CS 258-01 Data Communication System

Points: 5 Instructor: Prof. Navrati Saxena

END-TERM RESEARCH PLAN

Group Information: Max 2 students in a group

#	Student's Name	Student ID
1	Xiangyi Li	017415996
2		

1. Topic: Leveraging AI/ML for Proactive Anomaly Detection and Self-Healing in Software-Defined Networks (SDN).

2. Sub-topic:
Developing an Integrated AI/ML Framework for Enhanced SDN Security and Resilience.

3. Problem statement:
Software-Defined Networks (SDNs) offer significant advantages in network management but are also vulnerable to sophisticated cyber threats (like DDoS attacks) and internal system faults. Traditional security measures often struggle to provide rapid and adaptive responses. Anomalies can lead to severe performance issues, data breaches, and service interruptions. There's a pressing need for intelligent, automated systems that can proactively identify, diagnose, and respond to these challenges in real-time to maintain network integrity and operational continuity.

4. Motivation:

The increasing reliance on complex network infrastructures across critical sectors, coupled with the escalating sophistication of cyber threats, underscores the importance of robust network security and resilience. Applying Artificial Intelligence (AI) and Machine Learning (ML) to SDNs presents a powerful opportunity to build more adaptive, efficient, and self-sufficient network management systems. This research is driven by the potential to enhance security, improve operational efficiency, and reduce the need for manual intervention in managing network faults and responding to threats.

a. Why you are interested in this topic
The application of AI/ML in SDNs offers a novel approach to address complex networking challenges, providing an opportunity to explore cutting-edge solutions for enhanced network performance and security.

b. Why is this topic and the problem statement important for us in particular and for the society as a whole

For us, as students of Data Communication Systems, understanding and contributing to such advanced networking paradigms is crucial. For society, more resilient and secure network infrastructures are vital for everything from daily communication to critical services, making research in this area highly impactful.

5. Objective:

The core objective is to conceptualize and outline an integrated AI/ML framework designed to:

- Proactively detect anomalous network traffic patterns and potential security threats within an SDN environment.
- Automatically diagnose the nature and origin of detected anomalies or system faults.
- Initiate automated self-healing processes to mitigate issues and restore normal network operations with minimal human oversight.
- Enable the system to learn from historical data and past incidents to continuously improve its detection accuracy and response effectiveness.

The research will also explore suitable AI/ML algorithms and architectural considerations for such a framework.

6. Timeline:

Conceptual Timeline & Research Approach (Leading to Presentation):

Activity	**April 07 2025**					**April 28 2025**
Comprehensive Literature Review	Weeks 1-3					
Framework Design		Weeks 4-6				
Elaboration of Key Mechanisms			Weeks 7-9			
Evaluation Strategy and Metrics Definition				Weeks 10-11		
Presentation Preparation					Weeks 12-14	
Finalization and Rehearsal						Presentation Period

7. References:

1. Latif, Z., Umer, Q., Lee, C., Sharif, K., Li, F., & Biswas, S. (2022). A Machine Learning-Based Anomaly Prediction Service for Software-Defined Networks. Sensors, 22(21), 8434.

2. Alviz-Meza, A., Sossa-Sarmiento, A. H., & Villalba, L. J. G. (2024). Software defined network and artificial intelligence applied to IoT security. Journal of Network and Computer Applications, 227, 103912.
3. Perumallaplli, R. (2025). Self-Healing Networks: An AI Approach to Network Fault Management. SSRN Electronic Journal.
4. Santhosh K, Gary D. (2023). Self-Healing Networks: Implementing AI-Powered Mechanisms to Automatically Detect and Resolve Network Issues with Minimal Human Intervention. International Journal of Scientific Research and Engineering Development, 6(6).
5. Bhattacharya, A., & Thapliyal, H. (2024). Machine Learning and Deep Learning Approaches for Security and Trust in SDN and NFV: A Survey. IEEE Access, 12, 10418-10449.
6. (Additional relevant academic papers and key industry whitepapers will be added as research progresses)