Mitigating Insider Threats Using Zero Trust Architecture: A Behavioral Analytics Approach Using CERT r4.2

Md. Harun Or Rashid, Hossen Asiful Mustafa, Prottoy Saha

Abstract

Insider threats remain a dominant cybersecurity risk due to their exploitation of legitimate access privileges. This work presents a **Zero Trust Architecture (ZTA)-driven behavioral analytics framework** which was evaluated using the **CERT Insider Threat Dataset r4.2**. User behavior is modeled probabilistically, and insider threat detection is formulated as a **risk-based decision problem** by combining anomaly scores, behavioral deviation and contextual risk. The framework enforces continuous verification through dynamic trust evaluation. Experimental results on CERT r4.2 demonstrate a high detection accuracy (99.42%), recall (96.4%) and false positive reduction (0.46%) compared to traditional baselines, which confirm the effectiveness of the integration of the Zero Trust principles with behavioral intelligence.

Background & Motivation

Problem Context

Insider threats originate from authorized users

Traditional systems rely on:

- Static authentication
- Perimeter-based trust

Mathematical Limitation

Traditional model:

$$T(u) = constant$$

No temporal or behavioral dynamics

Motivation

Define dynamic trust:

$$T(u,t) = P(benign \mid S_u^{(t)})$$

Where $S_u^{(t)} = \{login, email, file\ access, download\}$
$= user\ activity\ sequence$

Enables:

(i) Continuous monitoring, and **(ii)** Context-aware decision making

Dataset & Experimental Setup

Dataset

- Source: CERT Insider Threat Dataset r4.2
- Users: ~10000 synthetic employees
- Time span: multiple months of activity
- Total records used: 450,000 user activity instances

Data Types	Labeling	Data Split
▪ Logon/logoff events ▪ Email communication ▪ File access ▪ HTTP activity	▪ Normal behavior → 0 ▪ Insider threat scenarios → 1	▪ Training: 70% ▪ Testing: 30%

Proposed Idea and Methodology

1. Behavioral Modeling

User actions:

$$a_t \sim P(a_t \mid H_{t-1})$$

2. Feature Engineering

From CERT logs:

Source	Feature	Short Description	Feature Type
Logon	Login Time	User login hour	Temporal
Logon	Deviation	Off-hours behavior	Behavioral
Email	Frequency	Emails sent count	Behavioral
Email	External	Outside communication	Contextual
File	Access Count	File operations	Behavioral
File	Sensitive	Critical file access	Contextual
HTTP	Activity	Web request volume	Behavioral
HTTP	Suspicious	Unusual domains	Contextual

3. Anomaly Score

$$A(u,t) = -log\ P(a_t \mid H_{t-1})$$

4. Behavioral Deviation

$$D(u,t) = distance\ from\ baseline\ behavior$$

5. Contextual Risk

$$C(u,t) = f(device, location, resource)$$

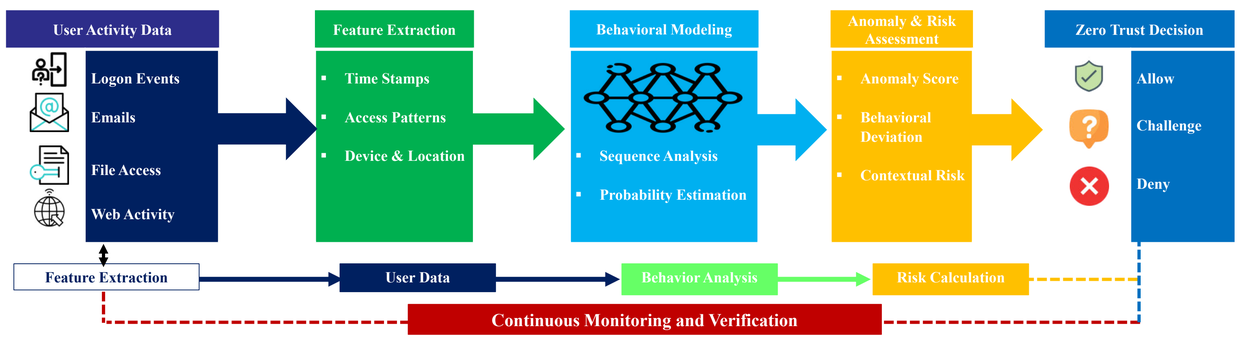
6. Risk Model

$$R(u,t) = \alpha A(u,t) + \beta D(u,t) + \gamma C(u,t)$$

7. Zero Trust Decision

$$Access = \begin{cases} Allow\ if & R(u,t) < \tau \\ Challenge\ if & \tau \le R(u,t) < \tau' \\ Deny\ if & R(u,t) \ge \tau' \end{cases}$$

Workflow



Inner Sight: Brief Overview

- How unusual is this behavior? → ANOMALY
- How far from normal? → DEVIATION
- Is the context risky? → CONTEXT
- Combine → RISK SCORE
- Decide → ALLOW / CHALLENGE / DENY

Results

Confusion Matrix (Test Set)

	Predicted Normal (0)	Predicted Attack (1)
Actual Normal (0)	TN = 430022	FP = 1974
Actual Attack (1)	FN = 650	TP = 17354

(Classification performed using two decision threshold of $\tau = 2.5$ & $\tau' = 4.0$)

Metric Calculation

$Accuracy$: $(TP + TN) / Total = (17354 + 430022) / 10000 = 99.42\%$
$Precision$: $TP / (TP + FP) = 17354 / (17354 + 1974) = 89.8\%$
$Recall$: $TP / (TP + FN) = 17354 / (17354 + 650) = 96.4\%$
$False\ Positive\ Rate$: $FP / (FP + TN) = 1974 / (1974 + 430022) = 0.46\%$

Metric	Traditional System (BASED ON PREVIOUS STUDIES)	Proposed System
Accuracy	78–82%	99.42%
Precision	70–75%	89.6%
Recall	65–70%	96.4%
FPR	15–20%	0.46%

Key Findings:

- High **attack detection performance (Recall: 96.4%)**
- Very low **false positive rate (0.46%)**, minimizing disruption to normal users
- High overall **accuracy (99.42%)**, demonstrating robust performance
- Effective identification of critical insider threat behaviors:
  - Data exfiltration
  - Privilege abuse
  - Lateral movement

Terminus: A Resilient Command-Line Shortcut System with Intelligent Path Recovery and Cloud-Aware Resolution

Sheikh Raisul Islam
Prottoy Saha

Abstract

Terminus is a command-line utility designed to provide fast and resilient access to files and folders using user-defined shortcuts. Unlike traditional systems, it introduces intelligent path recovery and a novel Google Drive mapper mechanism that reconstructs valid paths using stable folder IDs. By leveraging Google Drive's internal shortcut-target architecture and dynamically scanning multiple drive mounts, Terminus enables seamless access to numerous cloud directories across environments. This approach decouples logical file references from physical storage paths, significantly improving portability and reliability.

Background & Motivation

🔴 **Real-World Problems**

- Tiring Clicks to reach destination folder/file; Shortcuts/Quick Access overflows available spaces/desktop.
- Drive letters change frequently (Google Drive, USB, etc.)
- Setting up is into a new PC is tiresome even if using Cloud.
- Difficulty in accessing files of different shared google drives through desktop.

🎯 **Motivation**

- To build a system that: Adapts across environments
- Recovers broken paths automatically
- Works seamlessly with cloud storage systems

Existing Solutions & Market Gaps

Feature / Capability	OS Shortcuts	CLI Tools (e.g., Autojump, Zoxide)	Google Drive Interface	Alfred (Mac)	Terminus
Custom Shortcut Mapping	✅	❌ (auto-learn only)	❌	✅	✅
Works from Command Line	❌	✅	❌	⚠ Partial	✅
Handles Drive Letter Changes	❌	❌	❌	❌	✅
Multi-Drive Resolution (C–Z scan)	❌	❌	❌	❌	✅
Path Recovery Mechanism	❌	❌	❌	❌	✅
Cloud Path Awareness	❌	❌	✅	❌	✅
Google Drive Folder ID Usage 🚀	❌	❌	❌	❌	✅
Works Across Multiple Devices	❌	⚠ Partial	✅	❌	✅
Self-Healing Shortcuts 🚀	❌	❌	❌	❌	✅
Clipboard Integration	❌	❌	❌	✅	✅
Fuzzy Search Suggestions	❌	⚠ Partial	❌	✅	✅

Problem Statement & Innovation

Why Terminus?

- A user cannot experience different devices as a single consistent working environment.
- Even with one login, users cannot access shared folders of different cloud accounts.
- Navigation to deep nested path destinations without shortcuts enables unlimited quick access.

🟥 Identified Gap (Problem)	🟦 Innovation in Terminus (Solution)
Manual navigation is time-consuming	**Instant shortcut-based access + clipboard integration**
Device-dependent cloud file access – Paths differ across PC, laptop, environments	**Device-agnostic shortcut system** → Same shortcut works across all devices, "Any device feels like your own"
Cannot reliably access **multiple Google Drive folders**	**Scalable cloud access** → One login enables access to hundreds of drive directories.
Almost Impossible to save into a folder that is shared, not in the mounted Google Account	**Copy the ID through app and access them in window.**
No intelligent assistance in case of errors	**Fuzzy suggestion system** for quick recovery

Proposed Idea & Methodology

🔷 **Core Idea**

Self-healing shortcuts with multi-drive cloud path access through optional path reconstruction.

🔷 **Key Contribution:**

Cloud Drive Mapper.

Traditional Approach

❌ Uses fixed path: G:\My Drive\FolderName

Fails when: a) Drive changes (Different PC) b) Sync account changes

Terminus Approach

✅ Uses: Folder Name + Google Drive Folder ID

Reconstructs path dynamically:<Drive>:\.shortcut-targets-by-id\<FolderID>\<FolderName>\...

🔷 **Multi-Drive Resolution Engine:**

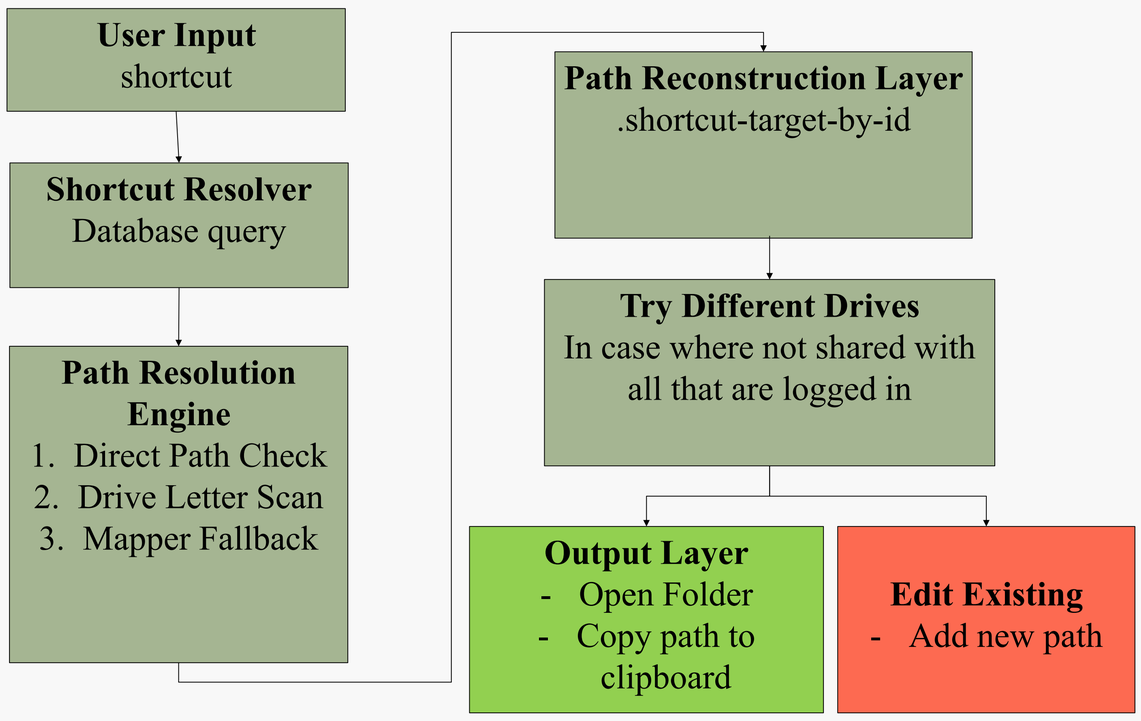
Iterates through all possible drives. Detects valid mount pointOpens correct path automatically

🔥 **INNOVATION:** Enables access to multiple Google Drives (even hundreds) using a single logged-in account — without knowing their actual mount locations

🔷 **Intelligent Path Recovery**

If original path fails: Try alternative drives + Use mapper reconstruction->Automatically restores access

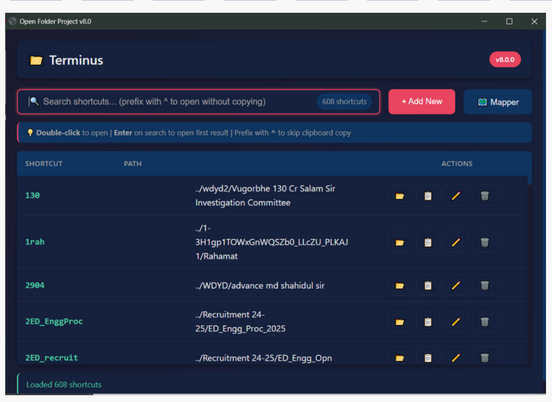
🔷 **Additional Features-** Fuzzy shortcut suggestions;
Clipboard integration, Edit Shortcut or Path.

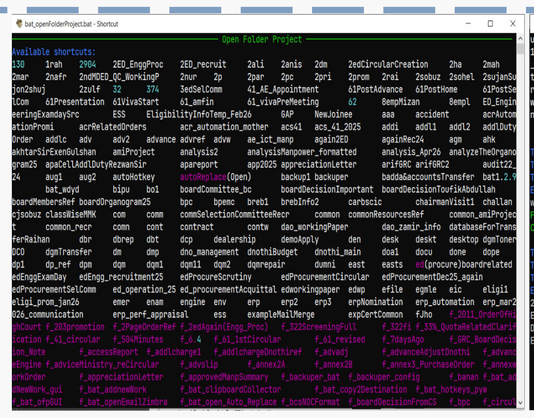


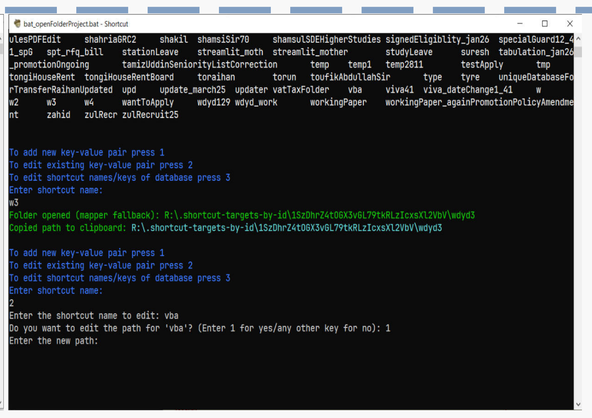
Future Scope

- ✅ Auto Path Detection (File/Folder)
- ✅ Auto Path Capture
- ✅ GUI (90% done)
- ✅ Cross-Device Sync (Already Achieved through Google Drive)
- ✅ Tag/Search System

Results







CNNMalNet: A CNN-RNN Hybrid Architecture for Obfuscated Malware Detection

Arnab Nath , Dr. Md. Saiful Islam

Abstract

Malware is becoming increasingly complex due to advanced obfuscation techniques such as polymorphism and metamorphism. Traditional signature-based detection methods fail to identify such evolving threats. This research proposes **CNNMalNet**, a hybrid deep learning model that integrates convolutional and recurrent neural networks to detect malware from both static and dynamic data sources. The model is evaluated on **EMBER 2018** and **CIC-MalMem-2022** datasets. Experimental results demonstrate that CNNMalNet achieves balanced and robust performance across both datasets while maintaining computational efficiency through feature reduction techniques.

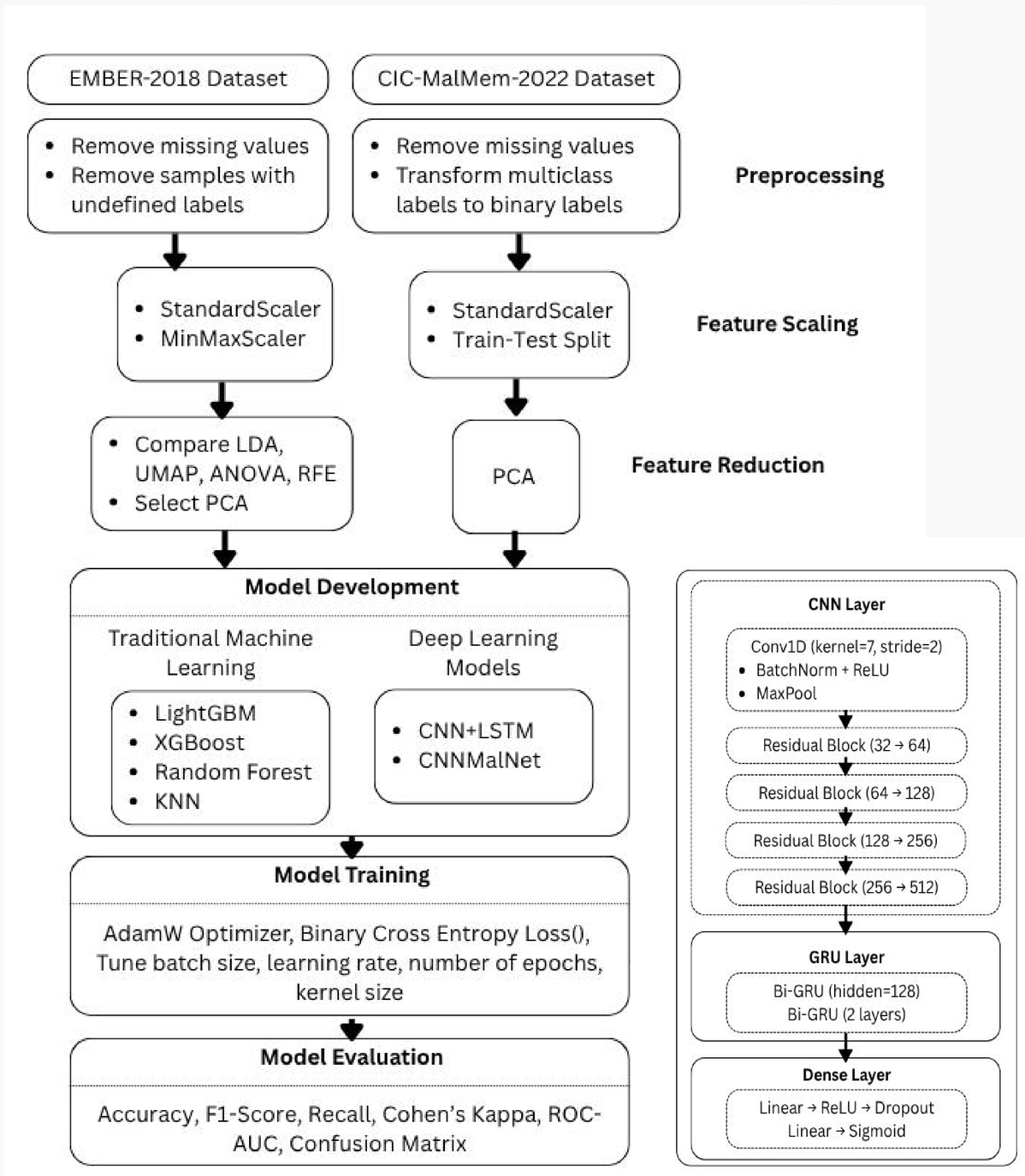
Background & Motivation

- Advanced malwares (Polymorphic and Metamorphic) are hard to detect.
- Metamorphic malware rewrites its code structure → **no fixed signature**.
- Signature-based detection is ineffective against evolving malware.
- Increasing need for **robust**, **adaptive** detection models.

Objectives

- Design a hybrid deep learning model (CNNMalNet)
- Detect malware using static-dynamic analysis
- Evaluate performance across multiple datasets
- Analyze impact of feature reduction techniques
- Compare with traditional machine learning models

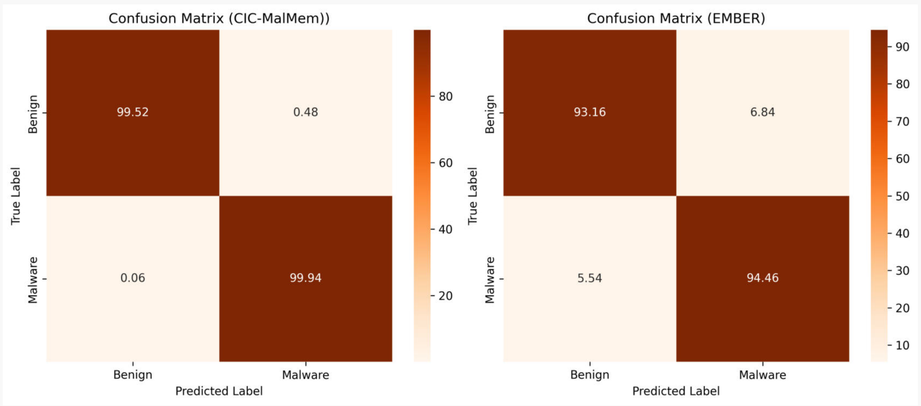
Proposed Idea and Methodology



Results

	EMBER				CIC-MalMem				
Methods	Accuracy	F1-score	Recall	Cohen Kappa (κ)	Accuracy	F1-score	Recall	Cohen Kappa (κ)	Params
LightGBM	0.9351	0.9366	0.9586	0.8703	1	1	1	1	12200
XGBoost	0.9278	0.9244	0.9506	0.8556	1	1	1	1	19844
Random Forest	0.9236	0.9243	0.9328	0.8473	1	1	1	1	992942
KNN	0.8823	0.8842	0.8899	0.7646	0.9866	0.9888	0.9899	0.9843	114336000
SVM	0.7854	0.8101	0.9126	0.5719	0.9735	0.9777	0.9801	0.9821	52682695
CNN+LSTM	0.8741	0.8762	0.8925	0.7481	0.9925	0.9962	0.9992	0.9912	139137
CNNMalNet	**0.9481**	**0.9487**	**0.9546**	**0.9162**	**0.9998**	**0.9997**	**0.9995**	**0.9995**	**2160000**

Methods	32	64	128	256	512	1024
PCA	0.9031	0.9073	**0.9277**	0.9255	0.9167	0.9117
LDA	0.7727	0.7963	0.8012	0.8244	0.8119	0.7998
UMAP	0.8020	0.8148	0.7858	0.7983	0.8174	0.7524
RFE	0.8516	0.8624	0.8734	0.8781	0.8637	0.8558
ANOVA	0.8927	0.9179	0.9264	0.9229	0.9088	0.9135



CNNMalNet achieves balanced accuracy across static and dynamic datasets. PCA improves efficiency without degrading performance. The model effectively detects obfuscated malware.

Conclusion: CNNMalNet delivers **robust, efficient detection** of advanced and metamorphic malware across both static and dynamic datasets.

LeafDet: A Lightweight and Interpretable Deep Learning Framework for Tomato Leaf Disease Detection

Vaskor Mostafa

Supervisor: Dr. Md. Rubaiyat Hossain Mondal

Abstract

LeafDet is a lightweight tomato leaf disease detection model based on the YOLOv8n framework, designed to overcome class imbalance, low interpretability, and limited generalization of existing models. A relatively balanced dataset, PlantTom (7,836 images; 8 disease classes), is introduced to improve fairness and robustness. The model integrates CBM, C2f, SPPF, ECA Attention, BiFPN, GSConv, VoVGSCSP, and Shuffle Attention, achieving 91.6% mAP@0.5 with only 2.69M parameters. LeafDet also supports real-time field deployment on a Raspberry Pi 5, enabling low cost, offline smart agriculture systems. Eigen CAM visualization provides interpretability for trustworthy predictions.

Background & Motivation

- Plant diseases cause up to 40% global crop loss, leading to major economic impact.
- Public datasets often have severe class imbalance, affecting evaluation reliability.
- Farmers require fast, accurate, low cost, interpretable AI solutions for early disease detection.
- Tomatoes are a globally important crop—early detection greatly reduces losses.

PlantTom Dataset

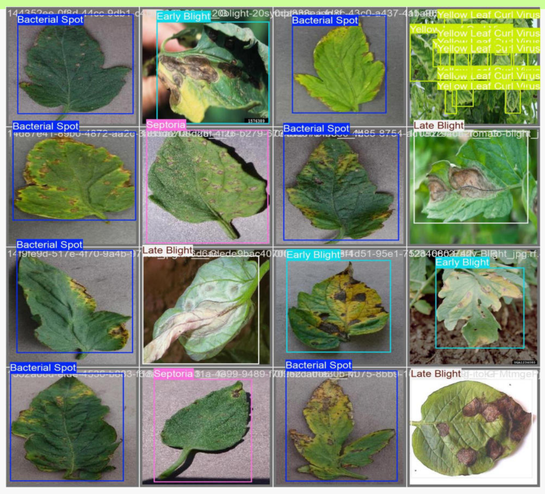


Fig 1: Sample Labeled Images

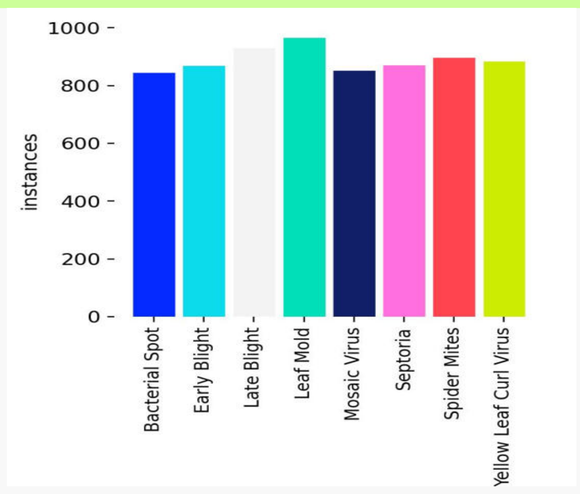


Fig 2: Class Distribution

Dataset Summary

- Images from multiple public datasets
- Contains 8 classes
- Applied augmentations (flip, brightness ±10%, noise injection)
- Final: 7,836 images

Dataset Split	No. of Images (Before Aug.)	No. of Images (After Aug.)
Training	3017	6034
Valid	1423	1423
Test	379	379
Total	4819	7836

Proposed Idea and Methodology

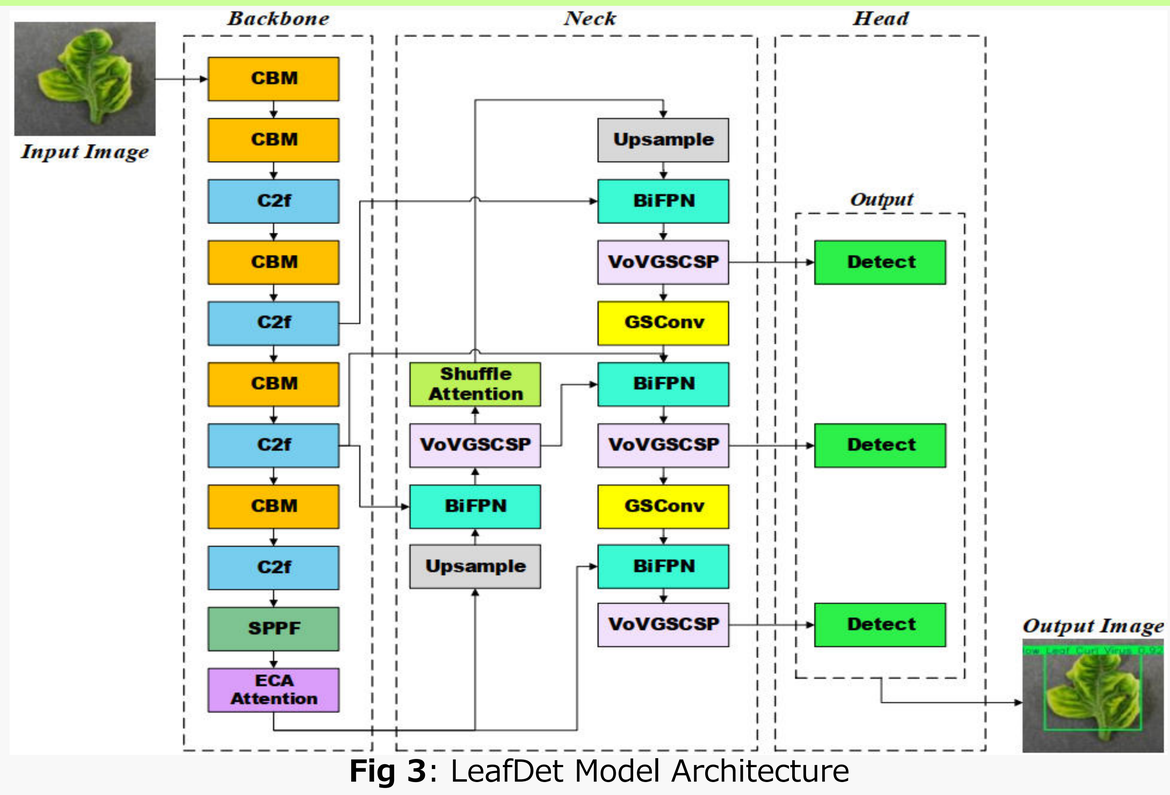


Fig 3: LeafDet Model Architecture

Enhancement Area	Module Name	Purpose
Backbone	CBM Block (Conv+BN+Mish)	Smoother gradients
	C2f	Efficient feature reuse
	SPPF	Multi scale feature aggregation
	ECA Attention	Lightweight channel attention
Neck	BiFPN	Bidirectional feature fusion
	VoVGSCSP	Lightweight CSP + GSConv
	GSConv	Reduced parameters
	Shuffle Attention	Spatial + channel attention

Loss Function & XAI

- **PIoUv2 loss** → improved object localization
- **Eigen-CAM** → interpretable feature attribution

EDGE Deployment

- **Raspberry Pi 5** → convert the .pt format into .onnx format for RPI 5 deployment

Results

Model	Parameters (M)	GFLOPS	Inference time (ms)	Model Size (MB)	mAP@0.5 (%)
RetinaNet	37.69	93.64	80.8	277	86.0
Faster R-CNN	41.48	89.41	87.2	315	84.1
YOLOv3-tiny	12.13	18.9	2.5	23.20	85.5
YOLOv5n	2.50	7.1	2.2	5.03	89.2
YOLOv6n	4.23	11.8	1.8	8.29	88.0
YOLOv8n	3.01	8.1	2.1	5.96	89.4
YOLOv9t	1.97	7.6	3.0	4.43	89.9
YOLOv10n	2.70	8.2	3.1	5.49	89.8
YOLOv11n	2.58	6.3	2.3	5.22	90.5
YOLOv12n	2.56	6.3	3.8	5.27	89.2
LeafDet (Proposed)	**2.69**	**7.3**	**2.4**	**5.44**	**91.6**

Results Summary

LeafDet achieves 91.6% mAP@0.5, surpassing the compared SOTA models, while Eigen-CAM visualizations confirm interpretable disease localization, and the model is also deployed on Raspberry Pi 5 for efficient edge inference.

Eigen-CAM Visualization

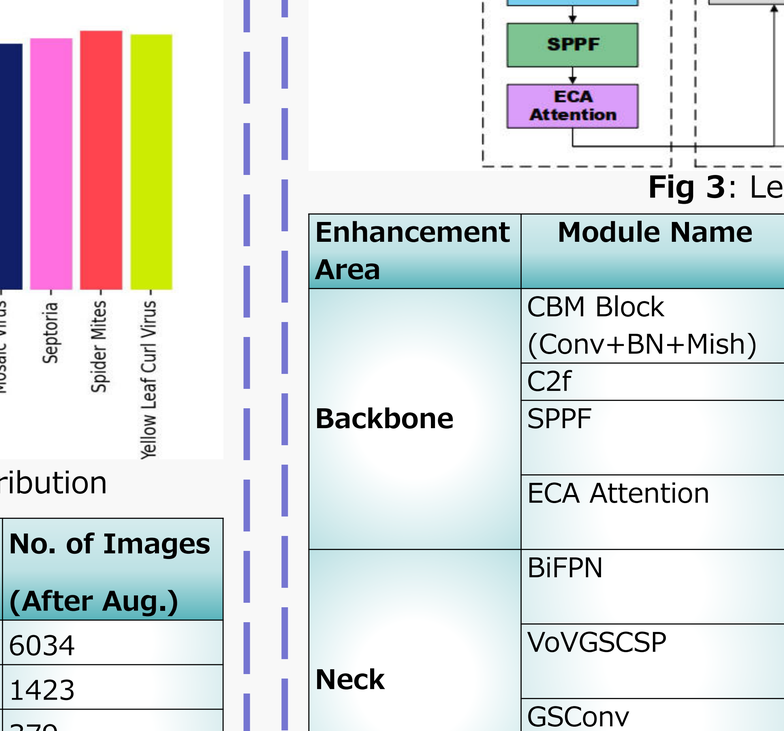


Fig 4: Eigen-CAM visualization

Raspberry Pi 5 Deployment (ONNX format)

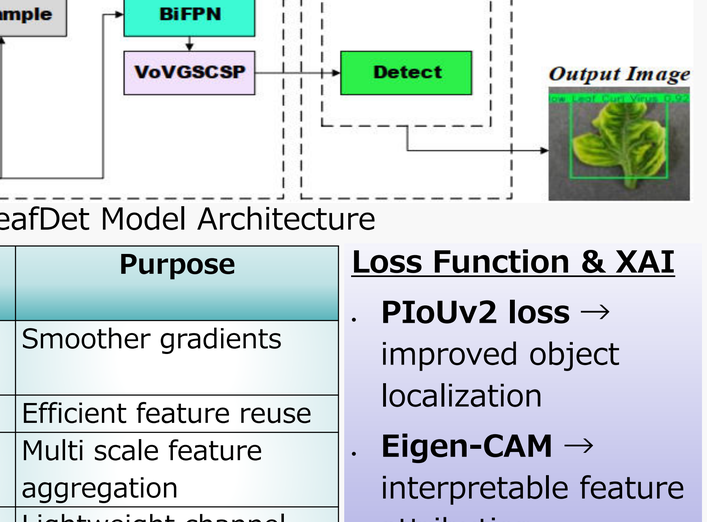


Fig 5: RPI 5 Experimental Setup

Metric	Platform 1 (Kaggle CPU Output)	Platform 2 (RPI 5 CPU Output)
Parameters (M)	2.69	2.69
Inference Latency (ms)	96.5	197.8
FPS	10.36	5.06
mAP@0.5 (%)	91.6	91.6

Institute of Information and Communication Technology (IICT)

https://iict.buet.ac.bd/

ML-Driven Analyte Classification Using a PCF-SPR Sensor

Mst Rokeya Khatun and Md. Saiful Islam

Abstract A classification-based machine learning (ML) framework is proposed for PCF-SPR sensors to directly identify analytes from spectral responses without explicit resonance wavelength extraction. Spectral data generated using COMSOL Multiphysics simulations are used to train and evaluate the model. The proposed approach achieves approximately 95% classification accuracy and an ROC-AUC of 0.996 using XGBoost. The method is validated on closely spaced ester analytes and offers a generalizable approach for advanced optical sensing applications.

Background

- Detection of closely spaced analytes is essential for safety and quality control in environmental monitoring, food safety, pharmaceutical production, and industrial processes.
- Conventional methods are accurate but costly, complex, and unsuitable for real-time, on-site monitoring.
- PCF-SPR sensors provide label-free, refractive index–based sensing
- ML in PCF-SPR sensors is mainly used for prediction and design optimization, not analyte identification

Motivation

- Enable direct analyte identification from spectral responses using data-driven ML models
- Eliminate manual resonance peak extraction
- Improve detection of closely spaced analytes
- Develop a robust and generalizable ML–PCF-SPR sensing framework for analyte identification

Proposed Idea and Methodology

✓Light–analyte interaction causes spectral changes

✓Spectral changes reflect refractive index variations

✓Spectral data used for supervised learning

✓ML enables automated sensing

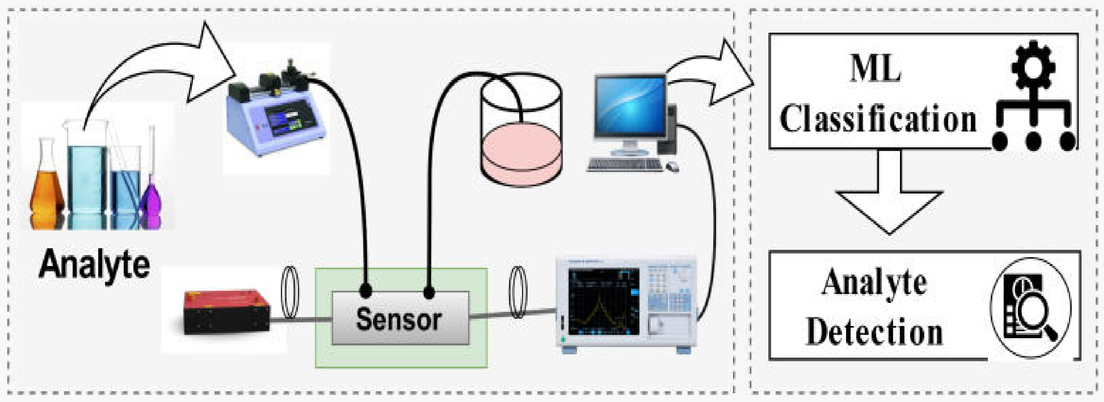


Fig. 1. ML–assisted PCF-SPR sensor working principle.

✓Effective wavelength window 0.55–0.85 μm

✓9,596 spectra samples

✓Features: n_eff, λ_peak, CL_peak

✓RI-based labels: Ethyl (1.360–1.380), Butyl (1.380–1.400), Others

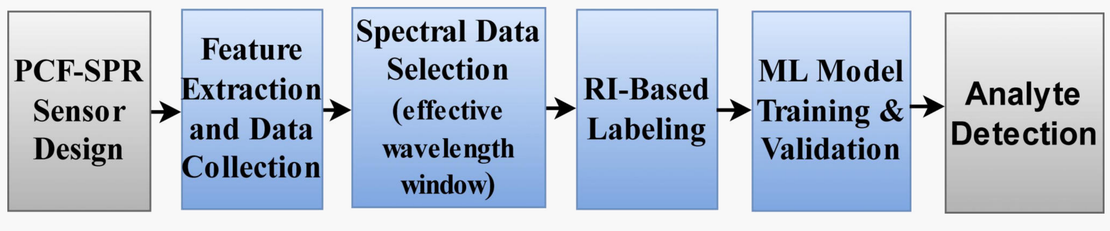


Fig. 2. ML Workflow for Analyte Classification.

Results

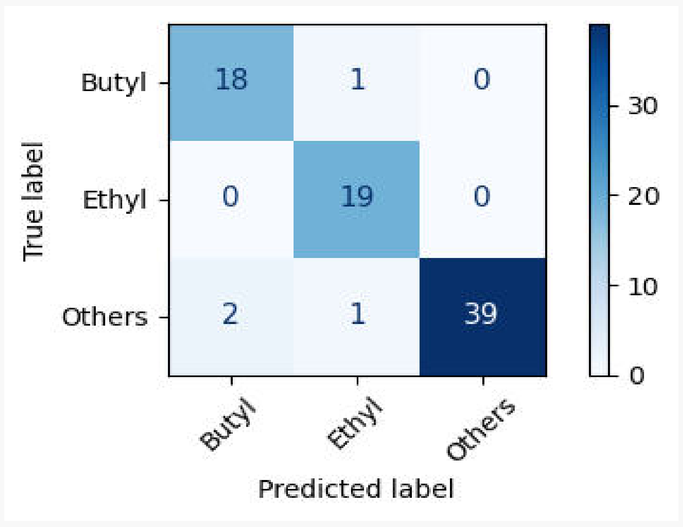


Fig. 3. Confusion matrix of the XGBoost classifier

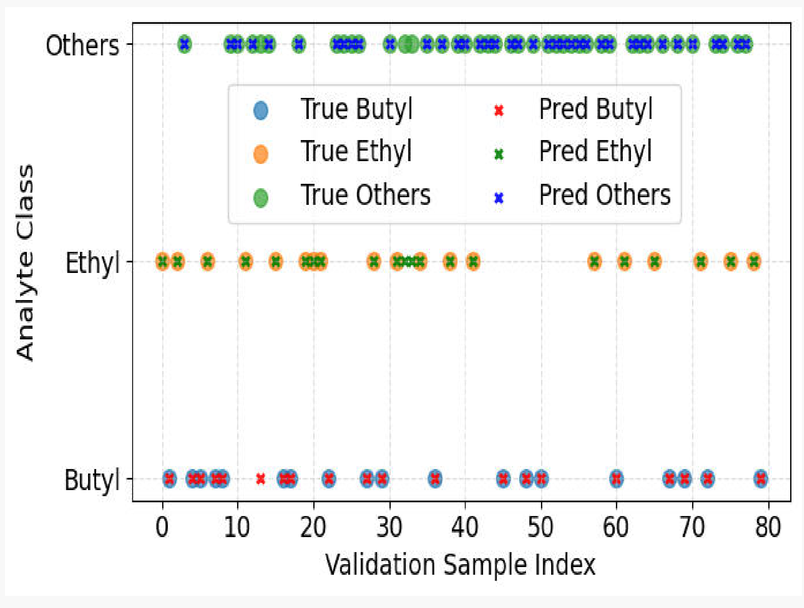


Fig. 4. Comparison of true and predicted analyte classes for validation using the XGBoost model.

Table: ML MODEL PERFORMANCE SUMMARY

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC
RF	0.875	0.867	0.882	0.871	0.981
CatBoost	0.914	0.904	0.912	0.907	0.987
XGBoost	0.950	0.935	0.959	0.945	0.996

➢Validation is based on simulation-generated data

➢The framework can be extended to experimental datasets

➢Future work includes real-time experimental validation of the proposed model

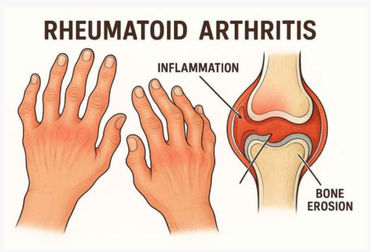
Identification of Common Potential Biomarkers in Rheumatoid Arthritis (RA) and Chronic Obstructive Pulmonary Disease (COPD) Using Bioinformatics and Machine Learning Approaches

Wahia Tasnim
Supervisor: Dr. Md. Rubaiyat Hossain Mondal

Abstract

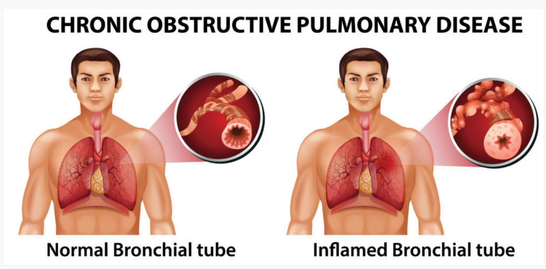
Chronic Obstructive Pulmonary Disease (COPD) and Rheumatoid Arthritis (RA) are the leading causes of illness and mortality globally. RA patients are more likely to acquire COPD, suggesting a clinical and biological link between the two conditions. However, the underlying molecular processes and common biomarkers of RA and COPD are still undiscovered. This research is aimed at discovering the common biomarkers between RA and COPD with the advancements of bioinformatics and Machine Learning approaches. The primary and validation analyses were performed using the microarray datasets from the NCBI-GEO database for this study. By performing the differential expression analysis, we discovered 90 common Differentially Expressed Genes (DEGs) be-tween RA and COPD. Further applying several bioinformatics and ML analyses, we have found four most promising genes from the common DEGs, namely ETS1, YY1, CREBP5,and GTF2H1. Further, the Receiver Operating Characteristic ROC curve and Nomogram analysis were used to validate these biomarkers. This research also identifies a list of possible drugs, Transcription Factors(TFs) and microRNAs (miRNAs) related to the biomarkers for physicians to make final recommendations. The identification of shared biomarkers using bioinformatics and machine learning techniques may lead to new opportunities for COPD and RA treatment and prevention.

Background and Motivation



- **RA** is a chronic **autoimmune condition** where the **immune system attacks healthy joint tissues**, leading to **pain, swelling, and stiffness,** especially in the hands and feet.

- **COPD** is a **progressive lung disease** that **causes breathing difficulties** due to airflow obstruction.



- **Recent studies** suggest a **clinical and molecular association between t**he two **diseases.**
- Most **existing studies** rely **on traditional statistical analyses** and **examine** each disease **independently.**
- Although both diseases shared strong molecular connection, the investigation of **shared molecular biomarkers** remains **limited and largely unexplored**.
- There is a clear need for an **integrated approach** to uncover **common genetic biomarkers** that may explain their potential connection.

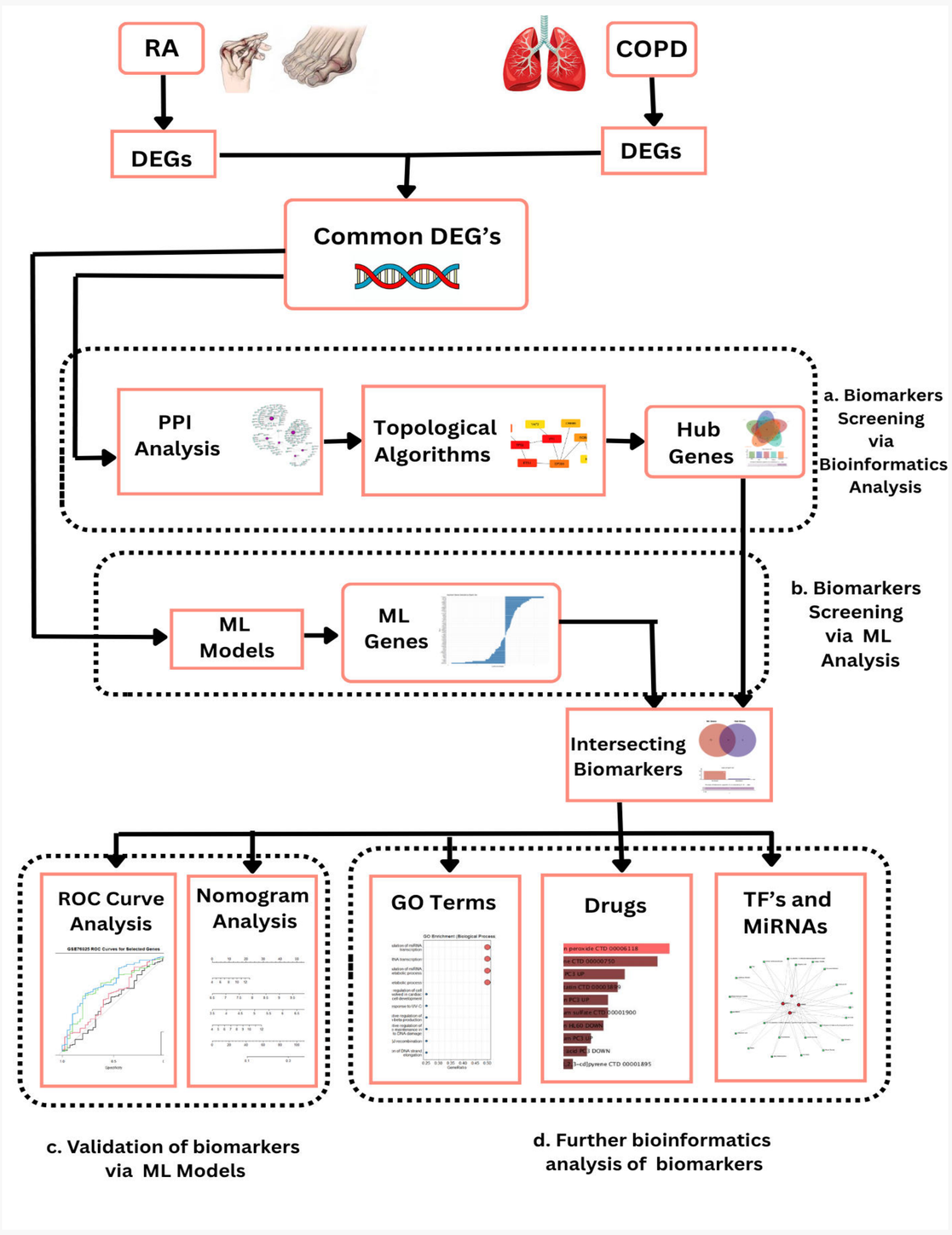
Development Tools

RStudio® Cytoscape 3.2 **NetworkAnalyst**

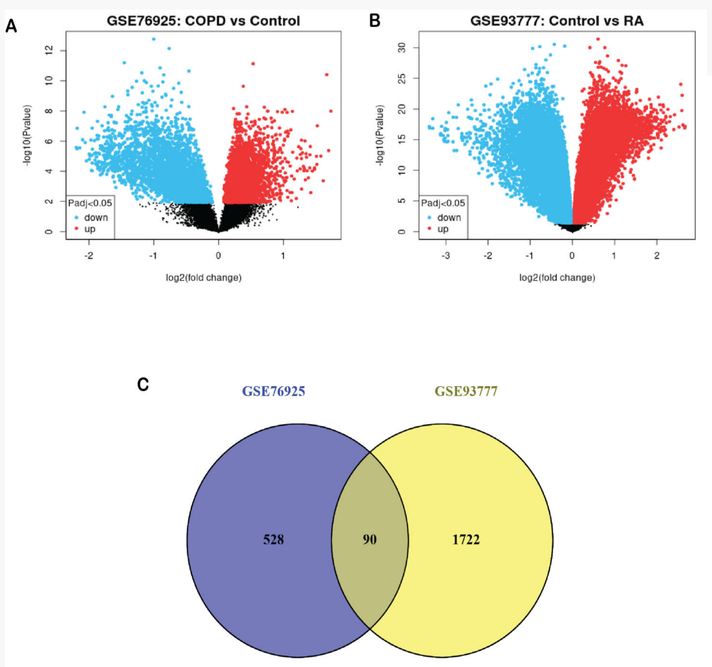
Research Contribution

- Identified common **potential biomarkers** via performing **several bioinformatics and ML analyses**
- Validation of biomarkers via ROC Curve Analyses
- Suggest possible drugs, Transcription Factors(TFs) and microRNAs (miRNAs) related to the biomarkers for physicians to make final recommendations.
- All of the analyses are done via **R programming.**

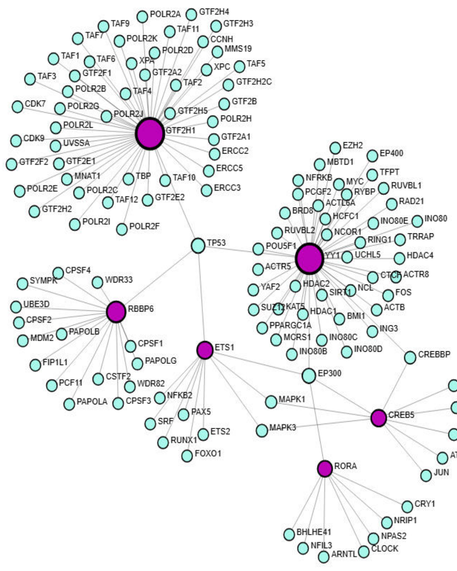
Proposed Methodology



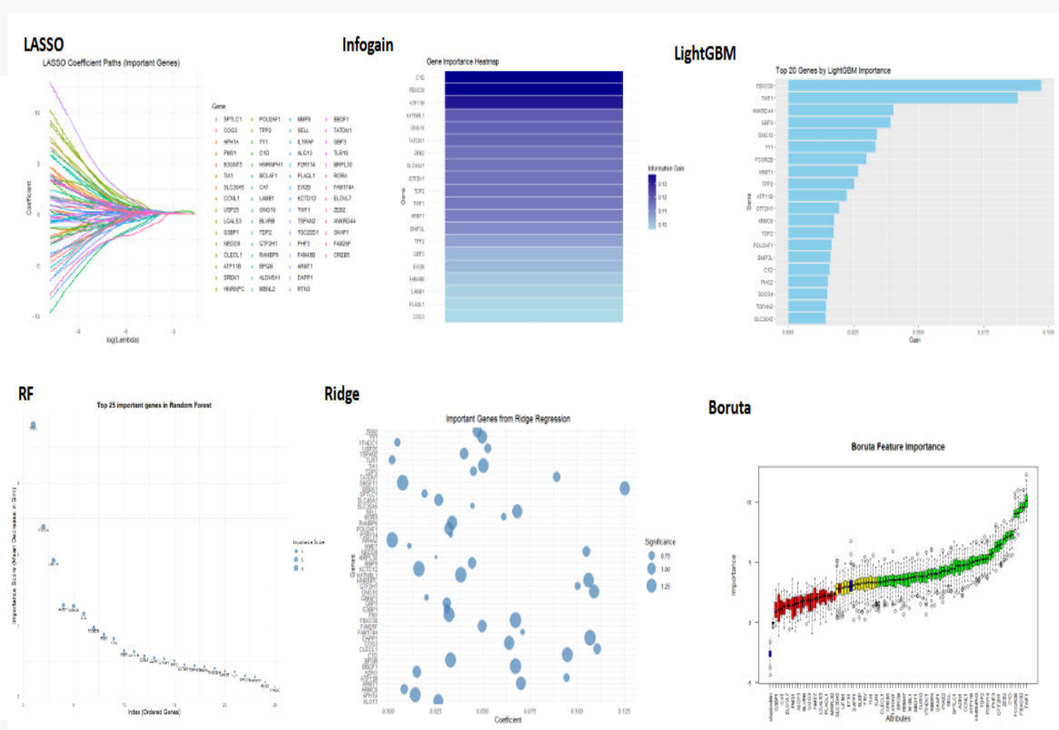
Results



DEG's Identification



PPI Analysis



ML Analysis

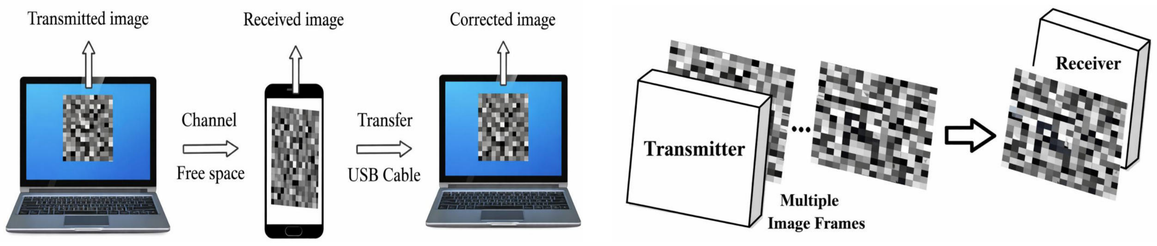
Conclusion

- In this study we have detect the common genes between RA and COPD using Bioinformatics and ML analyses.
- The differential gene expression analysis provided the significant DEGs in RA and COPD. Among these significant DEGs, common DEGs shared by both RA and COPD are used for further molecular analysis.
- From PPI and ML analysis potential genes were identified and validation of these genes were done by ROC curve and Nomogram analysis.
- Finally suggest possible drugs, Transcription Factors(TFs) and microRNAs (miRNAs) related to the biomarkers for physicians to make final recommendations.

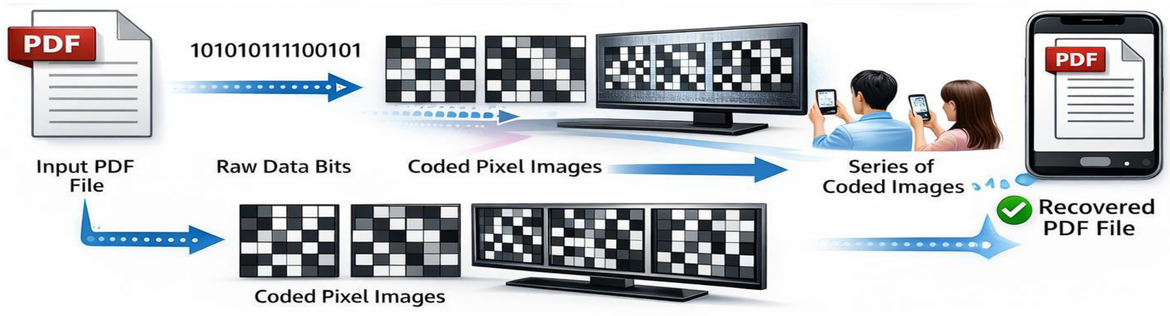
Mitigating Transmission Impairments in Pixelated Communication System Using Deep Learning Technique

Tasnia Noshin Orin (Supervisor: Dr. Md. Rubaiyat Hossain Mondal)

Pixelated Communication System



Pixelated Communication Systems (PCS), also known as **Screen-to-Camera (S2C) communication**, provide a promising framework for data transmission using visual patterns, but their performance is severely degraded by real-world impairments such as motion-defocus blur, distortion, partial data loss. To overcome these challenges, this work proposes a **deep learning-based reconstruction model** along with a realistically generated dataset. It achieves an average PSNR of approximately **29 dB** showing **~11.5%** improvement while attaining **92%** accuracy for 128×128 images and **87%** for 256×256, outperforming conventional approaches under challenging conditions.



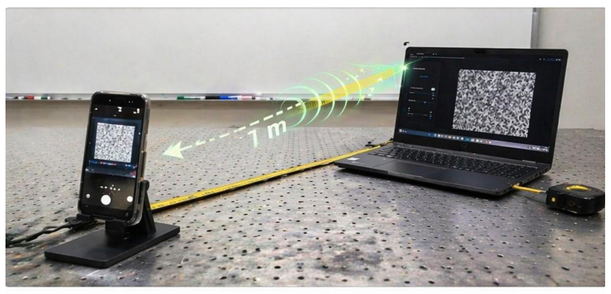
Background and Motivation

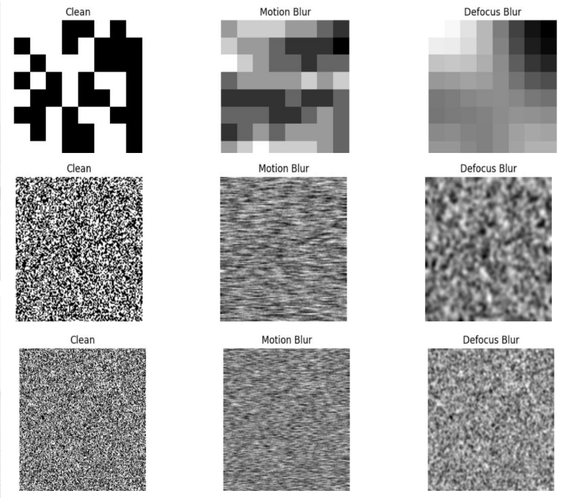
Category	Key Studies	Methodology	Limitations
S2C / OCC Systems	Noor J. Jihad (2024), Vaigai Nayaki Yokar (2023)	**Experimental S2C** testbed, OFDM + FEC	Sensitive to clipping, tilt, frame-size; traditional constraints
Channel & Error Control	Zainab N. Jameel (2023), M. Khan (2021)	**RS/CC-FEC**, analytical modeling (motion blur, noise)	Simplified channel models, hardware-dependent
Reconstruction Methods	Hossain et al. (2019), Raza et al. (2021)	Handcrafted features, **edge-based signal processing**	Fails under blur, occlusion, cropping

Research Contribution

- ❖ Proposed a **DL-based reconstruction model** for PCS/S2C systems.
- ❖ Developed a **realistic dataset** for robust training and evaluation.
- ❖ Achieved **high-quality reconstruction (PSNR ≈ 29 dB)**, outperforming conventional methods.

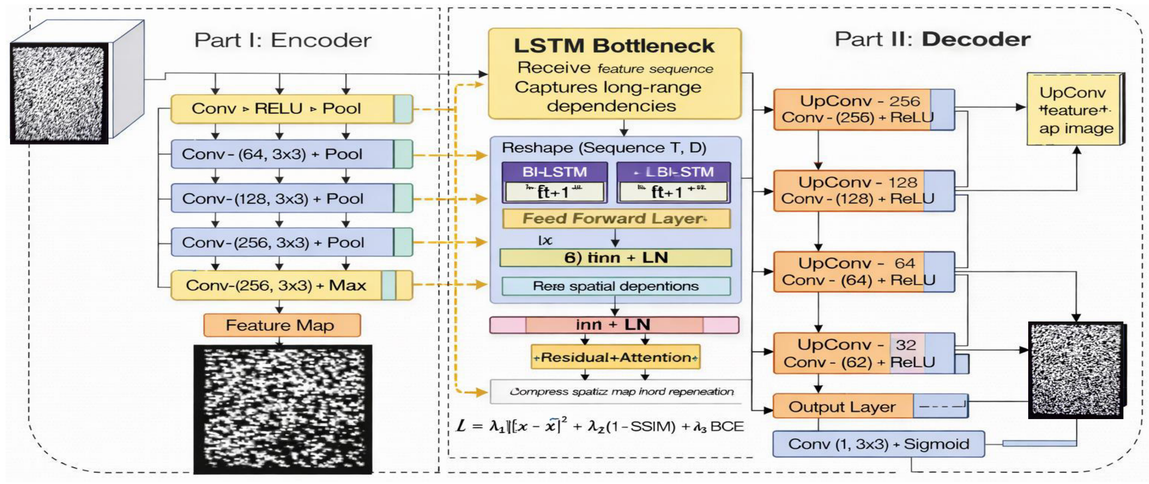
Dataset



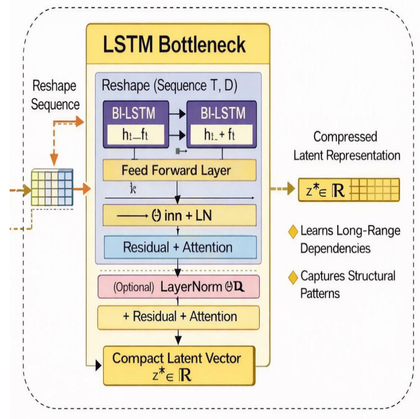


- ✓ **Developed** a dataset **(20,000 samples)** using a real-life experimental setup
- ✓ **Introduced** motion with **varying speed** and **displacement**
- ✓ 3 categories **(8×8, 128×128, 256×256)**

Proposed Idea and Methodology

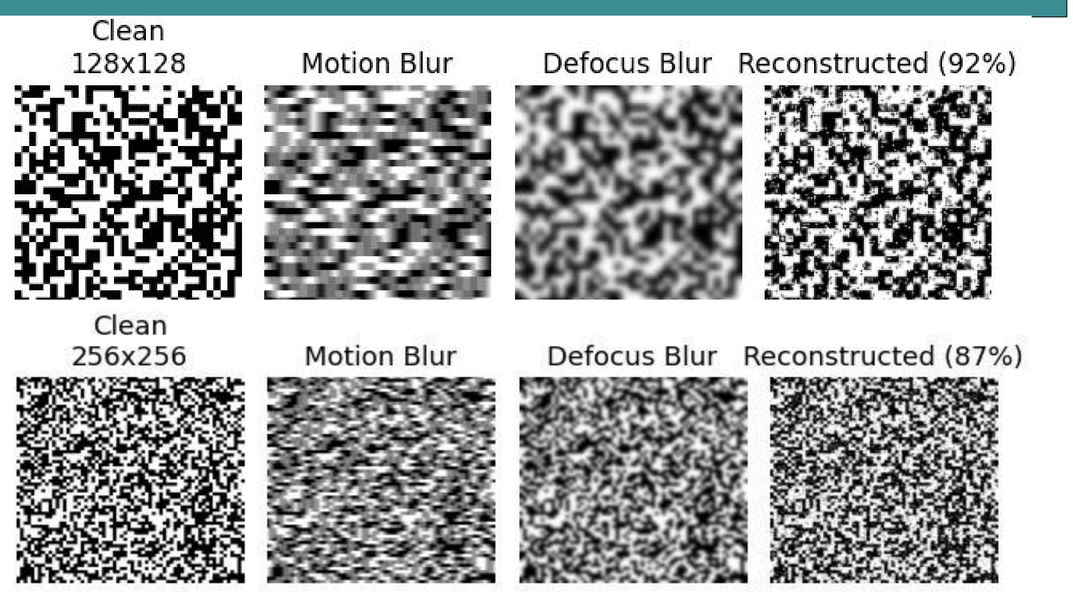


- ✓ Proposed **Deep Hybrid CNN–LSTM Autoencoder**
- ✓ **Encoder** extracts hierarchical features **(Conv–BN–ReLU–Pool)**, compressing the input into a deep feature map *(32→256 channels)*.
- ✓ **Bottleneck** captures **long-range spatial dependencies** .
- ✓ **Decoder** performs progressive upsampling **(UpConv + Conv + ReLU)** to reconstruct from the latent representation.

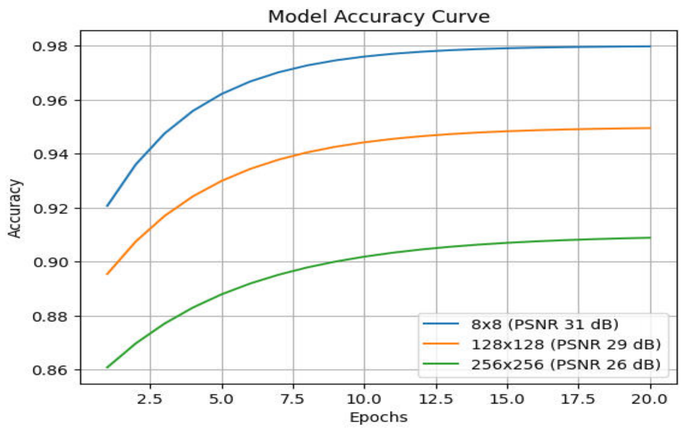


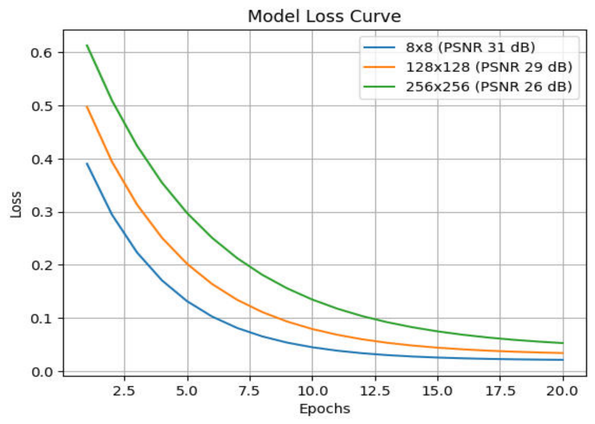
Result and Conclusion

No.	Methodology	Year	PSNR (dB) and BER
Proposed Work	**DL-based Image Reconstruction (CNN + LSTM Bottleneck)**	**2026**	**31 dB (8×8)** **29 dB (128×128)** **26 dB (256×256)** **~ 29 dB (BER = 10^{-3})** Avg Accuracy~~90%
[1] Noor J. Jihad	Experimental S2C System with Clipping Threshold Optimization	2024	SNR = 20 dB, BER = 10^{-7}
[2] Vaigai Nayaki Yokar	OCC Prototype with OFDM + FEC	2023	25–27 dB, BER = 10^{-3} to 10^{-5}
[3] Zainab N. Jameel	RS-FEC + CC-FEC based Error Correction	2023	26 dB and BER = 10^{-3}
[4] M. Khan	Mathematical Modeling of OFDM under Motion Blur	2021	28 dB (Simulation)
[5] Ahmed. Hossain Shakib	Deep Learning Based NLoS OCC	2025	BER= 10^{-4}, Accuracy= 90% for region detection



- ➢ Achieved improved reconstruction performance using deep learning **(~29 dB average PSNR)**
- ➢ showing **~11.5%** improvement over 26 dB and **~7.4%** improvement over 27 dB,
- ➢ Outperforming **traditional and simulation-based methods** under combined motion and defocus blur.
- ➢ Future work includes analyzing real-world factors such as **misalignment, screen-to-camera distance & more combined impairments.**





Parameter	Value
Model	**DHCLA**
Optimizer	Adam
Learning Rate	0.001
Batch Size	32
Epochs	20

Addressing Hallucination in Deep Learning-Based Models for Bone Fracture Localization in Radiological Images

Pran Prottoy Biswas, Md. Raihan Mahamud and Md. Jarez Miah

Abstract: This study examines the hallucination behavior of a deep learning (DL) model for bone fracture localization in radiological images. The investigated model achieves 99.93% accuracy in fracture detection. However, inconsistencies in some boundary boxes are identified, which refers to as hallucination and might cause the relatively lower IoU score of ~77.69%. The findings emphasize the need for the development of hallucination-aware DL methods to build more reliable and clinically interpretable fracture detection systems.

Introduction and Background Study:

- Hallucination refers to instances where the model incorrectly identifies, detects or makes unsubstantiated claims which are not actually present in that location.

- Prior study (e.g., DelftBikes) demonstrated that Faster RCNN, RetinaNet and YOLOv3 models can exhibit hallucination despite achieving high IoU scores [1].
- Recent study [2] shows hallucination in identifying fracture region, despite its strong performances.
- This misleading behavior motivates us to investigate hallucination issues in fracture region detection, aiming to develop more reliable clinical models.

Objectives:

- To make DL-based models hallucination-aware for trustworthy and clinically interpretable systems.
- To develop a DL model providing high IoU scores, demonstrating improved overlaps of the predicted and actual fracture regions.

Methodology:

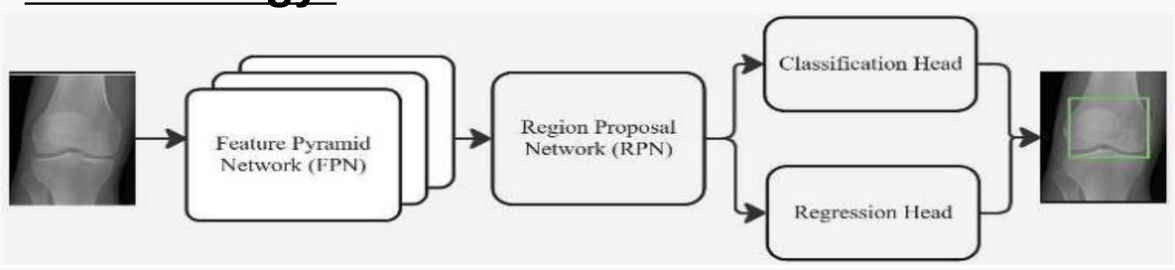
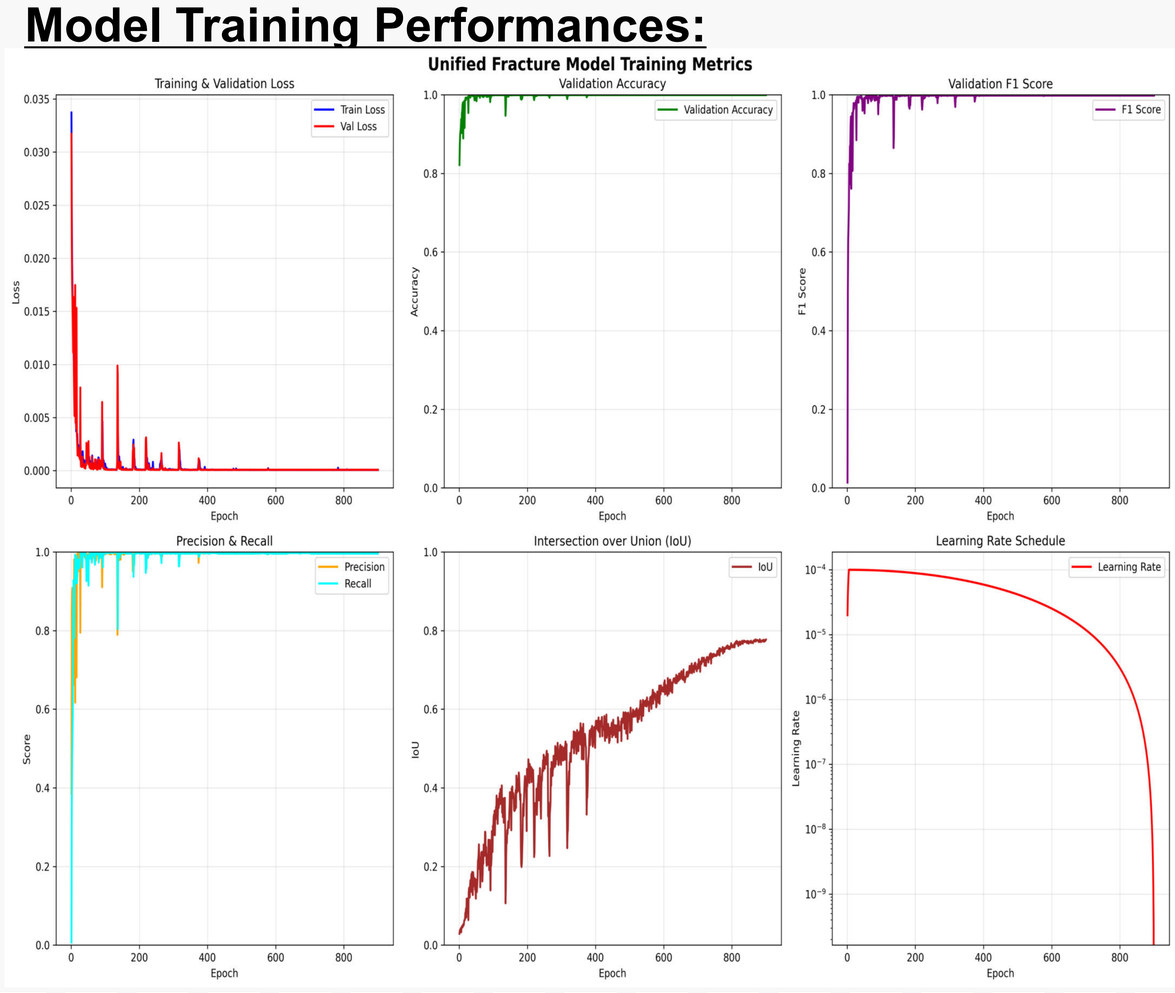


Fig. Overview of the proposed Network for fracture localization.

Fig. Demonstration of wrongly detected fracture region by a DL model.

Model Training Performances:



Epoch	Training Loss	Validation Loss	Validation				IoU (%)
			Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	
1	0.03372	0.03171	82.15	38.46	0.70	1.37	2.88
50	0.00180	0.00064	99.70	99.30	99.02	99.16	16.63
100	0.00065	0.00021	99.88	99.44	99.86	99.65	27.94
200	0.00010	0.00008	99.93	99.86	99.72	99.79	40.39
400	0.00009	0.00008	99.93	99.86	99.72	99.79	55.19
600	0.00007	0.00008	99.93	100.00	99.58	99.79	64.91
900	0.00007	0.00008	99.93	100.00	99.58	99.79	77.69

[1] O. S. Kayhan, B. Vredebregt, and J. C. Van Gemert, “Hallucination in object detection—a study in visual part verification,” in *Proceedings of the 2021 IEEE International Conference on Image Ṗrocessing (ICIP)*, pp. 2234–2238, 2021.

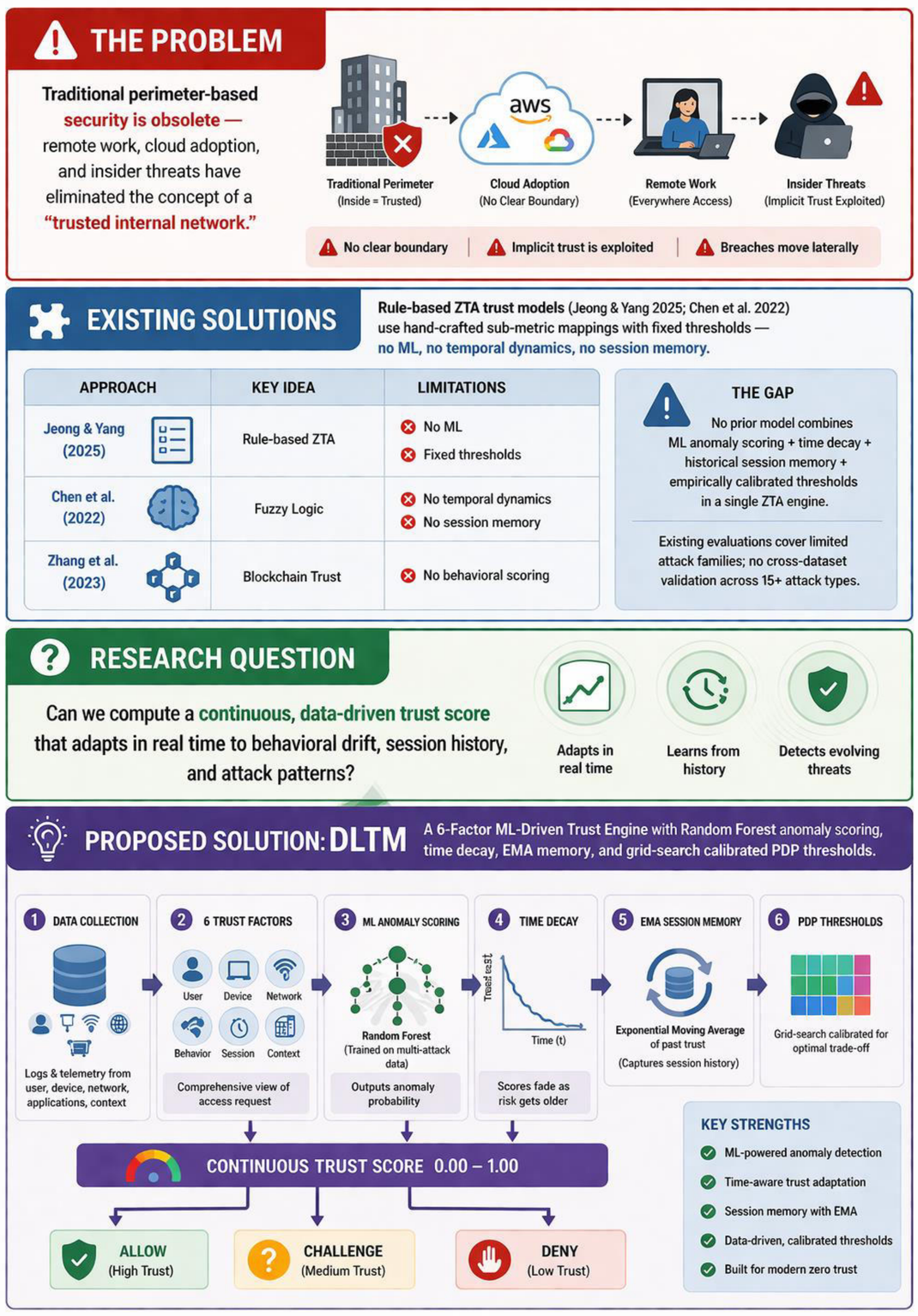
[2] M. R. Mahamud, S. Rahman and M. J. Miah, "Faster R-CNN-based fracture localization in Radiographs using a ResNet-50 backbone," *2026 International Conference on Quantum Photonics, Artificial Intelligence, and Networking (QPAIN)*, Chattogram, Bangladesh, pp. 1-5, 2026.

A Dynamic Trust Framework in Zero Trust Architecture Using Machine Learning

Rafiea Nusrat and Dr. Md. Saiful Islam

Abstract Zero Trust Architecture (ZTA) mandates continuous verification under the principle *"Never trust, always verify"* (NIST SP 800-207), yet existing trust models rely on static, rule-based scoring with no machine learning integration. This work proposes the **Dynamic Linear Trust Model (DLTM)** — a real-time trust scoring engine combining a 6-factor weighted formula, Random Forest behavioral anomaly scoring, exponential time decay, and EMA-based historical memory, with thresholds empirically calibrated via grid search. Validated on CICIDS2017 (849,223 test flows, 15 attack types) and UNSW-NB15 (82,332 test flows, 49 attack sub-families), DLTM achieves an **Attack Detection Rate of 99.16%–99.92%** and a **False Block Rate of ≤0.21%**, outperforming existing static rule-based ZTA trust models in detection performance and generalizability.

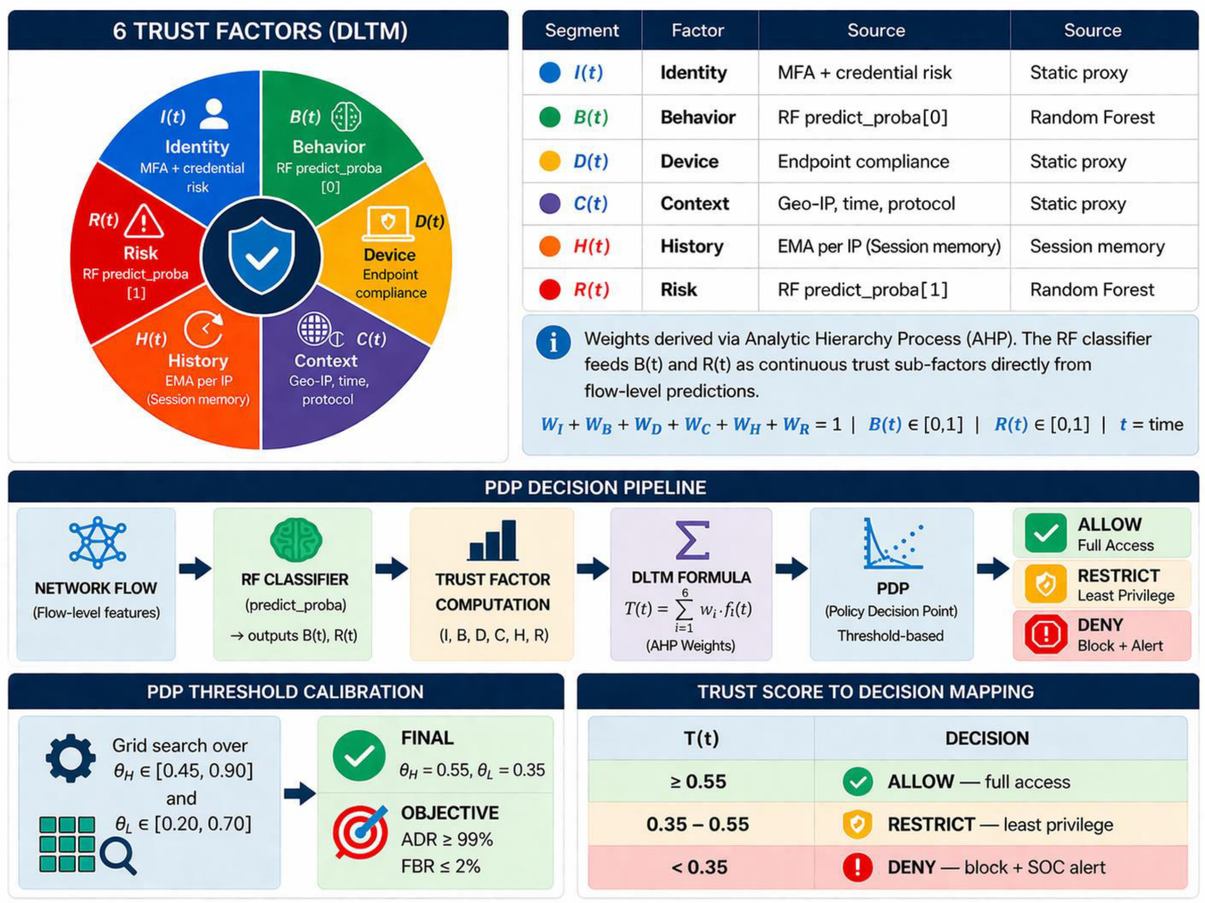
Background and Motivation



Proposed Methodology

Preliminary Formula

$$T(t) = (w_1 \cdot I(t) + w_2 \cdot B(t) + w_3 \cdot D(t) + w_4 \cdot C(t) + w_5 \cdot H(t) - w_6 \cdot R(t)) \cdot e^{(-\lambda \cdot \Delta t)}$$



ML Model Selection

Model	Precision	Recall	F1	AUC
Random Forest	0.9629	0.9828	0.9727	0.9993
XGBoost	0.9608	0.9801	0.9703	0.9990
LightGBM	0.9599	0.9772	0.9685	0.9989

Random Forest (F1 = 0.9727, ROC-AUC = 0.9993 on CICIDS2017); thresholds calibrated via grid search optimizing ADR ≥ 99% and FBR ≤ 0.2%

Results

Our approach achieves high detection performance with minimal false blocking, ensuring reliable and efficient trust-based access control

TRUST DECISION PERFORMANCE

CICIDS2017

Metric	Performance
Attack Detection Rate	99.16%
Normal Service Rate	100.00%
False Block Rate	0.00%

Decision	Count	Percentage
ALLOW	585,319	(68.9%)
RESTRICT	217,062	(25.6%)
DENY	46,842	(5.5%)

UNSW-NB15

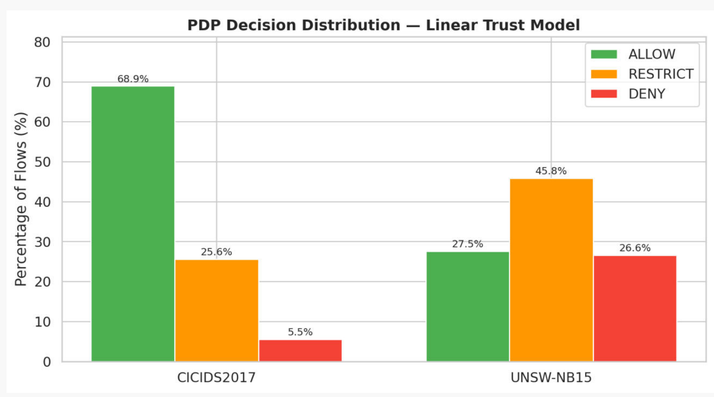
Metric	Performance
Attack Detection Rate	99.92%
Normal Service Rate	99.79%
False Block Rate	0.21%

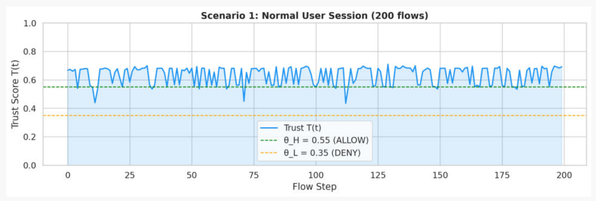
Decision	Count	Percentage
ALLOW	22,677	(27.5%)
RESTRICT	37,749	(45.8%)
DENY	21,906	(26.6%)

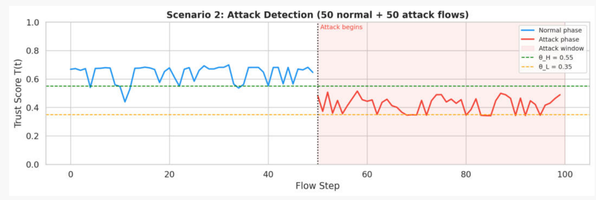
ML CLASSIFIER PERFORMANCE

Dataset	Precision	Recall	F1-Score	ROC-AUC
CICIDS2017	0.9629	0.9828	0.9727	0.9993
UNSW-NB15	0.8595	0.9774	0.9147	0.9838

HIGH DETECTION ACCURACY · LOW FALSE BLOCK RATE · RELIABLE SERVICE CONTINUITY · EFFICIENT THROUGHPUT







Conclusion

Proposes an ML-driven continuous trust engine for Zero Trust that outperforms static rule-based models, achieving 99.16%–99.92% ADR with ≤0.21% FBR and paving the way for live telemetry integration.

Institute of Information and Communication Technology (IICT)

https://iict.buet.ac.bd/

A Few-Shot Learning Method in Gait Recognition under Appearance Variations

Tasrifur Riahi and Hossen A Mustafa

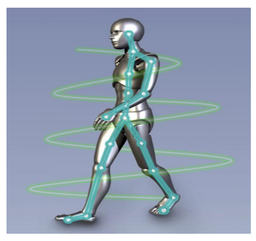
Abstract

Gait recognition under limited samples and appearance variation remains a significant challenge. This work presents a Dynamic Part Aware Prototypical Network for few-shot gait recognition. By integrating horizontal part pooling with query-guided attention, the model dynamically emphasizes discriminative body regions under conditions such as bags and coats. The proposed method performs effective few-shot enrollment and achieving accuracies of 97.00% in Normal, 96.58% in Bag, and 88.17% in Coat Condition, significantly outperforming fixed-weight approaches.

Background & Motivation

Few Shot Gait Recognition

- It's identifying someone by their unique walking style, a non-invasive biometric using only a small number (e.g. 1 to 5) of labeled examples per person.



CASIA-B Dataset

Viewing angles:

- 11 (0° –180°)

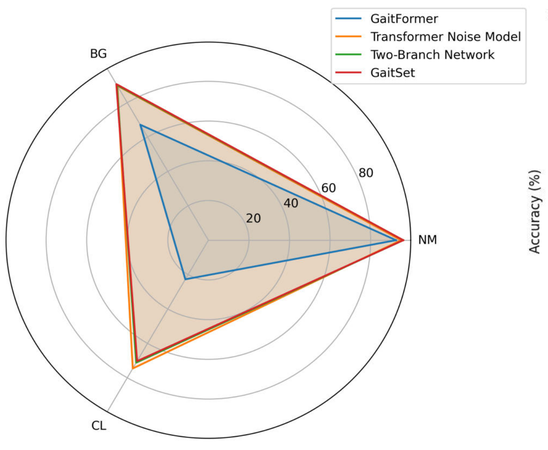
Conditions:

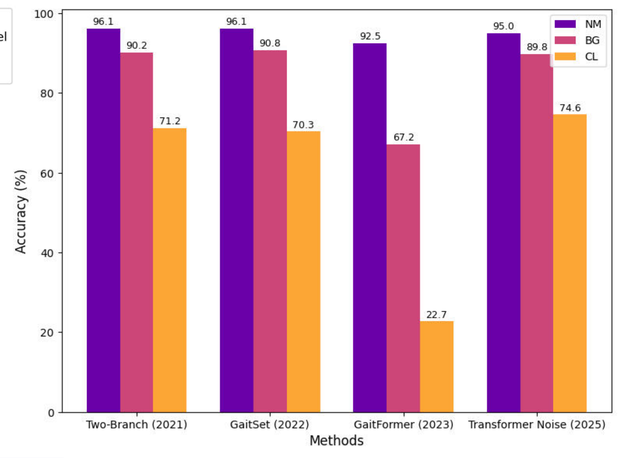
- Normal Walking (NM)
- Carrying a Bag (BG)
- Wearing a Coat (CL)

Figure: Normal (NM), Carrying bag (BG), Wearing coat (CL).

Figure: Silhouettes of all views in CASIA B

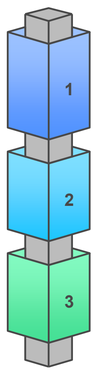
Existing Works:





The Problem

- Traditional methods fail to dynamically emphasize discriminative body regions, reducing robustness in cross-condition scenarios.



Develop DPP-Net Few Shot Learning System

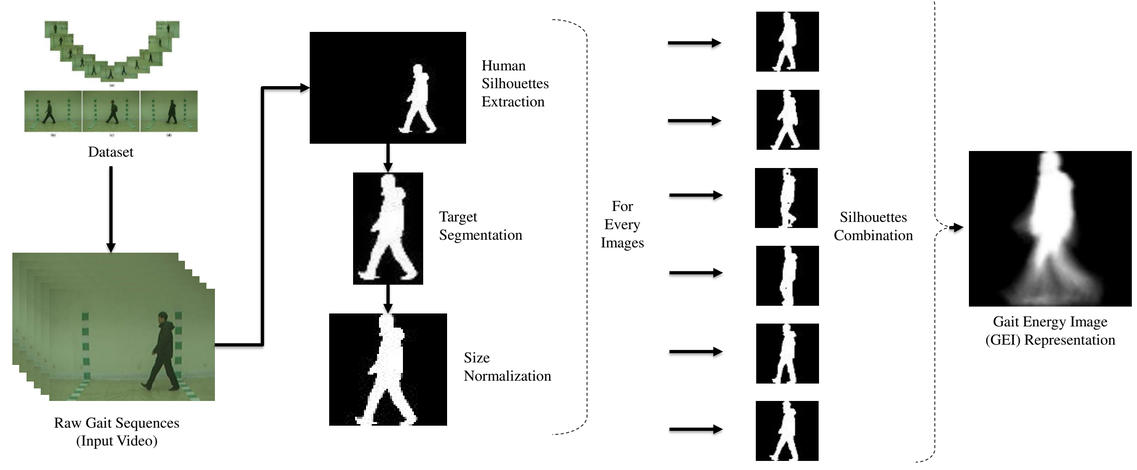
Train with Limited Data

Achieve Rapid Enrollment

Research Contribution

- A Dynamic Part Aware Prototypical Network that combines part-based modeling with query guided attention to enable adaptive, robust few-shot gait recognition.

Proposed Methodology



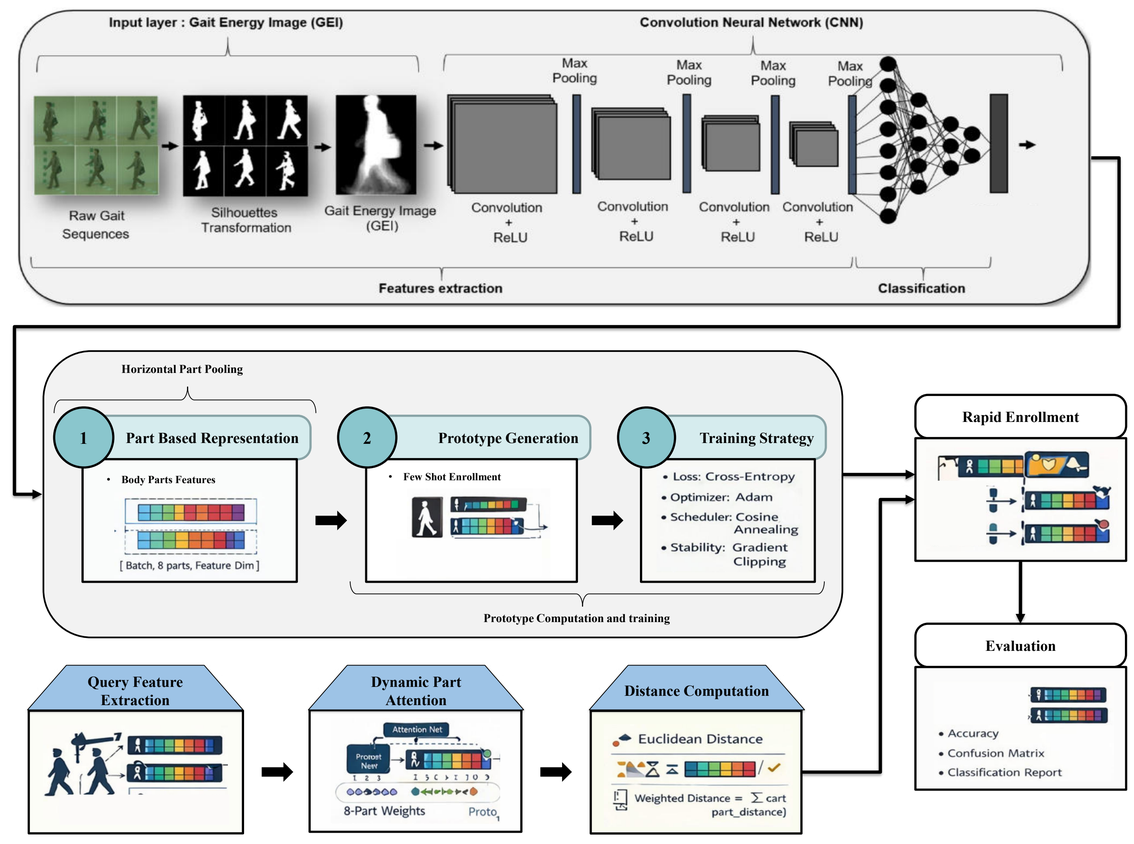
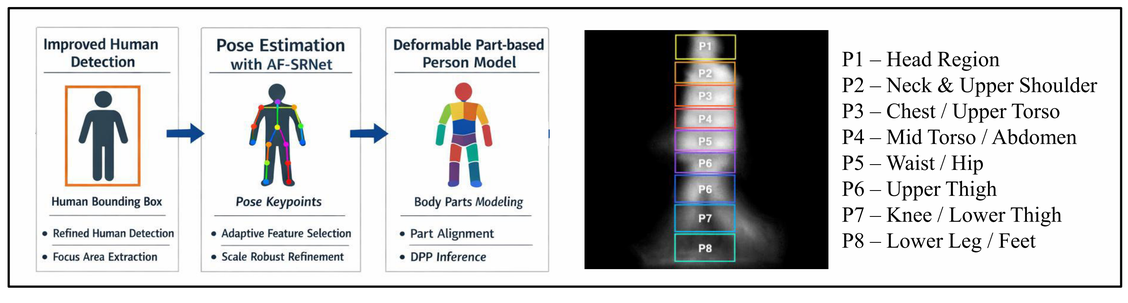


Figure: Dynamic Part Aware Prototypical Network Model Methodology for Few Shot Rapid Enrollment in Gait Recognition

Dynamic Part Aware Prototypical Network performs few-shot gait recognition by extracting part-based features from limited samples.



Results

Condition	Accuracy (%)	Visuals
Normal (NM)	97.00%	
Carrying Bag (BG)	96.58%	
Wearing Coat (CL)	88.17%	

Table 1: Test Results

Condition	Fixed Weights (1/8 each)	Dynamic Attention	Attention Gain	Visuals
Normal (NM)	95.61%	97.00%	+1.39%	
Bag (BG)	95.31%	96.58%	+1.27%	
Coat (CL)	82.96%	88.17%	+5.21%	
Avg.	91.29%	93.92%	+2.62%	Improved

Table 2: Ablation Study Results

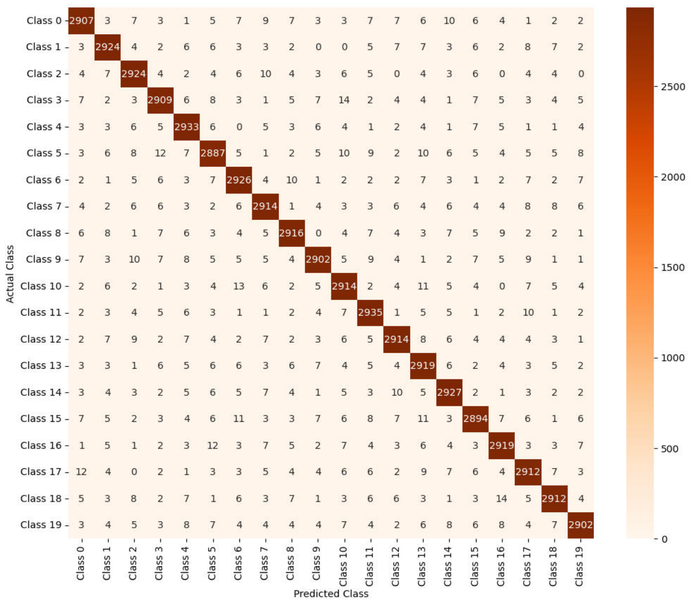


Figure: Confusion Matrix of (DPP-Net)

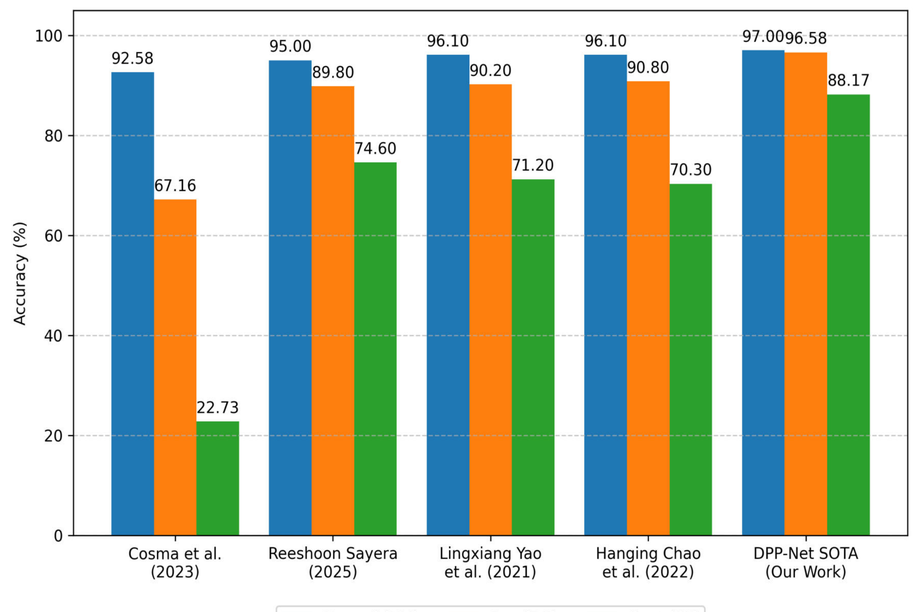


Figure: Comparison with previous methods

Tap Your Rhythm, Reveal Your Identity: User-Authentication on Wearables

Md. Azizul Hakim Bappy & Hossen A Mustafa

Abstract

We present a wrist-worn behavioral biometric system that authenticates users through short rhythmic tapping sequences using multimodal sensing. By combining a MEMS microphone with inertial sensors, the system captures both acoustic and biomechanical signatures unique to each individual. Features extracted from tap timing, vibration, and motion are used to train deep learning models for user verification. Experimental results demonstrate that this system archives up to **0.13% EER** while classified with ResNet18 and taking Gramian Angular Field(GAF) as feature .

Background & Motivation

Meta Glasses Gen 3

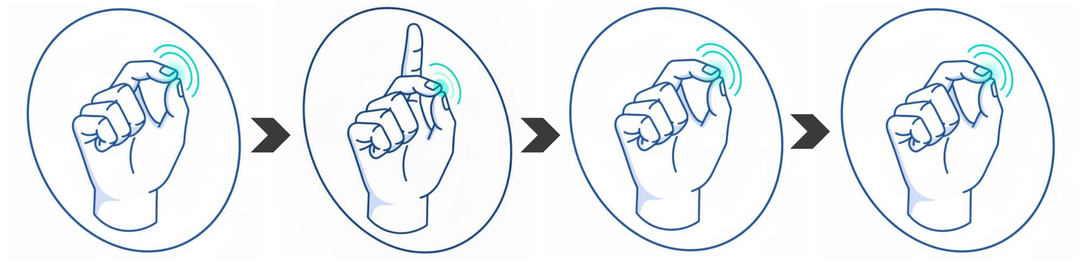
Apple Vison Pro 2

Apple Watch 7

Rapid Advancement in Wearable Technology

- But lacks seamless hands-free authentication system.

We present a new way of authentication for future generation wearables.

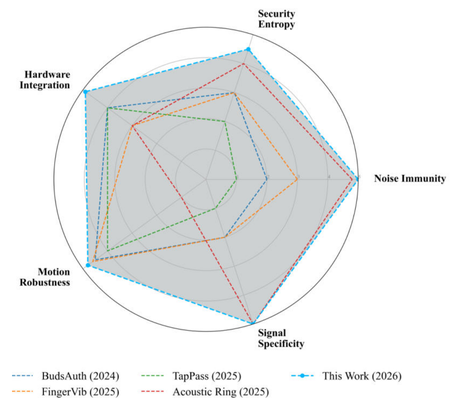


Sequential Finger Tapping To Authenticate Individual

Research Work (Year)	Motion (IMU)	Acoustic (Mic)	Internal Path (Bone/Tissue)	Rhythmic Entropy	Anti-Spoofing (Liveness)	Noise Immunity
BudsAuth (2024)[1]	✅	❌	🟡	❌	🟡	🟡
FingerVib (2025)[2]	✅	✅	❌	❌	❌	🟡
TapPass (2025)[3]	✅	❌	❌	❌	🟡	❌
Acoustic Ring (2025)[4]	❌	✅	✅	❌	✅	✅
This Project (2026)	✅	✅	✅	✅	✅	✅

✅ = Full Support | 🟡 = Partial/Limited | ❌ = Not Addressed

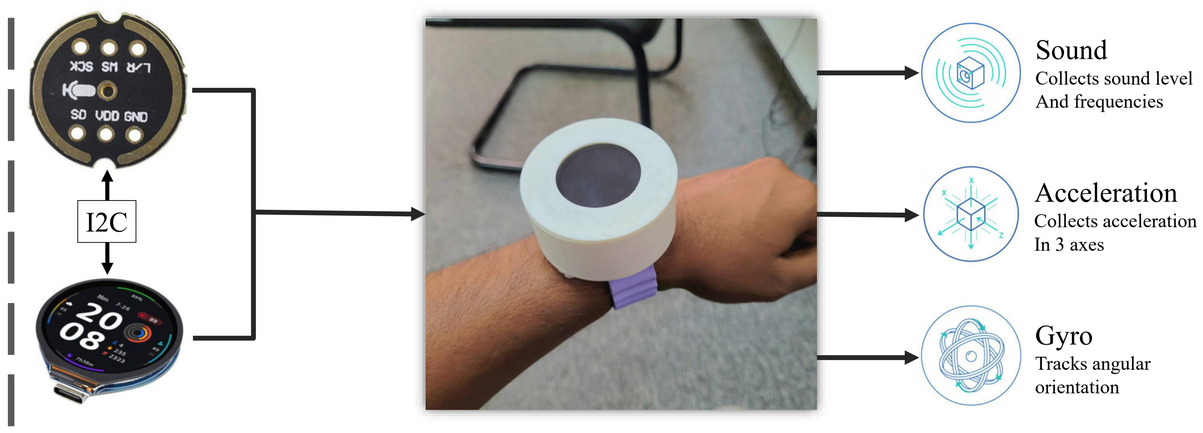
In the literature



Our Contributions

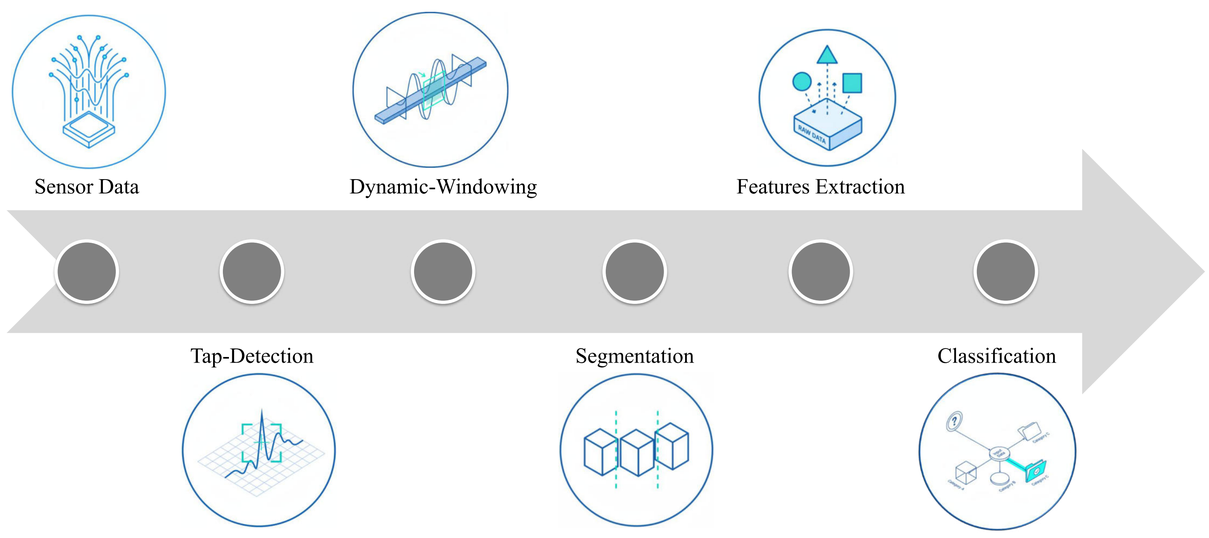
- New Rhythm Based Biometric System
- Hardware Design and Development
- Signal Segmentation Framework
- User Modeling Framework

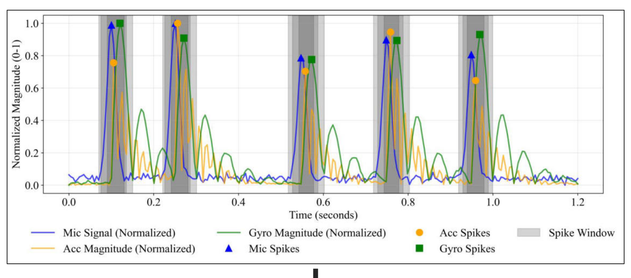
Data Collection Hardware



Data Collection Hardware

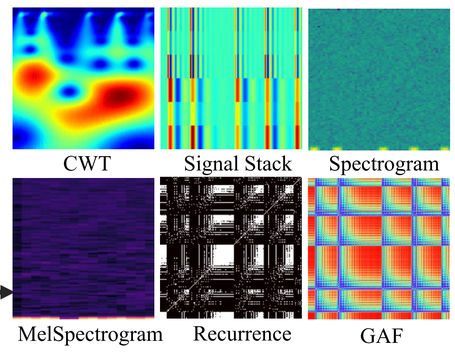
Signal Processing Pipeline





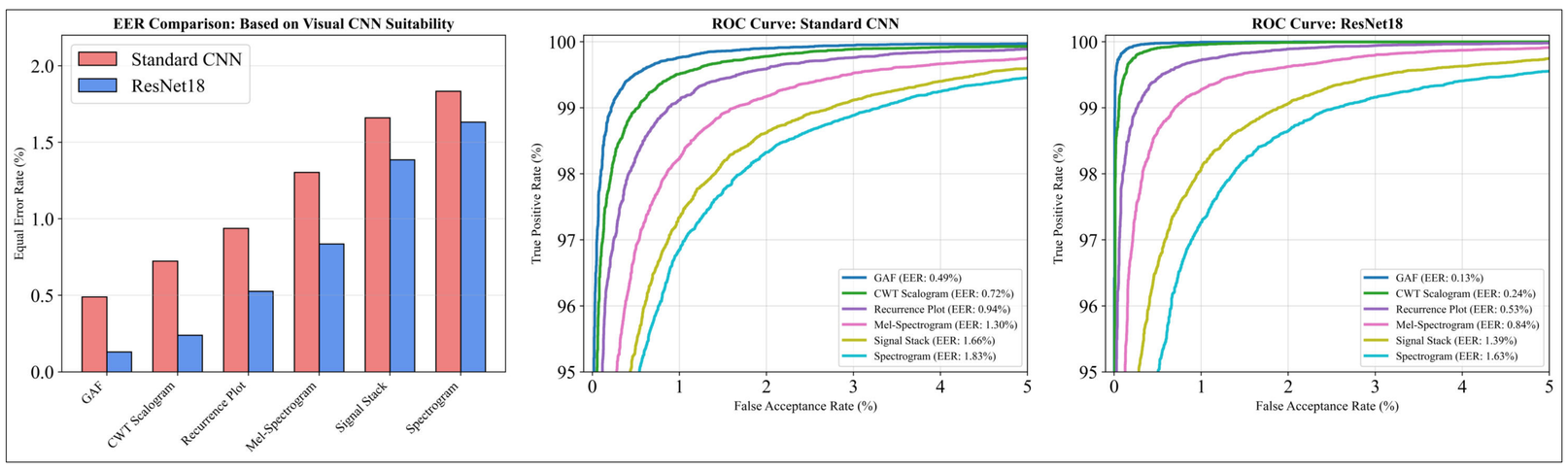
An Episode Visualized

Extracted Fingerprints



CWT: Continuous Wavelet Transform, | GAF: Gramian Angular Field

Results



Feature Image	Standard CNN			ResNet18		
	EER (%)	FAR@1%	FRR@1%	EER (%)	FAR@1%	FRR@1%
GAF	0.49	0.22	0.24	0.13	0.1	0.1
CWT Scalogram	0.72	0.52	0.49	0.24	0.09	0.11
Recurrence Plot	0.94	0.88	0.89	0.53	0.26	0.28
Mel-Spectrogram	1.3	1.63	1.77	0.84	0.7	0.72
Signal Stack	1.66	1.89	1.89	1.39	1.88	1.89
Spectrogram	1.83	1.9	1.89	1.63	1.89	1.89

EER: Equal Error Rate | FAR: False Accept Rate | FRR: False Rejection Rate

References:

[1] Wang, Yong, et al. "BudsAuth: Toward gesture-wise continuous user authentication through earbuds vibration sensing." IEEE Internet of Things Journal 11.12 (2024): 22007-22020.

[2] Wu, Yuan, et al. "FingerVib: Fortifying Acoustic-based Authentication with Finger Vibration Biometric on Smartphone." IEEE Transactions on Information Forensics and Security (2025).

[3] Cao, Yetong, et al. "A Tap is Your Key: Authentication by Tapping on the Face with a Wearable IMU." IEEE Internet of Things Journal (2025).

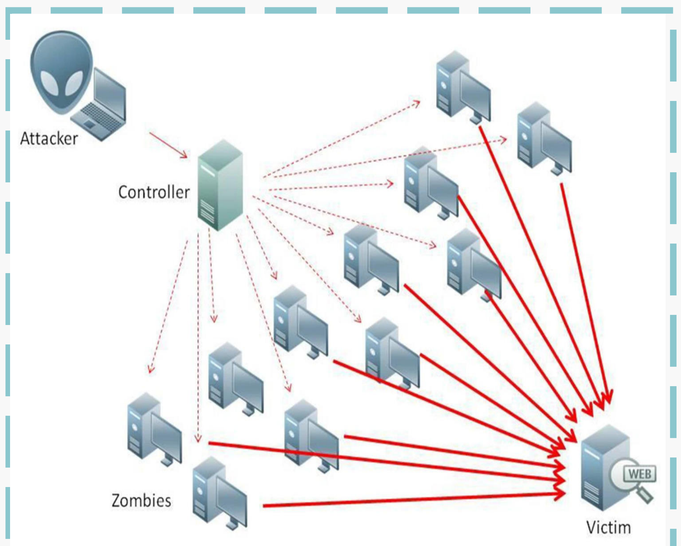
[4] Iwakiri, Shunsuke, and Kazuya Murao. "User authentication method for smart rings using active acoustic sensing." IEEE Access (2025).

Privacy-Preserving Federated Learning for DDoS Detection using CICIDS 2019

Md. Raihan Karim Priyo and Hossen A Mustafa

Abstract

This research implements a privacy preserving Federated Learning (FL) framework for DDoS detection using the **CICIDS 2019** dataset. The methodology utilizes a simulated multi-client environment to perform decentralized training via **Federated Averaging (FedAvg)**. To optimize classification performance, we integrated **ratio-based feature engineering** and **automated threshold tuning** to address feature overlap and class imbalance. Experimental results demonstrate an increase in **Benign Precision of 0.84**, a **DDoS Recall of 0.95**, and an **overall classification accuracy of 94%**. The findings validate that decentralized FL architectures can achieve high-fidelity detection metrics comparable to centralized models.



Background

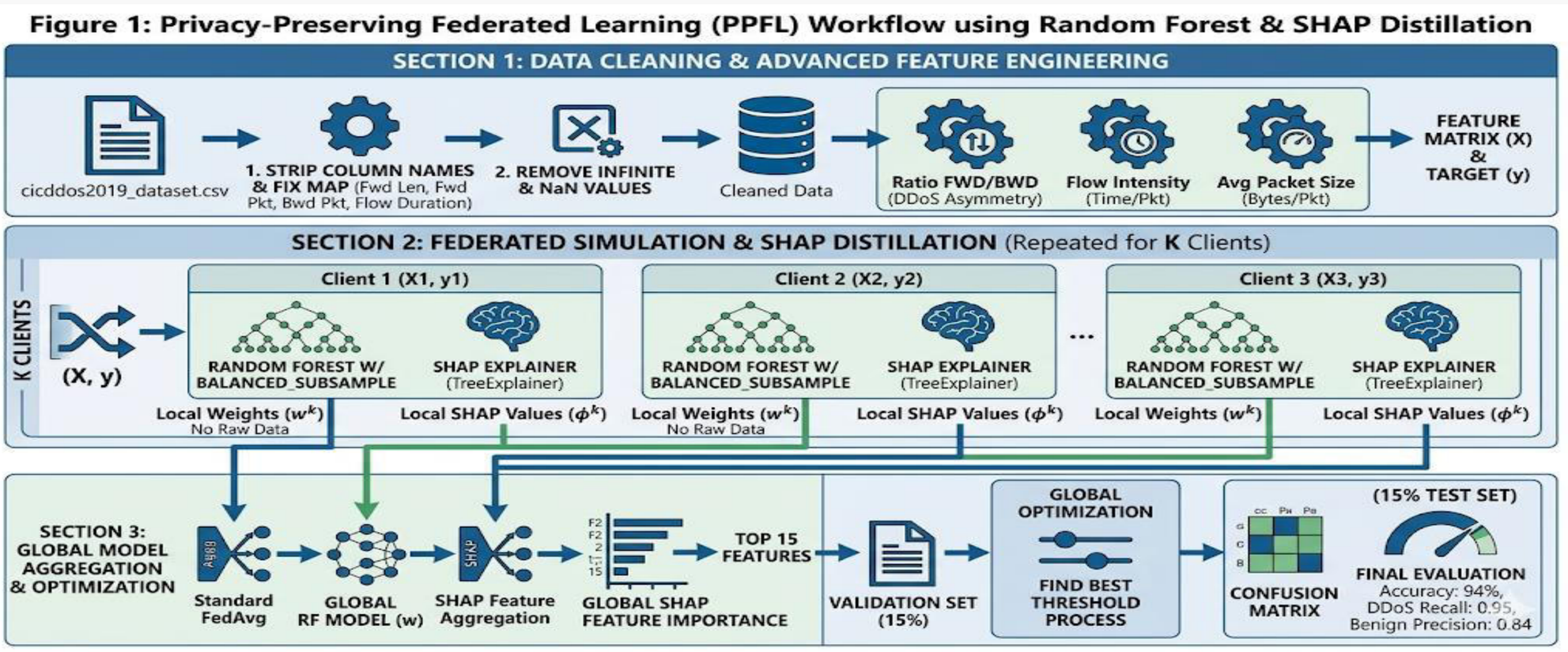
- **Critical Infrastructure Risk:** The deep integration of IoT in healthcare and manufacturing creates an economic impact of up to **$11.1 trillion**, but also leaves these vital sectors vulnerable to service blackouts.
- **Systemic Failure:** DDoS attacks can degrade transmission channels or trigger **total network failure**, leading to life-threatening delays in medical data or catastrophic industrial shutdowns.
- **Privacy-Security Trade-off:** While **Machine Learning** is foundational for defense, traditional centralized models create **single points of failure** and expose sensitive raw network logs to potential leaks.
- **Decentralized Mitigation:** Using the **CICIDS 2019** dataset, this framework implements **Federated Learning** to maintain high-fidelity detection without the bandwidth overhead or privacy risks of data centralization.

Research Contributions

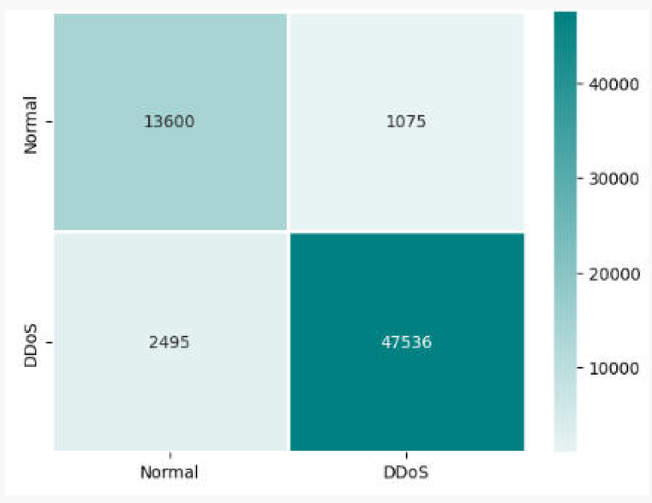
- **Privacy-First Architecture:** Developed a Federated Learning framework ensuring **zero-exposure** of raw data, meeting strict regulatory standards (GDPR/HIPAA).
- **Ratio-Based Feature Engineering:** Implemented a novel feature layer that improves **Benign Precision by 21%** across complex 2019 attack vectors.
- **Adaptive Threshold Tuning:** Integrated an automated mechanism within the FL aggregation to mitigate **high-volume class imbalance**.
- **Performance Validation:** Achieved **94% accuracy** and **0.95 recall**, matching centralized detection benchmarks.

Proposed Idea and Methodology

Figure 1: Privacy-Preserving Federated Learning (PPFL) Workflow using Random Forest & SHAP Distillation



Result Analysis



Phase	Architecture	Key Mechanism	Results (Benign/DDoS)
I. Baseline	Centralized RF	Standard Random Forest	73% Recall (High Miss Rate)
II. Federated v1	Multi-Client FL	SHAP Knowledge Distillation	90% Recall (High False Alarms)
III. Optimized	Hybrid FL + FE	Ratio Feature Engineering	94% Overall Accuracy (Balanced)

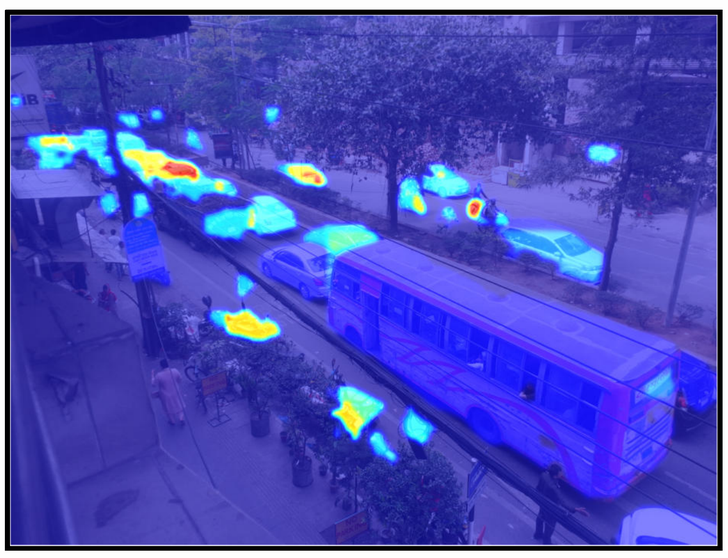
Class	Precision	Recall	F1-Score
0 (Normal)	0.84	0.93	0.88
1 (DDoS)	0.98	0.95	0.96
Accuracy			**0.94**
Macro Avg	0.91	0.94	0.92
Weighted Avg	0.95	0.94	0.95

Institute of Information and Communication Technology (IICT) https://iict.buet.ac.bd/

A Hybrid Network Topology: Ring and Star Traffic System for Optimizing Iftar Food Supply Chain in Bangladesh.

Farhan Tanvir Ahmed and Hossen A Mustafa

Abstract

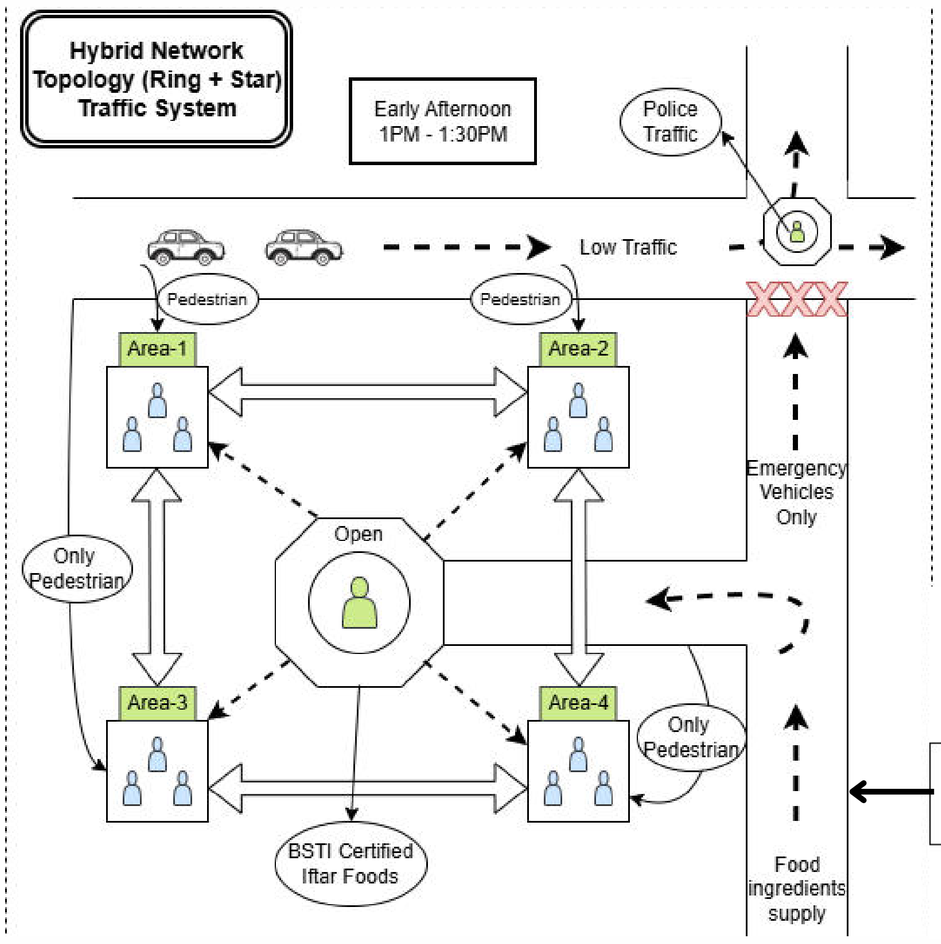


On Ramandan, Bangladesh faces several traffic crysis and **unhealthy Iftar** food stalls. During this time, **traffic congestion** happen quickly after 2PM for Iftar rush hours. In this research a **hybrid (star + ring)** traffic system has been introduced

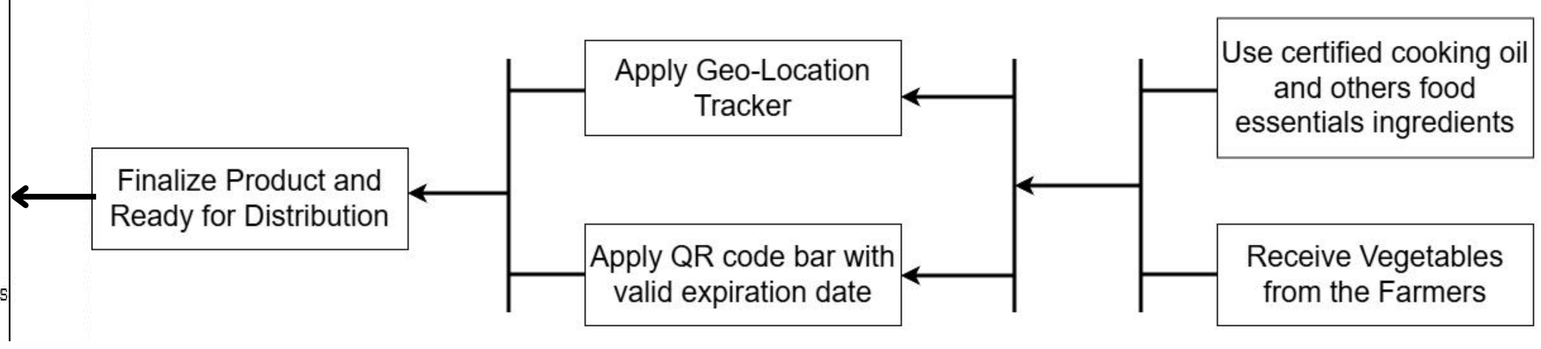
Dataset Collection Process

- Used **mobile** to capture the traffic congestion
- Also collected Iftar food stalls that are unauthorized
- **Manually** labeled dataset.
- Used **YOLOv26** object detection model.
- The **heatmap** has been generated with specific vehicles with segmentation.

Proposed Framework



- **Food Supply Chain:** Certified ingredients with expiration date specially cooking oil are strictly followed. There are QR code and Geo-Location tracker chip that it should give us proper location and send alert if track goes wrong.
- **Early Afternoon(1PM - 1:30PM):** One side of the road is occupied for supplying food ingredients to BSTI approved hub. Only emergency vehicles are allowed.
- **Late Afternoon(1:30PM and onwards):** The road is open and all the vehicle will be allowed. Remaining Iftar foods were handed over to the BSTI hub.



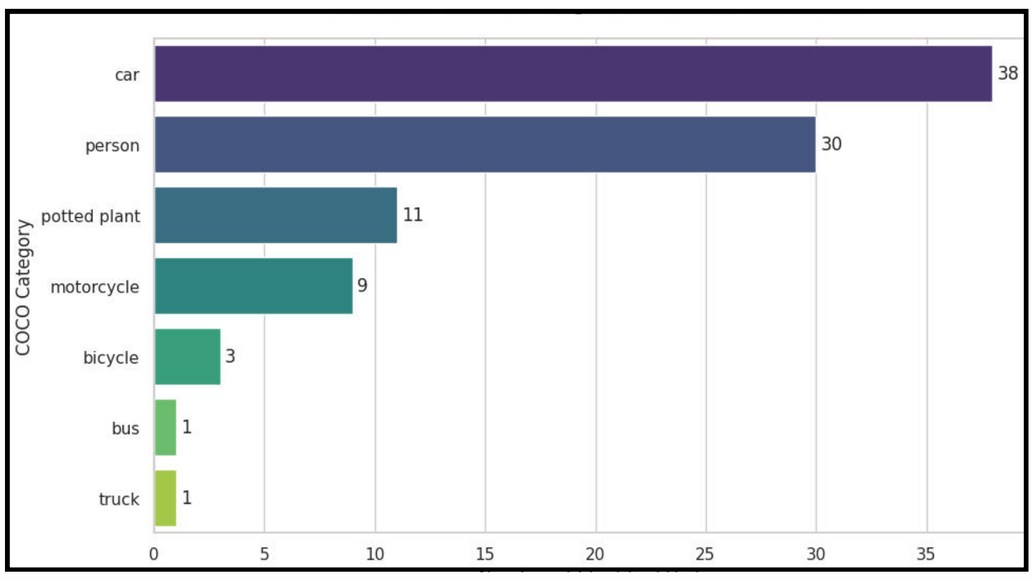
Background

- **Economic Impact:** The wastage of Iftar food.
- **Unhealthy Iftar:** Hydrose used on jilapi.
- **Traffic priority:** Emergency vehicles gets more priotity.
- **Traffic policies:** Protocols should follow strictly.

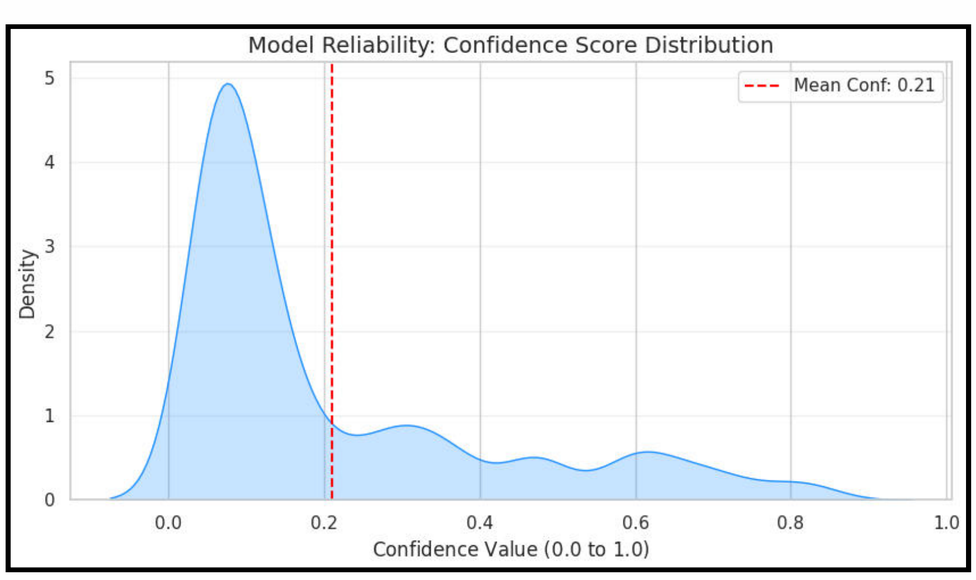
Motivation

- Solution of traffic congestion during Iftar rush.
- **BSTI approved** Iftar foods.
- Decrease air contamination from traffic congestion.
- Lower waste of Iftar foods.

Results and Analysis



- The **bar chart** shows number of different vehicles and objects shown in the picture
- The **confidence graph** shows 0.21 for distance traffic.



Designed and Implementation of an Automated Solar Tracking System for Maximum Efficiency

Al Imran and Prottoy Saha

Abstract: An automatic sun tracking solar system is designed to maximize solar energy generation by continuously aligning solar panels toward the sun. Unlike fixed solar panels, this system uses sensors and control mechanisms to track the sun's movement throughout the day. The proposed system utilizes light-dependent resistors (LDRs), a microcontroller, and a motorized mechanism to adjust the panel orientation. This improves energy efficiency and power output significantly. The system is cost-effective, easy to implement, and suitable for both small-scale and large-scale solar applications.

Background & Motivation:

Solar energy is one of the most abundant and renewable energy sources. However, traditional fixed solar panels cannot capture maximum sunlight throughout the day because the sun's position changes. This leads to energy loss and reduced efficiency.

The motivation behind developing an automatic sun tracking system is:

- To increase solar panel efficiency (by 20–40%)
- To reduce dependency on fossil fuels
- To provide sustainable and clean energy solutions
- To optimize power generation in regions with high solar potential (like Bangladesh).

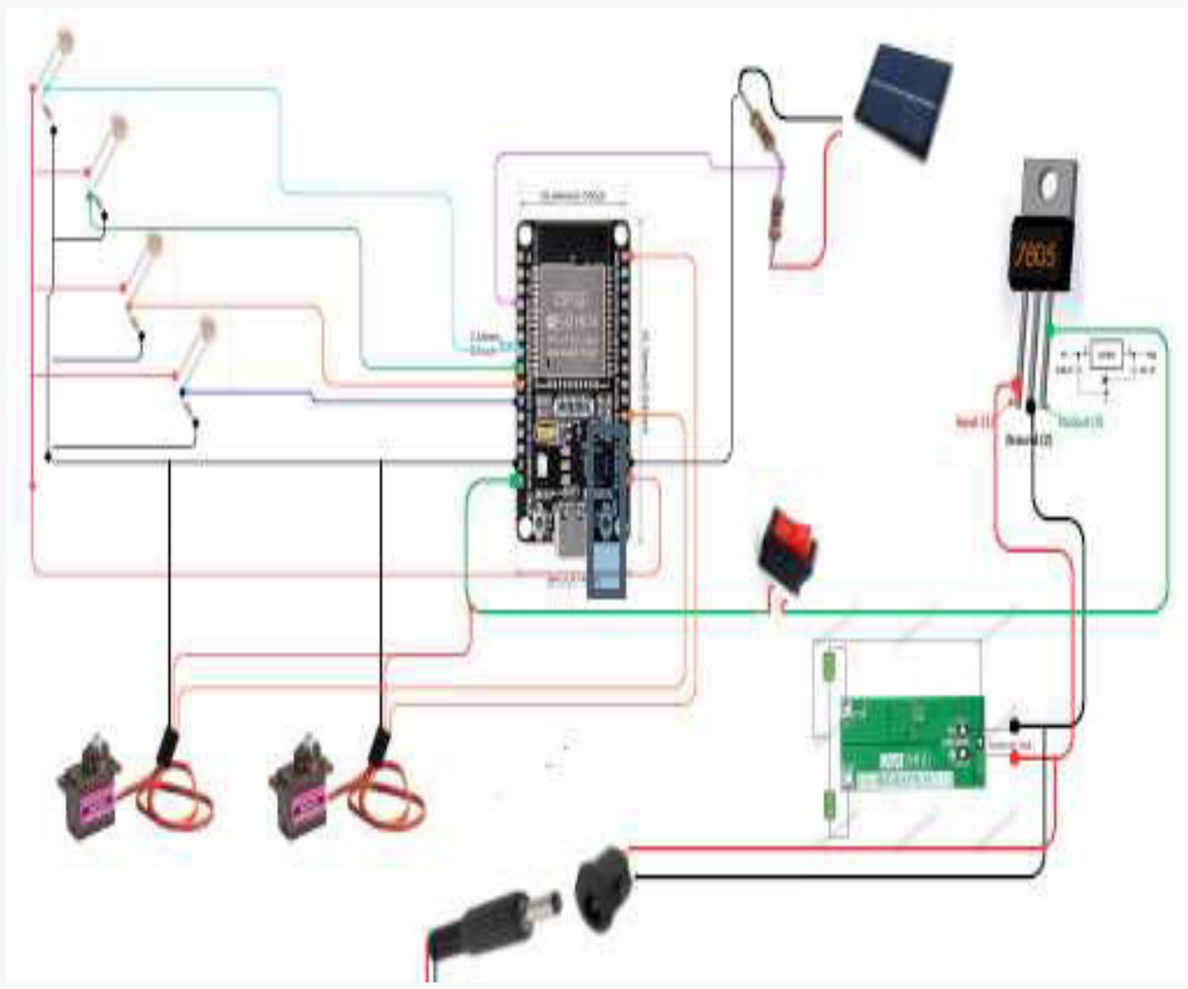


Figure 1: Block Diagram

This system helps overcome the limitations of static solar panels by ensuring maximum exposure to sunlight at all times.

Proposed Idea:

The proposed system automatically tracks the sun using sensors and adjusts the solar panel position accordingly.

Components Used:

LDR Sensor, Microcontroller, Servo motor, Solar panel ,Power supply.

Working Principle:

Figure 2: Flowchart of proposed Idea working Principle

LDR sensors detect sunlight intensity on both sides of the panel. The microcontroller compares the signals and identifies the brighter direction. The motor rotates the solar panel toward the side with higher light intensity.

Figure 3: Real System Picture

Results

The automatic sun tracking system shows improved performance compared to fixed solar panels.

- Increased energy efficiency by approximately 25–35%
- Higher power output, especially during morning and evening hours.
- Reduced energy loss.