TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KÌ MÔN BẢO MẬT THÔNG TIN**

**­­**

**THOẢ THUẬN KHOÁ XÁC THỰC HAI YẾU TỐ TRONG MẠNG CẢM BIẾN KHÔNG DÂY TÍCH HỢP 5G**

*Người hướng dẫn*: **TS HUỲNH NGỌC TÚ**

*Người thực hiện*: **HỒNG QUANG VINH – 186005004**

**NGUYỄN ĐẠI THỊNH – 186005035**

**VÕ ĐĂNG KHOA – 186005032**

Lớp**: 18600531**

Khoá**: 2018-2020**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2019**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**ĐỒ ÁN CUỐI KÌ MÔN BẢO MẬT THÔNG TIN**

**THOẢ THUẬN KHOÁ XÁC THỰC HAI YẾU TỐ TRONG MẠNG CẢM BIẾN KHÔNG DÂY TÍCH HỢP 5G**

*Người hướng dẫn*: **TS HUỲNH NGỌC TÚ**

*Người thực hiện*: **HỒNG QUANG VINH – 186005004**

**NGUYỄN ĐẠI THỊNH – 186005035**

**VÕ ĐĂNG KHOA – 186005032**

Lớp**: 18600531**

Khoá**: 2018-2020**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2019**

LỜI CẢM ƠN

Nhóm chúng em xin chân thành cảm ơn Cô Huỳnh Ngọc Tú đã giúp đỡ chúng em hoàn thành đồ án. Những hướng dẫn của Cô giúp chúng em có một nền tảng lý thuyết đủ để có thể ứng dụng và nghiên cứu phát triển đề tài này. Xin chân thành cảm ơn Cô.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của TS Huỳnh Ngọc Tú;. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày tháng năm*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Hồng Quang Vinh*

*Nguyễn Đại Thịnh*

*Võ Đăng Khoa*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Việc tích hợp mạng 5G và mạng cảm biến không dây (WSN) là rất quan trọng trong kỷ nguyên mới của Internet vạn vật (IoT), cho một loạt các ứng dụng. Tuy nhiên, bất chấp những lợi thế tiềm năng của việc tích hợp này, có những lo ngại về các mối đe dọa an ninh không lường trước có thể ảnh hưởng đến cuộc sống hàng ngày của chúng ta.

Thỏa thuận khóa xác thực là một tính năng bảo mật thiết yếu để liên lạc an toàn giữa người dùng và thiết bị IoT và để bảo vệ các ứng dụng IoT khỏi các mối đe dọa bảo mật. Một lược đồ xác thực và thỏa thuận khóa dựa trên khái niệm IoT gần đây đã được đề xuất cho các WSN không đồng nhất, tuyên bố cung cấp ẩn danh cho người dùng và xác thực lẫn nhau, cũng như khả năng chống lại một số loại tấn công.

Bài viết này dựa trên bài báo về xác thực 2 yếu tố [1], sẽ chỉ ra một số điểm yếu về bảo mật của mô hình nói trên. Ngoài ra sẽ đề xuất một thiết kế kiến ​​trúc mạng phù hợp cho việc tích hợp mạng 5G và WSN. Dựa trên kiến ​​trúc mạng, sơ đồ đề xuất về xác thực hai yếu tố và thỏa thuận khóa trong các WSN tích hợp 5G cho IoT có thể chống lại các cuộc tấn công khác nhau, bao gồm cả các cuộc tấn công được xác định trước đó và có thể bảo vệ các yêu cầu bảo mật, bao gồm cả khả năng không liên kết.

Cuối cùng, bài viết đánh giá tính bảo mật và hiệu suất của chương trình đề xuất và so sánh sơ đồ này với các chương trình liên quan khác.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc11580852)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc11580853)

[TÓM TẮT iv](#_Toc11580854)

[MỤC LỤC 1](#_Toc11580855)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 3](#_Toc11580856)

[CHƯƠNG 1 – GIỚI THIỆU 4](#_Toc11580857)

[1.1 Thị trường chứng khoán 4](#_Toc11580858)

[1.2 Các phương pháp được đề xuất 5](#_Toc11580859)

[CHƯƠNG 2 – DỮ LIỆU NGHIÊN CỨU 8](#_Toc11580860)

[2.1 Dữ liệu thể hiện dạng liên tục - chuỗi thời gian thực 12](#_Toc11580861)

[2.2 Dữ liệu thể hiện dạng rời rạc - dữ liệu xác định xu hướng 12](#_Toc11580862)

[CHƯƠNG 3 – CÁC MÔ HÌNH DỰ ĐOÁN 15](#_Toc11580863)

[3.1 Mô hình Mạng nơ-ron nhân tạo (ANN) 15](#_Toc11580864)

[3.2 Mô hình Support Vector Machin (SVM) 16](#_Toc11580865)

[3.3 Mô hình Random Forest 17](#_Toc11580866)

[3.4 Mô hình Naive Bayes 19](#_Toc11580867)

[CHƯƠNG 4 – KẾT QUẢ THỰC NGHIỆM 20](#_Toc11580868)

[CHƯƠNG 5 – KẾT LUẬN 31](#_Toc11580869)

[5.1 Thảo luận 31](#_Toc11580870)

[5.2 Kết luận 32](#_Toc11580871)

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

**CÁC CHỮ VIẾT TẮT**

IoT: Internet of things

WSN: Mạng cảm biến không dây

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 1: Tỷ lệ phần trăm tăng giảm của cổ phiếu S&P 8](#_Toc11579767)

[Hình 2: Dữ liệu 10 năm được trích 10% từ tổng 9](#_Toc11579768)

[Hình 3: Dữ liệu 10 năm được trích 50% từ tổng 10](#_Toc11579769)

[Hình 4: Mười chỉ số kỹ thuật được sử dụng 11](#_Toc11579770)

[Hình 5: Mười chỉ số kỹ thuật và công thức tính 12](#_Toc11579771)

[Hình 6: Kiến trúc 3 lớp feedforward của mô hình ANN 15](#_Toc11579772)

[Hình 7: Các thiết lập tham số cho mô hình ANN 16](#_Toc11579773)

[Hình 8: Các thiết lập tham số cho mô hình SVM 17](#_Toc11579774)

[Hình 9: Thuật toán cho mô hình Random Forest 18](#_Toc11579775)

[Hình 10: Độ chính xác cho các kết hợp tham số tốt nhất của mô hình ANN 21](#_Toc11579776)

[Hình 11: Độ chính xác cho các kết hợp tham số tốt nhất của mô hình SVM 22](#_Toc11579777)

[Hình 12: Độ chính xác cho các kết hợp tham số tốt nhất của mô hình Random Forest 23](#_Toc11579778)

[Hình 13: Độ chính xác của từng mô hình 24](#_Toc11579779)

[Hình 14: Quá trình dự đoán với dữ liệu liên tục 25](#_Toc11579780)

[Hình 15: Quá trình dự đoán với dữ liệu rời rạc 26](#_Toc11579781)

[Hình 16: Kết quả kết hợp tham số đối với mô hình ANN 27](#_Toc11579782)

[Hình 17: Kết quả kết hợp tham số đối với mô hình SVM 28](#_Toc11579783)

[Hình 18: Kết quả kết hợp tham số đối với mô hình Random Forest 29](#_Toc11579784)

[Hình 19: Kết quả so sánh cho tất cả mô hình 30](#_Toc11579785)

CHƯƠNG 1 – GIỚI THIỆU

1.1 Internet of Things (IoT)

Internet of Things (IoT) là một công nghệ mới nổi kết nối nhiều loại thiết bị, bao gồm điện thoại thông minh, thiết bị gia dụng, cảm biến và các thiết bị mạng khác. Công nghệ mới này có thể được áp dụng trong nhiều lĩnh vực ứng dụng, chẳng hạn như nhà thông minh (ví dụ: bảo mật, sưởi ấm và kiểm soát ánh sáng), thành phố thông minh, chăm sóc sức khỏe (ví dụ: từ xa theo dõi bệnh nhân) và sản xuất thông minh (ví dụ: từ xa giám sát và kiểm soát hệ thống sản xuất).

Các mạng (5G) hiện đang được phát triển đang hướng tới mục tiêu cung cấp cao tốc độ (1 Gbps), công suất thấp và độ trễ thấp (1 ms trở xuống). Do đó công nghệ 5G sẽ đẩy nhanh việc triển khai nhiều Các ứng dụng IoT, đòi hỏi sự phổ biến hơn, tính di động cao hơn, hiệu suất và tốc độ tốt hơn, và thời gian đáp ứng nhanh hơn.

Mạng cảm biến không dây (WSN) bao gồm một số lượng lớn các nút cảm biến nhỏ, không bị hạn chế về tài nguyên, triển khai trong một lĩnh vực quan tâm để theo dõi và thu thập vật lý hoặc các điều kiện môi trường, chẳng hạn như ánh sáng, nhiệt độ, áp suất, chuyển động, âm thanh hoặc chất ô nhiễm. WSN đóng vai trò quan trọng vai trò trong IoT bằng cách hỗ trợ cảm biến và thu thập thông tin môi trường. Do đó, để cung cấp thành công IoT các ứng dụng, sự tích hợp của mạng 5G và WSN là cần thiết.

Tuy nhiên, bất chấp tiềm năng của sự tích hợp này, nó cũng phơi bày chúng ta hơn nữa đối với các mối đe dọa về bảo mật.

Do đó, bảo mật và quyền riêng tư là rất quan trọng để bảo vệ IoT các ứng dụng từ các cuộc tấn công như vậy. Hơn nữa, sự không đồng nhất của các mạng có thể có một ảnh hưởng đáng kể đến bảo mật các ứng dụng IoT, trong đó hạn chế về tài nguyên các nút cảm biến phải mở một giao tiếp an toàn với nhiều hơn thiết bị mạnh mẽ.

Ví dụ, trong một ngôi nhà thông minh, ngôi nhà các nút cảm biến giao tiếp với điện thoại thông minh người dùng. Dành cho liên lạc an toàn giữa bất kỳ bên nào và để cung cấp mức độ bảo mật tương đương để liên lạc giữa các thiết bị khác nhau, thuật toán mã hóa tối ưu là rất cần thiết.

Hơn nữa, các thiết bị IoT yêu cầu tốc độ cao và hiệu quả an ninh nhẹ. Trong IoT, chỉ những người dùng hợp pháp mới có thể truy cập các thiết bị IoT xác thực (nghĩa là, một cổng hoặc nút cảm biến) và một phiên xác thực nên được thiết lập giữa người dùng và thiết bị IoT để truyền dữ liệu an toàn. Do đó, xác thực lẫn nhau với thỏa thuận chính là một yêu cầu quan trọng đối với IoT. Bởi vì IoT mang dữ liệu có thể chứa thông tin riêng tư cá nhân (nghĩa là, danh tính và vị trí) và bất kỳ ai cũng có thể truy cập thiết bị khác của người dùng, bất kỳ rò rỉ thông tin có thể ảnh hưởng đến quyền riêng tư của người dùng.

Trong 5G WSN được phân cấp cho IoT, ẩn danh là một khía cạnh bảo mật quan trọng, bởi vì nó bảo vệ quyền riêng tư của cả người dùng và các thiết bị IoT như các nút cảm biến. Ẩn danh thông thường đề cập đến trạng thái trong đó một cá nhân cá nhân hoặc thông tin nhận dạng cá nhân không được biết công khai. Khả năng không liên kết của hai hoặc nhiều mục quan tâm, từ một quan điểm của kẻ tấn công, có nghĩa là trong hệ thống, Kẻ tấn công không thể xác định liệu các mục này có liên quan. Pfitzmann và Hansen chỉ ra rằng tính không liên kết là đủ điều kiện ẩn danh, nhưng không phải là điều kiện cần thiết. Tuy nhiên, để hoàn toàn ẩn danh, hầu hết người dùng đều muốn ẩn danh mạnh mẽ, đòi hỏi không liên kết. Vì vậy, để bảo vệ quyền riêng tư của người dùng, cả hai ẩn danh và không liên kết nên được xem xét.

1.2 Các phương pháp được đề xuất

Năm 2006, Wong và cộng sự. đề xuất một lược đồ xác thực người dùng nhẹ cho các WSN dựa trên XOR và hàm băm hoạt động. Tuy nhiên, vào năm 2009, Das đã cho thấy kế hoạch này không thể chịu được một cuộc tấn công xác minh bị đánh cắp và một cuộc tấn công nơi nhiều người dùng đã đăng nhập với cùng một ID và do đó, đề xuất một sơ đồ xác thực người dùng dựa trên hai yếu tố để giải quyết những vấn đề này. Trong sơ đồ của mình, một mật khẩu và thẻ thông minh (Smart card) được sử dụng như hai yếu tố để xác thực người dùng. Tuy nhiên, vào năm 2010, một số nhà nghiên cứu - đã chỉ ra các vấn đề bảo mật trong sơ đồ Das, và đề xuất cải tiến vượt qua. Sau đó, Das và cộng sự vào năm 2012 và Xue và cộng sự năm 2013 trình bày xác thực người dùng và khóa các lược đồ thỏa thuận cho các WSN dựa trên việc sử dụng thông minh thẻ.

Gần đây, vào năm 2014, Turkanovic và cộng sự đề xuất một người dùng kế hoạch và thỏa thuận chính cho không đồng nhất các WSN đặc biệt, dựa trên IoT. Đề án của họ là nhẹ vì nó chỉ sử dụng các thao tác đơn giản, chẳng hạn như Hàm XOR và hàm băm. Thông qua IoT, một người dùng ngẫu nhiên có thể kết nối trực tiếp với một nút cảm biến từ WSN và đàm phán khóa phiên với nó mà không kết nối với nút cổng. Thật không may, kế hoạch này sau đó đã được chứng minh là dễ bị tấn công bởi nhiều cuộc tấn công, bởi Chang, Farashet, Amin và Biswas và Tai

Năm 2016, Chang và cộng sự chỉ ra rằng Turkanovic và cộng sự lược đồ dễ bị tấn công mạo danh với nút chụp, một cuộc tấn công thẻ thông minh bị đánh cắp, giả mạo nút cảm biến tấn công và tấn công xác minh bị đánh cắp, cũng như không đảm bảo bí mật lạc hậu. Chang và cộng sự đề xuất một cách linh hoạt giao thức xác thực bằng thẻ thông minh cho các WSN hoạt động ở hai chế độ: sơ đồ xác thực nhẹ, như một sự cải tiến so với Turkanovic và cộng sự sơ đồ, và ắc một giao thức nâng cao dựa trên mật mã đường cong elliptic (ECC), cung cấp bí mật hoàn hảo về phía trước. Đồng thời, Farash và cộng sự xác định rằng lược đồ Turkanovic không thể chống lại một cuộc tấn công thẻ thông minh bị đánh cắp và một cuộc tấn công trung gian và nó không cung cấp, không thể kiểm soát và bí mật tiến / lùi. Dựa trên phân tích của họ, họ đã đề xuất một xác thực người dùng được cải thiện và lược đồ thỏa thuận chính cho các WSN không đồng nhất. Tuy nhiên, Amin và cộng sự thấy rằng chương trình Farash và cộng sự chịu được thông tin tạm thời cụ thể theo phiên tấn công, một cuộc tấn công đoán mật khẩu ngoại tuyến bằng cách sử dụng một đánh cắp tấn công thẻ thông minh, tấn công phát hành thẻ thông minh mới và tấn công mạo danh người dùng. Hơn nữa, nó không bảo tồn ẩn danh người dùng và bí mật của khóa bí mật của nút cổng. Amin và cộng sự. sau đó trình bày một giao thức trao đổi khóa xác thực ba yếu tố ẩn danh đối với WSN, trong đó mật khẩu, thẻ thông minh và sinh trắc học được sử dụng như ba yếu tố.

Năm 2016, Amin và Biswas đã chứng minh rằng mô hình của Turkanovic không ngăn chặn mật khẩu nhận dạng ngoại tuyến đoán tấn công, tấn công trộm thẻ thông minh, tấn công mạo danh người dùng và tấn công mạo danh nút cảm biến, cũng như cung cấp một giai đoạn xác thực không hiệu quả. Như một Giải pháp, họ đề xuất một sơ đồ nhẹ an toàn cho người dùng xác thực và thỏa thuận quan trọng trong đa cổng dựa WSN.

Gần đây nhất, năm 2017, Tai và cộng sự cũng cho thấy rằng Sơ đồ Turkanovic và cộng sự không đảm bảo tính ẩn danh của người dùng, và rằng một khóa phiên được thiết lập trong sơ đồ có thể là rò rỉ bằng cách sử dụng các nút cảm biến bị xâm nhập. Để khắc phục những lỗ hổng bảo mật, họ đề xuất cải tiến cho lược đồ Turkanovic. Họ tuyên bố rằng chương trình của họ đảm bảo người dùng ẩn danh và xác thực lẫn nhau giữa tất cả các bên. Tuy nhiên, bài báo đã phát hiện ra rằng chương trình Tai và cộng sự cung cấp xác thực lẫn nhau và ẩn danh nút cảm biến và hơn nữa, nó dễ bị nút cảm biến tấn công giả mạo với việc bắt nút cảm biến, tấn công đặc quyền và thông tin tạm thời theo phiên cụ thể tấn công. Bài báo cũng tìm thấy những điểm yếu bảo mật bổ sung trong lược đồ, cụ thể là, dễ bị đánh cắp thẻ thông minh và các cuộc tấn công đoán mật khẩu ngoại tuyến và không đảm bảo ẩn danh người dùng.

1.3 Đóng góp của bài báo

Như thể hiện trong phần về các công việc liên quan, các nghiên cứu hiện có về xác thực người dùng và thỏa thuận chính cho WSN không đáp ứng các tính năng bảo mật mong muốn. Đặc biệt, hầu hết đề án đề xuất không cung cấp ẩn danh mạnh mẽ, được đề cập để không liên kết. Ngoài ra, họ tập trung chủ yếu vào các WSN, có nghĩa là kiến trúc mạng của họ không phù hợp với Các WSN tích hợp 5G cho IoT.

Bài báo phân tích bảo mật của Tai gần đây nhất xác thực người dùng và lược đồ thỏa thuận chính cho các WSN không đồng nhất về quảng cáo không đồng nhất. Cho thấy rằng sơ đồ của họ dễ bị tấn công bao gồm đánh cắp thẻ thông minh, đoán mật khẩu ngoại tuyến, cảm biến giả mạo nút, đặc quyền nội bộ và phiên cụ thể tấn công thông tin tạm thời. Họ cũng cho thấy rằng lược đồ của Tai không bảo tồn nút người dùng và cảm biến ẩn danh, xác thực lẫn nhau và bí mật của khóa bí mật của nút cổng.

Bài báo thiết kế kiến trúc mạng phù hợp với các WSN 5Gintegrated cho IoT. Theo mạng kiến trúc mới, họ đề xuất một xác thực hai yếu tố an toàn và sơ đồ thỏa thuận chính khắc phục điểm yếu bảo mật nói trên và bảo tồn tất cảc ác tính năng bảo mật của chương trình của Tai. Hơn thế nữa, kế hoạch đề xuất của họ chịu được tất cả các cuộc tấn công đã biết và đảm bảo tính không liên kết và do đó, ẩn danh mạnh mẽ.

Sử dụng đánh giá bảo mật, họ cho thấy rằng đề xuất của có thể chống lại nhiều cuộc tấn công, bao gồm cả những cuộc tấn công sẽ thỏa hiệp chương trình Tai. Ngoài ra, họ so sánh các tính năng bảo mật của chương trình đề xuất của họ với những đề án liên quan khác.

Thông qua đánh giá hiệu suất, họ so sánh thực hiện kế hoạch đề xuất của họ với các liên quan khác đề án về chi phí tính toán, chi phí truyền thông và chi phí lưu trữ.

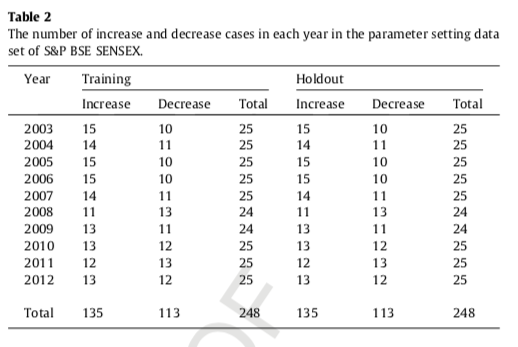
CHƯƠNG 2 – ĐÁNH GIÁ SƠ ĐỒ CỦA TAI

Sơ đồ của Tai bao gồm 6 giai đoạn: Tiền triển khai, đăng ký, đăng nhập, xác thực, thay đổi mật khẩu và thêm node động. Giai đoạn đăng ký được chia thành 2 giai đoạn phụ: Đăng ký người dùng và đăng ký node cảm biến. Các ký hiệu trong sơ đồ như bảng dưới:

Hình 1: Tỷ lệ phần trăm tăng giảm của cổ phiếu S&P

Nghiên cứu này sử dụng 20% toàn bộ dữ liệu làm dữ liệu lựa chọn tham số. Dữ liệu này được sử dụng để xác định các tham số thiết kế của các mô hình dự đoán. Tập dữ liệu lựa chọn tham số được xây dựng bằng cách lấy tỷ lệ dữ liệu bằng nhau từ mỗi mười năm. Tỷ lệ phần trăm tăng giảm trong mỗi năm cũng được duy trì. Phương pháp lấy mẫu này cho phép tập dữ liệu cài đặt tham số trở thành đại diện tốt hơn cho toàn bộ tập dữ liệu.

Dữ liệu lựa chọn tham số này được chia thành tập training và holdout. Mỗi bộ bao gồm 10% toàn bộ dữ liệu. Hình 2 mô tả số lượng các trường hợp tăng và giảm cho tập dữ liệu lựa chọn tham số. Những thống kê này dành cho S & P BSE Sensex. Phân tích dữ liệu tương tự được thực hiện cho CNX Nifty, Reliance Industries và Infosys Ltd.



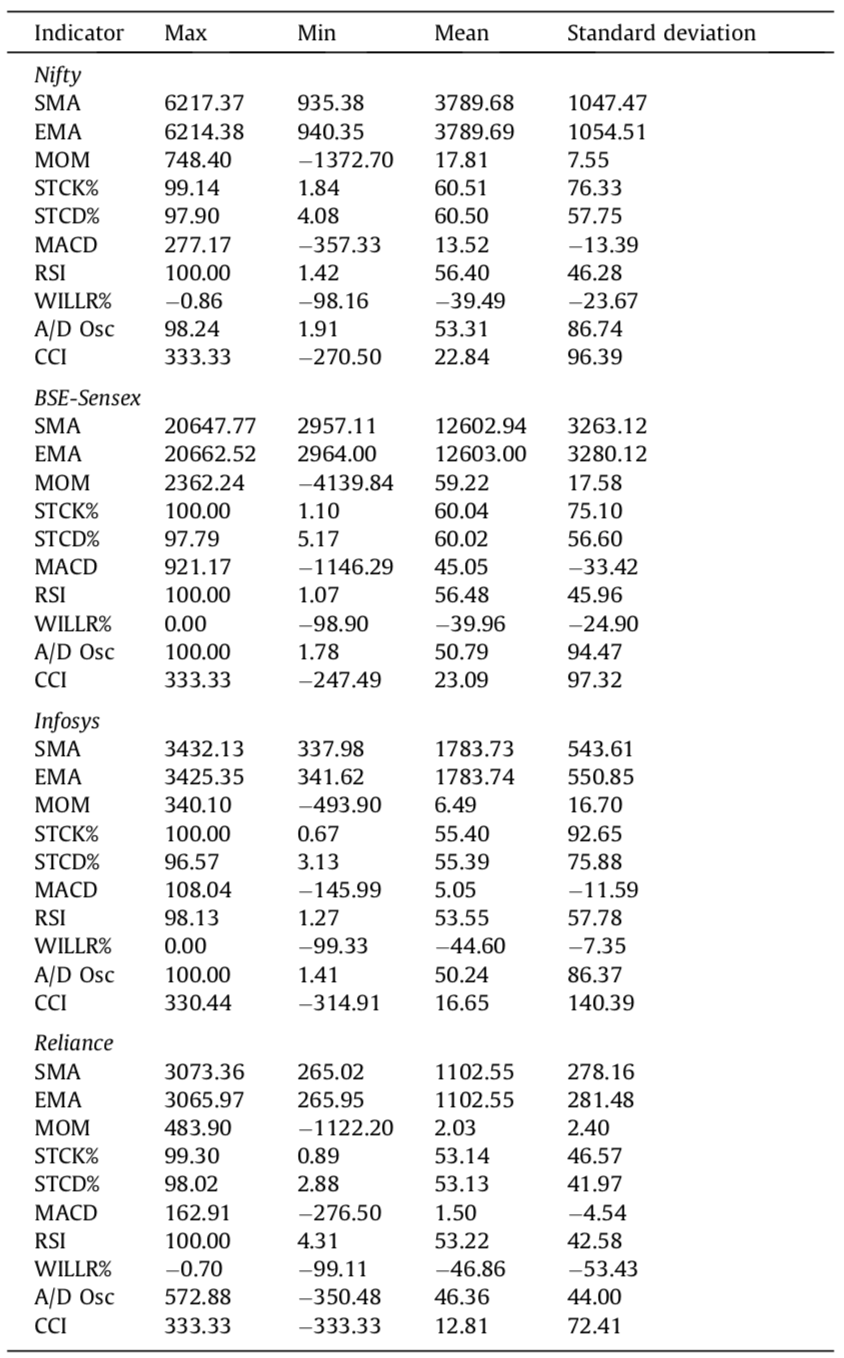
Hình 2: Dữ liệu 10 năm được trích 10% từ tổng

Các tham số tối ưu cho các mô hình dự đoán thu được bằng các thí nghiệm trên dữ liệu lựa chọn tham số. Sau đó, để so sánh ANN, SVM, Random forest và Naive-Bayes, bộ dữ liệu so sánh được đưa ra. Bộ dữ liệu này bao gồm toàn bộ mười năm dữ liệu. Nó cũng được chia trong đào tạo (50% toàn bộ dữ liệu) và giữ (50% toàn bộ dữ liệu) như bảng. Chi tiết về bộ dữ liệu này của S & P BSE SENSEX được hiển thị trong Hình 3.



Hình 3: Dữ liệu 10 năm được trích 50% từ tổng

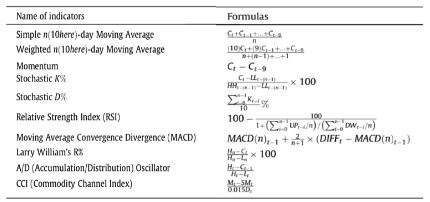
Có một số chỉ số kỹ thuật thông qua đó người ta có thể dự đoán sự chuyển động của cổ phiếu trong tương lai. Ở đây trong nghiên cứu này, tổng cộng mười chỉ số kỹ thuật được sử dụng trong Kara và cộng sự (2011) được sử dụng. Các chỉ số này được thể hiện trong Hình 4 cho thấy số liệu thống kê tóm tắt cho các chỉ số được chọn của hai chỉ số và hai cổ phiếu. Hai cách tiếp cận để biểu diễn dữ liệu đầu vào được sử dụng trong nghiên cứu này. Cách tiếp cận đầu tiên sử dụng biểu diễn giá trị liên tục, tức là chuỗi thời gian thực tế trong khi cách thứ hai sử dụng biểu diễn xác định xu hướng (có tính chất rời rạc) cho các đầu vào.



Hình 4: Mười chỉ số kỹ thuật được sử dụng

2.1 Dữ liệu thể hiện dạng liên tục - chuỗi thời gian thực

Mười chỉ số kỹ thuật được tính toán dựa trên công thức như được thảo luận trong Hình 5 được đưa ra làm đầu vào cho các mô hình dự đoán. Rõ ràng là mỗi chỉ số kỹ thuật được tính toán dựa trên công thức đã đề cập ở trên có giá trị liên tục. Các giá trị của tất cả các chỉ báo kỹ thuật được chuẩn hóa trong phạm vi giữa [-1, +1], để giá trị lớn hơn của một input params không áp đảo chỉ báo có giá trị nhỏ hơn. Hiệu suất của tất cả các mô hình đang nghiên cứu được đánh giá cho đại diện đầu vào này.



Hình 5: Mười chỉ số kỹ thuật và công thức tính

2.2 Dữ liệu thể hiện dạng rời rạc - dữ liệu xác định xu hướng

Một lớp quyết định mới được sử dụng để chuyển đổi các tham số kỹ thuật có giá trị liên tục thành giá trị rời rạc, đại diện cho xu hướng cổ phiếu. Lớp này được gọi là ‘‘Lớp chuyển đổi dữ liệu xác định xu hướng”. Công việc của lớp mới này là chuyển đổi các giá trị liên tục này thành +1 hoặc -1 bằng cách xem xét thuộc tính này trong quá trình rời rạc. Bằng cách này, dữ liệu đầu vào của từng mô hình dự đoán được chuyển đổi thành +1 hoặc -1, trong đó +1 là chuyển động đi lên và -1 hiển thị chuyển động xuống. Chi tiết về từng chỉ số kỹ thuật được nêu ra dưới đây.

Đường trung bình động (MA) là công cụ phân tích kỹ thuật đơn giản giúp làm mịn dữ liệu giá bằng cách tạo ra giá trung bình được cập nhật liên tục. Trong bài báo này, 10 ngày trung bình động đơn giản (SMA) và trung bình động có trọng số (WMA) được sử dụng vì dự đoán tương lai ngắn hạn. Theo nguyên tắc chung, nếu giá cao hơn mức trung bình động thì xu hướng tăng. Nếu giá dưới mức trung bình động, xu hướng giảm. Vì vậy, bài viết đã rút ra ý kiến của cả hai chỉ số SMA và WMA cho mỗi ngày từ giá trị của SMA và WMA so với giá hiện tại. Nếu giá hiện tại cao hơn các giá trị trung bình di động thì xu hướng sẽ tăng lên và được biểu thị là +1, và nếu giá hiện tại nằm dưới các giá trị trung bình di chuyển thì xu hướng đó sẽ giảm xuống và được biểu thị dưới dạng -1.

STCK%, STCD% và Williams R% là các dao động ngẫu nhiên. Những dao động là chỉ số xu hướng rõ ràng cho bất kỳ cổ phiếu. Khi các dao động ngẫu nhiên đang tăng lên, giá cổ phiếu có thể sẽ tăng lên và tiếp tục. Vì vậy nếu giá trị của các bộ dao động ngẫu nhiên tại thời điểm ‘t’ lớn hơn giá trị tại thời điểm ‘t - 1’ thì ý kiến về xu hướng là lên và được biểu thị dưới dạng +1 và ngược lại.

MACD đi theo xu hướng của cổ phiếu, tức là nếu MACD tăng thì giá cổ phiếu cũng tăng và ngược lại. Vì vậy, nếu giá trị của MACD tại thời điểm ‘t’ lớn hơn giá trị tại thời điểm ‘t-1’, xu hướng về cổ phiếu sẽ là ‘tăng’ và được biểu thị là +1 và ngược lại.

RSI thường được sử dụng để xác định các điểm mua quá mức và bán quá mức. Nó nằm trong khoảng từ 0 đến 100. Nếu giá trị của RSI vượt quá 70, điều đó có nghĩa là cổ phiếu bị mua quá mức, do đó, nó có thể giảm trong tương lai gần (biểu thị -1) và nếu giá trị của RSI giảm xuống dưới 30 mức độ, điều đó có nghĩa là cổ phiếu bị bán quá mức, vì vậy, nó có thể sẽ tăng trong tương lai gần (biểu thị ý kiến +1). Đối với các giá trị nằm trong khoảng (30, 70), nếu RSI tại thời điểm ‘t’ lớn hơn RSI tại thời điểm ‘t-1’, thì xu hướng được biểu thị là +1 và ngược lại.

CCI đo lường sự khác biệt giữa thay đổi giá cổ phiếu và thay đổi giá trung bình. Chỉ số tích cực cao cho thấy giá cao hơn mức trung bình, đó là một sự thể hiện sức mạnh. Chỉ số tiêu cực thấp cho thấy giá thấp hơn mức trung bình của họ, đây là một biểu hiện của sự yếu kém. CCI cũng được sử dụng để xác định mức mua quá mức và bán quá mức. Trong bài báo này, họ đã đặt 200 là mức mua quá mức và -200 là mức bán quá mức vì 200 là đại diện cho một thái cực thực sự. Điều này có nghĩa là nếu giá trị CCI vượt quá 200 cấp, xu hướng là -1 và nếu dưới mức 200 thì ý kiến cho xu hướng là +1. Đối với các giá trị trong khoảng (-200, 200), nếu CCI tại thời điểm ‘t’ lớn hơn CCI tại thời điểm t-1, thì ý kiến về xu hướng là +1 và ngược lại.

Bộ tạo dao động A/D cũng tuân theo xu hướng chứng khoán có nghĩa là nếu giá trị của nó tại thời điểm ‘t’ lớn hơn giá trị tại thời điểm ‘t - 1’, thì xu hướng là +1 và ngược lại.

Momentum đo tốc độ tăng giảm của giá cổ phiếu. Giá trị dương của biểu thị xu hướng tăng và được biểu thị bằng +1 trong khi giá trị âm biểu thị xu hướng giảm và được thể hiện dưới dạng -1.

Dữ liệu xác định xu hướng được chuẩn bị bằng cách khai thác thực tế rằng mỗi chỉ số kỹ thuật đều thể hiện biến động về giá cổ phiếu. Khi các dữ liệu này được cung cấp làm đầu vào trái ngược với dữ liệu thực tế, thông tin xu hướng được nhập vào dựa trên từng chỉ số kỹ thuật riêng lẻ. Các mô hình dự đoán cần phải xác định mối tương quan giữa xu hướng đầu vào và xu hướng đầu ra.

CHƯƠNG 3 – CÁC MÔ HÌNH DỰ ĐOÁN

3.1 Mô hình Mạng nơ-ron nhân tạo (ANN)

Là một mạng lưới dày đặc các nơ-ron liên kết với nhau được kích hoạt dựa trên các đầu vào. Một mạng nơ-ron 3 lớp feed-forward được sử dụng trong nghiên cứu. Đầu vào cho mạng là 10 chỉ số kỹ thuật được biểu thị bằng 10 nơ-ron trong lớp đầu vào. Lớp đầu ra có một nơ-ron duy nhất ứng với log sigmoid như là hàm chuyển. Điều này dẫn đến đầu ra giá trị liên tục trong khoảng từ 0 - 1. Ngưỡng 0,5 được sử dụng để xác định dự đoán chuyển động lên hoặc xuống. Lớn hơn 0,5 dự đoán là chuyển động tăng, ngược lại là giảm. Mỗi tầng nơ-ron ẩn sử dụng tan sigmoid như là hàm chuyển.



Hình 6: Kiến trúc 3 lớp feedforward của mô hình ANN

Kiến trúc 3 lớp feed-forward ANN được minh hoạ ở hình trên. Độ dốc giảm với động lượng được sử dụng để điều chỉnh các trọng số, trong đó tại mỗi thời kỳ, trọng số được điều chỉnh sao cho có thể đạt mức tối thiểu toàn cục. Các thử nghiệm thiết lập tham số toàn diện để xác định tham số cho từng cổ phiếu và chỉ số giá cổ phiếu.

Các tham số cho mô hình ANN bao gồm: Số tầng nơ-ron ẩn (n), giá trị của tỉ lệ huấn luyện (lr), hằng số động lượng (mc), và số thời kỳ (ep). Để xác định chúng một cách hiệu quả, 10 mức (n), 9 mức (mc), 10 mức (ep) được kiểm tra trong các thử nghiệm thiết lập tham số. Ban đầu, giá trị (lr) được cố định là 0,1. Các tham số này được thể hiện trong bảng dưới đây.



Hình 7: Các thiết lập tham số cho mô hình ANN

Các thiết lập tham số mang lại tổng cộng 10x10x9 = 900 phương pháp ANN cho một cổ phiếu. Xét 2 cổ phiếu và 2 chỉ số giá cổ phiếu, tổng số 3600 phương pháp được thực hiện.

Ba cách kết hợp tham số hàng đầu được chọn là 3 mô hình ANN hàng đầu cho các thử nghiệm so sánh trên tập dữ liệu. Đối với mô hình này, tỉ lệ huấn luyện (lr) được thay đổi trong khoảng [0,1 - 0,9].

3.2 Mô hình Support Vector Machin (SVM)

Lần đầu tiên được giới thiệu bởi Vapnik (1999). Có 2 loại chính là Support Vector Classification (SVC) và Support Vector Regression (SVR). SVM là hệ thống học sử dụng không gian đặc trưng có số chiều lớn. Trong SVM, các điểm được phân loại bằng các gán chúng vào hai nửa không gian khác nhau trong không gian mẫu hoặc ánh xạ sang không gian có số chiều lớn hơn.

Mục tiêu của SVM là xác định siêu phẳng có biên tối đa. Ý tưởng là khoảng cách từ siêu phẳng này tới các điểm positive và negative là bằng nhau và lớn nhất. Sự đánh đổi giữa khoảng cách và lỗi phân loại được kiểm soát bởi tham số chính quy (c). Các hàm nhân đa thức và cơ sở được sử dụng. Trong đó (d) là độ của hàm đa thức, (γ) là hằng số của hàm cơ sở.

Lựa chọn hàm kernel, mức độ (d) trong trường hợp kernel đa thức, gamma trong hàm kernel (γ) trong trường hợp kernel là hàm cơ sở và hằng số chính quy (c) là các tham số cho SVM.

Để xác định chúng một cách hiệu quả, 4 mức (d), 10 mức (γ) và 4 - 5 mức (c) được thử nghiệm trong các thử nghiệm thiết lập tham số. Các tham số được tóm tắt trong bảng dưới.



Hình 8: Các thiết lập tham số cho mô hình SVM

Với một cổ phiếu, các thiết lập tham số này mang lại tổng cộng 20 và 40 phương pháp cho SVM sử dụng các hàm nhân cơ sở đa thức và hướng tâm tương ứng. Xem xét 2 cổ phiếu và 2 chỉ số giá cổ phiếu, tổng số 240 phương pháp cho SVM được thực hiện. Một kết hợp tham số cho mỗi SVM kernel đa thức và SVM kernel cơ sở xuyên tâm dẫn đến hiệu suất đào tạo và tổ chức trung bình tốt nhất được chọn làm hai mô hình SVM hàng đầu cho các thử nghiệm so sánh.

3.3 Mô hình Random Forest

Cây quyết định là một trong những kỹ thuật phổ biến nhất để phân loại. Độ chính xác tương đương với các phương pháp phân loại khác, và nó rất hiệu quả. Mô hình học được thông qua kỹ thuật này được biểu diễn dưới dạng cây và được gọi là cây quyết định.

Random forest thuộc về loại thuật toán học. Nó sử dụng cây quyết định làm cơ sở cho việc học. Ý tưởng của việc học là một bộ phân loại duy nhất không đủ để xác định lớp dữ liệu kiểm tra. Lý do là, dựa trên dữ liệu mẫu, bộ phân loại không thể phân biệt giữa nhiễu và mẫu. Vì vậy, nó thực hiện lấy mẫu với sự thay thế sao cho (n) cây được học dựa trên các mẫu tập dữ liệu này. Cũng trong các thí nghiệm, mỗi cây được học bằng 3 đặc trưng được chọn ngẫu nhiên. Điều này cũng tránh được vấn đề về quá khớp dữ liệu. Việc thực hiện thuật toán Random Forest được tóm tắt như dưới đây.



Hình 9: Thuật toán cho mô hình Random Forest

Số lượng cây trong toàn bộ (n) cây được coi là tham số của Random Forest. Để xác định nó một cách hiệu quả, nó được thay đổi từ 10 đến 200 với mức tăng 10 mỗi lần trong các thử nghiệm thiết lập tham số. Đối với một cổ phiếu, các cài đặt tham số này mang lại tổng cộng 20 phương pháp. Xem xét 2 cổ phiếu và 2 chỉ số giá cổ phiếu, tổng số 80 phương pháp điều trị được thực hiện. Ba cách kết hợp tham số là ba mô hình Random Forest hàng đầu cho các thử nghiệm so sánh.

* 1. Mô hình Naive Bayes

Phân loại Naive Bayes giả định lớp độc lập có điều kiện. Phân loại Bayes dự đoán xác suất dữ liệu thuộc về một lớp cụ thể. Để dự đoán xác suất, nó sử dụng khái niệm định lý Bayes. Định lý Bayes, hữu ích ở chỗ nó cung cấp cách tính xác suất, cụ thể qua thông thức bên dưới.



Trong đó P là xác suất gỉả thuyết C đúng với sự kiện X đã xảy ra. Trong trường hợp giả thuyết C là xác suất thuộc về lớp “tăng” = “giảm” và sự kiện X là dữ liệu thử nghiệm. P(X|C) là một xác suất có điều kiện xảy ra sự kiện X với giả thuyết C là đúng. Nó có thể được ước tính từ dữ liệu đào tạo.

Các bộ phân loại Bayes cũng đóng vai trò là lý thuyết cho các phân lớp khác không sử dụng rõ ràng định lý Bayes. Ví dụ, theo các giả định cụ thể, có thể chứng minh rằng nhiều mạng thần kinh và thuật toán khớp đường cong đưa ra giả thuyết posteriori tối đa, giống như phân lớp Naive-Bayes.

CHƯƠNG 4 – KẾT QUẢ THỰC NGHIỆM

Độ chính xác và độ đo F được sử dụng để đánh giá hiệu suất của các mô hình được đề xuất. Việc tính toán các biện pháp đánh giá này đòi hỏi phải ước tính Độ rõ ràng (Precision) và Thu hồi (Recall) được đánh giá từ True Positive (TP), False Positive (FP), True Negative (TN) và False Negative (FN). Các tham số này được xác định trong các phương trình dưới đây.

Trong đó, Precision là trung bình có trọng số của độ chính xác positive và negative trong khi Recall là trung bình có trọng số của thu hồi positive và negative. Độ chính xác và độ đo F được tính bằng các phương trình.

Giai đoạn thử nghiệm đầu tiên coi đầu vào là dữ liệu có giá trị liên tục. Các kết hợp tham số tốt nhất được xác định bằng các thử nghiệm trên tập dữ liệu cài đặt tham số cho từng mô hình dự đoán. Các kết hợp tham số này với Độ chính xác và Độ đo F đáp ứng trong các thử nghiệm cài đặt tham số được báo cáo trong bảng dưới.

A screenshot of text

Description automatically generated

Hình 10: Độ chính xác cho các kết hợp tham số tốt nhất của mô hình ANN

A screenshot of a cell phone

Description automatically generated

Hình 11: Độ chính xác cho các kết hợp tham số tốt nhất của mô hình SVM

A screenshot of a cell phone

Description automatically generated

Hình 12: Độ chính xác cho các kết hợp tham số tốt nhất của mô hình Random Forest

Mục đích của các thử nghiệm trên tập dữ liệu so sánh là để hoàn thành hiệu suất dự đoán của các mô hình này cho các kết hợp tương đương tốt nhất được báo cáo trong các thử nghiệm cài đặt tham số. Trong thí nghiệm so sánh này, mỗi mô hình dự đoán được học dựa trên các tham số tốt nhất được báo cáo bởi các thử nghiệm cài đặt tham số.

A screenshot of a cell phone

Description automatically generated

Hình 13: Độ chính xác của từng mô hình

Bảng trên báo cáo độ chính xác trung bình và số đo F của từng mô hình trong quá trình thử nghiệm so sánh. Độ chính xác trung bình và số đo F được báo cáo trung bình trên các mô hình hoạt động hàng đầu. Có thể thấy rằng Naive-Bayes với quy trình Gaussian là ít chính xác nhất trong khi Random forest là chính xác nhất với độ chính xác trung bình gần 84%. Hình dưới mô tả quá trình dự đoán khi dữ liệu được định giá liên tục.



Hình 14: Quá trình dự đoán với dữ liệu liên tục

Giai đoạn thử nghiệm thứ hai giống hệt với giai đoạn đầu tiên ngoại trừ đầu vào của các mô hình là dữ liệu xác định xu hướng. Ý tưởng được mô tả trong hình dưới đây.



Hình 15: Quá trình dự đoán với dữ liệu rời rạc

Bảng dưới cho thấy các kết quả của các kết hợp hình thành tốt nhất cho ANN, SVM và Random forest tương ứng trong các thí nghiệm cài đặt tham số.



Hình 16: Kết quả kết hợp tham số đối với mô hình ANN

A screenshot of a cell phone

Description automatically generated

Hình 17: Kết quả kết hợp tham số đối với mô hình SVM

A screenshot of a cell phone

Description automatically generated

Hình 18: Kết quả kết hợp tham số đối với mô hình Random Forest

Cần lưu ý rằng khi dữ liệu được biểu diễn dưới dạng dữ liệu xác định xu hướng, phân lớp Naive-Bayes được học bằng cách phù hợp với phân phối đa biến Bernoulli cho dữ liệu. Kết quả về tập dữ liệu so sánh cho tất cả các mô hình được đề xuất được báo cáo trong Bảng dưới đây.



Hình 19: Kết quả so sánh cho tất cả mô hình

So sánh cuối cùng cho thấy tất cả các mô hình hoạt động tốt với dữ liệu đầu vào riêng biệt nhưng SVM, Random forest và Naive-Bayes hoạt động tốt hơn ANN. Độ chính xác của 3 mô hình trên là gần 90%.

CHƯƠNG 5 – KẾT LUẬN

Trong bài báo, họ đã xem xét sơ đồ của Tai và chứng minh rằng nó dễ bị tấn công bằng thẻ thông minh bị đánh cắp, tấn công đoán mật khẩu ngoại tuyến, tấn công giả mạo nút cảm biến, tấn công từ nội bộ và tấn công thông tin tạm thời theo phiên cụ thể.

Họ tiếp tục chỉ ra rằng lược đồ của Tai không bảo vệ ẩn danh nút người dùng và cảm biến, xác thực lẫn nhau và bí mật của khóa bí mật của nút cổng.. Dựa vào cái này kiến trúc mạng, họ đã đề xuất một yếu tố an toàn hai yếu tố xác thực và chương trình thỏa thuận quan trọng với khả năng không liên kết. Họ đã đánh giá tính bảo mật của chương trình đề xuất và so sánh nó với các đề án liên quan khác. Kết quả cho thấy kế hoạch đề xuất là an toàn chống lại nhiều người biết các cuộc tấn công và nó đáp ứng tất cả các tính năng bảo mật, bao gồm không liên kết, cần thiết để xác thực người dùng an toàn và thỏa thuận chính.

Họ cũng đã đánh giá hiệu suất của đề án đề xuất về chi phí tính toán, chi phí truyền thông và chi phí lưu trữ, sau đó họ so sánh với những đề án khác có liên quan. Các kết quả đánh giá về bảo mật và hiệu suất cho thấy chương trình của họ cung cấp tốt hơn an toàn mà không có hiệu suất khác biệt đáng kể so với khác đề án, và kết quả thực hiện được dự kiến sẽ cải thiện bởi vì cổng hoạt động tốt hơn nút cảm biến trong Các WSN tích hợp 5G cho IoT.

Trong công việc tương lai, họ sẽ đo lường hiệu suất của lược đồ được đề xuất bằng cách triển khai và thực hiện các thử nghiệm sử dụng các thiết bị thực tế trên các WSN tích hợp 5G cho IoT (ví dụ: điện thoại thông minh và thiết bị cảm biến) và, sẽ cải thiện đề án dựa trên kết quả thí nghiệm.

TÀI LIỆU THAM KHẢO

**Tiếng Anh**

[1] Two-Factor Authenticated Key Agreement Supporting Unlinkability in 5G-Integrated Wireless Sensor Networks, SOOYEON SHIN (Member, IEEE) and TAEKYOUNG KWON (Member, IEEE), Yonsei University, Seoul, 03722, South Korea