VASIREDDY VENKATADRI
INSTITUTE OF TECHNOLOGY

# *I*nternational *C*onference on *A*dvanced *C*omputing *T*echnologies

*[ICACT – 2025]*

# CNN DRIVEN DDoS DETECTION

# A DRILL DOWN ANALYSIS APPROACH

By

Kollapudi Venkata Mani Sai Lokesh, Konchada Rama Krishna,
Kundurthi Khuresh, Mr. M. Jeevan Babu
Dept. Computer Science & Engineering, Vasireddy Venkatadri Institute of Technology, India

# Outline:

- Abstract
- Introduction
- Methods, Implementation
- Results
- Conclusion, Limitations, Future Scope
- References
- Acknowledgements

# ABSTRACT

Volumetric DDoS attacks challenge detection systems due to their sophistication, causing delays and false positives in traditional volume-based analysis. This project proposes a CNN-driven framework, converting network traffic into images for granular pattern analysis. Multi-class classification will progressively identify targeted subnets and IPs.

The methodology involves capturing real-time traffic, converting it to images, and using CNNs for detailed analysis, aiming for real-time, accurate detection. This approach seeks to improve speed and reduce false positives. The project focuses on CNN model development for complex traffic analysis. While challenges exist, the framework aims to provide fine-grained DDoS target identification, enhancing network security

# INTRODUCTION

## Background

- DDoS attacks disrupt services by overwhelming networks.
- Attackers mimic legitimate traffic, making detection challenging.
- The rise of IoT and cloud computing has increased attack sophistication.

## Motivation

- Traditional methods struggle with evolving attack patterns.
- CNNs analyze network traffic as 2D images for better detection.
- A drill-down approach refines detection to pinpoint attack sources.

# INTRODUCTION

## Scope & Contributions

- CNN-based system achieves 97% accuracy in detecting malicious traffic.
- Drill-down approach reduces memory usage and enhances precision.
- Protocol-based classification helps distinguish different attack types.

## Key Features

- Converts raw network traffic into structured images for analysis.
- Classifies attack types by protocol (TCP SYN, UDP flood, ICMP).
- Scalable system efficiently processes high-volume network traffic.

# EXISTING METHODS

## Traditional DDoS Detection Approaches

- **Signature-Based Detection**: Matches traffic against known attack patterns but fails to detect zero-day attacks.
- **Anomaly-Based Detection**: Identifies deviations in network behavior but suffers from high false-positive rates.

## Limitations of the Existing System

- **Scalability Issues**: Struggles with processing large-scale traffic.
- **High Computational Overhead**: Requires extensive processing power, making real-time detection difficult.
- **Slow Response Time**: Delayed detection can cause severe network outages.

# PROPOSED METHOD

**A Drill Down Approach:** Utilizes CNN based learning for hierarchical attack classification.

Addresses limitations of traditional detection methods.

**Key Features**

- **CNN-Based Classification** – CNNs extract complex traffic patterns for accurate detection.
- **Drill-Down Attack Classification** – Classifies attacks into detailed subcategories for better mitigation.
- **Adaptive Learning** – Detects zero-day attacks by continuously learning new traffic patterns.

# PROPOSED METHOD

- **Reduced False Positives** – Differentiates between normal traffic surges and DDoS attacks.
- **Scalability** – Handles high dense and various intense traffic volumes in enterprise and cloud environments.

## ADVANTAGES

- **High Detection Accuracy** – CNNs enhance classification precision.
- **Granular Attack Classification** – Enables detailed attack categorization.
- **Lower False Positives** – Reduces misclassification of legitimate traffic.
- **Scalability** – Supports large-scale SDN networks efficiently.

# IMPLEMENTATION

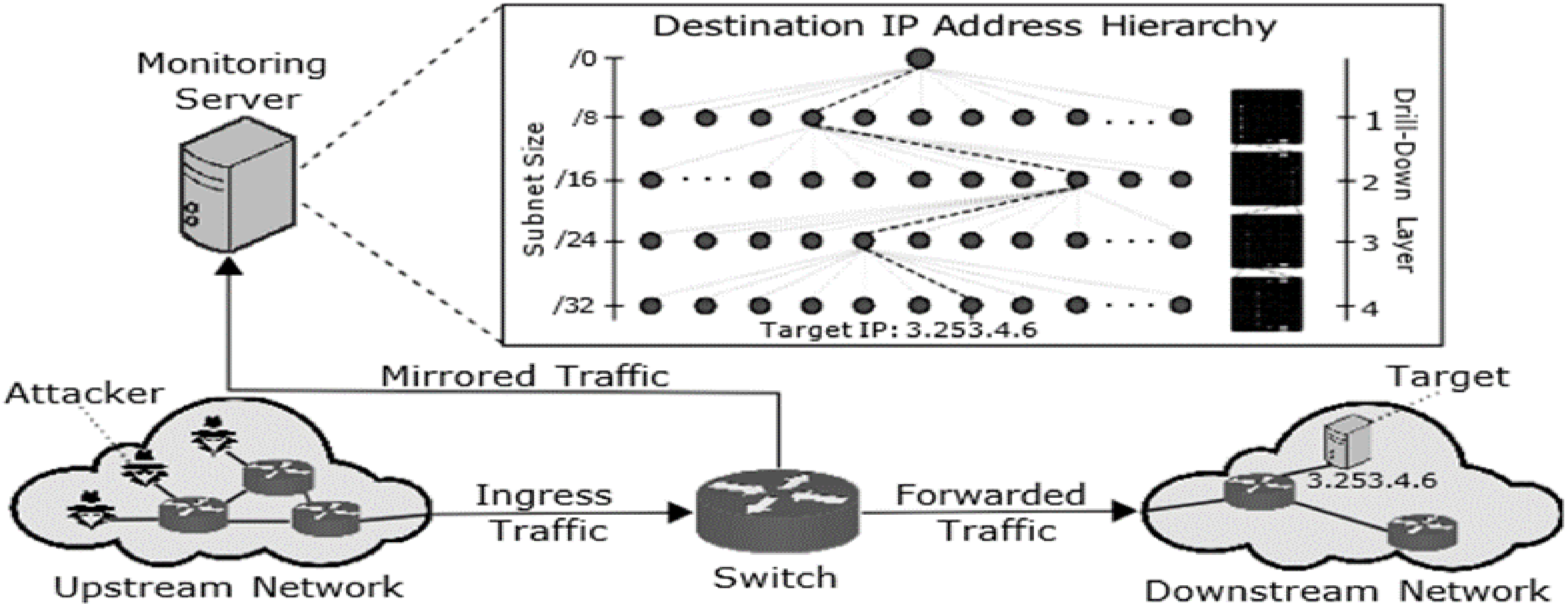
- **Dataset Acquisition:** Analysis of pre-captured network traffic datasets.
- **Feature Extraction :** Filters and extracts relevant network flow parameters.

  *Technologies*: Python, Scikit-learn.
- **Hierarchical CNN-based Classification:** Detects and categorizes different DDoS attack types within the dataset.

  *Technologies:* Python, TensorFlow.
- **Drill-Down Refinement:** Further classifies attack subtypes for targeted analysis.
  - If traffic is classified as malicious, further categorize the attack type.
  - Assign probabilities to each class for improved threat identification.
- **Results Presentation:** Flask API used to visualize the results.

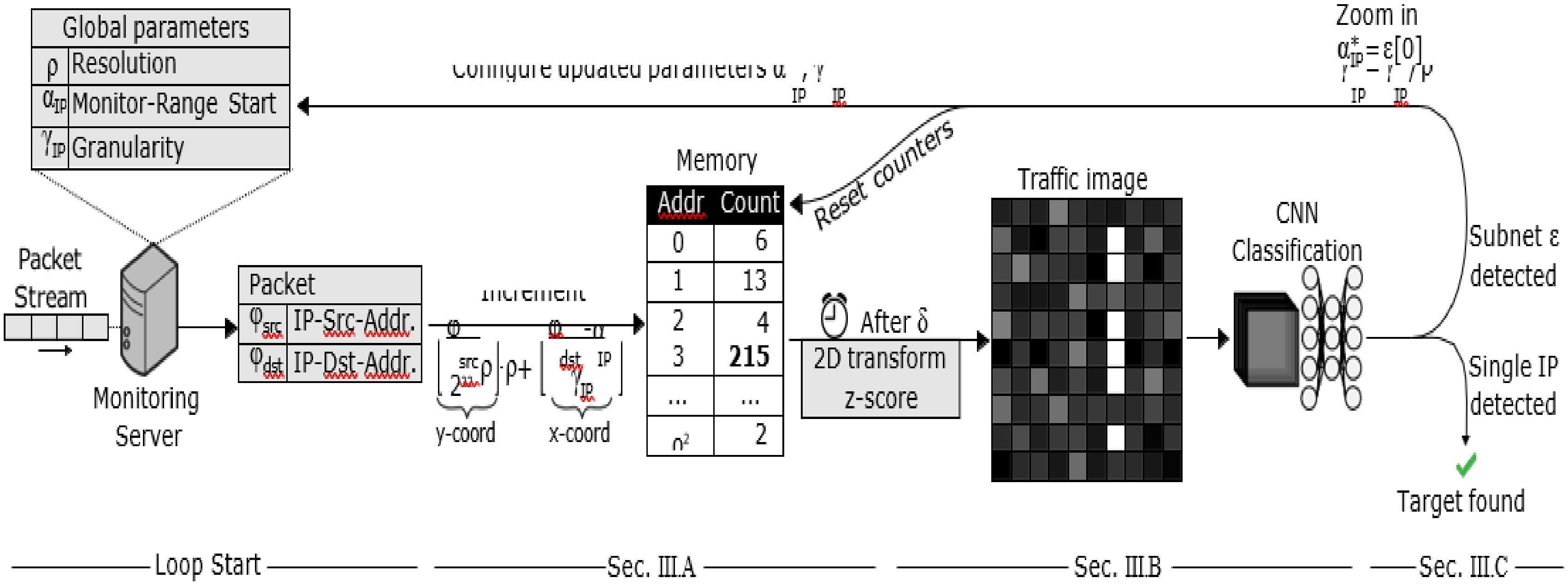
  *Technologies*: Python, Flask.

# IMPLEMENTATION



**Overview of DDoS Detection**

# IMPLEMENTATION



| Global parameters | |
|---|---|
| $\rho$ | Resolution |
| $\alpha_{IP}$ | Monitor-Range Start |
| $\gamma_{IP}$ | Granularity |

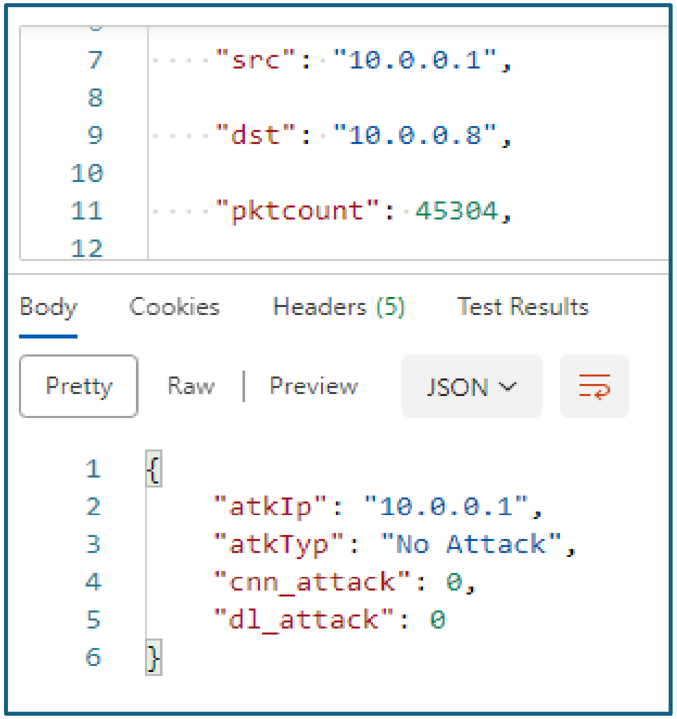
| Packet | |
|---|---|
| $\varphi_{src}$ | IP-Src-Addr. |
| $\varphi_{dst}$ | IP-Dst-Addr. |

Memory

| Addr | Count |
|---|---|
| 0 | 6 |
| 1 | 13 |
| 2 | 4 |
| 3 | **215** |
| ... | ... |
| $\rho^2$ | 2 |

**Drill Down Process**

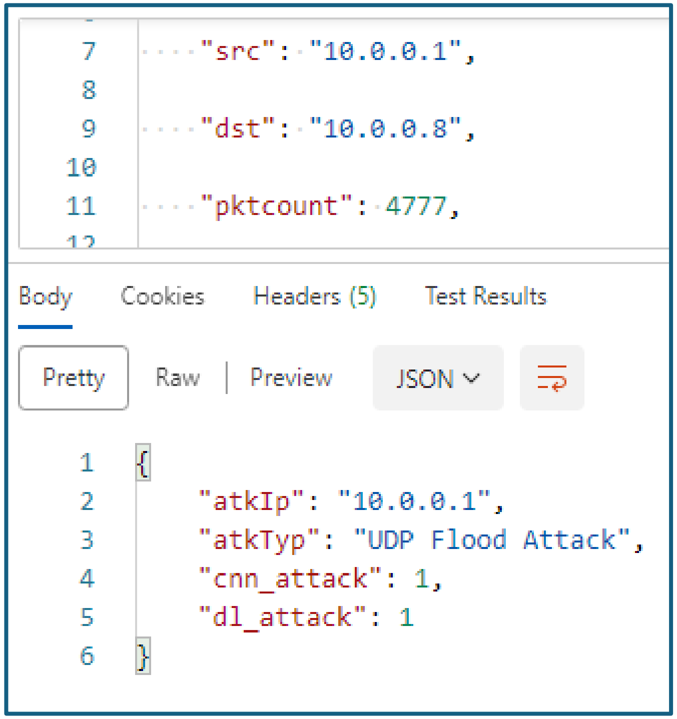
# RESULTS



```
    "src": "10.0.0.1",

    "dst": "10.0.0.8",

    "pktcount": 45304,
```

```
{
    "atkIp": "10.0.0.1",
    "atkTyp": "No Attack",
    "cnn_attack": 0,
    "dl_attack": 0
}
```

**Real Time Attack Prediction (Benign)**

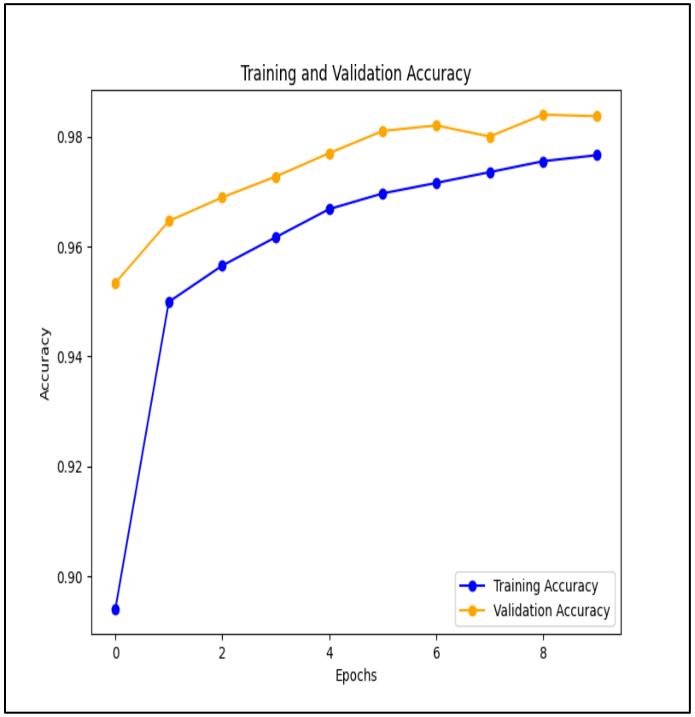


```
    "src": "10.0.0.1",

    "dst": "10.0.0.8",

    "pktcount": 4777,
```

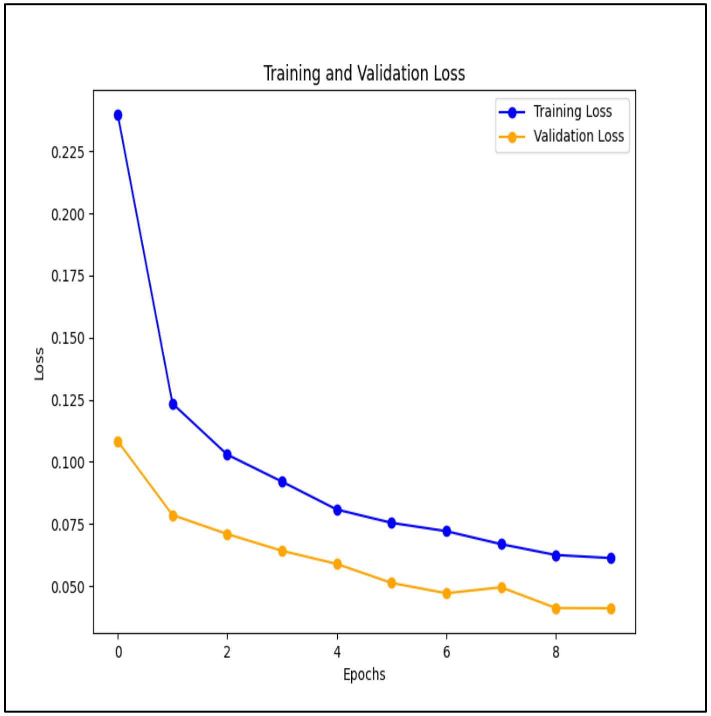
```
{
    "atkIp": "10.0.0.1",
    "atkTyp": "UDP Flood Attack",
    "cnn_attack": 1,
    "dl_attack": 1
}
```

**Real Time Attack Prediction (Malicious)**

# RESULTS

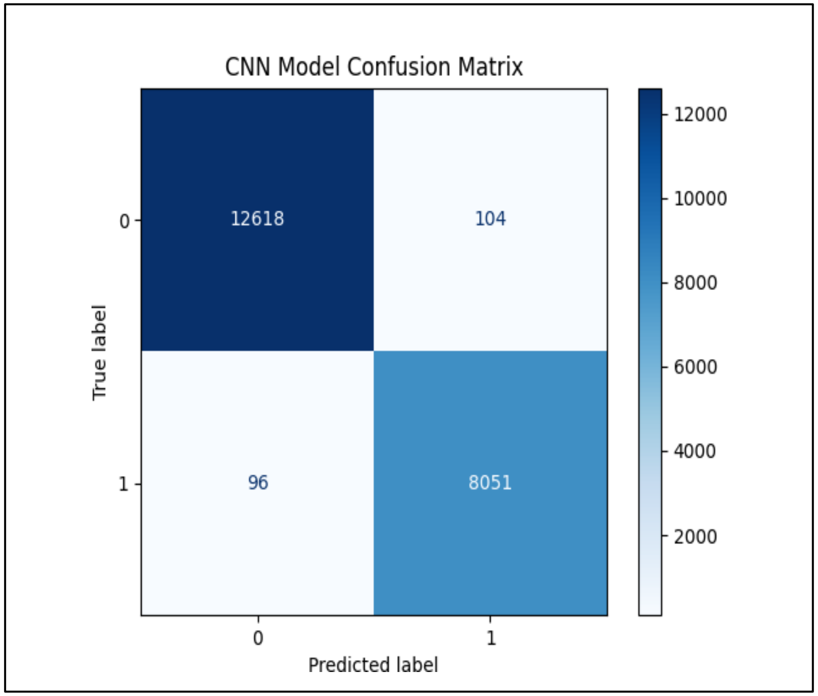


**Model Accuracy Plot**



**Model Loss Plot**

# RESULTS



**Confusion Matrix**

# CONCLUSION

The proposed Drill-Down CNN Model successfully improves accuracy, efficiency, and scalability in DDoS detection within SDN networks. By leveraging deep learning techniques, it eliminates the need for manual feature engineering, achieving fast and precise detection with low false positives.

With continued advancements in federated learning, edge-cloud integration, and explainable AI, the model can be further optimized for large-scale network security. Future enhancements will ensure its applicability in highly dynamic, privacy-sensitive, and real-time cyber defense scenario

# LIMITATIONS

- **Computational Cost:** Deep learning demands high processing power, challenging deployment in resource-limited environments.
- **Data Dependence:** Model accuracy hinges on diverse training data; insufficient data can lead to poor detection of novel attacks.
- **Maintenance Complexity:** Deep learning security systems require specialized expertise for deployment and ongoing updates.
- **Continuous Updates:** Regular model retraining is essential to adapt to evolving cyber threats.

# FUTURE SCOPE

- **Expand Attack Classification:** Incorporate multi-class detection for botnets, spoofing, phishing, and malware, enhancing overall threat coverage.
- **Decentralized Federated Learning (DFL):** Implement peer-to-peer learning via blockchain or gossip protocols for scalable, distributed model updates across SDN nodes.
- **Edge-Cloud Federated Learning:** Integrate edge devices for initial threat filtering with cloud-based advanced model refinement and global knowledge sharing.
- **Explainable AI (XAI):** Enhance model transparency with XAI techniques, providing visual explanations for decisions and improving incident response strategies.

# REFERENCES

- A. Alashhab et al., "Enhancing DDoS Attack Detection and Mitigation in SDN Using an Ensemble Online Machine Learning Model," in IEEE Access, vol. 12, pp. 51630-51649, 2024, doi: 10.1109/ACCESS.2024.3384398.
- H. Liu, Y. Sun, V. C. Valgenti and M. S. Kim, 2011 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2011, pp. 287-291, doi: 10.1109/CCNC.2011.5766474.
- J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in IEEE Access, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

# REFERENCES

- B. Jia and Y. Liang, "Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain," in China Communications, vol. 17, no. 9, pp. 11-24, Sept. 2020, doi: 10.23919/JCC.2020.09.002.
- M. Hassan, K. Metwally and M. A. Elshafey, "ZF-DDOS: An Enhanced Statistical-Based DDoS Detection Approach using Integrated Z-Score and Fast-Entropy Measures," 2024 6th International Conference on Computing and Informatics (ICCI), New Cairo - Cairo, Egypt, 2024, pp. 145-152, doi: 10.1109/ICCI61671.2024.10485097.
- J. Bhayo, S. Hameed and S. A. Shah, "An Efficient Counter-Based DDoS Attack Detection Framework Leveraging Software Defined IoT (SD-IoT)," in IEEE Access, vol. 8, pp. 221612-221631, 2020, doi: 10.1109/ACCESS.2020.3043082.

# ACKNOWLEDGEMENT

I extend my deepest gratitude to all supported this project.

- **Mr. Vasireddy Vidya Sagar, Chairman, VVIT:** For providing vital facilities and resources.
- **Dr. Y. Mallikarjuna Reddy, Principal, VVIT:** For unwavering support throughout the program.
- **Dr. V. Ramchandran, Professor & HOD, CSE, VVIT:** For constant encouragement, motivation, and guidance.
- **Mr. M. Jeevan Babu (Asst. Prof., Project Guide):** For insightful advice, invaluable guidance, and dedicated support.
- **CSE Department, VVIT (Teaching & Non-Teaching Staff):** For their generous assistance and support

# Thanks to All …

# Questions & Answers ?