THESIS INFORMATION

Title: **ENHANCING DEFENSE CAPABILITY AGAINST CYBER-ATTACKS IN SDN-BASED NETWORKS**

Major Code: **Information Technology**

Code: **9480201**

PhD Student: **PHAN THẾ DUY**

Supervisors: **PhD. PHẠM VĂN HẬU, Assoc. Prof. PhD. LÊ ĐÌNH DUY**

University: **UNIVERSITY OF INFORMATION TECHNOLOGY, VIETNAM NATIONAL UNIVERSITY-HCM**

ABSTRACT

The dissertation investigates and develops a federated intrusion detection and threat hunting framework for Software-Defined Networking (SDN) through the Federated Learning (FL) model. This approach enhances the effectiveness of detecting and mitigating emerging cyber-attacks in distributed SDN environments, where multiple organizations participate. In this model, training clients represent entities in the federated learning system, such as training machines managed by Security Operation Centers (SOCs) operating SDN environments. The deployment of Federated Learning-based Intrusion Detection Systems (FL-IDS) provides significant advantages in protecting sensitive data but also faces security weaknesses and challenges from untrusted participants. Therefore, the dissertation focuses on reinforcing key security aspects in the development of FL-based IDS frameworks, leveraging the advantages of FL for data privacy protection while addressing critical security challenges in FL-based systems within the cybersecurity landscape.

The dissertation achieves four key contributions, including:

1. Enhancing resistance against Privacy Attacks through a trust and privacy-preserving mechanism
    - The dissertation proposes a mechanism to ensure trustworthiness and privacy protection during federated machine learning training for intrusion detection and threat hunting applications in SDN networks.
    - This solution prevents sensitive data sharing and ensures secure aggregation of model updates from multiple sources.
2. Enhancing resistance against Poisoning Attacks through a detection and mitigation solution for federated intrusion detection models
    - The dissertation introduces a method to prevent global model poisoning attacks by analyzing the latent space of updates from local training clients, improving the security of federated machine learning models.
3. Enhancing resistance against Evasion Attacks through robustness evaluation and adversarial resilience mechanisms for intrusion detection systems

- The dissertation develops a model using adversarial networks to generate new attack samples, thereby evaluating and ensuring effective detection and mitigation of attacks.
- This contributes to strengthening the robustness of IDS systems in SDN networks.

4. Enhancing resistance against Abuse Attacks from untrusted network applications with a decentralized access control model for SDN applications
    - The dissertation proposes and experiments with a blockchain-based access control model to securely manage access rights and ensure security during network state monitoring and data collection.

These contributions not only improve the effectiveness of cyber-attack prevention in SDN-based networks but also reinforce security and information protection in multi-organizational network environments with collaborative participation.

During the implementation and completion of the dissertation, the Ph.D. candidate has published eight scientific papers, including five papers in reputable journals (05 SCIE Q1-ranked journals) and three scientific papers presented at prestigious international conferences.

Supervisors		**PhD Student**
Phạm Văn Hậu	**Lê Đình Duy**	**Phan Thế Duy**