DANH SÁCH KHÓA LUẬN KỸ SƯ NGÀNH ATTT - HỌC KỲ 2 NĂM HỌC 2025 - 2026

STT	Tên đề tài	Yêu cầu	GVHD	Email	Bộ môn	Định hướng đề tài (Ứng dụng, Nghiên cứu, Kết hợp, MMT)	Ghi chú
1	Phát hiện mã độc dựa trên đặc trưng hành vi sử dụng mạng học sâu.	- Cài đặt và sử dụng các công cụ thu thập và phân tích lưu lượng mạng nhằm phục vụ việc nghiên cứu hành vi giao tiếp mạng của mã độc và phần mềm hợp lệ, chẳng hạn như Wireshark, tcpdump, Argus hoặc các môi trường phân tích mã độc an toàn (sandbox). - Sử dụng các tập dữ liệu mạng công khai hoặc dữ liệu luồng mạng đã được xây dựng sẵn từ các nguồn uy tín để phục vụ cho quá trình huấn luyện và đánh giá mô hình phát hiện mã độc. - Thực hiện các bước tiền xử lý dữ liệu, bao gồm làm sạch, chuẩn hóa và trích xuất đặc trưng hành vi từ dữ liệu lưu lượng hoặc luồng mạng nhằm biểu diễn hiệu quả hoạt động mạng của đối tượng phân tích. - Xây dựng và huấn luyện mô hình học sâu phù hợp cho bài toán phân loại mã độc dựa trên hành vi sử dụng mạng, sử dụng các thư viện học sâu phổ biến như PyTorch hoặc TensorFlow. - Đánh giá hiệu quả của mô hình thông qua các chỉ số phổ biến trong lĩnh vực an toàn thông tin như Accuracy, Precision, Recall, F1-score và ROC-AUC. - So sánh mô hình học sâu đề xuất với một số mô hình học máy và học sâu cơ sở nhằm làm rõ ưu điểm và hạn chế của từng phương pháp. - Xây dựng chương trình hoặc mô hình minh họa (demo) nhằm kiểm chứng khả năng ứng dụng thực tế của phương pháp phát hiện mã độc dựa trên phân tích hành vi mạng.	Hồ Hải Quân	quanhh@huit.edu.vn	MMT&ATTT	Nghiên cứu	
2	Nghiên cứu xây dựng cơ chế Mã hóa Thích ứng (Adaptive Encryption), tối ưu hóa năng lượng và bảo mật cho các thiết bị IoT biên	- Nghiên cứu các chuẩn mã hóa hạng nhẹ (Lightweight Cryptography - LWC) hiện hành (như SIMON, SPECK, ASCON, PRESENT) và so sánh với chuẩn truyền thống (AES). - Đánh giá chi phí năng lượng và tài nguyên phần cứng của từng thuật toán để tạo cơ sở dữ liệu cho bộ quyết định. - Thiết kế thuật toán/logic chuyển đổi chế độ mã hóa dựa trên các tham số đầu vào động: Mức năng lượng còn lại của thiết bị (%), Độ quan trọng của gói tin, và Điều kiện mạng. - Xây dựng mô hình máy trạng thái (State Machine) cho thiết bị IoT để quản lý việc chuyển đổi giữa các mức độ bảo mật (Cao - Trung bình - Thấp). - Hiện thực hóa giải pháp trên nền tảng phần cứng vi điều khiển phổ biến (như ESP32 hoặc STM32). - Xây dựng mô hình mạng đơn giản (gồm Sensor Node và Gateway) để demo luồng dữ liệu được mã hóa động. - Đo lường thực tế mức tiêu thụ năng lượng, thông lượng (throughput) và độ trễ (latency) trong các kịch bản khác nhau. - So sánh hiệu quả năng lượng giữa giải pháp đề xuất (Adaptive) và giải pháp tĩnh (chỉ dùng AES hoặc chỉ dùng LWC)	Đinh Huy Hoàng	hoangdhuy@huit.edu.vn	MMT&ATTT	Nghiên cứu	
3	Nghiên cứu xây dựng hệ thống phát hiện xâm nhập mạng dựa trên cơ chế Self-Attention và kiến trúc Transformer	- Dữ liệu (Dataset): Sử dụng tập dữ liệu CIC-IDS2017 hoặc UNSW-NB15. - Nghiên cứu chuẩn hóa (Normalization), xử lý dữ liệu thiếu, và đặc biệt là kỹ thuật SMOTE để cân bằng dữ liệu (vì mẫu tấn công thường ít hơn mẫu bình thường). - Nghiên cứu và xây dựng cơ chế kiến trúc transformer (IDS-TRANSFORMER). - Huấn luyện, đánh giá & so sánh độ chính xác (Accuracy), F1-Score với các thuật toán truyền thống (Random Forest, SVM) - Yêu cầu lập trình: Ngôn ngữ Python, thư viện PyTorch hoặc TensorFlow.	Ngô Quốc Huy	huynq@huit.edu.vn	MMT&ATTT	Nghiên cứu	

4	Xây dựng tập dữ liệu WiFi Fingerprinting có bảo vệ quyền riêng tư bằng Differential Privacy	- Xây dựng phương pháp tạo tập dữ liệu ngoại tuyến WiFi Fingerprinting có bảo vệ quyền riêng tư bằng Differential Privacy, đồng thời tối ưu hóa độ chính xác của các mô hình định vị được huấn luyện trên dữ liệu đó. - Cài đặt thuật toán: Differential Privacy cho fingerprint DB; - Đánh giá kết quả thực nghiệm: so sánh kết quả định vị với dữ liệu gốc. - Các chỉ số đánh giá: Sai số định vị, accuracy loss, privacy budget	Nguyễn Hữu Khánh	khanhnh@huit.edu.vn	MMT&ATTT	Nghiên cứu	
5	Định vị trong nhà dựa trên WiFi Fingerprinting có bảo vệ quyền riêng tư người dùng bằng Differential Privacy	- Xây dựng mô hình định vị trong nhà dựa trên WiFi Fingerprinting, trong đó dữ liệu RSSI của người dùng được bảo vệ bằng Differential Privacy trước khi sử dụng cho bài toán định vị. - Cài đặt thuật toán: Áp dụng Local Differential Privacy trực tiếp lên RSSI của người dùng trong pha định vị trực tuyến; - Đánh giá kết quả thực nghiệm: so sánh kết quả định vị trước và sau khi cải tiến. - Các chỉ số đánh giá: Sai số định vị, accuracy loss, privacy budget	Dương Bảo Ninh	ninhdb@huit.edu.vn	MMT&ATTT	Nghiên cứu	
6	Nghiên cứu và triển khai AI-Driven NAC tự động hóa qui trình giám sát và cách ly mối đe dọa trong môi trường mạng doanh nghiệp	1. Xây dựng hệ thống Network Access Control (NAC) mã nguồn mở để phát hiện và cách ly thiết bị lạ/nhiễm mã độc trong mạng LAN 2. Phân tích, đề xuất và cấu hình các chính sách chặn/không chặn các máy có hành vi bất thường và tự động cách ly/chặn 3. Bài toán đặt ra là nếu máy, thiết bị đáp ứng chính sách và không bị cách ly và phát sinh hành vi bất thường ngoài chính sách thì hệ thống NAC sẽ không chặn, cần xây dựng một AI NAC thích ứng để tăng cường tính năng NAC 4. Yêu cầu kiến thức: sinh viên cần có kiến thức chuyên sâu về mạng, hạ tầng mạng, quản trị mạng windows, cấu hình thành thạo hệ điều hành máy chủ Windows/Linux, hệ thống ảo hóa, thành thạo lập trình Python và an hiểu các thuật toán nhằm triển khai được AI Engine 5. Yêu cầu cài đặt gồm có: + Giả lập máy chủ, dịch vụ mạng, thiết bị mạng, máy người dùng, thiết bị mạng trường hợp bình thường và bất thường trên EVE-NG hoặc GNS3, và triển khai bộ Controller, Collector, AI Engine + NAC Controller : PacketFence + Data Collector: Zeek hoặc tương đương + AI Engine: sinh viên ứng dụng Unsupervised Learning (như Isolation Forest hoặc K-Means) để phát hiện điểm bất thường	Nguyễn Quốc Sử	sunq@huit.edu.vn	MMT&ATTT	Ứng dụng	
7	Thiết kế và Triển khai hệ thống bảo mật đa lớp cho doanh nghiệp tích hợp trí tuệ nhân tạo (AI) trong giám sát và phát hiện tấn công	Xây dựng một hệ thống mạng doanh nghiệp giả lập an toàn, có khả năng phòng thủ chiều sâu (Defense in Depth) và sử dụng AI để phát hiện các bất thường mà các công cụ truyền thống bỏ sót. Tích hợp tối thiểu 03 giải pháp bảo mật: - Triển khai Next-Generation Firewall (NGFW) tích hợp chức năng IDS/IPS (Suricata/Snort) để kiểm soát ra/vào và ngăn chặn xâm nhập mạng. - Triển khai Web Application Firewall (WAF) (ví dụ: ModSecurity/Coraza) để bảo vệ ứng dụng web khỏi các lỗ hổng phổ biến (OWASP Top 10). -Triển khai hệ thống SIEM (Security Information and Event Management) để thu thập log tập trung, giám sát toàn vẹn file (FIM) và phát hiện mã độc trên các máy trạm (Endpoint). - Xây dựng module Machine Learning, học dữ liệu log từ SIEM (Wazuh) hoặc lưu lượng mạng để phát hiện các mẫu tấn công bất thường (Anomaly Detection) mà tập luật (Rule-based) của Firewall/WAF chưa phát hiện được. - Giả lập tối thiểu 03 tình huống bất thường: + Tấn công lớp ứng dụng: Hệ thống WAF phát hiện và chặn, AI phân tích log à cảnh báo + Tấn công mã độc/Ransomware: + Tấn công từ chối dịch vụ (DdoS)	Trần Thị Bích Vân	vanttb@huit.edu.vn	MMT&ATTT	Ứng dụng	
8	Nghiên cứu phương pháp phát hiện website phishing sử dụng mô hình học sâu kết hợp đặc trưng từ URL và HTML	"+Thu thập và xây dựng bộ dữ liệu website bao gồm URL và nội dung HTML của các website phishing và hợp lệ. + Thực hiện tiền xử lý dữ liệu và trích xuất đặc trưng từ URL và nội dung HTML. + Kết hợp các đặc trưng đã trích xuất để tạo dữ liệu đầu vào cho mô hình học máy và học sâu. + Áp dụng một mô hình học sâu để phân loại website phishing. + Đánh giá kết quả dựa trên các chỉ số Accuracy, Precision, Recall và F1-score. + Phân tích kết quả thực nghiệm: So sánh hiệu quả của mô hình học sâu với một mô hình học máy truyền thống.	Nguyễn Thị Hồng Thảo	thaonth@huit.edu.vn	MMT&ATTT	Nghiên cứu	

9	Nghiên cứu và xây dựng các kịch bản kiểm thử, khai thác lỗ hổng hệ điều hành và ứng dụng dựa trên định danh CVE trong môi trường thử nghiệm	- Nghiên cứu các lỗ hổng CVE điển hình trên hệ điều hành và ứng dụng. - Phân loại các lỗ hổng: Buffer Overflow, Command Injection, SQL Injection, RCE, Privilege Escalation... - Xây dựng các kịch bản mô phỏng khai thác lỗ hổng (trên môi trường ảo hoặc sandbox) - Xây dựng kịch bản khai thác giúp nâng cao nhận thức, khả năng phòng thủ và kiểm thử xâm nhập. - Đánh giá mức độ ảnh hưởng và biện pháp khắc phục	Lê Anh Tuấn	tuanla@huit.edu.vn	MMT&ATTT	Nghiên cứu	
10	Nghiên cứu, phát triển thuật toán phát hiện mã độc dựa trên kĩ thuật học máy và học sâu	- Nghiên cứu, tìm hiểu về mã độc và các biến thể - tìm hiểu các kỹ thuật học máy, học sâu để ứng dụng trong bài toán phát hiện mã độc - Cải tiến, phát triển thuật toán - Thực nghiệm trên các bộ dữ liệu ground-truth, biện luận kết quả, so sánh kết quả với các phương pháp SOTA	Phạm Nguyễn Huy Phương Phạm Văn Phùng	phuongpnh@huit.edu.vn , phungpv@huit.edu.vn	MMT&ATTT	Nghiên cứu	
11	Nghiên cứu phương pháp tấn công bằng kỹ thuật phishing sử dụng AI	- Nghiên cứu, tìm hiểu các kỹ thuật phishing hiện tại như Email, website, QR... - Xây dựng hệ thống phát hiện phishing dựa trên NLP và URL features - Cải tiến, phát triển thuật toán - Thực nghiệm trên các bộ dữ liệu ground-truth, biện luận kết quả, so sánh kết quả với các phương pháp SOTA - Đề xuất giải pháp triển khai cho doanh nghiệp trong thực tế	Phạm Nguyễn Huy Phương Phạm Văn Phùng	phuongpnh@huit.edu.vn , phungpv@huit.edu.vn	MMT&ATTT	Nghiên cứu	
12	Nghiên cứu phương pháp phát hiện xâm nhập hệ thống mạng dựa trên kỹ thuật học sâu	- Nghiên cứu tổng quan các hệ thống IDS/IPS truyền thống và hiện đại - Áp dụng mô hình học sâu (LSTM, CNN, Transformer…) để phát hiện: tấn công DoS/DdoS, tấn công quét cổng, brute-force - Thực nghiệm trên bộ dữ liệu chuẩn (NSL-KDD, CIC-IDS2017, UNSW-NB15) - So sánh hiệu năng với các thuật toán ML truyền thống (SVM, Random Forest)	Phạm Nguyễn Huy Phương Phạm Văn Phùng	phuongpnh@huit.edu.vn , phungpv@huit.edu.vn	MMT&ATTT	Nghiên cứu	

13	Triển khai các tính năng bảo mật xây dựng ứng dụng quản lý khóa học trực tuyến	* Triển khai trên hệ điều hành Oracle Linux, phân tích, thiết kế và cài đặt ứng dụng quản lý lớp học trực tuyến có áp dụng các tính năng bảo mật của Oracle * Cơ sở lý thuyết: - Khảo sát, phân tích, thiết kế hệ thống - Bảo mật hệ thống thông tin/ bảo mật cơ sở dữ liệu * Các chức năng chính trên website -Quản lý khóa học, học viên, giáo viên, đăng ký lớp học: có kết hợp các kỹ thuật mã hóa thông tin, profile, định danh và xác thực; kiểm toán và giải trình - Khóa học có có truy xuất bằng mã quét QR - Quản lý theo dõi mua bán khóa học - Phân quyền và điều khiển truy cập (kết hợp VPD, OLS) - Sao lưu, phục hồi cơ sở dữ liệu * Các chức năng trên app mobie: - Đăng ký, đăng nhập, đổi mật khẩu - Xem thông tin khóa học, lớp học, người học, đăng ký khóa học * Công nghệ sử dụng: - Web: asp.net mvc, angular, reactjs... - App mobile: flutter... - Hệ quản trị cở sở dữ liệu: Oracle - Hệ điều hành: Oracle Linux	Nguyễn Phương Hạc	hacnp@huit.edu.vn	MMT&ATTT	Ứng dụng	
14	Xây dựng hệ thống quản lý học tập tích hợp tính năng phát hiện và nhận diện khuôn mặt (FaceID) để quản lý lớp học	- Nghiên cứu, phân tích thiết kế các tính năng, xây dựng hệ thống quản lý học tập: + Quản lý giảng viên: hồ sơ giảng viên (cơ hữu và thỉnh giảng), lịch dạy, lớp dạy, v.v… + Quản lý sinh viên: hồ sơ sinh viên, lịch học, điểm số,.v… + Quản lý lớp học: Tạo lớp học, điểm danh, phân nhóm, kiểm tra, điểm số, xuất danh sách điểm danh, v.v… - Xây dựng tính năng FaceID và tích hợp vào hệ thống LMS: + Xử lý hình ảnh đầu vào từ camera để phục vụ cho các bước phân tích (computer vision) + Xây dựng tính năng phát hiện khuôn mặt từ camera . + Phát triển ứng dụng trên 2 nền tảng Web và Mobile	Vũ Đức Thịnh, Phạm Văn Phùng	thinhvd@huit.edu.vn	MMT&ATTT	Ứng dụng	
15	Phân loại vai trò người dùng trên mạng xã hội bằng phương pháp học máy	-Dự đoán và phân loại vai trò người dùng trên mạng xã hội, sử dụng dữ liệu định lượng từ Twitter Ego Networks. Các đặc trưng như các chỉ số Centrality (Degree, Betweenness, Eigenvector, Closeness) và thuộc tính người dùng (Num_Features) được khai thác để xây dựng tập dữ liệu đặc trưng, từ đó triển khai quy trình phân tích gồm: +Xây dựng đặc trưng phản ánh hành vi và vị trí người dùng; +Gán nhãn vai trò dựa trên ngưỡng hoặc K-means; + Mô phỏng lan truyền thông tin bằng mô hình SIR để đánh giá ảnh hưởng thực tế của từng vai trò ; + Đánh giá hiệu quả phân vai bằng Silhouette Score và ARI. + Báo cáo đầy đủ lý thuyết, phương pháp triển khai, kết quả kiểm thử, và phân tích hiệu quả.	Vũ Đức Thịnh, Phạm Văn Phùng	thinhvd@huit.edu.vn	MMT&ATTT	Nghiên cứu	

KT.TRƯỞNG KHOA
PHÓ TRƯỞNG KHOA

Nguyễn Thị Bích Ngân

NGƯỜI LẬP BIỂU

Lương Thị Quỳnh Mai