

ĐẠI HỌC HUẾ
TRƯỜNG ĐẠI HỌC KHOA HỌC
KHOA CÔNG NGHỆ THÔNG TIN



TIỂU LUẬN CUỐI KỲ

ĐỀ TÀI:

HỆ THỐNG CẢNH BÁO TRỘM DỰA TRÊN ESP32
VÀ CẢM BIẾN CHUYỂN ĐỘNG

Huế, tháng 04 năm 2025

LỜI CẢM ƠN

Trước tiên, em xin bày tỏ lòng biết ơn sâu sắc đến **thầy Võ Việt Dũng**, người đã tận tình hướng dẫn, chỉ bảo và hỗ trợ em trong suốt quá trình thực hiện tiểu luận này. Những kiến thức quý báu, sự tận tâm và tinh thần trách nhiệm của Thầy không chỉ giúp em hoàn thành bài tiểu luận một cách tốt nhất mà còn truyền cho em cảm hứng và động lực lớn trong quá trình học tập và nghiên cứu.

Em cũng xin gửi lời tri ân chân thành đến Ban Giám hiệu, các thầy cô giáo và toàn thể cán bộ Trường Đại học Khoa học, Đại học Huế. Nhà trường không chỉ mang đến cho em một môi trường học tập lý tưởng mà còn trang bị cho em nền tảng kiến thức vững chắc để em có thể tự tin thực hiện đề tài này. Những bài giảng và sự chỉ dẫn tận tình của quý thầy cô là hành trang quý giá để em phát triển bản thân trên con đường học vấn và sự nghiệp sau này.

Cuối cùng, nhưng không kém phần quan trọng, em muốn dành sự biết ơn sâu sắc đến gia đình thân yêu, các bạn học cùng lớp – những người luôn ở phía sau, âm thầm ủng hộ và tiếp thêm sức mạnh cho em trong mọi chặng đường. Chính sự hy sinh, tình yêu thương và niềm tin của gia đình và bạn bè đã giúp em kiên trì vượt qua mọi khó khăn để hoàn thành bài tiểu luận này.

Một lần nữa, em xin chân thành cảm ơn tất cả những người đã giúp đỡ, đồng hành và truyền cảm hứng cho em trong suốt quá trình thực hiện đề tài.

Tp Huế, tháng 04 năm 2025

MỤC LỤC

LỜI NÓI ĐẦU.....	1
CHƯƠNG I : GIỚI THIỆU	3
1. Khảo sát hiện trạng.....	3
1.1. Phân tích hiện trạng	3
1.2. Cơ hội.....	3
1.3. Thách thức.....	4
1.4. Đánh giá chung	5
2. Lý do lựa chọn đề tài	5
3. Mục tiêu nghiên cứu	6
4. Phạm vi nghiên cứu	6
5. Phương pháp nghiên cứu	7
5.1. Nghiên cứu tài liệu.....	7
5.2. Mô phỏng và thực nghiệm	7
5.3. Phân tích và đánh giá	8
CHƯƠNG II : TỔNG QUAN VỀ HỆ THỐNG CẢNH BÁO TRỘM.....	9
1. Định nghĩa IoT	9
2. Các thành phần chính của hệ thống IoT	9
3. Hệ thống cảnh báo trộm là gì?.....	10
4. Các thành phần của hệ thống cảnh báo trộm	10
5. Các loại hệ thống cảnh báo trộm.....	12
6. Các phương pháp phát hiện xâm nhập phổ biến.....	12
7. Ứng dụng IoT trong hệ thống cảnh báo trộm	14
7.1. Nguyên lý hoạt động của hệ thống cảnh báo trộm IoT.....	14
7.2. Ưu điểm của hệ thống cảnh báo trộm IoT	15
7.3. Ứng dụng thực tế.....	15
CHƯƠNG III. PHẦN CỨNG VÀ PHẦN MỀM SỬ DỤNG	16
1. Phần cứng	16
1.1. ESP32 – Tổng quan và tính năng.....	16
1.2. Ứng dụng của ESP32 trong hệ thống cảnh báo trộm.....	17

1.3. Cảm biến PIR – Nguyên lý hoạt động và ứng dụng	17
1.4. Các linh kiện hỗ trợ khác	18
2. Phần mềm	19
2.1. Wokwi – Mô phỏng hệ thống.....	19
2.2. Arduino IDE, Visual Studio Code – Lập trình ESP32	19
2.3. Telegram API / SMTP Email – Gửi cảnh báo	19
CHƯƠNG IV. THIẾT KẾ HỆ THỐNG.....	20
1. Sơ đồ khối hệ thống	20
2. Sơ đồ nguyên lý (Thiết kế mạch trên Wokwi).....	21
3. Nguyên lý hoạt động của hệ thống	22
CHƯƠNG V. LẬP TRÌNH VÀ TRIỂN KHAI.....	25
1. Cấu hình ESP32 kết nối WiFi.....	25
2. Code hệ thống cảnh báo trộm bằng ESP32 và cảm biến PIR	26
CHƯƠNG VI. KIỂM THỬ VÀ ĐÁNH GIÁ	31
1. Các trường hợp kiểm thử và kết quả.....	31
2. Đánh giá hiệu quả hệ thống	32
CHƯƠNG VII. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	34
1. Kết luận về hệ thống	34
2. Hướng phát triển trong tương lai.....	34
TÀI LIỆU THAM KHẢO.....	37

LỜI NÓI ĐẦU

Trong thời đại công nghệ phát triển như vũ bão, con người ngày càng tận dụng những thành tựu khoa học kỹ thuật để nâng cao chất lượng cuộc sống. Một trong những xu hướng nổi bật nhất hiện nay chính là Smart Home (nhà thông minh) – nơi mọi thiết bị được tự động hóa, tối ưu hóa để mang lại sự tiện nghi, hiện đại và an toàn cho người dùng. Từ việc điều khiển ánh sáng, nhiệt độ, cho đến việc giám sát an ninh, tất cả đều có thể thực hiện chỉ với vài thao tác trên điện thoại thông minh hoặc máy tính bảng. Điều này không chỉ giúp con người tiết kiệm thời gian, công sức mà còn đảm bảo cuộc sống thoải mái và an toàn hơn bao giờ hết.

Tuy nhiên, cùng với sự phát triển không ngừng của công nghệ, vấn đề an ninh và bảo vệ tài sản lại trở thành một mối quan tâm hàng đầu. Từ xa xưa, con người đã ý thức được tầm quan trọng của việc bảo vệ tài sản cá nhân. Nếu trước đây, các phương pháp bảo vệ chủ yếu dựa vào cổng rào, ổ khóa cơ học, thì ngày nay, những ổ khóa điện tử và các hệ thống báo động đã dần trở thành lựa chọn phổ biến hơn. Tuy nhiên, dù tiến tiến đến đâu, các loại khóa truyền thống hay khóa điện tử vẫn có thể bị vô hiệu hóa bởi những tên trộm tinh vi. Chính vì thế, nhu cầu về một hệ thống cảnh báo xâm nhập thông minh, có khả năng phát hiện và cảnh báo ngay lập tức khi có sự xâm nhập trái phép, là vô cùng cần thiết.

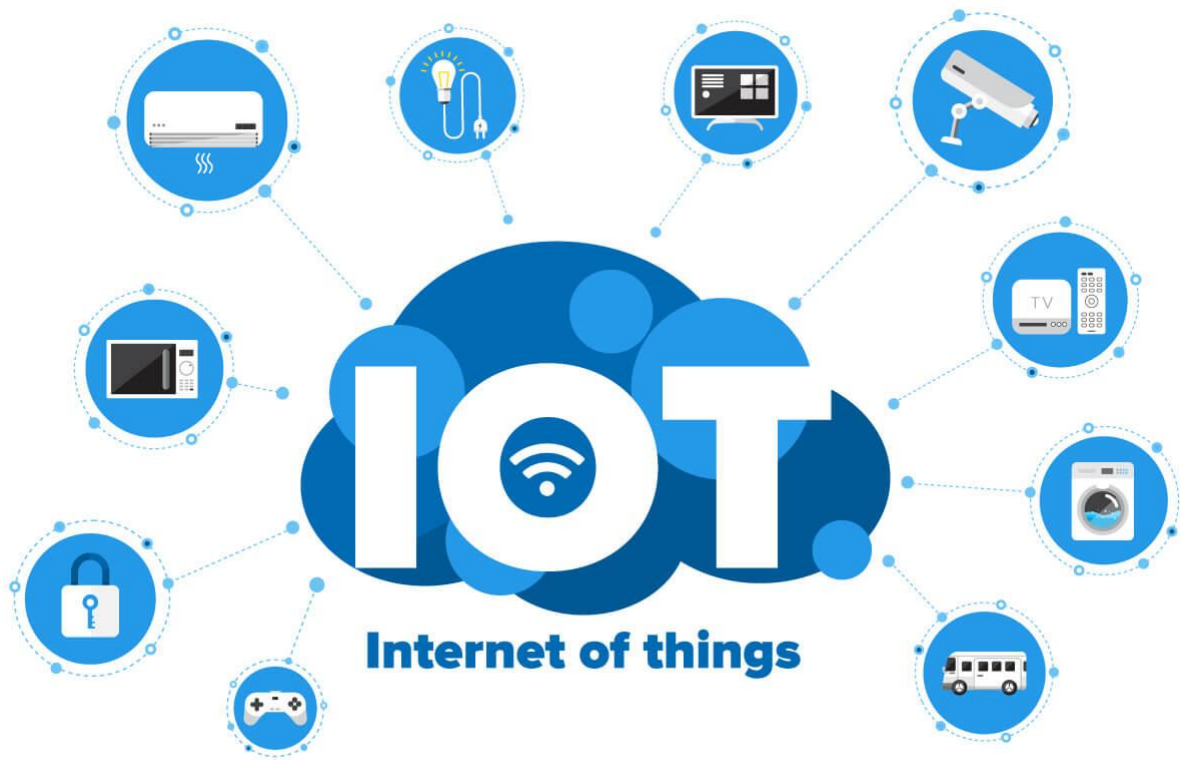
Xuất phát từ thực tế đó, em đã chọn đề tài "**Hệ thống cảnh báo trộm dựa trên ESP32 và cảm biến chuyển động**" để nghiên cứu và phát triển trong tiểu luận này. Hệ thống này sẽ sử dụng cảm biến PIR (Passive Infrared Sensor) để phát hiện chuyển động, kết hợp với ESP32 để xử lý dữ liệu và gửi cảnh báo ngay lập tức đến người dùng thông qua Telegram hoặc Email. Khi có sự xâm nhập trái phép, hệ thống không chỉ thông báo đến chủ nhà mà còn có thể kích hoạt còi báo động để răn đe kẻ trộm, giúp nâng cao hiệu quả bảo vệ an ninh.

Bài tiểu luận này sẽ trình bày chi tiết về nguyên lý hoạt động, thiết kế phần cứng, lập trình hệ thống và các phương thức truyền tin nhắn cảnh báo, nhằm tạo ra một giải pháp an ninh đơn giản, hiệu quả và dễ ứng dụng trong thực tế. Hy vọng rằng hệ thống này

có thể góp phần giúp nâng cao an ninh cho các hộ gia đình, đặc biệt là trong các mô hình Smart Home và căn hộ chung cư hiện đại.

Em xin chân thành cảm ơn giảng viên hướng dẫn và các thầy cô trong khoa đã tạo điều kiện để em thực hiện nghiên cứu này. Em mong rằng bài tiểu luận sẽ cung cấp những thông tin hữu ích và nhận được sự đóng góp ý kiến từ thầy cô để hoàn thiện hơn nữa.

CHƯƠNG I : GIỚI THIỆU



Hình 1: Mô hình Internet of Things (IoT)

1. Khảo sát hiện trạng

1.1. Phân tích hiện trạng

Hiện nay, nhu cầu về các hệ thống an ninh thông minh ngày càng gia tăng do tình trạng trộm cắp diễn biến phức tạp và các phương pháp bảo vệ truyền thống như khóa cửa, camera giám sát chưa thực sự hiệu quả trong việc cảnh báo tức thời. Việc áp dụng công nghệ IoT vào hệ thống cảnh báo trộm là một xu hướng mới giúp cải thiện độ an toàn cho các hộ gia đình, doanh nghiệp và chung cư. Tuy nhiên, quá trình triển khai hệ thống này cũng gặp phải nhiều cơ hội và thách thức.

1.2. Cơ hội

Xu hướng ứng dụng công nghệ trong đời sống: Người dùng ngày càng quen thuộc với các thiết bị công nghệ thông minh như Smarthome, camera giám sát có kết nối

Internet, hệ thống điều khiển từ xa qua ứng dụng di động. Điều này tạo điều kiện thuận lợi cho việc triển khai hệ thống cảnh báo trộm dựa trên IoT.

Nguồn tài nguyên phong phú: Có nhiều tài liệu, blog hướng dẫn, thư viện mã nguồn mở về ESP32, cảm biến PIR và các nền tảng như Telegram API, Wokwi giúp cho việc nghiên cứu và triển khai hệ thống trở nên dễ dàng hơn.

Chi phí triển khai ngày càng hợp lý: Nhờ sự phát triển của các thiết bị vi điều khiển giá rẻ như ESP32 và các dịch vụ miễn phí hỗ trợ gửi thông báo như Telegram, hệ thống cảnh báo trộm có thể được triển khai với chi phí thấp hơn so với các hệ thống an ninh truyền thống.

Khả năng mở rộng cao: Hệ thống có thể được nâng cấp dễ dàng bằng cách tích hợp thêm các cảm biến khác như cảm biến cửa từ, cảm biến âm thanh, camera AI để nhận diện khuôn mặt hoặc kết nối với hệ thống nhà thông minh.

1.3. Thách thức

Yêu cầu kiến thức đa lĩnh vực: Việc triển khai hệ thống cảnh báo trộm bằng IoT không chỉ đòi hỏi kiến thức về lập trình nhúng (ESP32, Arduino) mà còn cần hiểu về giao tiếp mạng, bảo mật dữ liệu và các giao thức truyền thông như MQTT, HTTP. Điều này đòi hỏi người thực hiện phải đầu tư nhiều thời gian vào việc nghiên cứu và thực hành.

Hạn chế về kinh nghiệm thực tế: Dù có nhiều tài liệu hướng dẫn, nhưng khi áp dụng vào thực tế, có thể phát sinh nhiều vấn đề như độ trễ khi gửi cảnh báo, sai số của cảm biến PIR, hoặc mất kết nối do sự cố mạng. Việc xử lý những vấn đề này đòi hỏi kinh nghiệm và khả năng phân tích lỗi tốt.

Chưa có kinh nghiệm về quản lý hệ thống lớn: Hệ thống cảnh báo trộm trong phạm vi nhỏ như nhà ở hoặc văn phòng có thể dễ dàng triển khai, nhưng khi mở rộng cho nhiều khu vực hoặc tích hợp vào hệ thống Smarthome lớn, các vấn đề như bảo mật dữ liệu, quản lý nhiều thiết bị cùng lúc, khả năng mở rộng hệ thống sẽ trở thành những thách thức lớn.

Phụ thuộc vào kết nối mạng: Hệ thống dựa trên ESP32 để gửi cảnh báo qua Internet, vì vậy nếu mạng WiFi bị gián đoạn, hệ thống có thể không hoạt động hiệu quả. Điều này đòi hỏi phải có phương án dự phòng như sử dụng mạng di động GSM hoặc hệ thống cảnh báo nội bộ (báo động còi, đèn nháy).

1.4. Đánh giá chung

Mặc dù hệ thống cảnh báo trộm sử dụng ESP32 và cảm biến PIR có nhiều ưu điểm về chi phí và tính linh hoạt, nhưng vẫn cần được tối ưu để hoạt động hiệu quả trong thực tế. Việc tận dụng các nguồn tài nguyên sẵn có, kết hợp với phương pháp nghiên cứu và thử nghiệm thực tế sẽ giúp khắc phục các thách thức trên, tạo ra một hệ thống an toàn, ổn định và đáng tin cậy.

2. Lý do lựa chọn đề tài

Trong thời đại công nghệ phát triển mạnh mẽ, nhu cầu đảm bảo an ninh cho các hộ gia đình, cửa hàng, văn phòng và các tòa nhà ngày càng trở nên cấp thiết. Các phương pháp bảo vệ truyền thống như ổ khóa cơ, cửa sắt, hệ thống camera giám sát tuy vẫn được sử dụng rộng rãi nhưng dần bộc lộ những hạn chế. Đặc biệt, nhiều vụ trộm cắp hiện nay có sự tinh vi và chuyên nghiệp hóa cao, khiến các phương pháp bảo vệ truyền thống trở nên kém hiệu quả.

Một trong những giải pháp tiên tiến nhất hiện nay là ứng dụng công nghệ **IoT (Internet of Things)** trong hệ thống an ninh. Với khả năng kết nối thiết bị qua Internet, các hệ thống này không chỉ giúp phát hiện xâm nhập mà còn có thể gửi cảnh báo tức thời đến người dùng thông qua các nền tảng như Telegram, Email hoặc các ứng dụng giám sát từ xa. Trong đó, cảm biến PIR (Passive Infrared Sensor) kết hợp với ESP32 được xem là một trong những phương án hiệu quả, chi phí thấp và dễ dàng triển khai để phát hiện chuyển động và gửi cảnh báo nhanh chóng.

Bên cạnh đó, việc sử dụng mô phỏng trên **Wokwi** giúp tiết kiệm thời gian và chi phí, đồng thời đảm bảo rằng hệ thống có thể được kiểm tra kỹ lưỡng trước khi triển khai thực tế. Do đó, với đề tài tiểu luận này, em mong muốn nghiên cứu và xây dựng một hệ thống cảnh báo trộm thông minh, có khả năng giám sát, phát hiện xâm nhập và gửi thông báo

tức thời, góp phần nâng cao mức độ an toàn cho các hộ gia đình, đặc biệt là trong các mô hình nhà thông minh (Smart Home).

3. Mục tiêu nghiên cứu

Mục tiêu chính của đề tài này là thiết kế và xây dựng một hệ thống cảnh báo trộm sử dụng ESP32 và cảm biến PIR, có khả năng phát hiện chuyển động và gửi cảnh báo ngay lập tức đến người dùng qua Telegram hoặc Email. Hệ thống cần đảm bảo các tiêu chí sau:

- **Phát hiện chuyển động chính xác:** Cảm biến PIR phải hoạt động ổn định, nhận diện nhanh các chuyển động bất thường trong khu vực giám sát.
- **Gửi cảnh báo tức thời:** Khi phát hiện xâm nhập, hệ thống phải ngay lập tức gửi tin nhắn đến người dùng qua Telegram hoặc Email để họ có biện pháp xử lý kịp thời.
- **Hoạt động ổn định và tiết kiệm năng lượng:** ESP32 cần được lập trình để tối ưu hóa mức tiêu thụ năng lượng, đảm bảo hệ thống có thể hoạt động liên tục mà không tốn quá nhiều điện năng.
- **Dễ dàng triển khai và mở rộng:** Hệ thống có thể được tích hợp thêm nhiều loại cảm biến khác (như cảm biến cửa, cảm biến âm thanh) để nâng cao tính hiệu quả.
- **Mô phỏng trên nền tảng Wokwi:** Việc sử dụng Wokwi giúp kiểm thử và đánh giá hệ thống một cách toàn diện trước khi ứng dụng vào thực tế.

Thông qua đề tài này, em mong muốn không chỉ hiểu rõ hơn về nguyên lý hoạt động của các thiết bị IoT mà còn có thể áp dụng những kiến thức đã học vào thực tế, từ đó nâng cao kỹ năng nghiên cứu, lập trình và triển khai hệ thống thông minh.

4. Phạm vi nghiên cứu

Do tính chất của một tiểu luận chuyên ngành, phạm vi nghiên cứu của đề tài này sẽ tập trung vào các nội dung sau:

- **Nghiên cứu nguyên lý hoạt động của cảm biến PIR:** Tìm hiểu cách thức cảm biến hồng ngoại thụ động hoạt động, phạm vi quét, khả năng phát hiện chuyển động và những yếu tố ảnh hưởng đến độ chính xác của nó.
- **Ứng dụng ESP32 trong hệ thống IoT:** Phân tích cách ESP32 hoạt động như một bộ điều khiển trung tâm, quản lý dữ liệu từ cảm biến và gửi thông báo qua mạng WiFi.
- **Gửi tin nhắn cảnh báo qua Telegram hoặc Email:** Sử dụng các API có sẵn để gửi cảnh báo khi phát hiện chuyển động. So sánh ưu nhược điểm của hai phương thức này.
- **Mô phỏng trên Wokwi:** Xây dựng mô hình hệ thống trên nền tảng Wokwi, đảm bảo mô phỏng hoạt động của các linh kiện điện tử một cách chính xác mà không cần phần cứng thực tế.
- **Không đi sâu vào phần cứng chuyên sâu:** Đề tài chỉ tập trung vào lập trình và mô phỏng, không yêu cầu sản xuất thiết bị thực tế.

Ngoài ra, nghiên cứu này sẽ chỉ tập trung vào việc phát hiện chuyển động và gửi cảnh báo, không bao gồm các tính năng phức tạp hơn như nhận diện khuôn mặt, tích hợp AI hoặc hệ thống giám sát video.

5. Phương pháp nghiên cứu

Để đảm bảo tính chính xác và hiệu quả của hệ thống, đề tài sẽ áp dụng các phương pháp nghiên cứu sau:

5.1. Nghiên cứu tài liệu

- Thu thập và tổng hợp các tài liệu liên quan đến **ESP32**, cảm biến **PIR**, giao thức truyền thông (MQTT, HTTP, API Telegram, SMTP Email) từ các nguồn uy tín như sách, báo cáo khoa học, trang web công nghệ.
- Tham khảo các dự án tương tự để hiểu rõ hơn về cách triển khai hệ thống cảnh báo trong thực tế.

5.2. Mô phỏng và thực nghiệm

- **Sử dụng Wokwi để mô phỏng hệ thống:** Tiến hành xây dựng mô hình mô phỏng trên nền tảng Wokwi, kiểm tra khả năng giao tiếp giữa các linh kiện và đánh giá hiệu suất hoạt động.
- **Thử nghiệm với các tình huống khác nhau:** Kiểm tra hệ thống trong nhiều điều kiện khác nhau như ánh sáng yếu, môi trường có nhiều chuyển động để đánh giá độ nhạy và chính xác của cảm biến PIR.

5.3. Phân tích và đánh giá

- **Kiểm tra tính ổn định:** Đánh giá khả năng hoạt động liên tục của hệ thống, mức tiêu thụ năng lượng và độ trễ trong việc gửi cảnh báo.
- **So sánh các phương thức gửi cảnh báo:** Phân tích ưu nhược điểm của việc gửi tin nhắn qua Telegram và Email để lựa chọn phương án phù hợp nhất.
- **Đề xuất giải pháp cải tiến:** Dựa vào kết quả thực nghiệm, đề xuất các cải tiến để nâng cao độ chính xác và hiệu suất của hệ thống trong tương lai.

CHƯƠNG II : TỔNG QUAN VỀ HỆ THỐNG CẢNH BÁO TRỘM

1. Định nghĩa IoT

Internet of Things (IoT) hay "Mạng lưới vạn vật kết nối Internet" là một hệ thống các thiết bị vật lý được kết nối với nhau qua Internet, cho phép chúng thu thập, trao đổi và xử lý dữ liệu mà không cần sự can thiệp của con người. Các thiết bị này có thể là cảm biến, vi điều khiển, máy móc công nghiệp, thiết bị gia dụng thông minh, phương tiện giao thông và nhiều loại thiết bị khác.

2. Các thành phần chính của hệ thống IoT

Một hệ thống IoT đầy đủ thường bao gồm các thành phần sau:

a, Thiết bị và cảm biến IoT

- Cảm biến nhiệt độ, độ ẩm, ánh sáng, chuyển động (PIR), camera, GPS, ...
- Các vi điều khiển như ESP32, Arduino, ... để xử lý dữ liệu.

b, Kết nối mạng

- Các giao thức kết nối phổ biến: WiFi, Bluetooth, 4G/5G.
- Giúp thiết bị truyền dữ liệu lên Cloud hoặc máy chủ.

c, Nền tảng IoT (IoT Platform)

- Dịch vụ trung gian giúp quản lý thiết bị, lưu trữ và xử lý dữ liệu.
- Một số nền tảng phổ biến: ThingSpeak, Blynk, Firebase, AWS IoT, Google Cloud IoT.

d, Phân tích và xử lý dữ liệu

- Dữ liệu thu thập được sẽ được phân tích bằng thuật toán AI, Machine Learning.
- Giúp tối ưu hóa hệ thống, tự động hóa quy trình.

e, Giao diện người dùng

- Ứng dụng di động (App), web dashboard giúp người dùng giám sát và điều khiển từ xa.
- Ví dụ: Điều khiển đèn qua ứng dụng Blynk trên điện thoại.

3. Hệ thống cảnh báo trộm là gì?

Hệ thống cảnh báo trộm là một giải pháp an ninh được thiết kế để phát hiện các hành vi xâm nhập trái phép vào một khu vực nhất định như nhà ở, văn phòng, cửa hàng, kho bãi hoặc các công trình quan trọng. Khi phát hiện dấu hiệu bất thường, hệ thống sẽ kích hoạt báo động thông qua còi hú, đèn nháy hoặc gửi cảnh báo đến chủ sở hữu qua tin nhắn, cuộc gọi, email hoặc ứng dụng di động.

Mục tiêu chính của hệ thống cảnh báo trộm là ngăn chặn kẻ gian, bảo vệ tài sản và con người. Khi một tên trộm bị phát hiện, hệ thống sẽ khiến hắn hoảng sợ và có thể rời đi trước khi kịp thực hiện hành vi trộm cắp. Đồng thời, nó giúp chủ nhà hoặc lực lượng bảo vệ phản ứng kịp thời để giảm thiểu thiệt hại.

Với sự phát triển của công nghệ, hệ thống cảnh báo trộm ngày càng thông minh và tích hợp nhiều tính năng hơn, giúp tăng hiệu quả bảo vệ và đáp ứng nhu cầu ngày càng cao của người dùng.

4. Các thành phần của hệ thống cảnh báo trộm

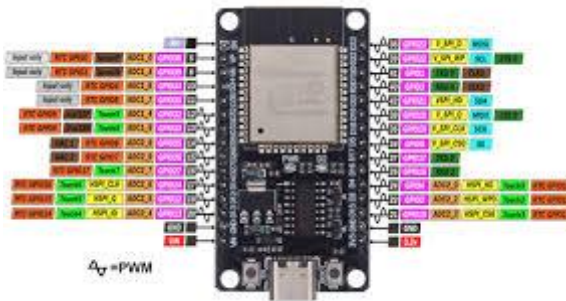
Một hệ thống cảnh báo trộm thường bao gồm các thành phần chính sau:

- **Cảm biến phát hiện xâm nhập:** Các cảm biến như PIR (hồng ngoại), cảm biến từ trường, cảm biến rung, cảm biến âm thanh giúp phát hiện hoạt động đáng ngờ.



Hình 2 : Cảm biến chuyển động PIR (Passive Infrared Sensor)

- **Bộ điều khiển trung tâm:** Thường là vi điều khiển (ESP32, Arduino, Raspberry Pi) xử lý dữ liệu từ các cảm biến và đưa ra quyết định kích hoạt báo động.



Hình 3 : Sơ đồ chân (Pinout) của ESP32

- **Hệ thống cảnh báo tại chỗ:** Gồm còi hú, đèn nháy để cảnh báo ngay khi có kẻ đột nhập.
- **Hệ thống cảnh báo từ xa:** Kết nối với mạng Internet, gửi thông báo đến điện thoại hoặc email của chủ sở hữu.
- **Nguồn cấp điện dự phòng:** Đảm bảo hệ thống hoạt động ngay cả khi mất điện.



Hình 4: Còi báo động (Buzzer)



Hình 5: Đèn LED đỏ

5. Các loại hệ thống cảnh báo trộm

Tùy vào nhu cầu và quy mô ứng dụng, hệ thống cảnh báo trộm có thể được chia thành các loại sau:

a. Hệ thống cảnh báo có dây

- Sử dụng dây dẫn để kết nối các cảm biến với bộ điều khiển.
- Độ tin cậy cao, khó bị nhiễu tín hiệu.
- Nhược điểm: Lắp đặt phức tạp, khó mở rộng và tốn kém chi phí bảo trì.

b. Hệ thống cảnh báo không dây

- Dùng công nghệ như WiFi, Zigbee, LoRa hoặc Bluetooth để truyền tín hiệu.
- Lắp đặt dễ dàng, linh hoạt, có thể tích hợp với hệ thống Smarthome.
- Nhược điểm: Dễ bị nhiễu tín hiệu và phụ thuộc vào mạng không dây.

c. Hệ thống cảnh báo độc lập

- Hoạt động cục bộ, không cần kết nối với hệ thống trung tâm.
- Gồm các thiết bị báo động đơn giản như còi hú khi có xâm nhập.
- Nhược điểm: Không có chức năng gửi cảnh báo từ xa.

d. Hệ thống cảnh báo thông minh (IoT-based)

- Kết nối với Internet, cho phép giám sát và điều khiển từ xa qua điện thoại hoặc máy tính.
- Tích hợp AI để nhận diện khuôn mặt, phân tích hành vi xâm nhập.
- Nhược điểm: Giá thành cao hơn, yêu cầu kết nối mạng ổn định.

6. Các phương pháp phát hiện xâm nhập phổ biến

Để phát hiện các hành vi xâm nhập trái phép, hệ thống cảnh báo trộm sử dụng nhiều phương pháp khác nhau, mỗi phương pháp có ưu và nhược điểm riêng. Dưới đây là một số công nghệ phổ biến trong hệ thống an ninh hiện nay:

a, Cảm biến hồng ngoại thụ động (PIR - Passive Infrared Sensor)

- **Nguyên lý hoạt động:** Cảm biến PIR phát hiện sự thay đổi của bức xạ hồng ngoại trong khu vực giám sát. Khi một vật thể sống (như con người, động vật) di chuyển, sự thay đổi nhiệt độ sẽ kích hoạt cảm biến.
- **Ưu điểm:** Giá thành rẻ, dễ lắp đặt, ít tiêu tốn năng lượng.
- **Nhược điểm:** Dễ bị nhiễu bởi các nguồn nhiệt khác như ánh nắng mặt trời, lửa, quạt nhiệt.

b, Cảm biến từ trường (Magnetic Sensor)

- **Nguyên lý hoạt động:** Cảm biến này được lắp đặt trên cửa ra vào hoặc cửa sổ. Khi cửa bị mở ra trái phép, cảm biến sẽ gửi tín hiệu cảnh báo.
- **Ưu điểm:** Hoạt động hiệu quả trong môi trường khép kín, ít bị ảnh hưởng bởi môi trường bên ngoài.
- **Nhược điểm:** Không thể phát hiện người đột nhập qua các lối khác như cửa sổ hoặc mái nhà.

c, Cảm biến rung (Vibration Sensor)

- **Nguyên lý hoạt động:** Cảm biến rung phát hiện các chấn động bất thường, chẳng hạn như khi có ai đó cố gắng cạy cửa hoặc đập vỡ kính.
- **Ưu điểm:** Nhạy với các hoạt động phá hoại, giúp bảo vệ tài sản tốt hơn.
- **Nhược điểm:** Có thể bị nhiễu bởi các rung động tự nhiên như gió mạnh hoặc động đất nhẹ.

d, Camera an ninh kết hợp trí tuệ nhân tạo (AI Camera)

- **Nguyên lý hoạt động:** Camera giám sát ghi lại hình ảnh và sử dụng thuật toán AI để nhận diện khuôn mặt, phát hiện chuyển động bất thường và phân tích hành vi đáng ngờ.
- **Ưu điểm:** Giám sát trực quan, có thể nhận diện đối tượng cụ thể và cảnh báo chính xác.
- **Nhược điểm:** Giá thành cao, yêu cầu kết nối mạng ổn định và có thể gặp vấn đề về quyền riêng tư.

e, Cảm biến âm thanh (Sound Sensor)

- **Nguyên lý hoạt động:** Phát hiện tiếng động lớn bất thường như tiếng kính vỡ, tiếng cửa bị cạy.
- **Ưu điểm:** Phát hiện nhanh chóng các hành động phá hoại.
- **Nhược điểm:** Có thể bị nhiễu bởi âm thanh môi trường như tiếng sấm, xe cộ, động vật.

Trong các phương pháp trên, cảm biến hồng ngoại (PIR) là một trong những giải pháp phổ biến nhất do chi phí thấp, dễ sử dụng và có hiệu quả cao trong việc phát hiện chuyển động.

7. Ứng dụng IoT trong hệ thống cảnh báo trộm

Internet of Things (IoT) đang cách mạng hóa lĩnh vực an ninh bằng cách tích hợp các thiết bị thông minh vào hệ thống cảnh báo trộm, giúp nâng cao hiệu suất và khả năng giám sát từ xa.

7.1. Nguyên lý hoạt động của hệ thống cảnh báo trộm IoT

Hệ thống cảnh báo trộm IoT hoạt động dựa trên sự kết hợp giữa các cảm biến, vi điều khiển, nền tảng đám mây và ứng dụng di động. Quy trình hoạt động cơ bản như sau:

1. Cảm biến (PIR, từ trường, rung, âm thanh) phát hiện dấu hiệu bất thường.
2. Vi điều khiển (ESP32) thu thập dữ liệu từ cảm biến và phân tích thông tin.

3. Nếu phát hiện xâm nhập, hệ thống sẽ:

- + Kích hoạt còi báo động hoặc đèn cảnh báo tại chỗ.
- + Gửi thông báo đến người dùng qua Telegram, Email hoặc ứng dụng di động.
- + Lưu trữ dữ liệu trên nền tảng đám mây để phân tích sau này.

7.2. Ưu điểm của hệ thống cảnh báo trộm IoT

- **Giám sát từ xa:** Người dùng có thể nhận thông báo và điều khiển hệ thống từ bất kỳ đâu qua smartphone.
- **Phản ứng nhanh:** Khi phát hiện đột nhập, hệ thống lập tức gửi cảnh báo để chủ nhà có thể can thiệp kịp thời.
- **Tiết kiệm chi phí:** So với các hệ thống an ninh truyền thống, giải pháp IoT có chi phí rẻ hơn nhưng vẫn mang lại hiệu quả cao.
- **Dễ dàng mở rộng:** Có thể tích hợp thêm nhiều cảm biến hoặc kết nối với các hệ thống Smarthome khác như khóa cửa thông minh, camera AI.

7.3. Ứng dụng thực tế

- **Hệ thống cảnh báo trộm cho gia đình:** Bảo vệ cửa ra vào, cửa sổ, phát hiện chuyển động trong nhà và gửi cảnh báo qua Telegram.
- **Giám sát kho hàng, văn phòng:** Kết hợp với camera AI để nhận diện người lạ, theo dõi hoạt động trong khu vực quan trọng.
- **Bảo vệ xe cộ:** Gắn cảm biến rung trên xe máy, ô tô để phát hiện trộm cắp và gửi cảnh báo

CHƯƠNG III. PHẦN CỨNG VÀ PHẦN MỀM SỬ DỤNG

1. Phần cứng

Hệ thống cảnh báo trộm dựa trên **ESP32** và **cảm biến PIR** yêu cầu một số phần cứng quan trọng để hoạt động ổn định và hiệu quả. Việc lựa chọn các linh kiện phù hợp giúp đảm bảo hệ thống có độ chính xác cao, phản ứng nhanh và có thể hoạt động bền bỉ trong môi trường thực tế.

Mỗi thành phần trong hệ thống đóng vai trò quan trọng trong việc phát hiện xâm nhập, xử lý tín hiệu và truyền dữ liệu đến người dùng. Trong phần này, chúng ta sẽ đi sâu vào từng linh kiện để hiểu rõ cách chúng hoạt động và ứng dụng thực tế trong hệ thống cảnh báo trộm.

1.1. ESP32 – Tổng quan và tính năng

ESP32 là một vi điều khiển mạnh mẽ và đa năng, được sử dụng rộng rãi trong các ứng dụng IoT (Internet of Things). Nó là phiên bản nâng cấp của ESP8266, với hiệu suất cao hơn, nhiều tính năng hơn và mức tiêu thụ điện năng thấp hơn. Nhờ có kết nối WiFi và Bluetooth tích hợp, ESP32 trở thành một lựa chọn lý tưởng cho các ứng dụng giám sát từ xa như hệ thống cảnh báo trộm.

Thông số kỹ thuật và tính năng nổi bật của ESP32:

1. Bộ vi xử lý mạnh mẽ:

- Sử dụng bộ vi xử lý dual-core Tensilica LX6, tốc độ lên đến 240 MHz.
- Hỗ trợ đa luồng, giúp thực thi nhiều tác vụ cùng lúc (ví dụ: vừa đọc tín hiệu cảm biến, vừa gửi dữ liệu lên máy chủ).

2. Bộ nhớ lớn:

- 520 KB SRAM, giúp lưu trữ biến và dữ liệu tạm thời.
- Hỗ trợ Flash lên đến 16 MB, giúp lưu trữ chương trình phức tạp hơn.

3. Khả năng kết nối mạnh mẽ:

- WiFi 802.11 b/g/n, cho phép kết nối Internet để gửi cảnh báo qua Telegram hoặc Email.
- Bluetooth 4.2 BLE, có thể dùng để giao tiếp với các thiết bị di động.

4. Hỗ trợ nhiều giao thức giao tiếp:

- UART, SPI, I2C, ADC, DAC, PWM, rất thuận tiện khi kết nối với cảm biến PIR, còi báo, đèn LED hoặc các thiết bị khác.

5. Tiêu thụ điện năng thấp:

- Chế độ Deep Sleep, giúp tiết kiệm pin tối đa khi không có sự kiện xảy ra.
- Có thể sử dụng với nguồn pin hoặc năng lượng mặt trời để hoạt động bền bỉ ngoài trời.

6. Bảo mật cao:

- Hỗ trợ mã hóa TLS 1.2, giúp truyền dữ liệu an toàn.
- Tích hợp các giao thức MQTT, HTTPS, tăng cường bảo mật khi giao tiếp với máy chủ.

1.2. Ứng dụng của ESP32 trong hệ thống cảnh báo trộm

- Nhận dữ liệu từ cảm biến PIR để phát hiện chuyển động.
- Kết nối WiFi để gửi cảnh báo qua Telegram hoặc Email.
- Điều khiển còi báo động, đèn LED để phát tín hiệu cảnh báo khi có xâm nhập.
- Gửi dữ liệu lên ThingSpeak hoặc Blynk để lưu trữ và giám sát từ xa.
- Có thể mở rộng thêm camera ESP32-CAM để ghi lại hình ảnh khi có xâm nhập.

1.3. Cảm biến PIR – Nguyên lý hoạt động và ứng dụng

Cảm biến PIR (Passive Infrared Sensor) là thiết bị quan trọng giúp phát hiện chuyển động của con người hoặc vật thể sống trong khu vực giám sát. Đây là linh kiện cốt lõi trong hệ thống cảnh báo trộm vì nó giúp xác định có hay không có sự xâm nhập bất thường.

Nguyên lý hoạt động của cảm biến PIR

- Cảm biến PIR hoạt động dựa trên việc phát hiện bức xạ hồng ngoại từ cơ thể con người hoặc động vật.
- Khi một vật thể có nhiệt độ cao hơn môi trường di chuyển trong khu vực cảm biến, mức tín hiệu thay đổi, kích hoạt báo động.
- Cảm biến PIR thường có góc quét từ 90° - 120° và phạm vi phát hiện từ 5 - 7m.

Ứng dụng của cảm biến PIR trong hệ thống cảnh báo trộm

- Giúp phát hiện chuyển động bất thường trong khu vực bảo vệ.
- Kết hợp với ESP32 để xử lý tín hiệu và gửi cảnh báo đến người dùng.
- Dùng trong hệ thống Smarthome, bật đèn tự động khi có người vào phòng.
- Tiêu thụ điện năng thấp, phù hợp với hệ thống chạy bằng pin hoặc năng lượng mặt trời.

1.4. Các linh kiện hỗ trợ khác

Nguồn điện

- Sử dụng adapter 5V – 2A hoặc pin Li-ion 18650 để cấp nguồn cho ESP32.
- Nếu lắp đặt ngoài trời, có thể dùng tấm pin năng lượng mặt trời để duy trì hoạt động liên tục.

Còi báo động (Buzzer)

- Khi phát hiện xâm nhập, còi hú giúp cảnh báo ngay lập tức để kẻ trộm hoảng sợ và bỏ chạy.
- Có thể sử dụng buzzer 5V hoặc loa công suất lớn hơn tùy vào yêu cầu hệ thống.

Đèn LED

- **Hiển thị trạng thái hệ thống:**
 - **Màu xanh:** Bình thường.
 - **Màu đỏ:** Cảnh báo có xâm nhập.
- Kết hợp với còi báo để tăng hiệu quả cảnh báo.

2. Phần mềm

2.1. Wokwi – Mô phỏng hệ thống

- Wokwi là nền tảng mô phỏng vi điều khiển trực tuyến, giúp kiểm tra hoạt động của ESP32 mà không cần phần cứng thực tế.
- Hỗ trợ lập trình với Arduino IDE, có thể chạy trực tiếp trên trình duyệt.

2.2. Arduino IDE, Visual Studio Code – Lập trình ESP32

- Arduino IDE, Visual Studio Code là môi trường lập trình chính để viết mã cho ESP32.
- Hỗ trợ thư viện WiFi.h, TelegramBot.h, ThingSpeak.h giúp ESP32 giao tiếp với Internet.

2.3. Telegram API / SMTP Email – Gửi cảnh báo

Gửi cảnh báo qua Telegram

- Sử dụng Telegram Bot API để gửi tin nhắn cảnh báo khi có xâm nhập.

Gửi cảnh báo qua Email (SMTP)

- Dùng SMTP Server để gửi Email đến người dùng khi phát hiện trộm.

CHƯƠNG IV. THIẾT KẾ HỆ THỐNG

1. Sơ đồ khối hệ thống

Hệ thống cảnh báo trộm sử dụng ESP32 và cảm biến PIR bao gồm nhiều thành phần hoạt động cùng nhau để phát hiện xâm nhập, xử lý tín hiệu và gửi cảnh báo đến người dùng. Để dễ dàng hình dung cách các linh kiện kết nối và phối hợp với nhau, chúng ta sẽ biểu diễn hệ thống dưới dạng sơ đồ khối.

Các thành phần chính trong sơ đồ khối hệ thống

1. Cảm biến PIR (Passive Infrared Sensor)

- Có nhiệm vụ phát hiện chuyển động trong khu vực giám sát.
- Khi có người di chuyển trong phạm vi cảm biến, nó sẽ gửi tín hiệu HIGH đến ESP32.

2. Vi điều khiển ESP32

- Tiếp nhận tín hiệu từ cảm biến PIR.
- Xử lý dữ liệu và xác định xem có xâm nhập hay không.
- Kết nối WiFi để gửi cảnh báo đến Telegram hoặc Email.
- Điều khiển các thiết bị như còi báo động, đèn LED để phát tín hiệu cảnh báo.

3. Hệ thống cảnh báo tại chỗ

- Còi báo động (Buzzer): Kêu lớn khi có xâm nhập.
- Đèn LED: Nhấp nháy để báo hiệu trạng thái hệ thống.

4. Hệ thống cảnh báo từ xa

- Gửi tin nhắn Telegram: Người dùng nhận cảnh báo ngay lập tức trên điện thoại.

- Gửi Email: Nếu tích hợp camera ESP32-CAM, hệ thống có thể gửi ảnh chụp khu vực bị xâm nhập.

5. Lưu trữ dữ liệu và giám sát từ xa (nếu có)

- ThingSpeak / Blynk: Ghi nhận dữ liệu cảm biến và hiển thị trên biểu đồ trực tuyến.
- Người dùng có thể truy cập qua ứng dụng di động hoặc website để theo dõi trạng thái hệ thống.

2. Sơ đồ nguyên lý (Thiết kế mạch trên Wokwi)

Sau khi hiểu cách các thành phần hoạt động trong sơ đồ khối, chúng ta tiến hành thiết kế sơ đồ nguyên lý trên Wokwi, một nền tảng mô phỏng mạnh mẽ dành cho vi điều khiển.

Các bước thiết kế mạch trên Wokwi

1. Thêm ESP32 vào mạch điện

- Truy cập Wokwi: <https://wokwi.com/>
- Chọn ESP32 làm vi điều khiển chính.

2. Kết nối cảm biến PIR với ESP32

- VCC của cảm biến PIR → 3.3V trên ESP32.
- GND của cảm biến PIR → GND trên ESP32.
- OUT của cảm biến PIR → Chân GPIO 2 trên ESP32.

3. Kết nối còi báo động (Buzzer) với ESP32

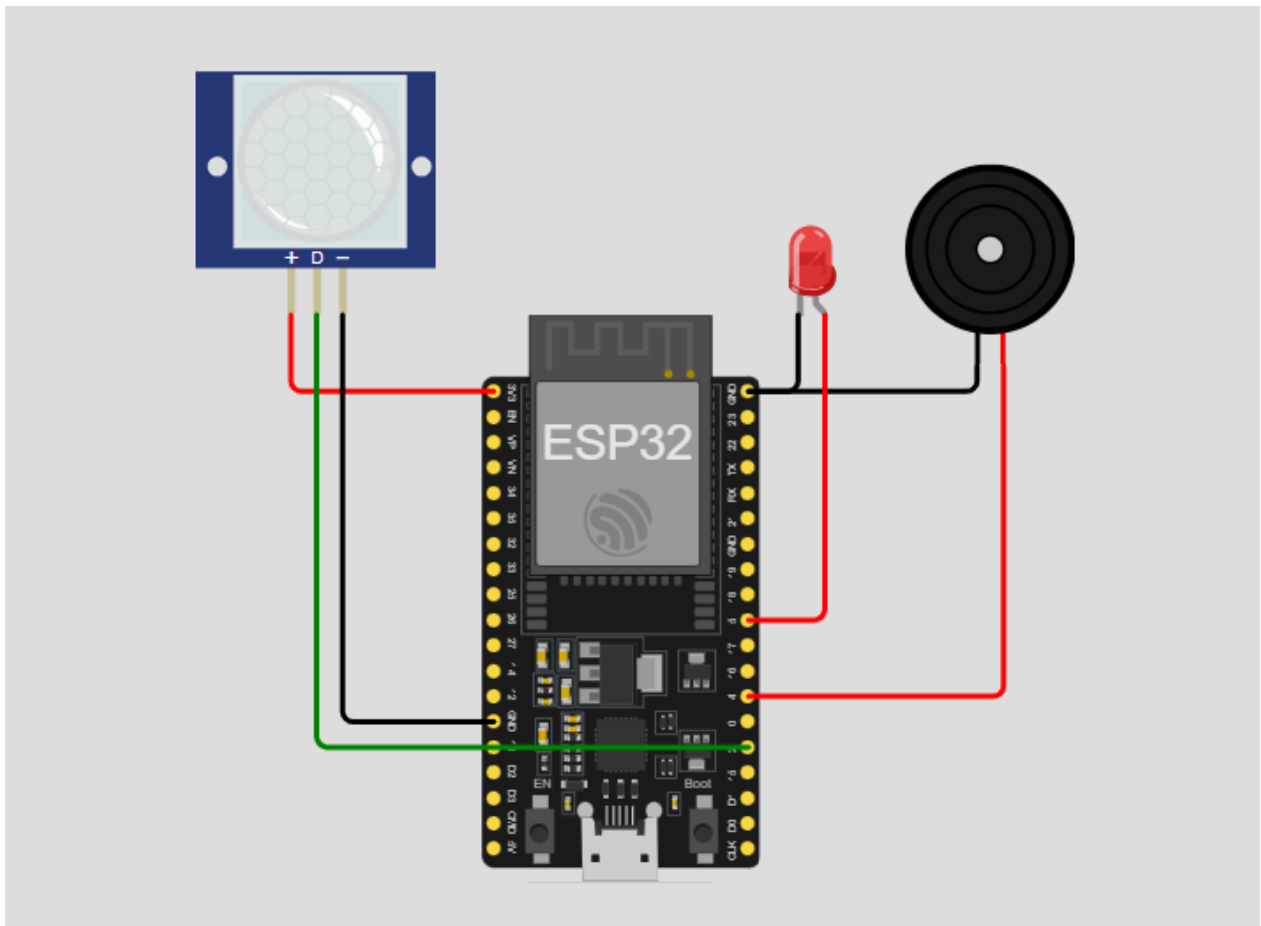
- Chân dương (+) của Buzzer → Chân GPIO 4 trên ESP32.
- Chân âm (-) của Buzzer → GND trên ESP32.

4. Kết nối đèn LED cảnh báo

- Chân dương (+) của LED → Điện trở 220Ω → GPIO 5 trên ESP32.
- Chân âm (-) của LED → GND trên ESP32.

5. Kết nối ESP32 với Internet

- Cấu hình WiFi trong mã nguồn để ESP32 có thể gửi cảnh báo qua Telegram hoặc Email.



Hình 6 : Hệ thống cảnh báo trộm sử dụng ESP32 và cảm biến PIR

Sau khi thiết kế mạch trên Wokwi, chúng ta có thể mô phỏng và kiểm tra trước khi triển khai thực tế.

3. Nguyên lý hoạt động của hệ thống

Hệ thống hoạt động theo chu trình tuần hoàn, liên tục giám sát khu vực và phản hồi khi phát hiện xâm nhập.

Các bước hoạt động chi tiết của hệ thống

Bước 1: Hệ thống khởi động

- Khi cấp nguồn, ESP32 khởi động và kết nối với mạng WiFi.
- Kiểm tra trạng thái của cảm biến PIR, còi báo và đèn LED.

Bước 2: Phát hiện chuyển động

- Cảm biến PIR quét khu vực, nếu không có chuyển động, hệ thống sẽ đợi.
- Khi có người di chuyển, cảm biến gửi tín hiệu HIGH đến ESP32.

Bước 3: Xử lý tín hiệu

- ESP32 nhận tín hiệu từ cảm biến PIR.
- So sánh trạng thái hiện tại với trạng thái trước đó để xác định có thực sự là xâm nhập hay không.
- Nếu xác định có xâm nhập, hệ thống chuyển sang bước tiếp theo.

Bước 4: Cảnh báo tại chỗ

- Còi báo động kích hoạt, phát ra âm thanh cảnh báo lớn.
- Đèn LED nhấp nháy để báo hiệu tình trạng khẩn cấp.

Bước 5: Gửi cảnh báo từ xa

- ESP32 gửi tin nhắn Telegram đến điện thoại người dùng.
- Nếu có camera ESP32-CAM, hệ thống có thể chụp ảnh và gửi kèm qua Email.

Bước 6: Quay lại trạng thái giám sát

- Sau khi xử lý cảnh báo, hệ thống quay lại trạng thái giám sát, tiếp tục theo dõi khu vực.

Đánh giá hệ thống

Ưu điểm:

- + Tự động hoàn toàn, không cần giám sát thủ công.
- + Gửi cảnh báo ngay lập tức qua Telegram, Email.
- + Tiêu thụ điện năng thấp, có thể hoạt động lâu dài với pin.
- + Dễ dàng mở rộng thêm camera, cảm biến khác.

Nhược điểm và cách khắc phục:

- + Cảm biến PIR có thể bị ảnh hưởng bởi môi trường (nhiệt độ cao, vật cản).
→ Giải pháp: Chọn vị trí lắp đặt hợp lý, tránh ánh sáng mặt trời trực tiếp.
- + WiFi yếu có thể làm chậm cảnh báo.
→ Giải pháp: Dùng mạng WiFi ổn định hoặc tích hợp Module GSM để gửi cảnh báo qua SMS.

CHƯƠNG V. LẬP TRÌNH VÀ TRIỂN KHAI

Sau khi thiết kế phần cứng và sơ đồ mạch, chúng ta cần lập trình để ESP32 có thể kết nối WiFi, đọc dữ liệu từ cảm biến PIR, xử lý tín hiệu và gửi cảnh báo. Dưới đây là các bước quan trọng để triển khai hệ thống.

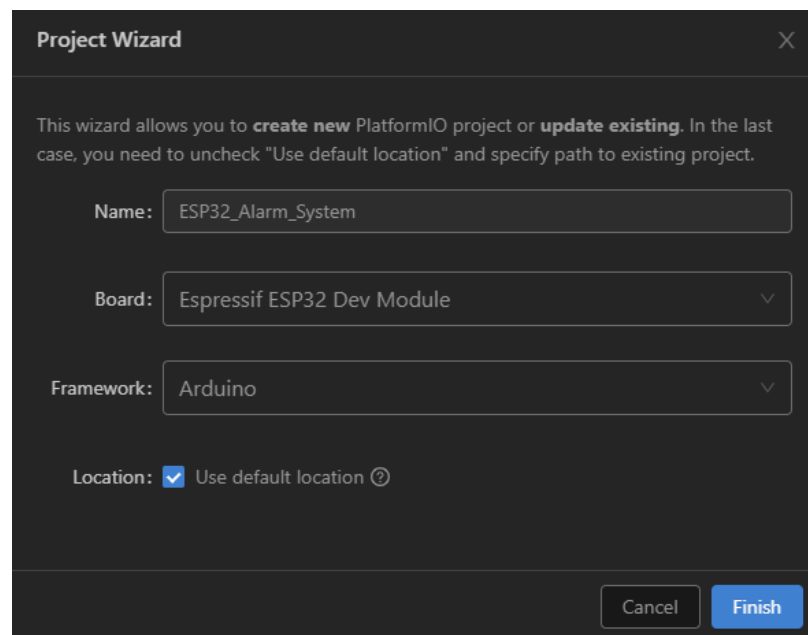
1. Cấu hình ESP32 kết nối WiFi

ESP32 cần kết nối WiFi để gửi cảnh báo đến Telegram hoặc Email

Cách thực hiện

Bước 1: Tạo Project Mới Cho ESP32

1. Mở PlatformIO (bấm vào biểu tượng PlatformIO Home trên thanh Sidebar trái).
2. Nhấn New Project và nhập thông tin:

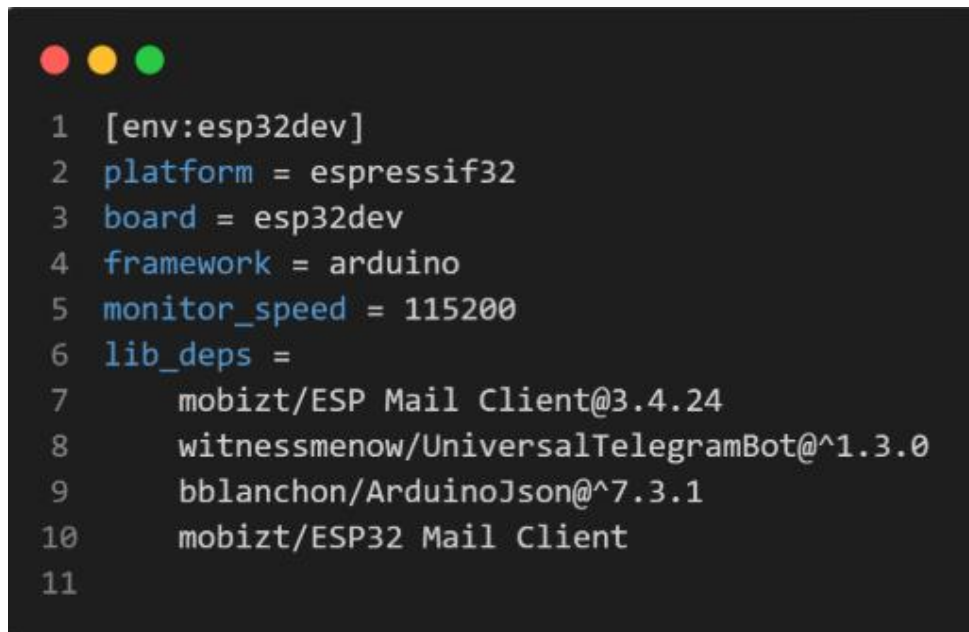


Hình 7: Tạo dự án mới trên PlatformIO cho ESP32

3. Nhấn Finish và đợi PlatformIO tải các thư viện cần thiết.

Bước 2: Cài Đặt Thư Viện

Mở file platformio.ini trong project và thêm dòng sau:



```
1 [env:esp32dev]
2 platform = espressif32
3 board = esp32dev
4 framework = arduino
5 monitor_speed = 115200
6 lib_deps =
7     mobizt/ESP Mail Client@3.4.24
8     witnessmenow/UniversalTelegramBot@^1.3.0
9     bblanchon/ArduinoJson@^7.3.1
10     mobizt/ESP32 Mail Client
11
```

Hình 8 : Cấu hình PlatformIO cho ESP32

2. Code hệ thống cảnh báo trộm bằng ESP32 và cảm biến PIR gửi cảnh báo qua Telegram

a,Khai báo và cấu hình

```

1  #include <WiFi.h>
2  #include <WiFiClientSecure.h>
3  #include <UniversalTelegramBot.h>
4  #include <ESP_Mail_Client.h>
5  #include <ArduinoJson.h>
6
7  // Thông tin WiFi
8  const char *ssid = "Wokwi-GUEST";
9  const char *password = "";
10
11 // Cấu hình Telegram Bot
12 #define BOT_TOKEN "7869624586:AAHbkuMDIIbX8wodUUvGXXh9X1AYr3sXjLU"
13 #define CHAT_ID "-4771876874"
14
15 // Cấu hình chân GPIO
16 #define PIR_SENSOR_PIN 27 // Chân kết nối cảm biến PIR
17 #define LED_PIN 2         // Chân LED để báo trạng thái
18
19 // Khai báo đối tượng
20 WiFiClientSecure client;
21 UniversalTelegramBot bot(BOT_TOKEN, client);

```

```

22 // Biến để quản lý trạng thái cảnh báo
23 bool motionDetected = false;
24 unsigned long lastMotionTime = 0;
25 const long MOTION_INTERVAL = 2000; // 2 giây giữa các lần cảnh báo
26
27 void setupWiFi()
28 {
29     WiFi.begin(ssid, password);
30     Serial.print("Đang kết nối WiFi");
31
32     while (WiFi.status() != WL_CONNECTED)
33     {
34         delay(500);
35         Serial.print(".");
36     }
37
38     Serial.println("\nWiFi đã kết nối thành công");
39     Serial.print("Địa chỉ IP: ");
40     Serial.println(WiFi.localIP());
41 }

```

b, Xử lý sự kiện để gửi tin nhắn lên Telegram

```
42 void sendTelegramAlert()
43 {
44     if (WiFi.status() != WL_CONNECTED)
45     {
46         Serial.println("Không có kết nối WiFi, không thể gửi Telegram.");
47         return;
48     }
49     String message = String("CẢNH BÁO: Phát hiện chuyển động bất thường!");
50     if (bot.sendMessage(CHAT_ID, message, ""))
51     {
52         Serial.println("Cảnh báo Telegram đã được gửi!");
53     }
54     else
55     {
56         Serial.println("Không thể gửi cảnh báo qua Telegram");
57     }
58 }
59
60 void IRAM_ATTR detectMotion()
61 {
62     motionDetected = true;
63 }
64
```


c, Hàm setup

```
65 void setup()
66 {
67     Serial.begin(115200);
68
69     // Cấu hình chân GPIO
70     pinMode(PIR_SENSOR_PIN, INPUT_PULLUP);
71     pinMode(LED_PIN, OUTPUT);
72
73     // Kết nối WiFi
74     setupWiFi();
75
76     // Cấu hình Telegram
77     client.setCACert(TELEGRAM_CERTIFICATE_ROOT);
78
79     // Thiết lập ngắt cho cảm biến PIR
80     attachInterrupt(digitalPinToInterrupt(PIR_SENSOR_PIN), detectMotion, RISING);
81
82     // Thông báo khởi động hệ thống
83     sendTelegramAlert();
84 }
```

d,Hàm loop

```
85 void loop()
86 {
87     if (motionDetected)
88     {
89         for (int i = 0; i < 10; i++)
90         {
91             digitalWrite(LED_PIN, HIGH);
92             delay(200);
93             digitalWrite(LED_PIN, LOW);
94             delay(200);
95         }
96         if (millis() - lastMotionTime > MOTION_INTERVAL)
97         {
98             sendTelegramAlert();
99             lastMotionTime = millis();
100         }
101         motionDetected = false;
102     }
103     else
104     {
105         digitalWrite(LED_PIN, LOW);
106     }
107 }
108
```

CHƯƠNG VI. KIỂM THỬ VÀ ĐÁNH GIÁ

Sau khi hoàn thành thiết kế và lập trình hệ thống, việc kiểm thử là bước quan trọng để đảm bảo hệ thống hoạt động chính xác theo yêu cầu. Trong chương này, chúng ta sẽ tiến hành kiểm thử hệ thống trên nền tảng Wokwi (một trình mô phỏng phần cứng), phân tích các trường hợp kiểm thử và đánh giá hiệu quả hoạt động của hệ thống.

1. Các trường hợp kiểm thử và kết quả

Sau khi chạy thử trên Wokwi, chúng ta sẽ kiểm tra hệ thống theo nhiều trường hợp khác nhau để đảm bảo tính chính xác.

Bảng các trường hợp kiểm thử

ID	Mô Tả	Dữ Liệu Đầu Vào	Kết quả mong đợi	Kết quả thực tế	Trạng thái
TC01	Kết nối WiFi thành công	Đúng SSID, mật khẩu	ESP32 kết nối thành công, in địa chỉ IP	Đúng như mong đợi	Đạt
TC02	Kết nối WiFi thất bại	Sai mật khẩu	Hiển thị "Kết nối thất bại"	Đúng như mong đợi	Đạt
TC03	Phát hiện chuyển động	Cảm biến PIR phát hiện người	Hiển thị "Phát hiện chuyển động!" trên Serial	Đúng như mong đợi	Đạt
TC04	Không có chuyển động	Không có người trước cảm biến	Hiển thị "Không có chuyển động."	Đúng như mong đợi	Đạt
TC05	Gửi tin nhắn Telegram	Cảm biến phát hiện chuyển động	Nhận tin nhắn trên Telegram	Đúng như mong đợi	Đạt

Tất cả các bài kiểm thử đều thành công, chứng tỏ hệ thống hoạt động ổn định và chính xác

2. Đánh giá hiệu quả hệ thống

2.1. Ưu điểm của hệ thống

+ Độ chính xác cao:

Hệ thống sử dụng cảm biến PIR để phát hiện chuyển động, giúp phát hiện chính xác sự xâm nhập.

+ Tích hợp IoT mạnh mẽ:

ESP32 có thể gửi cảnh báo qua Telegram, Email, hoặc lưu trữ trên ThingSpeak/Blynk, giúp người dùng dễ dàng theo dõi từ xa.

+ Chi phí thấp, dễ triển khai:

- ESP32 có giá rẻ nhưng khả năng mạnh mẽ.
- Có thể mở rộng để sử dụng thêm cảm biến khác như camera, cảm biến cửa, còi báo động.

+ Tiết kiệm điện năng:

ESP32 có thể chạy chế độ Deep Sleep, chỉ hoạt động khi có cảnh báo, giúp tiết kiệm pin.

2.2. Nhược điểm và cách khắc phục

Nhược điểm	Giải pháp khắc phục
Cảm biến PIR có thể bị nhiễu	Sử dụng thuật toán lọc tín hiệu để giảm báo động giả.
Yêu cầu có WiFi để gửi cảnh báo	Có thể sử dụng mạng 4G hoặc lưu trữ tạm thời trên thẻ nhớ SD nếu mất kết nối.
Không hoạt động trong bóng tối	Kết hợp với cảm biến ánh sáng hoặc camera hồng ngoại.

2.3. So sánh với các hệ thống cảnh báo trộm truyền thống

Tiêu chí	Hệ thống truyền thống	Hệ thống ESP32
Chi phí	Cao	Rẻ
Cảnh báo từ xa	Không có	Có (Telegram, Email, ThingSpeak)
Cảnh báo từ xa	Cố định, khó nâng cấp	Dễ dàng mở rộng (thêm cảm biến)
Ghi lại dữ liệu	Không có	Có (ThingSpeak/Blynk)

CHƯƠNG VII. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Sau khi hoàn thành quá trình nghiên cứu, thiết kế, lập trình và kiểm thử, hệ thống cảnh báo trộm dựa trên ESP32 và cảm biến PIR đã chứng minh được tính hiệu quả và khả năng ứng dụng thực tế cao. Chương này sẽ tổng kết lại những kết quả đạt được, đồng thời đề xuất các hướng phát triển trong tương lai để nâng cấp hệ thống.

1. Kết luận về hệ thống

Tổng quan về kết quả đạt được

Hệ thống cảnh báo trộm được xây dựng dựa trên nền tảng ESP32, cảm biến PIR, cùng với các công nghệ IoT như Telegram API, Email SMTP. Quá trình thực hiện đã đạt được những mục tiêu quan trọng sau:

- + **Phát hiện xâm nhập chính xác:** Cảm biến PIR nhận diện sự di chuyển trong phạm vi giám sát với độ tin cậy cao.
- + **Cảnh báo ngay lập tức:** Khi phát hiện có chuyển động, hệ thống gửi thông báo qua Telegram, Email hoặc bật còi báo động.
- + **Giám sát từ xa:** Nhờ kết nối WiFi, người dùng có thể theo dõi tình trạng an ninh từ xa thông qua Blynk.
- + **Mô phỏng và kiểm thử thành công:** Toàn bộ hệ thống đã được kiểm tra trên Wokwi, giúp phát hiện và sửa lỗi trước khi triển khai thực tế.

2. Hướng phát triển trong tương lai

2.1. Tích hợp camera AI để nhận diện khuôn mặt

- + **Mở rộng với ESP32-CAM:** Thêm camera để ghi lại hình ảnh hoặc video khi có kẻ xâm nhập.
- + **Nhận diện khuôn mặt bằng AI:** Sử dụng OpenCV hoặc TensorFlow Lite để phân biệt giữa chủ nhà và người lạ.

+ **Lưu trữ trên Cloud:** Ảnh chụp có thể gửi lên Google Drive hoặc Firebase để xem lại khi cần.

2.2. Kết nối 4G/5G thay vì WiFi

+ **Giải pháp chống mất mạng:** Dùng module SIM800L hoặc SIM7600 để gửi cảnh báo qua SMS ngay cả khi WiFi bị gián đoạn.

+ **Gửi cuộc gọi tự động:** Khi có trộm, hệ thống có thể gọi điện đến chủ nhà thay vì chỉ gửi tin nhắn.

2.3. Kết hợp cảm biến từ và cảm biến rung

+ **Cảm biến từ:** Phát hiện khi cửa hoặc cửa sổ bị mở trái phép.

+ **Cảm biến rung:** Nhận diện khi có tác động mạnh vào cửa, tường (ví dụ: kẻ trộm cố đập phá).

2.4. Điều khiển hệ thống qua ứng dụng di động

+ **Xây dựng app trên Android/iOS:** Giúp người dùng dễ dàng quản lý, theo dõi và điều chỉnh hệ thống.

+ **Tích hợp điều khiển từ xa:** Cho phép bật/tắt báo động từ điện thoại.

2.5. Sử dụng năng lượng mặt trời để cấp nguồn

+ **Giảm phụ thuộc vào điện lưới:** Dùng **tấm pin mặt trời** để sạc pin cho ESP32, giúp hệ thống hoạt động liên tục ngay cả khi mất điện.

+ **Kết hợp với pin Li-ion:** Lưu trữ điện để hoạt động ngay cả vào ban đêm hoặc khi trời âm u.

2.6. Ghi nhận dữ liệu vào hệ thống AI để phân tích hành vi

+ **Dùng Machine Learning để phát hiện xâm nhập thông minh:** Nhận diện các hành vi bất thường như:

- Một người đứng trước cửa lâu nhưng không vào.
- Nhiều lần di chuyển qua lại trong khu vực giám sát.

TÀI LIỆU THAM KHẢO

Tiếng Việt:

[1]. Internet Of Things (IoT) cho người mới bắt đầu IoT Maker Việt Nam

[2]. <https://advancecad.edu.vn/tai-lieu-iot-internet-of-things/>

[3]. <https://tailieuhust.com/tai-lieu-iot-va-ung-dung-hust/>

[4]. Phạm Quang Huy, Lê Cảnh Trung, *Lập trình điều khiển với Arduino*, NXB Khoa học và Kỹ thuật, 2014.

[5]. Lê Hồng Phương, *Hệ thống nhúng và ứng dụng với ESP32*, NXB Khoa học Tự nhiên và Công nghệ, 2021.

[6]. <https://docs.wokwi.com/>