VIỆN CÔNG NGHỆ THÔNG TIN VÀ ĐIỆN, ĐIỆN TỬ

ĐỀ TÀI THỰC TẬP TỐT NGHIỆP HỌC KỲ 1 NĂM 2025-2026

GVHD: TS.LÊ QUỐC TUẤN

CHỦ ĐỀ: PHÁT TRIỂN ỨNG DỤNG & GIẢI PHÁP CÔNG NGHỆ

1. Ứng dụng quản lý sinh viên bằng Python & SQLite

Mục tiêu: Xây dựng ứng dụng CRUD quản lý hồ sơ sinh viên. Ứng dụng phải đơn giản, dễ sử dụng và phù hợp với quy mô nhỏ, phục vụ việc học tập và thực hành.

Nội dung:

1. Thiết kế cơ sở dữ liệu SQLite gồm bảng sinh viên, lớp và khoa, kiểm tra dữ liệu đầu vào.
2. Lập trình giao diện bằng Tkinter hoặc Flask với chức năng thêm, sửa, xóa, tìm kiếm và xuất báo cáo.
3. Phân quyền người dùng (admin, user) và triển khai xuất file dữ liệu nếu cần.
4. Demo thực tế: thêm danh sách sinh viên và tìm kiếm theo tên/lớp.

Số SV: Tối đa 2.

2. Ứng dụng web bán hàng mini (Django/Flask)

Mục tiêu: Phát triển website thương mại điện tử đơn giản với giỏ hàng và thanh toán mô phỏng, nhằm giúp sinh viên làm quen với quy trình xây dựng website.

Nội dung:

1. Thiết kế mô hình dữ liệu bao gồm sản phẩm, người dùng, đơn hàng.
2. Xây dựng backend bằng Django/Flask sử dụng ORM hoặc API; triển khai đăng ký/đăng nhập và phân quyền.
3. Phát triển giao diện bằng HTML/CSS/Bootstrap; tích hợp chức năng giỏ hàng và thống kê đơn hàng.
4. Demo chức năng đặt hàng và hiển thị hoá đơn.

Số SV: Tối đa 2.

3. Ứng dụng To-do (Node.js + MongoDB)

Mục tiêu: Xây dựng ứng dụng quản lý công việc theo mô hình full-stack (REST API + client), giúp sinh viên hiểu quy trình lập trình backend và frontend.

Nội dung:

1. Thiết kế API bằng Node.js/Express cho các thao tác CRUD, xác thực người dùng bằng JSON Web Token.

2. Sử dụng MongoDB làm cơ sở dữ liệu; xây dựng schema và kiểm tra dữ liệu.

3. Phát triển frontend bằng React hoặc Vue; giao diện thêm/sửa/xóa công việc và trạng thái hoàn thành.

4. Demo triển khai ứng dụng trên máy ảo hoặc dịch vụ đám mây miễn phí.

Số SV: Tối đa 2.

4. Chatbot hỗ trợ sinh viên (ChatGPT API)

Mục tiêu: Tạo chatbot hỗ trợ tư vấn học tập, giải đáp thắc mắc về chương trình đào tạo và thông tin nhà trường.

Nội dung:

1. Tìm hiểu cách sử dụng API ChatGPT và các nguyên tắc xử lý ngôn ngữ tự nhiên.

2. Thiết lập chatbot: kết nối API, lưu trữ lịch sử hội thoại, phân loại câu hỏi.

3. Phát triển giao diện web với Flask/Django hoặc tích hợp với Telegram.

4. Demo: chatbot trả lời câu hỏi về chương trình học, thời khoá biểu, quy định.

Số SV: Tối đa 2.

5. Ứng dụng Blockchain lưu trữ chứng chỉ học tập

Mục tiêu: Lưu trữ và xác thực dữ liệu học tập (chứng chỉ, bảng điểm) trên nền tảng blockchain nhằm chống giả mạo.

Nội dung:

1. Nghiên cứu Ethereum hoặc Hyperledger, viết smart contract để lưu hash chứng chỉ học tập.

2. Xây dựng API để lưu và tra cứu chứng chỉ; tích hợp web3.js hoặc ethers.js.

3. Phát triển giao diện cho trường phát hành và người dùng tra cứu.

4. Demo: tạo chứng chỉ giả lập, lưu lên blockchain và xác thực.

Số SV: Tối đa 2.

6. Quản lý chuỗi cung ứng bằng Blockchain và IoT

Mục tiêu: Tích hợp IoT và blockchain để theo dõi hàng hoá, đảm bảo dữ liệu không bị giả mạo.

Nội dung:

1. Sử dụng cảm biến IoT (RFID, cảm biến nhiệt độ) để thu thập dữ liệu vận chuyển.

2. Lưu trữ dữ liệu lên blockchain nhằm chống chỉnh sửa và tăng tính minh bạch.

3. Thiết kế smart contract để xác nhận và theo dõi từng giai đoạn trong chuỗi cung ứng; hiển thị dashboard.

4. **Ghi chú:** Tài liệu nghiên cứu cho thấy blockchain mang lại nền tảng bảo mật cho IoT, loại bỏ điểm yếu tập trung và tăng cường bảo mật.

Số SV: Tối đa 2.

7. Ứng dụng AR hỗ trợ bảo trì mạng

Mục tiêu: Sử dụng thực tế tăng cường (Augmented Reality) để hỗ trợ kỹ thuật viên bảo trì thiết bị mạng.

Nội dung:

1. Nghiên cứu frameworks AR (ARCore/ARKit) và cách tích hợp mô hình mạng thực tế.

2. Thiết kế ứng dụng hiển thị sơ đồ thiết bị (router, switch) khi quét mã QR tại hiện trường.

3. Tích hợp API giám sát (SNMP) để hiển thị trạng thái thiết bị ngay trong AR.

Số SV: Tối đa 2.

8. Hệ thống Digital Twin cho nhà máy thông minh

Mục tiêu: Xây dựng bản sao số (Digital Twin) của một phân xưởng/nhà máy để giám sát và dự báo hiệu suất.

Nội dung:

1. Thu thập dữ liệu IoT từ máy móc (nhiệt độ, rung động), lưu trữ vào cơ sở dữ liệu.

2. Sử dụng mô hình học máy dự đoán hỏng hóc; hiển thị dữ liệu trong không gian 3D hoặc dashboard.

3. Triển khai mô phỏng quá trình sản xuất, phản hồi thời gian thực cho người vận hành.

Số SV: Tối đa 2.

CHỦ ĐỀ: KHOA HỌC DỮ LIỆU & TRÍ TUỆ NHÂN TẠO

9. Phân tích dữ liệu bán hàng và dự báo doanh thu

Mục tiêu: Dự báo doanh thu tương lai từ dữ liệu bán hàng, giúp doanh nghiệp lập kế hoạch tài chính.

Nội dung:

1. Thu thập dữ liệu bán hàng thực tế hoặc dataset công khai; làm sạch dữ liệu.
2. Phân tích thống kê, chọn mô hình dự báo (Linear Regression, ARIMA, LSTM) và đánh giá MAE/RMSE.
3. Trực quan hóa kết quả bằng Matplotlib/Plotly; xây dựng dashboard tương tác.

Số SV: Tối đa 2.

10. Khai phá dữ liệu mạng xã hội (Facebook/Twitter)

Mục tiêu: Phân tích xu hướng, từ khoá và sentiment trên mạng xã hội, phục vụ marketing hoặc nghiên cứu xã hội.

Nội dung:

1. Thu thập dữ liệu qua API Twitter hoặc Facebook, xử lý ngôn ngữ tự nhiên (lọc stopwords, stemming).
2. Thực hiện sentiment analysis (VADER/BERT) và LDA Topic Modeling để tìm chủ đề chính.
3. Xây dựng wordcloud và dashboard hiển thị xu hướng, biểu đồ sentiment.

Số SV: Tối đa 2.

11. Phân loại ảnh sản phẩm bằng Deep Learning

Mục tiêu: Huấn luyện mô hình CNN phân loại ảnh sản phẩm (thời trang, đồ ăn, động vật…).

Nội dung:

1. Thu thập dữ liệu (CIFAR10, Fashion-MNIST) hoặc tự tạo; tiền xử lý và augment dữ liệu.

2. Xây dựng và huấn luyện mô hình CNN (Keras/PyTorch), đánh giá accuracy và confusion matrix.

3. Tạo giao diện demo (Flask/Streamlit) cho người dùng tải ảnh và nhận kết quả.

Số SV: Tối đa 2.

12. Phát hiện bất thường trong log hệ thống

Mục tiêu: Ứng dụng Machine Learning để phát hiện hành vi bất thường trong log server, hỗ trợ an ninh.

Nội dung:

1. Thu thập log từ server (syslog hoặc Windows event log) và chuyển thành feature (TF-IDF, n-gram).

2. Huấn luyện các mô hình như Isolation Forest, One-Class SVM hoặc LSTM Autoencoder để phát hiện anomaly.

3. Demo cảnh báo bất thường và đánh giá mô hình.

Số SV: Tối đa 2.

13. Dự đoán lưu lượng giao thông (Smart City)

Mục tiêu: Phân tích dữ liệu giao thông (sensor, camera) để dự báo lưu lượng xe trong thành phố thông minh.

Nội dung:

1. Lấy dữ liệu lưu lượng xe và yếu tố thời tiết; trực quan hóa chuỗi thời gian.

2. Sử dụng mô hình dự báo ARIMA/Prophet hoặc LSTM, so sánh các mô hình.

3. Xây dựng dashboard dự báo và cảnh báo tắc đường.

Số SV: Tối đa 2.

14. Nhận diện biển số xe bằng AI

Mục tiêu: Ứng dụng YOLOv5/YOLOv8 và OpenCV để phát hiện và đọc biển số xe.

Nội dung:

1. Thu thập dataset biển số; huấn luyện mô hình YOLO phát hiện vùng chứa biển.

2. Áp dụng OCR (Tesseract) để đọc ký tự trên biển số.

3. Demo nhận diện biển số trong video và hiển thị kết quả trên giao diện.

Số SV: Tối đa 2.

15. AI chẩn đoán bệnh từ ảnh X-ray

Mục tiêu: Phân loại ảnh X-ray (COVID-19, viêm phổi) để hỗ trợ chẩn đoán.

Nội dung:

1. Thu thập dữ liệu X-ray từ Kaggle; cân bằng dataset.
2. Huấn luyện mô hình CNN hoặc transfer learning (ResNet, EfficientNet), đánh giá AUC/accuracy.
3. Triển khai demo dự đoán và hiển thị kết quả chẩn đoán.

Số SV: Tối đa 2.

16. Chatbot hỏi đáp tiếng Việt bằng Transformer

Mục tiêu: Xây dựng chatbot hỏi đáp tiếng Việt bằng mô hình Transformer (BERT/PhoBERT).

Nội dung:

1. Thu thập dữ liệu câu hỏi – câu trả lời; fine-tune mô hình pre-trained (PhoBERT/ViT5).
2. Xây dựng engine hỏi đáp dạng embedding search hoặc generative model.
3. Demo chatbot trên web/Telegram.

Số SV: Tối đa 2.

17. Phát hiện người đeo khẩu trang bằng AI

Mục tiêu: Nhận diện người đeo/không đeo khẩu trang trong ảnh/video, phù hợp bối cảnh dịch bệnh.

Nội dung:

1. Chuẩn bị dữ liệu ảnh đeo khẩu trang và không đeo khẩu trang; augment dữ liệu.
2. Huấn luyện CNN nhẹ (MobileNet) cho phân loại và đánh giá accuracy.
3. Demo real-time trên webcam, hiển thị kết quả.

Số SV: Tối đa 2.

18. Nhận diện cảm xúc khuôn mặt

Mục tiêu: Phân loại cảm xúc (vui, buồn, giận dữ…) từ ảnh và video.

Nội dung:

1. Sử dụng dataset FER2013/CK+; tiền xử lý và cân bằng dữ liệu.

2. Huấn luyện mô hình CNN hoặc ResNet; đánh giá accuracy/AUC.

3. Demo real-time bằng webcam và hiển thị trạng thái cảm xúc.

Số SV: Tối đa 2.

19. AI & Cybersecurity: Phát hiện tấn công tự động

Mục tiêu: Kết hợp AI và an ninh mạng để tự động phát hiện tấn công, nâng cao khả năng phản ứng.

Nội dung:

1. Thu thập và phân tích dữ liệu log mạng, lưu lượng và sự kiện hệ thống; chuẩn hoá thành feature vector.

2. Huấn luyện mô hình ML (Random Forest/LSTM) phát hiện bất thường và tích hợp vào hệ thống SIEM.

3. Tạo engine phản ứng tự động (chặn IP, thông báo) theo kết quả mô hình.

4. **Cơ sở:** Báo cáo năm 2024–2025 cho thấy Generative AI đang chuyển từ thử nghiệm sang triển khai rộng rãi, hỗ trợ tự động hoá tác vụ và xử lý dữ liệu lớn trong an ninh mạng.

Số SV: Tối đa 2.

20. Federated Learning cho dữ liệu y tế

Mục tiêu: Bảo vệ quyền riêng tư khi đào tạo mô hình trên dữ liệu nhạy cảm bằng federated learning.

Nội dung:

1. Nghiên cứu federated learning và differential privacy để giảm rủi ro lộ dữ liệu.

2. Cài đặt mô hình federated (TensorFlow Federated/PySyft) trên dữ liệu giả lập (chẩn đoán bệnh).

3. Đánh giá độ chính xác và mức độ bảo mật; xây dựng giao thức client–server.

Số SV: Tối đa 2.

CHỦ ĐỀ: MẠNG & AN NINH MẠNG

21. Hệ thống giám sát mạng nội bộ bằng Zabbix

Mục tiêu: Giám sát và cảnh báo trạng thái thiết bị mạng (server, router, switch).

Nội dung:

1. Cài Zabbix server và agent; cấu hình SNMP và template giám sát.
2. Tạo dashboard theo dõi CPU, RAM, lưu lượng mạng; thiết lập cảnh báo qua email.
3. Demo cảnh báo khi thiết bị quá tải hoặc mất kết nối; Zabbix hỗ trợ thu thập nhiều chỉ số như lưu lượng, kết nối TCP và trạng thái đường.

Số SV: Tối đa 2.

22. Xây dựng tường lửa mạng nội bộ bằng pfSense

Mục tiêu: Cài đặt và cấu hình pfSense để bảo vệ mạng nội bộ (NAT, firewall rule, VPN).

Nội dung:

1. Triển khai pfSense trên máy ảo; cấu hình interface WAN/LAN và NAT.
2. Tạo rule lọc gói, chặn/cho phép dịch vụ; cấu hình VPN.
3. Theo tài liệu pfSense, những tính năng firewall, NAT và VPN được cập nhật đầy đủ và cung cấp hướng dẫn chi tiết.

Số SV: Tối đa 2.

23. Mạng Wi-Fi doanh nghiệp an toàn (WPA3 & VLAN)

Mục tiêu: Thiết kế mạng Wi-Fi phân quyền (guest/staff) với bảo mật cao.

Nội dung:

1. Chọn thiết bị AP hỗ trợ WPA3/WPA2-Enterprise; cấu hình RADIUS.
2. Tạo SSID cho guest và staff, gắn VLAN tương ứng; cấu hình trunk trên switch.
3. Cấu hình DHCP, DNS và kiểm soát băng thông, captive portal.
4. Demo giám sát kết nối và phân quyền truy cập.

Số SV: Tối đa 2.

24. Phát hiện tấn công bằng Snort/Suricata

Mục tiêu: Cài đặt và cấu hình IDS (Snort/Suricata) để phát hiện tấn công mạng.

Nội dung:

1. Cài đặt Snort hoặc Suricata trên máy ảo; cập nhật rules.
2. Viết rule phát hiện port-scan, brute force và test bằng nmap/hydra.
3. So sánh hiệu suất giữa Snort và Suricata, báo cáo kết quả.

Số SV: Tối đa 2.

25. Triển khai mạng ảo hóa bằng Docker

Mục tiêu: Mô phỏng mạng container phức tạp và kiểm soát lưu lượng.

Nội dung:

1. Tìm hiểu các chế độ mạng của Docker (bridge, host, overlay).
2. Tạo nhiều container (web, DB) và sử dụng traefik/nginx làm reverse proxy.
3. Demo định tuyến giữa các container, giám sát và lọc lưu lượng.

Số SV: Tối đa 2.

26. Xây dựng VPN giữa hai chi nhánh bằng OpenVPN

Mục tiêu: Thiết lập VPN site-to-site và remote access giữa hai mạng riêng.

Nội dung:

1. Cài đặt OpenVPN server và client; cấu hình định tuyến mạng con.
2. So sánh chế độ PSK và SSL/TLS; theo pfSense docs, PSK bị khuyến cáo không an toàn và sẽ bị loại bỏ【625083750654782†L283-L299】.
3. Demo truy cập file server qua VPN và đánh giá băng thông.

Số SV: Tối đa 2.

27. Hệ thống IDS cho IoT (IoT IDS)

Mục tiêu: Phát hiện bất thường và tấn công trên mạng IoT bằng machine learning.

Nội dung:

1. Thu thập gói tin IoT bằng Wireshark/tshark và trích xuất đặc trưng (payload length, protocol, port).

2. Huấn luyện mô hình ML (Random Forest, SVM) hoặc Deep Learning (Autoencoder) phát hiện bất thường.

3. Tích hợp mô hình vào hệ thống giám sát và cảnh báo.

Số SV: Tối đa 2.

28. Tích hợp Service Mesh & Zero Trust trên Kubernetes

Mục tiêu: Triển khai kiến trúc Zero Trust cho các microservices trên Kubernetes.

Nội dung:

1. Cài đặt Kubernetes cluster (minikube/kind) và triển khai service mesh (Istio hoặc Linkerd).

2. Cấu hình mTLS, chính sách truy cập và mạng ảo để kiểm soát traffic giữa các service.

3. Mô phỏng tấn công lateral movement và kiểm thử chính sách Zero Trust.

Số SV: Tối đa 2.

29. Quản lý hạ tầng đa đám mây an toàn

Mục tiêu: Thiết kế nền tảng quản lý và bảo mật môi trường cloud đa nền tảng (AWS, Azure, GCP).

Nội dung:

1. Tự động triển khai tài nguyên cloud bằng Terraform hoặc Ansible; cấu hình IAM.

2. Thiết lập network security, logging và giám sát; đánh giá rủi ro.

3. Mô phỏng sự cố bảo mật (leak data) và khắc phục.

Số SV: Tối đa 2.

CHỦ ĐỀ TỔNG HỢP NÂNG CAO

30. Mô hình AI phối hợp Blockchain trong giám sát an ninh

Mục tiêu: Kết hợp AI và blockchain để phát hiện tấn công và ghi log an toàn.

Nội dung:

1. Sử dụng AI phát hiện lưu lượng bất thường (IDS) bằng model ML/DL.

2. Ghi log sự kiện an ninh lên blockchain để chống chỉnh sửa; smart contract quy định mức độ cảnh báo và phản ứng.
3. Demo quy trình phát hiện – ghi log – phản ứng tự động, giúp tăng tính minh bạch và an toàn

Số SV: Tối đa 2.

31. Nền tảng phân tích log phân tán bằng Apache Kafka & ML

Mục tiêu: Thiết kế hệ thống xử lý log real-time phân tán và phát hiện bất thường.

Nội dung:

1. Thu thập log từ nhiều nguồn qua Kafka; stream dữ liệu đến Spark Streaming hoặc Flink.

2. Xử lý, phân loại log và phát hiện bất thường bằng Isolation Forest hoặc các mô hình ML khác.

3. Lưu trữ dữ liệu xuống Elasticsearch và hiển thị trên Kibana; đánh giá hiệu suất hệ thống.

Số SV: Tối đa 2.

32. Ứng dụng Digital Forensics trong điều tra tấn công mạng

Mục tiêu: Thực hành kỹ thuật điều tra số (forensics) đối với máy tính và mạng, hỗ trợ truy vết tấn công.

Nội dung:

1. Thu thập và phân tích chứng cứ trên ổ cứng (disk imaging, file carving) và memory dump.

2. Phân tích log mạng, Wireshark và sử dụng các công cụ như Autopsy, Volatility.

3. Xây dựng báo cáo điều tra và xác định nguyên nhân, hành vi tấn công.

Số SV: Tối đa 2.

33. Hệ thống quản trị năng lượng thông minh

Mục tiêu: Giám sát và tối ưu hoá tiêu thụ năng lượng tại tòa nhà bằng IoT và ML.

Nội dung:

1. Thu thập dữ liệu tiêu thụ điện/nước qua cảm biến IoT; lưu trữ dữ liệu thời gian thực.

2. Huấn luyện mô hình ML dự đoán nhu cầu và đề xuất phương án tiết kiệm.

3. Tích hợp hệ thống điều khiển tự động (bật/tắt thiết bị) và dashboard báo cáo.

Số SV: Tối đa 2.

34. Đánh giá mô hình Zero-Trust trên mạng SD-WAN

Mục tiêu: Xây dựng mô hình Zero-Trust trên hệ thống SD-WAN và đánh giá hiệu quả.

Nội dung:

1. Triển khai SD-WAN (Cisco Viptela hoặc open-source) trong môi trường mô phỏng; phân đoạn mạng (micro-segmentation).
2. Áp dụng Zero-Trust: xác thực thiết bị và người dùng, giám sát phiên kết nối.
3. Đánh giá hiệu suất, độ trễ và khả năng bảo mật; so sánh với mô hình truyền thống.

Số SV: Tối đa 2.

35. Tổng hợp dữ liệu Threat Intelligence

Mục tiêu: Thu thập, phân tích và chia sẻ thông tin về mối đe doạ an ninh (threat intelligence).

Nội dung:

1. Thu thập dữ liệu IOC (Indicator of Compromise) từ nguồn open source (AlienVault OTX, MISP).
2. Phân tích xu hướng tấn công, phân loại threat actor và áp dụng ML dự đoán.
3. Tạo dashboard chia sẻ threat intelligence (STIX/TAXII) cho đội bảo mật.

Số SV: Tối đa 2.

36. Xây dựng hệ thống Data Lake cho doanh nghiệp

Mục tiêu: Thiết kế kiến trúc lưu trữ và phân tích dữ liệu lớn (Big Data) cho doanh nghiệp.

Nội dung:

1. Nghiên cứu kiến trúc Data Lake và các công cụ (Hadoop, S3, Delta Lake).
2. Thiết kế pipeline thu thập dữ liệu (ingestion) từ nhiều nguồn; áp dụng schema-on-read.
3. Triển khai quy trình phân tích và trực quan hoá dữ liệu; xây dựng báo cáo.

Số SV: Tối đa 2.

37. Ứng dụng AI trong hệ thống Robotics tự hành

Mục tiêu: Thiết kế robot tự hành (ví dụ robot giao hàng) tích hợp AI và IoT.

Nội dung:

1. Xây dựng mô hình điều khiển tự hành (SLAM) và nhận dạng vật cản bằng computer vision.
2. Tích hợp cảm biến (LIDAR, camera) và lập trình vi điều khiển (ROS, Arduino).
3. Demo robot di chuyển, né tránh vật cản và báo cáo vị trí.

Số SV: Tối đa 2.

38. Nền tảng học máy tích hợp bảo mật dữ liệu

Mục tiêu: Xây dựng pipeline ML với cơ chế privacy-by-design (bảo vệ dữ liệu ngay từ đầu).

Nội dung:

1. Kết hợp kỹ thuật differential privacy và homomorphic encryption trong quá trình xử lý dữ liệu.
2. Huấn luyện mô hình trên dữ liệu nhạy cảm (y tế, tài chính) mà vẫn bảo vệ quyền riêng tư.
3. Tạo API phục vụ mô hình kèm cơ chế kiểm tra quyền truy cập và giám sát truy vết.

Số SV: Tối đa 2.

39. Quản lý rủi ro an ninh thông tin bằng mô hình AI

Mục tiêu: Đánh giá và dự đoán rủi ro an ninh mạng bằng mô hình AI, đề xuất biện pháp giảm thiểu.

Nội dung:

1. Thu thập dữ liệu về lỗ hổng (vulnerability scans, CVE database) và sự kiện an ninh.
2. Xây dựng mô hình AI xếp hạng rủi ro và đưa ra gợi ý ưu tiên vá lỗi.
3. Demo dashboard hiển thị chỉ số rủi ro và đề xuất hành động khắc phục.

Số SV: Tối đa 2.

40. Hệ thống điều khiển giao thông thông minh bằng AI & Edge Computing

Mục tiêu: Thiết kế hệ thống phân luồng giao thông tự động dựa trên AI và tính toán biên (edge computing).

Nội dung:

1. Lắp đặt camera và sensor tại các nút giao; sử dụng AI nhận dạng biển số và đếm xe.

2. Xử lý dữ liệu tại thiết bị Edge (Jetson, Raspberry Pi) nhằm giảm độ trễ so với gửi lên cloud.

3. Điều chỉnh đèn giao thông tự động theo lưu lượng và đánh giá hiệu quả giảm ùn tắc.

Số SV: Tối đa 2.