# Vanshaj Patel

# Student ID: 2517969

# Module: Research Methods and Professional Development

# AI-Driven Intrusion Detection System in Software-Defined Networking (SDN)

Vanshaj Patel | MSc Cyber Security and Digital Forensics | Research Proposal

# Research Background

- Intrusion Detection Systems (IDS) monitor networks for threats
- Software-Defined Networking (SDN) separates control from data plane [2]
- AI/ML enables intelligent threat detection [3]
- Cyber threats growing exponentially


# Problem Statement

- Manual security monitoring is time-consuming
- Slow human response to threats
- High workload in enterprise networks
- Need for intelligent automation

# Proposed System Idea

- AI replaces manual monitoring
- Detects malicious activity automatically
- Takes automatic protective action
- Alerts human analyst if needed

# Research Aim

- Develop AI-driven IDS for SDN environments
- Enable real-time threat detection and response
- Improve detection accuracy and reduce false positives

# Research Objectives

Conduct comprehensive literature review

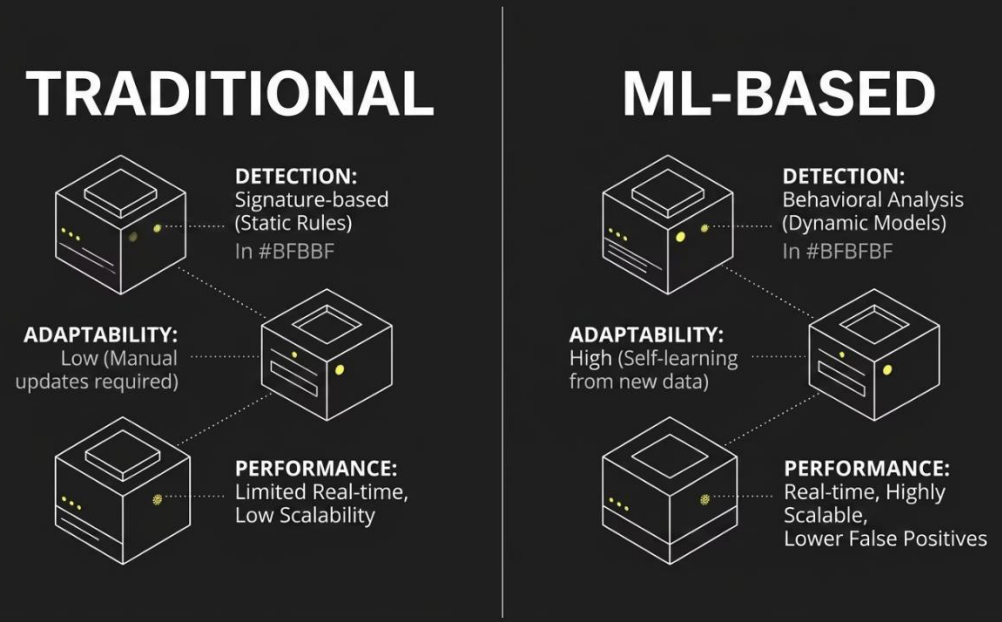
Design and train ML/DL models

Integrate AI model with SDN controller

Evaluate performance metrics and validate

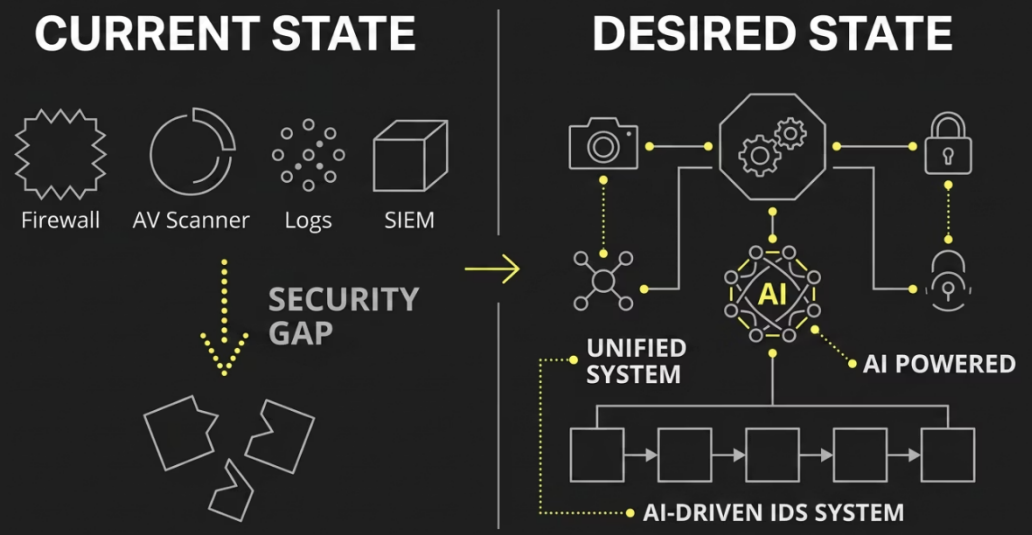
# Literature Insights

- Traditional IDS limited by signature-based detection [1]
- Machine Learning improves detection rates significantly [3]
- Deep Learning achieves high accuracy but high computational cost [1]
- Integration with SDN still emerging



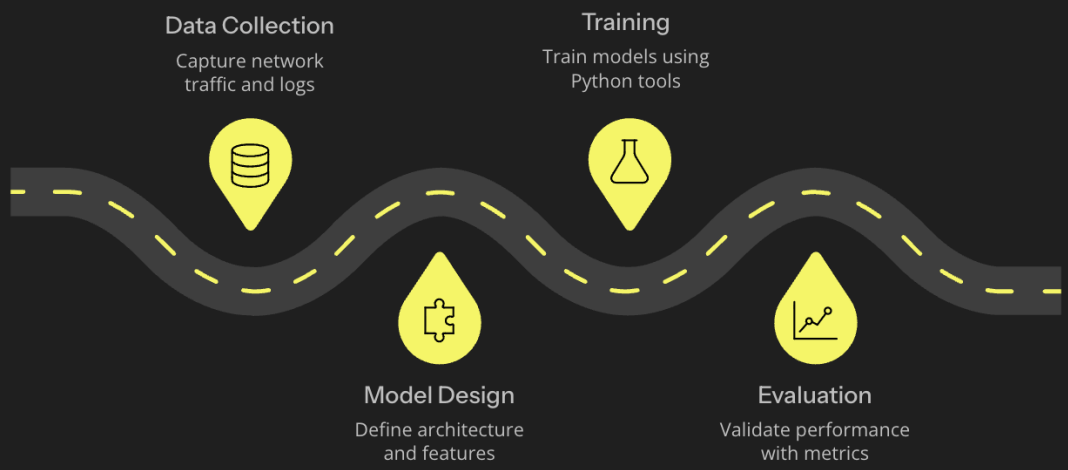
# Research Gap

- No unified AI-IDS framework for SDN [2]
- Lack of real-time automated response mechanisms [6]
- Limited adaptive learning in production environments
- Existing systems lack closed-loop automation (detect → decide → respond)



# Methodology

- Mininet: network simulation environment
- POX: SDN controller framework
- Wireshark: network traffic capture
- Python: AI/ML model development
- Random Forest: robustness with high-dimensional data, minimal overfitting risk [3]

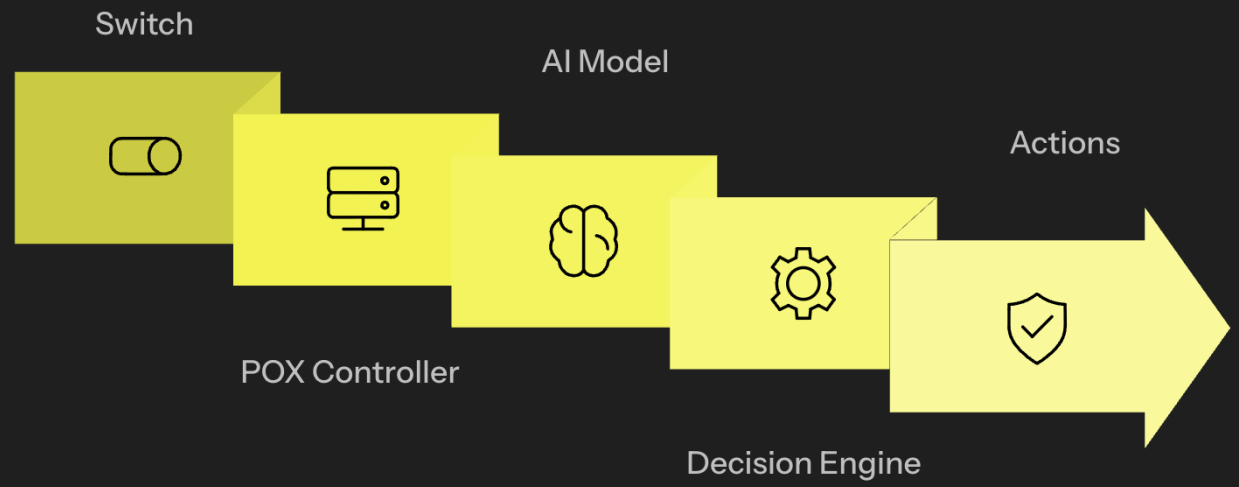


# Training Data & Model

- Use CICIDS2018 and NSL-KDD datasets [4]
- Train on real-world attack patterns
- Improve detection accuracy significantly
- Validate with diverse threat scenarios

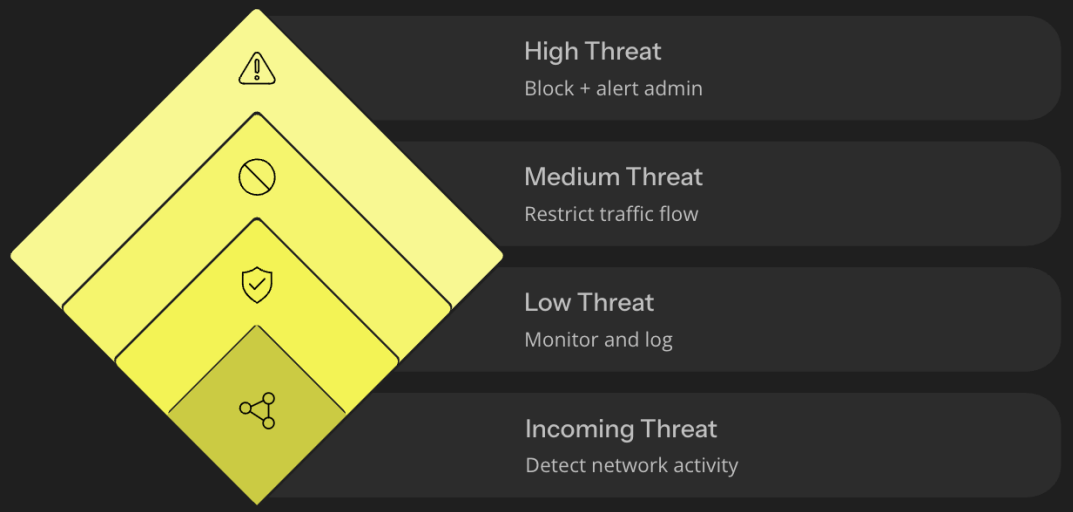
# System Architecture

- Network traffic captured at switches
- POX SDN controller processes packets
- AI model analyzes traffic patterns
- Decision engine determines threat level
- Automatic actions: block, restrict, or monitor



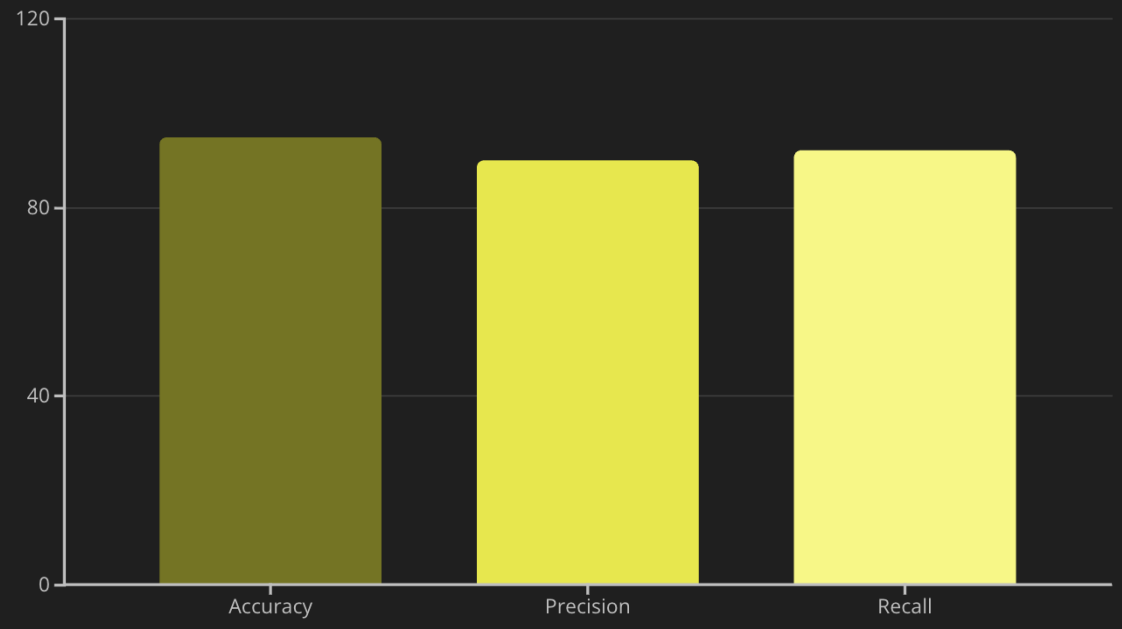
# Decision Logic

- Low threat: monitor and log
- Medium threat: restrict traffic flow
- High threat: block + alert admin



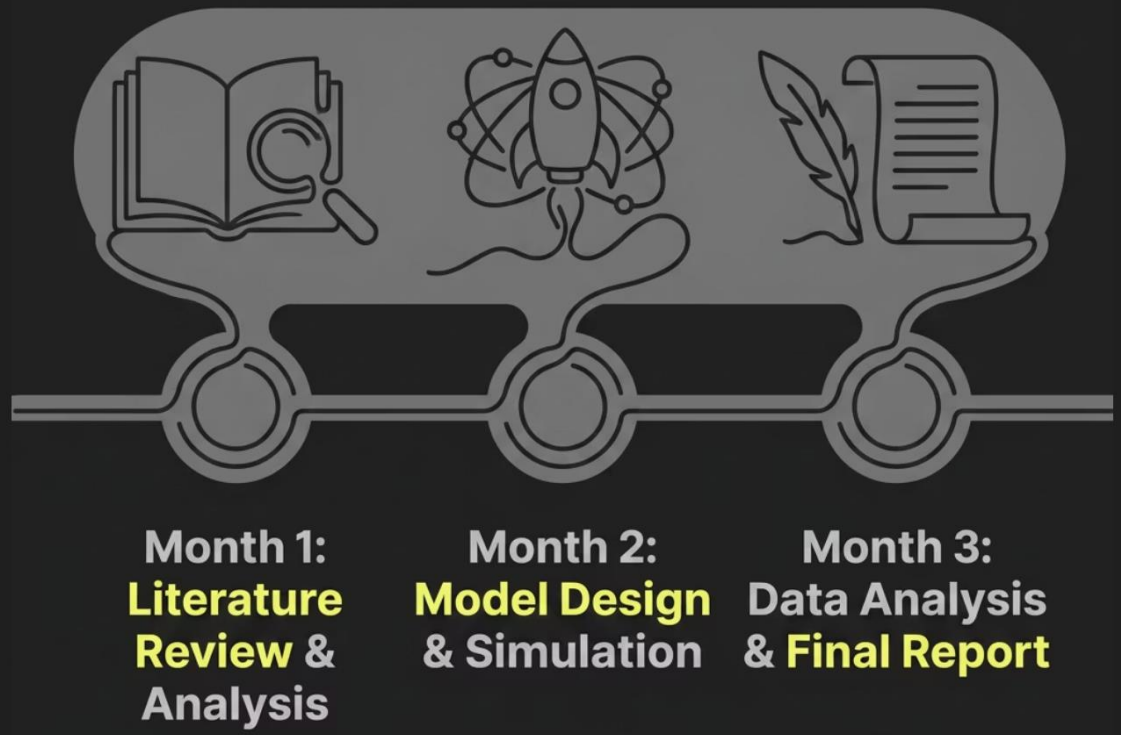
# Evaluation Metrics

- Real-time detection performance
- Response time measurement (milliseconds)
- Accuracy ≥95%, Precision ≥90%, Recall ≥92%
- Compare with traditional signature-based IDS baseline



# Project Timeline

- Month 1: Literature review + SDN setup (Mininet + POX)
- Month 2: Data collection + Model training (Python)
- Month 3: AI-SDN integration + Testing & evaluation



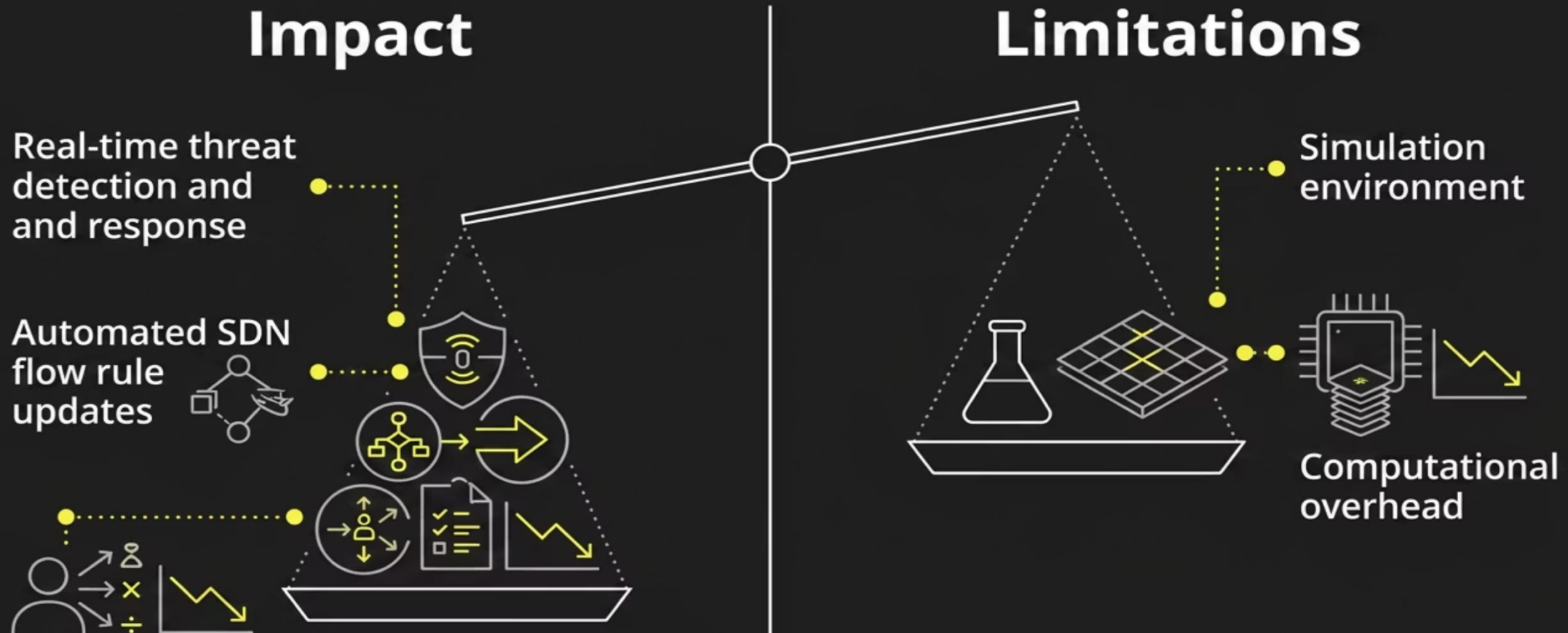
# Impact & Limitations

## Impact

- Reduced human workload significantly
- Faster threat response time
- Intelligent automated security decisions

## Limitations

- Simulation environment (not production)
- Computational overhead on controller



# Conclusion

- AI acts as intelligent security analyst
- SDN enables real-time automated control
- System improves enterprise security posture

# References


1. [1] J. Smith et al., "Deep Learning for Network Intrusion Detection in SDN Environments," Proc. IEEE Conf. on Communications, 2022.
2. [2] A. Gupta and S. Kumar, "Security Challenges and Solutions in Software-Defined Networking," J. Network Security, 2021.
3. [3] M. Chen et al., "Machine Learning-Based Anomaly Detection in Network Traffic," IEEE Trans. on Cybernetics, 2020.
4. [4] I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward a Comprehensive Cyber Security Dataset: A New Approach for Intrusion Detection," Proc. IEEE Symposium on Security and Privacy, 2018.
5. [5] M. Tavallaee et al., "A Novel Dataset for Intrusion Detection Systems," Proc. IEEE Symp. on Computers and Communications, 2009.
6. [6] P. Li and Y. Zhang, "An AI-Driven Intrusion Detection System for Software-Defined Networks," J. Computer Security, 2023.
7. [7] S. Kumar and R. Singh, "Leveraging Deep Learning for Enhanced Intrusion Detection," Int. J. Information Security, 2022.

# Thank You

Stay tuned for something amazing coming in a few months!