNe visualization of lung cancer dataset, showing the distribution of data in 3D space based on the three principal components generated from TSNe method.

The data was represented as dots in two colors, namely purple and yellow. Purple dots (value 0) represented patient without lung cancer, while yellow dots (value 1) indicated patient diagnosed with lung cancer, respectively.

4.7. RECEIVER OPERATING CHARACTERISTICS (ROC) ANALYSIS

ROC was used to explain, assess, and categorize the performance of RF, NB, SVM, NN, and k-NN algorithms [43]. Fig. 6 showed ROC curves for these algorithms with each curve representing performance across the target classes "Survived" and "Died". The curves were shown using different colors, namely cyan, orange, blue, purple, and green lines, respectively.

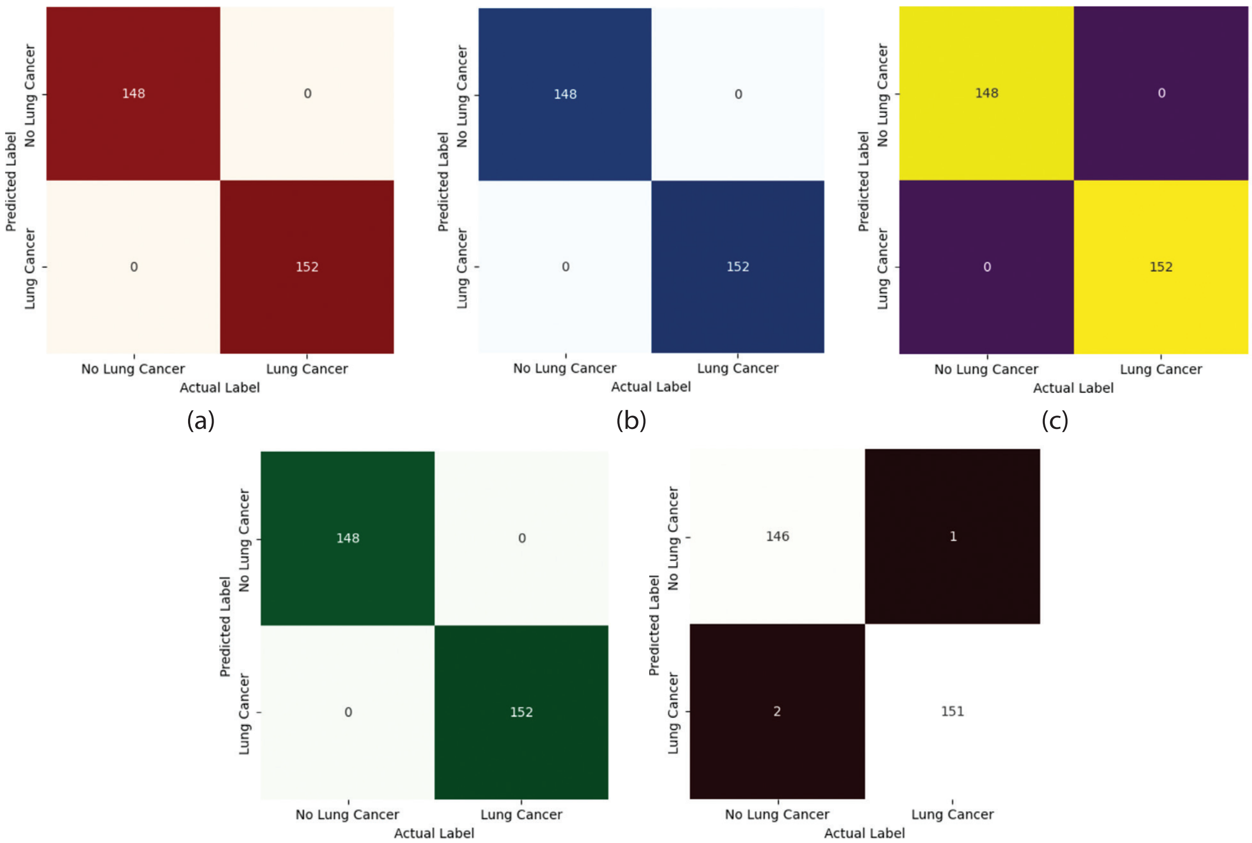


Fig. 4. Confusion matrix visualization (a) RF, (b) NB, (c) SVM, (d) NN, and (e) k-NN

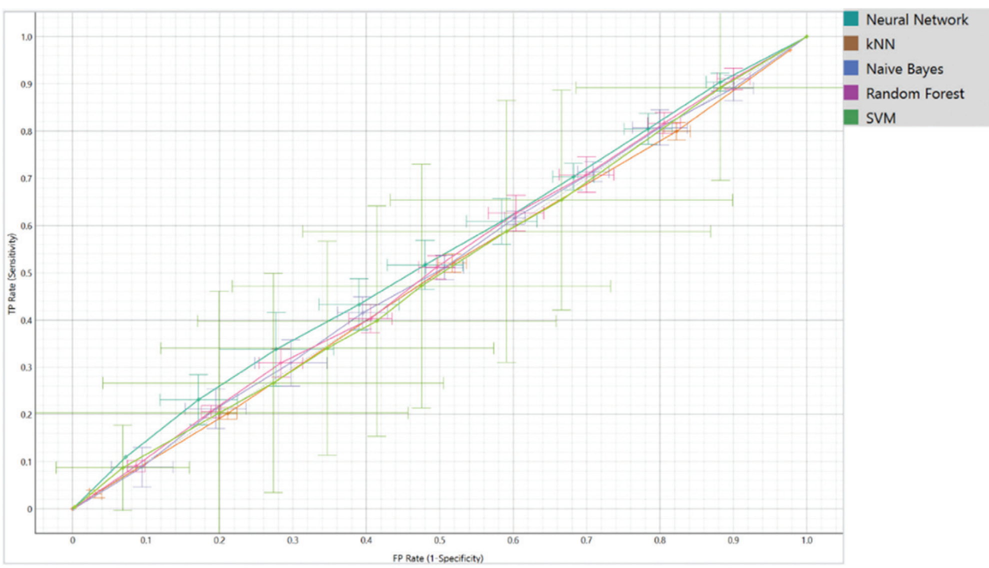


Fig. 6. Performance Curves of RF, NB, SVM, NN, and k-NN Algorithms

Table 5. Validation results of lung cancer patient detection predictions between neural RF, NB, SVM, NN, and k-NN algorithm

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P-0001	0	0	0	1	0	0	0.580	N	0.600	Y	0.506	Y	0.527	Y	0.500	Y
P-0002	0	0	1	1	1	0	0.668	N	0.600	Y	0.506	Y	0.654	Y	0.500	Y
P-0050	1	1	0	1	1	0	0.505	Y	0.600	N	0.585	Y	0.606	Y	0.500	Y
P-0117	1	0	1	1	1	0	0.618	N	0.600	Y	0.511	Y	0.572	Y	0.500	Y
P-0118	0	0	0	1	0	0	0.757	N	0.600	N	0.506	Y	0.712	N	0.500	Y
P-0158	0	1	1	0	1	1	0.701	Y	0.800	Y	0.531	N	0.565	Y	0.507	Y
P-0159	1	1	0	0	1	1	0.755	Y	0.800	N	0.516	Y	0.643	Y	0.500	Y
P-0211	0	1	1	1	1	1	0.810	Y	0.800	Y	0.533	Y	0.616	Y	0.532	Y
P-2999	1	0	1	0	1	1	0.539	N	0.600	Y	0.546	N	0.655	Y	0.500	Y
P-3000	1	0	1	0	0	1	0.735	N	0.600	Y	0.521	Y	0.681	N	0.536	Y

Note: 1=code patien, 2=actual, 3=NN, 4= k-NN, 5= NB, 6= RF, 7=svm, 8= NN numerical, 9=NN validation against actual, 10= k-NN numerical, 11= validation of k-NN against actual, 12=NB numerical, 13=validation of NB against actual, 14=RF numerical, 15=RF validation against actual, 16=SVM numerical, 17=SVM validation against actual Note: 1=code patien, 2=actual, 3=NN, 4= k-NN, 5= NB, 6= RF, 7=svm, 8= NN numerical, 9=NN validation against actual, 10= k-NN numerical, 11= validation of k-NN against actual, 12=NB numerical, 13=validation of NB against actual, 14=RF numerical, 15=RF validation against actual, 16=SVM numerical, 17=SVM validation against actual

4.8. COMPARISON OF NN ALGORITHMS, RF, NB, SVM, NN, AND K-NN ON PREDICTING LUNG CANCER

Fig. 7 showed a comparison of RF, NB, SVM, NN, and k-NN algorithms for detecting lung cancer patient.

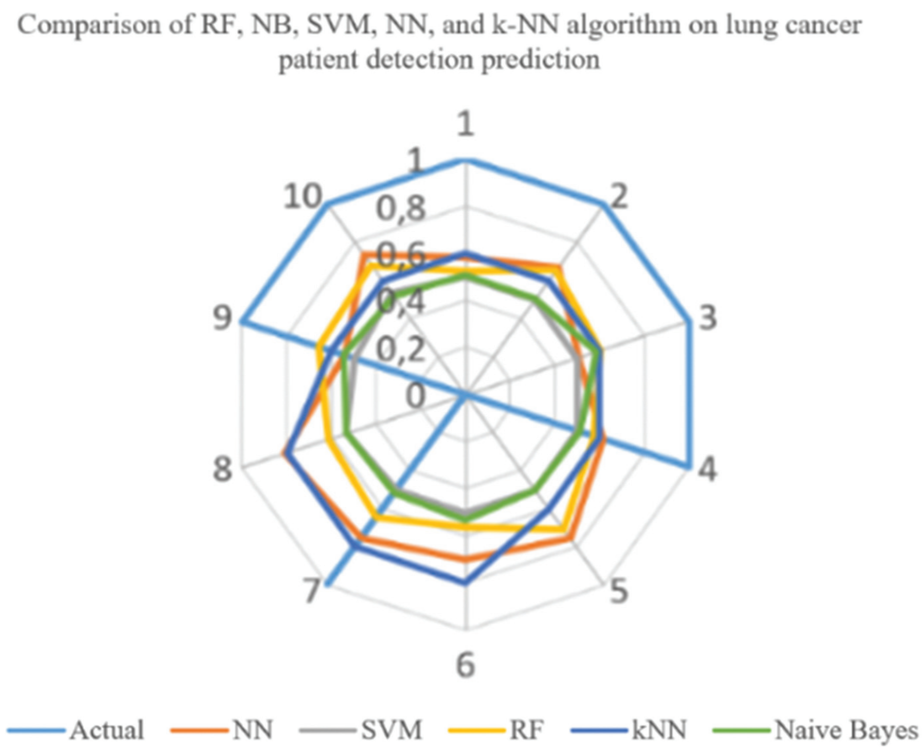


Fig. 7. Comparison of the Prediction Accuracy Performance for Lung Cancer Patient Detection using RF, NB, SVM, NN, and k-NN

5. DISCUSSION

This study evaluated the performance of five machine learning algorithms, namely, RF, NB, SVM, NN, and k-NN, for lung cancer prediction. The results showed that RF, NB, SVM, and NN achieved a perfect accuracy of 1.00, while k-NN obtained slightly lower accuracy of 0.99.

The high performance reported supported a previous study showing the suitability of ensemble and kernel-based methods for cancer diagnosis. For instance, [9] achieved strong classification accuracy using CNNs for lung cancer histology. [12] reported that incorporating machine learning classifiers with multi-attribute decision-making produced high performance in distinguishing benign from malignant lung X-rays. In many cases, tree-based methods such as RF excelled because the models captured nonlinear feature interactions and handled categorical as well as numerical variables effectively. The outcome might explain the perfect accuracy of RF in this study.

NB achieved near-perfect results, which were unexpected given its simplifying assumption of feature independence. However, previous studies [11] showed that NB performed competitively in medical diagnosis when datasets were relatively small or structured with limited feature interdependencies. SVM and NN achieved comparable performance, consistent with previous studies on lung and breast cancer prediction, where the ability to model complex nonlinear decision boundaries proved beneficial [14].

The comparatively lower performance of k-NN (though still at 99%) could be explained by its sensitivity to feature scaling and the curse of dimensionality. Having 16 input variables, the distances between samples might become less discriminative, leading to reduced performance compared to algorithms that modeled feature interactions more explicitly. Previous studies in medical prediction tasks observed strong baseline performance of k-NN but lower robustness compared to ensemble and kernel methods.

Achieving near-perfect accuracy across multiple algorithms was unusual in real-world biomedical datasets and raised concerns about potential overfitting, limited dataset diversity, or issues in ground-truth labeling. Different from previous analyses, such as [13], which validated the lung cancer classification models on independent test cohorts, this study did not describe the validation procedure. While the comparative trends between algorithms were consistent with the literature, the absolute performance values might be inflated.

As the results of this study showed promising potential for a multi-algorithm method in lung cancer prediction, several limitations should be acknowledged. First, the dataset used was obtained from a publicly available source (Kaggle) and contained 3,000 records. Although the size was sufficient for proof-of-concept analysis, it might not adequately represent the variability observed in real-world clinical populations. The dataset might not capture diverse demographic, genetic, and environmental factors that influence lung cancer incidence, limiting the generalizability of the findings to broader patient populations.

Second, the study lacked a clear description of how data were partitioned for training and testing. Without independent test sets or cross-validation procedures, the reported near-perfect accuracy might be inflated due to overfitting or data leakage. This concern was heightened by the unusually high performance across multiple algorithms, which was rarely observed in complex medical prediction tasks.

Third, the ground-truth labels were not independently validated against clinical or pathological standards. In some cases, labels appeared to be generated through algorithmic preprocessing (e.g., NB), which might bias performance metrics. Additionally, issues such as duplicate patient identifiers and inconsistent labeling in the dataset raised further questions about data quality as well as reliability.

Fourth, the study focused only on structured tabular data derived from 16 predefined variables. This method did not incorporate imaging, genomic, or longitudinal clinical data, even though the features were often crucial for accurate lung cancer diagnosis. Future studies should validate the software on larger, more diverse, and clinically verified datasets, while also incorporating multimodal data sources to improve predictive robustness as well as generalizability.

6. CONCLUSION

In conclusion, software was developed to detect lung cancer patient by predicting lung cancer status using multiple algorithms. The algorithms used to measure the accuracy of the predictions included RF, NB, SVM, NN, and k-NN. This software was designed for use by doctors, requiring the input of 16 patient variables related to lung cancer. Based on the dataset, the software predicted lung cancer status of each patient. The results showed that RF, NB, SVM, and NN each achieved an accuracy of 100%, while k-NN closely followed with 99%. Among the five algorithms, k-NN showed the lowest performance, despite the fact that it was still highly accurate.

This study had limitations related to dataset size, potential overfitting, and restricted clinical scope despite the promising results. Future studies should validate the model on larger and more diverse datasets, incorporate additional clinical and imaging variables, as well as apply rigorous cross-validation to ensure reliability. Expanding the system into a clinician-friendly decision-support tool with explainable outputs would further improve its practical value in real-world healthcare settings.

REFERENCES:

[1] S. Nageswaran et al. "Lung Cancer Classification and Prediction Using Machine Learning and Image Processing", BioMed Research International, Vol. 2022, 2022.

[2] P. Sathe, A. Mahajan, D. Patkar, M. Verma, "End-to-End Fully Automated Lung Cancer Volume Estimation System", International Journal of Electrical and Computer Engineering Systems, Vol. 15, No. 8, 2024, pp. 651-661.

[3] A. Shimazaki et al. "Deep learning-based algorithm for lung cancer detection on chest radiographs using the segmentation method", Scientific Reports, Vol. 12, No. 1, 2022, pp. 1-10.

[4] S. M. Lee, C. M. Park, "Application of artificial intelligence in lung cancer screening", Journal of the Korean Society of Radiology, Vol. 80, No. 5, 2022, pp. 872-879.

[5] L. Karunakaran, "Machine Learning Approach Of Lung Cancer Prediction Using Multi Machine Learning Models", StudyGate Data Science Track ComURS2025 Computing Undergraduate Study Symposium, Sabaragamuwa University of Sri Lanka, Belihuloya, March 2025.

[6] A. A. Shah, H. A. M. Malik, A. H. Muhammad, A. Alourani, Z. A. Butt, "Deep learning ensemble 2D CNN approach towards the detection of lung cancer", Scientific Reports, Vol. 13, No. 1, 2023, pp. 1-15.

[7] H. Sharma, J. S. Jain, P. Bansal, S. Gupta, "Feature extraction and classification of chest X-ray images using CNN to detect pneumonia", Proceedings of the 10th International Conference on Cloud Computing, Data Science & Engineering, Noida, India, 29-31 January 2020, pp. 227-231.

[8] D. Huang, Z. Li, T. Jiang, C. Yang, N. Li, "Artificial intelligence in lung cancer: current applications, future perspectives, and challenges", Frontiers in Oncology, Vol. 14, 2024, pp. 1-19.

[9] T. L. Chaunzwa et al. "Deep learning classification of lung cancer histology using CT images", Scientific Reports, Vol. 11, No. 1, 2021, pp. 1-13.

[10] Z. Zulkifli, F. A. Makkiyah, D. Antoni, F. Fitriana, T. Jamaan, A. Taufik, "Multi-Algorithm to Measure the Accuracy Level of Diabetes Status Prediction", Journal of Applied Data Sciences, Vol. 5, No. 2, 2024, pp. 736-746.

[11] N. Ghaffar Nia, E. Kaplanoglu, A. Nasab, "Evaluation of artificial intelligence techniques in disease diagnosis and prediction", Discover Artificial Intelligence, Vol. 3, No. 1, 2023.

[12] T. Meeradevi, S. Sasikala, L. Murali, N. Manikandan, K. Ramaswamy, "Lung cancer detection with machine learning classifiers with multi-attribute decision-making system and deep learning model", Scientific Reports, Vol. 15, No. 1, 2025, pp. 1-19.

[13] S. Alazwari, J. Alsamri, M. M. Asiri, M. Maashi, S. A. Asklany, and A. Mahmud, "Computer-aided diagnosis for lung cancer using waterwheel plant algorithm with deep learning", Scientific Reports, Vol. 14, No. 1, 2024, pp. 1-14.

[14] G. Sruthi, C. L. Ram, M. K. Sai, B. P. Singh, N. Majhotra, N. Sharma, "Cancer Prediction using Machine Learning", Proceedings of the 2nd International Conference on Innovative Practices in Technology and Management, Gautam Buddha Nagar, India, 23-25 February 2022, pp. 217-221.

[15] S. R. Abdani, N. Jamil, S. M. Z. Syed Zainal Ariffin, S. Ibrahim, "3D-based Convolutional Neural Networks for Medical Image Segmentation: A Review", International Journal of Electrical and Computer Engineering Systems, Vol. 16, No. 5, 2025, pp. 347-363.

[16] M. Phogat, D. Kumar, "A Hybrid Metaheuristics based technique for Mutation Based Disease Classification", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 6, 2023, pp. 635-646.

[17] E. Dritsas, M. Trigka, "Data-Driven Machine-Learning Methods for Diabetes Risk Prediction", Sensors, Vol. 22, No. 14, 2022.

[18] S. A. Ali, N. R. Roy, D. Raj, "Software Defect Prediction using Machine Learning", Proceedings of the 10th International Conference on Computing for Sustainable Global Development, New Delhi, India, 15-17 March 2023, pp. 639-642.

[19] I. Aydin, M. Karaköse, E. Akin, "Artificial immune based support vector machine algorithm for fault diagnosis of induction motors", Proceedings of

the International Aegean Conference on Electrical Machines and Power Electronics, Bodrum, Turkey, 10-12 September 2007, pp. 217-221.

[20] S. S. Cross, R. F. Harrison, R. L. Kennedy, "Introduction to neural networks", Lancet, Vol. 346, No. 8982, 1995.

[21] S. Goyal, “Handling Class-Imbalance with KNN (Neighbourhood) Under-Sampling for Software Defect Prediction”, Artificial Intelligence Review, Vol. 55, No. 3, 2022, pp. 2023-2064.

[22] J. Díaz-Ramírez, “Machine Learning and Deep Learning”, Ingeniare, Vol. 29, No. 2, 2021, pp. 182-183.

[23] M. A. Ijaz, M. K. Abid, N. Aslam, A. Q. Mudaseer, “Detecting Monkeypox in humans using deep learning”, VFAST Transactions on Software Engineering, Vol. 11, No. 2, pp. 265-272, 2023.

[24] A. Waheed, M. Goyal, D. Gupta, A. Khanna, F. Al-Turjman, P. R. Pinheiro, “CovidGAN: Data Augmentation Using Auxiliary Classifier GAN for Improved Covid-19 Detection”, IEEE Access, Vol. 8, 2020, pp. 91916-91923.

[25] A. Bhat, U. Bhardwaj, M. Singla, K. Garg, “Prediction of COVID 19 Using Chest X-Ray Images through CNN optimised using Genetic Algorithm”, Proceedings of the 2nd International Conference on Intelligent Technologies, Hubli, India, 24-26 June 2022, pp. 1-8.

[26] R. T. N. V. S. Chappa, M. El-Sharkawy, “Squeeze-and-Excitation SqueezeNext: An Efficient DNN for Hardware Deployment”, Proceedings of the 10th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 6-8 January 2020, pp. 691-697.

[27] S. M. Fati, E. M. Senan, N. ElHakim, “Deep and Hybrid Learning Technique for Early Detection of Tuberculosis Based on X-ray Images Using Feature Fusion”, Applied Sciences, Vol. 12, No. 14, 2022, p. 7092.

[28] A. Thakkar, D. Mungra, A. Agrawal, K. Chaudhari, “Improving the Performance of Sentiment Analysis Using Improved Preprocessing Technique and Artificial Neural Network”, IEEE Transactions on Affective Computing, Vol. 13, No. 4, 2022, pp. 1771-1782.

[29] A. K. Jean, M. Diarra, B. A. Bakary, G. Pierre, A. K. Jérôme, U. B. Franche-comté, “Application based on Hybrid CNN-SVM and PCA- SVM Approaches for Classification of Cocoa Beans”, International Journal of Advanced Science and Computer Applications, Vol. 13, No. 9, 2022, pp. 231-238.

[30] A. Fadli, Y. Ramadhani, M. S. Aliim, “Purwarupa Sistem Deteksi COVID-19 Berbasis Website Menggunakan Algoritma CNN”, Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), Vol. 5, No. 5, 2021, pp. 876-883.

[31] Ž. Vujović, “Classification Model Evaluation Metrics”, International Journal of Advanced Science and Computer Applications, Vol. 12, No. 6, 2021, pp. 599-606.

[32] D. Wang, H. Yu, D. Wang, G. Li, “Face recognition system based on CNN”, Proceedings of the International Conference on Computer Information and Big Data Applications, Guiyang, China, 17-19 April 2020, pp. 470-473.

[33] F. H. Bitew, C. S. Sparks, S. H. Nyarko, “Machine learning algorithms for predicting undernutrition among under-five children in Ethiopia”, Public Health Nutrition, Vol. 25, No. 2, 2022, pp. 269-280.

[34] F. Aldi, I. Nozomi, R. B. Sentosa, A. Junaidi, “Machine Learning to Identify Monkey Pox Disease”, Sinkron, Vol. 8, No. 3, 2023, pp. 1335-1347.

[35] P. Singh, S. Verma, “Multi-classifier model for software fault prediction”, International Arab Journal of Information Technology, Vol. 15, No. 5, 2018, pp. 912-919.

[36] W. Tan et al. “Classification of COVID-19 pneumonia from chest CT images based on reconstructed super-resolution images and VGG neural network”, Health Information Science and Systems, Vol. 9, No. 1, 2021, pp. 1-12.

[37] S. H. Basha, A. M. Anter, A. E. Hassanien, A. Abdalla, “Hybrid intelligent model for classifying chest X-ray images of COVID-19 patients using genetic algorithm and neutrosophic logic”, Soft Computing, Vol. 27, 2023, pp. 3427-3442.

[38] S. S. Shreem, H. Turabieh, S. Al Azwari, F. Baothman, “Improved binary genetic algorithm as a feature selection to predict student performance”, Soft Computing, Vol. 26, No. 4, 2022, pp. 1811-1823.

[39] A. Purbasari, F. R. Rinawan, A. Zulianto, A. I. Susanti, H. Komara, "CRISP-DM for Data Quality Improvement to Support Machine Learning of Stunting Prediction in Infants and Toddlers", Proceedings of the 8th International Conference on Advanced Informatics: Concepts, Theory and Applications, Bandung, Indonesia, 29-30 September 2021, pp. 1-6.

[40] H. El Massari, Z. Sabouri, S. Mhammedi, N. Gherabi, "Diabetes Prediction Using Machine Learning Algorithms and Ontology", Journal of ICT Standardization, Vol. 10, No. 2, 2022, pp. 319-338.

[41] O. Esteban et al. "fMRIPrep: a robust preprocessing pipeline for functional MRI", Nature Methods, Vol. 16, 2019, pp. 111-116.

[42] T. Byun et al. "Input prioritization for testing neural networks", Proceedings of the IEEE International Conference On Artificial Intelligence Testing, Newark, CA, USA, 4-9 April 2019.

[43] F. Movahedi, R. Padman, J. F. Antaki, "Limitations of receiver operating characteristic curve on imbalanced data: Assist device mortality risk scores", Journal of Thoracic and Cardiovascular Surgery, Vol. 165, No. 4, 2023, pp. 1433-1442.

Filtering Microstrip Patch Antenna Design Using Coupling Matrix Approach for ISM Applications

Original Scientific Paper

Kharmana Ramazan Ahmad
Department of Physics, College of Education, Salahaddin University-Erbil,
Erbil, Kurdistan Region, Iraq
kharmana.ahmed@su.edu.krd

Rashad H. Mahmud*
Department of Physics, College of Education, Salahaddin University-Erbil,
Erbil, Kurdistan Region, Iraq
Mechatronic Engineering, Faculty of Engineering, Tishk International University,
Erbil, Iraq
rashad.mahmud@su.edu.krd

*Corresponding author

Abstract – *This paper presents a novel design approach for a filtering microstrip patch antenna inspired by a bandpass filter (BPF). It is based on the coupling matrix approach, where the magnitudes of the matrix elements are utilized to extract the physical dimensions. Two rectangular microstrip patch resonators (RMPRs) are directly coupled via an air-gap to realize a second-order BPF and a filtering microstrip patch antenna. For the BPF, a 50-Ω microstrip feedline is employed at the input/output ports and extended into the center of the RMPRs to ensure strong impedance matching within the passband of interest. For the filtering antenna, the output feedline port is removed, and the second RMPR is modified to obtain the required radiation quality factor and provide radiation within the passband frequency range. To validate the proposed approach, both designs are fabricated and experimentally tested, showing excellent agreement with the simulation results. The measured 10-dB fractional bandwidth (FBW), passband peak gain, and total efficiency are 4.05%, 6.0 dBi, and 74.0%, respectively. These results demonstrate that the proposed designs offer a compact size, high gain, and high efficiency, making them promising candidates for ISM band applications.*

Keywords: *Bandpass filter, cavity resonators, coupling matrix, filtering antenna, microstrip patch*

Received: August 1, 2025; Received in revised form: September 28, 2025; Accepted: October 30, 2025

1. INTRODUCTION

Microstrip patch antennas are well-suited for industrial scientific medical (ISM) systems not only due to their compact size, light-weight and low profile characteristics [1-5], but also because they can be seamlessly integrated with other system components [6, 7]. This direct integration eliminates the need for additional matching circuits and realizes system miniaturization. However, conventional microstrip patch antennas suffer from their inherent narrow bandwidth performances, restricting their applications in wideband and ISM technologies [3, 8]. To remedy this limitation, filtering microstrip patch antennas have been introduced, combining both radiation and filtering functionalities into a single integrated component [9]. This integration offers miniaturizing the front-end size, eliminating the insertion loss caused by separate BPF filters, and simplifying the front-end system architecture [10]. Additionally, the bandwidth of filtering microstrip patch antennas can be broadened by appropriately tuning the resonant frequencies of the coupled-resonators within the antenna radiating structure.

Various design approaches have been investigated to implement filtering functionalities in microstrip patch antenna. Among these is the coupled-resonator filter synthesis approach [9, 11], where the patch serves as the last coupled-resonator in the filter while also acting as a radiator. Techniques such as the use of metal strips [12], shorting pins [13], stub-loaded resonators [14], coupling structures [15-17], and slot-loaded patches [18, 19] have been explored to improve the frequency selectivity and widen the bandwidth of filtering microstrip antennas [12-19]. Modified patch shapes, including U-shaped [20, 21], T-shaped [6], bow tie-shaped

[22], square ring [23], cross-shaped [24], ground slots [25], and inverted-F configuration [26] have also been employed. In addition, other enhancement techniques such as defected ground structure (DGS) [27, 28], and various feedline structures like fork-shaped [29], split-merge [30], and dual baluns [11] have been introduced to realize desired filtering characteristics to microstrip patch antennas. Equivalent circuit models based on the lumped *LC* elements have also been proposed for slot-loaded patch designs [31, 32].

Despite these advances in filtering patch antenna designs, many of the existing techniques require extra circuit structure, which increases the overall size and design complexity. To address this issue, we propose a new filtering microstrip patch antenna design approach based on the coupling matrix approach, in which no additional coupling structures or circuits are required to realize filtering functionality. In section 2, the approach is applied to a second-order BPF using rectangular patch resonators, where matrix elements are interpreted into physical dimensions. In Section 3, the filter's output port is removed, and the second-coupled patch is modified to achieve the required radiation quality factor (Q_r) while maintaining its dual functionality of frequency selectivity and radiation. Section 4 presents the fabrication and measurement of two prototypes to validate the proposed method. Finally, the conclusions are summarized in section 5.

2. BPF DESIGN

Fig. 1 illustrates the topology and corresponding physical layout of a second-order microstrip BPF with an all-resonator configuration. The substrate material chosen is Rogers RO4350B™, which has a relative permittivity (ε_r) of 3.48, thickness (h) of 1.524 mm, and a loss tangent of 0.0037. The patch and ground plane are both 0.035 mm thick, and made using copper with a conductivity of 5.8×10⁷ S/m. A two-pole Chebyshev low-pass prototype is chosen with a FBW of 3.0% at a center frequency (f_0) of 3.0 GHz, and a passband ripple of 0.0432 dB are chosen for the design. The simulated performance is obtained using the computer simulation technology (CST) simulator.

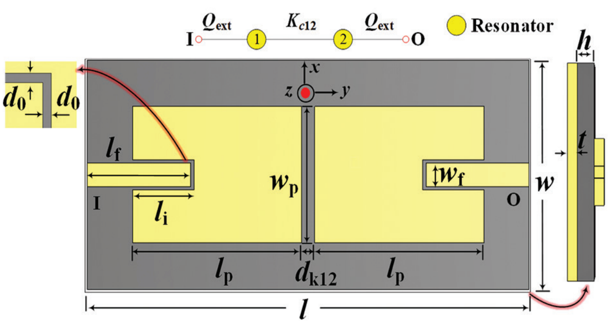


Fig. 1. Topology and physical layout of the second-order BPF. Dimensions in mm are: l=67.09, w=33.68, l_f=16.25, w_f=3.43, l_i=9.50, l_p=26.20, w_p=20, d_0=0.20, h=1.524, t=0.035, d_{k12}=0.8.

2.1. COUPLING MATRIX

The scaled external quality factors ($q_{ext1}= q_{ext2}$), scaled coupling coefficient between direct coupled-resonators ($m_{12}= m_{21}$), and reflection coefficient (S_{11}) of the BPF can be calculated using the relations [33]:

$$q_{\text{ext1}} = g_0 g_1 \quad (1)$$

$$m_{1,2} = \frac{1}{\sqrt{g_1 g_2}} \quad (2)$$

$$S_{11} = \pm\left(1 - \frac{2}{q_{\text{ext1}}}\right).[A]_{11}^{-1} \quad (3)$$

$$S_{21} = 2\frac{1}{\sqrt{q_{\text{ext1}} q_{\text{ext2}}}}.[A]_{11}^{-1} \quad (4)$$

$$[A] = \begin{bmatrix} \frac{1}{q_{\text{ext1}}} & 0 \\ 0 & \frac{1}{q_{\text{ext2}}} \end{bmatrix} + j\frac{1}{FBW}\left(\frac{\omega}{\omega_0} - \frac{\omega_0}{\omega}\right)\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - j\begin{bmatrix} 0 & m_{12} \\ m_{21} & 0 \end{bmatrix} \quad (5)$$

Here g_0, g_1, g_2 are the low-pass prototype parameters, and their values for the given topology can be found in [33] as: g_0=1.0, g_1=0.6648, g_2=0.5445. The ω and ω_0 are the center and passband edge angular frequencies, respectively. The un-scaled external quality factor Q_{ext1} (Q_{ext1}=$qext_1/FBW$) and un-scaled coupling coefficient M_{12} ($M_{12}= m_{12}\, FBW$) are calculated, using the aforementioned relations, and are found to be 22.16 and 0.049, respectively.

2.2. PARAMETRIC EXTRACTIONS

This section describes the extraction of the physical dimensions (d_0, d_{k12}) of the BPF illustrated in Fig. 1 using the calculated values of Q_{ext} and M_{12}. The dimensions of the patches (l_p, w_p) and feedlines (l_f, w_f) are calculated, utilizing the transmission line equations given in [34], and are provided in the caption of Fig. 1. To extract the dimension d0, the set up shown in Fig. 2a is employed. In this configuration, resonator 1 is weakly coupled to the output port (i.e. h_0 is large), while the dimension d_0 is tuned to achieve the desired Q_{ext} value from the S21 response as illustrated in Fig. 2b using the relation [9]:

$$Q_{\text{ext}} = \frac{f_0}{\Delta f_{3dB}} \quad (3)$$

As shown in Fig. 2c, the value of Q_{ext} increases with an increase in the d_0 dimension. The desired value of Q_{ext}=22.16 is obtained when d_0= 0.20 mm.

Fig. 3*a* shows the physical setup used to extract the (M_{12}) between resonators 1 and 2. In this configuration, both resonators are weakly coupled to the input and output ports. The gap dk_{12} is adjusted to achieve the desired M_{12} value from the S_{21} response shown in Fig. 3b using the relation [9]:

$$M_{12} = \frac{f_2^2 - f_1^2}{f_2^2 + f_1^2} \quad (4)$$

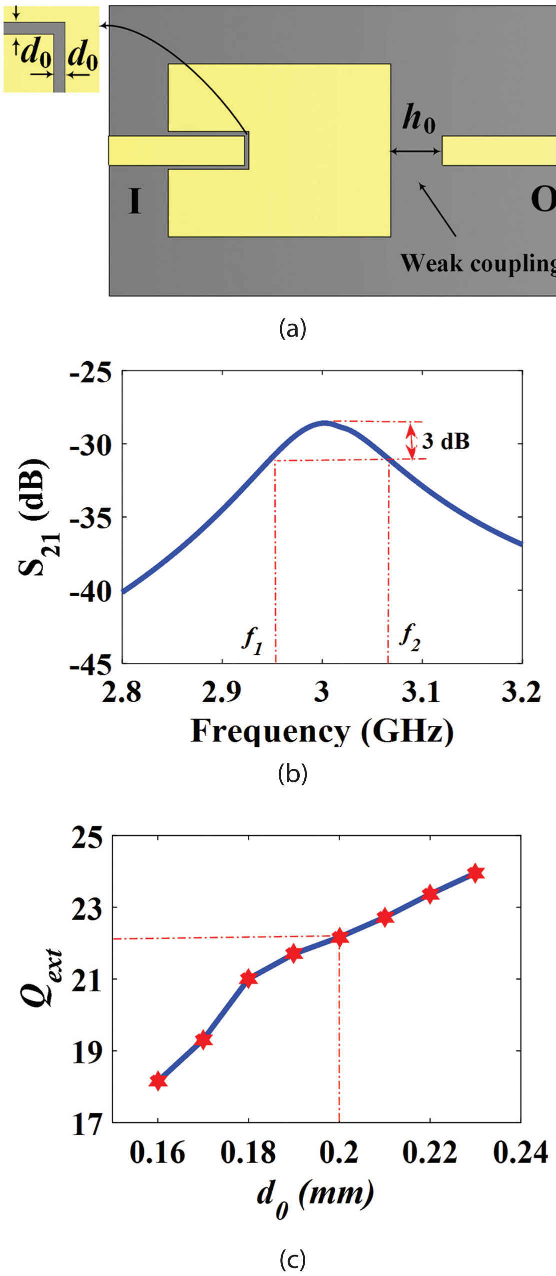


Fig. 2. (**a**) Physical layout set up for d_0 extraction, (**b**) its S_{21} response, and (c) variation of Q_{ext} versus d_0

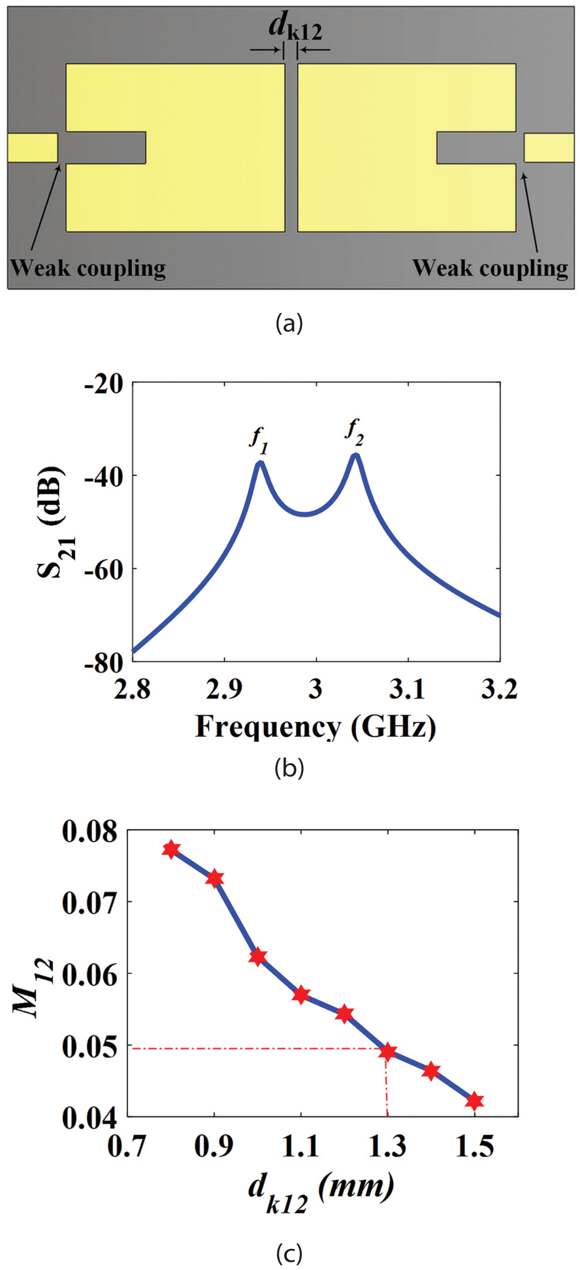


Fig. 3. (**a**) Physical layout set up for dk_{12} extraction, (**b**) S_{21} response, and (c) variation of M_{12} versus dk_{12}

Here, the f_1 and f_2 represent the split resonant frequencies of resonators 1 and 2, respectively. As illustrated in Fig. 3c, the value of M_{12} reduces with an increase in the gap d_{k12}. The required value of M_{12}=0.049 is achieved when d_{k12}=1.28 mm.

The dimensions d_0 and d_{k12} extracted above are considered as their initial values, and optimization is performed in CST to achieve the desired results. Fig. 4 shows the S_{11} and S_{21} responses of the proposed BPF, obtained both from the coupling matrix equations 4 and 5 and from CST simulator. As shown, the simulated and calculated results are in excellent agreement within the operating frequency band. The designed filter achieves a FBW of 3.0% centered at 3.0 GHz, with an insertion loss of 0.8 dB over the passband. The filter also exhibits a selectivity better than 30 dB in both the lower and upper stopbands.

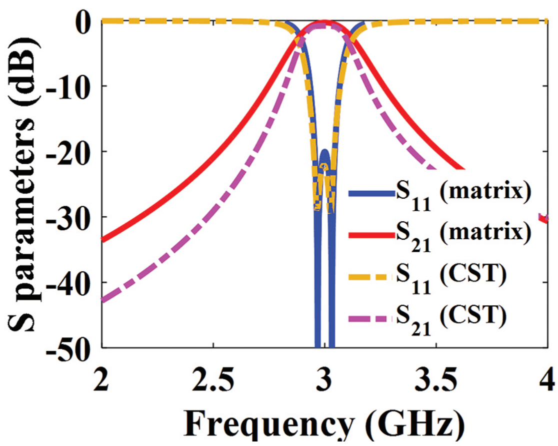


Fig. 4. Simulated and calculated S_{11} and S_{21} responses of the proposed second-order BPF.

3. FILTERING ANTENNA DESIGN

The topology and its corresponding physical layout of the proposed second-order filtering microstrip patch antenna is shown in Fig. 5. Unlike the BPF, where resonator 2 is coupled to an electrical output port, the filtering microstrip patch antenna connects resonator 2 (so-called *radiating-radiator*) to free space, enabling radiation at center frequency of 3.0 GHz. To keep its filtering functionality function alongside its radiation role within the bandwidth of interest, the dimensions of the *radiating resonator* and the coupling gap (d_{s12}) between resonators 1 and *radiating resonator* must be carefully optimized. Specifically, the Q_r value of the *radiating resonator* must match the Q_{ext} at the input port (i.e. $Q_r=Q_{ext}=22.16$) to ensure balanced power distribution and proper filtering performance.

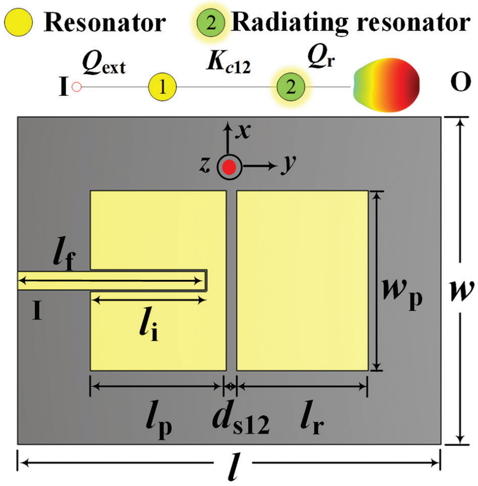
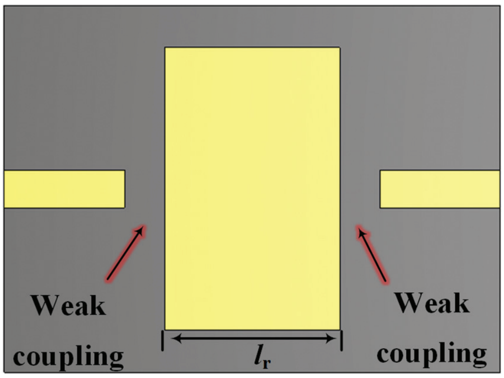


Fig. 5. Topology and physical layout of the second-order filtering antenna. Dimensions in mm are: l=80.28, w=61.78, l_f=35.59, w_f=3.43, l_i=22.0, l_p=25.70, l_r=24.90, w_p=34, d_0=0.30, h=1.524, t=0.035, d_{s12}=1.9

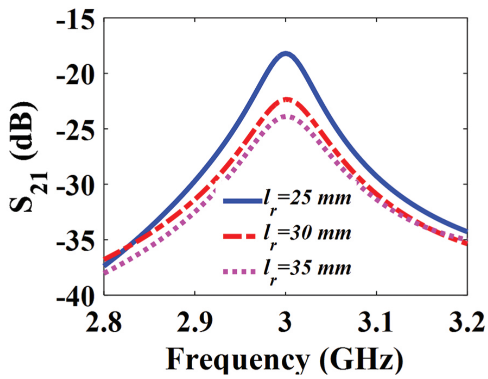
3.1. PARAMETRIC EXTRACTIONS

The configuration shown in Fig. 6a is utilized to extract the Q_r of the *radiating resonator*, following the procedure outlined in section 2.2. In this setup, the *radiating resonator* is very weakly coupled to the input and output ports. From the simulated S_{21} response shown in Fig 6b, the required Q_r is determined using the Δf_{3dB} magnitude and applying into equation 3. To minimize the number of design variables, only the length of the *radiating resonator* (l_r) is adjusted to control the Q_r value. As shown in Fig. 6b, the Δf_3dB value decreases (Q_r increases) with an increase in l_r dimension.

Fig. 7a shows the physical setup used to extract the coupling gap (d_{s12}) between resonator 1 and the *radiating resonator*. By following the extraction method described in Section 2.2 and inserting the split resonance frequencies of resonator 1 (f_1) and *radiating resonator* (f_r) obtained from the simulated S_{21} response shown in Fig. 7b into equation 4, the required M_{12} value can be determined by adjusting d_{s12} dimension.

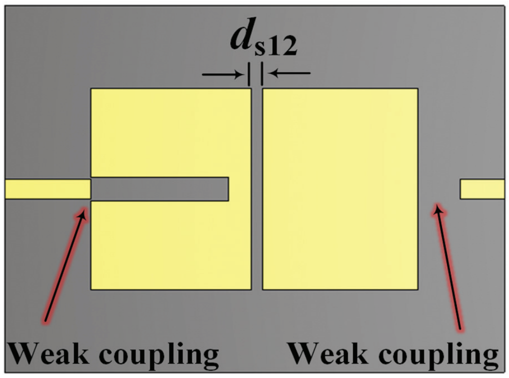


(a)

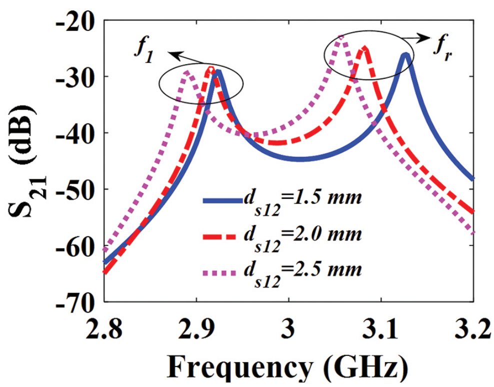


(b)

Fig. 6. (a) Physical layout set up for Q_r extraction, (b) its S_{21} response



(a)



(b)

Fig. 7. (**a**) Physical layout set up for d_{s12} extraction, and (**b**) S_{21} response

3.2. SIMULATED RESULTS AND COMPARISON

Fig. 8 compares the simulated responses of the proposed second-order BPF and the second-order filtering antenna. The S_{11} responses of both designs show excellent agreement across the operating frequency band. Furthermore, the normalized realized gain of the filtering microstrip patch antenna exhibits a filter-like S_{21} response within the passband of interest. Discrepancies observed at the lower and upper stop bands are attributed to unexpected radiation from patch structures.

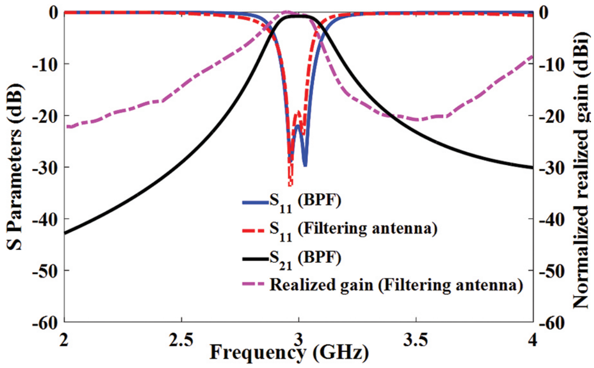
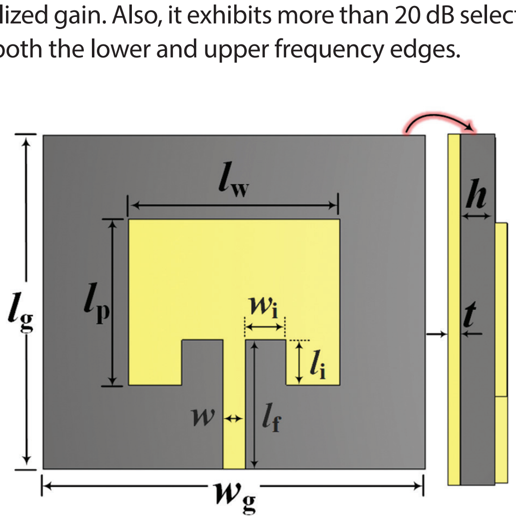
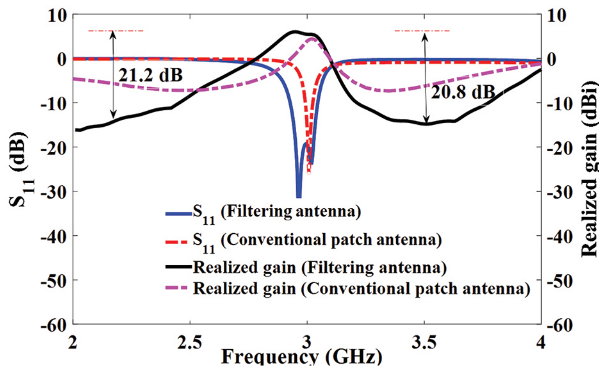


Fig. 8. Simulated S_{11}, S_{21} and realized gain of the proposed BPF and filtering antenna

To demonstrate the advantages of the proposed filtering antenna, its performance is compared with that of a conventional rectangular microstrip patch antenna, as shown in Fig. 9a. The dimensions of the patch are calculated based on the cavity model theory [34-36], and are provided in the caption of Fig. 9. For consistency, the materials used in the ground plane, patch, and substrate of the conventional patch antenna are the same as those employed in the proposed filtering antenna. The simulated S_{11} and realized gain of both conventional and proposed filtering patch antennas are shown in Fig. 9b. The proposed filtering microstrip patch antenna exhibits several improvements over the conventional one. For instance, within the passband, it provides a 1.0 dBi higher realized gain. Also, it exhibits more than 20 dB selectivity at both the lower and upper frequency edges.



(a)



(b)

Fig. 9. (**a**) Layout of a conventional rectangular microstrip patch antenna. (**b**) Simulated S_{11} and realized gain responses of proposed filtering microstrip patch antenna and conventional rectangular patch antenna. Dimensions in mm are: l_g=54.11, w_g=60.20, l_i=7.20, w_i=6.50, l_f=20.60, w=3.43, l_w=33.40, l_p=26.33.

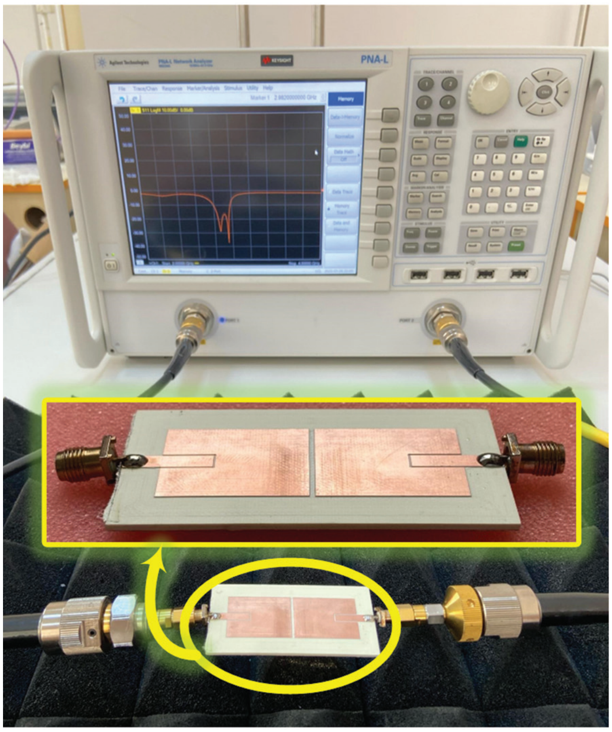
This enhanced selectivity can potentially eliminate the need for an additional BPF in the front-end of the wireless system, thereby reducing mismatch and insertion losses. The 10-dB FBW of the filtering microstrip patch antenna is 3.97%, which is approximately three times wider than that of the conventional patch antenna.

4. FABRICATIONS AND MEASUREMENTS

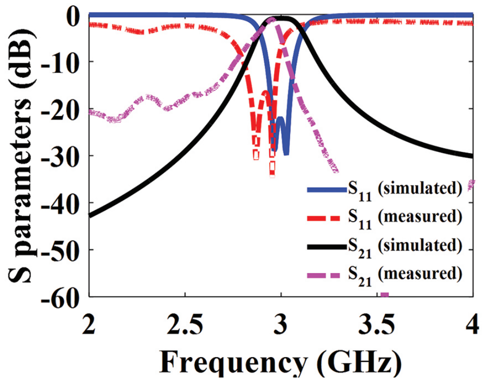
Fig. 10a shows the actual photograph of the proposed BPF under test. The scattering parameters were measured using an Agilent Vector Network Analyzer (VNA). Fig. 10b compares the measured and simulated S_{11} and S_{21} responses. The measured 10-dB FBW is 3.10 %, which is slightly larger than the simulated value of 3.0 %. The measured insertion loss across the passband is 1.10 dB, compared to 0.80 dB in simulation. The 3-dB passband bandwidths from the measurement and simulation are 0.10 GHz and 0.22 GHz, respectively. The measured start stop band rejection is below 20 dB, while the upper stop band reaches approximately 35 dB. The measured center frequency is 2.9 GHz, exhibiting a downward shift of 0.1 GHz from the simulated 3.0 GHz. These discrepancies are mainly attributed to fabrication tolerances, SMA connector effects, and dielectric loss.

Fig. 11a shows the manufactured filtering antenna. The S_{11} response was measured using the VNA. Radiation patterns were measured in an anechoic chamber room using a wide bandwidth reference horn antenna positioned in the far-field region. As shown in Fig. 11b, the measured S_{11} and realized gain match the simulated results across the operating frequency band. The measured 10-dB FBW is 4.05%, which is slightly wider than the simulated value of 3.97%. The realized gain across the passband is relatively flat, with a fluctuation of approximately 0.68 dBi. The measured peak gain is 6.0 dBi at 2.95 GHz, and the 3-dB gain bandwidth is 7.0%. Realized gain selectivity of around 20 dB is observed at both lower and upper frequency bands. Fig. 12 a shows the measured total efficiency, calculated as the ratio of measured realized gain to the simulated directivity. It is exceeding 74% within the passband, slightly lower than the simulated 81.0%. The efficiency degradation is attributed to the frequency-dependent variation of the substrate loss tangent and the unexpected radiation from the microstrip coupling edges. As depicted in Figs. 12 b and 12 c, the measured E-plane and H-plane radiation patterns align well with the simulations. The slight discrepancies in the backside radiation are likely due to the presence of the SMA connector and the transmission cable during the measurement.

Table 1 compares the measured performance of the proposed filtering microstrip patch antenna with related designs reported in the literature. Among the cited works, only [37] and the present design achieve filtering characteristics without requiring additional circuitry. The filtering antennas presented in [30, 32] demonstrate relatively high gains of 10 dBi and 7.55 dBi, respectively; however, their large physical dimensions and moderate FBW reduce their suitability for ISM band applications due to occupying larger area and limiting the operating frequency range. The designs in [37, 38] exhibit strong frequency selectivity at both lower and upper stop bands, but the low realized gains are as their main drawbacks. Antennas in [39] and [40] provided large bandwidths, but their bulky size and low gain are their main drawbacks. In contrast, the proposed filtering microstrip patch antenna offers a competitive profile, combining compact size, moderate bandwidth, high gain, and high efficiency. These features are extremely demanded for ISM band applications.

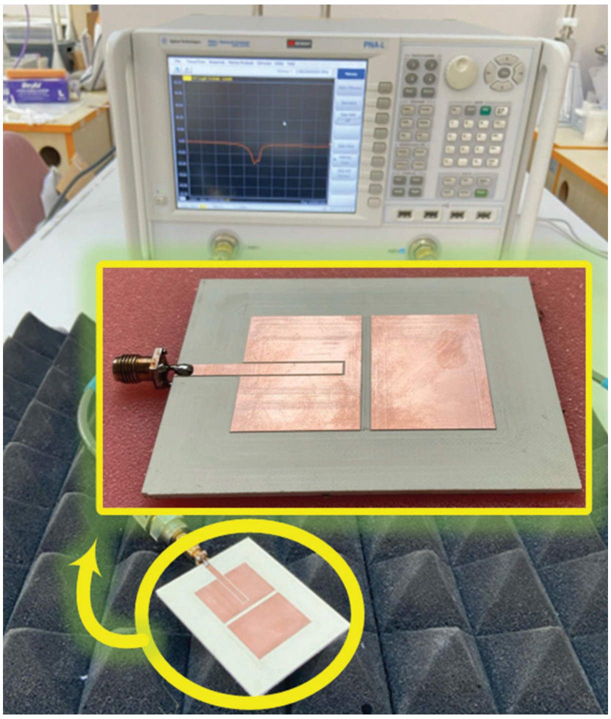


(a)

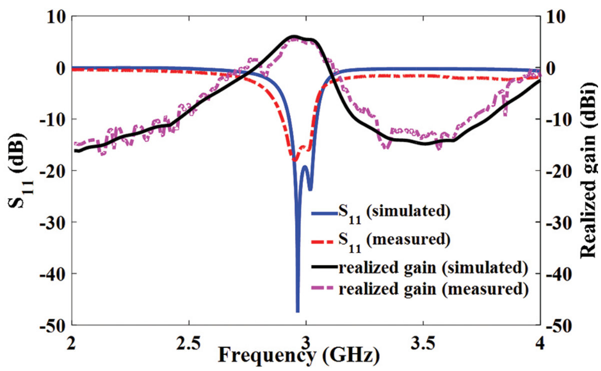


(b)

Fig. 10. (**a**) Actual BPF under test, and (**b**) measured S11 and S21 performances of BPF compared with simulated ones



(a)

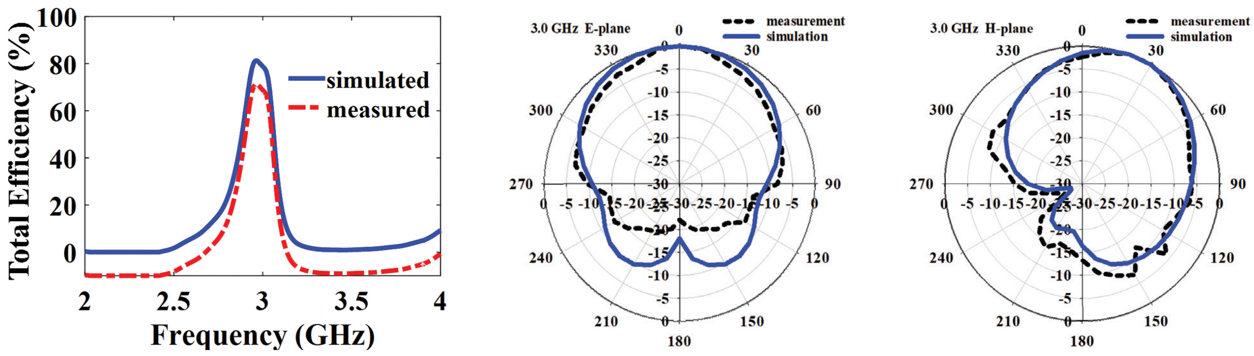


(b)

Fig. 11. (**a**) Actual filtering microstrip patch antenna under test, and (**b**) measured S_{11} and realized gain performances of filtering microstrip patch antenna compared with simulated ones

Table 1. Performance of the proposed filtering microstrip patch antenna compared with some related works

Refs.	Antenna types	f0 (GHz)	Size (λ_0^3)	10-dB FBW (%)	Peak gain (dBi)	Lower/Upper Rejection level (dB)	Total Efficiency (%)	extra circuit or structure
[6]	H-shaped patch	2.45	0.361×0.426×0.013	< 4.0	6.0	-40.1/-39	> 90	Yes
[30]	Slot-loaded patch	9.8	1.96 ×1.50×0.026	5.1	10	NA	> 90	Yes
[32]	Rectangular patch	10	0.94×0.94×0.017	3.7	7.55	17/17	NA	Yes
[37]	Rectangular patch	2.0	NA	2.03	5.0	15/23	NA	No
[38]	U-shaped split ring	3.6	18.33×11.11×0.27	33.4	4.5	> 20	NA	Yes
[39]	Monopole	3.8	0.31×0.83×0.011	62.9	3.0-3.5	NA	NA	Yes
[40]	U-shaped parasite patch	5.5	0.94×0.94×0.066	26.38	7.98	11	> 92	Yes
This work	Rectangular Patch	3.0	0.67 ×0.33×0.0152	4.05	6.0	21.2/20.5	74.0	No



(a) (b) (c)

Fig. 12. (**a**) measured total efficiency compared with simulation. (**b**) measured E-plane, and (**c**) H-plane patterns compared with simulated ones.

5. CONCLUSIONS

This paper presented a novel design approach for a filtering microstrip patch antenna based on the coupling matrix approach. The matrix elements were utilized to extract the physical dimensions of the antenna and to embed filtering characteristics without the need for additional physical structures. Two prototypes were fabricated, and the measured results showed good agreement with the simulated predictions, validating the proposed coupling matrix design approach. The proposed filtering microstrip patch antenna demonstrated competitive performance and is a promising candidate for ISM band applications.

ACKNOWLEDGEMENT

The authors would like to thank the EDT Research Center at the School of Engineering, University of Birmingham, and Iskenderun Technical University for providing technical support for antenna performance measurements. This work was supported by Salahaddin University-Erbil.

REFERENCES:

[1] C. Chen, “A single-layer single-patch dual-polarized high-gain cross-shaped microstrip patch antenna”, IEEE Antennas and Wireless Propagation Letters, Vol. 22, No. 10, 2023, pp. 2417-2421.

[2] R. H. Mahmud, “Terahertz microstrip patch antennas for the surveillance applications”, Kurdistan Journal of Applied Research, Vol. 5, No. 1, 2020, pp. 16-27.

[3] G. Mansour, E. Nugoolcharoenlap, R. H. Mahmud, T. Tippo, P. Akkaraekthalin, D. Torrungrueng, “Circularly Polarized Elliptical Patch Array Antennas for GPS”, Proceedings of the Research, Invention, and Innovation Congress: Innovation Electricals and Electronics, Bankok, Tahiland, 1-3 September 2021, pp. 92-96.

[4] R. Y. Khattak, Q. Z. Ahmed, S. Shoaib, P. I. Lazaridis, T. T. Alade, “Recent advances in antennas for biotelemetry and healthcare applications”, IEEE Open Journal of Antennas and Propagation, Vol. 5, No. 6, 2024, pp. 1499-1522.

[5] C. Liu, Y.-X. Guo, S. Xiao, “Capacitively loaded circularly polarized implantable patch antenna for ISM band biomedical applications”, IEEE transactions on antennas and propagation, Vol. 62, No. 5, 2014, pp. 2407-2417.

[6] Z. Zheng, D. Li, X. Tand, M. Wang, Y. Deng, "Compact low-profile differential filtering microstrip patch antenna with high selectivity and deep rejection using single-layer substrate", IEEE Access, Vol. 9, No. 1, 2021, pp. 76047-76055.

[7] H. Jin, G. Q. Luo, W. Che, K.-S. Chin, Y. Pan, Y. Yu, "Vertically-integrated differential filtering patch antenna excited by a balun bandpass filter", IET Microwaves, Antennas & Propagation, Vol. 13, No. 3, 2019, pp. 300-304.

[8] L. Ma, Z. Shao, J. Lai, C. Gu, J. Mao, "Bandwidth enhancement of H-plane MIMO patch antennas in integrated sensing and communication applications", IEEE Open Journal of Antennas and Propagation, Vol. 5, No. 1, 2023, pp. 90-103.

[9] R. H. Mahmud, H. N. Awl, Y. I. Abdulkarim, M. Karaaslan, M. J. Lancaster, "Filtering two-element waveguide antenna array based on solely resonators", AEU-International Journal of Electronics and Communications, Vol. 121, 2020, p. 153232.

[10] R. H. Mahmud, M. J. Lancaster, "High-gain and wide-bandwidth filtering planar antenna array-based solely on resonators", IEEE Transactions on Antennas and Propagation, Vol. 65, No. 5, 2017, pp. 2367-2375.

[11] C.-K. Lin, S.-J. Chung, "A filtering microstrip antenna array", IEEE transactions on microwave theory and techniques, Vol. 59, No. 11, 2011, pp. 2856-2863.

[12] J. Guo, Y. Chen, D. Yang, K. Sun, J. Pan, S. Liu, "Design of wideband filtering patch antenna array with high aperture efficiency and good filtering performance", IEEE Transactions on Antennas and Propagation, Vol. 72, No. 1, 2023, pp. 974-979.

[13] D. Yang, H. Zhai, C. Guo, H. Li, "A compact single-layer wideband microstrip antenna with filtering performance", IEEE Antennas and Wireless Propagation Letters, Vol. 19, No. 5, 2020, pp. 801-805.

[14] H.-Y. Xie, B. Wu, L.-W. Song, Y.-L. Xin, J.-Z. Chen, T. Su, "High-gain third-order filtering patch antenna array with two radiation nulls using cross-radiation", IEEE Transactions on Circuits and Systems II: Express Briefs, Vol. 70, No. 11, 2023, pp. 4053-4057.

[15] J. Liang, D. Wang, Z. Qi, Y. Gao, Q. Wei, "Design of A Microstrip Filtering Antenna without Extra Circuits and Its Application in Orbital Angular Momentum (OAM) Filtering Antenna", Progress In Electromagnetics Research Letters, Vol. 11, 2024, pp. 1-8.

[16] W. Yang, Y. Zhang, W. Che, M. Xun, Q. Xue, G. Shen, "A simple, compact filtering patch antenna based on mode analysis with wide out-of-band suppression", IEEE Transactions on Antennas and Propagation, Vol. 67, No. 10, 2019, pp. 6244-6253.

[17] C. Chen, "A compact wideband endfire filtering antenna inspired by a uniplanar microstrip antenna", IEEE Antennas and Wireless Propagation Letters, Vol. 21, No. 4, 2022, pp. 853-857.

[18] Q. Liu, L. Zhu, "A compact wideband filtering antenna on slots-loaded square patch radiator under triple resonant modes", IEEE Transactions on Antennas and Propagation, Vol. 70, No. 10, 2022, pp. 9882-9887.

[19] C. Chen, "A wideband coplanar L-probe-fed slot-loaded rectangular filtering microstrip patch antenna with high selectivity", IEEE Antennas and Wireless Propagation Letters, Vol. 21, No. 6, 2022, pp. 1134-1138.

[20] H. Chang, M. Liu, D. Lin, J. Wang, "A compact single layer filtering antenna with DGS for 5.1 GHz application", Progress In Electromagnetics Research Letters, Vol. 107, 2022, pp. 1-7.

[21] L. Li, G. Liu, "A differential microstrip antenna with filtering response", IEEE Antennas and Wireless Propagation Letters, Vo. 1, No. 5, 2016, pp. 1983-1986.

[22] B. Maity, S. K. Nayak, "Compact bowtie-shaped microstrip patch antennas with low cross-polarization and wideband harmonic suppression", AEU-International Journal of Electronics and Communications, Vol. 168, 2023, p. 154699.

[23] G. Liu, P. F. Hu, G. D. Su, Y. M. Pan, "Bandwidth and gain enhancement of a single-layer filtering patch antenna using reshaped TM mode", IEEE Antennas and Wireless Propagation Letters, Vol. 23, No. 1, 2023, pp. 314-318.

[24] R. Wu, W. Liu, Z. Jiang, W. Kuang, "A Low-Profile Broadband Filtering Antenna and Its Array for 5G Applications", IEEE Antennas and Wireless Propagation Letters, Vol. 23, No. 10, 2024, pp. 29220-2924.

[25] X. Lin, W. Liu, Z. Jiang, W. Kuang, "Broadband Filtering Circularly Polarized Patch Antenna Based on Ground Slot and Coupling Stub", IEEE Open Journal of Antennas and Propagation, 2025. (in press)

[26] M. Li, S. Tian, M.-C. Tang, L. Zhu, "A compact low-profile hybrid-mode patch antenna with intrinsically combined self-decoupling and filtering properties", IEEE Transactions on Antennas and Propagation, Vol. 70, No. 2, 2021, pp. 1511-1516.

[27] X. Chen, Q. Zhuge, G. Han, R. Ma, J. Su, Wenmei Zhang, "A wideband harmonic suppression filtering antenna with multiple radiation nulls", Progress In Electromagnetics Research Letters, Vol. 112, 2023, pp. 15-23.

[28] H. Gui, Z. Wang, W. Nie, M. Yang, M. Wang, "Design of a Compact Wideband Filtering Antenna with High Frequency Selectivity", Progress In Electromagnetics Research M, Vol. 131, 2025, pp. 27-35.

[29] S. Liu, Z. Wang, Y. Dong, "A compact filtering patch antenna with high suppression level and its CP application", IEEE Antennas and Wireless Propagation Letters, Vol. 22, No. 4, 2022, pp. 769-773.

[30] S. Ramkumar, M. Saravanan, S. Saran, S. S. Varshith, "A high gain filtenna with radiation nulls using a novel split-merge feed line on a slot-loaded rectangular patch for X-band RADAR application", AEU-International Journal of Electronics and Communications, Vol. 196, 2025, p. 155789.

[31] N. García-Alcaide, A. Fernandez-Prieto, R. R. Boix, V. Losada, J. Martel, F. Medina, "Design of broadband aperture-coupled stacked microstrip antennas using second-order filter theory", IEEE Transactions on Antennas and Propagation, Vol. 70, No. 7, 2022, pp. 5345-5356.

[32] Ji, S., Y. Dong, Y. Fan, "Bandpass filter prototype inspired filtering patch antenna/array", IEEE Transactions on Antennas and Propagation, Vol. 70, No. 5, 2021, pp. 3297-3307.

[33] J.-S. G. Hong, M. J. Lancaster, "Microstrip filters for RF/microwave applications", 1st Edition, John Wiley & Sons, 2004.

[34] C. A. Balanis, "Antenna theory: analysis and design", 4th Edition, John Wiley & Sons, 2016.

[35] S. O. Hasan, S. K. Ezzulddin, O. S. Hammd, R. H. Mahmud, "Design and performance analysis of rectangular microstrip patch antennas using different feeding techniques for 5G applications", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 8, 2023, pp. 833-841.

[36] S. O. Hasanet, S. K. Ezzulddin, R. H. Mahmud, M. J. Ahmed, "Design and simulation of microstrip antenna array operating at S-band for wireless communication system", International Journal of Electrical and Computer Engineering Systems, Vol. 14, No. 5, 2023, pp. 497-506.

[37] G. Mansour, M. J. Lancaster, P. S. Hall, P. Gardner, E. Nugoolcharoenlap, "Design of filtering microstrip antenna using filter synthesis approach", Progress In Electromagnetics Research, Vol. 145, 2014, pp. 59-67.

[38] X. Yang, L. Cui, Z. Ding, Z. Zhang, "A 5G filtering antenna simultaneously featuring high selectivity and band notch", AEU-International Journal of Electronics and Communications, Vol. 153, 2022, p. 154299.

[39] M. Ribó, M. Cabedo-Fabrés, L. Pradell, S. Blanch, M. Ferrando-Bataller, "Multimodal planar monopole filtenna for 5G applications", AEU-International Journal of Electronics and Communications, Vol. 180, 2024, p. 155338.

[40] W. Huang, P. Wang, S. Hou, "Wideband filtering antenna loading U-shaped parasitic patches based on characteristic mode analysis", Scientific Reports, Vol. 15, No. 1, 2025.

Area and Power Optimized Architecture of Sample Rate Converter for IoT Gateway Applications

Original Scientific Paper

Swetha Pinjerla*
Department of ECE, Jawaharlal Nehru Technological University,
Hyderabad, India
pswetha0823@gmail.com

Surampudi Srinivasa Rao
Department of ECE, Muffakham Jah College of Engineering and Technology,
Hyderabad, India
ssrao.atri@gmail.com

Puttha Chandrasekhar Reddy
Department of ECE, Jawaharlal Nehru Technological University,
Hyderabad, India
drpcsreddy@gmail.com

*Corresponding author

Abstract – *Nowadays, the Internet of things plays a major role in society for various applications such as medical diagnostics, telecommunications, agriculture, mobile computing, broadcasting, video surveillance etc. In Internet of Things (IoT) networks, several sensors with different data rates should be integrated to perform overall control or monitoring processes.High-speed data transmission technologies should be needed to communicate with IoT servers or storage. Generally, a gateway device is used to integrate low-data rate devices and IoT interfaces. Field Programmable Gate Array Logic (FPGA) can be utilized to implement high-speed and low-power gateway. The paper suggests a design of an FPGA-based IoT gateway architecture, which allows multi-protocol communications and an effective way of controlling sample rates. The design provides RF transceivers, protocol specific modules, and dynamic Sample Rate (SR) Selector to support smooth synchronization of data between diverse IoT devices. Clock generation and control blocks guarantee adaptive frequency assignment and upsampling and downsampling CIC filtering-based units ensure good signal conditioning. Experimental analysis shows that the presented method creates the low root mean square error (RMSE): 1.2 percent (downlink) and 1.4 percent (uplink), and high signal to noise ratios (SNR): 26.3 dB (downlink) and 24.8 dB (uplink) in 45 nm CMOS technology, resulting in better results than conventional 180 nm implementations. The Application-Specific Integrated Circuit (ASIC) implementation achieved a compact core area, reducing from 2.3 μm² at 180 nm to 0.3 μm² at 45 nm, demonstrating significant area efficiency with technology scaling. The results affirm that the architecture can provide reliable and high-quality data transfers of next-generation IoT gateways.*

Keywords: *Internet of things, Sample Rate Converter, Digital Gateway, IoT interface, Field Programmable Gate Array Logic, Xilinx FPGA*

Received: June 2, 2025; Received in revised form: September 9, 2025; Accepted: October 24, 2025

1. INTRODUCTION

FPGAs function as cost-effective integrated tools used in communication systems and various other application domains that continue to evolve. Software Defined Radio (SDR) systems employing FPGAs for hardware acceleration provide processors with extensive capabilities for deploying waveforms that promise both reconfigurability and portability.

A sampling rate conversion system contains the decimation filter (decimator) which serves as its foundational element. The decimation filter executes both low-pass filtering together with down-sampling operations. The filter changes high-frequency high-bit-rate low-resolution data into low-frequency high-resolution data. The system finds its primary applications in the areas of speech processing as well as radar antenna and communication systems. In recent years, researchers have actively worked on developing decimation filters with enhanced performance. Decimation depends on both a high-quality low-pass filter and a sampling rate converter to perform frequency reduction of the sampling data [1].

The changing of sampling rates for processed digital signals becomes vital or practical in numerous signal processing applications. The actual task proves simple for most cases yet high-ratio interpolation and decimation operations need digital low-pass filters to maintain small bandwidth areas along with narrow transition bands. When filter requirements include long impulse response duration it leads to very complex implementations for both interpolation and decimation algorithms. A solution to Frequency Response Masking (FRM) involves splitting the resampling filter design into separate filters with more achievable specifications. The implementation complexity decreases when non-zero coefficients are reduced across the entire filter structure in the design results [2].

Telecommunication businesses adopt Digital Down Converter (DDC) technology as their primary tool. Suppliers select DDC converters as a standard component for cellular phones. A cell phone chip contains variable frequency amplifiers together with high-speed (12 or 14 bits) Analog-to-Digital converters and DDC. Design operating specifications of the parts range from 50 MHz to 65 MHz with oscillations enabling usage of Signal parts at frequencies up to 300 MHz. DDC enables users to program the frequency together with bandwidth settings during data conversion operations. The conversion operation together with filtering takes place digitally through a linear sequence. The combination of DDC and a digital I / Q demodulator functions with frequency programmability [3]. Fixed-ratio multi-rate techniques using L/M, where both are positive integers, serve as standard sample rate conversion (SRC) methods.The B-spline interpolation performs the conversion process to change the sample rate. The approach enables the completion of Digital Audio Tape (DAT) to Compact Disc (CD) sample rate conversion while all CD-to-DAT filter coefficients remain unaffected. Hogenauer filters operate as cascaded integrated comb filters for digital systems to deliver major alterations in sampling rates [4].

The processing requirement for sample rate conversion is high while channelisation takes place in this stage. A bandlimited Intermediate Frequency (IF) digital signal processed at a high sampling rate obtains its low-frequency components by mixing it with digital oscillator samples in a quadrature position. After down-conversion, the signal gets decimated to its required sampling rate with subsequent filtering done to it. Paul Burns shows that each channel requires two expensive high-end Digital signal processors (DSPs) during the down-conversion operation. Reconfigurable FPGAs replace Digital signal processors while providing high-skill design options together with accurate computational power and better performance execution [5].

The proposed work introduces an optimized IoT gateway architecture that integrates multiple low-data-rate communication protocols (LoRa, Sigfox, and NarrowBand-Internet of Things (NB-IoT)) with a high-speed Wi-Fi interface using FPGA-based implementation. The core novelty lies in the design of an efficient sample rate conversion strategy, where cascaded CIC filters are employed for both interpolation and decimation processes. To further minimize distortion, the interpolation unit incorporates CIC filtering followed by D flip-flops and an averaging circuit, while the downsampling path integrates D flip-flops before the CIC stage to produce a smooth signal. The proposed architecture is optimized for reduced hardware resource utilization and low power consumption, making it suitable for energy-constrained IoT applications.

The main contributions of this work can be summarized as follows:

- A unified hardware architecture that supports multiple IoT protocols on the sensor side and Wi-Fi on the IoT server side.
- Introduction of cascaded CIC filters with auxiliary circuits (DFFs and averaging units) to reduce high-frequency distortions during upsampling and downsampling.
- Development of a multi-frequency clock generation mechanism using sequential counters and flip-flops to achieve flexible protocol switching with low area overhead.
- The architecture is tailored to minimize slice LUTs, registers, and flip-flops while reducing dynamic and static power consumption on FPGA and the proposed system achieves enhanced reconstruction quality, validated through RMSE and SNR analysis.

2. LITERATURE SURVEY

A review of significant research findings explores modern architectural and methodological strategies which enhance performance for SDR and electronic warfare and real-time data acquisition systems.

The power of the multichannel fractional sample rate convertor could be reduced through the optimization of filter coefficient hamming distance by using Genetic algorithms according to Vivek's proposal. The key element of the multichannel fractional sample rate convertor consists of the Cascaded multiple architecture finite impulse response filter (CMFIR filter). The CMFIR filter works through the successive implementation of CIC & multiply-accumulate architecture (MAC) FIR filter components. The genetic algorithm minimizes how well-matched successive filter coefficients of the CMFIR filter are to each other in terms of the Hamming distance.The reduction of the hamming distance between filter coefficients leads to reduced transitions between the values of 0 and 1 or 1 and 0. The methods minimize both Complementary Metal-Oxide-Semiconductor (CMOS) transistor switching and therefore decrease total Dynamic power usage in multichannel sample rate converters [6]. Brunel et al developed an FPGA circuit for Software Defined Radio applications which executes arbitrary-ratio signal re-sampling between the Low-Frequency band and Very High-Frequency ranges. This SDR application allows designers to manage Spurious-Free Dynamic Range (SFDR) with an easy implementation that functions independently of additional clock requirements which suits FPGA designs with limited clock resources [7]. The architecture proposed by Debarshi et al. consists of a COordinate Rotation Digital Computer (CORDIC) processor as a digital oscillator before a multi-stage CIC filter which acts as a high-rate decimation filter. An MSFIR decimation filter with multiple output channels performs perfect results through its design. Design and implementation of the entire proposed DDC architecture occurred in the Xilinx ISE 14.7 simulator through optimization techniques targeted to operate on a Xilinx Kintex-7 FPGA device. Implementing DDC on FPGA offers high flexibility, moderate cost, and customizable design options [8].

Xinxing et al. put forward an optimization design method which implements parallel digital down-conversion combined with polyphase filtering. The mathematical model of high-speed digital down-conversion starts with derivation followed by an efficient implementation design of traditional DDC architecture. A down-conversion structure for high-speed frequencies has been designed through parallel filtering and frequency conversion. The paper provides instructions for two main design aspects of parallel frequency conversion parameters and multi-path filter coefficient calculation methods [9]. The acquisition system designed by Dai et al incorporates a 5Gsps real-time sampling rate together with PXI bus-based mass storage. A system sampler achieves parallel sampling through its multi-core analog-to-digital converter (ADC). The system features an exact sampling timer along with sufficient digital values that support real-time sampling performances. FPGA technology serves as the solution to acquire fast data samples from the ADC.The serial-to-parallel module in the FPGA reduces the data rate. The trigger detection unit functions to manage storage procedures to increase detection capabilities for short-duration signals. The system gains improved capability to acquire high-speed signals because of its designed mass data storage structure [10].

Xiang et al. details an FPGA based analog to digital converter implementation tailored for extreme cryogenic conditions (liquid helium). They propose a soft-core, multi-lane ADC architecture—likely implying parallel digitization channels implemented as FPGA IP—to function robustly at extremely low temperatures. This work is significant because typical ADC hardware fails in cryogenic environments, and soft-core logic on FPGA provides flexibility and resilience. Applications could include quantum computing sensors or space-based cryogenic instrumentation [11]. Agarwal and Bopanna presents a reconfigurable pipelined architecture for a sample-rate conversion (SRC) filter, optimized for software-defined radio (SDR) receivers. Utilization of pipelining suggests a focus on high throughput and timing efficiency. The architecture likely supports dynamic reconfiguration, enabling different sample rates on-the-fly in SDR contexts, improving flexibility and performance under changing operational conditions [12]. Liu et al. introduces an FPGA design that executes 1024-channel channelization—dividing an input wideband signal into 1024 narrower sub-bands—for SDR applications. The architecture is reconfigurable, enabling adjustments to channel characteristics (like bandwidth or center frequency). This is particularly relevant for high-density SDR systems and spectral processing, such as cognitive radio or multiprotocol monitoring [13].

Zeineddine et al. propose an FPGA-based approach for arbitrary sample-rate conversion, facilitating multi-standard digital front-ends in one flexible architecture. This is key for devices that must handle diverse standards requiring different sampling rates. The focus is on efficiency—both in resource use and performance—supporting seamless interoperability among multiple RF standards [14]. Agarwal and Bopanna et al. describes a multi-rate filtering architecture for SDR receivers utilizing distributed arithmetic (DA). DA allows multiplierless implementation, saving FPGA logic, and offers low-latency, area-efficient performance, which is critical in real-time SDR applications. The multi-rate capability indicates adaptability to different sampling frequencies or standards [15].

Different effective approaches in multichannel sample rate conversion and digital down-conversion and high-speed data acquisition surface through the reviewed studies. Multichannel sample rate conversion systems achieve increased power efficiency and computational performance through Genetic Algorithms alongside FPGA-based architectures and parallel processing methods. The incorporation of modern filter structures with re-sampling protocols boosted SDR and electronic warfare system capabilities. Data processing together with storage at high speeds turns out to be highly effective when implemented using FPGA-based acquisition systems.The developed innovations create a solid basis which researchers can use to establish improved digital signal processing technologies that utilize resources efficiently at scale.

3. AREA AND POWER OPTIMIZED ARCHITECTURE OF SAMPLE RATE CONVERTER FOR IOT GATEWAY APPLICATIONS

3.1. IOT GATEWAY

The fast expansion of the IoT demands the incorporation of heterogeneous devices and communications protocols that have different power and networking capacities. The IoT gateways have thus become a very important element, allowing smooth connectivity and offering the computing power required in an edge computing environment. A home Internet Gateway links the Local Area Network (LAN) to the Internet Service

Provider network [16]. The IoT devices establish connections to the IoT Gateway through various wireless protocols that include Sub-Gigahertz (Sub-GHz), Long Range Wide Area Network (LoRaWAN), Sigfox, Long-Term Evolution (LTE), LTE-Machine Type Communication (LTE-M), and Wi-Fi. The system establishes Internet connectivity (Public Cloud) through either Ethernet LAN or Fiber Optics Wide Area Network (WAN) network connections. The connection between IoT devices and IoT Gateway and connected IoT systems as illustrated in Fig. 1 [17].

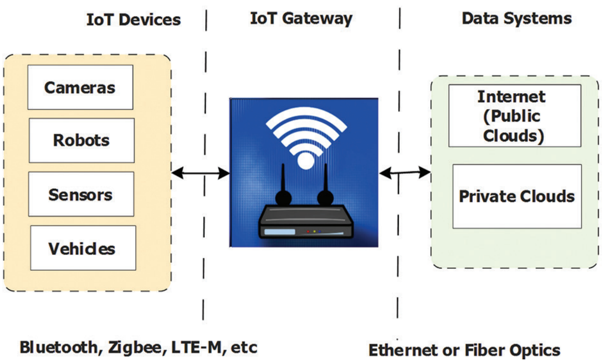


Fig. 1. Interface with IoT devices, IoT Gateway and, IoT systems

3.2. LORA

LoRa is a low-power wide-area network (LPWAN) modulation technology developed by Semtech, designed for long-range connectivity with minimal energy consumption. It enables communication up to 3 miles (5 km) in urban areas and over 10 miles (15 km) in rural environments. LoRaWAN, the networking standard built on LoRa, employs a star topology to connect large numbers of low-power devices requiring deep indoor or wide-area coverage [18].

3.3. SIGFOX

Sigfox is an ultra-narrowband low-power wide area network (LPWAN) technology that supports Binary Phase-Shift Keying (BPSK) modulation to transport data on unlicensed bands of the radio spectrum, including the 915 MHz ISM band in the US. Its end point radios are simple and make the devices low cost and low powered, whereas the communication is handled by complex base stations. Sigfox can transmit very low data rates, up to 300 baud, with small 12 bytes of payload per message. The uplink communication is mainly based on DBPSK and downlink on GFSK. Its long range low power transmission makes it applicable in smart metering and remote sensing, although the limited bandwidth is a disadvantage [19].

3.4. NBIOT

NB-IoT is an LPWAN based on standards that can support large-scale IoT deployments with improved power efficiency, capacity, and spectrum use. It enables deep indoor and rural coverage with ultra-low device complexity, enabling battery life of more than a decade. NB-IoT module is affordable, similar to Global System for Mobile Communications / General Packet Radio Service (GSM/GPRS) modules, and has the advantages of lower manufacturing costs the more it is adopted [20].

3.5. PROPOSED FPGA ARCHITECTURE

Fig. 2 shows the proposed FPGA-based architecture of an IoT gateway that enables multi-protocol communication and an efficient SRC. The RF transceivers have been used at the top and bottom of the framework to support the wireless communication interfaces that allow two-way data traffic between the IoT sensor nodes and the central gateway. The FPGA has a number of dedicated modules that work in unison to provide smooth protocol integration and data synchronization, as well as optimization of sample rates. The Wi-Fi interface provides high-speed access to IoT servers and storage and is the main data upload and downstream control channel.

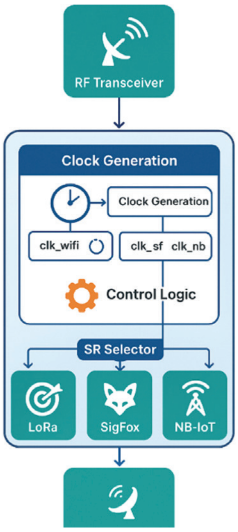


Fig. 2. Proposed Architecture

There is a special clock generation unit which generates numerous synchronised clock signals- such as clk_{WiFi} , clk_{sf}, clk_{nb}, and clk_{lora} which are in line with various wireless standards. A clock control block manages these clock signals and enables the flexibility and adaptive frequency assignment to various sensor protocols. The design can be considered as a central module, the Sample Rate (SR) Selector that enables a dynamic switch between different IoT communication protocols such as LoRa, Sigfox, and NB-IoT. All these communication blocks contain upsampling (U) and downsampling (D) blocks, which are also realized with CIC filters and allow interpolation and decimation. The upsamplers condition the low-data-rate sensor signals before they are transmitted and the downsamplers condition the high-data-rate incoming signals to be compatible with the storage and control interfaces. Such a configuration makes it possible to effectively synchronize and transfer data using heterogeneous devices without quality loss.

Fig. 3 has shown the block diagram of the proposed IoT Gateway that is capable of integrating various communication protocols by the centralized processing core that is based on FPGA. The architecture is aimed at easing the exchange of heterogeneous IoT devices with the internet infrastructure. On the front end, the Input RF Interface receives incoming wireless signals of IoT nodes with a wide range of protocols including NB-IoT, SigFox, and LoRa. These signals are then fed into an FPGA, where they are processed in a manner that includes protocol translation, data synchronization and filtering so that they are compatible with the system. The Output RF Interface is responsible on the transmission side to deliver processed data back to the IoT devices or IoT networks to which it is connected. The system also includes the Wi-Fi module to offer high-speed backhaul connection to cloud platforms or local servers to store, analyze and monitor. The design will be interoperable across a large range of IoT devices by incorporating NB-IoT, SigFox, and LoRa within the gateway, using those different frequency bands and communication protocols. The FPGA is the central controller, which coordinates protocol, switching, and real-time processing, and thus, the low-latency communication, scalability, and adaptability.

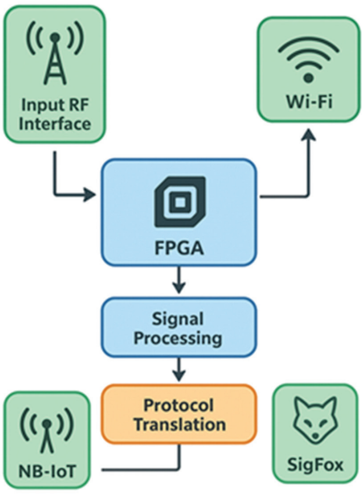


Fig. 3. IoT Gateway Block

3.6. CIC FILTER

The CIC digital filters represent a cost-effective method to implement narrowband low-pass filters that find applications in hardware solutions for decimation and interpolation functions and delta-sigma converter filtering. CIC filters excel in anti-aliasing functions during sample rate reduction operations as well as anti-imaging applications in signal sample rate increase scenarios. The applications require fast data processing which includes hardware quadrature modulation and demodulation for wireless systems as well as delta-sigma A/D and D/A converters. Tapped-delay line finite impulse response (FIR) filters with linear-phase work to fix the non-flat passband characteristics of CIC filters by following them or placing them before them.The cascaded-filter architectures have valuable benefits.

- The FIR filters operate at reduced clock rates minimizing power consumption in high-speed hardware applications
- CIC filters are popular in hardware devices; they need no filter coefficient data storage and require no multiplications. The arithmetic needed to implement CIC filters is strictly additions and subtractions only.
- Narrowband low-pass filtering can be attained at a greatly reduced computational complexity compared to using a single low-pass FIR filter. This property is why CIC filters are so attractive in decimating and interpolating DSP systems.

CIC filters structure the comb section either before or after their integrator section. Placing the comb section into the filter running at the lower sample rate demonstrates practical sense. The typical method of implementing CIC filters occurs when comb filters exchange positions with down-sampling operations. The world received CIC filters from Hogenauer in 1981 along with this fundamental characteristic. The comb component of the decimation filter shows a shorter delay length (differential delay) equal to $N = D/R$. The equivalent comb delay relationship exists between post-downsampling by R results in N samples but pre-downsampling by R produces D samples. Similarly, the comb delay between premultiplication by R with N samples provides the same result as post-sampling by R with D samples. The new configuration leads to two essential advantages that enable data storage reduction through $N = D/R$ differential delay line shortening as well as reduced clock frequency operation.The implementation shortens hardware power consumption through these two effects. Fig. 4 shows the interpolator using a CIC filter. Fig. 5 shows the decimated using the CIC filter.

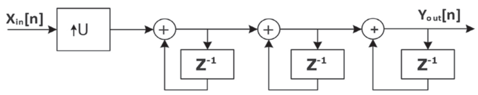


Fig. 4. Interpolator using CIC filter

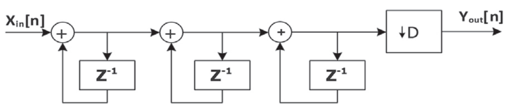


Fig. 5. Decimator using CIC filter

3.7. CIC FILTER BASED DOWN SAMPLER AND UPSAMPLER

Fig. 6. displays the sample rate converter with Interpolator and Decimater CIC filter. The architecture uses CIC filters with rate converters to do both interpolation and decimation operations. The CIC filter is applied to the incoming signal in the forward path and this helps reduce aliasing and spectral distortion before it is relayed to the rate converter where the sampling frequency is adjusted based on system needs. The filter control unit synchronizes the CIC filter functions, and provides adaptive filtering in both the upsampling and downsampling operations.

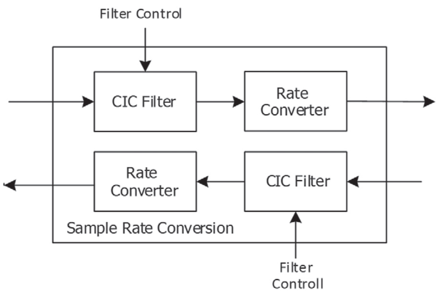


Fig. 6. Sample rate converter using Interpolator and Decimater with CIC filter

4. RESULT AND DISCUSSION

The proposed design is coded using Verilog HDL. The design is synthesized using Xilinx Vivado software. The system is implemented using Xilinx Virtex-4 FPGA device.The synthesis process is performed in a Windows 11 system with 6GB RAM @ 2.4 GHz operating frequency. The proposed design is synthesized in 180n and 45nm technology using cadence genus tools to evaluate the power and delay performance. Fig. 7 shows the simulated output using Modelsim.

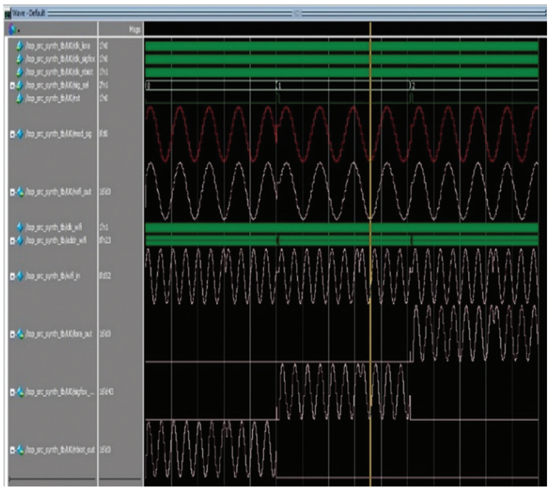


Fig. 7. Simulated output using Modelsim

Signal-to-Noise Ratio

SNR functions as a quality measure which indicates the potential for false switching through a basic estimation of implementation performance comparison as shown in Equation (1).

$$SNR = \frac{V_{sig}}{\sqrt{\sum_i^N V_n^2}} \quad (1)$$

V_1, V_2 … VN are noise sources which can be signal dependent, like the shot noise or signal independently.

Root Mean-Square Error

The RMSE of the estimated signal $\hat{x}(n)$ for M simulation, runs are calculated by Equation (2).

$$RMSE = \sqrt{\frac{1}{M}\sum_{j=1}^{M}\frac{1}{N}\sum_{n=1}^{N}\left(y(n) - \hat{x}_{hk}^{[j]}(n)\right)^2} \quad (2)$$

4.1. FPGA PERFORMANCE EVALUATION

Table 1 shows the individual module resource utilization. Table 2 presents a comparison of resource utilization between the proposed design and previously reported techniques. The results show that the proposed work requires significantly fewer registers (193), LUTs (246), and IOBs (70), highlighting its efficiency over existing methods.

Table 1. Individual Module Resource Utilization

Module Name	Slice LUTs (20,800)	Slice Registers (41,600)	Slices (81,650)	LUT as Logic (20,800)	Bonded IOBs (106)	BUFGCTRL (32)
top_src_synth	246	193	99	246	79	4
Uaddr (AddrGen)	84	24	27	84	0	0
Uclkdiv (ClockDiv)	2	1	2	2	0	0
Udec0 (Decimate)	40	20	20	40	0	0
Udec1 (Decimate_0)	40	19	19	40	0	0
Udec2 (Decimate_1)	40	20	20	40	0	0
Uint (Interpolate)	40	48	17	40	0	0

Table 2. Resource Utilization with Previous Techniques

Method	Number of Slice Registers	No. of LUT	No. of IOB	Number of Block RAM/FIFO	No. of DSP
[7]	560	298	-	-	26
[12]	24452	44724	-	-	-
[13]	46245	36995	-	170	-
[14]	4173	3275	-	-	-
This work	193	246	70	-	-

4.2. POWER PERFORMANCE

Table 3 shows the overall FPGA resource utilization, where LUTs (1.18%) and registers (0.46%) occupy a very small fraction of the available resources, while I/O usage is comparatively high at 74.53% due to external connectivity, and BUFG utilization remains moderate at 12.5%. Table 4 presents the power consumption analysis, indicating that dynamic power dominates at 99%, with I/O operations contributing the largest share (83%), while static power is minimal at only 1%. Fig.8 shows the overall Register–Transfer Level (RTL) schematic. Fig. 9 shows the implementation in Virtex-4 FPGA. Fig. 10. shows the RTL of the downconverter in the cadence genus tool. Fig. 11. shows the RTL of the Upconverter in the cadence genus tool. Fig. 12. shows the overall circuit in cadence genus tool.

Table 3. Overall Resource Utilization

Resource	Utilization	Available	Utilization %
LUT	246	20800	1.18%
FF	193	41600	0.46%
IO	79	106	74.53%
BUFG	4	32	12.50%

Table 4. Power consumption

Category	Sub-Category	Power (W)	Percentage
Dynamic (33.942 W, 99%)	Signals	3.129 W	9%
	Logic	2.667 W	8%
	I/O	28.147 W	83%
Static (0.485 W, 1%)	PL Static	0.485 W	100%

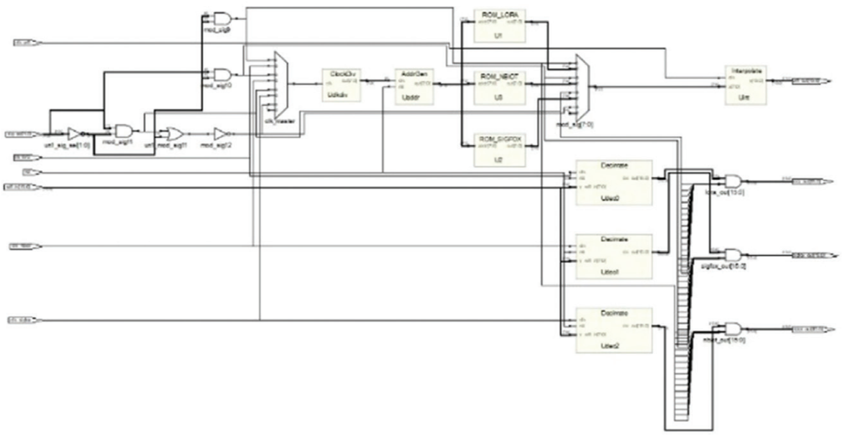


Fig. 8. Overall RTL schematic

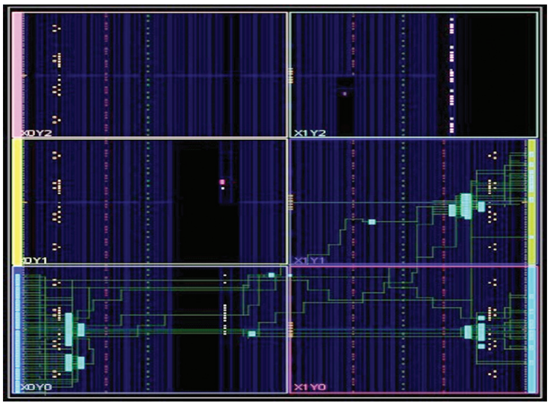


Fig. 9. Implemented in Virtex-4 FPGA

Table 5 presents the ASIC performance evaluation, where the proposed work achieves the lowest cell count (2701) with reduced power consumption (2 mW) and improved delay (1.02 ns) at 180 nm technology, demonstrating better efficiency compared to previous methods.

Table 5. ASIC Performance Evaluation

Methods	Number of Cells	Power (mW)	Delay (ns)	Technology
[5]	48362	3.63	2.11	45nm
[15]	3246748	2.491	8	90 nm CMOS
This work	2701	2	1.02	180nm

Table 6 shows the synthesized power output for 180 nm and 45 nm CMOS technologies, where scaling down to 45 nm reduces the number of cells and leakage power, while also lowering internal and net power compared to 180 nm, with switching power remaining nearly the same.

Table 6. Synthesised power output using 180 nm and 45 nm

Technology	Number of Cells	Leakage (nW)	Internal (nW)	Net (nW)	Switching (nW)
180 nm CMOS	2701	200.86	1225371.81	799191.57	2024563.38
45 nm CMOS	2006	109.39	1135487.67	689714.31	2021369.14

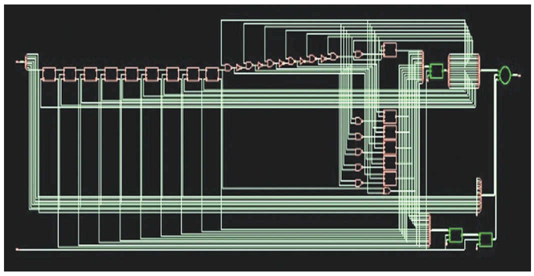


Fig. 10. RTL of downconverter in cadence genus tool

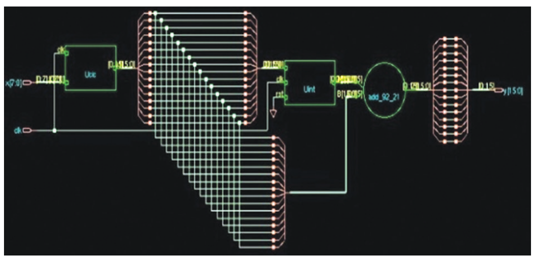


Fig. 11. RTL of Upconverter in cadence genus tool

Table 7 highlights the synthesized results for core area, showing that technology scaling from 180 nm to 45 nm significantly reduces the core area from 2.3 μm^2 to 0.3 μm^2, along with a decrease in the number of cells.

Table 7. Synthesized results for core area using 180nm and 45nm

Technology	Cells	Core Area(μm²)
180 nm CMOS	2701	2.3
45 nm CMOS	2006	0.3

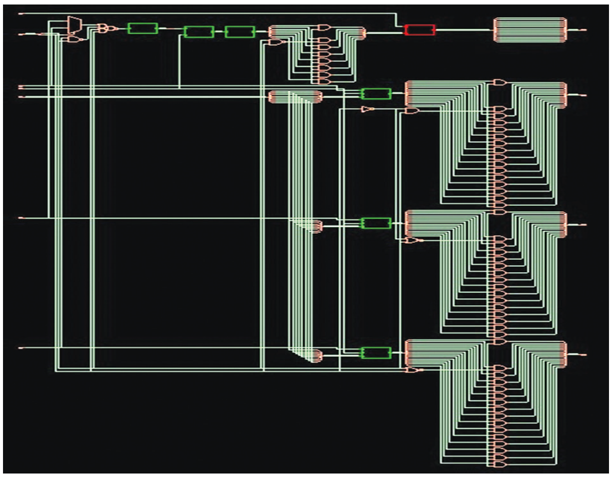


Fig. 12. Overall circuit in cadence genus tool

Table 8 compares RMSE and SNR across different technology nodes, showing that the 45 nm CMOS process achieves lower RMSE values (1.4% uplink, 1.2% downlink) and higher SNR (24.8 dB uplink, 26.3 dB downlink) compared to the 180 nm CMOS process, indicating superior signal quality and accuracy with scaling.

Table 8. Comparison of RMSE and SNR

Technology	Process (nm)	RMSE Uplink (%)	RMSE Downlink (%)	SNR Uplink (dB)	SNR Downlink (dB)
180 nm CMOS	180	3.2	2.8	18.5	20.1
45 nm CMOS	45	1.4	1.2	24.8	26.3

Table 9 provides a comparative evaluation of FPGA and ASIC implementations. The FPGA design shows very low logic utilization but high dynamic power consumption (33.94 W), while the ASIC implementations in 180 nm and 45 nm CMOS demonstrate significant improvements in power efficiency and area reduction, with the 45 nm technology achieving the most compact core area (0.3 μm²) and lowest leakage power.

Table 9. FPGA vs. ASIC Performance Comparison

Platform	Metric / Resource	Value
FPGA (Xilinx virtex-4)	LUT Utilization	246 / 20,800 (1.18%)
	FF (Registers)	193 / 41,600 (0.46%)
	IO	79 / 106 (74.53%)
	BUFG	4 / 32 (12.5%)
	Dynamic Power	33.942 W (99%)
	Static Power	0.485 W (1%)
	Total Power	34.427 W
	SNR / RMSE	63.4 dB / 0.0558
	Max Freq.	162.7 MHz
ASIC (180nm, 45nm)	Technology Node	180 nm CMOS
	Number of Cells	2,701
	Core Area	2.3 μm²
	Power Breakdown	Leakage: 200.86 nW Internal: 1,225,371.81 nW Net: 799,191.57 nW Switching: 2,024,563.38 nW
	Technology Node	45 nm CMOS
	Number of Cells	2,006
	Core Area	0.3 μm²
	Power Breakdown	Leakage: 109.39 nW Internal: 1,135,487.67 nW Net: 689,714.31 nW Switching: 2,021,369.14 nW

5. CONCLUSION

This work proposes a new area and power-optimized sample rate converter architecture for the IoT gate. Lora, SigFox and NbIoT protocols are used to generate low data rate input, and WiFi is used in the IoT storage interface side. A catch memory is used as the interface to receive the low data rate input and store it.The proposed work is implemented using Xilinx Virtex-4 FPGA and evaluated hardware resource utilization and power consumption performance.To evaluate hardware resource utilization, the number of slices, LUT, and flip flops are measured and compared with conventional implementation.This design achieved good performance regarding hardware resource utilization and power consumption. Experimental results demonstrate that the proposed method has low RMSE of 1.2% (downlink) and 1.4% (uplink), high SNR of 26.3 dB (downlink) and 24.8 dB (uplink) in 45 nm CMOS technology, which is better than conventional 180 nm implementations. Moreover, the ASIC implementation is also very area efficient, where the core area has been decreased by a factor of 8x between 180 nm (2.3 um 2) and 45 nm (0.3 um 2) due to the technology scaling. Future research directions will be aimed at the expansion of the proposed architecture to include acceptability of the latest 5G/6G IoT requirements, the machine learning-based traffic decision-making, and the energy efficient operation in ultra-low-power applications. In addition, the investigation of both reconfigurable hardware accelerators and security-aware integration of different protocols will contribute to the enlargement of the strength and deployment of the gateway in the big IoT environment.

REFERENCES

[1] R. Tejal Rahate, S. A. Ladhake, U. S. Ghate, "FPGA based implementation of decimator filter for hearing aid application", International Research Journal of Engineering and Technology, Vol. 5, No. 7, 2018, p. 2289.

[2] M. Blok, "Sample rate conversion based on frequency response masking filter", Proceedings of the International Conference on Signals and Electronic Systems, Kraków, Poland, 10-12 September 2018, pp. 137-142.

[3] M. Traykov, R. Mavrevski, I. Trenchev, "Modeling of digital converter for GSM signals with MATLAB", International Journal of Electrical and Computer Engineering, Vol. 9, No. 5, 2019.

[4] S.-L. Chen, J. F. Villaverde, H.-Y. Lee, D. W.-Y. Chung, T.-L. Lin, C.-H. Tseng, K.-A. Lo, "A power-efficient mixed-signal smart ADC design with adaptive resolution and variable sampling rate for low-power applications", IEEE Sensors Journal, Vol. 17, No. 11, 2017, pp. 3461-3469.

[5] A. Agarwal, L. Boppana, R. K. Kodali, "A factorization method for FPGA implementation of sample rate converter for a multi-standard radio communications", Proceedings of IEEE Tencon - Spring, Sydney, NSW, Australia, 17-19 April, pp. 530-534.

[6] V. Jain, N. Agrawal, "Implement multichannel fractional sample rate convertor using genetic algorithm", International Journal of Multimedia Data Engineering and Management, Vol. 8, No. 2, 2017, pp. 482-494.

[7] B. H. Tietche, O. Romain, B. Denby, "A practical FPGA-based architecture for arbitrary-ratio sample rate conversion", Journal of Signal Processing Systems, Vol. 78, 2015, pp. 147-154.

[8] D. Datta, P. Mitra, H. S. Dutta, "FPGA implementation of high performance digital down converter for software defined radio", Microsystem Technologies, Vol. 28, 2022, pp. 533-542.

[9] X. Zhou, Z. Xie, F. Wen, J. Yang, "An optimal design and implementation method of high speed digital down conversion based on FPGA", Proceedings of the International Conference on Computer Information Science and Artificial Intelligence, Kunming, China, 17-19 September 2021, pp. 1104-1107.

[10] D. Zhijian, X. Shuangman, L. Jingjing, Y. Xi, W. Qi, Z. Yijiu, "Design of acquisition system with real time sampling rate of 5Gsps", Proceedings of the 13th IEEE International Conference on Electronic Measurement & Instruments, Yangzhou, China, 20-22 October 2017, pp. 239-243.

[11] Z. Xiang, T. Wang, T. Geng, T. Xiang, X. Jin, M. Herbordt, "Soft-core multiple-lane FPGA-based ADCs for a liquid helium environment", Proceedings of the IEEE High Performance Extreme Computing Conference, Waltham, MA, USA, 25-27 September 2018, pp. 1-6.

[12] A. Agarwal, L. Boppana, "Design of a reconfigurable pipelined architecture for SRC filter for software radio receiver", International Journal of Electronics and Communication Engineering, Vol. 4, No. 2, 2015, pp. 23-30.

[13] X. Liu, Z.-K. Wang, Q.-X. Deng, "Design and FPGA implementation of a reconfigurable 1024-channel channelization architecture for SDR application", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 24, No. 7, 2016, pp. 2449-2461.

[14] A. Zeineddine, S. Paquelet, A. Nafkha, P.-Y. Jezequel, C. Moy, "Efficient arbitrary sample rate conversion for multi-standard digital front-ends", Proceedings of the 17th IEEE International New Circuits and Systems Conference, Munich, Germany, 23-26 June 2019, pp. 1-4.

[15] A. Agarwal, L. Boppana, "Low latency area-efficient distributed arithmetic based multi-rate filter architecture for SDR receivers", Journal of Circuits, Systems and Computers, Vol. 27, No. 08, 2018.

[16] P. Kulkarni, B. G. Hogade, V. P. Kulkarni, V. Turkar, "ASIC design of radix-2, 8-point FFT processor", Journal of Scientific & Industrial Research, Vol. 80, No. 3, 2021, pp. 230-238.

[17] A. Michalski, D. Buell, K. Gaj, "High-throughput reconfigurable computing: design and implementation of an IDEA encryption cryptosystem on the SRC-6E reconfigurable computer", Proceedings of the International Conference on Field Programmable Logic and Applications, Tampere, Finland, 24-26 August 2005, pp. 681-686.

[18] J. Harkins, T. El-Ghazawi, E. El-Araby, M. Huang, "Performance of sorting algorithms on the SRC-6 reconfigurable computer", Proceedings of the IEEE International Conference on Field-Programmable Technology, Singapore, 11-14 December 2005, pp. 295-296.

[19] S. Akella, M. C. Smith, R. T. Mills, S. R. Alam, R. F. Barrett, J. S. Vetter, "Sparse matrix vector multiplication on the SRC MAPstation", Proceedings of the 9th Annual High Performance Embedded Computing Workshop, 2005.

[20] D. DuBois, A. DuBois, T. Boorman, C. Connor, S. Poole, "An implementation of the conjugate gradient algorithm on FPGAs", Proceedings of the 16th International Symposium on Field-Programmable Custom Computing Machines, Stanford, CA, USA, 14-15 April 2008, pp. 296-297.

An Overview of Cybersecurity: Key Issues and Emerging Solutions

Review Paper

Medha Wyawahare*
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
medha.wyawahare@vit.edu

Milind Rane
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
milind.rane@vit.edu

Sharvari Bodas
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
sharvari.bodas21@vit.edu

Swarali Damle
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
sharvari.bodas21@vit.edu

*Corresponding author

Shoumik Daterao
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
shoumik.daterao21@vit.edu

Arya Chopda
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
arya.chopda21@vit.edu

Siddharth Bhorge
Department of Electronics and Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India
siddharth.bhorge@vit.edu

Abstract *– In an age where digital interconnectivity permeates every aspect of daily life, cyber threats have grown more advanced, and as a result, they pose very dangerous threats to individuals, enterprises, and governments all the same. This review offers a systematic synthesis of cyber threats, new attack surfaces, and new defense techniques, with emphasis on the convergence of artificial intelligence (AI) and domain-specific issues within cloud, IoT, and mobile networks. Upcoming new technologies like quantum and 5G further present risks that require further new developments in cryptography and solutions in network security. In addition to providing an overview of current work, this paper makes an original contribution by presenting a comparison of prominent methods and studies, divided by defense strategy, domain, and performance measures. The approach for the study focuses more on the requirement of technical innovation to be blended with frameworks that are ethical and regulatory in nature, addressing complex and dynamic threats in the nature of cybersecurity. Recommendations for further research in the future include quantum-resistant algorithms, improved AI models that can be used for more effective cybersecurity, and creation of ethical standards in the digital defense of the resources of the nation to do it more robustly and responsibly.*

Keywords: *information security, Cyberattacks, Intrusion detection system, SIEM, SOAR, Security system, security awareness*

Received: April 28, 2025; Received in revised form: July 3, 2025; Accepted: August 10, 2025

1. INTRODUCTION

Over the recent explosion of digital landscapes, unprecedented levels of cyber threats have threatened individual, corporate, and governmental lifelines. With the increasing interconnectedness of systems, the attack surface that threatens cybercriminals has more than expanded, allowing for greater sophistication in exploiting vulnerabilities [1]. The aftermath of cyber attacks tends to be multifarious; therefore, it may lead to financial damage, data breaches [2] [3]. The new world of cybersecurity also includes the challenge of growing threats. In addition to this, attacks such as Advanced Persistent Threats are well-financed adversaries that conduct sustained, targeted attacks on networks. APTs aim to breach into organizations' networks; often, these go unnoticed for long durations by exploiting zero-day vulnerabilities, thereby putting sensitive data and critical systems at a considerable risk [4], [5]. These attacks require defense systems not only to block the intrusion but to identify it and respond promptly.

Artificial Intelligence (AI) and Machine Learning (ML) now stand as weapons in this cyber battle. They can process huge amounts of real-time data for detecting malicious behavior which may be missed by traditional techniques [6]. AI-based solutions can be used to automatically identify threats, thus allowing cybersecurity teams to react more quickly to incoming threats [7]. Yet while AI offers new opportunities for improving cybersecurity, it also represents new challenges because attackers might try to defeat or trick AI models to avoid security controls [8]. IoT has further confused matters in its attempts to create an increasingly sophisticated Internet of Things, but on this count, the expanding global complexity does nothing but add to the challenge of cybersecurity. There are billions of IoT devices in operation today, many with weak or no security, which attackers have identified as routes to mount large-scale attacks, for instance, DDoS [9], [10]. Last is hard to secure because diversity makes it challenging to patch in the field found after deployment. Integration of IoT into critical infrastructure increases the demand for stronger security protocols in safeguarding such devices against cyberattacks [11]. In addition, blockchain technology is gaining attention for its potential application for cyber security. The decentralized nature of blockchain and its cryptographic foundations would make such a framework immune to tampering, hence providing a safe place for the storage and transmission of data [12]. Blockchain has been researched in applications involving secure communication, digital identity verification, and transaction monitoring. However, despite all this promise, it has numerous challenges facing it, with major ones having to do with scalability and high energy consumption. These aspects limit its higher adoption into cybersecurity frameworks [13].

The other tool part of the application in modern cybersecurity efforts is the Security Information and Event Management (SIEM) systems which facilitate the monitoring of data from different sources in support of real-time threat visibility [6]. With SOAR, SIEM platforms can provide faster and more effective incident responses and therefore potentially contain situations before significant damages are incurred [14]. Such systems are critical to guiding organizations to better manage the thousands of alerts thrown off by modern cybersecurity tools [7].

In the future, therefore, it is going to be one of the most significant challenges for cybersecurity. Once achieved, and fully realized, quantum computers may break most encryption algorithms that today are used to secure data [12]. This puts direct endangerment to confidentiality related to sensitive information because quantum algorithms can be used to decrypt data that currently is considered secure [15]. As an answer, researchers are developing quantum-resistant cryptographic algorithms, which will be obligatory to maintain data security post-quantum [13], [14].

While there are many review studies in the field of cybersecurity, the majority concentrate on either individual technologies, for instance, machine learning for intrusion detection, or individual fields like cloud or IoT security. Even fewer works offer a broad understanding across technical, architectural, and ethical aspects. This paper tries to bridge the gap by providing a systematic, multi-domain overview that categorizes and contrasts current threats and defenses and highlights their interdependencies and real-world implications. In contrast to descriptive only surveys, this overview focuses on comparative analysis through summarizing recent empirical literature, reviewing defense methods with performance-based assessments, and signaling new issues like AI-enabled attacks, quantum-age vulnerabilities, and the ethical need for governing cybersecurity systems.

Through synthesizing existing literature using a domain-based perspective and analysing strengths and weaknesses of dominating methodologies, this paper intends to act as an encompassing guide for researchers, professionals, and policymakers. Not only does it scan available work, but it also critically outlines areas of research gaps and suggests avenues for future investigation—especially in adaptive AI frameworks, quantum-resilient cryptographic protocols, and cross-disciplinary security paradigms.

2. CYBER THREATS AND ATTACK VECTORS

Cyber threats are diverse, employing various tactics to exploit vulnerabilities in systems and networks. The most common attack are as given below.

2.1. MALWARE

A malicious software whose forms include viruses, worms, ransomware, and spyware; they are primarily targeted at harming or stealing data from systems. It mainly spreads through phishing emails or com- promised websites or malicious downloads on personal as well as corporate devices [16]. A very destructive form of malware is ransomware that encrypts data and demands ransom payments for recovery. It has also shown a drastic surge in its attacks lately targeting sectors such as healthcare and finance that resulted in losses not only to the financial implications but also to the operational shutdowns [17]. The polymorphic malware does pose other kinds of challenges due to the constant changing of code so as not to be detected by the traditional antivirus solutions [18]. Mobile malware has gained and risen where attackers exploit flaws in mobile applications and utilize this to gain access to sensitive information on the smartphone [19].

2.2. PHISHING

Phishing remains one of the very successful attack vectors, operating on deception to steal sensitive information or install malware. While initially email-centric, phishing now encompasses various modes like social media and SMS, commonly known as smishing [20]. Phishing attacks typically capture login credentials, financial information, or personal details. One type of targeted phishing attack such as Spear phishing targets a specific individual, usually with a high position or handling sensitive and critical systems [21]. Most attacks use phishing as the entry point to launch a large-scale attack, for example, a business email compromise, wherein attackers impersonate executives to approve fraudulent financial transactions [22].

2.3. SOCIAL ENGINEERING AND INSIDER THREATS

They exploit psychological vulnerabilities rather than technical ones. In any case, their means is always the psychological manipulation that forces users to divulge confidential information. Other attacks with phishing or impersonation attempts are usually found along with these attacks. The insider threat is another major one-person threat. Insider refers to those who gain authorized access and accidentally or intentionally compromise security. A disgruntled employee or one who has mal-intentions may misuse this access to steal sensitive data or sabotage operations [23]. Even unintentional acts, for instance, clicking an email phishing, or sharing one's credentials, can potentially cause large breaches in security [24].

2.4. APT ADVANCED PERSISTENT THREATS

Advanced Persistent Threats, also known as APTs, are long-lasting attacks that are usually performed by nation-state actors or well-funded criminal enterprises. They usually employ a combination of social engineering, phishing, and zero-day exploits to gain a presence in the target's network and can evade detection for years. The purpose of such an attack is to steal sensitive data or disrupt operations in critical infrastructure sectors, such as energy, finance, or defense [25]. This is why APTs, with persistence and stealth attributes, are highly dangerous as they most of the time evade the traditional security measures implemented, and when caught late in the day, it might lead to catastrophic damage.

2.5. EMERGING THREATS

Cyber threats are numerous, using various tactics they are exploiting weaknesses in the network. Of the many attack vectors, malware, phishing, insider threats, and APTs are the most common. Each is constantly evolving, becoming more complicated and destructive with time.

2.5.1. IoT Vulnerabilities

IoT devices have drastically increased the attack surface for cybercriminals with their sheer growth. IoT devices are mostly not very secure with minimum encryption and authentication in place. As a result, these devices have now become the most sought-after by hackers [26]. They are increasingly connected to critical systems, including healthcare and industrial controls and their compromise will have very disastrous impacts. Botnet attacks, including the Mirai botnet, have proved the power of hacking unsecured IoT devices in massive Distributed Denial of Service (DDoS) attacks [27].

2.5.2. AI-driven Attacks

Cyber-criminals are now arming themselves with Artificial Intelligence to carry out more efficient and evasive attacks. It has been referenced that AI-based attacks use the algorithm in machine learning to auto-scanner vulnerabilities, craft sophisticated phishing campaigns, and avoid discovery while in the learning phase about defensive patterns of targeted systems [28]. For instance, AI can prepare customized phishing messages that may most probably fool their recipient, thus raising the success percentage of these assaults as seen in [29].

2.5.3. Ransomware Evolution

The trend with ransomware attacks has become even more aggressive in terms of methods, one of which is double extortion. In such an approach, unless a ransom is paid, attackers encrypt the data and they jeopardize divulging sensitive information. Indeed, this method has been widely proven to be highly effective at forcing organizations to pay ransoms due to reputational damage and legal consequences [30]. Critical infrastructure targeting, including hospitals and energy sectors, is also one of the types of attacks that made ransomware one of the significant cybersecurity threats of today [27].

3. CYBER DEFENSE TECHNIQUES

Cyber defense techniques have various techniques aimed at proactively identifying and mitigating cyber threats as well as preventing them. Based on the combination of detection, response, and adaptive security measures to ensure defense against evolving attack vectors that might otherwise compromise the systems, cyber defense techniques protect critical systems from evolving attack vectors and reduce potential risks.

3.1. INTRUSION DETECTION SYSTEM

IDS is a subelement within the cybersecurity, monitoring network and system activities for suspicious behavior. Intrusion detection means obtaining information regarding unauthorized access, violations of system policy, or malicious activity that may put the integrity, confidentiality, or availability of the system in danger. IDS operates through network packets as well as system logs, which are patterns indicating that an attack or policy violation is underway or has already been set in motion [31, 32]. Contemporary IDS solutions offer immediate alerts to their administrators regarding the occurrence of an intrusion, meaning that response time and damage are being achieved in a rather shorter period [33]. There are several types of IDS based on the detection methodology adopted:

3.1.1. Signature-based Intrusion Detection Systems (SIDS)

SIDS rely on the comparison of network traffic with a pre-established database containing a set of known attack signatures. These work well on the detection of known attacks because they match a specific pattern, for instance, a byte sequence, packet headers, or known malware footprints. However, SIDS, by their nature, cannot identify new, zero-day attacks because they rely solely on signatures that yet do not exist for threats [32, 34]. For example, if malware has assumed a new version that adopts a payload structure that is not known to any signature, then the SIDS will miss it until there has been an update in the signature database [35].

3.1.2. Rule-based IDS

Also known as policy-based IDS, these systems identify intrusions by comparing and checking net- work activity against predefined rules. Such systems are very highly adaptable because an administrator can define specific behaviors that should be flagged. For example, a rule may mark traffic coming from a particular IP address or volumes of traffic over a certain threshold within a timeframe [36, 37]. Although rule-based IDS are flexible, they need continuous tuning and maintenance to stay effective, especially as network configurations change and various new attack techniques appear [33].

3.1.3. Anomaly-Based Intrusion Detection Systems (AIDS)

AIDS use an altogether different approach: instead of trying to match specific signatures or rules, it identifies deviations from the norm. In these systems, ML is employed to baseline normal network behavior and detect intrusions based on recognizing activities that significantly deviate from this baseline [31, 36]. The strength of AIDS is its ability to identify zero-day attacks, since it does not depend on a database of known signatures [38]. However, when there's a higher false positive rate, benign anomalies are often mislabeled as a threat [35, 37].

3.1.4. Hybrid Intrusion Detection Systems

The hybrid IDS takes the best from the signature-based and anomaly-based approaches. They try to of- fer better defense from threats for which signatures exist and anomaly detection for emerging unknown threats. Hybrid systems are very efficient in all high-traffic production environments where a significant number of known and emerging threats is expected in place - this could be the case for enterprises or critical infrastructure [39, 40].

3.1.5. Host-based vs. Network-based IDS

IDS can also be classified based on what environment they monitor. The host-based IDS (HIDS) keeps an eye on each device, focusing on system logs, file integrity, and user activity to discover the malicious behavior at host level. This is as opposed to the NIDS which monitors in real-time network traffic for signs of attacks anywhere in the network. NIDS is more appropriate to detect high-level attacks that contain DDoS attacks, while HIDS is more appropriate to detect malware or insider threats at the endpoint [32, 41].

3.2. ANOMALY DETECTION

Anomaly detection techniques are critical to identify that there is some kind of deviation from normal behavior in a network, which might be raising signals towards probable cyber threats. Traditional, old school, rule-based systems have matured into more complex forms, namely graph-based methods as well as unsuper- vised learning, especially in such environments as the Internet of Battlefield Things (IoBT), where adversarial attacks prevail [38, 42]. Machine learning models combined with adversarial training, therefore, promise to resist such attacks by dynamically updating according to changing threat landscapes [39, 42]. In addition, ensemble learning is a proven method to improve the performances of anomaly detection systems in terms of precision and resistance within adversarial environments [38, 39].

3.3. ML AND DEEP LEARNING

ML and deep learning also bring new innovations in cybersecurity, specially in multi-stage complex attacks detection. Recent advances in the field involve state-of-art techniques, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), which are useful in malware classification and network intrusion detection [43]. As they are able to recognize patterns in huge amounts of data, it can be used in actual time to detect advanced threats, including ransomware and insider attacks [43, 44]. Also, unsupervised learning methods, often used for anomaly detection with unlabeled data, thus make them handy for discovering unknown patterns of attacks [45].

3.4. THREAT RESPONSE TECHNIQUES

Other than detection, strong incident response skills are required that can rapidly respond in appropri- ate and timely manners to incidents. Responding to the threat relates to what may be done in order to contain, to mitigate or remediative losses with security breaches that eventually will minimize its impacts against an organization's operations and assets.

3.4.1. Security Information and Event Management (SIEM)

The SIEM systems collect, aggregate, and analyze varied sources of information such as firewalls and endpoint logs, and even network devices, in real time to detect security-related incidents. With the advancement of recent machine learning algorithm integration, SIEM solutions are more equipped to detect mature advanced threats with much fewer false positives. SIEM use in a critical infrastructure environment has proven to be very efficient in managing large and multi-layered security operations [46, 47].

3.4.2. Security Orchestration, Automation, and Response (SOAR)

Security operations are automated by SOAR to facilitate fast and effective incident response. The SOAR platforms interface with the SIEM systems and other tools for seamless threat response across the total infrastructure while ensuring standard processes in managing incidents [48, 49]. A new version of SOAR technology also offers automation through artificial intelligence for threat hunting and remediation work, thereby saving much manual effort for the security analyst. On top of that, SOAR provides advanced case management and incident analysis capabilities with minimal complexity in post-incident reviews and increases the overall security posture [48].

3.4.3. Endpoint Detection and Response

The EDR tool is concentrated on continuous monitoring and response at the endpoint level, as it provides deep insights into the behavior of the individual devices. EDR systems build on the strengths of behavioral analysis and ML algorithms, to identify APTs which would otherwise avoid detection by traditional antivirus solutions [50]. EDR also includes forensics and threat hunting capabilities that allow security teams the ability to unpack incidents in full detail and neutralize threats before they can spread throughout a network [50],[51].

4. CYBERSECURITY IN DIFFERENT DOMAINS

Cybersecurity in various domains demands specialized approaches to address distinct challenges unique to each environment.The following section highlights attack vectors and remediation techniques for different domains like cloud, mobile, iot, network security and the role of artificial intelligence in cybersecurity.

4.1. CLOUD SECURITY

Multi-tenant architectures present gigantic challenges in terms of cloud security due to vulnerabilities exploited by potential attacks, which may take advantage of shared resources and thus compromise the isolation between the tenants and perhaps data leakage [52]. Data privacy becomes challenging in cloud infrastructure because it is stored in distributed networks scattered all over, allowing for potential unauthorized access and some accidental breaches [53]. Furthermore, regulatory requirements such as tighter conditions like GDPR make cloud security more complex because the cloud service providers handle data storage in geographically remote locations which complicates issues of legal jurisdiction as well as data sovereignty [54]. The best cloud security solutions will balance protection for high levels of data integrity in conjunction with confidentiality but with performance optimizations. Encryption and other security measures heavily impact system efficiency so that large amounts of data often become too slow to process easily with security measures on [55]. Techniques such as homomorphic encryption have demonstrated promising early results in performing computations on encrypted data using secure protocols in a Cloud-based environment but are quite limited for commercial use due to the high computational costs that pervade the development of efficient scalable versions [56].

4.2. MOBILE SECURITY

The malicious phishing and malware attacks are highly targeted on mobile apps due to the wide permissions given to applications as well as third-party invoked libraries within an application, which may lead to leakage of private user information to malicious parties [57]. This has also given rise to new forms of risks, as the increased complexity of the infrastructures involved in 5G is vulnerable to attacks on the signaling plane and DDoS attacks, affecting layers of both application and network [58]. These threats require counter-measures from Mobile Device Management (MDM) solutions for organizations to monitor and control usage on devices. However, MDM systems themselves are also vulnerable to such advanced persistent threats (APTs) and mobile botnets that potentially bypass traditional detection mechanisms and breach enterprise security [59]. Recent works have come forward with blockchain-based MDM solutions as a promising advancement for securing mobile devices, proposing a decentralized manner of managing and securing communication channels, while persistent scalability challenges remain [60]. Adaptive security measures capable of real-time responses will be indispensable in protecting both networks and devices from evolved mobile threats [61].

4.3. IOT SECURITY

IoT security is a complex issue for the widespread deployment of these IoT gadgets in a variety of environments and the minimal adoption of general security standards that expose these devices to multiple attack vectors [62]. Most of the IoT devices are always constrained in their potential for computational and power capacity to provide traditional security protocols like intrusion detection systems and encryption in terms of feasibility [63]. Adding to this, the heterogeneity of IoT systems-ranging from industrial applications to consumer devices-made it even harder to implement uniform security standards. This made communication channels and privacy over data very vulnerable [64]. Moreover, the high volume of interconnecting IoT devices significantly expands the attack surface and leaves them open for large-scale attacks like DDoS and malware- based intrusions [65]. With regard to such security issues, lightweight encryption techniques and adaptive architectures are some researches being carried out to protect IoT networks with minimal resource usage over individual devices [66]. Despite this, persistent challenges persist, such as inconsistent implementation of authentication protocols and the difficulty in managing timely software updates that expose many potential IoT threats [67].

4.4. NETWORK SECURITY

Network security is under immense pressure because of the fast and continually advancing network architectures that require strong and adaptive protocols to defend against sophisticated attacks [68]. Sophisticated secure communication protocols have especially been advanced in 5G, and it is still found to be vulnerable towards attacks on control planes and signaling systems that disrupt critical network functions [69]. Real-time network monitoring is typically deployed using anomaly-based detection systems, which can be well-suited to catching suspicious activities but are not without the challenge of finding an appropriate balance between high detection rates and low false positives [70]. SDN promises to open up centralized security management capabilities that might otherwise be unmanageable but poses a risk in favoring single points of failure that at- tackers might enjoy exploiting [71]. Addressing such weaknesses of SDN, frameworks are now surfacing that automatically react to the threats once discovered for a more responsive defense to novel attacks [72]. However, managing extremely large software-defined networks is challenging, which is why research continues in secure and efficient protocols for when those demands are needed [73].

4.5. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial Intelligence (AI) has transformed the field of cybersecurity as it offers real-time response and detection capabilities with greater accuracy through advanced machine learning models [74]. In fact, these innovations are significant for using anomaly detection and predictive analytics in detecting zero-day vulnerabilities in a more proactive manner than traditional approaches to threat identification [75]. Neural networks have improved the reliability of IDS but these systems still face challenges like high false-positive rates and dependence on large data sets [76]. AI-based defenses are still vulnerable to attacks in the form of adversarial inputs that could mislead models into producing certain output, which would further create dangers to security [77]. To counter this, researchers are developing Explainable AI, or XAI, as an essential intervention to increase the transparency of decisions in AI, which may also reduce vulnerabilities to adversarial attacks [78]. Despite the above developments, integrating AI into cybersecurity still faces challenges with meeting the balance between security and efficiency when dealing with these very extensive and ever-increasing datasets that characterize modern networks [79].

5. CYBERSECURITY CHALLENGES

Cybersecurity is a dynamic field, and with newer advanced technologies and more profound attackers, security professionals face more challenges. The following section outlines some of the key challenges in cybersecurity including human factors and social engineering, privacy and ethical issues, and regulatory and legal challenges.

5.1. HUMAN FACTORS AND SOCIAL ENGINEERING

Human factor is the most significant challenge in cybersecurity. Humans often are the most vulnerable point in the security chain, as it is said, and attackers have exploited this more over time using social engineering. Social engineering attacks include phishing, baiting, and pretexting, where users are convinced to provide information or access to secure systems [101]. Phishing attacks are one of the most common forms of social engineering where attackers are taking advantage of users' trust in official-looking communications to steal credentials or spread malware [102]. Another very significant risk in the case of cybersecurity is insider threats. Insider threats refer to persons inside the organization that may misuse their access to adversely affect the organization on purpose, accidentally, or otherwise [80]. According to [80], insider threats are very difficult to detect because they emanate from trusted employees or contractors who already have legitimate access to the system. Insider incidents can result from malicious intent or negligence; in the latter case, the user unintentionally compromises sensitive information due to unawareness or unsafe practices [80, 101]. A poor understanding among users is one of the major human-related causes. In most cases, users do not know about the emerging threats, and there is not adequate education provided to identify or control potential dangers [103]. The organizations that do not spend their money on continuous security education for its employees are prone to being breached [80, 101].

5.2. PRIVACY AND ETHICAL ISSUES

Balancing security and user privacy is also another major challenge in cybersecurity. Although organizations institute more enhanced security measures like surveillance, logging, and monitoring, privacy issues begin to creep in [84]. For instance, organizations may collect vast amounts of user data for security purposes; however, sometimes this collection might infringe on the user privacy rights if mishandled [83]. For example, the GDPR in Europe demonstrates how privacy and data protection laws have evolved in this regard with a tendency to develop more user control and their information [6]. Nonetheless, enforcement of such regulations might likely prove challenging while adhering to robust security. According to research, integration of such privacy-enhancing technologies into security solutions must be achieved to establish a good balance between protection of users' information and compliance with regulations [83]. Ethical hacking, or penetration testing, is the practice that attempts to unveil vulnerabilities within systems before these malicious actors can access them [90]. Even though this process is necessary for strengthening security, ethical concerns emerge when considering the possible misuse of testing tools [91]. Ethical boundaries must restrain hackers in penetration testing roles so that their activities do not violate law or user privacy requirements [84]. Second, ethical hacking, if performed well, enables organizations to examine and analyze security vulnerabilities without breaking users' trust or neglecting the privacy of any individual, laws [84], [90].

5.3. REGULATORY AND LEGAL CHALLENGES

Yet another challenge in the domain of cybersecurity is a complexity in the legal and regulatory land- scape. Regulations involving GDPR in Europe and HIPAA in the U.S. put stringent standards of data protection on organizations to adhere to these standards [90, 93]. However, a borderless internet has made laws radically vary from country to country, thus creating a patchwork of regulations where multinational organizations need to navigate through a different kind of legislation in almost every country [87, 94]. The challenge for businesses would then be to reconcile the divergent demands of different regulatory bodies in frequently conflicting jurisdictions [88]. For example, some countries impose data localization policies that mandate the storage of data within country borders, but other countries require data to be accessible for international investigations [87, 94]. Hence, organizations would have to adopt flexible yet robust cybersecurity policies that cater to a wide range of legal standards [93-95]. Another issue, therefore, is the fact that cyber threats evolve in manners that no one can keep track of with the pace of cybersecurity legislation [93]. Even though regulators try to make sure their rule-making remains abreast of the latest in cybersecurity issues, the law is too slow and often plays catch-up in catching up with new emerging threats [94]. Indeed, there has been a stream of recommendations to implement more flexible legal systems that can rapidly respond to new cybersecurity advances [87, 93, 95].

6. FUTURE TRENDS IN CYBERSECURITY

Future cybersecurity has many challenges along with opportunities. This section identifies some ar- eas where we can expect potential impacts on the future landscape of cybersecurity in the age of quantum computing, 5G networks, AI-driven systems, and edge computing.

6.1 QUANTUM COMPUTING AND CYBERSECURITY

Quantum Computing threatens to undermine the underpinning of modern cryptography. Algorithms like RSA and ECC rely on issues that may be challenging to solve for computers, such as factoring large numbers. Quantum computers are able to answer those issues much more rapidly using Shor's algorithm [97, 99], breaking many widely-used encryption methods. Most of today's secure communications are thus at risk when large-scale quantum computers come along. Pre-emption of this is being done by post-quantum cryptog- raphy which is developing quantum-resistant encryption algorithms. Methods like lattice-based cryptography and multivariate polynomials are some of the promising solutions considered [98]. As these methods do not depend on mathematical problems which can readily be answered by a quantum computer, they cannot be used to perform quantum attacks on them. This has resulted in active development of cryptographic standards that withstand threats from quantum computing, as led by organizations like NIST [98]. Lastly, blockchain technology is also vulnerable to the threats of quantum computing. The fundamental foundation for securing a blockchain relies on cryptographic principles that quantum computers may breach, primarily at public key algorithms related to transaction verification [99]. Scientists are thus looking to develop post-quantum crypto- graphic algorithms to secure blockchain and distributed ledger systems to ensure that blockchain systems can still function securely into the quantum future [97].

6.2. 5G SECURITY CHALLENGES

Apart from being faster and more real-time, 5G networks pose new security challenges in communi- cation. Unlike previous generations, 5G systems are much more decentralized, based on virtualization, with their attack surface increased [92]. Due to decentralization, several attacks could occur on these 5G networks by targeting virtualized environments and SDN. Here the attacker exploits weak points in the control systems of the network [91, 92]. The most critical problem with the surge of IoT devices is the case with 5G. Amount of IoT gadgets which are expected to be using 5G networks is very high, yet these devices do not have inbuilt security protections. A hacker can attack the network through vulnerable devices, and such an attack will likely result in a DDoS [100]. This large number of connected devices, coupled with heterogeneous security stan- dards developed by manufacturers, means securing the network is a task that is quite complex [100]. Against this backdrop, security researchers are concentrating on developing enhanced encryption protocols, anomaly detection systems, and zero-trust architectures for securing 5G networks. Network slicing, one of the major features of 5G, will allow for personalized and customized virtual networks for each application, but a breach in one slice can have a ripple effect on others [91]. This means that continuous innovation in network security solutions is then required to fill these vulnerabilities, such as more advanced real-time monitoring systems and adaptive encryption techniques [92].

6.3. CYBERSECURITY IN AI-DRIVEN SYSTEMS

AI is being incorporated into the cybersecurity defenses more and more, from real-time threat de- tection to automated systems of response. However, AI systems may be prone to many exploits including adversarial inputs-subtle changes to input data can deceive AI models into making wrong predictions [89]. These have been demonstrated in many domains, such as both image detection, natural language processing, demonstrating that there is a high critical need for better defenses [89]. Another emerging concern is that AI is increasingly being adopted by cyber attackers to enhance their malicious capability. Attackers use AI automa- tion tools to build up automated phishing campaigns, to create more sophisticated malware types and even for retaliating against adaptive cybersecurity efforts [85]. In this ”arms race” between defenders and attackers in wits, each of them becomes increasingly smart at outpacing the other in this cyber battle of wits [85]. Because of this reality, ensuring AI systems is of extreme importance, especially since maliciously applied AI automa- tion can now be deployed to execute attacks [81]. Multi-level Approach towards the Integrity and Security of AI Models The strength of adversarial training techniques combined with secure deployment of models and encrypted datasets prevent tampering with AI models [75]. In addition, the data used in the training of AI systems needs to be carefully chosen in order not to fall victim to any bias or manipulation that would lead to compromised decision-making processes in important systems, such as medical care and vehicles 4. With continued pace of AI evolution, it would also be important that its security be ensured to continue the trust value in AI-related systems 8.

6.4. EDGE AND FOG COMPUTING SECURITY

Fog computing pushes the cloud closer to the network's edge, providing better mobility with low latency for the IoT devices; however, this shift of data introduces an important security challenge [103]. For example, there is a need to secure data as it moves from fog nodes to multiple nodes in the cloud [103]. Because of the geographical distribution of fog nodes, they will face physical and cyber attacks based on the isolated nodes with lesser degrees of protection [104]. Indeed, maintaining data confidentiality and integrity at the edge is critical in carrying out operations in a secure manner as resources are limited [105]. Heterogeneity of devices involved in a fog environment complicates the implementation of uniform security protocols, hence possible security gaps [104]. To address the issues identified, researchers have developed access control systems and mechanisms for resource management specifically designed for fog environments [103]. An adaptive resource management framework presented to improve the protection of the fog, with monitoring user behavior through issue risk-based access certificates [105]. It conducts trust evaluations in real-time such that assessment whether to allow or deny will be made instantaneously thereby reducing the latency of the process in the access control mechanism [105]. Lightweight encryption frameworks are also important to achieve data protection on scalable and flexible resource-constrained fog devices with growing demands [104]. Such solutions are significant for ensuring security without any trade-off in the performance of fog-based networks [103]. Besides the protection of data transfer, protecting the nodes at the fog itself is a priority because the fog nodes are very critical in a fog architecture [104]. The distributed nodes usually have very limited security oversight, making these nodes suitable for use by a cybercrook to deploy malicious applications and manipulate sensitive data [103]. To overcome this, advanced risk estimation and trust management models are developed to detect anomalies and prevent unauthorized access of the deployed fog services [105]. These models will allow the fog network to dynamically assess the threat level and undertake proactive measures toward protecting infrastructure [104]. With these security advancements, fog computing can provide the flexibility required for future IoT applications while ensuring robust security [105].

7. COMPARATIVE ANALYSIS OF EXISTING RESEARCH

AI and machine learning approaches have become increasingly important in cybersecurity research and the goal being improving both defensive and offensive capabilities. By automating threat detection and response processes, AI has the ability to provide real-time and adaptive solutions for a wide range of cyber threats.

7.1. CATEGORIZATION OF RESEARCH

Both offensive and defensive applications of AI draw attention to the various machine learning tech- niques for proactive threat modeling and intrusion detection [106]. Developing AI/ML models have a privacy focus which handle sophisticated cyberthreats and balance security with ethical considerations [107]. There are IoT-specific cyberthreats which exist. Machine learning approaches have the capacity to improve real-world security in IoT frameworks. [108]. Highlights of research on big data analytics applications in cybersecurity, specifically in identifying trends and patterns in massive datasets to reduce security breaches is another area of research [109].

7.2. CRITICAL ANALYSIS

Existing AI methods have shortcomings in responding to new cyberthreats, especially when it comes to managing changing attack strategies. There is an absence of frameworks which are capable of evolving with these threats. Additionally, limitations in dataset generalizability affect real-time application which reduces the effectiveness of AI in dynamic cybersecurity [110]. Offensive AI applications with short exploration focus on adversarial AI techniques and defense mechanisms while pointing out the gap in strategic policies for such attacks. [111]. Underlining ethical risks such as privacy invasion, human deskilling and AI-controlled cyber escalation is another major area of study. These topics highlight the need for comprehensive policies on AI's role in cybersecurity [112]. To provide a quick glance of comparative knowledge of cybersecurity issues across future technologies, Table 1 consolidates into a single view the challenges, implications, and directions of future research.

8. RECOMMENDATIONS FOR FUTURE RESEARCH

Future research should focus on developing adaptive AI models. These should be capable of evolving in response to emerging threats and shifting cyber landscapes. Interdisciplinary collaboration is necessary to address complex cybersecurity concerns, including domains such as ethics, law and data science.

8.1. EMERGING AREAS NEEDING ATTENTION

A thorough investigation into quantum-resistant algorithms is required. There is also a need to establish cybersecurity policies for dangers posed by quantum computing [107]. Ethical framework in cybersecurity is another area which needs attention. Issues such as privacy, autonomy and surveillance risks should be taken into account. Integrating ethical standards into AI model development in cybersecurity can help solve these issues [112].

Table 1. Quick overview of the future trends in Cybersecurity

Technology	Key Challenges	Security Implications	Emerging Solutions	Research Gaps
5G	Decentralized architecture, network slicing vulnerability	DDoS, signaling plane attacks, inter-slice leaks	Zero-trust architectures, secure network slicing	Standardization across slices, real-time anomaly detection
Quantum Computing	Ability to break RSA, ECC encryption	Cryptographic failure, data leakage	Post-quantum cryptography (e.g., lattice-based, code-based)	Scalability, migration to quantum-resistant protocols
AI in Security	Adversarial attacks, model poisoning	Misclassification, bypassing IDS/EDR	Explainable AI, adversarial training, federated learning	Real-world robustness, transparency, ethics integration
Edge Computing	Distributed trust, physical node exposure	Data interception, rogue edge nodes	Lightweight encryption, risk-aware access control	Standardized security frameworks for fog/edge nodes

8.2. IMPROVEMENT IN EXISTING STRATEGIES

Enhanced data processing methods for real-time threat detection within big data framework displayed the potential of robust data-driven analytics to identify and prevent complex attacks effectively [109]. There should also be advancements in DL and metaheuristic algorithms to improve response accuracy. Some models are also proposed which are capable of handling dynamic cyber threats and reducing false positives [110].

9. NOVELTY OF THE WORK

The paper presents a comprehensive consolidation of existing research in cybersecurity with a structured, cross-domain perspective that distinguishes it from generic surveys. The key novelty lies in the multi-layered comparative analysis of cybersecurity techniques across five critical domains: cloud, IoT, mobile, network, and AI-integrated systems. By organizing content not just thematically but also through tabular performance comparisons, the study offers accessible and evaluative insight into complex technical trends such as anomaly detection, EDR systems, SOAR platforms, and post-quantum cryptographic considerations. Moreover, the inclusion of emerging threat vectors like AI-driven cyberattacks, evolving ransomware tactics (e.g., double extortion), and 5G-induced vulnerabilities adds depth and relevance to the review, reflecting the shifting cybersecurity landscape. Unlike many generic reviews, this paper highlights defense-offense symmetry in AI usage, covering both adversarial inputs and defensive ML strategies, which is further contextualized through a categorization of research efforts (Section 7.1) and critical analysis of dataset generalizability (Section 7.2).

The survey also integrates regulatory, ethical, and human-factor dimensions, an often-overlooked aspect in purely technical reviews by synthesizing insights from cross-disciplinary studies (Table 4), thus presenting a more holistic view of cybersecurity challenges. The forward-looking research agenda (Section 8) not only outlines future trends like post-quantum cryptography and Explainable AI (XAI) but also advocates for adaptive and scalable cybersecurity solutions, filling gaps identified in current implementations. Overall, the novelty stems from the structured synthesis of current research, comparative tabulations with performance metrics, and cross-domain evaluation of threats and solutions, all while embedding future-forward and ethical dimensions within the cybersecurity discourse.

10. NOVELTY IN THE DOMAIN OF CYBERSECURITY

Cybersecurity is no longer confined to firewalls and antivirus software; it is rapidly transforming into a dynamic, intelligent, and deeply integrated defense ecosystem. As highlighted in this paper, the domain is undergoing a paradigm shift, driven by the infusion of cutting-edge technologies and the ever-evolving nature of threats.

At the forefront of this transformation is the adoption of Artificial Intelligence (AI) and Machine Learning (ML), which are revolutionizing threat detection and response. These technologies enable cybersecurity systems to go beyond static defenses, learning from network behavior to detect zero-day attacks, uncover anomalies, and even automate responses in real time. The field is also witnessing a new breed of AI-powered threats, where adversaries use machine learning to craft evasive malware and hyper-personalized phishing campaigns marking the rise of an AI-versus-AI security battlefield.

The novelty further extends to the emergence of post-quantum cryptography, as the threat of quantum computing looms over conventional encryption algorithms. This has sparked a race to develop quantum-resistant protocols that can withstand the computational power of future quantum systems, an innovation critical to safeguarding national infrastructure and sensitive data. Cybersecurity is also being redefined by its expansion into complex, heterogeneous environments like 5G, IoT, cloud, and edge computing. Each of these domains introduces novel challenges ranging from securing billions of low-power IoT devices to protecting decentralized fog nodes against tampering. As a result, there is a surge in lightweight cryptography, real-time threat intelligence, and decentralized defense strategies. Meanwhile, advanced platforms such as SOAR and EDR are reshaping security operations through automation, orchestration, and behavioral analytics offering rapid containment of threats that would otherwise evade traditional controls. These systems embody the shift toward intelligent, scalable, and responsive cybersecurity frameworks. Equally groundbreaking is the integration of ethical, legal, and human-centric dimensions into the cybersecurity conversation. The focus is shifting from purely technical safeguards to responsible AI, privacy-aware design, and resilience against insider threats ensuring that future solutions are not just powerful, but also accountable and trustworthy. The domain of cybersecurity is evolving from reactive defense into a proactive, predictive, and adaptive discipline ready to meet the challenges of a hyperconnected and increasingly intelligent digital world.

11. CONCLUSION

This landscape of cybersecurity requires robust, adaptable, and forward-thinking defense mechanisms. This research has thrown light on how modern cyber threats, from traditional malware to AI-enhanced attacks, pose new challenges across different sectors of IoT, cloud, and network security. These are the defensive technologies that would fight these threats: IDS, SIEM, SOAR, and even solutions based on machine learning. But all of these have their limitations, especially as the evasion techniques become more sophisticated in the hands of cybercriminals. The newest entrants into the technologies - quantum computing and 5G - open new avenues of vulnerability and thus a call for quantum-resistant encryption and advanced network protocols. Moreover, ethical considerations need to be incorporated into the development of AI for cybersecurity as its role continues to expand so that there is no misuse and it gains trustworthiness. The paper underlines the fact that cybersecurity requires continuous research and adaptation, with innovative, data-driven, and ethically grounded solutions. The future directions remain in the development of tailored AI models for threat detection, resilient cryptographic frameworks for the quantum era, and regulatory challenges to establish a secure digital environment for all users.

REFERENCES

[1] M. N. Al-Suqri, M. Gillani, "A comparative analysis of information and artificial intelligence toward national security", IEEE Access, Vol. 10, 2022, pp. 64420-64434.

[2] H. James, M. Sabir, "AI-Driven Cybersecurity for Sustainable Healthcare Data: Protecting Patient Privacy and Environmental Impact", 2024.

[3] L. Ayala, "Cybersecurity for hospitals and Healthcare Facilities, A Guide to Detection and Prevention", Apress Berkeley, 2016.

[4] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, M. Xu, "A survey on machine learning techniques for cyber security in the last decade", IEEE Access, Vol. 8, 2020, pp. 222310-222354.

[5] D. Schlette, M. Caselli, G. Pernul, "A comparative study on Cyber Threat Intelligence: The security incident response perspective", IEEE Communications Surveys & Tutorials, Vol. 23, No. 4, 2021, pp. 2525-2556.

[6] M. Ahsan et al. "Cybersecurity threats and their mitigation approaches using Machine Learning—A Review", Journal of Cybersecurity and Privacy, Vol. 2, No. 3, 2022, pp. 527-555.

[7] S. Zong, A. Ritter, G. Mueller, E. Wright, "Analyzing the perceived severity of cybersecurity threats reported on social media", arXiv:1902.10680, 2019.

[8] US GAO - US Government Accountability Office, "Cybersecurity: Threats Impacting the Nation", 2012, https://www.gao.gov/products/gao-12-666t (accessed: 2025)

[9] E. Tyugu, "Artificial intelligence in cyber defense", Proceedings of the 3rd International Conference on Cyber Conflict, Tallinn, Estonia, 2011, pp. 1-11.

[10] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, R. Ahmad", Machine Learning and Deep Learning Approaches for CyberSecurity: A Review", IEEE Access, Vol. 10, 2022, pp. 19572-19585.

[11] F. R. Alzaabi, A. Mehmood, "A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods", IEEE Access, Vol. 12, 2024, pp. 30907-30927.

[12] Z. Zulkifl et al. "FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs", IEEE Access, Vol. 10, 2022, pp. 15644-15656.

[13] B. Guembe et al. "The emerging threat of AI-Driven Cyber Attacks: A Review", Applied Artificial Intelligence, Vol. 36, No. 1, 2022.

[14] R. Bace, P. Mell, "Intrusion Detection Systems", NIST, https://www.nist.gov/publications/intrusion-detection-systems (accessed: 2024)

[15] A. Chidukwani, S. Zander, P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations", IEEE Access, Vol. 10, 2022, pp. 85701-85719.

[16] O. Aslan, R. Samet, "A comprehensive review on malware detection approaches", IEEE Access, Vol. 8, 2020, pp. 6249-6271.

[17] D.-O. Won, Y.-N. Jang, S.-W. Lee, "Plausmal-Gan: Plausible malware training based on generative adversarial networks for analogous zero-day malware detection", IEEE Transactions on Emerging Topics in Computing, Vol. 11, No. 1, 2023, pp. 82-94.

[18] E. Gandotra, D. Bansal, S. Sofat, "Malware analysis and classification: A survey", Journal of Information Security, Vol. 05, No. 02, 2014, pp. 56-64.

[19] I. Gulatas, H. H. Kilinc, A. H. Zaim, M. A. Aydin, "Malware Threat on Edge/Fog Computing Environments from Internet of Things Devices Perspective", IEEE Access, Vol. 11, 2023, pp. 33584-33606.

[20] H. Abroshan, J. Devos, G. Poels, E. Laermans, "Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process", IEEE Access, Vol. 9, 2021, pp. 44928-44949.

[21] F. Castano, E. F. Fernandez, R. Alaiz-Rodrıguez, E. Alegre, "PhiKitA: Phishing Kit Attacks Dataset for Phishing Websites Identification", IEEE Access, Vol. 11, 2023, pp. 40779-40789.

[22] H. Abroshan, J. Devos, G. Poels, E. Laermans, "COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic", IEEE Access, Vol. 9, 2021, pp. 121916-121929.

[23] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review", IEEE Access, Vol. 10, 2022, pp. 39325-39343.

[24] F. R. Alzaabi, A. Mehmood", A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods", IEEE Access, Vol. 12, 2024, pp. 30907-30927.

[25] P. Lavanya, H. Anila Glory, V. S. Shankar Sriram, "Mitigating insider threat: A Neural Network approach for enhanced security", IEEE Access, Vol. 12, 2024, pp. 73752-73768.

[26] A. J. Hintaw, S. Manickam, M. F. Aboalmaaly, S. Karuppayah, "MQTT vulnerabilities, attack vectors and solutions in the internet of things (IoT)", IETE Journal of Research, Vol. 69, No. 6, 2021, pp. 3368-3397.

[27] K. Fahad Ali, G. Li, A. N. Khan, Q. W. Khan, My. Hadjouni, H. Elmannai. "AI-Driven CounterTerrorism: Enhancing Global Security Through Advanced Predictive Analytics." IEEE Access, Vol. 11, 2023, pp. 135864-135879.

[28] N. Kaloudi, J. Li, "The AI-Based Cyber Threat Landscape", ACM Computing Surveys, Vol. 53, No. 1, 2020, pp. 1-34.

[29] S. Sharma, R. Kumar, C. R. Krishna, "Ransom Analysis: The Evolution and Investigation of Android Ransomware", Proceedings of the International Conference on IoT Inclusive Life, Chandigarh, India, 19-20 December 2019, pp. 33-41.

[30] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, V. Pospelova, "The Emerging Threat of Ai-driven Cyber Attacks: A Review", Applied Artificial Intelligence, Vol. 36, No. 1, 2022, pp. 1-34.

[31] K. Ansam, I. Gondal, P. Vamplew, J. Kamruzzaman, "Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges", Cybersecurity, Vol. 2, No. 20, 2019, pp. 1-22.

[32] A. H. Almutairi, N. T. Abdelmajeed, "Innovative signature-based intrusion detection system: Parallel processing and minimized database", Proceedings of the International Conference on the Frontiers and Advances in Data Science, Xi'an, China, 23-25 October 2017, pp. 114-119.

[33] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches", Transactions on Emerging Telecommunications Technologies, Vol. 32, No. 1, 2020, pp. 1-29.

[34] T. Saba, A. Rehman, T. Sadad, H. Kolivand, S. A. Bahaj, "Anomaly-based Intrusion Detection System for IoT Networks Through Deep Learning Model", Computers and Electrical Engineering, Vol. 99, 2022, p. 107810.

[35] Ma lek, S. Zakiyabanu, B. Trivedi, A. Shah, "User behavior pattern-signature based intrusion detection", Proceedings of the Fourth World Conference on Smart Trends in Systems, Security and Sustainability, London, UK, 27-28 July 2020, pp. 549-552.

[36] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, S. Venkatraman", Deep Learning Approach for Intelligent Intrusion Detection System", IEEE Access, Vol. 7, 2019, pp. 41525-41550.

[37] P. Ioulianou, V. Vassilakis, I. Moscholios, M. Logothetis, "A Signature-based Intrusion Detection System for the Internet of Things", https://eprints.whiterose.ac.uk/133312/1/ictf2018IoT.pdf (accessed: 2025)

[38] D. A. Bierbrauer, A. Chang, W. Kritzer, N. D. Bastian, "Cybersecurity Anomaly Detection in Adversarial Environments", arXiv:2105.06742, 2021.

[39] A. Yaseen, "The Role of Machine Learning in Network Anomaly Detection for Cybersecurity", Sage Science Review of Applied Machine Learning, Vol. 6, No. 8, 2023, pp. 16-34.

[40] Q. Liu, V. Hagenmeyer, H. B. Keller, "A review of rule learning-based intrusion detection systems and their prospects in smart grids", IEEE Access, Vol. 9, 2021, pp. 57542-57564.

[41] F. E. Ayo, S. O. Folorunso, A. A. Abayomi-Alli, A. O. Adekunle, J. B. Awotunde, "Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection", Information Security Journal: A Global Perspective, Vol. 29, No. 6, 2020, pp. 267-283.

[42] M. Evangelou, N. M. Adams, "An anomaly detection framework for cyber-security data", Computers & Security, Vol. 97, No. C, 2020.

[43] F. R. Alzaabi, A. Mehmood, "A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods", IEEE Access Vol. 12, 2024, pp. 30907-30927.

[44] A. Nassar, M. Kamal, "Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies", Journal of Artificial Intelligence and Machine Learning in Management, Vol. 5, No. 1, 2021, pp. 51-63.

[45] S. Yuan, X. Wu, "Deep Learning for Insider Threat Detection: Review, Challenges and Opportunities", Computers & Security, Vol. 104, 2021.

[46] G. G. Granadillo, S. G. Zarzosa, R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", Sensors, Vol. 21, No. 14, 2021, pp. 1-28.

[47] M. A. Hussein, E. K. Hamza, "Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM)", International Journal of Intelligent Engineering and Systems, Vol. 15, No. 6, 2022, pp. 667-6681.

[48] U. Bartwal, S. Mukhopadhyay, R. Negi, S. Shukla. "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots", Proceedings of the IEEE Conference on Dependable and Secure Computing, Edinburgh, Scotland, UK, 22-24 June 2022, pp. 1-8.

[49] J. Kinyua, L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions", Intelligent Automation & Soft Computing, Vol. 28, No. 2, 2021, pp. 527-545.

[50] G. Karantzas, C. Patsakis, "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors", Journal of Cybersecurity and Privacy, Vol. 1, No. 3, 2021, pp. 387-421.

[51] W. U. Hassan, A. Bates, D. Marino, "Tactical Provenance Analysis for Endpoint Detection and Response Systems", Proceedings of the IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 18-21 May 2020, pp. 1172-1189.

[52] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, M. Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies", IEEE Access, Vol. 9, 2021, pp. 57792-57807.

[53] S. An, A. Leung, J. B. Hong, T. Eom, J. S. Park, "Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security", IEEE Access, Vol. 10, 2022, pp. 75117-75134.

[54] Q. Wang, Z. Wang, W. Wang, "Research on Secure Cloud Networking Plan Based on Industry-Specific Cloud Platform", IEEE Access, Vol. 11, 2023, pp. 51848-51860.

[55] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review", IEEE Access, Vol. 9, 2021, pp. 20717-20735.

[56] V. Chang, M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework", IEEE Transactions on Services Computing, Vol. 9, No. 1, 2016, pp. 138-151.

[57] S. Mavoungou, G. Kaddoum, M. Taha, G. Matar, "Survey on Threats and Attacks on Mobile Networks", IEEE Access, Vol. 4, 2016, pp. 4543-4572.

[58] J. Cao et al. "A Survey on Security Aspects for 3GPP 5G Networks", IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, 2020, pp. 170-195.

[59] I. Ahmad et al. "An Overview of the Security Landscape of Virtual Mobile Networks", IEEE Access, Vol. 9, 2021, pp. 169014-169030.

[60] R. Khellaf, S. Boudouda, "Enhancing Mobile Enterprise Security: A Blockchain and Agent Paradigm-Based Approach for Continuous Protection and Rapid Adaptation," IEEE Access, Vol. 12, 2024, pp. 108108-108120.

[61] M. Sajjad, A. Ahmad, A. W. Malik, A. B. Altamimi, I. Alseadoon, "Classification and Mapping of Adaptive Security for Mobile Computing," IEEE Transactions on Emerging Topics in Computing, Vol. 8, No. 3, 2020, pp. 814-832.

[62] N. M. Karie, N. M. Sahri, W. Yang, C. Valli, V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments", IEEE Access, Vol. 9, 2021, pp. 121975-121995.

[63] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security", IEEE Internet of Things Journal, Vol. 7, No. 10, 2020, pp. 10250-10276.

[64] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations", IEEE Communications Surveys & Tutorials, Vol. 21, No. 3, 2019, pp. 2702-2733.

[65] M. Adam, M. Hammoudeh, R. Alrawashdeh, B. Alsulaimy, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems", IEEE Access, Vol. 12, 2024, pp. 57128-57149.

[66] M. Frustaci, P. Pace, G. Aloi, G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges", IEEE Internet of Things Journal, Vol. 5, No. 4, 2018, pp. 2483-2495.

[67] W. Zhou, Y. Jia, A. Peng, Y. Zhang, P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE Internet of Things Journal, Vol. 6, No. 2, 2019, pp. 1606-1616.

[68] H. Wang, D. Zhao, X. Li, "Research on Network Security Situation Assessment and Forecasting Technology", Journal of Web Engineering, Vol. 19, No. 7-8, 2020, pp. 1239-1266.

[69] V. P. Singh, M. P. Singh, S. Hegde, M. Gupta, "Security in 5G Network Slices: Concerns and Opportunities", IEEE Access, Vol. 12, 2024, pp. 52727-52743.

[70] J.-Y. Yu, E. Lee, S.-R. Oh, Y.-D. Seo, Y.-G. Kim, "A Survey on Security Requirements for WSNs: Focusing on the Characteristics Related to Security", IEEE Access, Vol. 8, 2020, pp. 45304-45324.

[71] C. De Alwis, P. Porambage, K. Dev, T. R. Gadekallu, M. Liyanage, "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions", IEEE Communications Surveys & Tutorials, Vol. 26, No. 1, 2024, pp. 534-570.

[72] G. Arfaoui et al. "A Security Architecture for 5G Networks", IEEE Access, Vol. 6, 2018, pp. 22466-22479.

[73] D. Fang, Y. Qian, R. Q. Hu, "Security for 5G Mobile Wireless Networks", IEEE Access, Vol. 6, 2018, pp. 4850-4874.

[74] M. Gupta, C. Akiri, K. Aryal, E. Parker, L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy", IEEE Access, Vol. 11, 2023, pp. 80218-80245.

[75] L. Yee Por et al. "A Systematic Literature Review on AI-Based Methods and Challenges in Detecting Zero-Day Attacks", IEEE Access, Vol. 12, 2024, pp. 144150-144163.

[76] R. Shevchuk, V. Martsenyuk, "Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges", IEEE Access, Vol. 12, 2024, pp. 81265-81280.

[77] S. Zeadally, E. Adi, Z. Baig, I. A. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity", IEEE Access, Vol. 8, 2020, pp. 23817-23837.

[78] N. Capuano, G. Fenza, V. Loia, C. Stanzione, "Explainable Artificial Intelligence in CyberSecurity: A Survey", IEEE Access, Vol. 10, 2022, pp. 93575-93600.

[79] S. A. A. Bokhari, S. Myeong, "The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective", IEEE Access, Vol. 11, 2023, pp. 69783-69797.

[80] J. Jeong, J. Mihelcic, G. Oliver, C. Rudolph, "Towards an Improved Understanding of Human Factors in Cybersecurity", Proceedings of the IEEE 5th International Conference on Collaboration and Internet Computing, Los Angeles, CA, USA, 12-14 December 2019, pp. 338-345.

[81] S. Lee, S. Kim, "Blockchain as a Cyber Defense: Opportunities, Applications, and Challenges", IEEE Access, Vol. 10, 2022, pp. 2602-2618.

[82] M. A. Khatun, S. F. Memon, C. Eising, L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation", IEEE Access, Vol. 11, 2023, pp. 145869-145896.

[83] J. Pastor-Galindo, P. Nespoli, F. G. Marmol, G. M. Perez, "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends", IEEE Access, Vol. 8, 2020, pp. 10282-10304.

[84] T. Sauter, A. Treytl, "IoT-Enabled Sensors in Automation Systems and Their Security Challenges", IEEE Sensors Letters, Vol. 7, No. 12, 2023, pp. 1-4.

[85] M. Aljabri et al. "Detecting Malicious URLs Using Machine Learning Techniques: Review and Research Directions", IEEE Access, Vol. 10, 2022, pp. 121395-121417.

[86] R. Shevchuk, V. Martsenyuk, "Neural Networks Toward Cybersecurity: Domain Map Analysis of State-of-the-Art Challenges", IEEE Access, Vol. 12, 2024, pp. 81265-81280.

[87] A. Khurshid, R. Alsaaidi, M. Aslam, S. Raza, "EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme", IEEE Access, Vol. 10, 2022, pp. 129932-129948.

[88] A. Sundararajan, T. Khan, A. Moghadasi, A. I. Sarwat", Survey on Synchrophasor Data Quality and Cybersecurity Challenges, And Evaluation of Their Interdependencies", Journal of Modern Power Systems and Clean Energy, Vol. 7, No. 3, 2019, pp. 449-467.

[89] M. Gupta, C. Akiri, K. Aryal, E. Parker, L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy", IEEE Access, Vol. 11, 2023, pp. 80218-80245.

[90] A. W. Khan, S. Zaib, F. Khan, I. Tarimer, J. T. Seo, J. Shin, "Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach", IEEE Access, Vol. 10, 2022, pp. 65044-65054.

[91] A. Dutta, E. Hammad, "5G Security Challenges and Opportunities: A System Approach", Proceedings of the IEEE 3rd 5G World Forum, Bangalore, India, 10-12 September 2020, pp. 109-114.

[92] L. Shi, "Analysis of the Security of 5G Technology from the Network Level", SHS Web of Conferences, Vol. 144, 2022.

[93] P. G. Chiara, "The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements", International Cybersecurity Law Review, Vol. 3, 2022, pp. 255-272.

[94] A. Joshi, "Study of Cybersecurity Laws and Regulations", Indian Journal of Law, Vol. 2, No. 3, 2024, pp. 7-14.

[95] R. Ducato, "Data protection, scientific research, and the role of information," Computer Law & Security Review, Vol. 37, 2020, p. 105412.

[96] S. Patil, A. Jangra, M. Bhale, A. Raina, P. Kulkarni, "Ethical hacking: The need for cyber security", Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, Chennai, India, 21-22 September 2017, pp. 1602-1606.

[97] M. Njorbuenwu, B. Swar, P. Zavarsky, "A Survey on the Impacts of Quantum Computers on Information Security", Proceedings of the 2nd International Conference on Data Intelligence and Security, South Padre Island, TX, USA, 28-30 June 2019, pp. 212-218.

[98] K. Roy, "Quantum Computing and its Impact on Cryptography", https://www.idsa.in/backgrounder/quantum-computing-and-its-impact-on-cryptographykroy190717 (accessed: 2025)

[99] H. Yalcin, T. Daim M. M. Moughari, A. Mermoud, "Supercomputers and quantum computing on the axis of cyber security", Technology in Society, Vol. 77, 2024, p. 102556.

[100] G. Sahu, S. S. Pawar, "Security Challenges in 5G Network", Software Defined Networking for Ad Hoc Networks, Springer, 2022, pp. 75-94.

[101] K. Chetioui, B. Bah, A. O. Alami, A. Bahnasse, "Overview of Social Engineering Attacks on Social Networks", Procedia Computer Science, Vol. 198, 2022, pp. 656-661.

[102] J. Hunker, C. W. Probst, "Insiders and insider threats an overview of definitions and mitigation techniques", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1, 2011, pp. 4-27.

[103] S. Parikh, D. Dave, R. Patel, N. Doshi, "Security and Privacy Issues in Cloud, Fog and Edge Computing", Procedia Computer Science, Vol. 160, 2019, pp. 734-739.

[104] R. Rezapour, P. Asghari, H. H. S. Javadi, S. Ghanbari, "Security in fog computing: A systematic review on issues, challenges and solutions", Computer Science Review, Vol. 41, 2021.

[105] W. B. Daoud, S. Othmen, M. Hamdi, R. Khdhir, H. Hamam, "Fog computing network security based on resources management", EURASIP Journal on Wireless Communications and Networking, Vol. 50, 2023.

[106] I. D. Aiyanyo, H. Samuel, H. Lim, "A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning", Applied Sciences, Vol. 10, No. 17, 2020.

[107] M. Roshanaei, M. R. Khan, N. N. Sylvester, "Enhancing Cybersecurity through AI and ML: Strategies, Challenges, and Future Directions", Jour-

nal of Information Security, Vol. 15, No. 3, 2024, pp. 320-339.

[108] T. S. AlSalem, M. A. Almaiah, A. Lutfi, "Cybersecurity Risk Analysis in the IoT: A Systematic Review", Electronics, Vol. 12, No. 18, 2023.

[109] D. B. Rawat, R. Doku, M. Garuba, "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security", IEEE Transactions on Services Computing, Vol. 14, No. 6, 2021, pp. 2055-2072.

[110] A. H. Salem, S. M. Azzam, O. E. Emam, A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques", Journal of Big Data, Vol. 11, 2024, p. 105.

[111] M. Malatji, A. Tolah, "Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI", AI and Ethics, Vol. 5, 2025, pp. 883-910.

[112] M. Taddeo, "Three Ethical Challenges of Applications of Artificial Intelligence in Cybersecurity", Minds and Machines, Vol. 29, No. 2, 2019, pp. 187-191.

Trends and Networks in the Application of MCDM Methods in Computer Science: Analysis of the Web of Science Database

Review Paper

Ana Veljić*
University Business Academy in Novi Sad,
Faculty of Applied Management, Economics and Finance, Belgrade, Serbia
ana.veljic@mef.edu.rs

Dejan Viduka*
University Alfa BK,
Faculty of Mathematics and Computer Sciences
Belgrade, Serbia
dejan.viduka@alfa.edu.rs

Luka Ilić
University Business Academy in Novi Sad,
Faculty of Applied Management, Economics and Finance, Belgrade, Serbia
luka.ilic@mef.edu.rs

*Corresponding authors

Aleksandar Šijan
University Business Academy in Novi Sad,
Faculty of Applied Management, Economics and Finance
Belgrade, Serbia
aleksandar@mef.edu.rs

Darjan Karabašević
University Business Academy in Novi Sad,
Faculty of Applied Management, Economics and Finance, Belgrade, Serbia
Korea University,
College of Global Business,
Sejong, Republic of Korea
darjankarabasevic@korea.ac.kr

Abstract *– This paper presents a comprehensive bibliometric analysis of scientific output in the field of Multi-Criteria Decision-Making (MCDM) within the context of computer science, focusing on the period from 2019 to mid-2025. Using data from the Web of Science Core Collection, a total of 302 relevant papers were identified based on criteria such as publication year, language, document type, open access status, and research area. The analysis covers publication dynamics, the most influential authors and institutions, thematic directions, and collaboration structures. Special emphasis is placed on citation analysis of the most impactful works, as well as the visualization of co-authorship networks using the PRISMA methodology and tools such as RStudio and Biblioshiny. The results reveal a growing trend in publications, high activity by certain authors (e.g., Akram M and Liu Y), and strong collaboration within research clusters. Dominant topics include decision-making models, alternative selection, aggregation operators, and priority evaluation. This study provides insights into the structure and dynamics of the scientific community engaged in MCDM methods in computer science and may serve as a guide for future researchers, practitioners, and scientific development strategies.*

Keywords: *Multi-Criteria Decision-Making (MCDM), Bibliometric Analysis, Computer Science, AHP, TOPSIS, VIKOR, Fuzzy Logic, Web of Science*

Received: July 21, 2025; Received in revised form: October 20, 2025; Accepted: November 3, 2025

1. INTRODUCTION

In today's world, strongly shaped by digital transformation, information technologies, and pervasive automation, computer science plays a crucial role in solving complex problems that require systematic decision-making [1]. Decisions are increasingly made in contexts marked by uncertainty, resource limitations, and the presence of multiple conflicting criteria [2]. Under such conditions, Multi-Criteria Decision Making (MCDM) emerges as a necessary methodological framework that enables analytical ranking, selection, and evaluation of alternatives based on clearly defined criteria [3]. Due to its flexibility and applicability, MCDM methods have found a solid foundation in various areas of computer science, from algorithm optimization and software evaluation to technology selection, resource planning, and large-scale data system management [4].

With the rapid development of artificial intelligence methods, machine learning, IoT technologies, natural language processing, and decision support systems, there is a growing need for structured and transparent decision-making approaches [5]. In this context, MCDM methods such as the Analytic Hierarchy Process (AHP), TOPSIS, VI-KOR, ELECTRE, PIPRECIA, and SWARA provide formal models that integrate both quantitative and qualitative criteria, allowing for a balance between technical performance, functional requirements, and system constraints [6]. These methods not only enable multidimensional problem analysis but also provide a basis for objectively comparing complex alternatives in real-time, with minimal risk of subjectivity [7].

Alongside methodological advancements, scientific output in the field of MCDM has seen a significant increase, indicating growing interest from the academic community [8]. However, due to its wide application and fragmented terminology, there is a need for mapping, systematizing, and critically analyzing the existing research to identify key trends, influential authors, institutions, journals, and thematic focuses. In this regard, bibliometric analysis emerges as an effective tool for quantitatively mapping scientific production and gaining insight into the structure, dynamics, and evolution of a specific research domain.

This study aims to provide a comprehensive overview of research activities related to the application of MCDM methods within computer science through bibliometric analysis. The focus is on analyzing publication trends over the past seven years (2019–2025), identifying the most influential authors and institutions, detecting key research topics, and evaluating collaboration networks. Using data from the Web of Science database and tools such as Biblioshiny, RStudio, and Excel, this paper offers an empirically grounded view of the state of the field and highlights directions for its future development [9].

The significance of this analysis lies not only in its descriptive representation of scientific output but also in its ability to offer researchers a clear orientation regarding strategic positioning within the research community, the selection of relevant journals, and the identification of thematic niches with innovation potential. Furthermore, the results of this study can serve as a foundation for meta-research syntheses, strategic research management, and the promotion of interdisciplinary and international collaboration in decision-making within computer science.

1.1. BACKGROUND AND IMPORTANCE OF THE TOPIC

Multi-Criteria Decision Making (MCDM) represents a class of quantitative methods that enable structured problem-solving in situations requiring the simultaneous consideration of multiple, often conflicting, criteria [3]. In today's information-driven society, simple analyses are increasingly insufficient for making high-quality decisions, particularly in fields such as system design, risk management, algorithm selection, and performance evaluation [10]. MCDM methods have become essential in computer science because they offer the capability for precise, transparent, and replicable evaluation of alternative solutions' qualities that are especially critical in software engineering, computational intelligence, automation, and other related disciplines [4].

In this context, particular attention is given to methods such as AHP, TOPSIS, ELECTRE, VIKOR, PIPRECIA, and SWARA, which allow for the evaluation and ranking of alternatives based on weighted criteria [11, 12]. This makes them suitable for complex engineering and information technology applications. Their use in computer science spans a wide range from the selection of computer networks, algorithms, and system architectures to the analysis of security, energy efficiency, and user experience. The growing complexity of information systems and the need for decisions that integrate technical, functional, and operational factors further emphasize the value of the MCDM approach [4].

The significance of this topic is also reflected in the increasing volume of global scientific output. The large number of publications in recent years demonstrates not only the academic maturity of this field but also the expanding application of MCDM methods in real-world and interdisciplinary contexts. Therefore, a comprehensive bibliometric analysis is necessary to map the research landscape, identify major research streams, and provide a foundation for future strategic directions.

1.2. OBJECTIVES AND RESEARCH QUESTIONS

The main objective of this paper is to identify and analyze scientific publications related to the application of MCDM methods in computer science through bibliometric analysis, focusing on the period from 2019 to 2025. By applying quantitative methods of scientific production analysis, the study aims to present the main thematic directions, influential authors, institutions, and sources, as well as collaboration patterns that shape this field.

The specific research objectives are to:

- Map the volume and dynamics of scientific production related to MCDM methods in computer science
- Identify the most influential authors, institutions, and journals in the field
- Detect the most common research topics and key terms associated with the use of MCDM methods
- Analyze the citation impact of individual publications
- Examine the structure of collaborative networks among authors and institutions
- Based on these goals, the following research questions have been formulated

- What are the trends in publishing scientific papers on MCDM methods in computer science between 2019 and 2025?
- Which authors, institutions, and journals have the greatest influence in this field?
- What are the most common research topics and terms associated with the application of MCDM methods?
- Which papers have the highest citation impact, and how has their influence evolved?
- How are collaboration networks among researchers structured, and what are the key nodes of connection within these networks?

Answers to these questions will enable a deeper understanding of the current state of research and serve as a foundation for future studies and applications of MCDM methodology in computer science.

2. FUNDAMENTAL DEFINITIONS AND CONCEPTS OF MCDM METHODS

MCDM is an approach used for making decisions in situations where multiple options must be evaluated based on several criteria [13]. MCDM methods enable systematic analysis and comparison of different alternatives by taking into account their strengths and weaknesses with respect to defined evaluation criteria [14]. The core concepts include identifying relevant criteria, assigning weights to each criterion, and applying mathematical or heuristic models to rank or select the best options [15]. MCDM methods are widely used in fields such as management, engineering, and economics because they provide an objective and transparent basis for decision-making [16].

2.1. ANALYTIC HIERARCHY PROCESS (AHP)

The Analytic Hierarchy Process (AHP) is an MCDM method developed by Thomas L. Saaty in the 1970s [17]. The first significant work that formally describes AHP is "A scaling method for priorities in hierarchical structures", published in 1977 in the Journal of Mathematical Psychology [18]. AHP facilitates structural analysis of complex decisions by decomposing a problem into hierarchical levels, which typically include the overall goal, criteria, and alternative options [19].

Users first construct a hierarchy of the problem and then perform pairwise comparisons of the elements at each level of the hierarchy using a relative importance scale [18]. These comparisons allow for the calculation of weights for the criteria and for the alternatives. The outcome is a ranked list of alternatives based on their overall weighted scores.

AHP is particularly useful in decision-making scenarios that require the integration of subjective judgments and intuitive preferences, making it a valuable tool when both qualitative and quantitative data must be considered.

2.2. PIPRECIA METHOD

The PIPRECIA (PIvot Pairwise RElative Criteria Importance Assessment) method is an advanced technique for determining the weights of criteria through pairwise comparisons [20]. This method is relatively recent compared to other MCDM methods. The first work describing the PIPRECIA method is "A novel multi-criteria decision-making method: pivot pairwise relative criteria importance assessment (PIPRECIA)", authored by R.K. Pamučar and M. Ćirović and published in 2015 in the journal Operational Research in Engineering Sciences: Theory and Applications. PIPRECIA involves iterative comparisons of criteria, where the relative weights are gradually adjusted based on mutual relationships. This method is especially useful in situations that require flexibility and adaptability in assigning criteria weights during the decision-making process.

2.3. TOPSIS METHOD

TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) is an MCDM method developed by Hwang and Yoon in 1981. [21]. The foundational work that describes this method in detail is the book "Multiple Attribute Decision Making: Methods and Applications", published in the same year [22]. The TOPSIS method is based on identifying a positive ideal solution (the best values for all criteria) and a negative ideal solution (the worst values for all criteria) [23]. Alternatives are ranked according to their distance from these ideal solutions. This method is particularly useful in scenarios where it is important to balance multiple criteria and choose the option that represents the most optimal combination of characteristics.

2.4. ELECTRE METHOD

ELECTRE (ELimination and Choice Expressing Reality) is a family of MCDM methods developed by Bernard Roy and collaborators [24]. The foundational work introducing the ELECTRE method is "Classement et choix en présence de points de vue multiples (La méthode ELECTRE)", published in 1968 [25]. ELECTRE methods use the principles of concordance and discordance to evaluate alternatives by establishing outranking relationships based on multiple criteria and eliminating those that do not meet specific thresholds [26]. ELECTRE is often applied to problems with conflicting criteria and where compromise solutions need to be identified. It is particularly valuable in situations characterized by high levels of uncertainty and complexity.

2.5. VIKOR METHOD

VIKOR (VIseKriterijumska Optimizacija i Kompromisno Rešenje - Multicriteria Optimization and Compromise Solution) is an MCDM technique developed by Opricovic and Tzeng [27]. The first significant publication describing the VIKOR method is "Compromise solution by MCDM methods: A comparative analysis of

VIKOR and TOPSIS", published in 2004 in the European Journal of Operational Research [23]. VIKOR focuses on identifying a compromise solution that best satisfies the conflicting criteria. The method uses linear programming to rank alternatives based on their proximity to an ideal solution, taking into account both the weights of criteria and the degree of compromise. VIKOR is especially helpful in decision-making scenarios where finding a balanced trade-off among criteria is critical, particularly when there is uncertainty in setting criteria priorities [28].

2.6. SWARA METHOD

SWARA (Step-wise Weight Assessment Ratio Analysis) is an MCDM method developed by Kersuliene, Zavadskas, and Turskis [29]. The first significant work describing the SWARA method is "Selection of rational dispute resolution method by applying new step-wise weight assessment ratio analysis (SWARA)", published in 2010 in the Journal of business economics and management [29]. The SWARA method involves an iterative assessment of the relative importance of criteria through a series of pairwise comparisons and successive adjustments of weights based on the outcome of each iteration [30]. SWARA supports decision-making processes that require accounting for changes in priorities and the importance of criteria over time [31]. This method is particularly useful in situations where criterion weights need to be dynamically adjusted to reflect evolving decision contexts.

3. RESEARCH METHODOLOGY

To achieve a systematic and comprehensive analysis of scientific output in the field of Multi-Criteria Decision Making (MCDM) within the domain of

computer science, this study applies a bibliometric methodology, with a particular focus on scientometric techniques and PRISMA (Fig. 1) guidelines [32]. This approach enables the quantitative mapping of scientific publications, identification of key researchers and themes, as well as the visualization of research networks and trends.

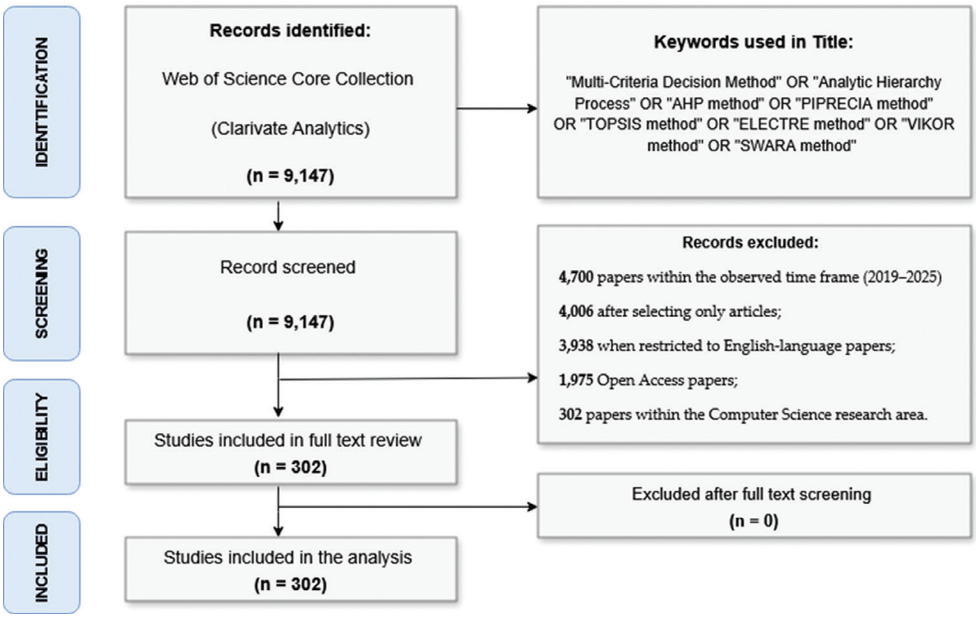


Fig. 1. PRISMA flowchart

3.1. DATABASE SELECTION

For the purpose of this study, the Web of Science Core Collection (Clarivate Analytics) was used as the primary database [33]. It is considered one of the most relevant sources for tracking scientific output in technical and engineering disciplines.

The search was conducted on June 15, 2025, and the selection of the WoS database is justified by its high relevance, standardized bibliographic records, and rich metadata necessary for conducting bibliometric analyses (including authors, institutions, citations, keywords, journals, etc.), as illustrated in Fig. 2.

3.2. DATABASE SELECTION

The search was conducted in line with the predefined thematic orientation, focusing specifically on MCDM methods within the field of computer science. The following terms were used in the search query:

"Multi-Criteria Decision Method" (Title) OR "Analytic Hierarchy Process" (Title) OR "AHP method" (Title) OR "PIPRECIA method" (Title) OR "TOPSIS method" (Title) OR "ELECTRE method" (Title) OR "VIKOR method" (Title) OR "SWARA method" (Title) All terms were searched within the titles of the papers to ensure specificity and to exclude publications that mention these methods only incidentally. The initial search yielded 9,147 results.

3.3. FILTERING CRITERIA AND RESULT REFINEMENT

Following the initial search, the following filtering criteria were applied to narrow down the focus to the most relevant publications:

- Publication years: 2019–2025.
- Document type: Articles only.
- Language: English only.
- Access type: Open Access only.
- Research area: Computer Science.

- After applying these filters, the number of results was successively reduced as follows:
- 4,700 papers within the observed time frame (2019–2025).
- 4,006 after selecting only articles.
- 3,938 when restricted to English-language papers.
- 1,975 Open Access papers.
- 302 papers within the Computer Science research area.

As shown in Fig. 3, these 302 papers comprise the final dataset analyzed in this study.

Completeness of bibliographic metadata - **302** documents from **Isi**

Metadata	Description	Missing Counts	Missing %	Status
AB	Abstract	0	0.00	Excellent
C1	Affiliation	0	0.00	Excellent
AU	Author	0	0.00	Excellent
CR	Cited References	0	0.00	Excellent
RP	Corresponding Author	0	0.00	Excellent
DI	DOI	0	0.00	Excellent
DT	Document Type	0	0.00	Excellent
SO	Journal	0	0.00	Excellent
LA	Language	0	0.00	Excellent
PY	Publication Year	0	0.00	Excellent
TI	Title	0	0.00	Excellent
TC	Total Citation	0	0.00	Excellent
DE	Keywords	32	10.60	Acceptable
ID	Keywords Plus	46	15.23	Acceptable
WC	Science Categories	302	100.00	Completely missing

Fig. 2. Completeness of bibliographic metadata

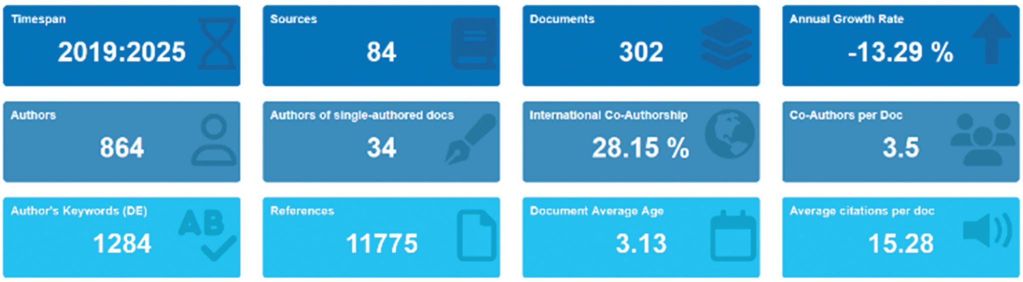


Fig. 3. Main data information

3.4. ANALYSIS FLOW ACCORDING TO THE PRISMA FRAMEWORK

The selection and screening process was conducted in accordance with the PRISMA guidelines (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), which require transparent reporting of the inclusion and exclusion flow of publications [33]. The PRISMA flow diagram (Fig. 1) illustrates the complete search and selection process, providing a clear overview of the steps taken from initial identification to the final inclusion of articles.

3.5. TOOLS AND ANALYTICAL APPROACH

The following tools were used for processing and visualizing bibliometric data:

- RStudio 2023.12.1 (Build 402) and Biblioshiny 4.1.4 – for conducting quantitative analyses, mapping thematic clusters, and generating network visualizations.
- Microsoft Excel v2407 – for additional data processing, tabular presentations, and the creation of summary diagrams.

- VOSviewer and Gephi (optional) – for advanced visualization of collaboration and citation networks.

This methodological framework ensures a comprehensive and reliable approach to identifying key research actors, thematic clusters, collaborative structures, and emerging trends in the domain of MCDM methods in computer science.

3.6. LIMITATIONS OF THE SEARCH AND METHODOLOGY

Although the search was carried out systematically and meticulously, with clearly defined criteria and adherence to the PRISMA framework, there are several important limitations to consider when interpreting the results:

- The analysis is based exclusively on the Web of Science database, thereby excluding relevant papers indexed in other databases such as Scopus, Google Scholar, IEEE Xplore, and Dimensions. As a result, some influential papers or authors may not be captured.
- The search query was limited to article titles, meaning studies that apply MCDM methods but do not mention them explicitly in the title (only in the abstract or body text) might have been omitted.
- The filtering by research area (Computer Science only) and language (English only) excludes potentially relevant interdisciplinary work or research published in other languages.
- The focus on Open Access publications may also affect the representativeness of the dataset, as some significant contributions may be found in subscription-based journals.
- Finally, data for the year 2025 only includes the first half (up to June 15), and the number of publications for that year is not final and should be interpreted with caution.

Despite these limitations, the applied methodological approach provides a solid foundation for conducting a reliable bibliometric analysis and enables the identification of key trends, influential contributors, and thematic directions within the dynamic field of MCDM methods in computer science.

4. RESULTS

This section provides a detailed overview of the key findings of the research, focusing on the analysis of the number of publications, influential authors, journals, and institutions in the field of Multi-Criteria Decision Making (MCDM). The analysis of publication trends and patterns contributes to a better understanding of the dynamics of research activity and identifies the main contributors to the advancement of this field.

4.1. GENERAL PUBLICATION TRENDS

The overview of general trends includes an analysis of the publication dynamics during the observed period, identification of key research areas, and prominent journals. The focus is on recognizing shifts in research interest and potential factors influencing fluctuations in publication volume, providing essential context for deeper result interpretation.

4.1.1. Publications

The number of publications per year reveals the dynamics of research activity in the field of MCDM in computer science over the past seven years. The analysis highlights oscillations in publishing intensity resulting from a combination of global events, institutional policies, resource availability, and evolving research interests.

From 2019 to 2022, a stable growth in publication volume was recorded:

- 2019: 40 papers.
- 2020: 37 papers.
- 2021: a notable increase to 53 publications.
- 2022: 53 publications again.

This continuity indicates a strong academic interest in applying MCDM methods to address complex problems in computer science. In 2023, a slight decline to 48 publications was observed, which may be attributed to a redistribution of research priorities or a delay between research execution and publication. However, 2024 marks a recovery, reaching a peak of 54 publications, suggesting a regained momentum and increasing interest in the topic.

For 2025, 17 publications were recorded by the data extraction date (June 15), representing only the first half of the year. This preliminary figure suggests continued researcher engagement, although results for this year must be interpreted with caution.

Fluctuations in publication volume may stem from factors such as reduced research funding, shifting funding priorities, or global crises such as the pandemic. On the other hand, a temporary decrease may prompt deeper and more focused studies with higher scientific contribution. Such a qualitative shift in research practice can enhance theoretical frameworks and promote the development of new methodological approaches in MCDM.

Despite annual variations, the overall trend remains positive, and the analysis confirms that MCDM in computer science continues to be a vital and relevant field, maintaining consistent research interest and potential for future development.

4.1.2. Number of Publications by Year

The year-by-year breakdown provides a detailed view of the trajectory and intensity of research activity in the field of MCDM methods within computer science. Changes in annual publication numbers reflect the impact of global conditions, evolving priorities, and availability of research resources.

2019: A total of 40 papers marked a strong start, indicating growing interest in applying MCDM methods in computing, largely driven by digital transformation and increasing system complexity.

2020: Publications slightly dropped to 37, likely influenced by the COVID-19 pandemic, which disrupted research cycles and publication dynamics.

2021: A sharp increase to 53 papers signals recovery from pandemic-related constraints and a growing reliance on quantitative and data-driven methodologies.

2022: The same total of 53 papers suggests stability and maturity in the application of MCDM techniques across various computing subfields.

2023: A modest drop to 48 papers may reflect a temporary reallocation of research funding or a shift toward emerging topics such as AI ethics and sustainable digital solutions.

2024: A new peak is reached with 54 publications, indicating renewed momentum and broader MCDM adoption in industry and academia, possibly aided by open data and increased global collaboration.

2025: 17 papers recorded by June 15. Although partial, this count points to a sustained interest, with expectations for a significant increase by the end of the year.

The overall publication trend (illustrated in Fig. 4) shows gradual growth between 2019 and 2025, with peak years in 2021 and 2024. While minor fluctuations are natural, the trend is overall stable and positive, affirming the relevance of MCDM in contemporary research and its necessity for further application and refinement.

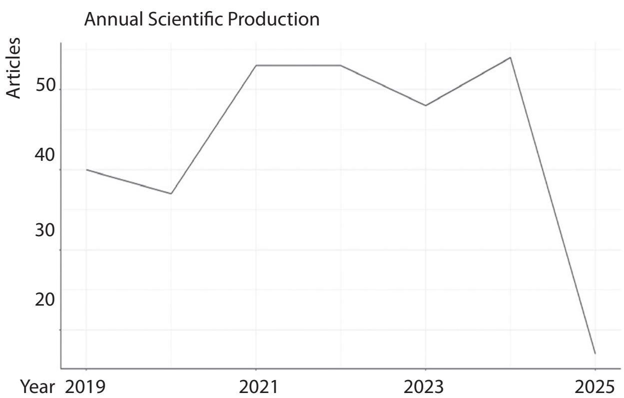


Fig. 4. Number of Publications by Year

4.1.3. Most Influential Journals

The analysis of publication sources provides insight into the most represented journals in which papers related to Multi-Criteria Decision Making (MCDM) in computer science are published (as shown in Table 1). This analysis helps identify the platforms that serve as the main channels for disseminating research findings and advancing the field. Below is an overview of the ten most represented journals based on the number of published papers:

Table 1. Top 10 leading publishers

No.	Journal	Number of Publications
1.	IEEE Access	74
2.	International Journal of Intelligent Systems	14
3.	Complex & Intelligent Systems	13
4.	Expert Systems with Applications	13
5.	ISPRS International Journal of Geo-Information	9
6.	Mobile Information Systems	9
7.	Soft Computing	9
8.	International Journal of Computational Intelligence Systems	8
9.	Scientific Programming	8
10.	Algorithms	7

IEEE Access, with 74 published papers, stands out as the most represented journal in the field of MCDM methods. Its broad thematic scope, open access policy, and fast peer-review process contribute to its popularity within the research community. This journal is particularly suitable for interdisciplinary studies that integrate decision-making methods with contemporary challenges in engineering and information technology.

International Journal of Intelligent Systems, Complex & Intelligent Systems, and Expert Systems with Applications rank among the leading journals by publication volume, with similar numbers of papers (13–14). These journals are known for their focus on artificial intelligence, computational intelligence, and the application of intelligent methods to real-world problems, making them ideal for publishing research that applies MCDM approaches.

In addition, a significant number of publications come from journals such as ISPRS International Journal of Geo-Information, Mobile Information Systems, and Soft Computing, indicating the broader application of MCDM methods in areas such as spatial information, mobile systems, and soft computing algorithms.

It is important to note that data on total citations and average citations per paper are currently unavailable, which somewhat limits a comprehensive assessment of these journals' impact. Nevertheless, the number of publications provides a clear picture of which journals serve as dominant platforms for research in this domain. Identifying the most prominent publication sources can help researchers choose appropriate journals for submitting future work and staying informed about current research trends. Focusing on these journals can contribute to greater visibility, wider readership, and stronger positioning of research findings within the global scientific community.

4.2. GENERAL PUBLICATION TRENDS

This section focuses on identifying the most influential authors and institutions shaping the development of the Multi-Criteria Decision Making (MCDM) field. Analyzing research productivity, citation impact, and inter-institutional collaboration provides insight into the key factors contributing to scientific advancement, defining research trends, and disseminating results within this domain.

4.2.1. Key Author Analysis

Based on updated bibliometric data, two authors stand out as the most influential and productive in the MCDM field: Liu Y and Akram M (as shown in Fig. 5). Their research spans a wide range of MCDM applications, with a focus on integrating traditional decision-making techniques with modern approaches such as fuzzy logic, optimization, geoinformation technologies, and artificial intelligence.

Liu Y consistently appears as one of the most prolific researchers in this domain. His most cited work from 2019, "Distance Measure for Fermatean Fuzzy Linguistic Term Sets Based on Linguistic Scale Function: An Illustration of the TODIM and TOPSIS Methods" [34], published in the International Journal of Intelligent Systems, has garnered 76 citations, averaging 10.8 citations per year, confirming his strong influence in the area of fuzzy MCDM models.

Another 2019 publication on landslide susceptibility assessment using GIS and the AHP method (published in ISPRS International Journal of Geo-Information) has received 42 citations (6.0 per year), highlighting his contribution to spatial decision-making and the application of MCDM methods in geographic contexts. In the past three years, Liu Y has also published several works applying extended MCDM approaches, including PSO-VIKOR, topological optimization, and AHP in the design of electric trucks and energy-efficient buildings. However, his 2024 article in Engineering Reports has not yet been cited, which is expected due to its recent publication.

Akram M stands out as the leading author in 2023 in terms of citation intensity. His article, "Enhanced ELECTRE II Method with 2-Tuple Linguistic M-Polar Fuzzy Sets for Multi-Criteria Group Decision Making" [35], published in Expert Systems with Applications, already has 35 citations, averaging 11.6 citations per year.

Two other works from the same year also show high impact:

- One on applying fuzzy ELECTRE for water system management (32 citations).
- Another on the selection of rehabilitation centers using M-polar fuzzy N-soft information (20 citations).
- Overall, Akram M demonstrates a very high annual citation rate, indicating not only the relevance of his research but also its strong practical applicability, especially in group decision-making and AI applications in healthcare.

Considering their publication output, annual citation rates, and multidisciplinary scope, these authors represent the core of contemporary MCDM research. Their contributions expand the theoretical foundation of decision-making methods and open new research directions through integration with intelligent systems, optimization, and applied statistics.

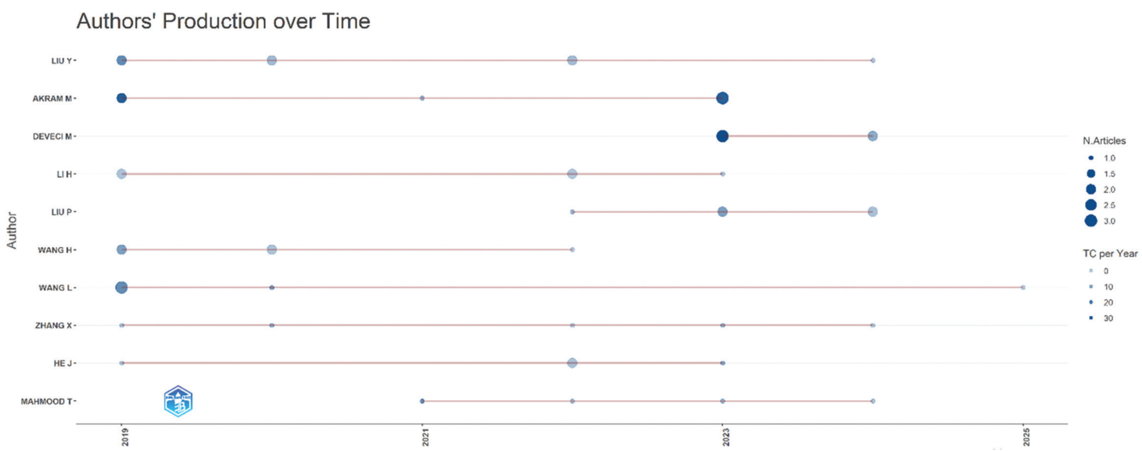


Fig. 5. Key Author Analysis

4.2.2. Key Author Analysis

The analysis of institutional research productivity in the field of MCDM indicates a clear increase in global interest (as shown in Table 2), with several universities contributing a significant number of publications. Based on the latest data, the ten most active institutions in terms of the number of published papers during the observed period are presented in the table below.

Three institutions share the top position in terms of publication count (11 papers each): King Mongkut's University of Technology Thonburi (KMUTT) from Thailand, National Defense University, and Sichuan University from China. Their leading positions indicate significant and ongoing dedication to research in decision theory, with particular emphasis on the application of MCDM methods in contexts such as engineering, security, and analytical systems.

Table 2. Top 10 leading publishers by publications

No.	Institution (Affiliation)	Number of Publications
1.	King Mongkut's University of Technology Thonburi (KMUTT)	11
2.	National Defense University	11
3.	Sichuan University	11
4.	University of the Punjab	10
5.	University of Salamanca	10
6.	Air Force Engineering University	9
7.	International Islamic University Islamabad	9
8.	Islamic Azad University	9
9.	Jiangxi University of Finance and Economics	9
10.	Budapest University of Technology and Economics	8

University of the Punjab (Pakistan) and University of Salamanca (Spain), each with 10 publications, highlight the geographical diversity of research and point to the wide international dissemination of knowledge in this field. Both institutions demonstrate consistent productivity, likely supported by multidisciplinary research teams and international collaborations.

Other notable institutions on the list include Islamic Azad University, International Islamic University Islamabad, and Air Force Engineering University, which have previously been recognized as key contributors in this field. Their continued presence among the most productive institutions reflects a stable research strategy and a sustained focus on the development and implementation of MCDM methods.

Although Jiangxi University of Finance and Economics and Budapest University of Technology and Economics, with 9 and 8 papers respectively, have slightly fewer publications, their inclusion in the list signals a growing interest in applying multi-criteria analysis in economic and technical domains.

It is important to note that this analysis covers only the quantitative aspect (number of publications), while qualitative metrics such as citation count and research impact are not included. Nevertheless, these figures offer a reliable insight into the institutions that contribute the most to advancing knowledge and promoting the use of MCDM approaches in computer science.

4.3. ANALYSIS OF MAIN RESEARCH TOPICS AND APPLICATION AREAS

The analysis of keyword frequency in titles and abstracts allows for the identification of the most frequently studied topics in the MCDM field (shown in Fig. 6), as well as insight into their evolution over time. Based on the analysis of term frequency and their occurrence quartiles (Q1 – initial presence, Q2 – peak frequency year, Q3 – end of active phase), several thematic focuses emerge:

The most frequent terms include model (47 occurrences), selection (36), sets (31), decision-making (30), AHP (29), and aggregation operators (23). These terms represent the core foundations of current MCDM research, indicating the prevalent use of decision-making models in alternative selection, work with various data sets, and a theoretical-operational base grounded in methods like AHP and aggregation theory.

Terms such as ranking (14), criteria (11), and weights (6) have become more prominent during the 2022–2024 period, suggesting a growing interest in sophisticated ranking techniques and weight optimization in the evaluation of alternatives. The relevance of expressions like multicriteria decision-making and priorities, which appear predominantly between 2022 and 2024, reflects a focus on formalizing priorities and the importance of criteria in increasingly complex problem domains.

Interestingly, terms such as extension (20) and aggregation operators have been active since as early as 2019, indicating that extending existing methods and developing new aggregation functions were among the top research priorities even in the early stages of the observed period. Methods such as VIKOR (9) and concepts like information (11) also hold a stable position within the thematic network, reaffirming the importance of multi-criteria compromise decision-making and the growing integration with information systems and data management.

The analysis of key terms confirms that MCDM research has evolved from foundational structural models and classical methods (such as AHP and VIKOR) toward more complex approaches involving criteria prioritization, weight management, and extended versions of existing methods. The increased frequency of terms related to selection, ranking, and aggregation points to a high level of practical application in domains such as engineering decision-making, system performance evaluation, and intelligent informatics frameworks.

These findings confirm that the field of multi-criteria decision-making is continuously expanding and adapting to the demands of modern problems, relying on mathematical formalization, heuristic approaches, and intelligent models to support decision-making under conditions of complexity and uncertainty.

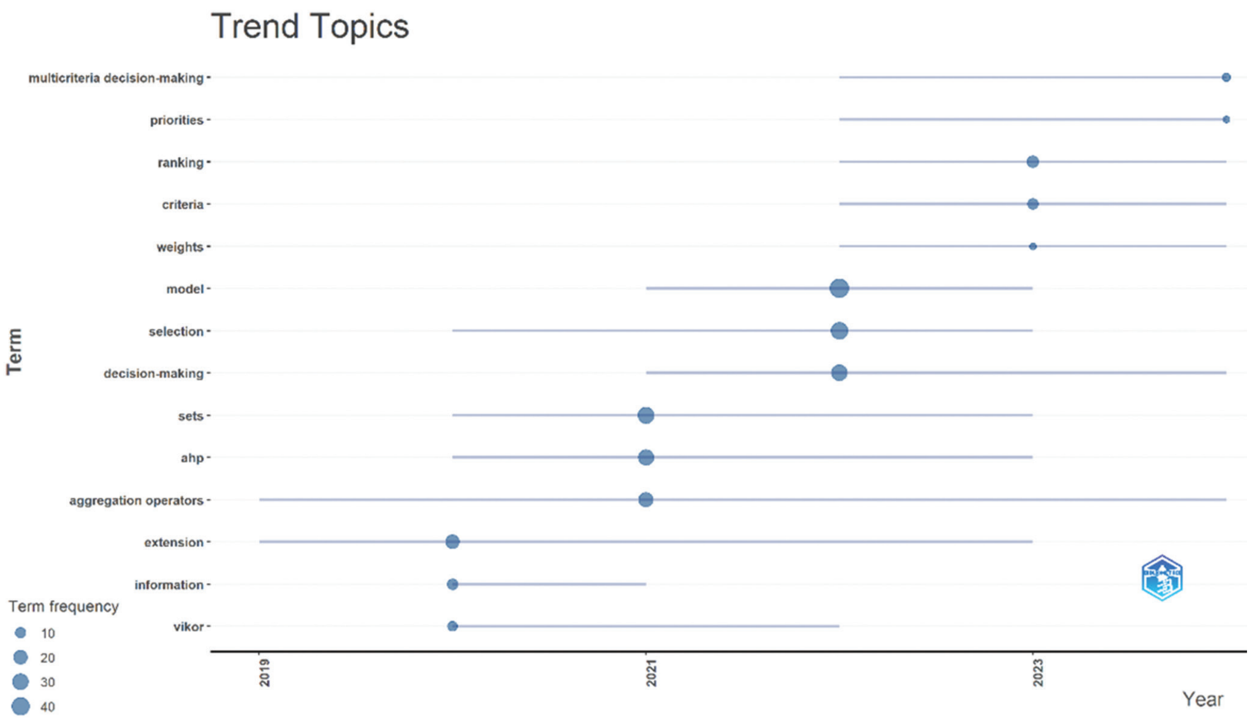


Fig. 6. Trend topics

4.4. CITATION ANALYSIS: IDENTIFYING THE MOST INFLUENTIAL PAPERS AND AUTHORS

Citation analysis is a key element in identifying the most influential authors and publications in the MCDM field. By using metrics such as total citation count, average citations per year (TC/year), and normalized citation count (Normalized TC), it is possible to highlight the papers that have a long-term and global impact on the development of this discipline (as shown in Fig. 7).

According to the analysis, the most cited paper in the dataset is a 2019 article by Akram M, published in the International Journal of Intelligent Systems (DOI: 10.1002/int.22103), with 172 total citations and an average of 24.5 citations per year, confirming its sustained relevance. Moreover, its normalized citation value (5.54) indicates that this work is widely used as a reference in numerous studies.

Another standout publication is the 2024 paper by Moslem S, published in Engineering Applications of Artificial Intelligence, which, despite its recency, has already reached 85 citations in less than two years (averaging 42.5 per year) with a normalized TC of 18.14, making it the most intensely cited work over a short timeframe. This reflects its high relevance and rapid integration into ongoing research.

Other significant papers include:

- Chan HK (2019) – Decision Support Systems (DOI: 10.1016/j.dss.2019.113114): 120 citations, 17.1 per year, Normalized TC: 3.86.
- Mohammed MA (2020) – IEEE Access: 115 citations, 19.1 per year, Normalized TC: 5.21.
- Alkan N (2021) – Applied Soft Computing: 94 citations, Normalized TC: 4.35.
- Al-Shami TM (2023) – Two papers in Complex & Intelligent Systems and Information with high normalized citation counts: 5.59 and 4.94, respectively.

Among authors with multiple influential publications, Liu D stands out with two papers in the International Journal of Intelligent Systems, published in 2019 and 2020 (with 76 and 69 citations, respectively), confirming his consistent contribution to the fields of fuzzy logic and intelligent systems.

Additionally, a considerable number of high-impact papers are published in journals such as IEEE Access, Expert Systems with Applications, Engineering Applications of Artificial Intelligence, and Applied Soft Computing, underlining their central role in disseminating MCDM research results.

Beyond total citations, the normalized citation count is a crucial metric for comparing the impact of papers published in different years, as it adjusts for the time advantage older publications have. Hence, papers from 2023–2024 with high normalized values can be considered emerging references in the coming years.

In conclusion, the citation analysis reveals that the most influential papers cover a wide spectrum of topics from group decision-making and fuzzy logic to artificial intelligence applications and real-world solution evaluation. These works are shaping the theoretical foundations, methodological innovations, and practical implementations of MCDM approaches in modern research.

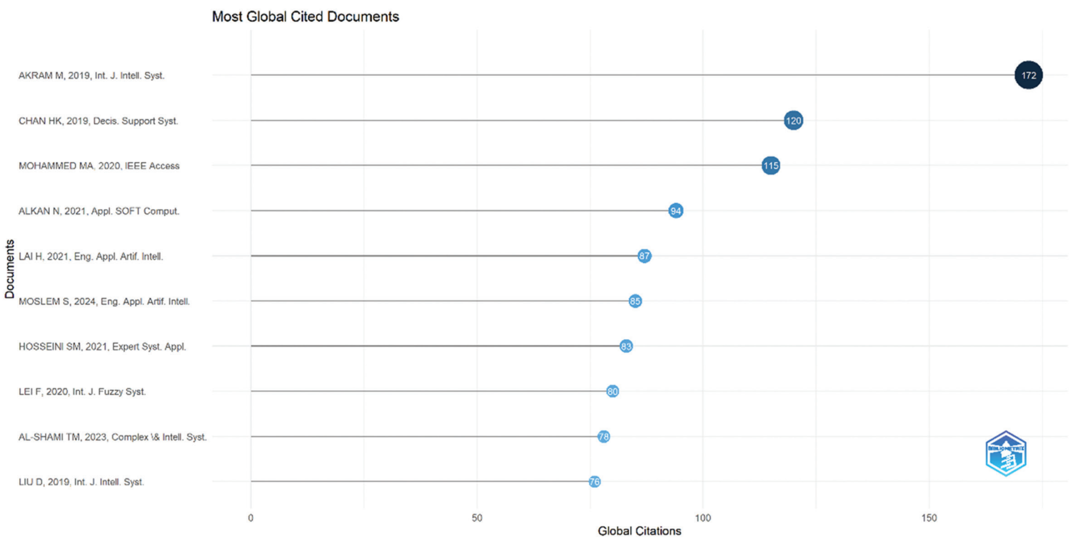


Fig. 7. Most Global Cited Documents

4.5. NETWORK ANALYSIS: COLLABORATION AMONG AUTHORS AND INSTITUTIONS

Network analysis enables the identification of collaboration patterns among researchers, highlighting key authors and institutions that act as connectors and hubs of influence in the MCDM field (as shown in Fig. 8). The analysis was conducted using network metrics such as betweenness centrality (intermediary importance), closeness centrality (network proximity), and PageRank (influence based on connectivity).

Based on cluster analysis, several research groups have been identified as shaping the global MCDM community:

Cluster 1 – "Li-Wu-Xu-Chen" Network

This group is led by authors such as Li F (betweenness: 69), Li J, and Wu Y, known for their high interconnectedness and strategic network positioning. This cluster likely represents strong regional collaboration within Chinese institutions, with a focus on applications of AHP and GIS in decision-making. Their proximity in the network reflects frequent co-authorship and mutual citation.

Cluster 2 – "Wang-Li-Xu-Zhang" Network

The largest cluster by number of authors includes some of the most influential figures, such as Wang Y (betweenness: 124.46, closeness: 0.017), Wang Z (120), Li Q, Xu J, Zhang C, and Wang Q. These authors form a dense collaboration network with high centrality, indicating their key role in bridging various research subgroups. Their high PageRank and closeness values further affirm their visibility and role in knowledge dissemination within the community.

Cluster 3 – "Liu-Zhang" Group

Led by Liu Y, Liu P, Liu D, Zhang X, and Li Y, this cluster exhibits strong internal collaboration, especially through work linking MCDM with fuzzy logic, heuristic methods, and complex decision-making models. Notably, Zhang X has a high PageRank (0.0356), while Liu Y plays a crucial intermediary role (betweenness: 60.52), positioning him as a central figure in the global research network.

Cluster 4 – "Akram-Deveci-Alcantud" Network

Dominated by Akram M, who has a high closeness centrality (0.0417) and a solid PageRank (0.0265), this cluster highlights his role as a key actor in international collaborations. Alongside Deveci M, Mahmood T, Al-Kenani AN, and Alcantud JCR, the group focuses on group decision-making, fuzzy sets, and the application of ELECTRE and VIKOR methods in practical domains such as healthcare and resource management.

Cluster 5 – "Moslem-Duleba"

This smaller cluster includes Moslem S and Duleba S, with relatively lower centrality values but recognizable contributions in applied studies, likely in the areas of urban planning and spatial analysis using MCDM techniques.

Clusters 6 and 7 – "Kumar-Agrawal" and "Salabun-Watrobski"

These clusters include authors like Kumar R, Agrawal A, Salabun W, Wieckowski J, and Kizielewicz B, with high closeness centrality (up to 1.0 for Cluster 6 and 0.333 for Cluster 7), but lower PageRank and betweenness values. This suggests that they are positioned in peripheral yet internally cohesive research groups, likely working on specialized methodologies within national or institutional research projects.

The network analysis reveals that the MCDM research community is structured around clearly defined centers of influence and strong collaborative links, with key hubs connecting different knowledge clusters. Authors with high betweenness centrality play a critical role in knowledge transfer across groups, while those with high PageRank values indicate greater global visibility and impact on research directions.

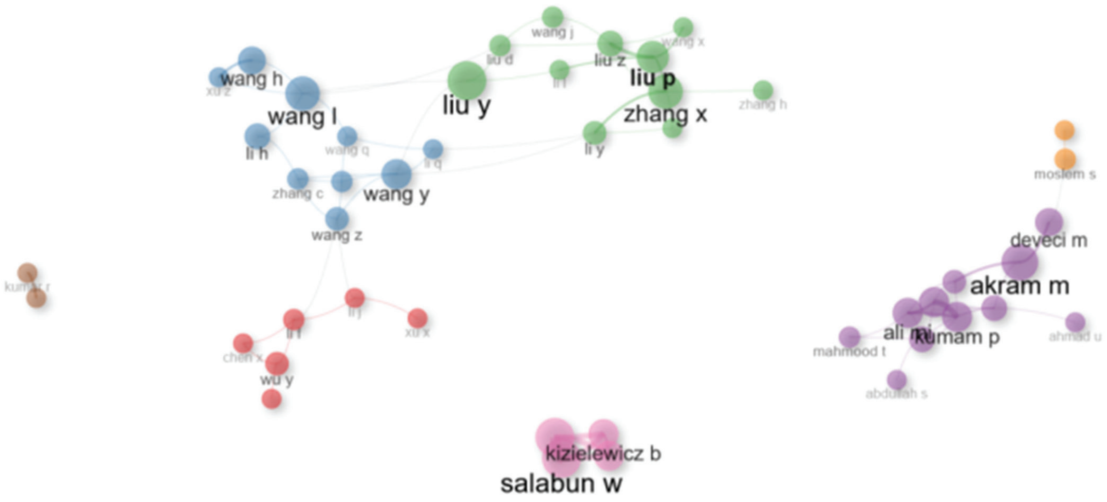


Fig. 8. Collaboration Among Authors and Institutions

5. DISCUSSION

The discussion of recent findings in the MCDM field reveals several important trends and insights that shed light on the dynamics of scientific activity during the period from 2019 to mid-2025. Quantitative data on publication output indicate steady growth in research interest, with peaks in 2021 and 2024, and slight declines in 2020 and 2023. Notably, even in the first half of 2025, there is evident research activity with 17 published papers, suggesting that the current year will also be productive. This trend shows that the MCDM domain remains highly relevant despite global challenges such as the COVID-19 pandemic, economic uncertainty, and shifts in research priorities.

Citation analysis further confirms the importance of specific authors and publications. Akram M stands out with the most cited paper from 2019 (172 citations), while Moslem S demonstrates an exceptionally high citation rate (42.5 citations per year) for his 2024 publication and holds the highest normalized citation value (18.14), despite the short time since publication. These findings confirm that high research impact can be achieved in a short time when the topics are innovative and practically relevant. The cited works span diverse applications of MCDM approaches from healthcare, energy efficiency, and urban planning to soft computing systems and intelligent platforms, highlighting the transdisciplinary nature of the methodology.

In terms of research topics, the analysis of key terms reveals a shift in researchers' focus over time from classical methods such as AHP and VIKOR toward extended models, complex aggregation operators, and strategies for ranking, criteria weighting, and option selection. Dominant terms like model, decision-making, and selection confirm the practical orientation of research toward the development of methodological frameworks for solving real-world decision problems. Newer terms like priorities and multicriteria decision-making, especially prevalent during 2023–2024, reflect a growing need to formalize decision hierarchies in increasingly complex systems.

Similar conclusions are supported by the analysis of key institutions. KMUTT, National Defense University, and Sichuan University emerge as leading research institutions, each with 11 publications. Their top rankings suggest systemic support for decision-making research and well-organized research teams. Other highly active institutions include the University of the Punjab, Islamic Azad University, and University of Salamanca, highlighting global coverage and collaboration in this scientific domain.

Additional insights into collaboration are provided by the network analysis of authors and institutions, which identified key collaboration clusters. For instance, the "Wang–Li–Zhang" cluster demonstrates strong internal connectivity and a high degree of centrality, enabling effective knowledge transfer within the network. Wang Y shows the highest betweenness centrality (124.46), positioning him as a "bridge" between different research groups. Akram M, in a separate cluster, also has a high closeness centrality and PageRank, confirming his role as a central figure in the global MCDM network. The presence of authors with high local centrality (e.g., Moslem S, Zhang X, Liu D) points to highly influential micro-clusters generating specialized knowledge.

This comprehensive analysis demonstrates that the MCDM field is dynamic and expanding, with stable growth in publication volume, high citation levels for key works, and increasingly diverse geographic and thematic coverage. Despite fluctuations caused by global events, it is evident that MCDM methods remain essential tools for solving complex problems in computer science and beyond.

For future research, it is recommended to:

- continue monitoring normalized citation scores of newer works;
- identify emerging topics through trend analysis of key terms;

- conduct expanded network analyses with a focus on international projects and co-authorship networks.

Additionally, integrating qualitative approaches, such as content analysis and assessments of methodological quality, could complement quantitative findings and contribute to a deeper understanding of the impact and relevance of MCDM research.

6. CONCLUSIONS

This bibliometric analysis provides a comprehensive overview of research activity in the field of Multi-Criteria Decision Making (MCDM) in computer science from 2019 to mid-2025. Based on the analysis of 302 publications extracted from the Web of Science database, key trends, authors, institutions, research topics, and collaboration networks shaping the field have been identified. The total number of publications indicates a steady and growing interest from the research community, with notable peaks in 2021 and 2024, while preliminary data for 2025 already demonstrate continued productivity. This quantitative trend reinforces the increasing use of MCDM methods in solving complex problems, especially in areas such as artificial intelligence, resource optimization, urban planning, and information security.

The citation analysis highlights the most influential papers and authors, notably Akram M, Moslem S, and Liu D, whose works combine classical MCDM techniques with advanced approaches such as fuzzy sets, group decision-making, and hybrid models. Papers published in 2023 and 2024 are already achieving high citation rates, suggesting rapid recognition of quality and relevance in recent research. The most frequently studied themes include terms such as model, decision-making, selection, aggregation operators, AHP, and ranking, reflecting a focus on practical applications and algorithmic frameworks for complex system evaluation. The rising use of terms like multicriteria decision-making and priorities in the last two years reflects a deepening of both theoretical and operational aspects of the field.

Key institutions KMUTT, National Defense University, Sichuan University, University of the Punjab, and Islamic Azad University, emerge as regional centers of expertise and collaboration. Network analysis further illuminates the structure of academic cooperation, with authors such as Wang Y, Zhang X, and Akram M occupying central positions within interconnected clusters.

The findings of this study not only confirm the steady growth of the MCDM field but also point to the key contributors, thematic directions, and institutional hubs that are likely to shape its future development. This analysis serves as a reference point for researchers and institutions aiming to position themselves within the global MCDM community, and as a foundation for strategic planning in scientific projects and international collaborations.

6.1. SIGNIFICANCE AND SCIENTIFIC CONTRIBUTION

The significance of this study lies in its ability to map the entire research structure of MCDM methods through quantitative indicators. The analysis highlights the most active authors, most cited papers, key institutions, and leading journals, offering a valuable tool for researchers seeking to understand thematic and network flows in the field. The work also contributes to the identification of dominant thematic trends, including AHP, VIKOR, fuzzy sets, aggregation operators, and alternative evaluation.

Beyond academic value, the results offer practical insights for researchers and decision-makers, helping them identify reliable sources of knowledge, high-potential research niches, and valuable collaborators. In this way, the study not only reflects the current landscape but also encourages strategic planning, resource optimization, and increased international visibility for both domestic and regional scholars.

6.2. RESEARCH LIMITATIONS

Despite its comprehensive approach, this study has several methodological limitations. The analysis relies solely on the Web of Science database, which may exclude important contributions indexed in Scopus, Google Scholar, or Dimensions. Additionally, data for 2025 covers only the first half of the year, making results for this period incomparable to full-year data from previous years.

The study is predominantly quantitative, lacking a deeper qualitative evaluation of the most cited papers, which could enhance the understanding of their scientific contributions and methodological rigor. Moreover, citation normalization does not account for disciplinary differences in citation behavior, which may impact the objectivity of comparisons between authors from different domains.

6.3. RECOMMENDATIONS FOR FUTURE RESEARCH

Future studies should consider incorporating data from multiple databases to gain a more comprehensive view of global scientific output. Combining quantitative bibliometrics with qualitative content analysis would provide deeper insights into the impact and value of the most cited works. Researchers are also encouraged to follow emerging interdisciplinary trends, such as the application of MCDM in AI, cybersecurity, energy efficiency, and smart cities.

Time-series analyses of keyword trends and thematic shifts can help detect new research niches early. Particular attention should also be given to network dynamics to identify authors with key intermediary roles in connecting different research communities. Lastly, fostering international and interdisciplinary collaboration remains one of the most critical factors for the continued growth and evolution of the MCDM field.

ACKNOWLEDGEMENTS

This paper was created as part of the project "*Multi-Criteria Analysis Modeling for Decision Optimization in Computer Science,*" Project No. 1760.

REFERENCES

[1] P. Brauner et al. "A computer science perspective on digital transformation in production", ACM Transactions on Internet of Things, Vol. 3, No. 2, 2022, pp. 1-32.

[2] J. C. Ascough II et al. "Future research challenges for incorporation of uncertainty in environmental and ecological decision-making", Ecological Modelling, Vol. 219, No. 3-4, 2008, pp. 383-399.

[3] P. P. Bonissone, R. Subbu, J. Lizzi, "Multicriteria decision making (MCDM): A framework for research and applications", IEEE Computational Intelligence Magazine, Vol. 4, No. 3, 2009, pp. 48-61.

[4] R. Kumar, "A comprehensive review of MCDM methods, applications, and emerging trends", Decision Making Advances, Vol. 3, No. 1, 2025, pp. 185-199.

[5] M. Andronie et al. "Artificial intelligence-based decision-making algorithms, internet of things sensing networks, and deep learning-assisted smart process management in cyber-physical production systems", Electronics, Vol. 10, No. 20, 2021, p. 2497.

[6] N. Rane, A. Achari, S. Choudhary, "Multi-criteria decision-making (MCDM) as a powerful tool for sustainable development: Effective applications of AHP, FAHP, TOPSIS, ELECTRE, and VIKOR in sustainability", International Journal of Modern Research in Engineering and Technology, Vol. 5, No. 4, 2023, pp. 2654-2670.

[7] R. Statnikov et al. "Multicriteria analysis tools in real-life problems", Computers & Mathematics with Applications, Vol. 52, No. 1-2, 2006, pp. 1-32.

[8] S. K. Sahoo, S. S. Goswami, "A comprehensive review of multiple criteria decision-making (MCDM) methods: Advancements, applications, and future directions", Decision Making Advances, Vol. 1, No. 1, 2023, pp. 25-48.

[9] B. D. Ghorbani, "Bibliometrix: Science mapping analysis with R Biblioshiny based on Web of Science in applied linguistics", A Scientometrics Research Perspective in Applied Linguistics, Springer Nature, 2024, pp. 197-234.

[10] M. Yazdi et al. "Navigating the power of artificial intelligence in risk management: A comparative analysis", Safety, Vol. 10, No. 2, 2024, p. 42.

[11] G. Hodosi, E. Sule, T. Bodis, "Multi-criteria decision making: A comparative analysis", Proceedings of the 103rd International Scientific Conference Economic and Social Development, Varaždin, Croatia, 21-22 November 2023.

[12] K. Jaukovic Jocic et al. "A novel integrated PIPRECIA-interval-valued triangular fuzzy ARAS model: E-learning course selection", Symmetry, Vol. 12, No. 6, 2020, p. 928.

[13] E. K. Zavadskas, Z. Turskis, "Multiple criteria decision making (MCDM) methods in economics: An overview", Technological and Economic Development of Economy, Vol. 17, No. 2, 2011, pp. 397-427.

[14] P. Chowdhury, S. K. Paul, "Applications of MCDM methods in research on corporate sustainability: A systematic literature review", Management of Environmental Quality, Vol. 31, No. 2, 2020, pp. 385-405.

[15] M. Aruldoss, T. M. Lakshmi, V. P. Venkatesan, "A survey on multi-criteria decision making methods and its applications", American Journal of Information Systems, Vol. 1, No. 1, 2013, pp. 31-43.

[16] G. P. Bhole, T. Deshmukh, "Multi-criteria decision making (MCDM) methods and its applications", International Journal for Research in Applied Science and Engineering Technology, Vol. 6, No. 5, 2018, pp. 899-915.

[17] T. L. Saaty, "The analytic hierarchy process (AHP)", Journal of the Operational Research Society, Vol. 41, No. 11, 1980, pp. 1073-1076.

[18] T. L. Saaty, "A scaling method for priorities in hierarchical structures", Journal of Mathematical Psychology, Vol. 15, No. 3, 1977, pp. 234-281.

[19] E. Albayrak, Y. C. Erensal, "Using analytic hierarchy process (AHP) to improve human performance: An application of multiple criteria decision-making problem", Journal of Intelligent Manufacturing, Vol. 15, 2004, pp. 491-503.

[20] D. Stanujkic et al. "The use of the pivot pairwise relative criteria importance assessment method for determining the weights of criteria", Romanian Journal of Economic Forecasting, Vol. 10, No. 4, 2017, pp. 116-133.

[21] M. Amudha et al. "A study on TOPSIS MCDM techniques and its application", Data Analytics and Artificial Intelligence, Vol. 1, No. 1, 2021, pp. 9-14.

[22] G. H. Tzeng, J. J. Huang, "Multiple Attribute Decision Making: Methods and Applications", CRC Press, 2011.

[23] S. Opricovic, G.-H. Tzeng, "Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS", European Journal of Operational Research, Vol. 156, No. 2, 2004, pp. 445-455.

[24] J. Figueira et al. "ELECTRE methods", Multiple Criteria Decision Analysis: State of the Art Surveys, Springer, 2005, pp. 133-153.

[25] B. Roy, "Classement et choix en présence de points de vue multiples", Revue Française D'automatique, D'informatique et de Recherche Opérationnelle, Vol. 2, No. 8, 1968, pp. 57-75.

[26] J. R. Figueira et al. "An overview of ELECTRE methods and their recent extensions", Journal of Multi-Criteria Decision Analysis, Vol. 20, No. 1-2, 2013, pp. 61-85.

[27] J. J. Thakkar, "ViseKriterijumska optimizacija i kompromisno rešenje (VIKOR)", Multi-Criteria Decision Making, Springer, 2021, pp. 129-138.

[28] N. I. Jaini, S. V. Utyuzhnikov, "A fuzzy trade-off ranking method for multi-criteria decision-making", Axioms, Vol. 7, No. 1, 2017, p. 1.

[29] V. Keršulienė, E. K. Zavadskas, Z. Turskis, "Selection of rational dispute resolution method by applying new step-wise weight assessment ratio analysis (SWARA)", Journal of Business Economics and Management, Vol. 11, No. 2, 2010, pp. 243-258.

[30] S. H. Zolfani, P. Chatterjee, "Comparative evaluation of sustainable design based on step-wise weight assessment ratio analysis (SWARA) and best worst method (BWM): A perspective on household furnishing materials", Symmetry, Vol. 11, No. 1, 2019, p. 74.

[31] S. H. Zolfani, J. Saparauskas, "New application of SWARA method in prioritizing sustainability assessment indicators of energy system", Engineering Economics, Vol. 24, No. 5, 2013, pp. 408-414.

[32] J. Nyulas et al. "Twenty-five years of scientific production on geoparks from the perspective of bibliometric analysis using PRISMA", Sustainability, Vol. 17, No. 5, 2025, p. 2218.

[33] Q.-H. Vuong et al. "The status of educational sciences in Vietnam: A bibliometric analysis from Clarivate Web of Science database between 1991 and 2018", Scientometrics, Vol. 122, No. 2, 2020, pp. 837-860.

[34] D. Liu, Y. Liu, L. Wang, "Distance measure for Fermatean fuzzy linguistic term sets based on linguistic scale function: An illustration of the TODIM and TOPSIS methods", International Journal of Intelligent Systems, Vol. 34, No. 11, 2019, pp. 2807-2834.

[35] M. Akram, U. Noreen, M. Deveci, "Enhanced ELECTRE II method with 2-tuple linguistic m-polar fuzzy sets for multi-criteria group decision making", Expert Systems with Applications, Vol. 213, 2023, p. 119237.

INTERNATIONAL JOURNAL OF ELECTRICAL AND COMPUTER ENGINEERING SYSTEMS

Published by Faculty of Electrical Engineering, Computer Science and Information Technology Osijek,
Josip Juraj Strossmayer University of Osijek, Croatia.

About this Journal

The International Journal of Electrical and Computer Engineering Systems publishes original research in the form of full papers, case studies, reviews and surveys. It covers theory and application of electrical and computer engineering, synergy of computer systems and computational methods with electrical and electronic systems, as well as interdisciplinary research.

Topics of interest include, but are not limited to:

- Power systems
- Renewable electricity production
- Power electronics
- Electrical drives
- Industrial electronics
- Communication systems
- Advanced modulation techniques
- RFID devices and systems
- Signal and data processing
- Image processing
- Multimedia systems
- Microelectronics
- Instrumentation and measurement
- Control systems
- Robotics
- Modeling and simulation
- Modern computer architectures
- Computer networks
- Embedded systems
- High-performance computing
- Parallel and distributed computer systems
- Human-computer systems
- Intelligent systems
- Multi-agent and holonic systems
- Real-time systems
- Software engineering
- Internet and web applications and systems
- Applications of computer systems in engineering and related disciplines
- Mathematical models of engineering systems
- Engineering management
- Engineering education

Paper Submission

Authors are invited to submit original, unpublished research papers that are not being considered by another journal or any other publisher. Manuscripts must be submitted in doc, docx, rtf or pdf format, and limited to 30 one-column double-spaced pages. All figures and tables must be cited and placed in the body of the paper. Provide contact information of all authors and designate the corresponding author who should submit the manuscript to https://ijeces.ferit.hr. The corresponding author is responsible for ensuring that the article's publication has been approved by all coauthors and by the institutions of the authors if required. All enquiries concerning the publication of accepted papers should be sent to ijeces@ferit.hr.

The following information should be included in the submission:

- paper title;
- full name of each author;
- full institutional mailing addresses;
- e-mail addresses of each author;
- abstract (should be self-contained and not exceed 150 words). Introduction should have no subheadings;
- manuscript should contain one to five alphabetically ordered keywords;
- all abbreviations used in the manuscript should be explained by first appearance;
- all acknowledgments should be included at the end of the paper:
- authors are responsible for ensuring that the information in each reference is complete and accurate. All references must be numbered consecutively and citations of references in text should be identified using numbers in square brackets. All references should be cited within the text;
- each figure should be integrated in the text and cited in a consecutive order. Upon acceptance of the paper, each figure should be of high quality in one of the following formats: EPS, WMF, BMP and TIFF;
- corrected proofs must be returned to the publisher within 7 days of receipt.

Peer Review

All manuscripts are subject to peer review and must meet academic standards. Submissions will be first considered by an editor-in-chief and if not rejected right away, then they will be reviewed by anonymous reviewers. The submitting author will be asked to provide the names of 5 proposed reviewers including their e-mail addresses. The proposed reviewers should be in the research field of the manuscript. They should not be affiliated to the same institution of the manuscript author(s) and should not have had any collaboration with any of the authors during the last 3 years.

Author Benefits

The corresponding author will be provided with a .pdf file of the article or alternatively one hardcopy of the journal free of charge.

Units of Measurement

Units of measurement should be presented simply and concisely using System International (SI) units.

Bibliographic Information

Commenced in 2010.
ISSN: 1847-6996
e-ISSN: 1847-7003

Published: semiannually

Copyright

Authors of the International Journal of Electrical and Computer Engineering Systems must transfer copyright to the publisher in written form.

Subscription Information

The annual subscription rate is 50€ for individuals, 25€ for students and 150€ for libraries.

Postal Address

Faculty of Electrical Engineering,
Computer Science and Information Technology Osijek,
Josip Juraj Strossmayer University of Osijek, Croatia
Kneza Trpimira 2b
31000 Osijek, Croatia

IJECES Copyright Transfer Form

(Please, read this carefully)

This form is intended for all accepted material submitted to the IJECES journal and must accompany any such material before publication.

TITLE OF ARTICLE (hereinafter referred to as "the Work"):

COMPLETE LIST OF AUTHORS:

The undersigned hereby assigns to the IJECES all rights under copyright that may exist in and to the above Work, and any revised or expanded works submitted to the IJECES by the undersigned based on the Work. The undersigned hereby warrants that the Work is original and that he/she is the author of the complete Work and all incorporated parts of the Work. Otherwise he/she warrants that necessary permissions have been obtained for those parts of works originating from other authors or publishers.

Authors retain all proprietary rights in any process or procedure described in the Work. Authors may reproduce or authorize others to reproduce the Work or derivative works for the author's personal use or for company use, provided that the source and the IJECES copyright notice are indicated, the copies are not used in any way that implies IJECES endorsement of a product or service of any author, and the copies themselves are not offered for sale. In the case of a Work performed under a special government contract or grant, the IJECES recognizes that the government has royalty-free permission to reproduce all or portions of the Work, and to authorize others to do so, for official government purposes only, if the contract/grant so requires. For all uses not covered previously, authors must ask for permission from the IJECES to reproduce or authorize the reproduction of the Work or material extracted from the Work. Although authors are permitted to re-use all or portions of the Work in other works, this excludes granting third-party requests for reprinting, republishing, or other types of re-use. The IJECES must handle all such third-party requests. The IJECES distributes its publication by various means and media. It also abstracts and may translate its publications, and articles contained therein, for inclusion in various collections, databases and other publications. The IJECES publisher requires that the consent of the first-named author be sought as a condition to granting reprint or republication rights to others or for permitting use of a Work for promotion or marketing purposes. If you are employed and prepared the Work on a subject within the scope of your employment, the copyright in the Work belongs to your employer as a work-for-hire. In that case, the IJECES publisher assumes that when you sign this Form, you are authorized to do so by your employer and that your employer has consented to the transfer of copyright, to the representation and warranty of publication rights, and to all other terms and conditions of this Form. If such authorization and consent has not been given to you, an authorized representative of your employer should sign this Form as the Author.

Authors of IJECES journal articles and other material must ensure that their Work meets originality, authorship, author responsibilities and author misconduct requirements. It is the responsibility of the authors, not the IJECES publisher, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it.

- The undersigned represents that he/she has the authority to make and execute this assignment.
- For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.
- The undersigned agrees to indemnify and hold harmless the IJECES publisher from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.

______________________________ ______________________________

Author/Authorized Agent **Date**

CONTACT
International Journal of Electrical and Computer Engineering Systems (IJECES)
Faculty of Electrical Engineering, Computer Science and Information Technology Osijek
Josip Juraj Strossmayer University of Osijek
Kneza Trpimira 2b
31000 Osijek, Croatia
Phone: +38531224600,
Fax: +38531224605,
e-mail: ijeces@ferit.hr