FPT UNIVERSITY

BỘ GIÁO DỤC VÀ ĐÀO TẠO

Đại học FPT

Tài liệu Dự án Tốt nghiệp

Phát triển hệ thống tự động giám sát tuân thủ chính sách bảo mật hồ sơ bệnh án điện tử (EHR) tại các cơ sở y tế quy mô nhỏ và vừa.

Thành viên nhóm	**Tên học sinh**	**Thẻ sinh viên**
	Trần Gia Quý	DA170010
	Nguyễn Khánh Toàn	DE170585
	Nguyễn Xuân Hoàng	DE170316
	Nguyễn Khánh Linh	DE170403
	Nguyễn Hữu Khôi	DE170017
Người giám sát	**Tên người hướng dẫn** Nguyễn Văn Điền Phạm Hồ Trọng Nguyên	
Mã dự án tốt nghiệp	IAP491	

- Hà Nội, tháng 9/2025 -

TÓM TẮT

Bối cảnh: Hồ sơ sức khỏe điện tử (EHR) đang nhanh chóng trở nên phổ biến tại các cơ sở y tế vừa và nhỏ ở Việt Nam. Điều này là do các chương trình y tế số quốc gia và các quy định chặt chẽ hơn về bảo vệ dữ liệu cá nhân. Tuy nhiên, các cơ sở này gặp khó khăn trong việc chứng minh họ tuân thủ các quy tắc bảo mật vì thiếu nguồn lực công nghệ, hệ thống phân quyền bị lỗi và không có hệ thống giám sát tự động. Các phương pháp hiện tại phụ thuộc quá nhiều vào kiểm toán thủ công và điều tra phản ứng, không đủ để chứng minh rằng mọi truy cập vào dữ liệu sức khỏe nhạy cảm đều hợp pháp, cần thiết, đúng mục đích và có thể kiểm toán được.

Phương pháp: Nghiên cứu này tạo ra một kiến trúc kết hợp kiểm soát danh tính và truy cập, quy trình làm việc của hồ sơ bệnh án điện tử và giám sát tuân thủ tự động. Keycloak được sử dụng để xác thực tập trung, NGINX được sử dụng làm điểm thực thi chính sách yêu cầu Open Policy Agent đưa ra quyết định ủy quyền theo thời gian thực, FastAPI được sử dụng làm cốt lõi của EHR để quản lý dữ liệu lâm sàng, và hệ thống quản lý thông tin và sự kiện bảo mật (SIEM) tự động kiểm tra nhật ký dựa trên các quy tắc tuân thủ theo yêu cầu pháp lý của Việt Nam. Phương pháp đánh giá sử dụng mô phỏng "Đội Đỏ đấu với Đội Xanh" để kiểm tra hệ thống chống lại ba kịch bản tấn công quan trọng: Xác thực vét cạn, Tấn công SQL Injection và Xóa dấu vết pháp y (Làm giả nhật ký).

Kết quả: Hệ thống đã có thể ngăn chặn các cuộc tấn công Brute-Force và SQL Injection ở lớp Nhận dạng và lớp Cổng, tương ứng. Trong kịch bản Giả mạo nhật ký, cơ chế toàn vẹn chuỗi băm của hệ thống đã phát hiện ra rằng ai đó đã xóa nhật ký kiểm toán mà không được phép, điều này đã kích hoạt cảnh báo nghiêm trọng. Những kết quả này cho thấy rằng kiến trúc phòng thủ nhiều lớp có thể thực thi hiệu quả việc tuân thủ và duy trì tính toàn vẹn bằng chứng mà không cần sử dụng phát hiện bất thường thống kê ẩn.

Kết luận: Hệ thống đề xuất đã chuyển đổi hiệu quả các yêu cầu quy định của Việt Nam thành các biện pháp kiểm soát kỹ thuật có thể thực hiện được và cung cấp khả năng giám sát tuân thủ tự động, có thể kiểm toán, được thiết kế riêng cho các cơ sở chăm sóc sức khỏe có nguồn lực hạn chế. Kiến trúc hệ thống cho thấy các nhà cung cấp dịch vụ y tế quy mô nhỏ và vừa hoàn toàn có thể thực hiện điều này trong khi vẫn đảm bảo an toàn cho bệnh nhân và năng suất lâm sàng ở mức cao. Trong tương lai, cần tập trung vào việc mở rộng phạm vi bao phủ quy định, đơn giản hóa việc phát hiện các mô hình vi phạm phức tạp và đáp ứng các tiêu chí tuân thủ ở nhiều khu vực pháp lý khác nhau để triển khai quốc tế.

Từ khóa: Hồ sơ sức khỏe điện tử, Giám sát tuân thủ, Chính sách bảo mật, Cơ sở y tế, Kiểm toán tự động, Thực thi chính sách, Kiểm soát truy cập.

LỜI CẢM ƠN

Lời đầu tiên, nhóm thực hiện đề tài xin gửi lời tri ân sâu sắc nhất đến hai giảng viên hướng dẫn: **Thầy Nguyễn Văn Điền** và **Thầy Phạm Hồ Trọng Nguyên**.

Mặc dù đề tài đi sâu vào lĩnh vực y tế số với nhiều quy trình nghiệp vụ đặc thù và mới mẻ, nhưng chính sự định hướng sắc bén về tư duy nghiên cứu cùng những kinh nghiệm quý báu của các thầy trong lĩnh vực Công nghệ và An toàn thông tin đã chỉ ra hướng đi chính xác để giúp chúng em không hiểu sai vấn đề. Từ những ngày đầu loay hoay xác định bài toán cho đến khi hoàn thiện hệ thống, các thầy không chỉ là người truyền đạt kiến thức mà còn là người truyền lửa, kiên nhẫn động viên chúng em vượt qua những giai đoạn bế tắc nhất về giải pháp kỹ thuật.

Đặc biệt, chúng em xin cảm ơn những phản hồi khắt khe nhưng đầy tính xây dựng của các thầy về phương pháp triển khai và cách trình bày vấn đề. Những câu hỏi phản biện của các thầy đã thúc đẩy chúng em phải tự tìm tòi, đào sâu nghiên cứu để hiểu rõ hơn về tính tuân thủ trong y tế dưới góc nhìn của một kỹ sư công nghệ.

Cuối cùng, luận văn này chắc chắn sẽ không thể hoàn thiện nếu thiếu đi sự hỗ trợ từ gia đình và bạn bè – những người đã luôn bên cạnh chia sẻ và khích lệ tinh thần cho nhóm trong suốt hành trình vừa qua.

Dù đã rất nỗ lực, nhưng do giới hạn về thời gian và kinh nghiệm thực tiễn, luận văn khó tránh khỏi những thiếu sót. Chúng em rất mong nhận được sự đóng góp ý kiến của quý Thầy Cô để đề tài ngày càng hoàn thiện hơn.

Chúng em xin chân thành cảm ơn!

MỤC LỤC

VIẾT TẮT

Từ viết tắt	Nghĩa
API	Giao diện lập trình ứng dụng
Hồ sơ bệnh án điện tử	Hồ sơ sức khỏe điện tử
TÔI LÀ	Quản lý danh tính và quyền truy cập
JSON	Ký hiệu đối tượng JavaScript
JWT	Mã thông báo web JSON
KPI	Chỉ số hiệu suất chính
MTTD	Thời gian trung bình để phát hiện
MTTR	Thời gian phản hồi trung bình
OPA	Đại lý Chính sách Mở
PEP	Điểm thực thi chính sách
PDP	Điểm quyết định chính sách
PIPEDA	Đạo luật bảo vệ thông tin cá nhân và tài liệu điện tử
RBAC	Kiểm soát truy cập dựa trên vai trò
NGHỈ NGƠI	Chuyển đổi trạng thái đại diện
SIEM	Quản lý thông tin và sự kiện an ninh
SSO	Đăng nhập một lần
TLS	Bảo mật lớp vận chuyển

***Bảng 1** – Danh sách các từ viết tắt*

CHƯƠNG 1 - INTRODUCTION

(Cung cấp thông tin nền, giới thiệu vấn đề nghiên cứu và nêu rõ mục đích cũng như ý nghĩa của nghiên cứu.)

1.1. Bối cảnh

Trong xu thế chuyển đổi số đang diễn ra mạnh mẽ và nhanh chóng trên toàn cầu thì ngành y tế Việt Nam cũng đang từng bước thực hiện quá trình hiện đại hoá hệ thống quản lý và khám chữa bệnh. Trọng tâm của chiến lược này là việc chuyển đổi từ hồ sơ bệnh án giấy truyền thống sang hệ thống Hồ sơ sức khỏe điện tử toàn dân (Electronic Health Record – EHR), đây là một nền tảng dữ liệu y tế tập trung, cho phép tích hợp và quản lý thông tin sức khỏe trọn đời của mỗi cá nhân, từ lịch sử tiêm chủng, tiền sử bệnh lý đến các kết quả chẩn đoán hình ảnh. Cơ sở pháp lý vững chắc cho định hướng này đã được xác lập thông qua Quyết định số 5349/QĐ-BYT của Bộ Y tế về kế hoạch triển khai Hồ sơ sức khỏe điện tử, và đặc biệt là Luật khám bệnh, chữa bệnh số 15/2023/QH15. Những bộ luật này không chỉ công nhận giá trị pháp lý của dữ liệu điện tử mà còn quy định bắt buộc về việc liên thông dữ liệu giữa các cơ sở khám chữa bệnh với Cơ sở dữ liệu quốc gia về dân cư, từ đó đã đánh dấu một bước mới về sự chuyển đổi cơ bản từ quản lý phân tán sang quản lý tập trung dựa trên dữ liệu [1], [2]. Được thúc đẩy mạnh mẽ bởi kế hoạch phát triển của Chính phủ, việc triển khai hệ thống Hồ sơ bệnh án Điện tử trong thời gian vừa qua đã ghi nhận một kết quả rất đáng kể. Theo số liệu thống kê chính thức từ bộ Y tế và Bảo hiểm xã hội Việt Nam tính đến tháng 10 năm 2024, cả nước đã thiết lập thành công hơn 32,1 triệu hồ sơ sức khỏe điện tử cho người dân. Và điều đáng nói hơn là việc triển khai Hồ sơ bệnh án Điện tử đã kết nối dữ liệu từ hơn 12.000 cơ sở khám bệnh trên toàn quốc để tích hợp trực tiếp vào ứng dụng định danh điện tử VneID, từ đó tạo điều kiện thuận lợi cho người dân trong việc tiếp cận và quản lý thông tin y tế thuận tiện hơn [3], [4]. Từ việc triển khai hồ sơ sức khỏe điện tử trên quy mô toàn quốc đã cho chúng ta nhận ra rằng sự chuyển đổi

số hoá đã đi sâu vào các mạng lưới y tế cơ sở, bao phủ từ các bệnh viện trung ương đến các phòng khám tư nhân.

Tuy nhiên, bên cạnh những mặt tích cực về việc triển khai Hồ sơ sức khỏe điện tử thì các phòng khám tư nhân hay những cơ sở chăm sóc sức khoẻ vừa và nhỏ cũng tham gia triển khai nhưng từ đó cũng kéo theo những rủi ro rất lớn về an ninh mạng. Bởi vì thực tế cho thấy đang tồn tại một khoảng cách lớn về khả năng tự bảo vệ hệ thống của họ. Nếu như các bệnh viện lớn tuyến Trung ương có đội ngũ kỹ thuật xịn và hệ thống máy móc bảo mật hiện đại, thì ngược lại đã có hàng nghìn phòng khám tư nhân và các cơ sở y tế vừa và nhỏ, nơi cũng đang nắm giữ rất nhiều dữ liệu nhạy cảm của người bệnh nhưng những vấn đề bảo mật thì vẫn còn rất lỏng lẻo và bị hạn chế rất nhiều, và đôi khi họ ít quan tâm tới vấn đề sẽ có hacker xâm nhập vào hệ thống của họ, nếu có thì các biện pháp hết sức sơ sài và lỏng lẻo [5], [6]. Sự yếu kém này cũng xuất phát từ 2 lý do chính mà các cơ sở nhỏ đều gặp phải: đó là thiếu nhân sự và thiếu tài chính. Đầu tiên về nhân sự, thực trạng chung là các phòng khám này rất hiếm khi tuyển dụng được nhân viên chuyên trách về an toàn thông tin. Cán bộ IT ở các cơ sở vừa và nhỏ này họ phải đảm nhận hầu hết đủ việc tạp vụ về công nghệ, từ việc phải sửa máy in, cài Win cho đến kéo dây mạng, nên hầu như họ không còn thời gian và cũng thiếu các kiến thức chuyên sâu để lo cho mảng bảo mật [7]. Bên cạnh đó thì họ ít được đi học các chứng chỉ quốc tế về an ninh mạng, nên thường không biết cách xử lý khi có sự cố tấn công xảy ra. Tiếp theo là về mặt kinh phí, đây cũng là một vấn đề gây ra nhiều bất lợi cho các cơ sở y tế vừa và nhỏ. Bởi vì các cơ sở như tư nhân thường ưu tiên tiền bạc để mua sắm máy móc khám chữa bệnh để có thể dễ dàng kiếm lợi nhuận nhưng lại không chi nhiều tiền cho các phần mềm diệt virus bản quyền hay hệ thống tường lửa đắt đỏ. Thậm chí theo thống kê, mức chi an toàn thông tin tại nhiều nơi còn chưa đạt nổi con số tối thiểu là 10% tổng ngân sách công nghệ thông tin, một con số bắt buộc mà chính phủ đã quy định rõ trong Chỉ thị 14/CT-TTg [8]. Chính vì sự lỏng lẻo "từ con

người đến công cụ" này mà các phòng khám nhỏ đang trở thành mục tiêu dễ bị tấn công nhất, là con đường để tin tặc xâm nhập sâu hơn vào hệ thống dữ liệu y tế [9]

1.2 Phát biểu vấn đề

Sau khi đã hiểu rõ được bối cảnh mà các cơ sở y tế vừa và nhỏ gặp phải trong quá trình chuyển đổi sang Hồ sơ bệnh án điện tử (EHR) thì sau đây chúng ta sẽ đi sâu hơn vào vấn đề là "liệu việc hạn chế về nhân sự và cũng như hạ tầng hay không quá quan tâm về vấn đề bảo mật có thật sự đang diễn ra ở mỗi cơ sở y tế vừa và nhỏ thôi hay các cơ sở lớn cũng đang gặp phải vấn đề đó ?". Để hiểu rõ hơn thì chúng ta sẽ có những bài báo, dẫn chứng nêu rõ ra câu hỏi này. Theo bài báo cáo của Ponemon Sullivan Privacy report thì tác giả của bài báo có nói rằng "Current legacy technologies have difficulty protecting the enormous amounts of PHI across our systems (66 percent of respondents)" có nghĩa là đã có tới 66% các giải pháp công nghệ hiện hành tại các cơ sở này bị đánh giá là đã cũ và không đủ khả năng bảo vệ hồ sơ bệnh nhân trước các cuộc tấn công hiện đại [10], và nguyên nhân sâu xa của tình trạng này cũng đã được nêu rõ trong bài khảo sát của Black Book Market Research (2024), những nhà nghiên cứu có nói rằng "Legacy systems and EHR/RCM software (77% strongly agree). Hospitals and physician practices still rely on legacy systems and outdated software that do not receive regular security updates making them vulnerable to attacks, the cost and compatibility issues of migrating to more secure cloud technologies is still implementing better solutions", dẫn chứng này có nghĩa là đã có 77% các bệnh viện và phòng khám bác sĩ sử dụng các hệ thống cũ, phần mềm EHR/RCM, bên cạnh đó thì các phần mềm lỗi thời không được cập nhật bảo mật thường xuyên, từ đó khiến chúng dễ bị tấn công hơn và tạo lỗ hổng gây hại cho hệ thống, ngoài ra thì vấn đề chi phí và sự tương thích khi chuyển sang các công nghệ tốt, an toàn hơn chẳng hạn như đám mây vẫn đang cản trở việc triển khai các giải pháp tốt hơn [11]. Từ những bài khảo sát đó, chúng ta có thể

thấy rằng việc hạn chế về cơ sở hạ tầng cũng như chi phí vận hành đã nảy sinh ra ba vấn đề kỹ thuật nghiêm trọng:

Thứ nhất, cơ chế kiểm soát truy cập phân quyền theo vai trò (RBAC) mặc dù cũng là mô hình tiêu chuẩn trong việc kiểm soát người dùng và hạn chế việc lạm dụng quyền khi truy cập vào Hồ sơ bệnh án điện tử nhưng bản chất tĩnh của nó đang trở thành một điểm yếu trong môi trường y tế hiện đại ngày nay. Đã có những báo cáo nói về vấn đề này, chẳng hạn theo báo cáo "Claroty's State of CPS Security Report: Healthcare Exposures 2025" về an ninh hệ thống thực-ảo (CPS), CISOs phải quản lý các hệ thống thiết bị kết nối, và một số thiết bị vẫn chạy trên các hệ điều hành cũ không cong được các nhà cung cấp hỗ trợ cập nhật bảo mật và tính năng, đây là một tình huống thật sự đáng lo ngại vì phân tích của họ đã phát hiện ra các thiết bị chứa các lỗ hổng bảo mật đã bị khai thác (KEV) trong 99% các tập dữ liệu của họ, điều đó cho thấy được rằng khi các cơ sở y tế chỉ sử dụng mô hình RBAC hiện tại sẽ hoàn toàn gặp vấn đề rủi ro vì nó chỉ cấp quyền dựa trên "vai trò" mà không kiểm tra trạng thái an ninh cũng như ngữ cảnh của người dùng và , thiết bị họ sử dụng khi truy cập vào Hồ sơ bệnh án điện tử [12]. Về mặt lý thuyết, Park và R.Sandhu (2004) đã chỉ ra trong báo cáo của họ rằng các mô hình truyền thống như Role Based Access Control vốn chỉ được thiết kế trong môi trường khép kín [14], việc đó gây ra một số bất lợi đối với các bác sĩ, khi họ muốn truy cập vào Hồ sơ bệnh án điện tử thì chỉ có thể sử dụng máy tính ở nơi làm việc cũng như chỉ sử dụng mạng nội bộ của cơ sở họ làm việc, họ bị hạn chế cũng như bất tiện khi muốn làm việc từ xa và mô hình RBAC còn hoàn toàn thiếu khả năng kiểm soát liên tục, một sự cần thiết cho các môi trường y tế ngày nay.

Vấn đề tiếp theo, một thách thức lớn khác là các file log hiện tại còn thiếu sót những thông tin cần thiết và quan trong cho việc kiểm toán sau này vấn đề là do nhật ký kiểm toán (Audit logs) bị thiếu đi thông tin ngữ cảnh và còn chưa nêu rõ đầy đủ thông tin của người truy cập vào hệ thống. Chẳng hạn như Bác sĩ A

truy cập vào hồ sơ bệnh án điện tử thì nhật ký chỉ ghi lại khoảng thời gian và địa chỉ IP và tên máy chủ mà bác sĩ sử dụng chứ không ghi lại rõ tài khoản của người truy cập và mục đích truy cập là gì ?. Theo bài hướng dẫn quản lý nhật ký an toàn NIST SP 800-92 (một tiêu chuẩn nền tảng cho cả hệ thống HIPAA), đã nêu ở mục 3.3.1 (Syslog Format) rằng "Syslog is intended to be very simple, and each syslog message has only three parts. The first part specifies the facility and severity as numerical values. The second part of the message contains a timestamp and the hostname or IP address of the source of the log. The third part is the actual log message content. No standard fields are defined within the message content; it is intended to be humanreadable, and not easily machine-parseable", từ đó có thể thấy ở bài báo này cũng chỉ ra rằng hoàn toàn không có trường thông tin nào quy định về mục đích nghiệp vụ hay ý định người dùng, và không có dữ liệu raw để hệ thống có thể phân tích được hành vi người dùng[13].Tiếp theo ở bài báo Park và R.Sandhu (2004) cũng chỉ ra rõ rằng "Traditionally, access control has focused on the protection of computer and information resources in a closed system en-vironment. The enforcement of control has been primarily based on identities and attributes of known users by using a reference monitor and specified au-thorization rules [Sandhu and Samarati 1994].", như vậy có thể thấy rằng việc kiểm soát hành vi của người dùng dựa trên ngữ cảnh còn rất hạn chế và phụ thuộc theo cách truyền thống là sử dụng RBAC hơn, tuy nhiên, họ đã giới thiệu mô hình UCON-ABC thông qua trích dẫn "we introduce the UCON-ABC (Authorizations, oBligations, and Conditions)model family as a core model for UCON that covers these aspects in a sin-gle framework systematically and comprehensively", từ đó chúng ta nhận ra được rằng: Hệ thống cần phải tích hợp thêm yếu tố ngữ cảnh và nghĩa vụ thì mới đạt được khả năng kiểm soát tối đa đối với hành vi người dùng và ngăn chặn được các hành vi lạm dụng quyền hạn hơn, điều mà các mô hình kiểm soát truyền thống khó thực hiện được [14].

Vấn đề cuối cùng cũng rất quan trọng và gây nhiều rủi ro trong việc kiểm soát truy cập người dùng đó chính là nhật ký kiểm toán nằm rải rác và dễ bị tác động vào, từ đó bằng chứng kiểm toán có thể bị sửa đổi hoặc khó có thể truy vết lại sau này. Đặc biệt những tổ chức chăm sóc sức khoẻ vừa và nhỏ, thiếu chuyên môn thì dữ liệu thường nằm rải rác trên nhiều phần mềm khác nhau mà không có sự liên kết. Dựa vào tài liệu hướng dẫn quản trị dữ liệu của AHIMA (2022), với trích dẫn "Many healthcare organizations have given some thought to data governance but perhaps are unsure where to start or how to achieve a robust data governance program. An obstacle to implementing organizational healthcare data governance may be a lack of understanding of data as an asset by key stakeholders which may lead to data silos and delays in the formation of an organizational wide program." đã nêu ra được vấn đề quan trọng rằng ở các tổ chức y tế thiếu hiểu biết về cách quản lý dữ liệu sẽ dẫn đến tình trạng hình thành các "kho dữ liệu bị cô lập" và ngăn cản sự thống nhất và gây ra sự chậm trễ cho hệ thống chăm sóc sức khỏe [15]. Bên cạnh đó thì vấn đề thiếu nhân lực có chuyên môn về bảo mật cũng gây ra trở ngại lớn cho các doanh nghiệp vừa và nhỏ này, theo báo cáo của ENISA (2021) về an ninh mạng cho doanh nghiệp SMEs đã nêu ra rằng "Cybersecurity is a specialized topic, requiring specialized knowledge, however it is quite common within an SME that individuals multitask and may have multiple roles assigned to them. As a result, an employee within a SME may be responsible for cybersecurity, as well as for other processes" ," Compounding the challenges in this area is that many cybersecurity solutions require specialized IT knowledge to implement and manage them properly. All of these issues combined make managing cybersecurity within a SME a big challenge.". Họ đã chỉ ra rằng ở các doanh nghiệp y tế vừa và nhỏ thì việc cá nhân đảm nhận nhiều nhiệm vụ và được giao nhiều vai trò thì khá là phổ biến, vì vậy nên một nhân viên có thể chịu trách nhiệm về an ninh mạng cũng như các quy trình khác, điều này sẽ gây thách thức lớn cho doanh nghiệp chăm sóc sức khỏe đó [16]

1.3 Mục tiêu nghiên cứu

Sau khi đã đi sâu vào những rủi ro và điểm yếu mà trong các cơ sở y tế vừa và nhỏ đều gặp phải thì chúng ta đã nhận ra rằng việc quan trọng nhất cần phải thay đổi và khắc phục đó chính là vấn đề hạn chế nghiêm trọng về cơ chế kiểm soát và giám sát trong các hệ thống cũ, vì vậy mục tiêu nghiên cứu lần này của chúng ta hướng tới đó chính là xây dựng một hệ thống tự động giám sát tuân thủ chính sách dành cho Hồ sơ bệnh án điện tử (EHR) tại các cơ sở y tế vừa và nhỏ ở Việt Nam, và hệ thống này sẽ khắc phục được thêm điểm yếu đó là nguồn nhân sự hạn chế và tài chính hạn hẹp. Bên cạnh đó hệ thống sẽ triển khai theo mô hình đã có sẵn ở các bài báo nghiên cứu trước đây để khắc phục được nhược điểm của mô hình phân quyền tĩnh (RBAC) là yêu cầu truy cập bị hạn chế và các ràng buộc nghiêm ngặt, bằng cách kết hợp thêm mô hình Attribute Based Access Control (ABAC), mô hình này chứa nhiều thuộc tính liên quan đến môi trường, tài nguyên và người dùng được xem xét để thực thi chính sách hiệu quả, chi tiết và tối ưu hơn trong quá trình thu thập hành động truy cập của người dùng khi vào EHR bởi vì các thuộc tính này bao gồm vai trò người dùng, giới hạn thời gian, vị trí và ngữ cảnh khác nên rất thuận lợi trong việc kiểm toán sau này. Chúng tôi sẽ đưa ra các bài báo nghiên cứu, dẫn chứng cho thấy rằng việc sử dụng mô hình RBAC kết hợp ABAC đạt hiệu quả cao hơn rất nhiều, chẳng hạn như theo trích dẫn trong bài nghiên cứu: ‘An access control system for cloud-based healthcare systems driven by blockchain’ đã cho chúng ta thấy “sự kết hợp giữa blockchain với kiến trúc kiểm soát truy cập lại là sử dụng kết hợp ABAC và RBAC có thể cung cấp cơ chế kiểm soát truy cập mạnh mẽ cho các tài nguyên điện toán không đồng nhất, đặc biệt là trong môi trường điện toán đám mây, và việc tích hợp này được thực hiện qua các thành phần sau như: Lưu trữ vai trò/thuộc tính trên các kho lưu trữ chống giả mạo, Thực thi chính sách thông qua hợp đồng thông minh, Kiểm soát phi tập trung và Khả năng kiểm toán và tính minh bạch”. Qua nghiên cứu triển khai ABAC và RBAC trong hệ thống blockchain cho chúng ta thấy được nó mang lại nhiều lợi ích, chẳng hạn như

tăng cường bảo mật, tính minh bạch, quyền sở hữu và ghi nhật ký chặt chẽ, bảo hiểm chống lại quản lý rủi ro…[17]. Song song với đó, chúng tôi cũng tìm thấy những bài nghiên cứu nói về việc tập trung phát triển kỹ thuật làm giàu nhật ký để bổ sung thông tin ngữ cảnh vào bằng chứng kiểm toán. Bài nghiên cứu "Context-Aware Electronic Health Record - Internet of Things and Blockchain Approach" của Tiago Guimaraes đã đề xuất rằng việc tích hợp nhận thức ngữ cảnh (Context-awareness) vào hệ thống EHR là yếu tố then chốt có thể giúp phân biệt chính xác hành vi truy cập hợp lệ và các hành vi lạm dụng quyền hạn tinh trong môi trường Y tế, cụ thể hơn trong bài nghiên cứu này ở mục "5.Pervasive and Context-Aware EHR" với 3 phases: (1) Phase A- Fine the location of the users, (2) Phase B - Development of a Mobile EHR app, (3) Phase C - Maintain an immutable log of the data generated, với các giai đoạn này thì bài nghiên cứu này đã cho chúng ta thấy rằng việc có ngữ cảnh cũng như quyền hạn được phân rõ ràng với mỗi vai trò truy cập vào EHR đã trở thành một lớp tường lửa chắc chắn. Nó giám sát và ngăn chặn các hành vi truy cập không đúng phận sự hoặc trái phép từ xa mà người quản trị không cần phải cài đặt thủ công hay quá nhiều thao tác phức tạp. Thông tin ngữ cảnh được ghi lại trong bằng chứng kiểm toán rất chi tiết, nếu có sự cố xảy ra trong y khoa thì người vi phạm không thể chối cãi [18]

1.4. Ý nghĩa của nghiên cứu

Việc chúng ta có mục tiêu nghiên cứu được đề ra ở 1.3 đã mang lại một ý nghĩa rất to lớn đối với các cơ sở y tế vừa và nhỏ trong lúc họ đang gặp khó khăn và thách thức khi phải đảm bảo những bộ luật và pháp lý khắt khe trong quy trình khám chữa bệnh, bên cạnh đó họ còn phải ghi nhật ký kiểm toán liên tục để đảm bảo mọi người dùng truy cập đều phải đúng quyền và đúng ngữ cảnh trong pháp lý nêu ra, và những khó khăn đó đã được Hệ thống tự động giám sát tuân thủ chính sách của chúng tôi giải quyết, nó bao gồm 2 vấn đề: Thứ nhất đó là giúp cho các cơ sở y tế vừa và nhỏ đều đảm bảo những điều khoản khắt khe

trong các pháp lý về chăm sóc sức khỏe. Chẳng hạn như Nghị Định 13/2023/NĐ-CP có đặt ra các yêu cầu khắt khe về bảo vệ dữ liệu cá nhân và các quy định về khả năng truy xuất nguồn gốc hành vi của người dùng và tính toàn vẹn của hồ sơ dữ liệu bệnh án [19]. Tuy cơ sở hạ tầng kỹ thuật còn hạn chế nhưng hệ thống tự động của chúng tôi vẫn hoạt động như một cơ chế có thể xác định mọi hành vi truy cập vào EHR đều có thể cung cấp bằng chứng tuân thủ chính xác và thức thời theo các điều luật, khung pháp lý của cơ quan chính phủ đưa ra mà không cần phải can thiệp thủ công, từ đó có thể giải quyết triệt để rủi ro sai sót trong quy trình báo cáo giải trình và điều này còn giúp cho các đơn vị y tế đó đảm bảo tuân thủ đầy đủ các điều khoản mà pháp lý đã đưa ra, từ đó tránh được những mức phát pháp lý mà các cơ sở y tế vừa và nhỏ khó có thể chấp nhận được. Vấn đề thứ hai là củng cố niềm tin với người bệnh để nâng cao hiệu quả khám chữa bệnh, việc đảm bảo an toàn dữ liệu không còn là vấn đề kỹ thuật mà là yếu tố ảnh hưởng đến quá trình chăm sóc sức khoẻ cho bệnh nhân. Theo bài nghiên cứu có tiêu đều là "Trust and digital privacy in healthcare: a cross-sectional descriptive study of trust…." đã chứng minh được sự liên hệ rõ rệt giữa niềm tin vào hệ thống bảo mật và mức độ sẵn lòng chia sẽ dữ liệu sức khoẻ của bệnh nhân [20]. Cụ thể hơn trong bài khảo sát đã chỉ ra rằng có khoảng 81,9% người tham gia có mức độ tin tưởng cao sẽ sẵn sàng chia sẻ dữ liệu riêng tư của họ trong quá trình khám chữa bệnh, ngược lại những người có niềm tin thấp thường có xu hướng yêu cầu kiểm soát khắt khe hơn và đôi khi họ có thể chủ động giấu đi thông tin bệnh lý nhạy cảm của họ. Hệ quả của việc thiếu niềm tin này là rất nghiêm trọng vì nếu bệnh nhân thấy không an toàn, họ sẽ không cung cấp đầy đủ thông tin bệnh lý, dẫn đến bác sĩ thiếu thông tin sức khoẻ của họ và không thể đưa ra hướng điều trị chính xác. Vì vậy, hệ thống của chúng tôi phải đảm bảo bảo vệ được quyền riêng tư chặt chẽ và từ đó mới có thể giúp bệnh nhân yên tâm chia sẽ và hợp tác tối đa đối với các bác sĩ.

1.5. Phạm vi và giới hạn

1.5.1. Phạm vi nghiên cứu:

Về đối tượng và không gian triển khai: Nghiên cứu của chúng tôi được xây dựng và triển khai theo mô hình ABAC + RBAC để khắc phục nhiều vấn đề mà các cơ sở y tế vừa và nhỏ gặp phải. Chúng tôi chọn nhóm đối tượng bao gồm các phòng khám đa khoa, trung tâm y tế nhỏ hoặc các bệnh viện tư nhân tầm trung vì chúng tôi nhận thấy rằng đặc điểm chung của nhóm này là hạ tầng công nghệ thông tin thường bị phân tán, nguồn lực tài chính còn hạn chế và nhân sự IT thì chưa có chuyên môn cao về an ninh mạng, họ còn dễ gặp rủi ro về vấn đề tuân thủ pháp lý. Còn các bệnh viện lớn thì nằm ngoài đối tượng nghiên cứu của chúng tôi vì nhân sự cũng như hạ tầng ở đó rất mạnh mẽ, họ có thể đảm bảo được tuân thủ các pháp lý nhờ có các công cụ giám sát mạnh mẽ. Về quy trình của hệ thống này sẽ tập trung vào việc kiểm soát và giám sát chặt chẽ các luồng truy cập vào Hồ sơ bệnh án điện tử (EHR). Phạm vi giám sát của hệ thống chúng tôi bao gồm 3 quy trình chính: 1. Quy trình truy cập xem chi tiết Hồ sơ bệnh án điện tử và lịch sử khám chữa bệnh, 2. Quy trình chỉnh sửa và cập nhật kết quả thăm khám lâm sàng đối với các bác sĩ chuyên khoa (bao gồm kết quả xét nghiệm và hình ảnh chẩn đoán). 3. Quy trình tra cứu thông tin bệnh nhân và các thủ tục hành chính. Còn các quy trình như quản lý vật liệu y tế hay chấm công cho các nhân sự sẽ không thuộc quyền giám sát của hệ thống chúng tôi. Tiếp đến là giới hạn về mặt kỹ thuật: Hệ thống này sẽ giám sát tại tầng Ứng dụng (Application) và tầng Dữ liệu (Data Layer) bởi vì hệ thống sẽ thu thập lại các hành vi người dùng và đưa ra các bằng chứng kiểm toán bao gồm tên người dùng đó, hành động của họ trong EHR là gì và họ có truy cập đúng ngữ cảnh không, sau đó sẽ tiến hành so sánh với các điều khoản pháp lý và cho người quản trị hệ thống biết được liệu hành vi này có tuân thủ hay vi phạm. Các biện pháp ngăn chặn hacker tấn công vào hệ thống cũng triển khai và ngăn chặn, sau

đó được đưa lên bảng giám sát chung (Dashboard) để người quản trị cũng có thể nắm rõ tình trạng của hệ thống.

1.5.2. Giới hạn của nghiên cứu:

Mặc dù hệ thống này đã giúp cho các cơ sở y tế vừa và nhỏ khắc phục những điểm yếu thì bên cạnh đó nó cũng có 2 giới hạn cụ thể mà hệ thống này gặp phải. Đầu tiên là về khả năng mở rộng: vì ưu tiên tính khả thi và chi phí thấp để phù hợp với cơ sở nhỏ, thì kiến trúc hệ thống chưa được triển khai để chịu được một lượng truy cập đồng thời cực lớn thường thấy ở các hệ thống SIEM nước ngoài. Tiếp theo là mô hình đe doạ: những thuật toán mà chúng tôi sử dụng chủ yếu để phát hiện các hành vi vi phạm chính sách nội bộ, ví dụ: nhân viên xem hồ sơ không thuộc phạm vi của mình. Còn khả năng ngăn chặn các cuộc tấn công mạnh như sử dụng mã độc hay những lỗ hổng chưa được công bố thì đều nằm ngoài khả năng của hệ thống chúng tôi.

1.6. Cấu trúc luận văn

Luận văn này được tổ chức thành sáu chương, cung cấp một phân tích toàn diện về những thách thức trong giám sát an ninh mạng y tế trong quá trình chuyển đổi số y tế tại Việt Nam và giải pháp kỹ thuật được đề xuất sử dụng kiến trúc ba luồng (IAM/Gateway, EHR, SIEM).

Chương 1: Giới thiệu đặt nền tảng cho nghiên cứu này bằng cách trình bày bối cảnh các sáng kiến số hóa y tế của Việt Nam và những thách thức an ninh mạng đang nổi lên. Chương này xác định vấn đề cụ thể về năng lực giám sát an ninh chưa đầy đủ tại các cơ sở y tế Việt Nam, nêu rõ các mục tiêu nghiên cứu nhằm phát triển một giải pháp giám sát tích hợp, và giải thích tầm quan trọng của công trình này đối với cả an ninh y tế Việt Nam và cộng đồng tin học y tế quốc tế rộng lớn hơn. Phần phạm vi và hạn chế làm rõ các giới hạn kỹ thuật và những ràng buộc trong việc thực hiện nghiên cứu này.

Chương 2: Tổng quan tài liệu cung cấp phân tích toàn diện về các nghiên cứu hiện có trong lĩnh vực an ninh mạng y tế, giám sát an ninh hồ sơ sức khỏe điện tử và các tiêu chuẩn tương tác dữ liệu y tế. Chương này xem xét các nghiên cứu trước đây về triển khai bảo mật HL7/FHIR, ứng dụng SIEM trong môi trường chăm sóc sức khỏe và những thách thức về an ninh CNTT y tế tại Việt Nam. Phần tổng quan này tổng hợp những khoảng trống kiến thức hiện tại và

thiết lập nền tảng lý thuyết cho kiến trúc giám sát được đề xuất, kết luận bằng việc xác định rõ ràng đóng góp của nghiên cứu này vào kho kiến thức hiện có.

Chương 3: Phần Phương pháp luận trình bày chi tiết thiết kế nghiên cứu và phương pháp kỹ thuật được sử dụng để phát triển hệ thống. Chương này mô tả kiến trúc hệ thống ba luồng (IAM/Gateway, EHR, SIEM), giải thích việc lựa chọn các thành phần mã nguồn mở (Keycloak, NGINX, OPA, FastAPI), và phác thảo quy trình mô hình hóa chính sách dựa trên các quy định của Việt Nam. Nó cũng bao gồm thiết kế môi trường mô phỏng tấn công "Đội Đỏ đấu với Đội Xanh" được sử dụng để đánh giá.

Chương 4: Phần Thực nghiệm và Kết quả trình bày việc đánh giá hệ thống được đề xuất thông qua ba kịch bản tấn công cụ thể: Xác thực vét cạn (Brute-Force Authentication), Tấn công chèn mã SQL (SQL Injection) và Xóa dấu vết pháp y (Forensic Trace Deletion). Chương này cung cấp bằng chứng chi tiết về khả năng phòng thủ nhiều lớp của hệ thống, phân tích cách mỗi cuộc tấn công bị chặn hoặc phát hiện bởi các lớp Nhận dạng, Cổng và Dữ liệu tương ứng.

Chương 5: Phần thảo luận diễn giải các phát hiện chính, so sánh phương pháp dựa trên quy tắc với các tài liệu hiện có và các phương pháp dựa trên trí tuệ nhân tạo. Phần này thảo luận về ý nghĩa thực tiễn của việc triển khai tại các cơ sở có nguồn lực hạn chế, phân tích những hạn chế của hệ thống liên quan đến dữ liệu tổng hợp và phạm vi bao phủ quy tắc, đồng thời đề xuất các cơ chế để mở rộng quy mô và cập nhật tự động.

Chương 6: Phần Kết luận và Hướng nghiên cứu tương lai tóm tắt những đóng góp của nghiên cứu, trả lời các câu hỏi nghiên cứu và vạch ra lộ trình phát triển trong tương lai, bao gồm việc tích hợp Kiểm thử Chấp nhận Người dùng (UAT) và mở rộng thư viện quy tắc.

Mỗi chương đều dựa trên nội dung của chương trước để tạo nên một câu chuyện mạch lạc, tiến triển từ việc xác định vấn đề, phát triển giải pháp kỹ thuật đến triển khai thực tiễn và đánh giá, thể hiện toàn bộ quy trình nghiên cứu và phát triển cần thiết để giải quyết các thách thức an ninh mạng trong lĩnh vực y tế số đang phát triển của Việt Nam.

CHAPTER 2: LITERATURE REVIEW

Mục tiêu của chương này là khảo sát các nghiên cứu, tiêu chuẩn và giải pháp hiện có liên quan đến bảo mật EHR, tập trung vào các câu hỏi: những gì đã được thực hiện và những hạn chế khi áp dụng trong bối cảnh các cơ sở y tế vừa và

nhỏ. Từ đó, chương này tổng hợp khoảng trống nghiên cứu và làm cơ sở cho sự đóng góp của dự án.

2.1. Review of Previous Studies

2.1.1. An ninh mạng trong y tế kỹ thuật số

2.1.1.1. Các mối đe dọa và xu hướng tấn công

Nghiên cứu về an ninh mạng trong y tế kỹ thuật số thường mô tả chuỗi phòng thủ chuyên sâu: từ quản lý rủi ro, quy trình vận hành, kiểm soát truy cập, chính sách, phân đoạn mạng, mã hóa và giám sát liên tục. Tuy nhiên, thực tế cho thấy điểm yếu thường xuất hiện ở khâu vận hành: quyền truy cập tăng theo thời gian, cấu hình thay đổi mà thiếu truy vết kiểm toán, và khi có nghi vấn thì không đủ dữ liệu/ngữ cảnh để xác minh đúng hay sai. Ngoài ra, với ransomware, một nghiên cứu định tính về ransomware tại các bệnh viện Hoa Kỳ giai đoạn 2016–2022 cho biết riêng dữ liệu OCR đã ghi nhận 562 sự cố; tuy nhiên chỉ 65 trường hợp có đủ thông tin để phân tích chuyên sâu về động cơ tấn công và phản hồi/ứng phó sự cố [47]. Điều này cho thấy rào cản lớn không chỉ nằm ở tần suất tấn công, mà còn ở chất lượng và mức đầy đủ của dữ liệu phục vụ điều tra. Bên cạnh đó, DBIR 2024 lưu ý rằng trong lĩnh vực chăm sóc sức khỏe, ba nhóm kiểu sự cố (miscellaneous errors, privilege misuse và system intrusion) chiếm tỷ lệ lớn (tổng cộng 83%), đồng thời tác nhân nội bộ xuất hiện trong phần đáng kể các vụ việc (70% so với 30% tác nhân bên ngoài), nhấn mạnh nhu cầu giám sát hành vi truy cập và phát hiện bất thường dựa trên bằng chứng log [45].

2.1.1.2. Khuôn khổ pháp lý của Việt Nam và các yêu cầu tuân thủ

Tại Việt Nam, các quy định về bảo vệ dữ liệu cá nhân và an ninh mạng như Nghị định 13/2023/NĐ-CP, Luật An ninh mạng 2018 cùng các văn bản hướng dẫn đã đặt ra những yêu cầu cơ bản về kiểm soát truy cập, xử lý dữ liệu đúng mục đích và khả năng truy vết khi có sự cố xảy ra [25], [26], [27]. Trong phạm vi hồ sơ bệnh án điện tử (EHR), Thông tư 46/2018/TT-BYT cũng nhấn mạnh

khá rõ việc hệ thống cần ghi nhận đầy đủ dấu vết thao tác của người dùng. Cụ thể, nhật ký cần thể hiện thời điểm thực hiện (ngày, giờ) và loại thao tác (chẳng hạn như xem, nhập mới, chỉnh sửa, hủy hay khôi phục dữ liệu). Việc ghi vết này không chỉ áp dụng với nhân viên y tế (bác sĩ, điều dưỡng) mà cả đội ngũ quản trị hệ thống (IT) cũng cần được đưa vào phạm vi giám sát, nhằm phục vụ kiểm tra, kiểm toán hoặc điều tra khi cần thiết, đồng thời góp phần bảo đảm quyền riêng tư cho người bệnh [28]. Dù vậy, phần lớn các văn bản hiện hành vẫn dừng ở mức nêu yêu cầu mang tính nguyên tắc. Khi đi vào thực tế vận hành, câu hỏi "làm sao tự động hóa việc giám sát tuân thủ hằng ngày" lại phụ thuộc khá nhiều vào năng lực triển khai của từng cơ sở, mức độ chuẩn hóa nhật ký, và đặc biệt là khả năng gắn log với ngữ cảnh nghiệp vụ (ai truy cập – truy cập hồ sơ nào – vì lý do gì – trong bối cảnh nào). Khoảng trống này thường bộc lộ rõ ở các cơ sở vừa và nhỏ: hệ thống có thể có log, nhưng log chưa đủ ngữ cảnh để kiểm chứng tuân thủ một cách nhất quán [25], [26], [27], [28].

Ở cấp quản lý, Quyết định 326/QĐ-BYT (2024) tiếp tục nhấn mạnh yêu cầu giám sát an toàn thông tin và quản lý nhật ký trong quá trình vận hành hệ thống. Điều này cho thấy tuân thủ không chỉ nằm ở việc đáp ứng "quy định trên giấy", mà còn nằm ở năng lực ghi nhận, theo dõi và truy vết trong thực tế [28], [50].

2.1.1.3. Tiêu chuẩn quốc tế (HIPAA/NIST/ISO) và bài học thực hiện

Ở nhiều quốc gia, các khung chuẩn và hướng dẫn đều xem nhật ký log và cơ chế giám sát là nền tảng để đảm bảo tuân thủ trong môi trường y tế, đặc biệt với dữ liệu nhạy cảm như ePHI. Chẳng hạn, HIPAA Security Rule (nhóm biện pháp kỹ thuật) yêu cầu hệ thống phải ghi nhận và cho phép rà soát các hoạt động liên quan đến ePHI. Nói cách khác, không chỉ dừng ở việc ai được quyền truy cập, mà còn phải để lại dấu vết để khi cần có thể kiểm tra và đối chiếu [21]. Ở góc độ quản trị, ISO 27799 nhìn vấn đề rộng hơn: thay vì coi log như một tính năng kỹ thuật rời rạc, tiêu chuẩn này đặt nó trong khung tổng thể về quản trị an

toàn thông tin y tế, gắn với kiểm soát truy cập, phân quyền, quản lý rủi ro và các cơ chế đảm bảo vận hành an toàn [22]. Bổ sung cho hai khung trên, NIST SP 800-92 đi sâu vào cách quản lý log một cách bài bản (từ thu thập, chuẩn hóa, lưu giữ đến bảo vệ tính toàn vẹn và khai thác log cho kiểm toán/điều tra), còn NIST SP 800-137 nhấn mạnh tinh thần giám sát liên tục: theo dõi thường xuyên, có ngưỡng cảnh báo và cơ chế phản hồi, thay vì chỉ đợi đến kỳ mới rà soát [39], [24]. Điểm giống nhau của các tài liệu này là: tuân thủ cần đi kèm bằng chứng vận hành. Khi kiểm toán hoặc điều tra, hệ thống cần trả lời được những câu hỏi rất cụ thể như ai đã truy cập dữ liệu, truy cập vào thời điểm nào, thao tác gì và trên đối tượng nào. Tuy nhiên, khi đưa vào môi trường EHR, khoảng cách thường nằm ở bước chuyển từ nguyên tắc sang triển khai. Trong các hệ thống vận hành kiểu phân tán, log có thể nằm rải rác ở ứng dụng, cơ sở dữ liệu, API gateway… nhưng lại thiếu đồng bộ thời gian, thiếu chính sách lưu giữ phù hợp, không được chuẩn hóa định dạng, hoặc chưa có cơ chế bảo vệ khỏi sửa/xóa. Khi đó, log vẫn tồn tại, nhưng giá trị làm bằng chứng để đối chiếu lại bị giảm đi đáng kể [39]. Thậm chí, ngay cả khi log đầy đủ, bài toán vẫn chưa hẳn đã xong vì để kết luận tuân thủ, thường cần đi ngữ cảnh nghiệp vụ. Ví dụ cùng là hành vi "xem hồ sơ", nhưng còn phải biết người truy cập có thuộc nhóm điều trị hay không, truy cập trong ca trực hay ngoài giờ, truy cập một hồ sơ hay truy cập hàng loạt, và truy cập đó phục vụ nghiệp vụ hay có dấu hiệu bất thường. Các khung như HIPAA/ISO/NIST nhấn mạnh yêu cầu kiểm soát và giám sát, nhưng thường không đi sâu đến mức "làm thế nào gắn log kỹ thuật với ngữ cảnh EHR" để giảm mơ hồ khi đánh giá vi phạm [21], [22], [24], [39].

Với các cơ sở y tế vừa và nhỏ, khó khăn thực sự còn đến từ nguồn lực. Vận hành SIEM không đơn giản là gom log về một chỗ, mà còn cần dung lượng lưu trữ, chính sách lưu giữ đủ dài, có quy trình vận hành rõ ràng, và đội ngũ theo dõi để xử lý cảnh báo, tinh chỉnh luật cũng như hạn chế cảnh báo giả. Trong khi đó, các hướng dẫn về quản lý log nhấn mạnh việc cần xác định mục tiêu và ưu tiên những yêu cầu quan trọng do nguồn lực có hạn [39]; còn các nghiên cứu tổng

quan về SIEM cũng cho thấy xu hướng hướng tới việc cải thiện hiệu quả phát hiện và giảm tải cho người vận hành [41]. Vì vậy, trong triển khai thực tế, cách tiếp cận "tối giản nhưng tập trung" thường khả thi hơn: ưu tiên một số kịch bản tuân thủ rủi ro cao (ví dụ truy cập ngoài quan hệ điều trị, truy cập ngoài giờ, truy cập khối lượng lớn…), thiết kế các quy tắc phát hiện phù hợp, và khi điều kiện cho phép thì bổ sung thêm ngữ cảnh từ EHR/IAM (vai trò, khoa/phòng, ca trực, quan hệ điều trị…) để cảnh báo trở nên sát thực tế hơn và giảm gánh nặng vận hành. So với việc cố gắng bao quát mọi loại sự kiện ngay từ đầu, cách làm này thường dễ triển khai và dễ duy trì hơn [39], [41].

2.1.2. Hồ sơ sức khỏe điện tử (EHR)

2.1.2.1. HL7 FHIR và SMART theo tiêu chuẩn FHIR

Hồ sơ sức khỏe điện tử hiện đại thường phải kết nối và trao đổi dữ liệu với nhiều hệ thống khác nhau như xét nghiệm, chẩn đoán hình ảnh, dược hay quản lý, thậm chí còn cần chia sẻ dữ liệu giữa các cơ sở. Trên thực tế, mỗi hệ thống có thể dùng một cách biểu diễn dữ liệu và cách tích hợp riêng, nên nếu thiếu một chuẩn chung thì việc liên thông sẽ khó đồng bộ và khó mở rộng. Và HL7 chính là bộ chuẩn trao đổi dữ liệu y tế; trong đó FHIR (Fast Healthcare Interoperability Resources) mô hình hóa dữ liệu dưới dạng các "tài nguyên", cung cấp cơ chế truy cập theo kiểu web/API giúp cho việc trình bày và trao đổi dữ liệu trở nên nhất quán hơn. Trên nền FHIR, mô hình SMART on FHIR bổ sung cơ chế tích hợp ứng dụng bên thứ ba dựa trên OAuth 2.0 và OIDC. OAuth 2.0 cho phép cấp quyền truy cập bằng token thay vì chia sẻ mật khẩu, còn OIDC bổ sung lớp xác thực danh tính trên nền OAuth 2.0, từ đó cho phép người dùng/ứng dụng truy cập tài nguyên FHIR theo phạm vi quyền được cấp. Nhờ vậy, nhiều hệ thống EHR có thể phát triển theo hướng mô-đun, đồng thời tái sử dụng các dịch vụ xác thực và ủy quyền dùng chung [29], [30], [35], [36].

2.1.2.2. Kiểm toán Sự kiện và theo dõi hoạt động trong EHR

Trong chuẩn HL7 FHIR, AuditEvent là một đối tượng dữ liệu dùng để ghi nhận dấu vết kiểm toán cho các hoạt động truy cập hoặc xử lý dữ liệu. Theo đặc tả, AuditEvent có thể mô tả tương đối đầy đủ "ai làm gì, tác động lên đối tượng nào, tại thời điểm nào và từ nguồn/kênh nào" [31]. So với các log thuần kỹ thuật như trạng thái HTTP, endpoint, thông tin kết nối…, AuditEvent có ưu điểm ở chỗ thông tin được tổ chức theo cấu trúc chuẩn và hướng tới ý nghĩa nghiệp vụ, nhờ đó thuận lợi hơn cho việc truy xuất, điều tra và đánh giá tuân thủ.

Dù vậy khi triển khai thực tế, mức độ hữu dụng của AuditEvent lại phụ thuộc nhiều vào cách từng hệ thống ghi nhận sự kiện. Lý do là trong đặc tả, một số phần liên quan đến phân loại/diễn giải sự kiện cho phép linh hoạt theo cách của từng đơn vị triển khai, nên nếu mỗi hệ thống ghi theo một kiểu thì dữ liệu audit dễ thiếu nhất quán [31]. Vì vậy, nếu không có quy ước chuẩn hóa nội bộ (chẳng hạn thống nhất mức độ chi tiết cần ghi, cách đặt loại sự kiện, cách gắn đối tượng liên quan…), audit log có thể rơi vào tình trạng khó tổng hợp, khó đối chiếu giữa các hệ thống, và khi cần kiểm toán hay truy vết thì thiếu căn cứ để kết luận rõ ràng [31].

2.1.2.3. Hạn chế và lỗ hổng trong đánh giá tuân thủ dựa trên EHR

FHIR/SMART giúp chuẩn hóa việc liên thông dữ liệu và tạo điều kiện tích hợp ứng dụng, trong đó trọng tâm chủ yếu nằm ở cách biểu diễn dữ liệu và cơ chế ủy quyền truy cập ở mức API [29]. Nhờ vậy, hệ thống có thể xác định một yêu cầu truy cập có đúng phạm vi quyền được cấp về mặt kỹ thuật hay không. Tuy nhiên, khi nói đến tuân thủ trong vận hành EHR, mục tiêu thường rộng hơn: để khẳng định một lần truy cập là phù hợp, cần đối chiếu thêm các yếu tố mang tính nghiệp vụ như mối quan hệ điều trị, khoa/phòng phụ trách, mục đích sử dụng, ca trực, hay các trường hợp ngoại lệ (chẳng hạn tình huống khẩn cấp). Ở phía ghi nhận hoạt động, FHIR có AuditEvent để mô tả sự kiện truy cập/xử lý dữ liệu theo một cấu trúc tương đối rõ ràng (ai làm gì, trên đối tượng nào, khi

nào, qua kênh nào) [31]. Dẫu vậy, audit log về bản chất mới chỉ là "dữ liệu đầu vào". Nói đơn giản, log thô thường phải được xử lý và tổng hợp trước khi dùng cho giám sát. Một scoping review trên JAMIA cho thấy raw event log trong EHR có thể rất lớn (tới mức hàng trăm GB mỗi năm ở một cơ sở), và để tạo được các thước đo sử dụng được thì thường phải xử lý dữ liệu đáng kể, chẳng hạn gom chuỗi thao tác thành hoạt động và xử lý khoảng trống giữa các thao tác [53]. Bài tổng quan này cũng chỉ ra rằng cách định nghĩa thước đo giữa các nghiên cứu còn khác nhau, khiến việc xây dựng chỉ số theo một cách nhất quán (và từ đó áp dụng vào giám sát thực tế) gặp nhiều khó khăn [53].

2.1.2.4. Quan điểm thực hiện ở Việt Nam và khoảng trống tại các cơ sở y tế vừa và nhỏ

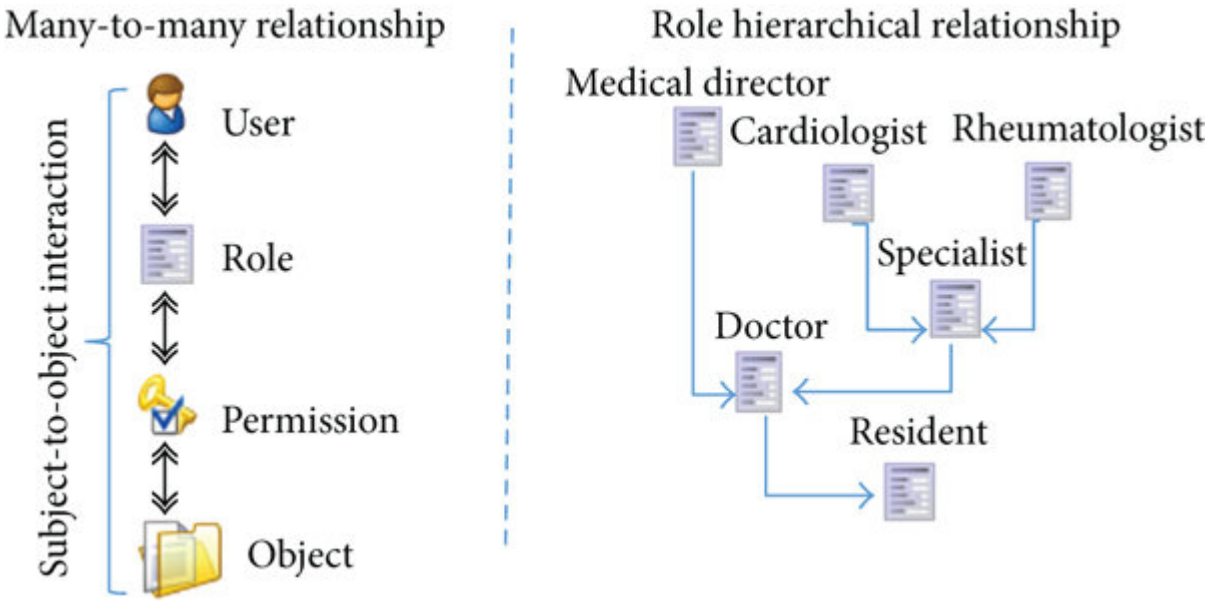
Ở Việt Nam, khi triển khai EHR, nhiều đơn vị thường chọn cách làm là trước mắt tập trung số hóa quy trình khám chữa bệnh để hệ thống vận hành ổn, rồi sau đó mới tính đến việc chuẩn hóa và liên thông dữ liệu giữa các hệ thống. Vì ưu tiên triển khai nhanh, phần ghi vết/audit ở giai đoạn đầu thường chỉ dừng ở những thao tác cơ bản trong từng phần mềm. Điều này khiến việc trả lời các câu hỏi kiểm toán quan trọng vẫn còn khó, chẳng hạn ai đã truy cập hồ sơ nào, truy cập trong bối cảnh nào, và truy cập đó có gắn với quan hệ xử lý/điều trị hợp lệ hay không.

Trong khi đó, yêu cầu ghi dấu vết theo Thông tư 46/2018/TT-BYT không chỉ là "có log", mà còn cần đủ thông tin để tra cứu và đối chiếu khi cần [28]. Vì vậy, để đáp ứng tốt hơn, các cơ sở thường phải có thêm một lớp tổng hợp: chuẩn hóa và liên kết nhật ký từ các hệ thống liên quan, thay vì chỉ dựa vào log cục bộ của một hệ thống duy nhất [28], [31].

2.1.3. Kiểm soát truy cập

2.1.3.1. RBAC: đơn giản và dễ vận hành

RBAC là mô hình kiểm soát truy cập khá phổ biến vì cách làm tương đối trực quan: phân quyền theo vai trò. Trong môi trường bệnh viện, nơi các nhóm công việc như bác sĩ, điều dưỡng hay dược sĩ đã được phân định rõ, RBAC thường dễ triển khai và dễ giải thích cho người dùng. Chuẩn INCITS RBAC cũng cung cấp nền tảng để thiết kế vai trò và quyền theo nhóm một cách có cấu trúc [32]. Nhưng khi đưa vào EHR, câu chuyện thường phức tạp hơn vì một lượt truy cập hợp lệ nhiều khi còn phụ thuộc vào ngữ cảnh: người đó có đang trong ca trực không, có liên quan điều trị với bệnh nhân không, hay có rơi vào tình huống khẩn cấp cần truy cập ngoại lệ hay không. Những yếu tố này RBAC không thể hiện tốt nếu chỉ dựa vào vai trò. NIST SP 800-162 cũng nhận xét rằng chỉ dùng các "định danh" như identity, groups và roles của người yêu cầu truy cập thường chưa đủ để diễn đạt các chính sách truy cập trong thực tế, và vì vậy cần xem xét thêm các thuộc tính của chủ thể/đối tượng/hành động, thậm chí cả điều kiện môi trường tại thời điểm ra quyết định [33].



2.1.3.2. ABAC và xu hướng Chính sách dưới dạng mã (OPA, PEP/PDP)

ABAC (Attribute-Based Access Control) mở rộng cách phân quyền bằng việc dựa trên nhiều loại thuộc tính hơn: thuộc tính của chủ thể (người dùng/ứng dụng), của đối tượng (tài nguyên), của hành động và cả điều kiện môi trường tại thời điểm truy cập. Theo NIST SP 800-162, ABAC là một cách tiếp cận linh hoạt để biểu diễn các ràng buộc theo ngữ cảnh, đồng thời đưa ra các lưu ý khi triển khai [33]. Song song với ABAC, xu hướng "chính sách dưới dạng mã" (policy-as-code) nhấn mạnh việc tách logic chính sách ra khỏi mã ứng dụng để chính sách dễ đọc, dễ kiểm thử và dễ quản lý phiên bản. Một cách triển khai thường gặp là kiến trúc PEP/PDP: PEP đóng vai trò điểm thực thi tại nơi phát sinh yêu cầu truy cập (chặn/cho phép), còn PDP là thành phần đánh giá chính sách và trả về quyết định dựa trên dữ liệu đầu vào và bộ chính sách hiện hành. OPA là một công cụ tiêu biểu cho hướng tiếp cận này, hỗ trợ viết và quản lý chính sách dưới dạng mã, đồng thời thuận tiện tích hợp với nhiều dịch vụ khác nhau [34]. Về mặt vận hành, các mô hình trên giúp quyết định quyền truy cập ngay tại thời điểm phát sinh yêu cầu. Tuy nhiên, nếu mục tiêu là theo dõi tuân thủ sau truy cập, hệ thống vẫn cần ghi lại "dấu vết quyết định" (chẳng hạn ngữ cảnh đầu vào, phiên bản chính sách đã áp dụng và kết quả cho phép/từ chối), rồi đối chiếu với nhật ký truy cập thực tế để phục vụ kiểm toán và truy vết.

Mô hình	Ưu điểm	Hạn chế	Ghi chú trong EHR
RBAC	Dễ hiểu, dễ quản trị theo vai trò; phù hợp phân quyền cơ bản	Khó mô tả ngữ cảnh (ca trực, quan hệ điều trị); dễ phát sinh ngoại lệ	Thường dùng làm lớp quyền nền [32]
ABAC	Linh hoạt, mô tả theo thuộc tính và ngữ cảnh; giảm nở vai trò	Cần quản trị thuộc tính tốt; policy phức tạp, khó debug	Phù hợp ràng buộc theo khoa/phòng, mục đích [33]

PEP/PDP + OPA	Tách policy khỏi ứng dụng; policy-as-code dễ kiểm thử/phiên bản hóa	Cần thiết kế điểm chặn (PEP) và bối cảnh đầu vào; phụ thuộc chất lượng log/ngữ cảnh	Hữu ích khi nhiều ứng dụng cùng dùng chính sách [34]

Bảng 2.1. So sánh các mô hình kiểm soát truy cập thường được sử dụng

2.1.3.3. Hạn chế khi đưa mô hình vào tuân thủ EHR

ABAC/PEP–PDP giúp mô tả và thực thi chính sách theo ngữ cảnh, nhưng khi áp dụng vào tuân thủ EHR thì thường phát sinh hai vấn đề chính: đầu vào ngữ cảnh và bằng chứng sau truy cập. Tài liệu NIST SP 800-162 mô tả rằng, ABAC đưa ra quyết định bằng cách đối chiếu các thuộc tính của chủ thể, đối tượng, hành động và điều kiện môi trường với chính sách đang áp dụng [33]. Trong EHR, những thuộc tính dùng để kết luận tuân thủ lại thường thay đổi theo thời điểm và nằm ở nhiều nguồn khác nhau (quan hệ điều trị, ca trực, sự đồng ý của bệnh nhân, ngoại lệ khẩn cấp…). Vì vậy, nếu dữ liệu ngữ cảnh không được đồng bộ và đảm bảo chất lượng, chính sách rất dễ bị áp dụng thiếu nhất quán [33]. Thêm vào đó, cơ chế thực thi thường chỉ chặn hoặc cho phép tại một số điểm truy cập; trong khi thực tế hệ thống có thể có nhiều luồng truy cập khác nhau, nên việc bao phủ đầy đủ cũng là một thách thức khi triển khai.

Cuối cùng, để phục vụ tuân thủ, việc ra quyết định tại thời điểm truy cập vẫn chưa đủ, còn cần "dấu vết" để kiểm tra lại về sau: quyết định dựa trên ngữ cảnh nào, áp dụng chính sách phiên bản nào, và có khớp với nhật ký truy cập thực tế hay không. Hướng dẫn log management của NIST nhấn mạnh rằng log muốn dùng cho kiểm toán/điều tra cần được quản lý theo hướng chuẩn hóa, đồng bộ thời gian, bảo vệ khỏi sửa hoặc xóa và lưu giữ phù hợp [39].

2.1.3.4. Ứng dụng thực tế ở Việt Nam: Phân cấp còn rời rạc, khó kiểm chứng

Trong thực tế triển khai ở Việt Nam, nhiều cơ sở thường ưu tiên làm từng bước: trước hết ưu tiên số hoá vận hành (HIS, xét nghiệm, chẩn đoán hình

ảnh…), sau đó mới dần mở rộng sang liên thông dữ liệu và giám sát tuân thủ. Báo cáo nghiên cứu của UNDP khi khảo sát tại Lạng Sơn, Bình Thuận và Tây Ninh mô tả khá rõ việc triển khai hồ sơ sức khỏe điện tử còn gặp nhiều điểm nghẽn về kết nối và chia sẻ dữ liệu; dữ liệu và phần mềm chuyên ngành có xu hướng phân tán theo từng mảng, khiến việc đồng bộ và khai thác chéo gặp nhiều trở ngại [54]. Khi hệ thống và dữ liệu bị phân tán, việc kiểm chứng tuân thủ cũng thường trở nên nặng hơn. Mỗi hệ thống có thể tự phân quyền và tự ghi nhật ký, nhưng để trả lời đầy đủ các câu hỏi kiểm toán như ai truy cập hồ sơ nào, truy cập trong bối cảnh nào và có hợp lệ hay không thì thường phải tổng hợp và đối chiếu từ nhiều nguồn. Nhìn ở tầm hệ thống, báo cáo PHSSR/WEF về Việt Nam cũng chỉ ra tình trạng trùng lặp hoặc phân mảnh của các hệ thống thông tin y tế do thiếu một chiến lược quốc gia toàn diện về e-Health [55]. Ngoài ra, khảo sát về mức độ ứng dụng công nghệ y tế số tại 5 bệnh viện công tuyến cao ở Việt Nam cho thấy việc chia sẻ dữ liệu lâm sàng ra ngoài đơn vị theo chuẩn HL7 chưa phải là thực hành phổ biến, phản ánh rằng liên thông liên cơ sở vẫn còn là điểm yếu [56].

2.1.4. Quản lý danh tính (IAM)

2.1.4.1. OAuth 2.0, OpenID Connect và JWT

Trong kiến trúc EHR hiện đại, lớp IAM đóng vai trò nền tảng cho xác thực và ủy quyền, giúp hệ thống biết chính xác ai đang truy cập và người đó được phép làm gì. OAuth 2.0 chuẩn hóa cơ chế ủy quyền truy cập bằng token, nhờ đó ứng dụng có thể truy cập tài nguyên thay mặt người dùng cho mà không cần chia sẻ mật khẩu. OpenID Connect (OIDC) được xây dựng trên OAuth 2.0 để bổ sung lớp xác thực danh tính và thống nhất đăng nhập giữa các hệ thống. Trong khi đó, JWT thường được dùng làm định dạng token gọn nhẹ, thuận tiện cho việc mang theo “claims” và kiểm tra chữ ký để xác thực tính hợp lệ. Nhờ các chuẩn này, nhiều hệ thống EHR có thể tích hợp ứng dụng theo mô hình bên thứ

ba (ví dụ SMART trên FHIR), nhưng vẫn giữ được cơ chế quản lý định danh và quyền truy cập theo hướng tập trung [35], [36], [37], [30].

2.1.4.2. IAM nguồn mở và các khả năng phù hợp cho các cơ sở vừa và nhỏ

Trong quá trình triển khai, nhiều tổ chức chọn các giải pháp IAM nguồn mở như Keycloak để giảm chi phí nhưng vẫn đáp ứng được những nhu cầu nền tảng: quản lý người dùng, nhóm/vai trò, SSO và liên kết với các nguồn danh tính khác (federation/brokering) [38]. Khi đặt Keycloak ở trước cổng FHIR hoặc cổng API, luồng xác thực và cấp quyền giữa ứng dụng và dịch vụ EHR thường được chuẩn hóa hơn vì mọi yêu cầu đều đi qua cơ chế phát hành token và kiểm tra token tập trung. Ngoài ra, Keycloak cũng có cơ chế ghi nhận sự kiện xác thực/ủy quyền (ví dụ đăng nhập, cấp token, lỗi xác thực…), nên có thể xem như một điểm tập trung để thu thập dấu vết ở lớp IAM, hỗ trợ đối chiếu khi cần [38].

2.1.4.3. Hạn chế: IAM không tự mình tạo ra giám sát tuân thủ

IAM chủ yếu giải quyết xác thực và ủy quyền, tức là xác định ai đang truy cập và truy cập với phạm vi quyền gì (thông qua cơ chế token/claims trong OAuth 2.0 và JWT) [35], [37]. Tuy nhiên, trong EHR, tuân thủ không chỉ là đúng quyền kỹ thuật mà còn phụ thuộc ngữ cảnh nghiệp vụ như quan hệ điều trị, ca trực, mục đích sử dụng hoặc ngoại lệ khẩn cấp; các yếu tố này thường không nằm trong token nên IAM khó tự kết luận truy cập có hợp lệ hay không. Ngoài ra, tuân thủ cần bằng chứng để kiểm tra lại về sau. Log của IAM thường chỉ phản ánh đăng nhập hoặc cấp token, trong khi kiểm toán truy cập EHR cần nhật ký ở nhiều lớp và phải được quản lý đủ tin cậy. NIST SP 800-92 nhấn mạnh log muốn phục vụ kiểm toán/điều tra cần được thu thập, chuẩn hóa, đồng bộ thời gian, bảo vệ khỏi sửa/xóa và lưu giữ phù hợp [39].

2.1.4.4. Thực tế ở cơ sở vừa và nhỏ: SSO có tồn tại nhưng thiếu cơ chế tuân thủ

Ở các cơ sở vừa và nhỏ, SSO/IAM thường được ưu tiên triển khai sớm để giảm gánh nặng quản trị tài khoản và thống nhất đăng nhập. Các chuẩn như OAuth 2.0, OpenID Connect và JWT cung cấp nền tảng kỹ thuật cho việc xác thực và ủy quyền tập trung [35], [36], [37], [38]. Tuy nhiên, các tài liệu và hướng dẫn liên quan đều cho thấy IAM chủ yếu trả lời câu hỏi về danh tính và quyền kỹ thuật, trong khi đánh giá tuân thủ trong EHR còn cần bằng chứng truy cập gắn với ngữ cảnh nghiệp vụ và khả năng kiểm tra lại về sau.

Theo hướng dẫn về quản lý nhật ký, để phục vụ kiểm toán/điều tra, log cần được thu thập và quản lý đủ tin cậy (chuẩn hóa, đồng bộ thời gian, bảo vệ tính toàn vẹn và lưu giữ phù hợp) [39]. Vì vậy, trong nhiều trường hợp, dù đã có SSO, điểm cần cải thiện vẫn nằm ở chỗ thiếu cơ chế giám sát và đối chiếu dựa trên nhật ký để kiểm chứng tuân thủ một cách nhất quán [39].

2.1.5. SIEM và quản lý nhật ký

2.1.5.1. Quản lý nhật ký theo NIST SP 800-92

Quản lý nhật ký là một nền tảng quan trọng cho an toàn thông tin: giúp phát hiện sự cố, hỗ trợ điều tra sau sự kiện và cung cấp bằng chứng phục vụ kiểm toán, tuân thủ. NIST SP 800-92 nhấn mạnh các yêu cầu mang tính thực tiễn của quản lý log, từ việc xác định các nguồn nhật ký quan trọng, tổ chức thu thập và chuẩn hóa định dạng, đồng bộ thời gian giữa các hệ thống, đến bảo vệ nhật ký khỏi bị chỉnh sửa/xóa và thiết kế chính sách lưu giữ phù hợp với rủi ro [39]. Ở các hệ thống quy mô lớn, SIEM thường được dùng như lớp tập trung để thu thập nhật ký từ nhiều nguồn, liên hệ các sự kiện và tạo cảnh báo dựa trên quy tắc hoặc mô hình phân tích. Nhờ đó, log không chỉ phục vụ vận hành kỹ

thuật mà còn hỗ trợ trả lời các câu hỏi kiểm toán cơ bản như ai đã làm gì, vào thời điểm nào, trên hệ thống nào và theo chuỗi sự kiện ra sao [39].

2.1.5.2. SIEM: kiến trúc, xu hướng nghiên cứu và bài học triển khai

Về mặt kiến trúc, các hệ thống SIEM thường xoay quanh một chuỗi chức năng khá ổn định: thu thập log/sự kiện từ nhiều nguồn, chuẩn hoá và lưu trữ, sau đó tương quan các sự kiện để tạo cảnh báo và báo cáo phục vụ vận hành an toàn thông tin. Các tổng quan về SIEM cũng mô tả SIEM như một nền tảng trung tâm có khả năng thu thập, tổng hợp, lưu trữ và tương quan sự kiện từ hạ tầng được quản lý, từ đó hỗ trợ xử lý cảnh báo và báo cáo an ninh [40]. Ở góc độ xu hướng, các nghiên cứu tổng quan ghi nhận SIEM đang dịch chuyển dần từ vai trò giám sát/cảnh báo thuần túy sang các mục tiêu rộng hơn như đáp ứng yêu cầu kiểm toán và tuân thủ, đồng thời kết hợp nhiều kỹ thuật phân tích dữ liệu hơn để nâng hiệu quả phát hiện [41]. Tuy vậy, bằng chứng triển khai thực tế ở quy mô lớn vẫn còn hạn chế: một systematic review về SIEM cho biết trong tập bài báo được phân tích, khoảng một nửa là các đề xuất mới tại thời điểm công bố, còn phần được kiểm chứng trong kịch bản thực tế chiếm tỷ lệ thấp hơn [41].

Từ góc nhìn triển khai, các tổng quan này gợi ý một bài học quan trọng: SIEM chỉ thực sự hữu ích khi dữ liệu đầu vào được chuẩn hoá và có ngữ cảnh đủ tốt để việc tương quan/cảnh báo bớt "nhiễu", đồng thời giúp người vận hành giải thích được vì sao một hành vi bị coi là rủi ro hay vi phạm [41].

2.1.5.3. Hạn chế của SIEM khi đánh giá tuân thủ EHR

Khi đưa SIEM vào bài toán tuân thủ trong EHR, khó khăn thường gặp nhất là thiếu ngữ cảnh nghiệp vụ để hiểu đúng ý nghĩa của cảnh báo. Một yêu cầu truy cập API có thể hoàn toàn hợp lệ nếu người dùng đang tham gia điều trị hoặc đang thực hiện nhiệm vụ được phân công; nhưng cũng cùng hành vi đó lại có thể trở thành vi phạm nếu truy cập ngoài phạm vi điều trị hoặc sai mục đích. Trong khi đó, nhiều nguồn log phổ biến lại thiên về thông tin kỹ thuật như

endpoint, trạng thái phản hồi, mã lỗi hay thông tin phiên, mà thiếu các chi tiết giúp kết luận tuân thủ như vai trò theo nghiệp vụ, khoa/phòng, quan hệ điều trị, lý do truy cập hoặc tình huống khẩn cấp. Vì vậy, cảnh báo dễ rơi vào tình trạng khó giải thích và khó dùng như căn cứ kiểm tra tuân thủ. Ngoài vấn đề ngữ cảnh, các tổng quan về SIEM cũng chỉ ra những điểm vướng quen thuộc khi triển khai, chẳng hạn cảnh báo giả vẫn nhiều, thiếu dữ liệu gán nhãn để đánh giá mô hình, và kết quả khó được kiểm chứng ngoài môi trường thử nghiệm [40], [41]. Với các cơ sở vừa và nhỏ, rào cản còn nằm ở chi phí và nguồn lực vận hành: lưu trữ log, duy trì hệ thống và có người theo dõi, tinh chỉnh cảnh báo thường không đơn giản.

2.1.6. Anchor Hash

2.1.6.1. Chuỗi băm và ghi nhật ký giả mạo

Một thách thức quan trọng trong giám sát tuân thủ là độ tin cậy của bằng chứng. Nếu nhật ký có thể bị chỉnh sửa hoặc xóa sau khi ghi, thì việc kết luận tuân thủ sau đó sẽ khó thuyết phục. Vì vậy, nhiều nghiên cứu đề xuất cơ chế ghi nhật ký theo hướng chống giả mạo, trong đó phổ biến là dùng chuỗi băm để liên kết các bản ghi: mỗi bản ghi mới phụ thuộc vào giá trị băm của bản ghi trước, nhờ đó các thay đổi về sau có thể bị phát hiện. Trong các công trình nền tảng, Kelsey và Schneier (1999) trình bày hướng tiếp cận về secure audit logs, đặt nền cho ý tưởng kiểm tra tính toàn vẹn của nhật ký; Ma và Tsudik (2008) tiếp tục mở rộng theo hướng ghi nhật ký chuyển tiếp an toàn hơn, tăng khả năng chống sửa đổi trong quá trình lưu trữ và vận hành [42], [43].

2.1.6.2. Cơ chế anchor hash định kỳ và đánh dấu thời gian

Trong bối cảnh đề tài, anchor hash có thể hiểu là việc định kỳ tổng hợp giá trị băm của chuỗi nhật ký (ví dụ theo giờ hoặc theo ngày) rồi ghi nhận giá trị này tại một nơi lưu trữ khó sửa đổi, chẳng hạn một dịch vụ ghi nhận độc lập hoặc

dịch vụ đánh dấu thời gian. Cách làm này giúp tăng khả năng đối chiếu về sau: nếu nhật ký nội bộ bị can thiệp, có thể so sánh lại với giá trị đã được ghi nhận trước đó để phát hiện sai lệch. Bên cạnh việc đặt mốc bằng giá trị băm, đánh dấu thời gian cũng là một bước quan trọng để chứng minh dữ liệu đã tồn tại tại một thời điểm nhất định. RFC 3161 mô tả giao thức Time-Stamp Protocol (TSP), là cơ chế phổ biến để cấp tem thời gian cho dữ liệu băm nhằm hỗ trợ kiểm chứng về sau [44].

2.1.6.3. Hạn chế và vấn đề vận hành

Về mặt vận hành, cơ chế băm/anchor hash thường kéo theo thêm việc quản lý khóa, quy trình đối soát định kỳ và yêu cầu đồng bộ thời gian, lưu giữ dữ liệu bài bản. Nếu log đến từ nhiều nguồn mà định dạng và dấu thời gian không nhất quán, hoặc khối lượng log quá lớn so với nguồn lực xử lý, thì "có cơ chế chống sửa" cũng chưa chắc biến log thành bằng chứng dễ dùng cho kiểm toán. NIST SP 800-92 nhấn mạnh đúng các vướng mắc này: nhiều nguồn log, khác định dạng, khác timestamp và khối lượng log lớn khiến thu thập–lưu trữ–phân tích trở nên phức tạp; đồng thời log cũng cần được bảo vệ tính bí mật/toàn vẹn/sẵn sàng của log, và đảm bảo phải có quy trình phân tích đều đặn thì mới tạo ra giá trị [39].

Ở góc độ kỹ thuật, Trong Schneier & Kelsey (Secure Audit Logs to Support Computer Forensics, 1999), họ nêu rất rõ các giới hạn quan trọng: không có biện pháp nào bảo vệ được các bản ghi được tạo ra sau khi máy đã bị chiếm quyền; và mật mã chủ yếu giúp phát hiện can thiệp sau này chứ không thể ngăn xóa log nếu không có cơ chế ghi kiểu write-once [42]. Vì vậy, băm/anchor hash phù hợp để tăng độ tin cậy của bằng chứng, nhưng thường chỉ là một mảnh trong chuỗi giải pháp lớn hơn: vẫn cần lớp thu thập - chuẩn hóa - phân tích và các quy tắc tuân thủ ở phía trên để phát hiện vi phạm và giải thích được sự kiện.

2.2. Summary of the Literature Review

Tổng hợp các nhóm tài liệu cho thấy:

(i) các tiêu chuẩn và khung tuân thủ như HIPAA, ISO và NIST đều nhấn mạnh yêu cầu kiểm soát truy cập và quản lý nhật ký như một phần bắt buộc để phục vụ kiểm toán và truy vết;

(ii) FHIR/SMART đóng vai trò quan trọng trong liên thông dữ liệu và tạo nền tảng để ghi nhận, kiểm tra hoạt động theo ngữ nghĩa y tế;

(iii) các mô hình RBAC/ABAC cùng xu hướng chính sách dưới dạng mã hỗ trợ đưa ra quyết định truy cập ngay tại thời điểm thực thi;

(iv) SIEM giúp tập trung thu thập và tương quan sự kiện, nhưng khi áp dụng cho EHR thường gặp khó ở khâu gắn log kỹ thuật với ngữ cảnh nghiệp vụ để kết luận tuân thủ. Đáng chú ý, các tổng quan về SIEM cũng cho thấy số lượng nghiên cứu có đánh giá thực nghiệm trong môi trường thực tế còn hạn chế [41], trong khi các báo cáo về an ninh y tế ghi nhận quy mô sự cố/vi phạm ở mức đáng kể và thiên về nhóm xâm nhập hệ thống; chẳng hạn DBIR 2024 ghi nhận System Intrusion chiếm 83% các vụ trong ngành chăm sóc sức khỏe, và dữ liệu dài hạn cho thấy tỷ lệ rò rỉ do hack/sự cố CNTT tăng từ 4% lên 81% (2010–2024), với ransomware là một mối đe doạ nổi bật [45], [46].

Văn bản/chuẩn (Việt Nam)	**Yêu cầu trọng tâm**	**Hàm ý kỹ thuật**	**Chức năng trong hệ thống đề xuất**
Thông tư 46/2018/TT-BYT [28]	Ghi vết thao tác người dùng trên bệnh án điện tử	Thu thập log đầy đủ và liên kết theo người dùng, hồ sơ, thời điểm	Chuẩn hóa log EHR; truy vấn theo người dùng, hồ sơ, thời điểm
Nghị định 13/2023/NĐ-CP [25]	Bảo vệ dữ liệu cá nhân; kiểm soát	Chính sách truy cập gắn với mục đích và bối cảnh; phải truy vết được	Bộ quy tắc kiểm tra tuân thủ; báo cáo vi phạm theo

	truy cập và xử lý đúng mục đích	việc sử dụng dữ liệu	mục đích và phạm vi dữ liệu
Quy chế ATTT/ANM Bộ Y tế (QĐ 326/2024) [50]	Theo dõi hoạt động hệ thống, lưu nhật ký, phục vụ giám sát và xử lý sự cố	Gom log về một điểm, lọc theo quy tắc, tạo cảnh báo và bảo toàn bằng chứng	Pipeline log tập trung; rule engine; dashboard; bảo toàn log bằng hash chain
Luật ANM 2018 và NĐ 53/2022 [26], [27]	Giám sát an ninh mạng và ứng phó sự cố	Theo dõi truy cập bất thường; cung cấp nhật ký phục vụ điều tra khi có yêu cầu	Chỉ báo cảnh báo theo quy tắc; xuất báo cáo phục vụ kiểm tra

Bảng 2.2. Liên hệ các yêu cầu pháp lý của Việt Nam và ý nghĩa kỹ thuật đối với hệ thống giám sát tuân thủ.

Tại Việt Nam, các đánh giá gần đây cũng cho thấy nghiên cứu về hệ thống y tế số trong bệnh viện còn khá hạn chế, đặc biệt là nghiên cứu triển khai và đánh giá vận hành. Điều này làm cho khoảng cách giữa các quy định/tiêu chuẩn và thực tiễn tuân thủ càng rõ ràng hơn, đặc biệt là ở các cơ sở vừa và nhỏ [52].

Nhóm giải pháp	Đã làm được	Hạn chế thường gặp	Hàm ý cho đồ án
Khung tuân thủ (HIPAA/ISO/NIST)	Định nghĩa yêu cầu bảo mật, audit, quản trị rủi ro	Mô tả ở mức nguyên tắc; triển khai phụ thuộc tổ chức	Cần biến yêu cầu thành quy tắc kiểm tra trên log
FHIR/SMART & AuditEvent	Chuẩn hóa dữ liệu, hỗ trợ tích hợp ứng dụng và mô tả sự kiện audit	AuditEvent không tự suy luận đúng/sai theo chính sách nội bộ	Chuẩn hóa log theo bối cảnh EHR để kiểm chứng tuân thủ

RBAC/ABAC/Policy-as-code	Ra quyết định truy cập linh hoạt theo vai trò/thuộc tính	Khó quản trị thuộc tính và ngoại lệ nghiệp vụ; thiếu vòng kiểm chứng sau truy cập	Kết hợp enforcement + evidence để truy vết và đối soát
SIEM & phân tích log	Thu thập/tương quan sự kiện, cảnh báo theo luật/mẫu	Thiếu ngữ cảnh nghiệp vụ; chi phí vận hành; cảnh báo giả [41]	Tối giản use-case, ưu tiên cảnh báo có ý nghĩa tuân thủ
Tamper-evident logging (hash chain)	Bảo vệ toàn vẹn, bắt buộc phải có bằng chứng kiểm toán	Không tự phát hiện vi phạm; cần quản lý khóa/thời gian	Dùng để tăng độ tin cậy bằng chứng cho pipeline giám sát

Từ các tài liệu đã khảo sát, có thể thấy khi đặt vào bối cảnh cơ sở y tế vừa và nhỏ vẫn còn một vài điểm chưa thật sự trọn vẹn:

- Nhiều hướng tiếp cận hiện nay mới giải quyết tốt từng phần riêng lẻ, chẳng hạn có IAM/SSO để quản lý đăng nhập, có phân quyền để kiểm soát truy cập, hoặc có log để ghi nhận hoạt động. Tuy vậy, việc nối các mảnh này lại thành một quy trình liền mạch : từ chính sách, đến thực thi, rồi đến kiểm chứng tuân thủ dựa trên bằng chứng vẫn chưa dễ thực hiện một cách nhất quán.
- Với SIEM và các giải pháp giám sát đầy đủ, rào cản thường nằm ở nguồn lực. Không chỉ là chi phí công cụ, mà còn là dung lượng lưu trữ, công vận hành và nhân sự theo dõi, tinh chỉnh cảnh báo. Vì vậy, nhiều cơ sở có xu hướng chỉ triển khai ở mức tối thiểu, hoặc ưu tiên vận hành trước rồi mới tính đến giám sát tuân thủ bài bản.

- Ở lớp bằng chứng, nhật ký đôi khi đã được ghi lại nhưng chất lượng chưa đủ để dùng cho kiểm toán/điều tra: dữ liệu phân tán ở nhiều hệ thống,

thiếu chuẩn hoá, thiếu đồng bộ thời gian, hoặc chưa có cơ chế đảm bảo tính toàn vẹn để đối chiếu về sau.

- Cuối cùng, các bằng chứng đánh giá trong bối cảnh cơ sở vừa và nhỏ vẫn còn hạn chế. Nhiều công trình về SIEM chủ yếu dừng ở mức đề xuất hoặc thử nghiệm nhỏ, nên việc khẳng định hiệu quả khi áp dụng rộng rãi trong thực tế vẫn cần thêm dữ liệu và đánh giá [41].

2.3. Contribution of Research

Dựa trên các điểm còn thiếu ở phần trên, đề tài này hướng tới một vài đóng góp theo hướng thực tế hơn:

- Trước hết, đề tài đặt mục tiêu xây dựng một cách nhìn về giám sát tuân thủ dựa trên chính sách cho hệ thống hồ sơ bệnh án điện tử, trong đó trọng tâm là làm sao để những hoạt động truy cập có thể được kiểm chứng lại bằng dấu vết cụ thể.
- Tiếp theo, đề tài phác thảo một kiến trúc kết hợp điểm thực thi (PEP), nơi ra quyết định (PDP) và quy trình thu thập – phân tích nhật ký, đồng thời ưu tiên một số kịch bản tuân thủ cốt lõi để triển khai gọn và dễ vận hành hơn.
- Để tăng độ tin cậy của bằng chứng, đề tài đưa thêm cơ chế anchor hash và ghi nhật ký chống giả mạo theo chu kỳ, nhằm giúp việc đối chiếu và phát hiện can thiệp vào nhật ký trở nên rõ ràng hơn.
- Cuối cùng, đề tài định hướng triển khai theo hướng tối giản và tận dụng các thành phần nguồn mở, để phù hợp hơn với điều kiện hạ tầng và nhân lực của các cơ sở y tế vừa và nhỏ.

CHAPTER 3: PHƯƠNG PHÁP NGHIÊN CỨU

3.1. Thiết kế nghiên cứu và cách tiếp cận

Sau khi đã trình bày xong ở chương 1 về việc EHR đang dần được triển khai rộng rãi trên toàn quốc và bên cạnh đó là sự ràng buộc, khắt khe về những điều luật, pháp lý, và những hạn chế về mặt hạ tầng cũng như chi phí ở các cơ sở y tế vừa và nhỏ tại Việt Nam thì ở chương 2 chúng tôi đã đưa ra mục tiêu nghiên cứu để khắc phục những nhược điểm ở các cơ sở y tế đó. Sau khi đã biết được mục tiêu rõ ràng mà chúng tôi đã nghiên cứu thì tiếp theo đây sẽ là nội dung chúng tôi nói về những phương pháp mà chúng tôi triển khai trong hệ thống này. Để có thể từ mô hình nghiên cứu thành khả năng ứng dụng thực tiễn và triển khai được ngoài thực tế thì chúng tôi đã áp dụng quy trình Phương pháp luận nghiên cứu Khoa học thiết kế (Design Science Research Methodology) được để xuất bởi nhà nghiên cứu Peffers và các cộng sự của ông trong bài báo "A Design Science Research Methodology for Information Systems Research" [57], bởi ở bài nghiên cứu này đã đưa ra một mô hình nghiên cứu tiêu chuẩn được sử dụng rộng rãi trong lĩnh vực hệ thống thông tin theo dẫn chứng "The DS process includes six steps: problem identification and motivation, definition of the objectives for a solution, design and development, demonstration, evaluation, and communication", và sáu bước này phù hợp với các đề tài có mục tiêu xây dựng kỹ thuật để giải quyết các vấn đề còn nan giải cho các doanh nghiệp. Sau khi dựa trên cách làm của bài nghiên cứu này thì quá trình nghiên cứu của chúng tôi được chia thành 4 giai đoạn chính, đảm bảo được đi đầy đủ từ các bước phân tích nhu cầu thực tế đến việc triển khai thực tế và kiểm chứng giải pháp

Giai đoạn 1: Xác định vấn đề và động lực nghiên cứu

Khi chúng tôi bắt đầu nghiên cứu về cách triển khai hệ thống này để giải quyết các vấn đề còn khó khăn ở cơ sở y tế vừa và nhỏ tại Việt Nam đó là khi các luật lệ về chăm sóc sức khoẻ hoặc Nghị Định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân chính thức có hiệu lực , Nghị Định này nhằm bắt buộc các tổ chức có hoạt động xử lý dữ liệu nhạy cảm, trong đó có dữ liệu sức khoẻ đều phải tuân thủ nghiêm ngặt các yêu cầu về kiểm soát truy cập, lưu lại các sự kiện truy cập vào

hệ thống và phải đảm bảo quyền riêng tư cho chủ thể dữ liệu, và lí do chúng tôi lại nhận thấy rằng đối tượng nghiên cứu mà chúng tôi nhắm tới là các cơ sở y tế vừa và nhỏ bởi vì trong quá trình tìm hiểu thực tế tại các cơ sở, doanh nghiệp chăm sóc sức khoẻ thì chúng tôi phát hiện ra có một khoảng cách rất lớn giữa các yêu cầu pháp lý và năng lực phải đảm bảo những tuân thủ đó tại các cơ sở y tế vừa và nhỏ. Cụ thể hơn, các khó khăn đó bao gồm: Thiếu nhân sự và chuyên trách an ninh, bởi vì đa số các phòng khám vừa và nhỏ không có bộ phận IT chuyên biệt như đã nêu ra các dẫn chứng ở Chapter 1, vì vậy nên việc giám sát tuân thủ thường được giao cho nhân viên kiêm nhiệm, họ không có đủ kiến thức để phát hiện các hành vi vi phạm tuân thủ mặc dù mỗi người dùng truy cập vào EHR đều được phân quyền rõ ràng cũng như sai sót trong cấu hình của hệ thống EHR. Tiếp theo là chi phí triển khai các giải pháp thương mại cao: các hệ thống giám sát tuân thủ có bản quyền như Splunk hay IBM QRadar thường có giá rất cao và có thể nằm ngoài khả năng tài chính của các cơ sở vừa và nhỏ này hoặc nếu có thể mua được thì họ cũng sẽ rất khó có thể sử dụng vì không có chuyên môn trong lĩnh vực an toàn thông tin. Cuối cùng là nhật kí kiểm toán có thể dễ bị xoá hoặc sửa đổi: bởi vì trong trường hợp có sự cố an ninh nội bộ như bác sĩ bị vi phạm điều khoản nào đó trong pháp lý hoặc chính IT Admin bị vi phạm thì nếu không có cơ chế bảo vệ thì việc dấu vết truy cập cũng có thể bị chính người vi phạm xoá trước khi bị phát hiện.

Từ những khó khăn trên thì việc chúng tôi có giải pháp triển khai hệ thống tự động giám sát tuân thủ vừa tự động hoá vừa có thể dễ dàng sử dụng, phù hợp với hạ tầng yếu cũng như đảm bảo được tính toàn vẹn của bằng chứng kiểm toán càng trở nên cần thiết hơn. Đây chính là động lực chính mà chúng tôi càng phải cố gắng triển khai thành công một hệ thống giám sát tuân thủ tự động dành riêng cho các đối tượng là cơ sở y tế vừa và nhỏ ở Việt Nam.

Giai đoạn 2: Mô hình thiết kế và Các giải pháp có trong hệ thống

Dựa trên những gì các nhà nghiên cứu đã phân tích thì chúng tôi đã có đề xuất một kiến trúc hệ thống tổng thể bao gồm hai khối chức năng hỗ trợ lẫn nhau trong việc giám sát và phân tích hành vi người dùng, đó là Mô hình chức năng Kiểm soát truy cập và Mô hình chức năng Giám sát tuân thủ.

Mô hình chức năng kiểm soát truy cập (Access Control Architecture)

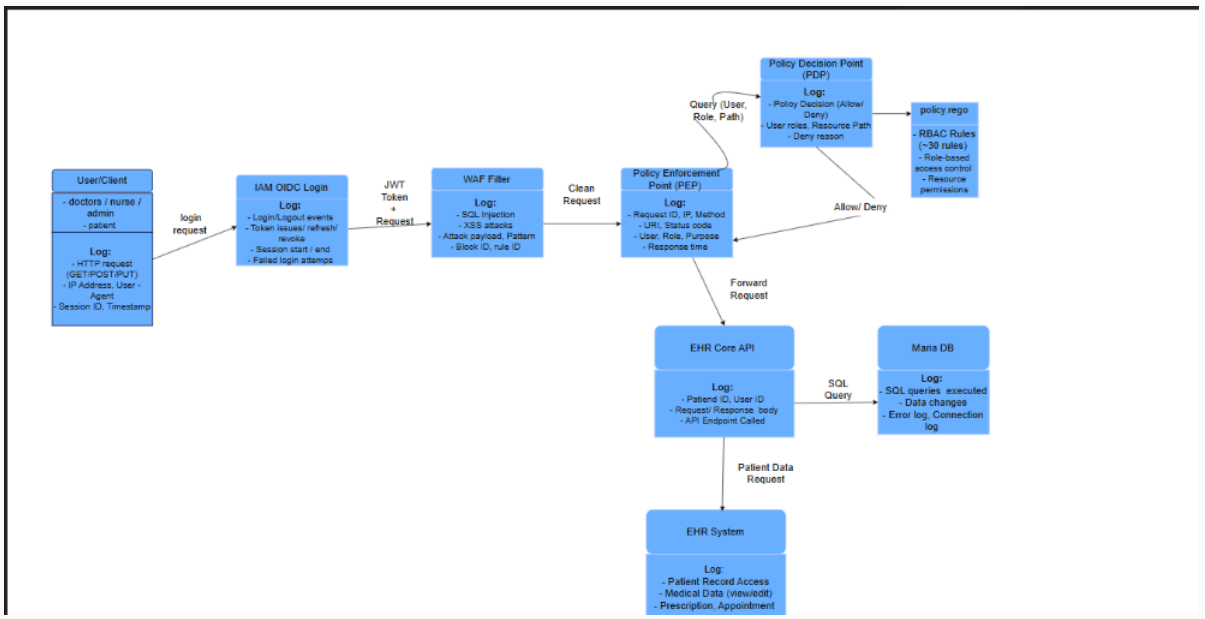


Figure 3.1.1. Hình ảnh sơ đồ mô tả cách vận hành của mô hình kiểm soát truy cập

Trên đây là sơ đồ mô tả toàn bộ quy trình xử lý một yêu cầu truy cập người dùng (Doctors, Nurse, Admin) được thiết kế qua các lớp bảo vệ tuần tự như sau: Đầu tiên là lớp định danh và xác thực (IAM Authentication). Đây là lớp đầu tiên mà người dùng truy cập vào EHR phải đi qua. Khi bác sĩ hoặc y tá mở trình duyệt và truy cập vào hệ thống, họ sẽ thấy giao diện đăng nhập có yêu cầu tên đăng nhập và mật khẩu. Hệ thống IAM sử dụng Keycloak để thực hiện sẽ xác thực thông tin đăng nhập dựa trên cơ sở dữ liệu người dùng đã được tạo sẵn trong keycloak. Nếu thông tin xác thực đúng, Keycloak sẽ cấp cho người dùng một mã JSON Web Token. Token này sẽ chứa các thông tin quan trọng của người truy cập như: tên người dùng, vai trò người truy cập là gì, khoa làm việc,...Mọi yêu

cầu truy cập dữ liệu sau đó của người dùng này đều phải đính kèm token này để có thể chứng minh được danh tính và hành vi.

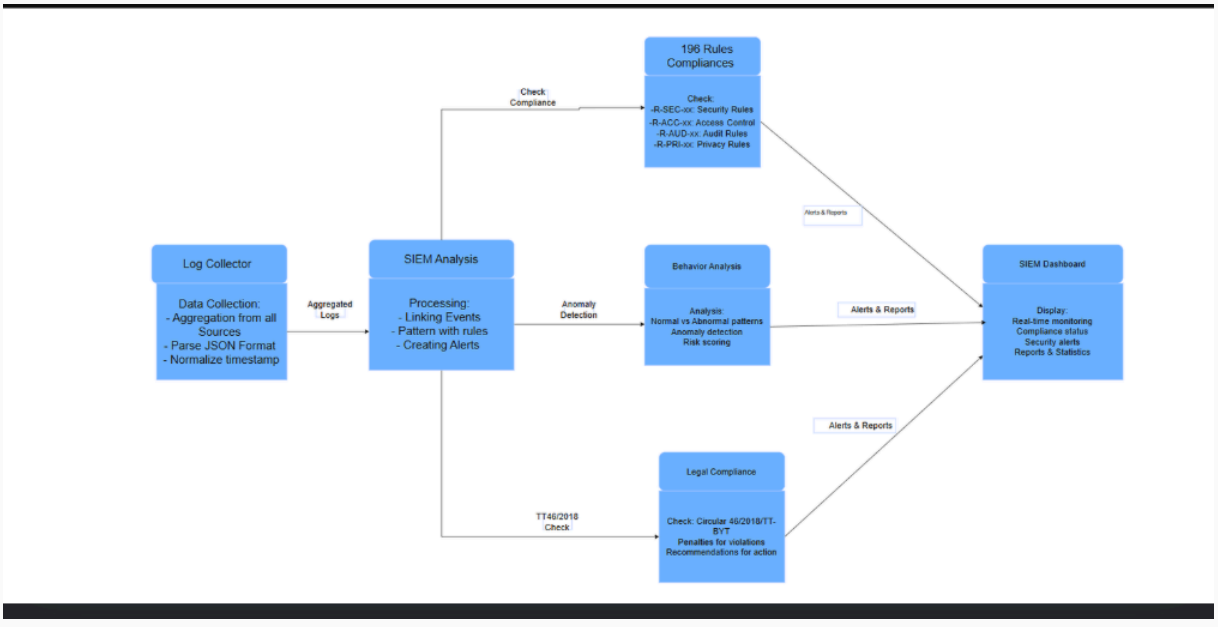
Tiếp theo là lớp Lọc tấn công ứng dụng (WAF Filter). Sau khi người dùng đã có JSON Web Token được cấp phát ở lớp đăng nhập thì các yêu cầu truy cập dữ liệu của họ đều được gửi đến hệ thống giám sát. Tuy nhiên, trước khi yêu cầu của họ có thể đến được dữ liệu hồ sơ bệnh án của bệnh nhân thì nó phải đi qua bộ lọc Web Application Firewall hay còn được gọi là lớp tường lửa của hệ thống. Việc tăng cường thêm WAF vào hệ thống nhằm kiểm tra xem trong yêu cầu của người dùng có chứa các đoạn mã độc hại hay không. Ví dụ như nếu có kẻ tấn công cố tình chèn câu lệnh SQL vào ô đăng nhập hay những lệnh SQL phức tạp hoặc chèn mã JavaScript độc hại (XSS) thì bộ lọc WAF sẽ phát hiện và ngăn chặn ngay lập tức, không cho yêu cầu đó tiếp tục đi vào trong dữ liệu. Từ đó sẽ giúp cho hệ thống được tăng cường an ninh hơn bởi vì chỉ có những yêu cầu đảm bảo an toàn mới được phép tiếp cận đến lớp sau.

Kế tiếp là lớp quan trọng nhất trong toàn bộ hệ thống kiểm soát đó là lớp thực thi chính sách truy cập (PEP- Policy Enforcement Point). Sau khi một yêu cầu an toàn được WAF cho qua thì nó tiến đến lớp bảo vệ thứ hai là PEP, hệ thống sẽ tạm dừng yêu cầu của người dùng và đặt ra một câu hỏi để xác thực quyền của người dùng sau khi đã xác thực danh tính của họ thành công ở lớp đăng nhập. Để trả lời cho câu hỏi đó thì PEP sẽ trích xuất các thông tin ngữ cảnh theo mô hình (ABAC) bao gồm: Ai đang yêu cầu (User) ? Họ muốn làm gì ? (Method: GET/POST) ? Họ muốn xem hồ sơ của bệnh nhân nào ? và yêu cầu được gửi trong khoảng thời gian nào (Timestamp) ? Toàn bộ những thông tin này sẽ được đóng gói và gửi đến Điểm quyết định thực thi chính sách (PDP - Policy Decision Point), khối chức năng PDP sẽ tiến hành đối chiếu những thông tin này với tập luật Policy.rego bao gồm khoảng 30 luật xác thực phân quyền và ngữ cảnh đã được định nghĩa sẵn, ví dụ: Bác sĩ Khoa nội chỉ được xem hồ sơ bệnh nhân thuộc Khoa nội trong giờ hành chính. Nếu thông tin đó khớp với luật thì PDP sẽ

trả về kết quả cho PEP là Allow. Còn nếu vi phạm bất kì điều kiện nào thì PDP trả về Deny và kèm lý do cụ thể.

Cuối cùng là lớp Truy xuất dữ liệu (EHR Core và Database): Chỉ khi yêu cầu được chấp nhận Allow từ PDP, nó mới được PEP chuyển tiếp đến lõi ứng dụng EHR Core API. Tại đây, ứng dụng sẽ thực hiện truy vấn mà người dùng yêu cầu đến cơ sở dữ liệu Maria DB để lấy chính xác thông tin bệnh nhân đó. Dữ liệu sau đó sẽ được trả về cho người dùng thông qua giao diện web. Đồng thời, mọi yêu cầu hoặc hành động thao tác của người dùng truy cập vào EHR đều được ghi lại vào bảng nhật ký access_log để phục vụ cho việc kiểm toán sau này. Nếu yêu cầu bị Deny, thì người dùng sẽ nhận được thông báo "Từ chối truy cập" và hệ thống sẽ ghi nhận sự kiện này như một cảnh báo an ninh để quản trị viên xem xét.

Song song với quá trình kiểm soát truy cập của người dùng dựa trên danh tính và ngữ cảnh thì chúng tôi triển khai ra được một hệ thống giám sát độc lập hoạt động liên tục ở chế đo



REFERENCES

[1] thuvienphapluat.vn – Quyet dinh 5349 QD BYT 2019 phe duyet Ke hoach trien khai ho so suc khoe dien tu 428071. https://thuvienphapluat.vn/van-ban/The-thao-Y-te/Quyet-dinh-5349-QD-BYT-2019-phe-duyet-Ke-hoach-trien-khai-ho-so-suc-khoe-dien-tu-428071.aspx

[2] xaydungchinhsach.chinhphu.vn – nhung diem moi quan trong trong luat kham benh chua benh sua doi 119230203112956887. https://xaydungchinhsach.chinhphu.vn/nhung-diem-moi-quan-trong-trong-luat-kham-benh-chua-benh-sua-doi-119230203112956887.htm

[3] vanban.chinhphu.vn. https://vanban.chinhphu.vn/?pageid=27160&docid=205022

[4] baohiemxahoi.gov.vn – hoat dong bo nganh lien quan. https://baohiemxahoi.gov.vn/tintuc/Pages/hoat-dong-bo-nganh-lien-quan.aspx?CateID=0&ItemID=23491

[5] chiefhealthcareexecutive.com – small hospitals and clinics emerge as big targets for cyberattacks. https://www.chiefhealthcareexecutive.com/view/small-hospitals-and-clinics-emerge-as-big-targets-for-cyberattacks

[6] ruralhealthinfo.org – cybersecurity attacks. https://www.ruralhealthinfo.org/rural-monitor/cybersecurity-attacks

[7] cyberinsurancenews.org – healthcare cybersecurity medicaid cuts small hospitals 2025.

https://cyberinsurancenews.org/healthcare-cybersecurity-medicaid-cuts-small-hospitals-2025/

[8] chinhphu.vn – default.
https://chinhphu.vn/default.aspx?pageid=27160&docid=193779

[9] ncsgroup.vn – rhysida tuyen bo tan cong ransomware vao prospect medical de doa ban du lieu.
https://ncsgroup.vn/rhysida-tuyen-bo-tan-cong-ransomware-vao-prospect-medical-de-doa-ban-du-lieu/

[10] ponemonsullivanreport.com – the protected health information crisis in healthcare.
https://ponemonsullivanreport.com/2024/05/the-protected-health-information-crisis-in-healthcare/

[11] blackbookmarketresearch.com – 2024 State of the Cybersecurity Industry 01 12 23.
https://blackbookmarketresearch.com/images/2024-State-of-the-Cybersecurity-Industry-01-12-23.pdf

[12] claroty.com – Clarotys state of cps security report healthcare exposures 2025.
https://claroty.com/blog/clarotys-state-of-cps-security-report-healthcare-exposures-2025

[13] nvlpubs.nist.gov – nistspecialpublication800 92.
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

[14] dl.acm.org – 984334.984339.
https://dl.acm.org/doi/epdf/10.1145/984334.984339

[15] ahima.org – healthcare data governance practice brief final.
https://www.ahima.org/media/pmcb0fr5/healthcare-data-governance-practice-brief-final.pdf

[16] enisa.europa.eu – ENISA Report Cybersecurity for SMES Challenges and Recommendations. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cybersecurity%20for%20SMES%20Challenges%20and%20Recommendations.pdf

[17] link.springer.com – s13677 025 00831 z. https://link.springer.com/article/10.1186/s13677-025-00831-z

[18] mdpi.com – 11 4 98. https://www.mdpi.com/2227-9709/11/4/98

[19] thuvienphapluat.vn – Nghi dinh 13 2023 ND CP bao ve du lieu ca nhan 465185. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx

[20] link.springer.com – s12910 022 00758 z. https://link.springer.com/article/10.1186/s12910-022-00758-z

[21] U.S. Department of Health & Human Services, 45 CFR § 164.312 - Technical safeguards, HIPAA Security Rule. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

[22] ISO, ISO 27799 - Health informatics - Information security management in health, International Organization for Standardization. https://www.iso.org/standard/62777.html

[23] NIST, SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations, 2020. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[24] NIST, SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, 2011. https://csrc.nist.gov/publications/detail/sp/800-137/final

[25] Government of Vietnam, Decree No. 13/2023/ND-CP on personal data protection, 2023. https://vanban.chinhphu.vn/?classid=0&docid=207759&pageid=27160 (Alternative PDF: https://files.thuvienphapluat.vn/uploads/FileLargeTemp/2023/4/17/13_2023_ND-CP_465185.pdf)

[26] Vietnam National Assembly, Law No. 24/2018/QH14 (Cybersecurity Law), 2018. https://vanban.chinhphu.vn/?docid=206114&pageid=27160 (Alternative: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx)

[27] Government of Vietnam, Decree No. 53/2022/ND-CP detailing a number of articles of the Cyber Security Law, 2022. https://vanban.chinhphu.vn/?classid=1&docid=206381&orggroupid=2&pageid=27160 (Alternative: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-53-2022-ND-CP-huong-dan-Luat-An-ninh-mang-398695.aspx)

[28] Ministry of Health, Circular 46/2018/TT-BYT regulating the use and management of electronic medical records, 2018. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Thong-tu-46-2018-TT-BYT-su-dung-va-quan-ly-ho-so-benh-an-dien-tu-391438.aspx

[29] HL7, FHIR Specification (R4/R4B/R5), Health Level Seven International. https://hl7.org/fhir/

[30] HL7, SMART on FHIR, Health Level Seven International. https://www.hl7.org/fhir/smart-app-launch/

[31] HL7, FHIR Resource: AuditEvent, Health Level Seven International. https://hl7.org/fhir/auditevent.html

[32] INCITS, ANSI INCITS 359-2012: Role Based Access Control, 2012. https://www.incits.org/standards/all-standards

[33] NIST, SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014. https://csrc.nist.gov/publications/detail/sp/800-162/final

[34] Open Policy Agent, OPA Documentation - Policy as Code, Open Policy Agent Project. https://www.openpolicyagent.org/docs/latest/

[35] IETF, RFC 6749: The OAuth 2.0 Authorization Framework, 2012. https://datatracker.ietf.org/doc/html/rfc6749

[36] OpenID Foundation, OpenID Connect Core 1.0, 2014. https://openid.net/specs/openid-connect-core-1_0.html

[37] IETF, RFC 7519: JSON Web Token (JWT), 2015. https://datatracker.ietf.org/doc/html/rfc7519

[38] Keycloak, Keycloak Documentation, Keycloak Project. https://www.keycloak.org/documentation

[39] NIST, SP 800-92: Guide to Computer Security Log Management, 2006. https://csrc.nist.gov/publications/detail/sp/800-92/final

[40] González-Granadillo, G.; González-Zarzosa, S.; Diaz, R., Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures, Sensors, vol. 21, no. 14, 4759, 2021. DOI: 10.3390/s21144759. https://doi.org/10.3390/s21144759

[41] López Velásquez, J.M.; Martínez Monterrubio, S.M.; Sánchez Crespo, L.E.; Garcia Rosado, D., Systematic review of SIEM technology: SIEM-SC birth, International Journal of Information Security, vol. 22, pp. 691–711, 2023. DOI: 10.1007/s10207-022-00657-9. https://doi.org/10.1007/s10207-022-00657-9

[42] Schneier, B.; Kelsey, J., Secure Audit Logs to Support Computer Forensics, ACM Transactions on Information and System Security, vol. 2, no. 2, pp. 159–176, 1999. https://doi.org/10.1145/317087.317092

[43] Ma, D.; Tsudik, G., A New Approach to Secure Logging, IACR Cryptology ePrint Archive, Report 2008/185, 2008. https://eprint.iacr.org/2008/185

[44] IETF, RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), 2001. https://datatracker.ietf.org/doc/html/rfc3161

[45] Verizon. (2024). Data Breach Investigations Report (DBIR) 2024. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[46] Jiang, J. X., Ross, J. S., & Bai, G. (2025). Ransomware attacks and data breaches in U.S. health care systems. JAMA Network Open, 8(5), e2510180. https://doi.org/10.1001/jamanetworkopen.2025.10180

[47] Munoz Cornejo, G., Lee, J., & Russell, B. A. (2024). A thematic analysis of ransomware incidents among United States hospitals, 2016–2022. Health and Technology, 14, 1059–1070. https://doi.org/10.1007/s12553-024-00890-3

[48] Government Electronic Information Portal, 100% of hospitals must deploy electronic medical records before October 2025, March 19, 2025. https://baochinhphu.vn/100-benh-vien-phai-trien-khai-benh-an-dien-tu-truoc-thang-10-2025-102250319135405888.htm

[49] Ministry of Health, Decision 1150/QD-BYT dated April 3, 2025 approving the Plan to deploy electronic medical records, 2025. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-1150-QD-BYT-2025-phe-duyet-Ke-hoach-trien-khai-ho-so-benh-an-dien-tu-650763.aspx

[50] Ministry of Health, Decision 326/QD-BYT dated February 7, 2024 promulgating the Regulations on ensuring information security and network security of the Ministry of Health, 2024. https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-326-QD-B

YT-2024-Quy-che-dam-bao-an-toan-thong-tin-an-ninh-mang-cua-Bo-Y-te-638785.aspx

[51] Viettel Threat Intelligence, Situation of information security risks in Vietnam in the first quarter of 2024, 2024. https://viettel.com.vn/media/viettel/documents/Final_Tinh_hinh_nguy_co_mat_ATTT_tai_Viet_Nam_quy_1_nam_2024_1.pdf

[52] Tran, D. M., Thwaites, C. L., Van Nuil, J. I., et al., Digital Health Policy and Programs for Hospital Care in Vietnam: Scoping Review, Journal of Medical Internet Research, 2022;24(2):e32392. https://doi.org/10.2196/32392

[53] Rule, A., Melnick, E. R., & Apathy, N. C., Using event logs to observe interactions with electronic health records: an updated scoping review shows increasing use of vendor-derived measures. Journal of the American Medical Informatics Association, 2023;30(1):144-156. https://academic.oup.com/jamia/article/30/1/144/6730799

[54] United Nations Development Programme (UNDP), Enhancing Digital Transformation in the Health Sector in Viet Nam: A Case Study on Application of Electronic Health Records in Lang Son, Binh Thuan and Tay Ninh Provinces, 2024. https://www.undp.org/vietnam/publications/enhancing-digital-transformation-health-sector-viet-nam-case-study-application-electronic-health-records-lang-son-binh-thuan-and

[55] World Economic Forum (PHSSR), Sustainability and Resilience in the Vietnamese Health System, PHSSR country report, 2021. https://www3.weforum.org/docs/WEF_PHSSR_Vietnam_Report.pdf

[56] Thwaites, C. L., Tran, D. M., et al., Status of Digital Health Technology Adoption in 5 Vietnamese Hospitals and Their Needs for Digital

Transformation: Cross-Sectional Assessment. JMIR Formative Research, 2025;9:e53483. https://formative.jmir.org/2025/1/e53483