NGHIÊN CỨU GIẢI PHÁP PHÁT HIỆN SỚM LỪA ĐẢO GIỌNG NÓI SỬ DỤNG PROGRESSIVE LEARNING

EARLY DETECTION OF VOICE SCAM USING PROGRESSIVE LEARNING APPROACH

Nguyễn Thanh Hoài Lộc - 240202009

Tóm tắt

- Lớp: CS2205.NOV2024
- Link Github của nhóm: https://github.com/locnthIA/CS2205.NOV2024
- Link YouTube video: https://www.youtube.com/watch?v=d0Om41uPnN4
- Ảnh + Họ và Tên: Nguyễn Thanh Hoài Lộc

Giới thiệu

- Lừa đảo qua điện thoại là mối đe dọa phổ biến tại Việt Nam, ngày càng tinh vi nhờ công nghệ mới.
- Phương pháp phân tích hậu kiểm thường không kịp thời ngăn chặn.
- Progressive Learning giúp mô hình liên tục thích nghi với dữ liệu mới mà không mất kiến thức cũ.

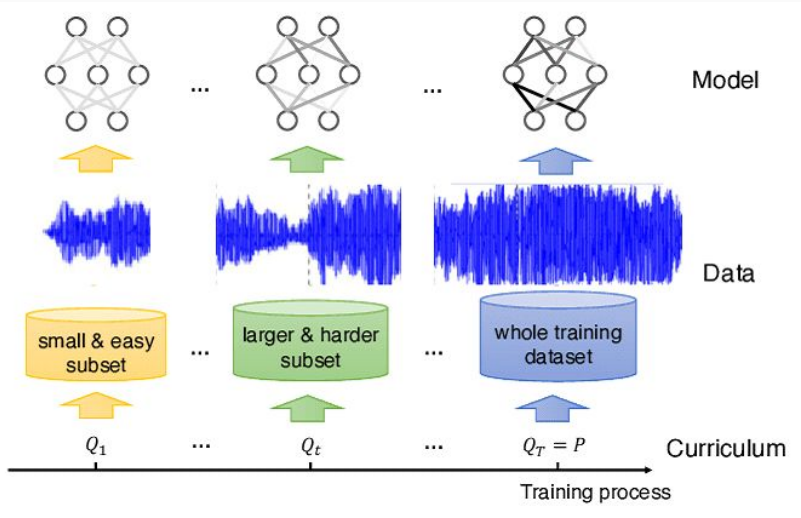
Mục tiêu

- ✅ Xây dựng hệ thống thông minh tích hợp Progressive Learning kết hợp Deep Learning, cho phép cảnh báo nhanh chóng các cuộc gọi đáng ngờ trong vòng 30 giây đầu tiên.
- ✅ Thiết lập kho dữ liệu chuyên biệt về cuộc gọi lừa đảo với chú thích chi tiết, phục vụ nghiên cứu và phát triển các giải pháp bảo vệ người dùng.
- ✅ Nâng cao hiệu quả phát hiện thông qua cơ chế tự học liên tục, cho phép hệ thống thích nghi với các chiến thuật lừa đảo mới.

Nội dung và Phương pháp

Nội dung nghiên cứu:

- Kết hợp xử lý âm thanh thời gian thực với deep learning
- Cho phép học và cập nhật liên tục
- Vượt trội so với các mô hình tĩnh truyền thống
- Cải thiện hiệu suất theo thời gian



Nội dung và Phương pháp

Giai đoạn 1: Xử lý tín hiệu âm thanh

- Mục đích: Chuẩn hóa và trích xuất đặc trưng từ dữ liệu cuộc gọi thô.
- Cách thực hiện:
  - Xử lý tín hiệu số để loại bỏ nhiễu và chuẩn hóa âm thanh đầu vào.
  - Phân đoạn cuộc gọi theo khoảng thời gian để tập trung vào 30 giây đầu tiên.
  - Trích xuất đặc trưng âm thanh bao gồm đặc trưng ngôn ngữ và phi ngôn ngữ.
  - Đầu ra: Véc-tơ đặc trưng đã được chuẩn hóa, sẵn sàng cho phân tích bằng Deep Learning.

Nội dung và Phương pháp

Giai đoạn 2: Mô hình Deep Learning

- Mục đích: Phân tích các đặc trưng âm thanh để phát hiện dấu hiệu lừa đảo.
- Cách thực hiện:
  - Kiến trúc module: Chia hệ thống thành các thành phần độc lập chuyên biệt.
  - Sử dụng các mạng neural sâu để phát hiện mẫu bất thường trong giọng nói.
  - Tích hợp các thành phần phân tích ngôn ngữ và ngữ điệu để nhận diện hành vi lừa đảo.
  - Đầu ra: Xác suất cuộc gọi là lừa đảo dựa trên các mẫu đã học.

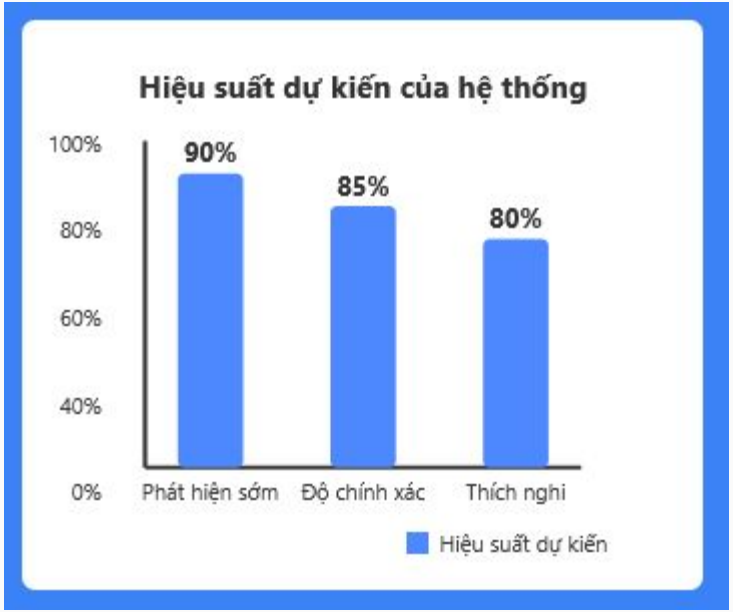
Nội dung và Phương pháp

Giai đoạn 3: Progressive Learning Framework

- Mục đích: Cho phép hệ thống liên tục học và thích nghi với các chiến thuật lừa đảo mới.
- Cách thực hiện:
  - Xây dựng framework học tăng tiến để duy trì kiến thức cũ trong khi tích hợp kiến thức mới.
  - Học tăng cường để liên tục cập nhật mô hình dựa trên phản hồi từ hệ thống giám sát.
  - Cơ chế thích nghi cho phép điều chỉnh ngưỡng cảnh báo dựa trên dữ liệu mới.
  - Nhiệm vụ phụ trợ: Phân loại các loại lừa đảo để cung cấp thông tin chi tiết hơn về mối đe dọa.

Kết quả dự kiến

- Hệ thống thông minh có khả năng phát hiện cuộc gọi lừa đảo trong 30 giây với độ tin cậy cao.
- Kho dữ liệu chuyên sâu với trên 10,000 mẫu cuộc gọi được phân tích và chú thích.
- Giải pháp hoàn chỉnh sẵn sàng triển khai với giao diện API và hệ thống giám sát.



Tài liệu tham khảo

[1] M. K. Bae, S. Kim, và H. Ko, "Class-Incremental Learning for Sound Event Localization and Detection," *arXiv preprint arXiv:2411.12830*, 2024.

[2] N. H. Tuấn, "Cơ sở toán và MFCCs – Trích xuất đặc trưng âm thanh," *Tạp chí Khoa học Trường Đại học Sư phạm TP Hồ Chí Minh*, tập 20, số 4, trang 55–67, 2024.

[3] J. Zhang, A. Kumar, và S. Tan, "Progressive Continual Learning for Spoken Keyword Spotting," trong *Kỷ yếu Hội nghị ICASSP 2024*, trang 3255–3259.

[4] L. Wang và K. Patel, "Towards Robust Few-shot Class Incremental Learning in Audio Classification using Contrastive Representation," *arXiv preprint arXiv:2407.19265*, 2024.

[5] H. Lee, J. Park, và M. Chen, "Audio-Visual Class-Incremental Learning," *arXiv preprint arXiv:2308.11073*, 2023.