# A SEQUENTIAL DEEP LEARNING FRAMEWORK FOR ROBUST AND RESILIENT NETWORK INTRUSION DETECTION SYSTEM

**Hai Nguyen Duy**

[1] University of Information Technology, Ho Chi Minh City, Vietnam
[2] Vietnam National University, Ho Chi Minh City, Vietnam

### What ?

- **Context:** Modern cyberattacks (e.g., APTs, Polymorphic Malware) are increasingly sophisticated, stealthy, and persistent.
- **Existing Problems:**

+ Lack of Context: Traditional NIDS process discrete packets, failing to detect sequential patterns.

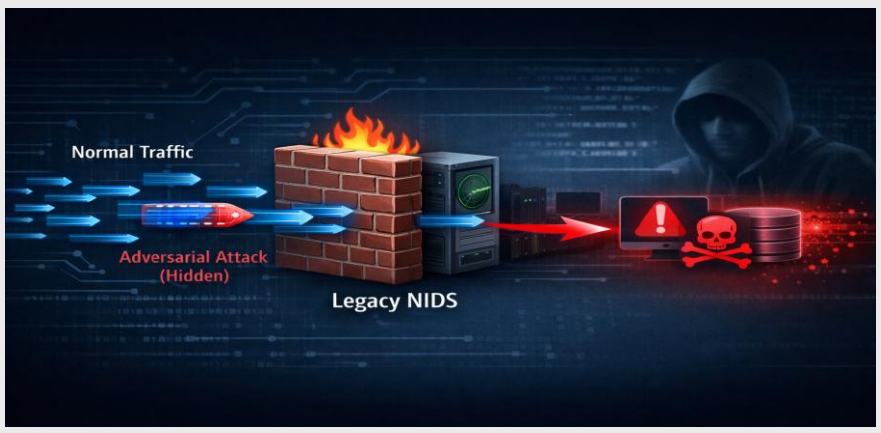
+ AI Vulnerability: Deep Learning models are highly susceptible to Adversarial Examples—minor input perturbations can cause misclassification.

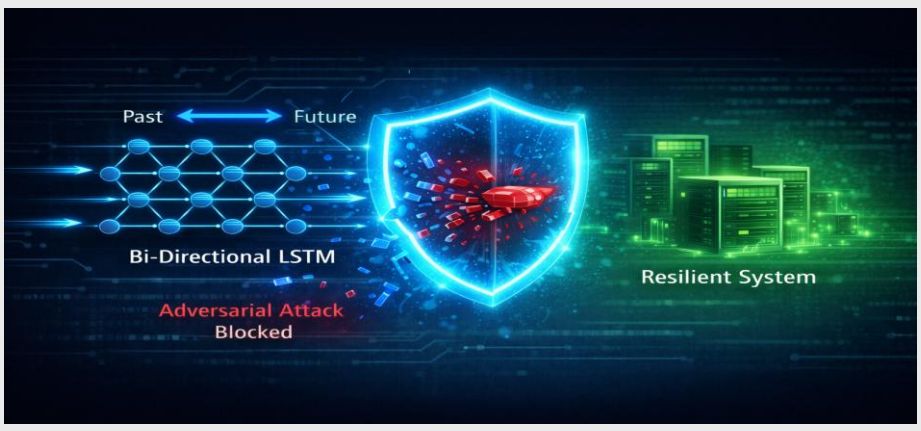
### Why ?

- **Bi-LSTM Model:** Detects sequential patterns (past & future).
- **Resilient Defense:** Uses **Adversarial Training** to resist attacks.
- **Validation:** Verified on **CIC-IDS-2017** & **FGSM**.

## Overview

This research addresses critical vulnerabilities in modern Network Intrusion Detection Systems (NIDS). We propose a novel Sequential Deep Learning framework that not only detects sophisticated cyberattacks using contextual patterns but also defends against Adversarial Examples, ensuring both high accuracy and system resilience




## Description

### 1. Research Objectives

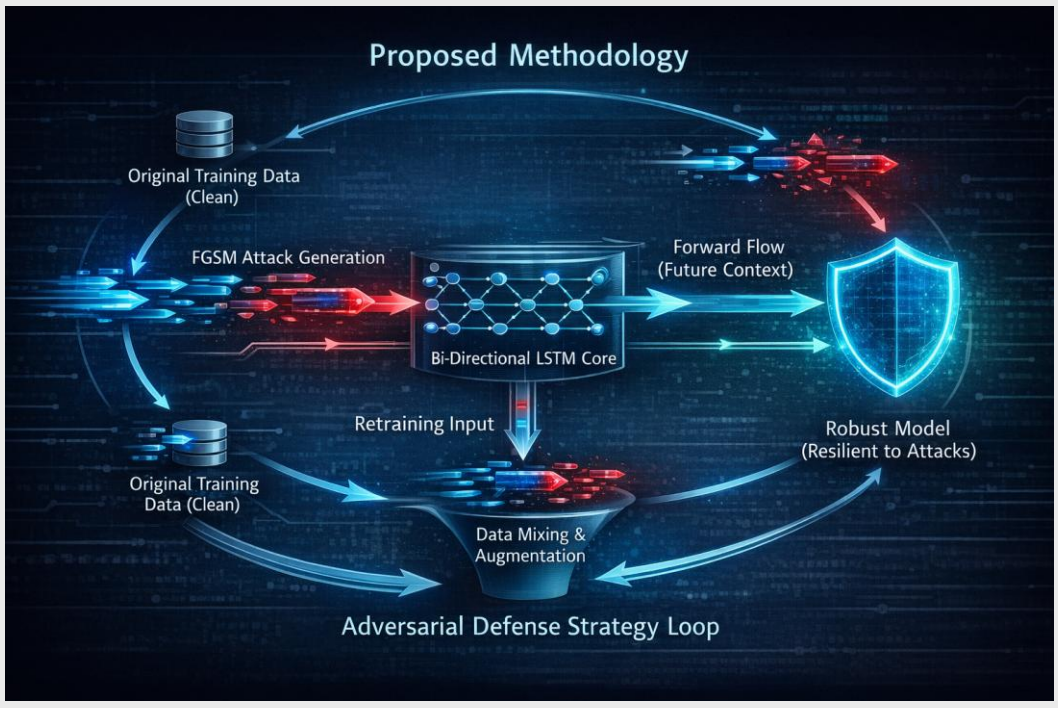
- **Build Bi-LSTM Framework:** Leverage Bi-Directional LSTM to capture temporal context and sequential patterns in network traffic.
- **Enhance Resilience:** Integrate **Adversarial Training** to defend against evasion attacks (e.g., FGSM) and improve model robustness
- **Evaluate Performance:** Validate the system's accuracy and resilience on the **CIC-IDS-2017** dataset.

### 2. Proposed Methodology

- **Sequential Architecture:** Utilize **Bi-Directional LSTM** to capture time-series dependencies in both forward and backward directions of network traffic
- **Adversarial Defense Strategy:** Implement an **Adversarial Training** loop: Generate FGSM attack samples → Mix with training data → Retrain model to immunize against perturbations.

### 3. Key Contributions

- **Resilient NIDS Framework:** A novel framework that successfully combines **contextual awareness** (Deep Learning) with **active defense** (Adversarial Robustness).
- **Superior Performance:** Achieves **F1-Score > 95%** on benign traffic and maintains **> 85% Accuracy** under FGSM attacks (significantly outperforming traditional models).




Hai Nguyen Duy – University of Information Technology, Ho Chi Minh City, Vietnam
TEL : 0972181089 Email : haingd.20@grad.uit.edu.vn