National Forensic Sciences University
Knowledge | Wisdom | Fulfilment
An Institution of National Importance
(Ministry of Home Affairs, Government of India)

Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network

A Deep Learning Approach to 5G Cybersecurity

Department: School of Cyber Security and Digital Forensics
Program: M.Tech Artificial Intelligence & Data Science
(Specialization in Cyber Security Specialization)
Year / Sem: 1st / 2nd - Session: 2024-26

Subject Name: Advanced Machine Learning for Cyber Security and Forensics
Subject Code: CTMTAIDS SII P1
Guided By: Dr. Ahlad Kumar Sir

Presented by:	Pratham Badge	Suraj Verma	Amit Gupta
Enrolment No.:	2401003007003	2401003007012	2401003007023

Paper Highlights

- **Authors:** B. Hussain, Q. Du, B. Sun, Z. Han
- **Journal:** IEEE Transactions on Industrial Informatics, Feb 2021
- **Goal:** Efficient DDoS detection using Deep Learning (CNN & BLSTM)
- **Key Contribution:** Real-time detection for CPS in 5G
- **DOI:** 10.1109/TII.2020.2974520

Problem Statement:
DDoS Detection in 5G Network Slices

- 5G connects billions of devices, increasing the attack surface.
- Network slicing creates isolated yet interdependent segments.
- Real-time applications need ultra-fast protection.
- Traditional DDoS detection is too slow and rule-based.
- Encrypted and dynamic traffic bypasses static filters.
- CNNs offer fast, adaptive, lightweight, and accurate detection.

Objectives

- Design and implement a **CNN-based model** to **detect DDoS attacks** in **5G networks**.
- Focus on **protecting network slices** in **Cyber–Physical Systems (CPS)**.
- Train a **binary classifier** to distinguish between benign and **malicious traffic.**
- Achieve high accuracy, precision, and **low false positives**.
- Integrate the solution into **Software Defined Networking (SDN)** and **Network Function Virtualization (NFV)** environments.

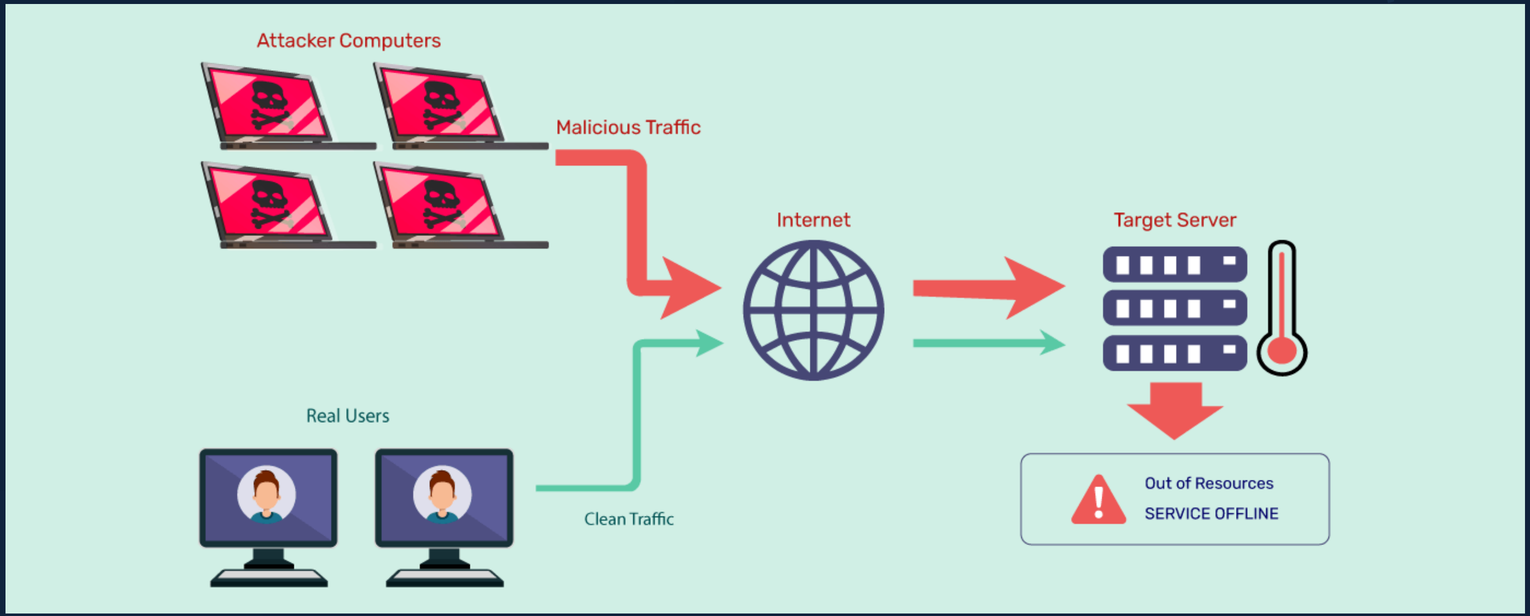
Introduction - DDoS

What is a DDoS Attack?

- DDoS (Distributed Denial-of-Service) attacks **overwhelm a system or network** with massive traffic.
- Aim to make a **service or network resource unavailable** to legitimate users.
- Widely used in **cyber warfare, botnets, and extortion campaigns**.

Real-World Consequences:

- Service Outages
- Financial Losses
- Data Breach Risk
- Customer Trust Damage
- Degraded Performance



Introduction – 5G

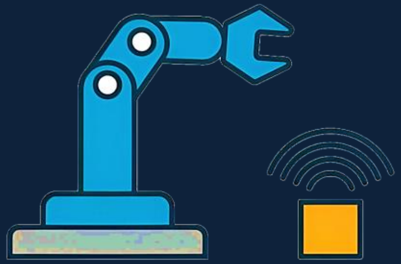
Why is 5G Vulnerable?

- 5G offers **ultra-reliable, low-latency communication** and **massive device connectivity**.
- **Network slicing** enables customized virtual networks—but also increases the **attack surface**.
- The real-time nature of 5G requires **instant threat detection and response**.

Why 5G ?

- More Speed, More Devices, More Risk
- Massive Attack Surface
- Network Slicing Makes It Worse
- Edge Computing & AI Need Real-Time Security

Introduction - CPS

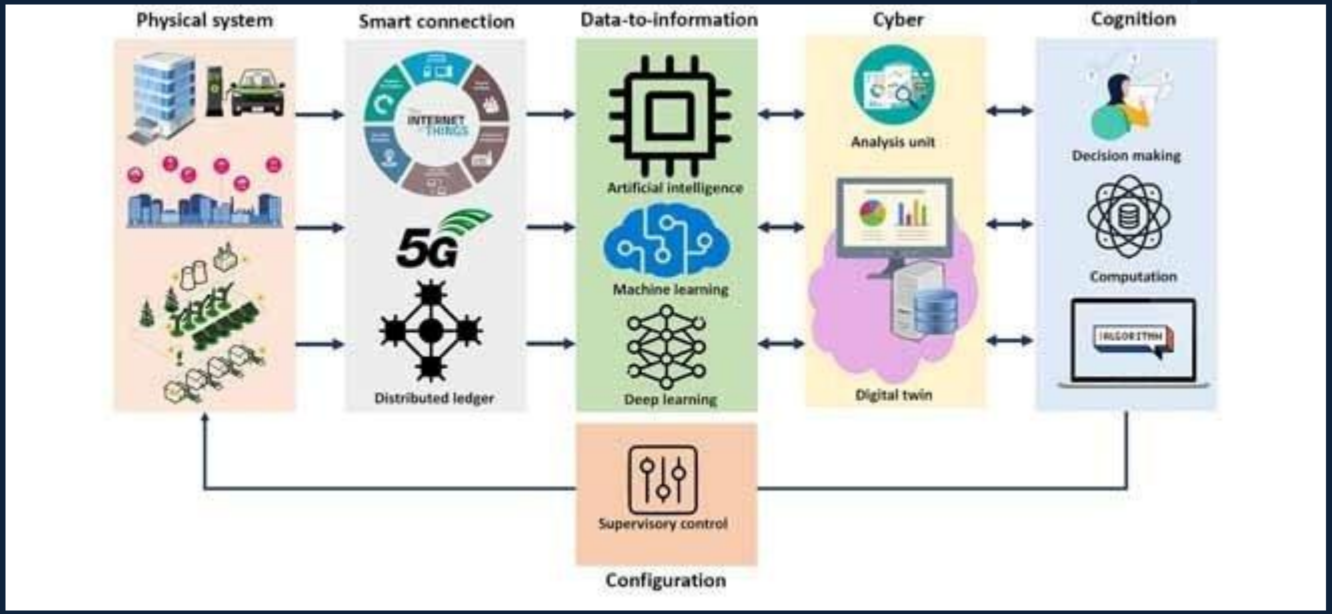


What is Cyber Physical System?

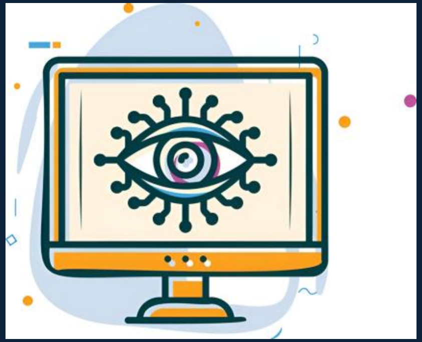
- Integrations of **computation, networking**, and **physical processes**..
- 5G enables CPS to operate in real time with ultra-low latency and high reliability.
- Common in smart grids, healthcare, industrial IoT, autonomous vehicles, and critical infrastructure..

Importance of CPS?

- Critical Infrastructure Backbone
- Healthcare & Life-Critical Systems
- Autonomous & Smart Transportation
- Real-Time Operation Requirements
- Target of Cyber Attacks



Introduction - CNN

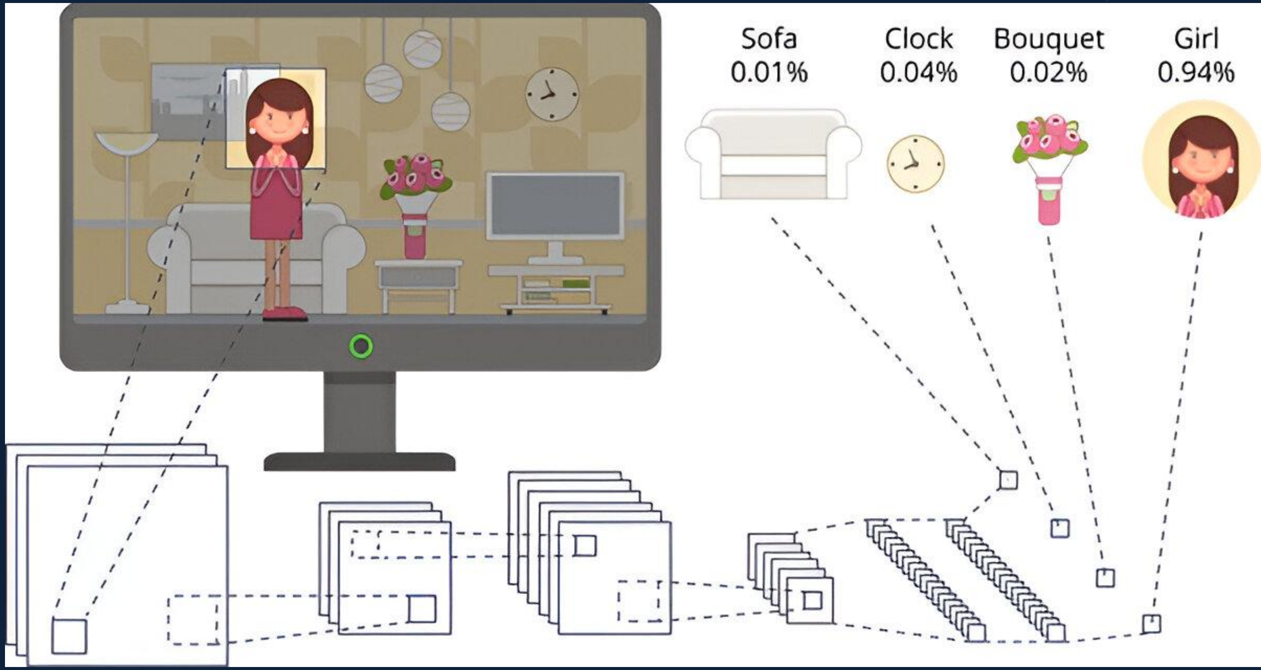


🧠 Why Use Deep Learning (CNN)?

- Traditional ML techniques struggle with **dynamic patterns** in 5G data.
- CNNs can automatically extract **spatial and temporal features** from network traffic.
- Achieve **higher accuracy**, **lower false positives**, and better **generalization**.

🧠 What is CNN?

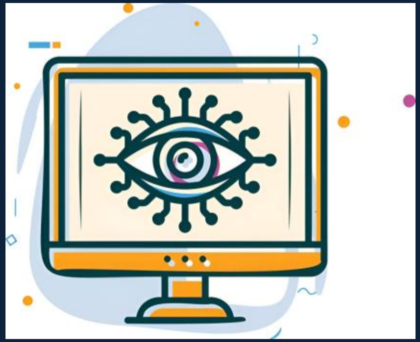
A Convolutional Neural Network (CNN) is a type of deep learning model designed to automatically extract patterns from data originally for images ,but now used widely for network traffic, time-series, and anomaly detection too.



🔍 Key Components of CNN:

Layer	Function
🧱 **Convolution Layer**	Extracts features using filters (kernels) from the input data.
🎛️ **Activation (ReLU)**	Introduces non-linearity (e.g., detects complex attack patterns).
🌀 **Pooling Layer**	Reduces feature size, improves performance, and focuses on key info.
🧩 **Flatten Layer**	Converts feature maps into a 1D vector for prediction.
🎯 **Fully Connected Layer**	Final decision-making (e.g., DDoS = 0, Benign = 1)

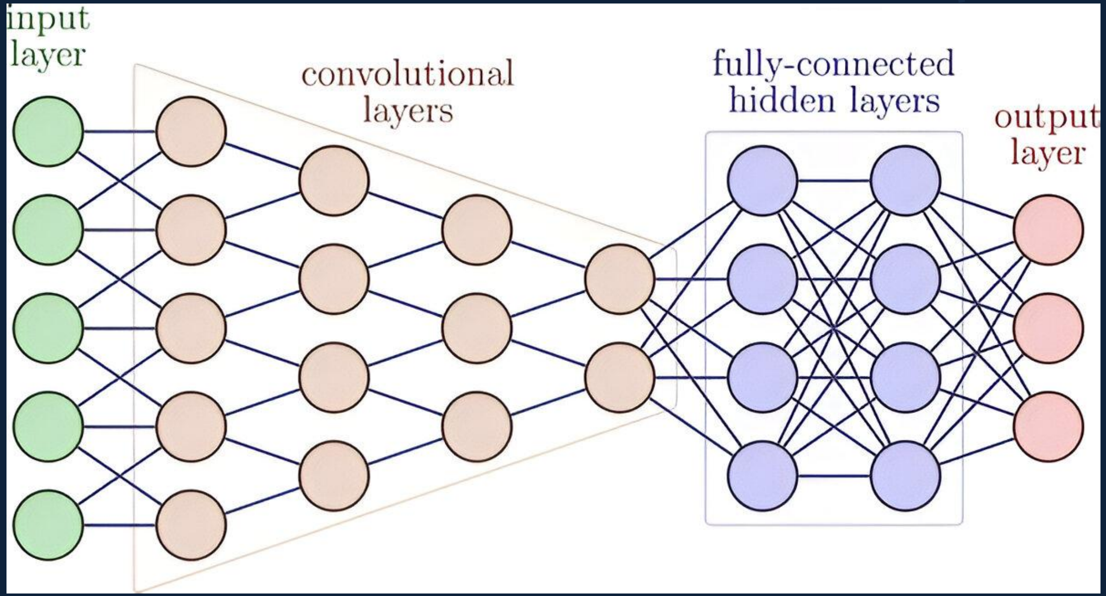
CNN Architecture



1. **Input Layer:**
   - Data: Features extracted from network traffic (e.g., flow duration, packet lengths, protocols).
   - Shape: (number of samples, number of features, 1)
2. **Convolution Layers:**
   - Apply filters (kernels) to extract spatial features from the input.
   - Purpose: Detect patterns like traffic spikes or irregularities, potentially indicating DDoS attacks.
3. **Activation Function (ReLU):**
   - Introduces non-linearity to detect complex patterns that simpler models may miss.
4. **Pooling Layer (Optional):**
   - Reduces spatial dimensions, keeping only essential features.
   - Benefit: Improves performance and reduces overfitting.

CNN Architecture

5. **Flattening Layer:**
   - Converts 2D features (from convolution and pooling) into a 1D vector for classification.
6. **Fully Connected Layer:**
   - Neurons in this layer are connected to all the previous layer's neurons.
   - **Purpose: Final classification (DDoS or benign traffic).**
7. **Output Layer:**
   - Sigmoid activation function for binary classification:
     - ➢ 0 = Attack
     - ➢ 1 = Benign



LSTM Architecture

An advanced Recurrent Neural Network (RNN) variant, excel at capturing long-term dependencies in sequential data, essential for detecting temporal DDoS patterns in 5G traffic.

- Key Components:

▪ Cell State:

✓A persistent memory conduit that retains critical information across time steps, enabling long-term context retention.

▪ Forget Gate:

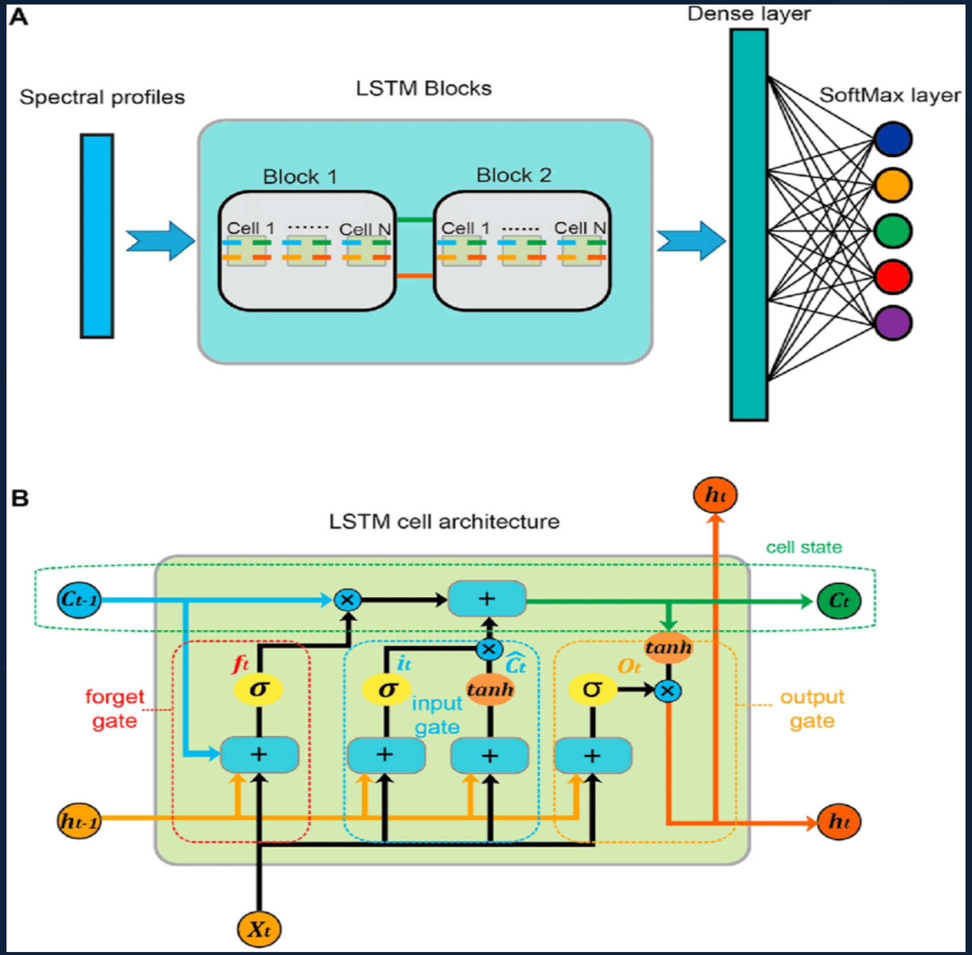
✓Selectively discards irrelevant data using a sigmoid function ($\sigma(W_f * [h_{t-1}, x_t] + b_f)$).

▪ Input Gate:

✓ Regulates new information addition via sigmoid ($\sigma(W_i * [h_{t-1}, x_t] + b_i)$) and tanh ($W\_C * [h_{t-1}, x_t] + b_C$)) activation.

▪ Output Gate:

✓Filters the cell state to produce output using sigmoid ($\sigma(W_o * [h_{t-1}, x_t] + b_o)$) and tanh($C_t$).



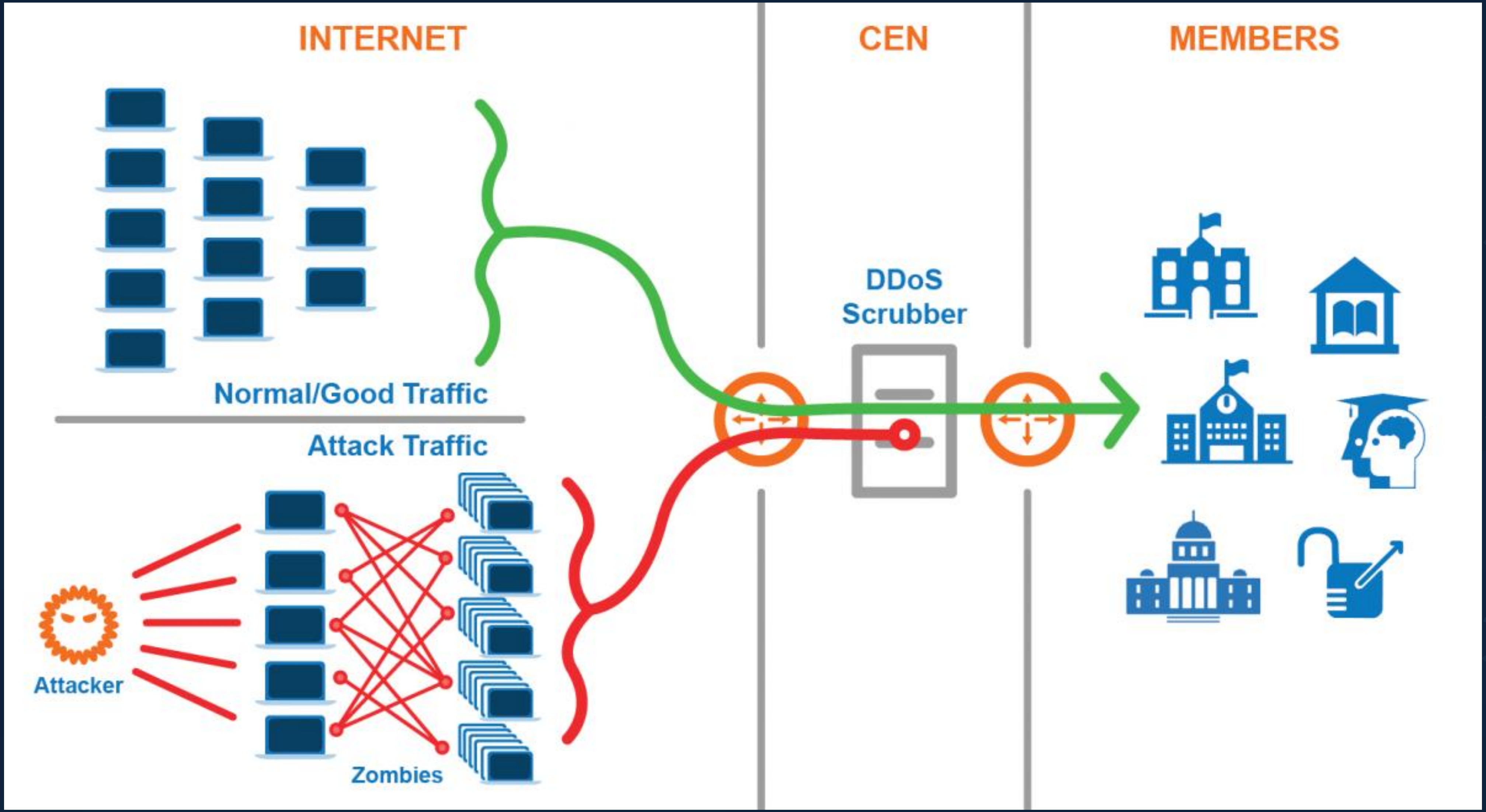
System Architecture and Flowchart

- **Architecture:**
  - Input Layer: Processed 5G traffic features.
  - CNN Layers: Two layers with ReLU activation for feature extraction.
  - LSTM Layer: Sequential modeling of traffic anomalies.
  - Output Layer: Fully connected with softmax for classification.
- **Validation:** Rigorous cross-validation to ensure model robustness.

System Architecture and Flowchart

- **Architecture:**
  - Input Layer: Processed 5G traffic features.
  - CNN Layers: Two layers with ReLU activation for feature extraction.
  - LSTM Layer: Sequential modeling of traffic anomalies.
  - Output Layer: Fully connected with softmax for classification.
- **Validation:** Rigorous cross-validation to ensure model robustness.

How Model Prevents DDoS



Model Training and Optimization

- **Configuration:**
  - **Optimizer:** Adam with adaptive learning rate.
  - **Loss Function:** Binary cross-entropy for two-class classification.
  - **Hyperparameters:** 50 epochs, batch size of 64, dropout rate of 0.2.
- **Regularization:** L2 normalization and dropout to prevent overfitting.

Comparative Project Analysis

- **Project Title**: DDoS Attack Detection for 5G Network Slice using CNN
- **Source**: GitHub Repo - DDoS Attack Detection for 5G Network Slice using CNN https://github.com/sajidkhan2067/DDoSAttackDetectionUsingCNN
- **Objective**: Develop a CNN-based solution for DDoS detection in 5G network slices, achieving >99% accuracy.
- **Dataset**: Custom 10-million-row dataset, accessible via IEEE DataPort (DoS/DDoS Attack Dataset for 5G Network Slicing).

Strengths and Innovations

- **Real-Time Capability**: Sub-millisecond detection latency, optimized for 5G.
- **Scalability**: Handles terabyte-scale traffic in CPS environments.
- **Adaptability**: Evolves with emerging attack signatures.
- **Cyber Security Impact**: Fortifies critical infrastructure resilience.

Limitations and Challenges

- **Data Requirements**: Reliant on large, high-quality labeled datasets.
- **Computational Overhead**: Intensive GPU resources for training and inference.
- **Scope Limitation**: Optimized for specific DDoS variants; broader testing needed.
- **Network Specificity**: Performance unvalidated in non-5G contexts.

Alignment with AML Curriculum

- **Core Topics**:
  - **Deep Learning:** CNN, LSTM (Unit 2: Advanced Neural Networks).
  - **Anomaly Detection:** Cyber security applications (Unit 3: ML in Security).
  - **Data Preprocessing:** Feature engineering (Unit 1: Data Science Foundations).
- **Competencies**:
  - Advanced model design and hyperparameter tuning.
  - Application of ML to solve real-world security challenges.

Future Research Directions

- **Enhancements**:
  - Implement transfer learning for multi-attack detection.
  - Optimize for edge computing in CPS.
- **Applications**:
  - Extend to IoT ecosystems and smart city frameworks.
  - Integrate with proactive intrusion prevention systems.
- **Innovations**:
  - Explore federated learning for privacy-preserving detection.
  - Develop lightweight models for resource-constrained environments.

Conclusion

- **Summary**: The research paper and project showcase pioneering deep learning solutions for DDoS detection in 5G CPS, with accuracies of 98.7% and >99%, respectively.
- **Contribution**: Advances the field of cyber security for next-generation networks.
- **Takeaway**: Deep learning offers a transformative approach to securing critical infrastructures in the 5G era.

References

- Hussain, B., Du, Q., Sun, B., & Han, Z. (2021). "Deep Learning-Based DDoS-Attack Detection for Cyber–Physical System Over 5G Network." *IEEE Transactions on Industrial Informatics*, 17(2), 860-870. DOI: 10.1109/TII.2020.2974520.
- AML Syllabus, National Forensic Sciences University, M.Tech AI & DS (Cyber Security), 2024-26.
- **GitHub Repository:** DDoS Attack Detection for 5G Network Slice using CNN , https://github.com/sajidkhan2067/DDoSAttackDetectionUsingCNN

THANK YOU