**BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM**

**KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**

****

**BÁO CÁO ĐỒ ÁN**

**MÔN: BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG**

**NGHIÊN CỨU VÀ TRIỂN KHAI XÁC THỰC HAI NHÂN TỐ TRÊN NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY**

Giảng viên hướng dẫn: **Th.S Phạm Trọng Huynh**

Sinh viên thực hiện: **Trương Đăng Quý 0850080039**

**Nguyễn Thị Ngọc Hiền 0850080072**

**Châu Tú Hoa 0850080073**

Lớp **: 08CNPM**

Khoá  **: 08**

***TP. Hồ Chí Minh, tháng 04 năm 2023***

**BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG**

**TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM**

**KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM**

****

**BÁO CÁO ĐỒ ÁN**

**MÔN: BẢO MẬT MẠNG MÁY TÍNH VÀ HỆ THỐNG**

**NGHIÊN CỨU VÀ TRIỂN KHAI XÁC THỰC HAI NHÂN TỐ TRÊN NỀN TẢNG ĐIỆN TOÁN ĐÁM MÂY**

Giảng viên hướng dẫn: **Th.S Phạm Trọng Huynh**

Sinh viên thực hiện: **Trương Đăng Quý 0850080039**

**Nguyễn Thị Ngọc Hiền 0850080072**

**Châu Tú Hoa 0850080073**

Lớp **: 08CNPM**

Khoá  **: 08**

***TP. Hồ Chí Minh, tháng 04 năm 2023***

**MỞ ĐẦU**

Trong thời đại công nghệ số hiện nay, việc bảo vệ thông tin cá nhân và dữ liệu quan trọng trở thành một vấn đề đặc biệt quan trọng. Các cuộc tấn công mạng ngày càng phức tạp và tinh vi hơn, đặc biệt là với những tổ chức lớn sử dụng nền tảng điện toán đám mây để lưu trữ và xử lý dữ liệu.

Để đảm bảo an toàn cho hệ thống thông tin của mình, việc triển khai các phương pháp xác thực người dùng là rất quan trọng. Hiện nay, xác thực hai nhân tố được coi là một trong những phương pháp an toàn và hiệu quả nhất để đảm bảo rằng chỉ có người dùng hợp lệ mới có thể truy cập vào hệ thống.

Đề tài nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây sẽ tập trung vào việc nghiên cứu các phương pháp và công nghệ xác thực hai nhân tố, đồng thời triển khai và áp dụng chúng trên môi trường điện toán đám mây để tăng cường bảo mật thông tin và dữ liệu cho các tổ chức.

Phần nghiên cứu của đề tài sẽ tập trung vào việc tìm hiểu về các phương pháp xác thực hai nhân tố như xác thực bằng mật khẩu và mã OTP, xác thực bằng vân tay, khuôn mặt, hoặc giọng nói. Ngoài ra, phần nghiên cứu cũng sẽ tìm hiểu về các công nghệ điện toán đám mây như AWS, Google Cloud, và Microsoft Azure, và cách triển khai các phương pháp xác thực hai nhân tố trên các nền tảng này.

Phần triển khai của đề tài sẽ tập trung vào việc áp dụng các phương pháp và công nghệ đã nghiên cứu vào một môi trường thực tế trên một hệ thống điện toán đám mây. Kết quả của phần triển khai sẽ giúp đánh giá tính hiệu quả và tính khả thi của việc triển khai các phương pháp xác thực hai nhân tố trên nền tảng điện toán đám mây.

**LỜI CẢM ƠN**

Trong suốt quá trình học tập và hoàn thành đồ án này, chúng em đã nhận được rất nhiều sự hướng dẫn, giúp đỡ quý báu của các thầy cô giáo bộ môn, ban giám hiệu, gia đình và bạn bè.

Với lòng kính trọng và biết ơn sâu sắc chúng em xin được bày tỏ lời cảm ơn chân thành tới: Ban giám hiệu, Phòng đào tạo trường Đại học Tài Nguyên và Môi Trường đã tạo mọi điều kiện thuận lợi giúp đỡ chúng em trong quá trình học tập và hoàn thành đồ án này. Cảm ơn thầy Phạm Trọng Huynh, giảng viên bộ môn Bảo Mật Mạng Máy Tính Và Hệ Thống và cũng là người thầy kính mến đã đã tận tình chỉ dạy những kiến thức bổ ích mà thầy đã mang đến cho chúng em, hết lòng giúp đỡ, dạy bảo, động viên chúng em trong suốt quá trình học tập và hoàn thành bài tiểu luận môn Bảo Mật Mạng Máy Tính Và Hệ Thống.

Mặc dù chúng em đã có nhiều cố gắng cũng như nỗ lực bằng tất cả sự nhiệt tình và năng lực của mình để hoàn thiện bài tiểu luận, tuy nhiên vẫn khó tránh khỏi những thiếu sót, rất mong nhận được những đóng góp quý báu của thầy.

Một lần nữa chúng em xin chân thành cảm ơn, chúc thầy sức khỏe và thành đạt và mong thầy giữ mãi lửa nhiệt huyết trong công việc để những lứa học sinh sau có được những trải nghiệm tốt trong môn học.

**Chúng em xin chân thành cảm ơn!**

**NHẬN XÉT**

……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

|  |
| --- |
| **Điểm** |

**MỤC LỤC**

[Chương 1. TỔNG QUAN 1](#_Toc15668)

[1.1. Định nghĩa vấn đề 1](#_Toc25614)

[1.2. Phạm vi 1](#_Toc20961)

[1.3. Mục tiêu đề tài 2](#_Toc881)

[1.4. Tính cấp thiết của đề tài 2](#_Toc22298)

[1.5. Lý do chọn đề tài 3](#_Toc22211)

[Chương 2. PHÂN TÍCH ĐỀ TÀI 4](#_Toc3274)

[2.1. Phân tích yêu cầu 4](#_Toc7391)

[2.2. Yêu cầu chức năng 4](#_Toc8854)

[2.3. Yêu cầu phi chức năng 5](#_Toc19005)

[2.4. Công việc cần giải quyết 6](#_Toc22743)

[Chương 3. THIẾT KẾ 7](#_Toc19597)

[3.1. Giới thiệu các phương pháp xác thực hai nhân tố trên đám mây 7](#_Toc16973)

[3.1.1. SMS xác thực 7](#_Toc8218)

[3.1.2. Xác thực email 7](#_Toc29815)

[3.1.3. Mã hóa dữ liệu Firebase bằng thuật toán AES 7](#_Toc27967)

[3.1.4. Xác thực bằng giọng nói 8](#_Toc9151)

[3.1.5. Xác thực bằng vân tay 8](#_Toc22124)

[3.2. Công cụ thực nghiệm 8](#_Toc20942)

[3.2.1. Xác thực hai nhân tố trên Firebase Authentication 8](#_Toc9115)

[3.2.2. Xác thực firebase authentication với thiết bị android 10](#_Toc10187)

[3.2.3. Mã hóa dữ liệu Android với Firebase bằng thuật toán AES 11](#_Toc7714)

[Chương 4. HIỆN THỰC 12](#_Toc9047)

[4.1. Khái quát sơ lược 12](#_Toc18491)

[4.2. Thực hiện mô phỏng 17](#_Toc13429)

[Chương 5. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 23](#_Toc13764)

[5.1. Kết quả đạt được 23](#_Toc7118)

[5.2. Hạn chế 23](#_Toc14337)

[5.3. Hướng phát triển 23](#_Toc5096)

[5.4. Kết luận 24](#_Toc23652)

[DANH MỤC TÀI LIỆU THAM KHẢO 25](#_Toc25933)

**DANH MỤC HÌNH**

[Hình 3. 1. Mô hình xác thực hai nhân tố trên firebase 9](#_Toc132575431)

[Hình 3. 2. Thiết bị Android 10](#_Toc132575432)

[Hình 3. 3. Thuật toán AES 11](#_Toc132575433)

[Hình 4. 1. Cơ sở dữ liệu firebase authentication……………………………………...12](#_Toc132575440)

[Hình 4. 2. Ứng dụng Android studio 13](#_Toc132575441)

[Hình 4. 3. Kết nối Android với firebase database realtime 13](#_Toc132575442)

[Hình 4. 4. Kết nối Android với firebase authentication 14](#_Toc132575443)

[Hình 4. 5. Java version 19.0.2 14](#_Toc132575444)

[Hình 4. 6. Mã SHA-1 15](#_Toc132575445)

[Hình 4. 7. PhoneAuthoptions 15](#_Toc132575446)

[Hình 4. 8. Xác thực qua Email với firebase authentication 16](#_Toc132575447)

[Hình 4. 9. Thuật toán AES 16](#_Toc132575448)

[Hình 4. 10. Kích hoạt xác thực 17](#_Toc132575449)

[Hình 4. 11. Hình mô phỏng 1 17](#_Toc132575450)

[Hình 4. 12. Hình mô phỏng 2 18](#_Toc132575451)

[Hình 4. 13. Hình mô phỏng 3 19](#_Toc132575452)

[Hình 4. 14. Hình mô phỏng 4 19](#_Toc132575453)

[Hình 4. 15. Hình mô phỏng 5 20](#_Toc132575454)

[Hình 4. 16. Hình mô phỏng 6 20](#_Toc132575455)

[Hình 4. 17. Hình mô phỏng 7 21](#_Toc132575456)

[Hình 4. 18. Hình mô phỏng 8 21](#_Toc132575457)

[Hình 4. 19. Hình mô phỏng 9 22](#_Toc132575458)

1. TỔNG QUAN
   1. **Định nghĩa vấn đề**

Vấn đề đề tài nghiên cứu và triển khai là bảo mật thông tin và dữ liệu trên nền tảng điện toán đám mây. Với sự phát triển của công nghệ điện toán đám mây, ngày càng có nhiều tổ chức và cá nhân lưu trữ dữ liệu quan trọng của họ trên các dịch vụ điện toán đám mây như AWS, Firebase, Microsoft Azure, v.v. Tuy nhiên, việc bảo mật dữ liệu trên nền tảng điện toán đám mây đối mặt với nhiều thách thức và rủi ro bảo mật.

Một trong những phương pháp bảo mật thông tin và dữ liệu trên nền tảng điện toán đám mây là triển khai các phương pháp xác thực hai nhân tố. Phương pháp này yêu cầu người dùng phải xác thực bằng hai yếu tố khác nhau để truy cập vào hệ thống. Điều này giúp tăng cường bảo mật thông tin và dữ liệu trên nền tảng điện toán đám mây bằng cách đảm bảo rằng chỉ có người dùng hợp lệ mới có thể truy cập vào hệ thống.

* 1. Phạm vi

Phạm vi trong đề tài nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây có thể bao gồm những nội dung sau:

*Tìm hiểu và phân tích các phương pháp xác thực hai nhân tố hiện có:* Đầu tiên, ta sẽ nghiên cứu các phương pháp xác thực hai nhân tố được sử dụng phổ biến hiện nay như mã OTP (One-Time Password), SMS OTP, ứng dụng di động OTP, mã QR và hình thức sinh trắc học.

*Triển khai các phương pháp xác thực hai nhân tố trên nền tảng điện toán đám mây:* Sau khi phân tích và đánh giá các phương pháp xác thực hai nhân tố, ta sẽ tiến hành triển khai các phương pháp này trên một số nền tảng điện toán đám mây phổ biến như AWS, Google Cloud và Microsoft Azure. Việc triển khai sẽ bao gồm cài đặt, cấu hình và kiểm tra tính năng của các phương pháp xác thực hai nhân tố.

*Đánh giá tính khả thi và tính hiệu quả của việc triển khai các phương pháp xác thực hai nhân tố:* Cuối cùng, ta sẽ đánh giá tính khả thi và tính hiệu quả của việc triển khai các phương pháp xác thực hai nhân tố trên nền tảng điện toán đám mây. Điều này bao gồm đánh giá các yếu tố như tính bảo mật, tính tiện lợi, tính khả dụng và hiệu quả trong việc ngăn chặn các cuộc tấn công truy cập trái phép vào hệ thống và bảo vệ dữ liệu của người dùng trên nền tảng điện toán đám mây.

* 1. Mục tiêu đề tài

Mục tiêu trong đề tài nghiên và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây có thể bao gồm những mục tiêu sau:

* Nghiên cứu và đánh giá các phương pháp xác thực hai nhân tố hiện có để tìm ra các phương pháp tốt nhất trong việc ngăn chặn các cuộc tấn công truy cập trái phép vào hệ thống và bảo vệ dữ liệu của người dùng trên nền tảng điện toán đám mây.
* Triển khai các phương pháp xác thực hai nhân tố trên các nền tảng điện toán đám mây phổ biến để kiểm tra tính khả dụng và tính bảo mật của chúng.
* Đánh giá tính khả thi và tính hiệu quả của việc triển khai các phương pháp xác thực hai nhân tố trên nền tảng điện toán đám mây, đồng thời đưa ra những khuyến nghị và đề xuất để tăng cường bảo mật và cải thiện trải nghiệm sử dụng cho người dùng.
* Từ các mục tiêu này, đề tài mong muốn đóng góp vào việc nâng cao độ tin cậy và bảo mật của hệ thống điện toán đám mây, giúp người dùng có thể yên tâm sử dụng các dịch vụ điện toán đám mây một cách an toàn và hiệu quả hơn.
  1. Tính cấp thiết của đề tài

Hiện nay, việc sử dụng các dịch vụ điện toán đám mây đang trở nên phổ biến và ngày càng được ưa chuộng hơn. Tuy nhiên, việc bảo vệ thông tin cá nhân và dữ liệu trên các nền tảng điện toán đám mây vẫn còn là một thách thức lớn đối với người dùng và các nhà cung cấp dịch vụ.

Vấn đề xác thực người dùng là một trong những vấn đề quan trọng nhất trong bảo mật thông tin trên các nền tảng điện toán đám mây. Hiện nay, nhiều người dùng chỉ sử dụng một yếu tố xác thực như mật khẩu để đăng nhập vào các tài khoản của mình trên nền tảng điện toán đám mây, điều này có thể dẫn đến các rủi ro bảo mật, chẳng hạn như lộ thông tin cá nhân, dữ liệu quan trọng hay truy cập trái phép từ bên ngoài.

Do đó, đề tài nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây là rất cấp thiết để nâng cao độ tin cậy và bảo mật của hệ thống điện toán đám mây, giảm thiểu các rủi ro bảo mật, đảm bảo an toàn cho dữ liệu và thông tin cá nhân của người dùng trên các nền tảng điện toán đám mây.

Việc triển khai các phương pháp xác thực hai nhân tố sẽ giúp ngăn chặn các cuộc tấn công truy cập trái phép vào hệ thống, đồng thời tăng cường khả năng phát hiện và xử lý các cuộc tấn công khi có sự cố xảy ra. Từ đó, người dùng sẽ có thể sử dụng các dịch vụ điện toán đám mây một cách an toàn và hiệu quả hơn.

* 1. Lý do chọn đề tài

Việc chọn đề tài nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây đến từ nhu cầu thực tiễn và sự phát triển của công nghệ thông tin hiện nay. Với sự phổ biến của các dịch vụ điện toán đám mây, người dùng cần có một cơ chế xác thực bảo mật để bảo vệ thông tin cá nhân và dữ liệu trên các nền tảng này.

Mật khẩu đơn giản hiện nay đã không còn đảm bảo độ bảo mật cao như trước, nên việc triển khai phương pháp xác thực hai nhân tố là hợp lý và cần thiết để tăng cường bảo mật cho hệ thống điện toán đám mây. Đồng thời, với sự phát triển của các công nghệ như trí tuệ nhân tạo, học máy và khai phá dữ liệu, việc áp dụng các phương pháp xác thực hai nhân tố vào nền tảng điện toán đám mây cũng trở nên dễ dàng và hiệu quả hơn.

1. PHÂN TÍCH ĐỀ TÀI
   1. Phân tích yêu cầu

Yêu cầu đề tài là mục tiêu nghiên cứu và triển khai các phương pháp xác thực hai nhân tố trên nền tảng điện toán đám mây bao gồm:

* **Hiệu quả:** Phương pháp xác thực hai nhân tố phải đảm bảo tính hiệu quả trong việc xác thực người dùng trên nền tảng điện toán đám mây. Các phương pháp phải được thiết kế sao cho không gây ra quá nhiều phiền toái cho người dùng nhưng vẫn đảm bảo tính bảo mật cao.
* **Bảo mật:** Yêu cầu về bảo mật là rất quan trọng trong việc triển khai phương pháp xác thực hai nhân tố. Hệ thống xác thực phải đảm bảo tính bảo mật cao, tránh được các mối đe dọa bảo mật từ bên ngoài. Đồng thời, các thông tin xác thực phải được mã hóa và bảo vệ an toàn.
* **Linh hoạt:** Phương pháp xác thực hai nhân tố phải linh hoạt và có thể được triển khai trên nhiều nền tảng điện toán đám mây khác nhau. Việc triển khai phương pháp xác thực không được giới hạn bởi các giới hạn kỹ thuật hoặc các yêu cầu cụ thể của nền tảng.
* **Thân thiện với người dùng:** Phương pháp xác thực hai nhân tố cần được thiết kế để đáp ứng các yêu cầu của người dùng và đảm bảo tính thân thiện với người dùng. Hệ thống xác thực phải dễ sử dụng và đảm bảo tính tiện dụng trong quá trình sử dụng.
* **Dễ dàng triển khai:** Phương pháp xác thực hai nhân tố cần được triển khai một cách dễ dàng và tiện lợi. Hệ thống xác thực phải được thiết kế để có thể được triển khai một cách nhanh chóng và hiệu quả, đồng thời phải đảm bảo tính tương thích với các công nghệ và hệ thống hiện có của tổ chức.
  1. Yêu cầu chức năng

Yêu cầu chức năng đề tài nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây bao gồm:

* **Xác thực hai nhân tố:** Hệ thống phải có khả năng xác thực hai nhân tố, bao gồm cả thông tin đăng nhập (username/password) và yếu tố thứ hai như mã xác thực, thông qua điện thoại di động, email hoặc token bảo mật. Quá trình xác thực phải được thiết kế sao cho đáp ứng được yêu cầu về bảo mật và tính linh hoạt.
* **Quản lý tài khoản:** Hệ thống phải có khả năng quản lý tài khoản của người dùng, bao gồm cả việc đăng ký tài khoản mới, quản lý thông tin tài khoản, cập nhật thông tin và đặt lại mật khẩu.
* **Bảo mật thông tin:** Hệ thống phải đảm bảo tính bảo mật cao đối với thông tin cá nhân của người dùng, bao gồm cả thông tin đăng nhập và các thông tin khác như thông tin tài khoản và thông tin thanh toán.
* **Tích hợp với nền tảng điện toán đám mây:** Hệ thống phải được thiết kế để tích hợp với nhiều nền tảng điện toán đám mây khác nhau, đảm bảo tính linh hoạt trong việc triển khai và sử dụng.
* **Điều chỉnh cấu hình:** Hệ thống phải cho phép người quản trị điều chỉnh cấu hình xác thực, bao gồm cả cấu hình yếu tố thứ hai, thời gian đăng nhập và đặc quyền quản trị viên.
* **Ghi nhật ký và báo cáo:** Hệ thống phải có khả năng ghi nhật ký hoạt động của người dùng và báo cáo về các hoạt động xác thực, để quản trị viên có thể theo dõi và phát hiện các hoạt động đáng ngờ.
  1. Yêu cầu phi chức năng
* Bảo mật: Hệ thống xác thực hai nhân tố cần đảm bảo tính bảo mật cao để ngăn chặn các cuộc tấn công từ bên ngoài như tấn công từ chối dịch vụ (DDoS), tấn công người giả mạo (phishing), hoặc tấn công đánh cắp thông tin cá nhân.
* Tính khả dụng: Hệ thống xác thực hai nhân tố cần đảm bảo tính khả dụng để đảm bảo người dùng có thể sử dụng mọi lúc mọi nơi, ngay cả khi có tình huống không mong muốn xảy ra như mất kết nối hoặc sự cố hệ thống.
* Hiệu suất: Hệ thống xác thực hai nhân tố cần đảm bảo hiệu suất cao để xác thực người dùng nhanh chóng và hiệu quả.
* Dễ sử dụng: Hệ thống xác thực hai nhân tố cần có giao diện đơn giản, dễ sử dụng và thân thiện với người dùng để tăng tính tiện dụng và giảm thời gian đào tạo cho người dùng.
* Mở rộng: Hệ thống xác thực hai nhân tố cần có khả năng mở rộng để đáp ứng nhu cầu sử dụng của các doanh nghiệp trong tương lai.
  1. Công việc cần giải quyết

Các công việc cần giải quyết trong đề tài nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây bao gồm:

* **Tìm hiểu các phương pháp xác thực hai nhân tố:** Cần phải tìm hiểu các phương pháp xác thực hai nhân tố để chọn ra phương pháp phù hợp nhất cho nền tảng điện toán đám mây.
* **Thiết kế kiến trúc hệ thống:** Dựa trên phương pháp xác thực hai nhân tố được lựa chọn, cần thiết kế kiến trúc hệ thống để triển khai trên nền tảng điện toán đám mây.
* **Lựa chọn và tích hợp các công nghệ:** Cần lựa chọn và tích hợp các công nghệ để triển khai hệ thống xác thực hai nhân tố trên nền tảng điện toán đám mây, bao gồm các công nghệ liên quan đến bảo mật, giao tiếp và lưu trữ.
* **Phát triển phần mềm:** Cần phát triển phần mềm để triển khai hệ thống xác thực hai nhân tố trên nền tảng điện toán đám mây.
* **Kiểm thử và đánh giá hệ thống:** Sau khi triển khai, cần thực hiện kiểm thử và đánh giá hệ thống để đảm bảo tính ổn định, hiệu quả và đáp ứng được yêu cầu của người dùng.
* **Triển khai và hỗ trợ:** Sau khi hoàn thành và đánh giá hệ thống, cần triển khai và cung cấp hỗ trợ cho người dùng sử dụng hệ thống xác thực hai nhân tố trên nền tảng điện toán đám mây.

1. THIẾT KẾ
   1. Giới thiệu các phương pháp xác thực hai nhân tố trên đám mây
      1. SMS xác thực

Đây là phương pháp đơn giản và phổ biến nhất, trong đó một mã xác thực OTP sẽ được gửi đến điện thoại di động của người dùng qua tin nhắn văn bản. Người dùng sau đó phải nhập mã này vào trang web hoặc ứng dụng để xác thực đăng nhập hoặc đăng ký.

* + 1. Xác thực email

Xác thực bằng mã OTP: Sau khi người dùng đăng nhập bằng mật khẩu, hệ thống sẽ gửi một mã OTP đến địa chỉ email đã đăng ký của người dùng. Người dùng sau đó phải nhập mã OTP này để hoàn thành quá trình đăng nhập.

Xác thực bằng hình ảnh hoặc câu hỏi: Để đảm bảo tính bảo mật của email, người dùng có thể được yêu cầu cung cấp một hình ảnh hoặc câu hỏi bảo mật được đặt trước đó để xác thực danh tính của họ. Hình ảnh hoặc câu hỏi này sẽ xuất hiện mỗi khi người dùng đăng nhập vào tài khoản email của họ.

Một số nhà cung cấp email đã tích hợp phương pháp xác thực email hai nhân tố vào hệ thống của họ để cung cấp bảo mật cao hơn cho tài khoản email của người dùng. Việc sử dụng phương pháp xác thực hai nhân tố này giúp ngăn chặn các cuộc tấn công mạng bằng cách yêu cầu người dùng cung cấp nhiều yếu tố để xác thực danh tính của họ, đồng thời tăng cường tính bảo mật của email bằng cách yêu cầu một bước xác thực thêm sau khi người dùng nhập mật khẩu.

* + 1. Mã hóa dữ liệu Firebase bằng thuật toán AES

Mã hóa dữ liệu Android với Firebase bằng thuật toán AES là quá trình mã hóa dữ liệu trong ứng dụng Android của bạn bằng cách sử dụng thuật toán mã hóa AES (Advanced Encryption Standard) và lưu trữ dữ liệu đã được mã hóa trên nền tảng Firebase Realtime Database hoặc Cloud Firestore.

Thuật toán AES là một trong những thuật toán mã hóa đối xứng phổ biến nhất được sử dụng trong các ứng dụng mã hóa dữ liệu. Nó có thể được sử dụng để mã hóa và giải mã các tệp và thông tin cá nhân nhạy cảm của người dùng.

**Để mã hóa dữ liệu Android với Firebase bằng thuật toán AES, bạn cần thực hiện các bước sau:**

**Bước 1:** Tạo khóa mã hóa (encryption key) và vector khởi tạo (initialization vector) để mã hóa và giải mã dữ liệu. Khóa mã hóa được sử dụng để mã hóa dữ liệu và phải được bảo vệ chặt chẽ để đảm bảo rằng không ai có thể giải mã dữ liệu. Vector khởi tạo được sử dụng để bảo vệ khóa mã hóa khỏi việc tấn công theo kiểu "brute-force".

**Bước 2:** Sử dụng API của AES để mã hóa dữ liệu. Để mã hóa dữ liệu bằng AES, bạn có thể sử dụng lớp Cipher trong Java. Lớp Cipher cung cấp các phương thức để mã hóa và giải mã dữ liệu bằng các thuật toán mã hóa khác nhau, bao gồm AES.

**Bước 3:** Lưu trữ dữ liệu đã được mã hóa lên Firebase Realtime Database hoặc Cloud Firestore. Để lưu trữ dữ liệu đã được mã hóa, bạn có thể sử dụng API của Firebase Realtime Database hoặc Cloud Firestore để lưu trữ dữ liệu đã được mã hóa và giải mã dữ liệu khi cần thiết.

* + 1. Xác thực bằng giọng nói

Kỹ thuật xác thực bằng giọng nói yêu cầu người dùng đọc một câu hoặc một loạt các từ được cung cấp bởi hệ thống. Hệ thống sau đó sẽ so sánh giọng nói của người dùng với dữ liệu giọng nói được lưu trữ để xác thực.

* + 1. Xác thực bằng vân tay

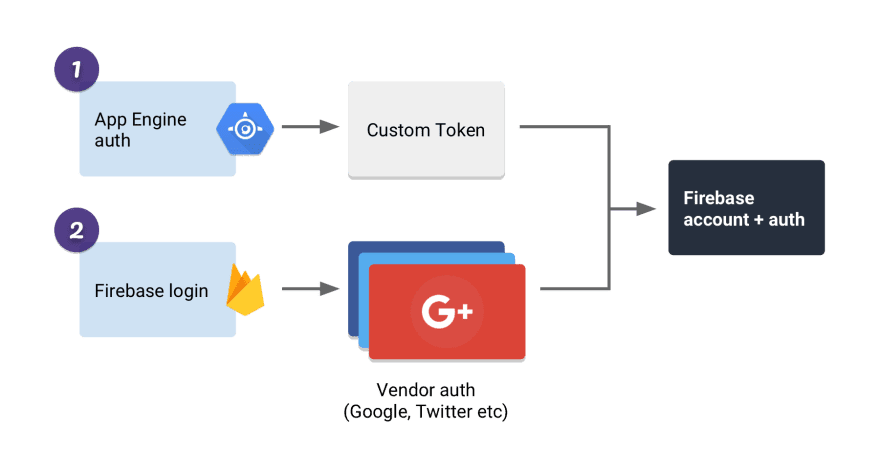
Kỹ thuật xác thực bằng vân tay yêu cầu sử dụng máy quét vân tay để xác thực danh tính của người dùng. Khi người dùng cố gắng truy cập vào tài khoản của họ, họ phải quét vân tay của mình trên máy quét vân tay để được xác thực.

* 1. Công cụ thực nghiệm
     1. Xác thực hai nhân tố trên Firebase Authentication

Firebase Authentication là một dịch vụ quản lý xác thực người dùng của Google Firebase, cung cấp các công cụ và tính năng để xác thực người dùng và quản lý đăng nhập đăng ký của người dùng trong ứng dụng của bạn.

**Firebase Authentication hỗ trợ nhiều phương pháp xác thực khác nhau, bao gồm:**

1. *Email/password:* Xác thực người dùng bằng cách yêu cầu họ nhập địa chỉ email và mật khẩu.
2. *Xác thực số điện thoại:* Xác thực người dùng bằng cách yêu cầu họ nhập số điện thoại và xác minh mã OTP được gửi đến số điện thoại của họ.
3. *Xác thực bên thứ ba:* Firebase Authentication cung cấp tích hợp với các nhà cung cấp xác thực bên thứ ba như Google, Facebook, Twitter, GitHub, Apple và Microsoft.
4. *Xác thực theo dõi:* Xác thực người dùng bằng cách yêu cầu họ sử dụng tài khoản Google hoặc Apple đã đăng nhập trên thiết bị của họ để đăng nhập vào ứng dụng.



**Hình 3. 1. Mô hình xác thực hai nhân tố trên firebase**

* + 1. Xác thực firebase authentication với thiết bị android



**Hình 3. 2. Thiết bị Android**

Xác thực trên Firebase Authentication với Android Studio là quá trình tích hợp và sử dụng Firebase Authentication để xác thực người dùng trong ứng dụng Android của bạn.

Để xác thực người dùng trên Firebase Authentication với Android Studio, bạn cần thực hiện các bước sau:

**Bước 1:** Thêm dependency Firebase Authentication vào ứng dụng Android của bạn.

**Bước 2:** Kết nối ứng dụng của bạn với Firebase bằng cách thêm tệp cấu hình Firebase vào ứng dụng của bạn. Bạn có thể làm điều này bằng cách thêm tệp google-services json vào thư mục app của ứng dụng của bạn. Tệp google-services json chứa thông tin xác thực của ứng dụng và được sử dụng để thiết lập kết nối giữa ứng dụng của bạn và dịch vụ Firebase.

**Bước 3:** Sử dụng API của Firebase Authentication để xác thực người dùng trong ứng dụng của bạn. Firebase Authentication cung cấp nhiều phương pháp xác thực khác nhau, bao gồm email/password, xác thực số điện thoại, xác thực bên thứ ba và xác thực theo dõi. Bạn có thể sử dụng các phương thức này để xác thực người dùng trong ứng dụng của bạn.

* Sau khi xác thực thành công, Firebase Authentication sẽ cấp cho người dùng một mã thông báo truy cập để xác thực các hoạt động sau này trong ứng dụng của bạn.
  + 1. Mã hóa dữ liệu Android với Firebase bằng thuật toán AES

- Mã hóa dữ liệu Android với Firebase bằng thuật toán AES là quá trình mã hóa dữ liệu trong ứng dụng Android của bạn bằng cách sử dụng thuật toán mã hóa AES (Advanced Encryption Standard) và lưu trữ dữ liệu đã được mã hóa trên nền tảng Firebase Realtime Database hoặc Cloud Firestore.

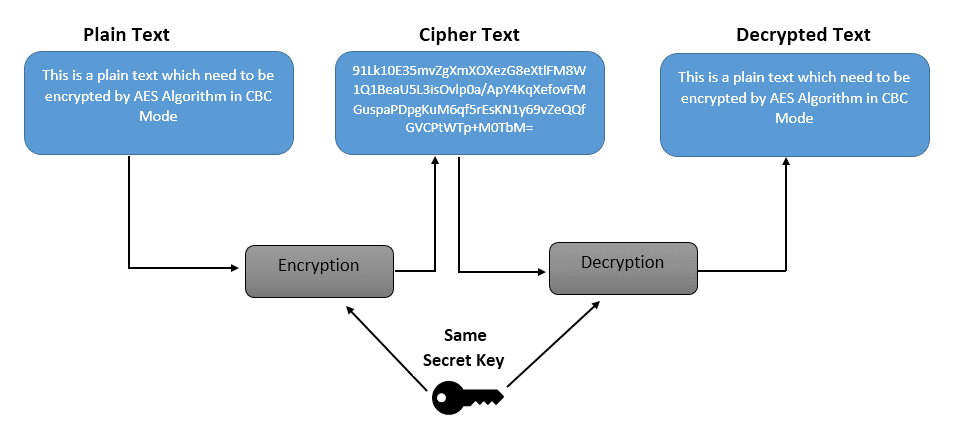
- Thuật toán AES là một trong những thuật toán mã hóa đối xứng phổ biến nhất được sử dụng trong các ứng dụng mã hóa dữ liệu. Nó có thể được sử dụng để mã hóa và giải mã các tệp và thông tin cá nhân nhạy cảm của người dùng.

**Để mã hóa dữ liệu Android với Firebase bằng thuật toán AES, bạn cần thực hiện các bước sau:**

**Bước 1:** Tạo khóa mã hóa (encryption key) và vector khởi tạo (initialization vector) để mã hóa và giải mã dữ liệu. Khóa mã hóa được sử dụng để mã hóa dữ liệu và phải được bảo vệ chặt chẽ để đảm bảo rằng không ai có thể giải mã dữ liệu. Vector khởi tạo được sử dụng để bảo vệ khóa mã hóa khỏi việc tấn công theo kiểu "brute-force".

**Bước 2:** Sử dụng API của AES để mã hóa dữ liệu. Để mã hóa dữ liệu bằng AES, bạn có thể sử dụng lớp Cipher trong Java. Lớp Cipher cung cấp các phương thức để mã hóa và giải mã dữ liệu bằng các thuật toán mã hóa khác nhau, bao gồm AES.

**Bước 3:** Lưu trữ dữ liệu đã được mã hóa lên Firebase Realtime Database hoặc Cloud Firestore. Để lưu trữ dữ liệu đã được mã hóa, bạn có thể sử dụng API của Firebase Realtime Database hoặc Cloud Firestore để lưu trữ dữ liệu đã được mã hóa và giải mã dữ liệu khi cần thiết.



**Hình 3. 3. Thuật toán AES**

1. HIỆN THỰC
   1. Khái quát sơ lược

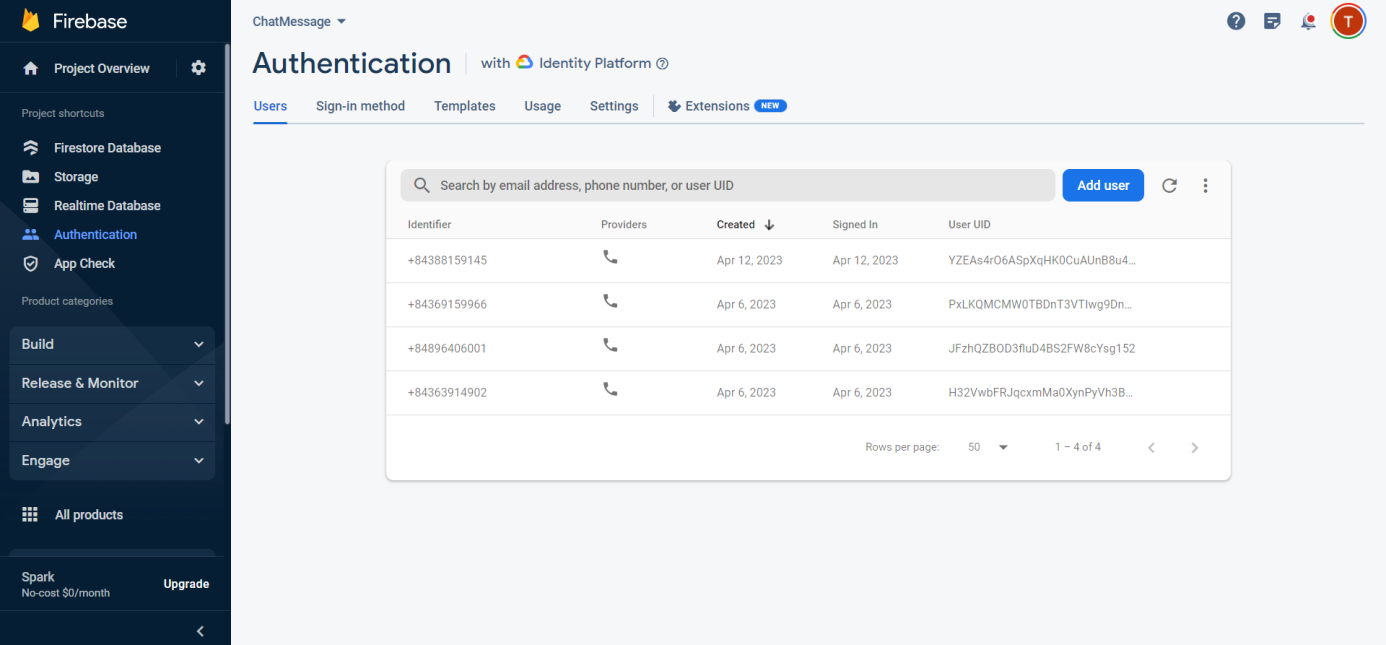
**Thực hiện việc thử nghiệm xác thực hai nhân tố trên đám mây sử dụng các công cụ như sau:**

* **Firebase Authentication**

Firebase Authentication là một dịch vụ của Firebase, được cung cấp bởi Google, giúp cho việc xác thực người dùng trong ứng dụng trở nên dễ dàng hơn. Firebase Authentication cung cấp một API đơn giản để phát triển các tính năng đăng nhập, đăng ký và đăng xuất trong ứng dụng của bạn.

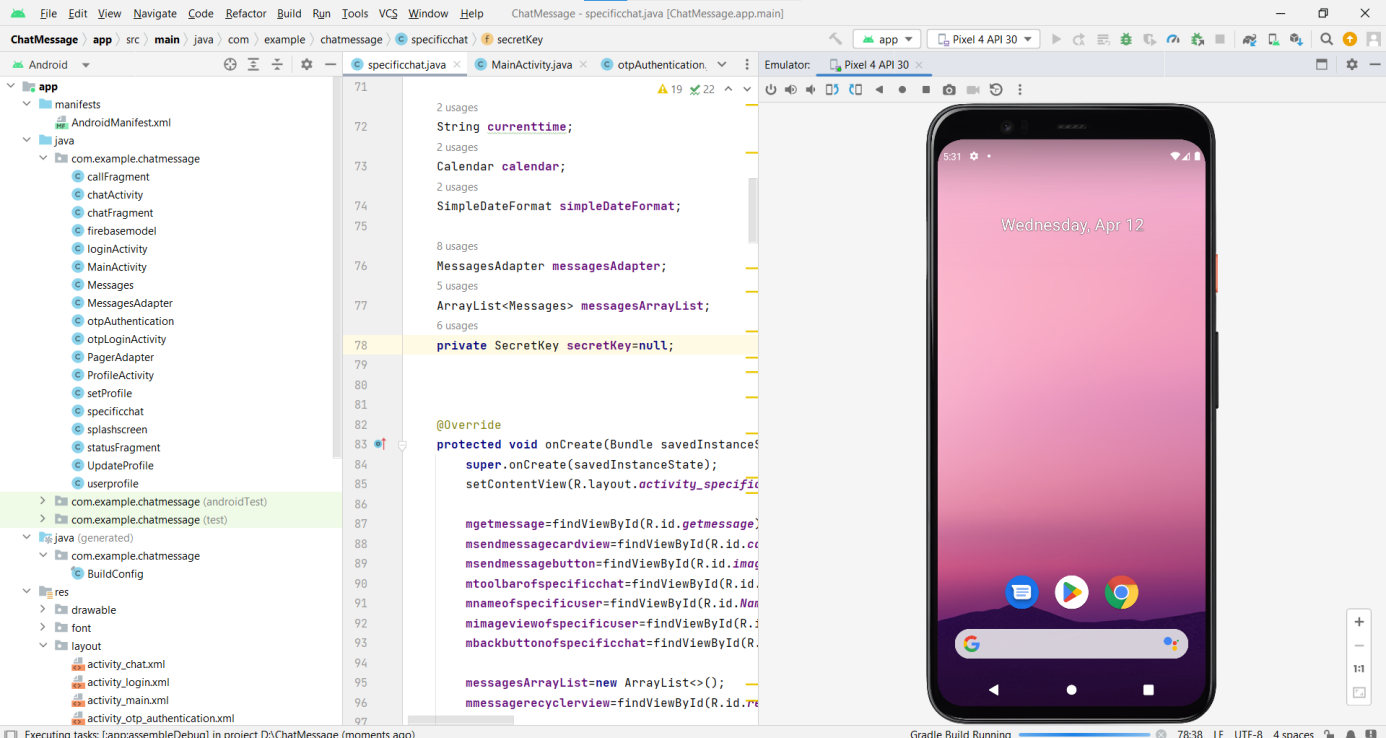
Firebase Authentication hỗ trợ nhiều phương thức đăng nhập như email và mật khẩu, đăng nhập với Google, Facebook, Twitter, GitHub, và các phương thức xác thực khác. Nó cũng hỗ trợ xác thực người dùng bằng cách sử dụng số điện thoại di động, đó là một tính năng quan trọng để có thể xác minh số điện thoại của người dùng một cách nhanh chóng và dễ dàng.

Firebase Authentication cũng cung cấp các tính năng bảo mật như bảo vệ dữ liệu người dùng với mức độ an toàn cao, chống lại tấn công brute-force, quản lý đăng nhập đa yếu tố, và phân quyền truy cập dựa trên vai trò người dùng. Với Firebase Authentication, bạn có thể xây dựng các ứng dụng đáng tin cậy, đảm bảo an toàn cho người dùng của mình.



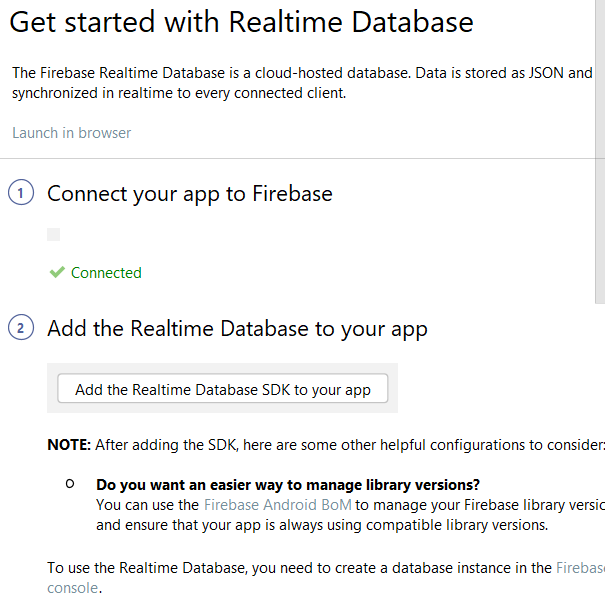
**Hình 4. 1. Cơ sở dữ liệu firebase authentication**

1. **Sử dụng Adroid studio để tương tác với firebase**



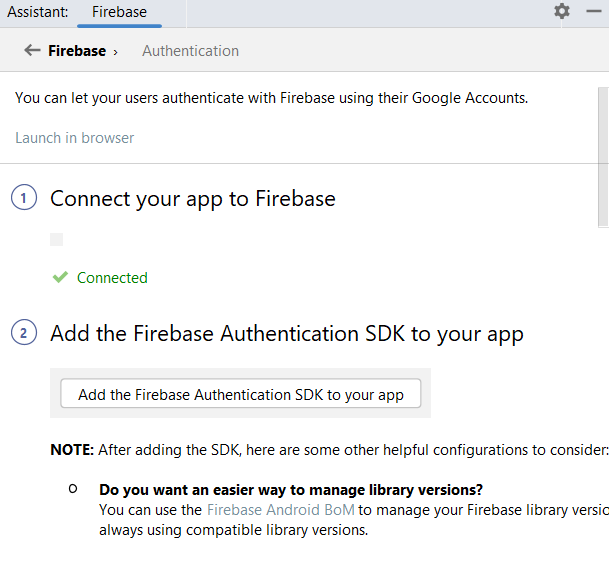
**Hình 4. 2. Ứng dụng Android studio**

1. **Kết nối Android studio với firebase database realtime**



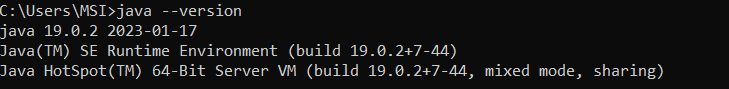
**Hình 4. 3. Kết nối Android với firebase database realtime**

1. **Kết nối Android studio với firebase authentication**



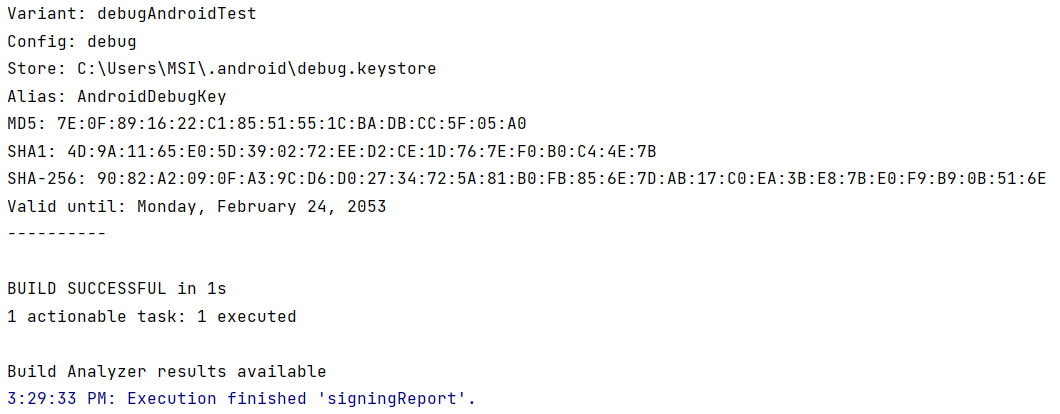
**Hình 4. 4.**  **Kết nối Android với firebase authentication**

1. **Ngôn ngữ lập trình: Java 19.0.2**



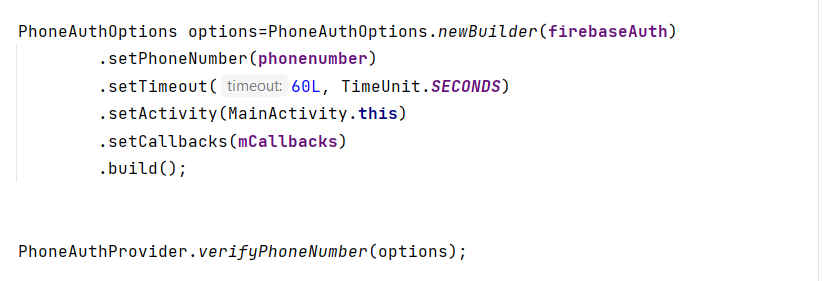
**Hình 4. 5. Java version 19.0.2**

1. **Sử dụng mã SHA-1 trong ứng dụng Android để đăng ký xác thực SMS với firebase authentication**



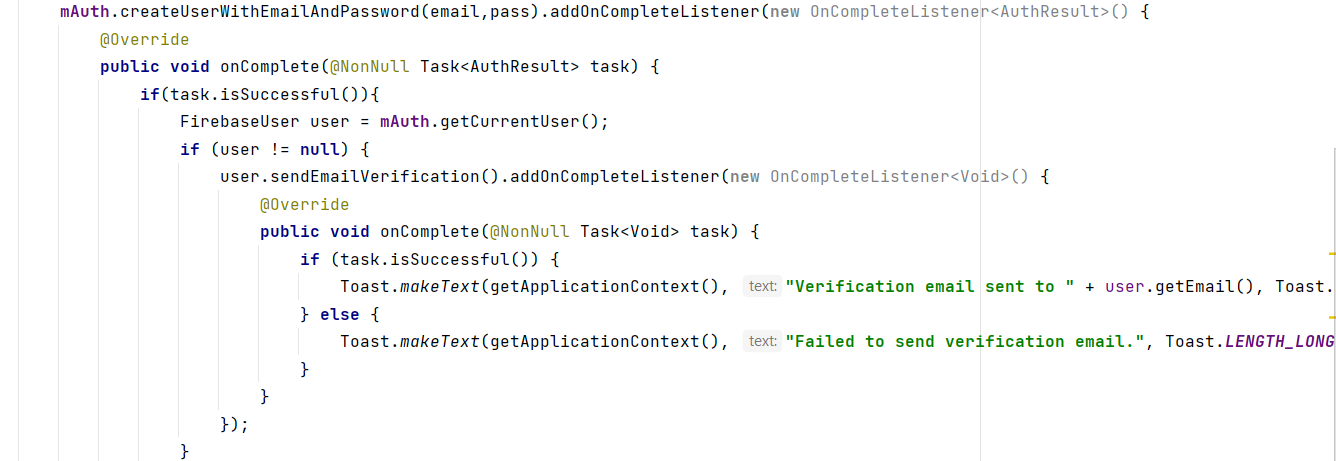
**Hình 4. 6. Mã SHA-1**

1. **Sử dụng PhoneAuthoptions trong java cho phép gửi OTP qua SMS để xác thực hai nhân tố với firebase authentication**



**Hình 4. 7.** **PhoneAuthoptions**

1. **Sử dụng mAuth.createUserWithhEmailAndPassword trong java cho phép link xác thực qua Email trong xác thực hai nhân tố với firebase authentication**



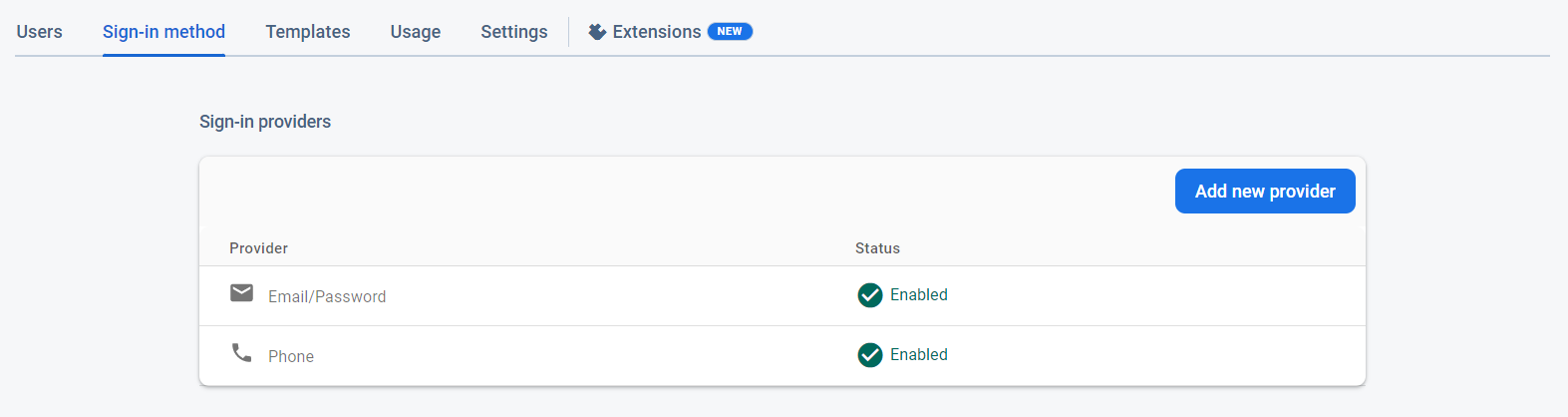
**Hình 4. 8. Xác thực qua Email với firebase authentication**

1. **Thuật toán AES trên java sử dụng mã hóa và giải mã dữ liệu trên firebase database realtime**



**Hình 4. 9.** **Thuật toán AES**

1. **Cho phép kích hoạt xác thực email và số điện thoại trên firebase authentication**

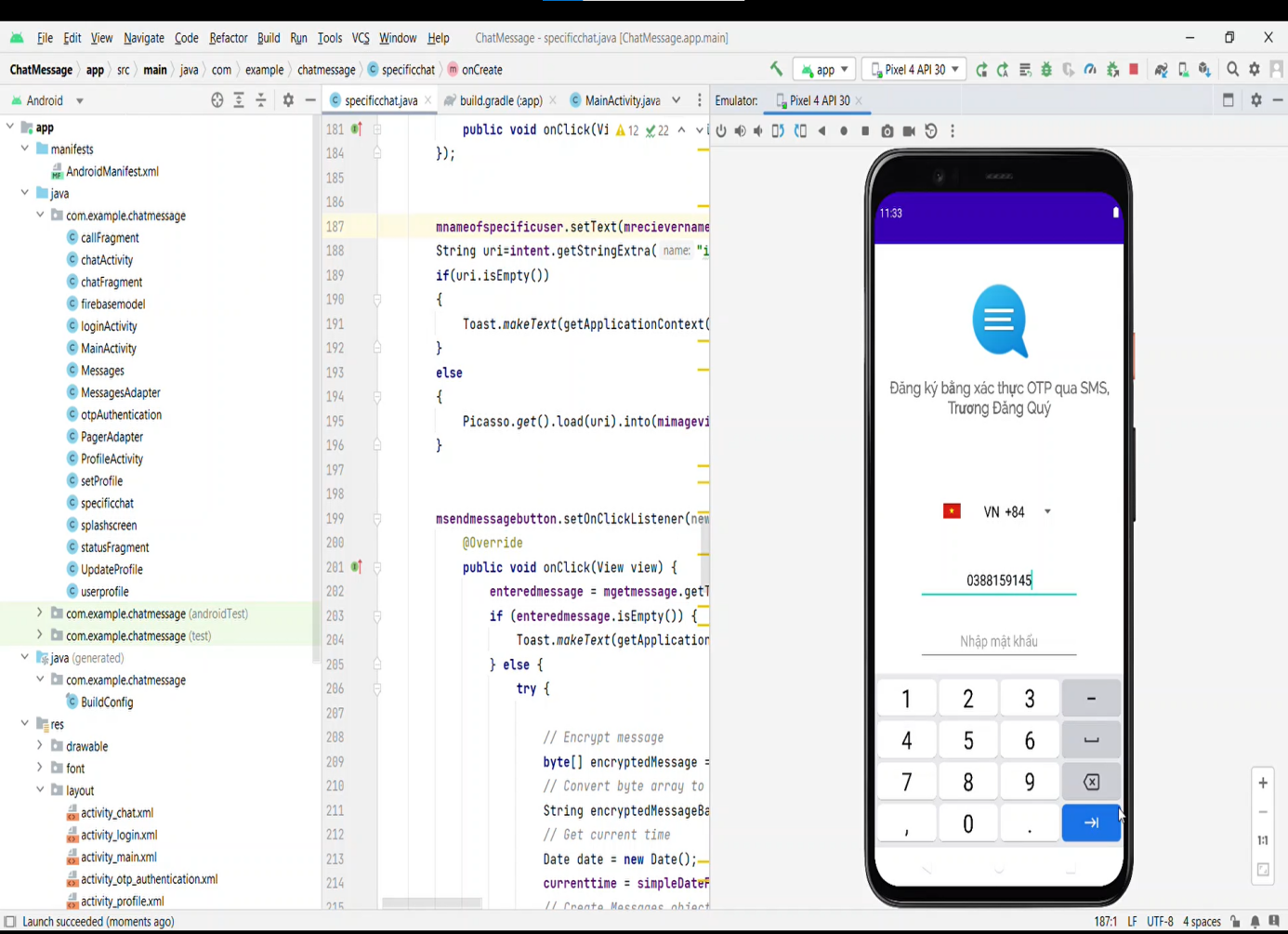


**Hình 4. 10. Kích hoạt xác thực**

* 1. Thực hiện mô phỏng

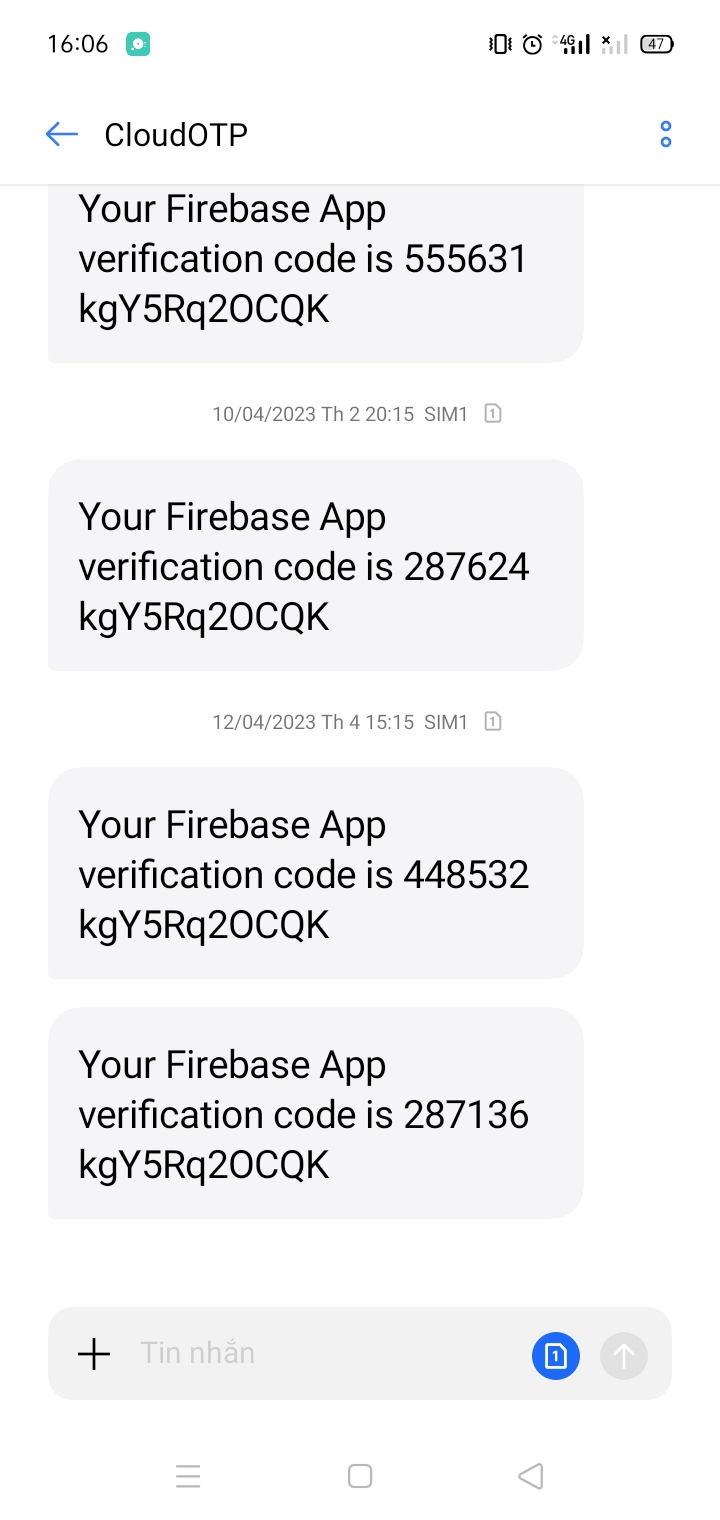
Xác thực hai nhân tố firebase authentication bằng số điện thoại trên Android studio

- Thực hiện lựa chọn mã vùng theo quốc gia và nhập số điện thoại, mật khẩu



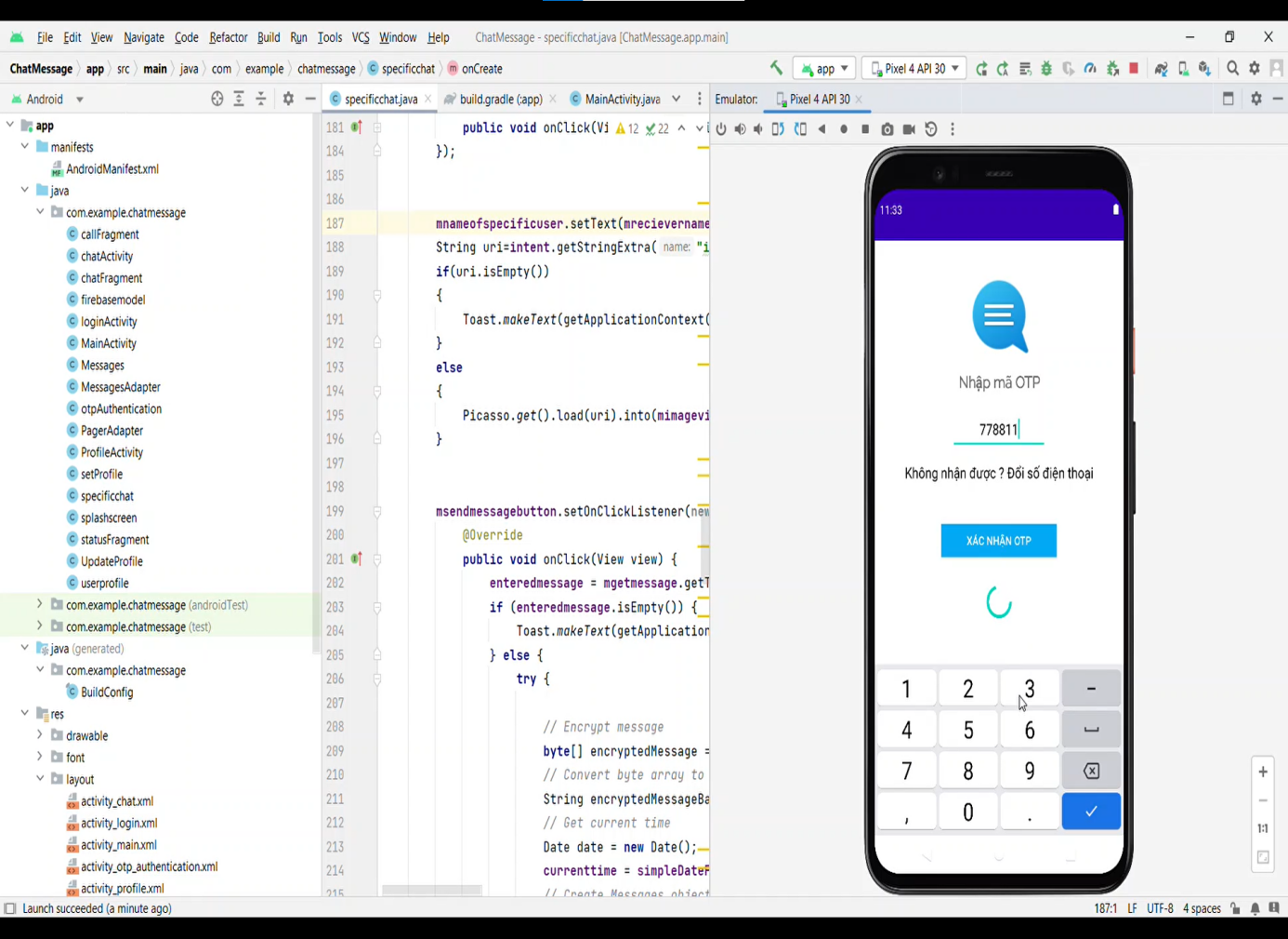
**Hình 4. 11. Hình mô phỏng 1**

- Số điện thoại được xác thực trên firebase authentication sẽ gửi mã OTP đến thiết bị đó để xác minh, bao gồm 6 số.



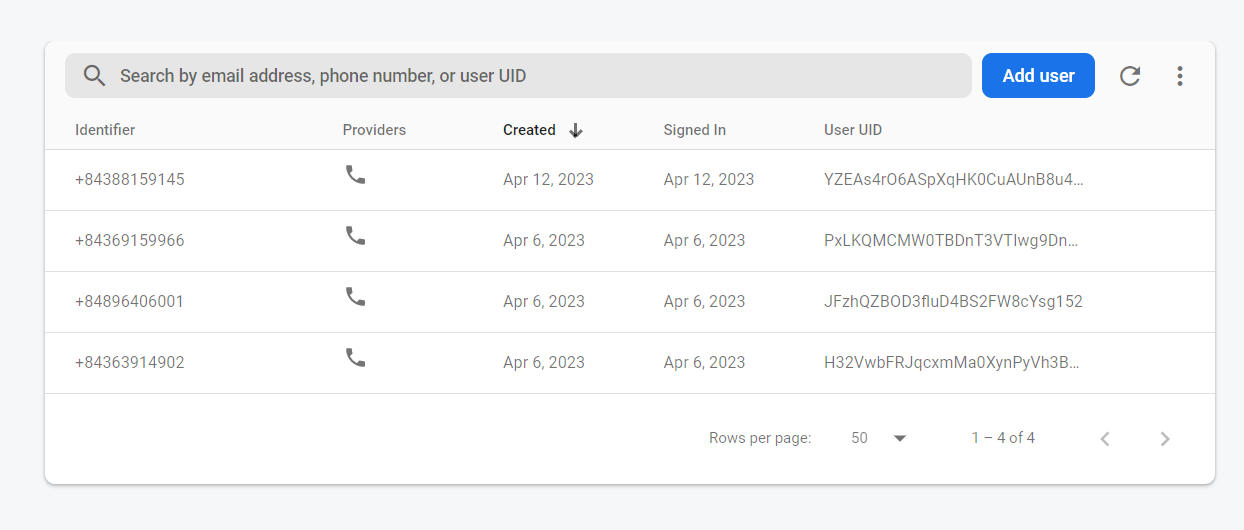
**Hình 4. 12. Hình mô phỏng 2**

- Nhập mã OTP đã được gửi đến thiết bị để tiến hành đăng ký thông tin tài khoản và cho phép đăng nhập vào hệ thống và truy cập vào cơ sở dữ liệu nhằm tăng tính bảo mật.



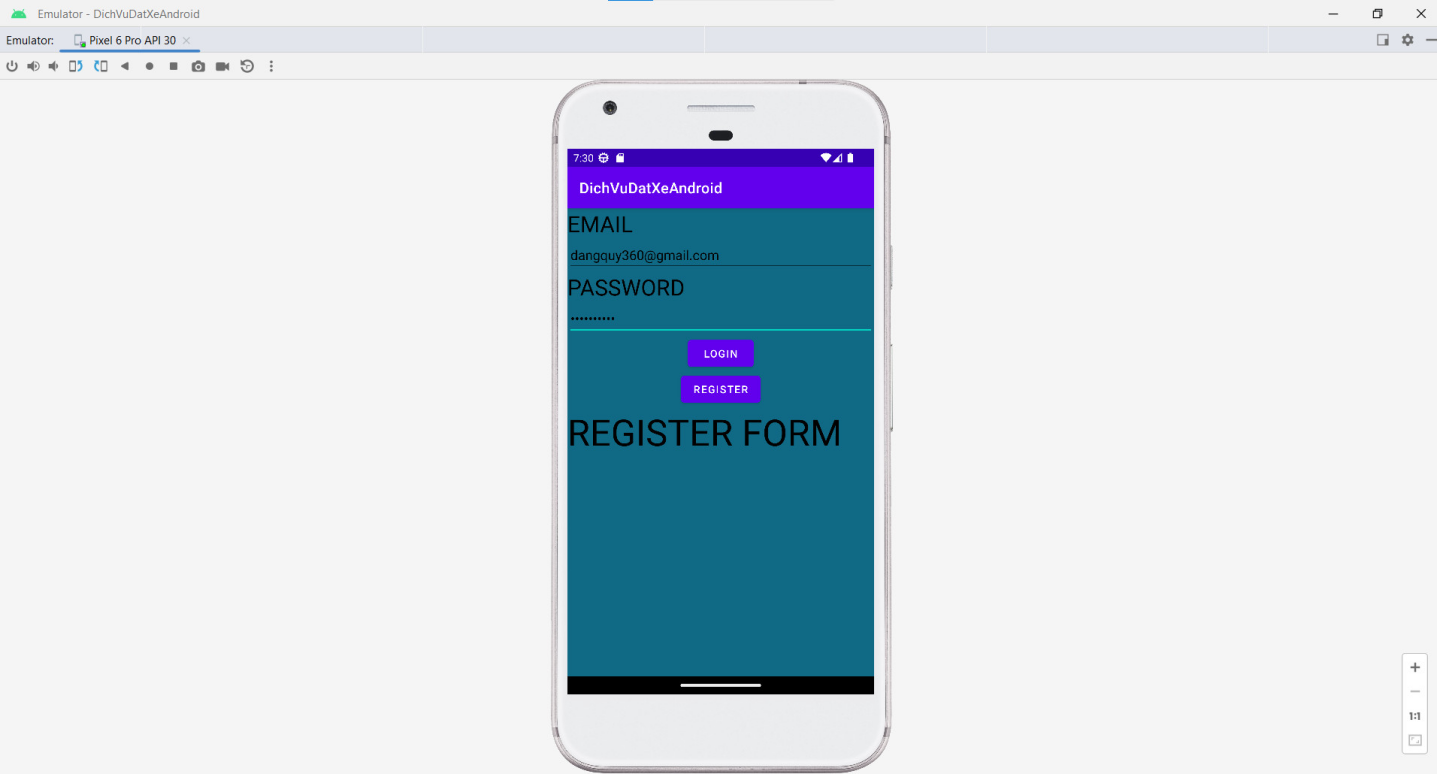
**Hình 4. 13. Hình mô phỏng 3**

- Số điện thoại sau khi đăng ký sẽ được lưu vào firebase authentication



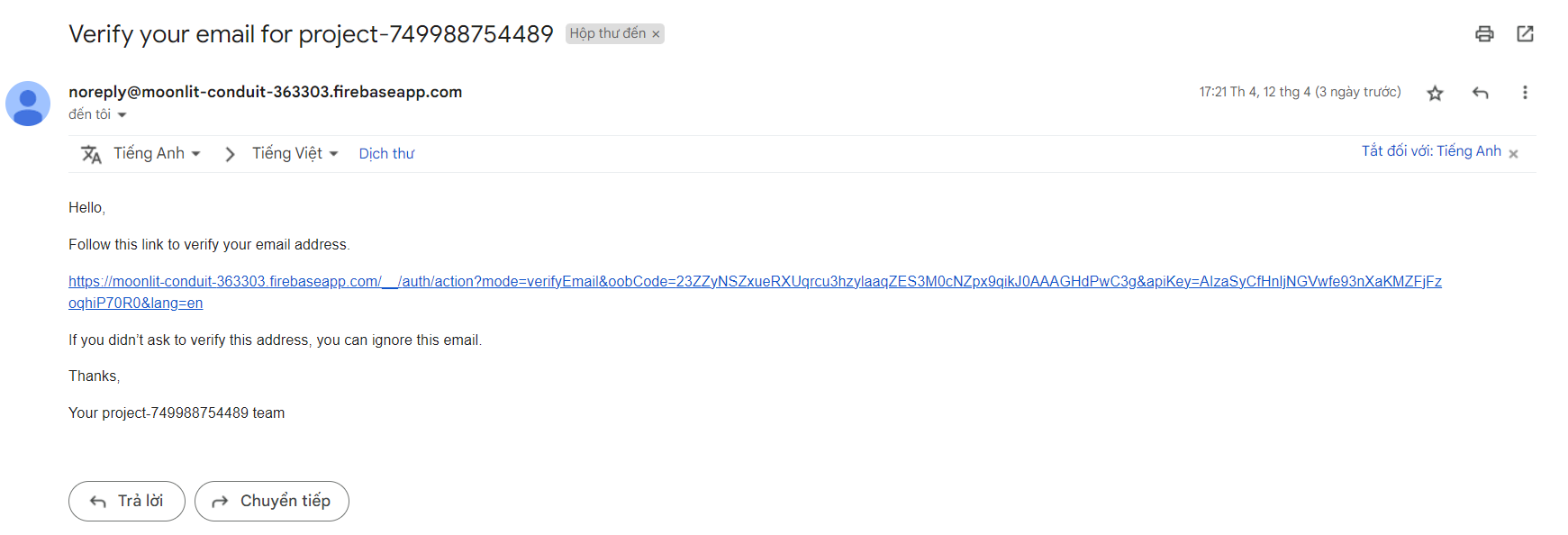
**Hình 4. 14. Hình mô phỏng 4**

- Đăng ký tài khoản bằng phương pháp xác hai nhân tố trên firebase authentication, sử dụng email và mật khẩu



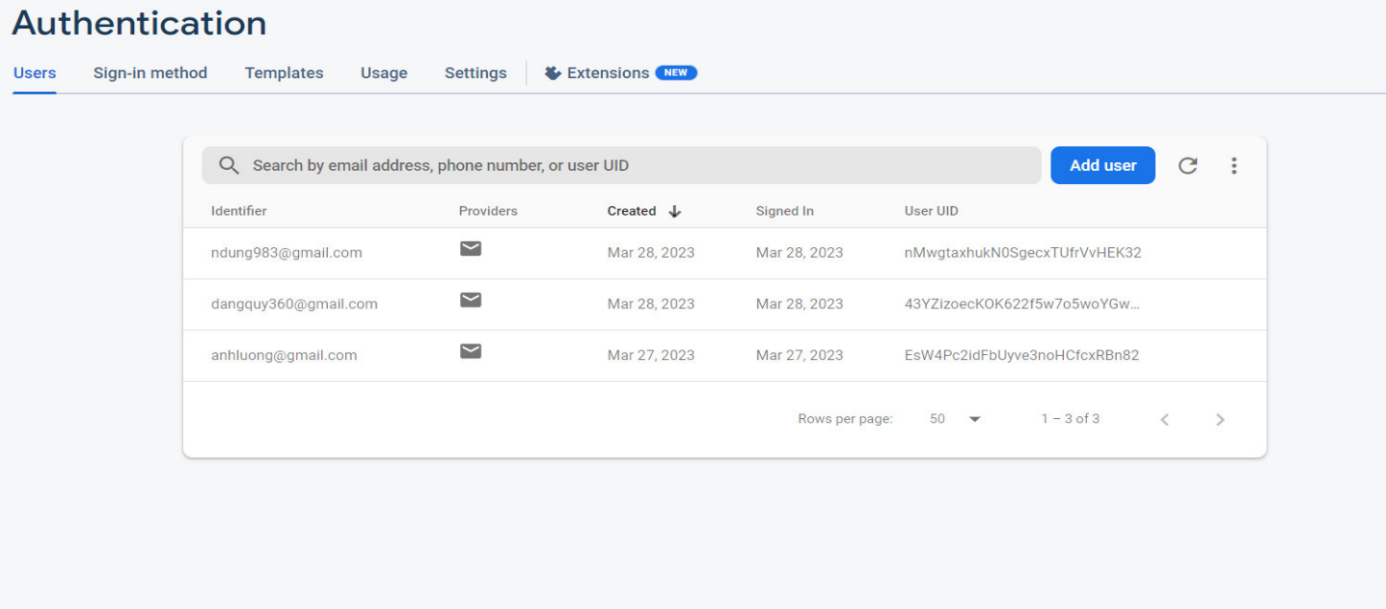
**Hình 4. 15. Hình mô phỏng 5**

- Sau khi đăng ký, thì tài khoản email đó sẽ nhận được một liên kết cho phép bấm xác thực để hoàn thành đăng ký



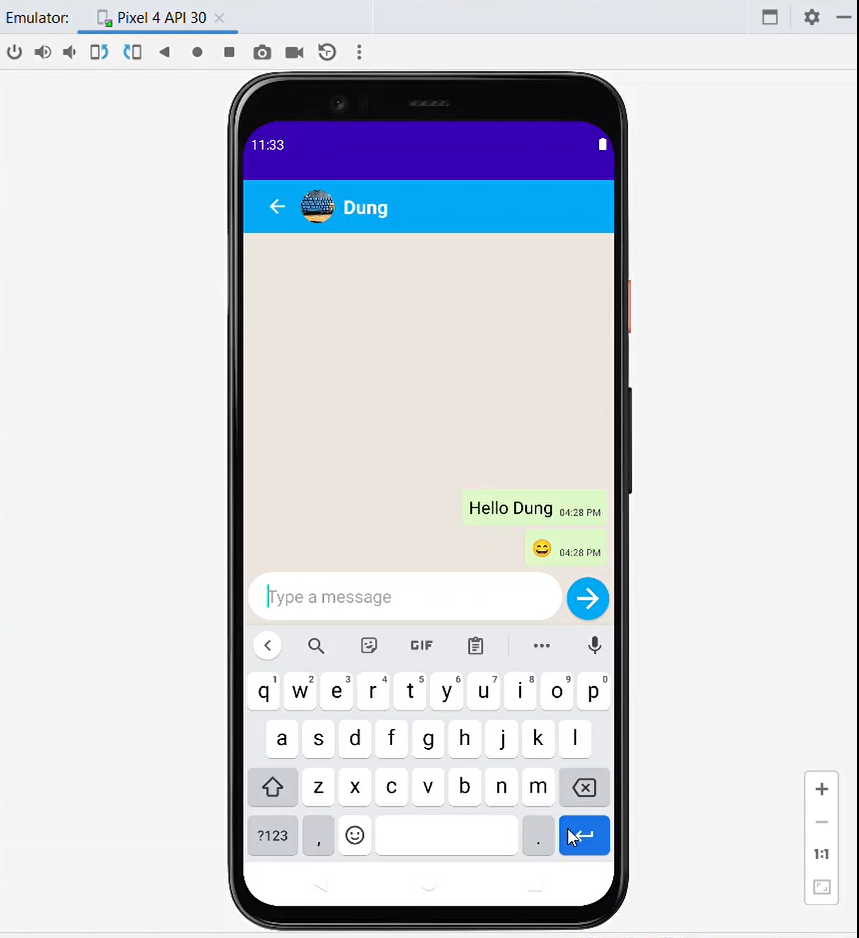
**Hình 4. 16. Hình mô phỏng 6**

- Sau khi đăng ký thành công thì tài khoản email đó sẽ được lưu vào firebase authentication



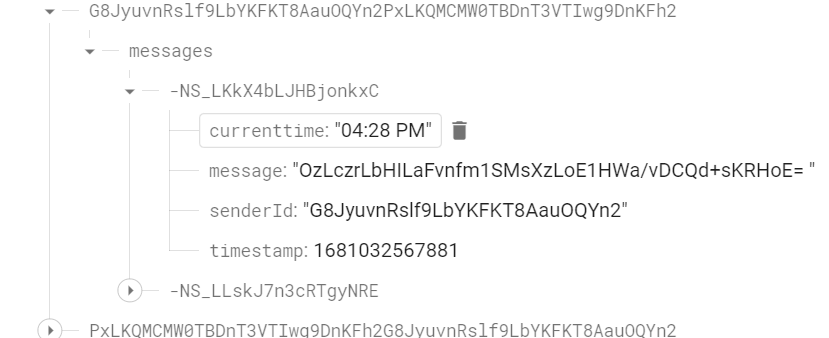
**Hình 4. 17. Hình mô phỏng 7**

- Giao diện nhắn tin sử dụng thuật toán mã hóa khóa đối xứng AES, sau khi nhắn tin thì nội dung sẽ được truyền trên internet và lưu vào firebase database realtime sau khi đã được mã hóa và chỉ giải mã trên thiết bị có sử dụng khóa



**Hình 4. 18. Hình mô phỏng 8**

* Kết quả của đoạn tin nhắn sử dụng thuật toán mã hóa khóa đối xứng AES được lưu vào firebase database realtime bằng nội dung mã hóa, không thể đọc được và chỉ có thể được giải mã trên thiết bị có khóa



**Hình 4. 19. Hình mô phỏng 9**

1. KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN
   1. Kết quả đạt được

- Nghiên cứu và xây dựng thành công phương pháp xác thực hai nhân tố trên điện toán đám mây và thuật toán mã hóa và giải mã khóa đối xứng AES.

- Sử dụng cho xác thực email và số điện thoại nhanh chóng và tiện lợi, không tốn chi phí.

- Độ bảo mật của ứng dụng là khá tương đối, khó có thể tấn công bởi bên ngoài.

* 1. Hạn chế

Hệ thống còn nhiều khuyết điểm như:

*- Phụ thuộc vào dịch vụ SMS:* Để sử dụng Phone Authentication trên Firebase, người dùng cần có một số điện thoại di động và dịch vụ SMS đang hoạt động. Trong một số trường hợp, việc sử dụng dịch vụ SMS có thể gây ra chi phí.

*- Khả năng bị tấn công xác thực giả mạo:* Phone Authentication trên Firebase vẫn có thể bị tấn công bằng các phương pháp giả mạo xác thực, nhưng Firebase cung cấp các tính năng bảo mật bổ sung để hạn chế rủi ro này.

*- Không thể tránh được tấn công các phương pháp tấn công mới:* Mặc dù AES được thiết kế để chống lại các cuộc tấn công phổ biến hiện nay, nhưng nó không thể tránh được tất cả các cuộc tấn công mới được phát triển trong tương lai.

*- Có thể bị tấn công bằng một số phương pháp:* Mặc dù AES là một thuật toán rất bảo mật, nó vẫn có thể bị tấn công bằng một số phương pháp, bao gồm các cuộc tấn công side-channel, cuộc tấn công hoán đổi khối, và cuộc tấn công từ điển.

* 1. Hướng phát triển
* Tăng cường tính linh hoạt: Nghiên cứu đang tập trung vào việc phát triển các giải pháp 2FA có tính linh hoạt cao, cho phép người dùng sử dụng các phương thức xác thực khác nhau tùy theo ngữ cảnh sử dụng.

Ví dụ, hệ thống 2FA có thể cho phép người dùng chọn sử dụng mã OTP (One-Time Password), đăng nhập bằng vân tay hoặc khuôn mặt, hoặc sử dụng thiết bị thông minh để xác thực.

* Nghiên cứu về tính an toàn: Với sự gia tăng của các cuộc tấn công mạng và tình trạng đe dọa an ninh, các nghiên cứu liên quan đến tính an toàn của các phương pháp 2FA trên nền tảng điện toán đám mây đang được quan tâm.
* Phát triển các giải pháp 2FA phù hợp với nền tảng đám mây: Các giải pháp 2FA hiện nay thường được thiết kế dựa trên mô hình kiến trúc truyền thống và khó tích hợp với các nền tảng điện toán đám mây.
* Tích hợp các công nghệ mới:

- Sử dụng trí tuệ nhân tạo (AI): AI có thể được sử dụng để phát hiện các hành vi lạ trong hệ thống và cung cấp cơ chế xác thực bổ sung.

Ví dụ: nếu hệ thống phát hiện ra một người dùng đăng nhập từ một địa điểm mới, hệ thống sẽ yêu cầu người dùng nhập thêm thông tin xác thực để đảm bảo tính bảo mật.

- Sử dụng blockchain: Blockchain có thể được sử dụng để lưu trữ thông tin xác thực và tăng tính bảo mật.

Ví dụ: thông tin xác thực của người dùng có thể được lưu trữ trên blockchain và chỉ có thể được truy cập bằng cách sử dụng mã xác thực đặc biệt.

- Sử dụng các thiết bị IOT (Internet of Things): Các thiết bị IOT có thể được sử dụng để cung cấp các cơ chế xác thực bổ sung, như sử dụng các thiết bị đeo tay thông minh hoặc các thiết bị định vị để xác định vị trí của người dùng.

- Sử dụng phương pháp xác thực dựa trên âm thanh: Phương pháp xác thực dựa trên âm thanh có thể được sử dụng để đảm bảo tính bảo mật và tiện lợi.

Ví dụ: người dùng có thể sử dụng giọng nói của mình để xác thực và đăng nhập vào hệ thống.

* 1. Kết luận

Qua quá trình học tập môn Bảo mật mạng máy tính và hệ thống, thực hành trên đề tài “**Nghiên cứu và triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây**”. Đã giúp cho nhóm em có thêm kiến thức cũng như việc thực hành thực tế trong quá trình bảo mật tài khoản và dữ liệu. Việc triển khai xác thực hai nhân tố trên nền tảng điện toán đám mây được cho là mang lại nhiều lợi ích như tính bảo mật cao hơn cho người dùng, giúp ngăn chặn các cuộc tấn công mạng và giảm thiểu rủi ro cho doanh nghiệp.

DANH MỤC TÀI LIỆU THAM KHẢO

**Tài Liệu:**

Tiếng Việt:

1. AES eBook. Available at: https://link.springer.com/book/10.1007/978-3-662-60769-5 (Accessed: 2023).
2. Learning Firebase-cloud-messaging eBook. Available at: https://riptutorial.com/ebook/firebase-cloud-messaging (Accessed: 2023).
3. Learning Android eBook (chapter 100 - 104). Available at: https://riptutorial.com/ebook/android (Accessed: 2023).

[4] Phương Lan (2002), “Lập trình Windows với C# .NET” Lao động xã hội.

[5] Phạm Quang Huy (2008), “Lập trình hướng đối tượng” Đại Học Đà Lạt.

[6] Hoàng Vũ (2014),”Tài liệu hướng dẫn thực hành lập trình trên môi trường window”, Đại Học Quốc Gia TPHCM.

[7] Trung Thành (2019),”Giáo trình lập trình cơ bản” Đại Học Quốc Gia TPHCM.

[8] Văn Xuân (2013),”Viết chương trình trò chuyện đơn giản bằng C#” Đại học sư phạm Đà Nẵng.

[9] Thị Lan (2011), “Chuyển đổi giữa cơ sở dữ liệu quan hệ và XML” Đại Học Quốc Gia Hà Nội.

[10] Quý Hào (2012), “Nghiên cứu phối hợp hai phương pháp nén và mã hóa thông tin” Đại Học Quốc Gia Hà Nội.

Tiếng Anh:

[1] AES eBook. Available at: https://link.springer.com/book/10.1007/978-3-662-60769-5 (Accessed: 2023).

[2] Learning Firebase-cloud-messaging eBook. Available at: https://riptutorial.com/ebook/firebase-cloud-messaging (Accessed: 2023).

[3] Learning Android eBook (chapter 100 - 104). Available at: https://riptutorial.com/ebook/android (Accessed: 2023).

[4] Robert C. Martin (2010), “The Clean Coder: A Code of Conduct for Professional Programmers” Prentice Hall.

[5] Steve McConnell (2010), “Code Complete: A Practical Handbook of Software Construction” Microsoft Press.

[6] Erich Gamma (2009), “Design Patterns: Elements of Reusable Object-Oriented Software” Addison-Wesley Professional.

[7] David Thomas (2021) “The Pragmatic Programmer” Addison-Wesley Professional.

[8] Eric Freeman (2020), “A Brain-Friendly Guide” O’Reilly Media.

[9] Martin Fowler (2007), “Improving the Design of Existing Code” Addison-Wesley Professional.

[10] Donald E. Knuth (2008), “The Art of Computer Programming” Addison-Wesley Professional.