BỘ CÔNG THƯƠNG
TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP TP. HỒ CHÍ MINH
KHOA CÔNG NGHỆ THÔNG TIN

----ꕥ📖ꕥ----

BÁO CÁO TIỂU LUẬN

MÔN HỌC: CÔNG NGHỆ MỚI TRONG PHÁT TRIỂN ỨNG DỤNG CÔNG NGHỆ THÔNG TIN

ĐỀ TÀI: GIỚI THIỆU CÔNG NGHỆ MỚI TRONG ĐỀ TÀI NGHIÊN CỨU BẢO MẬT WEB – ỨNG DỤNG XÂY DỰNG WEBSITE XỬ LÝ HỌC VỤ

Giảng viên hướng dẫn: Ths. Võ Ngọc Tấn
Phước Lớp học phần: DHHTTT17B
Mã lớp học phần : 4203003144
Sinh viên thực hiện :
21071141 – Đặng Bảo Chánh

Thành phố Hồ Chí Minh, ngày 15 tháng 05 năm 2025

MỤC LỤC

DANH MỤC HÌNH ẢNH

DANH MỤC BẢNG

DANH MỤC VIẾT TẮT

Từ viết tắt	Ý nghĩa
API	Application Programming Interface

CHƯƠNG 1: GIỚI THIỆU CHUNG

1.1. GIỚI THIỆU TỔNG QUAN

Trong thời đại công nghệ số phát triển nhanh chóng, các hệ thống quản lý học vụ truyền thống đang dần được thay thế bởi các nền tảng số hóa nhằm tối ưu hóa hiệu quả giảng dạy, học tập và quản lý. Việc tích hợp các công nghệ mới như quét mã độc tự động, gửi cảnh báo qua email, xác thực bằng reCAPTCHA, hay hỗ trợ người dùng qua chatbot AI đã và đang góp phần nâng cao tính bảo mật, độ tin cậy và tính thân thiện của hệ thống. Đề tài này tập trung xây dựng một hệ thống web học vụ ứng dụng các công nghệ hiện đại nói trên nhằm phục vụ hiệu quả nhu cầu sử dụng của sinh viên, giảng viên và quản trị viên trong môi trường giáo dục trực tuyến.

1.2. MỤC TIÊU

Báo cáo này được thực hiện nhằm mục đích phân tích chi tiết các công nghệ mới và hiện đại được tích hợp trong quá trình xây dựng hệ thống web học vụ bảo mật. Đây là nền tảng hỗ trợ quản lý học tập, giảng dạy và hành chính một cách toàn diện giữa sinh viên, giảng viên và quản trị viên trong môi trường giáo dục đại học. Thông qua việc ứng dụng các công nghệ tiên tiến như quét mã độc tự động, xác thực đa lớp bằng OTP, reCAPTCHA của Google, tích hợp chatbot AI và hệ thống xử lý email cảnh báo, báo cáo giúp người đọc hiểu rõ cách những công nghệ này phối hợp để đảm bảo an toàn, hiệu quả và thân thiện với người dùng.

Cụ thể, báo cáo sẽ tập trung vào các mục tiêu sau:

- Phân tích nguyên lý hoạt động và vai trò của từng công nghệ chính:
    - Cơ chế quét mã độc khi nộp bài nhằm phát hiện sớm và chặn các mã nguy hiểm có thể gây ảnh hưởng đến hệ thống.
    - reCAPTCHA Google để ngăn chặn bot và hành vi đăng nhập trái phép.
    - Xác thực OTP qua email sau khi vượt quá số lần đăng nhập giới hạn, giúp tăng cường bảo mật tài khoản.
    - Tích hợp chatbot Gemini API hỗ trợ người dùng tra cứu thông

tin, giải đáp nhanh các thắc mắc học vụ.

- Cơ chế gửi email tự động khi phát hiện hành vi bất thường như nộp bài chứa mã độc.

- Đánh giá ưu – nhược điểm của từng công nghệ trong triển khai thực tế:

  - Khả năng bảo vệ an ninh mạng thông qua kiểm tra mã độc và xác thực nhiều lớp.

  - Trải nghiệm người dùng được nâng cao nhờ chatbot và giao diện tương tác nhanh.

  - Tính mở rộng và dễ tích hợp giữa các mô-đun qua hệ thống API, tuy nhiên đi kèm là thách thức về quản lý phiên đăng nhập và tài nguyên hệ thống.

- Trình bày cách thức tích hợp các công nghệ vào quy trình phát triển và vận hành hệ thống học vụ:

  - Từ khâu quản lý tài khoản, sinh viên nộp bài và đăng ký học phần, giảng viên lên bài tập và chấm điểm, đến quản trị viên theo dõi công nợ và quản lý học phần.

  - Hệ thống kiểm tra, cảnh báo và xác thực được tích hợp liền mạch nhằm đảm bảo tính bảo mật, ổn định và tự động hóa cao nhất.

Thông qua việc phân tích và đánh giá này, báo cáo không chỉ cung cấp kiến thức nền tảng về các công nghệ liên quan mà còn là tài liệu tham khảo thực tiễn cho những nhà phát triển, quản trị viên CNTT và các tổ chức giáo dục đang có nhu cầu chuyển đổi số hoặc nâng cấp hệ thống học vụ theo hướng hiện đại, an toàn và thông minh hơn.

1.3. DANH SÁCH CÁC CÔNG NGHỆ SỬ DỤNG

Hình 1.1. Logo PHP

Nguồn: Sưu tầm trên Internet

PHP (Hypertext Preprocessor) là một ngôn ngữ lập trình phía máy chủ, được sử dụng rộng rãi trong phát triển web nhờ khả năng xử lý linh hoạt, tích hợp tốt với cơ sở dữ liệu và hỗ trợ nhiều hàm xử lý tệp, biểu thức chính quy và các thao tác hệ thống. [1].

Hình 1.2. reCAPTCHA GOOLE

Nguồn: Sưu tầm trên Internet

Google reCAPTCHA là một dịch vụ bảo mật miễn phí do Google cung cấp, giúp bảo vệ website khỏi các cuộc tấn công tự động từ bot và các hành vi đăng nhập trái phép. Công nghệ này sử dụng các thuật toán học máy và phân tích hành vi người dùng để phân biệt giữa người thật và phần mềm độc hại một cách hiệu quả mà không làm gián đoạn trải nghiệm người dùng [2].

Hình 1.3. Logo GEMINI

Nguồn: Sưu tầm trên Internet

Chatbot Gemini API là một công nghệ trí tuệ nhân tạo được tích hợp vào hệ thống web học vụ nhằm hỗ trợ người dùng – đặc biệt là sinh viên – tra cứu thông tin nhanh chóng và giải đáp các thắc mắc học vụ một cách tự động.

Hình 1.3. Logo PHPMailer

Nguồn: Sưu tầm trên Internet

Hệ thống web học vụ được trang bị cơ chế xác thực OTP qua email nhằm tăng cường bảo mật cho tài khoản người dùng. Khi một tài khoản thực hiện quá số lần đăng nhập không thành công (ví dụ: 10 lần), hệ thống sẽ tự động khóa tạm thời quá trình đăng nhập và yêu cầu người dùng xác minh danh tính qua mã OTP được gửi về email đã đăng ký. Điều này giúp ngăn chặn các cuộc tấn công brute-force hoặc hành vi truy cập trái phép.

1.4. CÁCH THỨC ỨNG DỤNG CÔNG NGHỆ VÀO BÀI TOÁN THỰC TẾ

Trong hệ thống web học vụ, các công nghệ hiện đại được áp dụng nhằm giải quyết hiệu quả các nhu cầu thực tế trong môi trường giáo dục số như: đăng ký học phần, tra cứu điểm, nộp bài tập, và quản lý công nợ sinh viên. Hệ thống được xây dựng hoàn toàn bằng PHP kết hợp với HTML, CSS và JavaScript, xử lý trực tiếp giữa giao diện người dùng và máy chủ mà không thông qua tầng API backend trung gian.

Tuy nhiên, để tăng tính thông minh và bảo mật, hệ thống vẫn tích hợp một số API quan trọng. Cụ thể, Google reCAPTCHA được sử dụng tại trang đăng nhập nhằm ngăn chặn các hành vi đăng nhập tự động từ bot, giúp bảo vệ hệ thống khỏi các cuộc tấn công brute-force hoặc dò mật khẩu. Ngoài ra, AI chatbot sử dụng Gemini API cũng được tích hợp nhằm hỗ trợ sinh viên tra cứu thông tin học vụ như lịch học, điểm số, hoặc hướng dẫn sử dụng hệ thống – mà không cần đến sự hỗ trợ trực tiếp từ nhân viên kỹ thuật.

Bên cạnh đó, hệ thống còn được tích hợp cơ chế quét mã độc tự động khi người dùng nộp bài, giúp phát hiện và ngăn chặn kịp thời các tệp tin có chứa đoạn mã nguy hiểm. Nếu phát hiện bất thường, hệ thống sẽ gửi email cảnh báo cho quản trị viên để xử lý. Ngoài ra, khi người dùng đăng nhập sai quá số lần cho phép, hệ thống sẽ kích hoạt tính năng xác thực OTP qua email, tăng cường lớp bảo vệ tài khoản.

Sự kết hợp giữa các công nghệ truyền thống (PHP thuần) và các dịch vụ hiện đại như reCAPTCHA, AI chatbot giúp hệ thống web học vụ không chỉ đơn giản, dễ vận hành mà còn thông minh, bảo mật và thân thiện với người dùng.

1.5. BỐ CỤC BÀI BÁO CÁO

GIAI ĐOẠN 1: GIAI ĐOẠN LÊN KẾ HOẠCH VÀ TÌM HIỂU VỀ CÔNG NGHỆ

CHƯƠNG 1: "GIỚI THIỆU CHUNG". Giới thiệu sơ về các công nghệ.

GIAI ĐOẠN 2: GIAI ĐOẠN PHÂN TÍCH

CHƯƠNG 2: "PHÂN TÍCH SÂU VÀO CÁC CÔNG NGHỆ". Phân tích sâu vào các công nghệ nhằm hiểu rõ hơn về lợi ích cũng nghe nguyên lý hoạt động của chúng

GIAI ĐOẠN 3: GIAI ĐOẠN KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

CHƯƠNG 3: "KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN". Tóm tắt lại, nêu rõ kết quả mà sản phẩm đạt được là gì và hướng phát triển trong tương lai.

CHƯƠNG 2: CÁC CÔNG NGHỆ SỬ DỤNG

2.1. PHP

2.1.1. Giới thiệu PHP và lý do lựa chọn

PHP là một ngôn ngữ lập trình mã nguồn mở chạy trên máy chủ, được sử dụng để tạo ra các trang web, ứng dụng, hệ thống quản lý quan hệ khách hàng và nhiều hơn nữa. Đây là một ngôn ngữ đa dụng được sử dụng rộng rãi và có thể nhúng vào HTML. Nhờ khả năng tích hợp với HTML, PHP vẫn được các nhà phát triển ưa chuộng vì giúp đơn giản hóa mã HTML..

Lý do lựa chọn:

- PHP – ngôn ngữ lập trình phía server mạnh mẽ và phổ biến: PHP được sử dụng để xử lý logic nghiệp vụ, kết nối cơ sở dữ liệu và quản lý các hoạt động như đăng nhập, đăng ký học phần, nộp bài, và quản lý điểm số. PHP có cộng đồng lớn, dễ học và hỗ trợ đa dạng thư viện cũng như framework, giúp phát triển nhanh chóng và hiệu quả.
- Dễ triển khai và bảo trì: Các công nghệ này không yêu cầu cấu hình phức tạp, có thể chạy trên nhiều môi trường hosting phổ biến với chi phí thấp, đồng thời dễ dàng nâng cấp và tích hợp thêm các tính năng mới trong tương lai.

2.1.2. Ứng dụng PHP trong hệ thống học vụ

Ứng dụng PHP trong hệ thống này cho phép tiếp nhận và xử lý các yêu cầu từ người dùng thông qua giao diện web, quản lý tương tác với cơ sở dữ liệu để lưu trữ và truy xuất thông tin như điểm số, danh sách học phần, và tình trạng công nợ. Đồng thời, PHP xử lý việc quét mã độc khi sinh viên nộp bài, gửi email cảnh báo khi phát hiện hành vi bất thường nhằm đảm bảo an toàn cho hệ thống.

Nhờ khả năng mở rộng và sự linh hoạt trong phát triển, PHP là nền tảng phù hợp để xây dựng hệ thống web học vụ quy mô, đảm bảo vận hành trơn tru và dễ dàng bảo trì trong môi trường giáo dục hiện đại.

2.2. GOOGLE reCAPTCHA

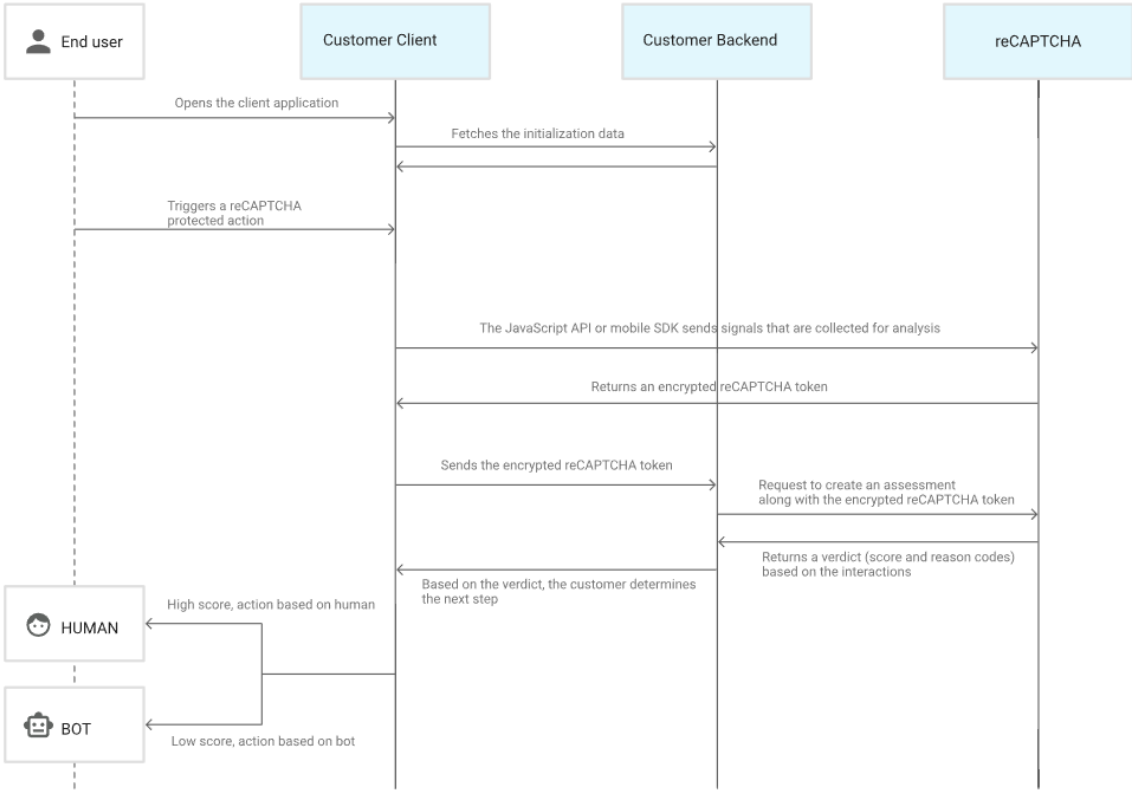
2.2.1. Tổng quan về GOOGLE reCAPTCHA

Google reCAPTCHA là một dịch vụ bảo mật miễn phí do Google phát triển, nhằm bảo vệ các trang web khỏi các hành vi tự động như spam, đăng nhập trái

phép hoặc các cuộc tấn công bot. reCAPTCHA giúp phân biệt giữa người dùng thực và phần mềm tự động thông qua việc yêu cầu người dùng thực hiện các thao tác như chọn hình ảnh, đánh dấu checkbox hoặc các bài kiểm tra tương tác đơn giản.

Google reCAPTCHA ra đời dựa trên nền tảng của dự án CAPTCHA truyền thống (Completely Automated Public Turing test to tell Computers and Humans Apart) – một bài kiểm tra Turing tự động hoàn toàn nhằm phân biệt người và máy. Tuy nhiên, Google đã phát triển reCAPTCHA theo hướng thông minh hơn, dễ sử dụng và hiệu quả hơn cho người dùng thực sự, đồng thời bảo vệ hệ thống một cách mạnh mẽ.

2.2.2 Cấu trúc reCAPTCHA



Hình 2.1. Cấu trúc tổng quan reCAPTCHA

Nguồn: Sưu tầm trên Internet

2.2.3. Vì sao chọn reCAPTCHA?

Google reCAPTCHA dựa trên nhiều công nghệ và thuật toán phức tạp, trong đó bao gồm:

- Thu thập dữ liệu hành vi: reCAPTCHA thu thập và phân tích các thông

tin như cách người dùng di chuyển chuột, nhấn phím, thời gian thao tác, và các tín hiệu mạng để đánh giá xem người dùng có phải là bot hay không.

- Machine Learning và AI: Google sử dụng các mô hình học máy (machine learning) để phân tích dữ liệu hành vi người dùng và cải thiện liên tục khả năng phát hiện bot. Mô hình này dựa trên dữ liệu lớn từ hàng triệu lượt truy cập trên toàn thế giới.

- Xử lý thử thách (Challenge): Khi hệ thống nghi ngờ, reCAPTCHA sẽ đưa ra các thử thách như chọn ảnh đúng theo yêu cầu, nhận dạng văn bản, hoặc thậm chí câu hỏi đơn giản để đảm bảo người dùng là con người.

2.3.4. Ứng dụng thực tiễn của reCAPTCHA

Trong hệ thống web học vụ, Google reCAPTCHA được ứng dụng chủ yếu để:

- Ngăn chặn đăng nhập trái phép: Bảo vệ form đăng nhập khỏi các tấn công brute-force, tự động thử mật khẩu.

- Chống spam trong các form liên hệ, đăng ký: Giúp lọc bỏ các đăng ký tài khoản giả hoặc gửi form tự động từ bot.

- Bảo vệ hệ thống nộp bài tập: Ngăn chặn bot thực hiện thao tác nộp bài hoặc tải file tự động gây ảnh hưởng đến hệ thống.

2.3. CƠ CHẾ QUÉT MÃ ĐỘC KHI NỘP BÀI

2.3.1. Tổng quan

Trong môi trường học tập trực tuyến, việc sinh viên nộp bài qua các tệp tin như Word, PDF, ZIP,... là điều phổ biến. Tuy nhiên, các file này có thể chứa mã độc, mã lệnh độc hại gây tổn hại đến hệ thống quản lý học vụ nếu không được kiểm soát nghiêm ngặt.

Theo báo cáo của [CERT/CC 2023], hơn 30% các vụ tấn công qua web ứng dụng bắt nguồn từ việc tải lên file chứa mã độc. Do vậy, hệ thống quản lý học vụ cần được trang bị cơ chế quét mã độc hiệu quả để giảm thiểu rủi ro [3].

2.3.2. Công nghệ và cơ chế thực thi

Phân tích tĩnh (Static analysis): Phân tích mã nguồn hoặc nội dung file mà

không cần thực thi, bằng cách tìm kiếm các từ khóa nguy hiểm, hàm hệ thống nhạy cảm (eval(), exec(), base64_decode(),...). Đây là phương pháp được triển khai phổ biến trong hệ thống web sử dụng PHP.

Cơ chế thực thi

- Kiểm tra nội dung file nộp: PHP sử dụng các hàm như file_get_contents(), preg_match() để đọc và phân tích file.
- Giải nén file nén: Sử dụng các thư viện PHP như ZipArchive để mở và kiểm tra từng file bên trong.
- Tự động cách ly file nghi ngờ: Không cho phép lưu trữ hoặc xử lý file khi phát hiện nghi vấn.
- Gửi cảnh báo: Tự động gửi email cảnh báo cho người dùng và quản trị viên.

2.3.3. Ưu điểm và hạn chế

Ưu điểm	Hạn chế
Phát hiện kịp thời các file nguy hiểm.	Có thể bỏ sót nếu mã độc được mã hóa phức tạp.
Giúp bảo vệ toàn vẹn hệ thống và dữ liệu.	Tốn tài nguyên nếu số lượng file lớn.
Giảm thiểu rủi ro bảo mật cho người dùng và nhà trường.	Đòi hỏi cập nhật chữ ký liên tục.

Bảng 2.1: Ưu điểm – hạn chế quét mã độc

2.3.4. Ứng dụng trong web học vụ

Trong hệ thống web học vụ, cơ chế quét mã độc đóng vai trò quan trọng trong việc đảm bảo an toàn thông tin. Hệ thống có khả năng tự động kiểm tra các tệp được sinh viên nộp bài, nhằm phát hiện sớm những file có dấu hiệu nguy hiểm. Các tệp chứa mã độc sẽ bị ngăn chặn lưu trữ trên máy chủ, từ đó giảm thiểu nguy cơ gây lỗi hệ thống hoặc mất mát dữ liệu. Đồng thời, hệ thống sẽ gửi cảnh báo tự động qua email đến người dùng và quản trị viên để có thể kịp thời xử lý. Cơ chế này góp phần tạo ra một môi trường học tập an toàn, nâng cao sự tin tưởng của người sử dụng đối với hệ thống.

2.4. Cơ chế gửi email và xác thực OTP qua email

2.4.1. Giới thiệu chung

Hệ thống gửi email tự động sử dụng các dịch vụ SMTP (Simple Mail Transfer Protocol) hoặc các API gửi email của bên thứ ba (như SendGrid, Mailgun, Amazon SES) để gửi các thông báo hoặc cảnh báo đến người dùng.

Cơ chế hoạt động

- Phát hiện hành vi bất thường: Hệ thống liên tục theo dõi các hành vi đăng nhập hoặc nộp bài, phát hiện các dấu hiệu khả nghi như đăng nhập thất bại nhiều lần, nộp bài chứa mã độc.

- Kích hoạt gửi email: Khi có hành vi bất thường, hệ thống tự động tạo email cảnh báo và gửi đến địa chỉ email đã đăng ký của người dùng.

- Nội dung email: Thường bao gồm thông báo về hành vi bất thường, hướng dẫn các bước cần thiết,hoặc chứa mã OTP để xác thực.

- Gửi email: Email được gửi qua máy chủ SMTP hoặc dịch vụ email để đảm bảo chuyển đến hộp thư của người dùng một cách nhanh chóng và an toà.

Xác thực OTP qua email

Xác thực OTP qua email là quá trình người dùng nhận một mã số (thường là dãy số ngẫu nhiên 6-8 chữ số) gửi đến email, và phải nhập mã này vào hệ thống để xác nhận danh tính hoặc hoàn tất một thao tác quan trọng như đăng nhập hoặc thay đổi mật khẩu.

Quy trình xác thực OTP:

- Yêu cầu OTP: Khi người dùng vượt quá số lần đăng nhập thất bại hoặc có dấu hiệu nghi ngờ, hệ thống yêu cầu xác thực OTP.

- Tạo mã OTP: Mã OTP được tạo ngẫu nhiên và có tính duy nhất để tăng tính bảo mật.

- Gửi mã OTP qua email: Mã OTP được gửi tự động đến email người dùng.

- Nhập mã OTP: Người dùng nhập mã OTP trên giao diện hệ thống để xác nhận.

- Xác nhận và xử lý: Nếu mã OTP đúng và còn hiệu lực, người dùng được phép tiếp tục đăng nhập hoặc thực hiện thao tác. Nếu sai hoặc hết hạn, hệ thống yêu cầu gửi lại mã hoặc khóa tạm thời tài khoản.

2.5. Tích hợp Chatbot Gemini API

2.5.1. Giới thiệu chung

Chatbot Gemini API là một dịch vụ API cung cấp chức năng chatbot thông minh dựa trên mô hình AI tiên tiến của Google Gemini (thế hệ AI mới của Google, kết hợp các kỹ thuật học máy để xử lý ngôn ngữ tự nhiên). Chatbot này có khả năng hiểu, phân tích và trả lời các câu hỏi từ người dùng một cách tự nhiên và chính xác.

Cơ chế hoạt động

Cấu trúc API thường gồm các thành phần chính như: Endpoint (địa chỉ URL để gửi yêu cầu), Request (dữ liệu đầu vào do người dùng gửi), Response (kết quả phản hồi từ API), và Authentication (cơ chế xác thực như API key hoặc OAuth để đảm bảo bảo mật). Các thành phần này giúp API hoạt động hiệu quả và an toàn.

Quy trình hoạt động của API diễn ra như sau: Người dùng nhập câu hỏi hoặc yêu cầu trên giao diện học vụ, sau đó ứng dụng gửi dữ liệu này qua HTTP request (POST/GET) đến endpoint của Gemini API kèm theo các tham số cần thiết. API sẽ xử lý truy vấn bằng mô hình AI để phân tích nội dung và trả về câu trả lời. Cuối cùng, ứng dụng hiển thị phản hồi một cách thân thiện cho người dùng.

2.5.2. Ứng dụng thực tiễn của Chatbot Gemini API

Chatbot Gemini API được ứng dụng rộng rãi trong nhiều lĩnh vực thực tiễn như: hỗ trợ khách hàng bằng cách tự động giải đáp thắc mắc về sản phẩm, dịch vụ; tư vấn trong y tế và tài chính với thông tin nhanh chóng, chính xác; hỗ trợ giáo dục qua việc tra cứu bài giảng, giải bài tập; và ứng dụng trong nông nghiệp thông minh hay dịch vụ công để hướng dẫn kỹ thuật, quy trình, thủ tục.

2.5.3. Ứng dụng trong hệ thống web học vụ

Trong hệ thống học vụ trực tuyến, việc tích hợp Chatbot Gemini API mang lại nhiều lợi ích thiết thực. Chatbot giúp tra cứu thông tin học vụ nhanh chóng như lịch học, điểm số, thủ tục mà không cần chờ đợi. Ngoài ra, nó hỗ trợ giải đáp thắc mắc về bài giảng, bài tập, giúp học viên học tập hiệu quả hơn. Chatbot hoạt động 24/7, giảm tải cho giảng viên và nhân viên hành chính, đồng thời cá nhân hóa trải nghiệm học tập bằng cách gợi ý tài liệu phù hợp với từng người dùng.

2.4.5. Kết luận

Việc tích hợp Chatbot Gemini API vào hệ thống học vụ giúp nâng cao trải nghiệm người dùng, tối ưu hóa hỗ trợ học tập và giảm thiểu chi phí vận hành. Đây là một ứng dụng công nghệ AI hiện đại mang tính thực tiễn cao, phù hợp với xu hướng chuyển đổi.

CHƯƠNG 3: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

3.1. TÓM TẮT LẠI CÁC CÔNG NGHỆ ĐÃ SỬ DỤNG

Trong quá trình phát triển hệ thống web học vụ, nhóm đã tích hợp nhiều công nghệ hiện đại như cơ chế quét mã độc bằng PHP, Google reCAPTCHA và xác thực OTP qua email nhằm nâng cao bảo mật. Chatbot Gemini API hỗ trợ tra cứu thông tin và giải đáp học vụ nhanh chóng. Hệ thống còn tự động gửi email cảnh báo khi phát hiện hành vi bất thường. Những giải pháp này góp phần nâng cao trải nghiệm và đảm bảo an toàn cho người dùng.

3.2. HIỆU QUẢ ĐẠT ĐƯỢC KHI ÁP DỤNG CÔNG NGHỆ MỚI

Việc áp dụng các công nghệ mới mang lại nhiều lợi ích rõ rệt:

- Bảo mật được tăng cường nhờ cơ chế quét mã độc tự động và xác thực OTP, giảm thiểu rủi ro tấn công hoặc truy cập trái phép.
- Ngăn chặn hiệu quả các hành vi gian lận và bot với Google reCAPTCHA, giữ cho môi trường học tập trực tuyến công bằng và minh bạch.
- Tăng trải nghiệm người dùng với chatbot Gemini API, giúp học sinh, sinh viên dễ dàng tiếp cận thông tin, giải đáp nhanh các thắc mắc mà không cần phải chờ đợi sự hỗ trợ từ nhân viên.
- Tự động hóa cảnh báo bảo mật qua email giúp đội ngũ quản trị kịp thời phát hiện và xử lý các tình huống bất thường, từ đó giảm thiểu thiệt hại có thể xảy ra.

3.3. ĐỀ XUẤT CẢI TIẾN/HƯỚNG MỞ RỘNG TRONG TƯƠNG LAI

Trong tương lai, hệ thống có thể được cải tiến và phát triển thêm ở các hướng sau:

- Nâng cấp cơ chế quét mã độc với các thuật toán phức tạp hơn hoặc sử dụng trí tuệ nhân tạo để phát hiện nhanh và chính xác các nguy cơ bảo mật mới.
- Mở rộng ứng dụng xác thực đa yếu tố (MFA) không chỉ qua email mà còn qua tin nhắn SMS hoặc các ứng dụng xác thực khác để tăng cường bảo mật tài khoản.
- Tối ưu và nâng cao hiệu quả của chatbot Gemini API với khả năng nhận diện ngôn ngữ tự nhiên và hỗ trợ đa ngôn ngữ, giúp phục vụ đa dạng đối tượng người dùng.
- Xây dựng hệ thống báo cáo và phân tích hành vi người dùng dựa trên dữ liệu thu thập, từ đó cải thiện dịch vụ và phát hiện sớm các hành vi bất thường.

LỜI CẢM ƠN

Để hoàn thành được đề án này, em xin chân thành cảm ơn thầy Võ Ngọc Tấn Phước đã tận tình giúp đỡ và tạo điều kiện cho em trong quá trình học tập.
Trong quá trình thực hiện bài tiểu luận này, do hiểu biết còn nhiều hạn chế nên bài làm khó tránh khỏi những thiếu sót. Em rất mong nhận được những lời góp ý của quý thầy cô để bài tiểu luận ngày càng hoàn thiện hơn.
Em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

Developers, G. (2023). *Tạo cuộc trò chuyện (trò chuyện) nhiều lượt bằng API Gemini*. From Firebase: https://firebase.google.com/docs/ai-logic/chat?hl=vi&api=dev

Duy, N. (2022). *Ngôn ngữ lập trình PHP là gì? Tất tần tật những điều bạn cần biết về PHP*. From topdev.vn: https://topdev.vn/blog/ngon-ngu-lap-trinh-php-la-gi-tat-tan-tat-nhung-dieu-ban-can-biet-ve-php/

Mr.Son. (n.d.). *reCAPTCHA overview* . From Cloud Google: https://cloud.google.com/recaptcha/docs/overview

Rebelo, M. (2024, 7 8). *Google Gemini API: How to create a key and use the Gemini API*. From Zapier: http://zapier.com/blog/gemini-api/