การประยุกต์ใช้แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท ร่วมกับการพัฒนาระบบสารสนเทศด้วยลาราเวลเฟรมเวิร์ก เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูล

ทศพล งามวิชชุกร* และ ศันสนีย์ สุ่มกล่ำ[2]

รับบทความ 16 ธันวาคม 2567 แก้ไขบทความ 13 พฤษภาคม 2568 ตอบรับบทความ 28 พฤษภาคม 2568

บทคัดย่อ

การควบคุมสิทธิ์การเข้าถึงข้อมูลในระบบสารสนเทศเป็นเรื่องสำคัญที่นักวิเคราะห์ออกแบบและพัฒนาระบบสารสนเทศต้องคำนึงถึง ผู้ใช้งานระบบสารสนเทศควรเข้าถึงข้อมูลได้เฉพาะตามบทบาทของตนเองเท่านั้น เพื่อสร้างความมั่นคงปลอดภัยให้กับข้อมูลในระบบสารสนเทศและเพื่อสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีหลักการสำคัญในการคุ้มครองข้อมูลส่วนบุคคลของเจ้าของข้อมูล และกำหนดให้ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจโดยมิชอบ แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control: RBAC) จึงถูกนำมาประยุกต์ใช้ในการออกแบบโครงสร้างฐานข้อมูลและพัฒนาระบบสารสนเทศร่วมกับลาราเวลเฟรมเวิร์กที่มีคุณลักษณะรองรับการพัฒนาระบบสารสนเทศในเรื่องการเข้าถึงระบบตามสิทธิ์ที่กำหนด ทำให้สามารถพัฒนาระบบสารสนเทศในเรื่องการเข้าถึงระบบตามสิทธิ์บทฐานบทบาทได้สะดวกรวดเร็วและถูกต้อง ส่งผลให้ผู้ควบคุมข้อมูลของระบบสารสนเทศนั้นสามารถบริหารจัดการสิทธิ์ในการเข้าถึงข้อมูลในระบบสารสนเทศให้เป็นไปตามระดับสิทธิ์การใช้งานในแต่ละบทบาท ทำให้มีความยืดหยุ่น รองรับการปรับเปลี่ยนโยกย้ายบทบาทของบุคลากรที่เป็นผู้ใช้งานระบบสารสนเทศ สร้างความมั่นคงปลอดภัย และป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตให้กับข้อมูลในระบบสารสนเทศได้อย่างมีประสิทธิภาพ

คำสำคัญ: แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท; การบริหารจัดการสิทธิ์เข้าถึงข้อมูล; การพัฒนาระบบสารสนเทศด้วยลาราเวลเฟรมเวิร์ก

นักวิชาการคอมพิวเตอร์ ภาควิชาอายุรศาสตร์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

*ผู้ประสานงานหลัก: tossapon.nga@mahidol.ac.th

Secure Data Access Management in Information Systems Using Role-Based Access Control with Laravel Framework

Tossapon Ngamwitchukorn* and Sansanee Sumklam

Received 16 December 2024.; Revised 13 May 2025; Accepted 28 May 2025

Abstract

Access control in information systems is a critical aspect that system analysts and developers must carefully consider. Users should be granted access to information strictly based on their roles, in order to ensure data security and comply with the Personal Data Protection Act B.E. 2562 (2019). This law emphasizes the protection of personal data and mandates that data controllers implement appropriate security measures to prevent the unauthorized loss, access, use, alteration, modification, or disclosure of personal data.The concept of Role-Based Access Control (RBAC) has therefore been applied in the design of database structures and the development of information systems. When integrated with the Laravel framework which supports role-based access control system development becomes more efficient, accurate, and streamlined. This integration enables the system administrator to manage user access rights according to defined role levels. It also provides flexibility in adapting to personnel role changes and ensures robust data protection by preventing unauthorized access to sensitive information within the system.

Keywords: Role-Based Access Control; Access Rights Management; Information System Development with Laravel Framework

Computer Technical Officer, Department of Medicine, Faculty of Medicine, Siriraj Hospital, Mahidol University
*Corresponding Author: tossapon.nga@mahidol.ac.th

บทนำ

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีผลบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน พ.ศ. 2565 ได้กำหนดบุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ประกอบด้วย เจ้าของข้อมูลส่วนบุคคล (Data Subject) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) และมีประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 โดยเนื้อหาส่วนหนึ่งได้กำหนดให้มีการบริหารจัดการสิทธิ์การเข้าถึงตามสิทธิ์ (management of privileged access rights) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (review of user access rights) และการถอดถอนหรือปรับปรุงสิทธิ์การเข้าถึง (removal or adjustment of access rights) ซึ่งนักวิชาการคอมพิวเตอร์ผู้ได้รับมอบหมายจากผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) ให้มีหน้าที่พัฒนาระบบสารสนเทศและประมวลผลข้อมูลส่วนบุคคลในระบบสารสนเทศอยู่ในฐานะผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) จำเป็นต้องศึกษาเทคนิคหรือแนวคิดทฤษฎีที่สอดคล้องกับกฎหมาย ระเบียบ ประกาศข้อบังคับภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แล้วนำไปประยุกต์ใช้พัฒนาปรับปรุงระบบสารสนเทศจนสำเร็จตามที่ได้รับมอบหมาย

แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control: RBAC) คือ แนวคิดในการกำหนดสิทธิ์โดยใช้บทบาทของผู้ใช้งาน ซึ่งจะมีส่วนประกอบ 3 ส่วน คือ ผู้ใช้ (User) บทบาท (Role) และสิทธิ์ (Permission) ซึ่งแนวคิดการควบคุมการเข้าถึงบนฐานบทบาทไม่ได้กำหนดสิทธิ์ให้กับผู้ใช้โดยตรง แต่จะกำหนดสิทธิ์ให้กับบทบาทว่าสามารถมีสิทธิ์ใดบ้าง โดยผู้ใช้จะถูกกำหนดบทบาทให้อย่างน้อย 1 บทบาท หรือมากกว่า โดยบทบาทสามารถสืบทอดได้ (inherited) และให้ส่วนของการกำหนดสิทธิ์สามารถทำการเปลี่ยนแปลงได้ง่าย โดยจะส่งผลให้กับผู้ใช้ทุกคนภายใต้บทบาทที่ได้ทำการเปลี่ยนแปลง (จิตติภัทร ผสมทรัพย์, 2563) จึงเป็นแนวคิดที่สอดคล้องกับข้อกำหนดในมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ในเรื่องการบริหารจัดการสิทธิ์การเข้าถึงตามสิทธิ์ และสอดคล้องกับบริบทบทบาทและสิทธิ์ที่ผู้ใช้งานระบบต้องการ

ลาราเวลเฟรมเวิร์ก (Laravel Framework) เป็นเฟรมเวิร์ก PHP แบบโอเพ่นซอร์สที่ออกแบบมาเพื่อทำให้การพัฒนาเว็บแอปพลิเคชันสามารถทำได้ง่าย มีประสิทธิภาพ และมีคุณภาพ สำหรับนักพัฒนาทุกระดับ โดยมีคุณสมบัติหรือเครื่องมือสำหรับการพัฒนาระบบที่สมบูรณ์แบบ ซึ่งรวมทุกสิ่งที่นักพัฒนาเว็บแอปพลิเคชันต้องการไว้ในที่เดียว ด้วยชุดเครื่องมือที่หลากหลาย เช่น dependency injection, an expressive database abstraction layer, queues and scheduled jobs, unit and integration testing เป็นต้น และมีชุดเครื่องมือเริ่มต้นอย่าง Laravel Breeze หรือ Laravel Jetstream ที่ทำให้สามารถเริ่มต้นพัฒนาแอปพลิเคชันได้อย่างรวดเร็ว พร้อมโครงสร้างที่ยืดหยุ่นและสามารถขยายต่อได้ง่าย

แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control: RBAC)

Role-Based Access Control: RBAC คือ การควบคุมการเข้าถึงโดยแบ่งตามบทบาทหน้าที่ ประกอบด้วยส่วนประกอบ 3 ส่วน คือ ผู้ใช้ (User) บทบาท (Role) และสิทธิ์ (Permission) ซึ่ง RBAC ไม่ได้กำหนดสิทธิ์ให้กับผู้ใช้โดยตรง แต่จะกำหนดสิทธิ์ให้กับบทบาทว่าสามารถมีสิทธิ์ใดบ้าง โดยผู้ใช้จะถูกกำหนดบทบาทให้อย่างน้อย 1 บทบาท หรือมากกว่า โดยบทบาทสามารถสืบทอดได้ (inherited) และให้ส่วนของการกำหนดสิทธิ์สามารถทำการเปลี่ยนแปลงได้ง่าย โดยจะส่งผลให้กับผู้ใช้ทุกคนภายใต้บทบาทที่ได้ทำการเปลี่ยนแปลง (จิตติภัทร ผสมทรัพย์, 2563)

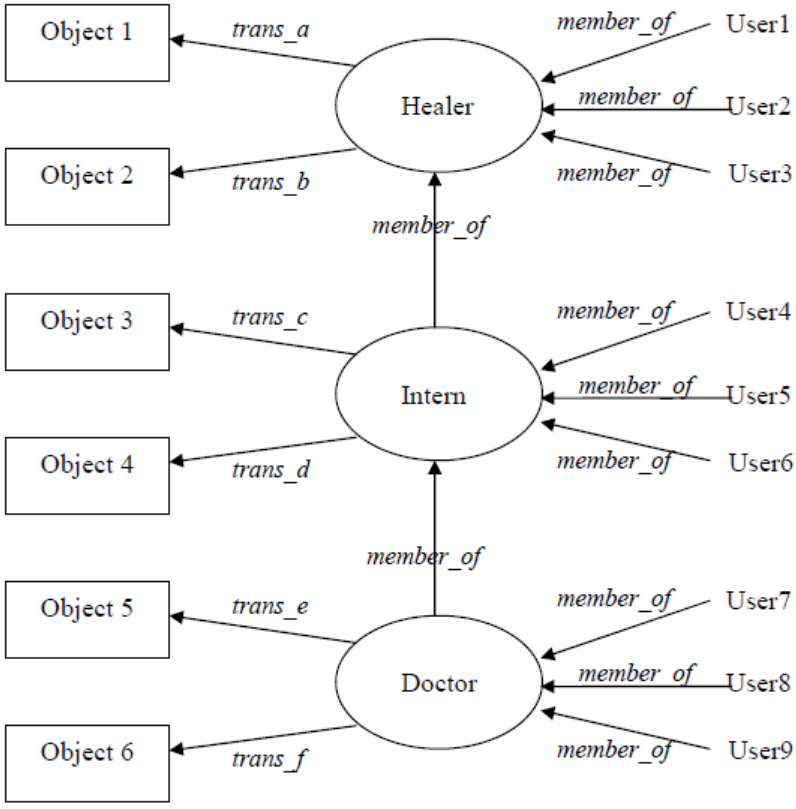
การควบคุมการเข้าถึงบนพื้นฐานของบทบาท (Role-Based Access Control: RBAC) ถือเป็นแนวทางที่มีศักยภาพในการบริหารจัดการชุดสิทธิ์การเข้าถึง โดยมีความสะดวกในการดูแลและบำรุงรักษา ได้ถือกำเนิดขึ้นตั้งแต่ช่วงทศวรรษ 1970 ในระบบออนไลน์ที่มีผู้ใช้และแอปพลิเคชันจำนวนมาก โดยมอบสิทธิ์การเข้าถึงให้กับ “บทบาท” แทนการกำหนดสิทธิ์ให้แก่ “ผู้ใช้” โดยตรง และผู้ใช้จะได้รับสิทธิ์ผ่านการสวมบทบาทที่ตนได้รับมอบหมาย (Jaibir Singh, Suman Rani & Vipin Kumar, 2024)

เอกสารบทความตีพิมพ์เรื่อง Role-Based Access Control ที่เขียนโดย David F.Ferraiolo , D. Richard Kuhn ถูกเผยแพร่โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ในการประชุม 15th National Computer Security Conference (NCSC) ที่จัดขึ้นเมื่อวันที่ 13-16 ตุลาคม 2535 ที่ Baltimore, Maryland, United States. เขียนอธิบายไว้ดังนี้

RBAC (Role-Based Access Control) มีความยืดหยุ่นในด้านนโยบายและโครงสร้างขององค์กร ซึ่งหนึ่งในข้อดีที่ดีที่สุดก็คือ ความสามารถในการบริหารจัดการ

เมื่อบทบาทถูกกำหนดภายในระบบแล้ว บทบาทเหล่านี้มักจะค่อนข้างคงที่หรือเปลี่ยนแปลงช้าเมื่อเวลาผ่านไป งานบริหารคือการมอบและเพิกถอนการเป็นสมาชิกของบทบาทที่ระบุไว้ในระบบ เมื่อมีคนใหม่เข้ามาในองค์กร ผู้ดูแลระบบเพียงแค่มอบการเป็นสมาชิกให้กับบทบาทที่มีอยู่ เมื่อบทบาทของบุคคลเปลี่ยนแปลง การเป็นสมาชิกในบทบาทเดิมสามารถลบออกได้ง่ายและมอบบทบาทใหม่ได้ ในที่สุดเมื่อบุคคลออกจากองค์กร การเป็นสมาชิกในทุกบทบาทจะถูกลบออก ซึ่งสำหรับองค์กรที่มีการหมุนเวียนบุคลากรสูง นโยบายความปลอดภัยที่อิงตามบทบาทจึงเป็นทางเลือกที่สมเหตุสมผลที่สุด (David F.Ferraiolo & D. Richard Kuhn, 1992)

ตัวอย่าง องค์กรโรงพยาบาลมีผู้ที่มีบทบาทในการรักษาหลายบทบาท เช่น ผู้บำบัด (Healer), แพทย์ฝึกหัด (Intern), แพทย์ (Doctor) เป็นต้น



ภาพที่ 1 Multiple-Role relationships

หมายเหตุ. จาก “Role-Base Access Controls”, David F.Ferraiolo & D. Richard Kuhn, 1992, p. 8 (https://csrc.nist.gov/files/pubs/conference/1992/10/13/rolebased-access-controls/final/docs/ferraiolo-kuhn-92.pdf)

จากภาพที่ 1 การให้สิทธิ์การเป็นสมาชิกแก่บทบาทแพทย์ หมายความว่าสามารถเข้าถึงธุรกรรมทั้งหมดที่กำหนดโดยบทบาทแพทย์ฝึกหัดและบทบาทผู้บำบัด รวมถึงธุรกรรมของแพทย์ด้วย ในทางกลับกัน การให้สิทธิ์การเป็นสมาชิกแก่บทบาทแพทย์ฝึกหัดและบทบาทผู้บำบัด จะไม่สามารถเข้าถึงธุรกรรมของแพทย์ได้ และการให้สิทธิ์การเป็นสมาชิกแก่บทบาทผู้บำบัดหมายความว่าเข้าถึงทรัพยากรที่ได้รับอนุญาตภายใต้บทบาทผู้บำบัดเท่านั้น

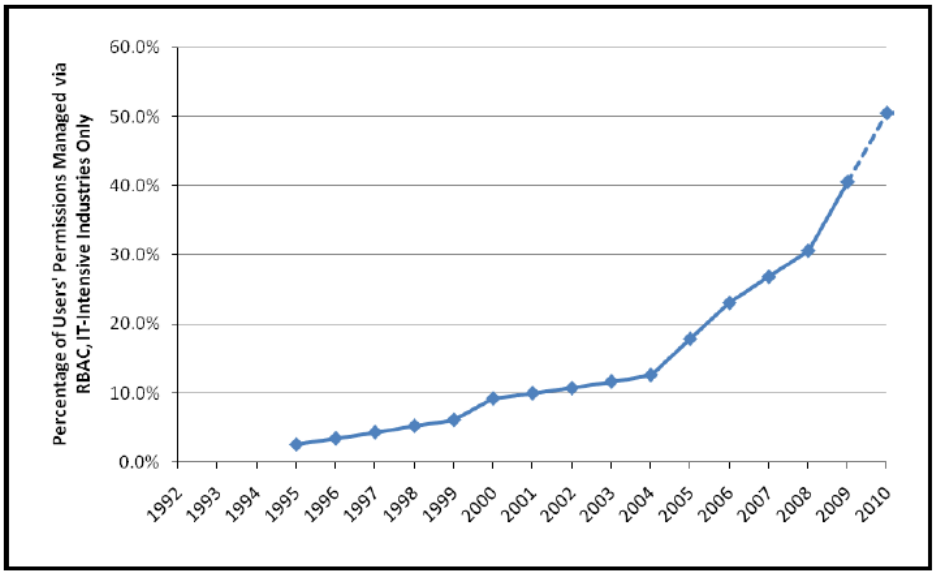
ในปี พ.ศ. 2553 มีการเผยแพร่เอกสารผลการศึกษาการนำแนวคิด Role-Based Access Control ไปประยุกต์ใช้งานในองค์กรต่าง ๆ มากมาย จากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology: NIST) ที่แสดงให้เห็นว่า Role-Based Access Control: RBAC ได้รับการยอมรับว่าเป็นการทำให้การบริหารการเข้าถึงง่ายขึ้นและเพิ่มความชัดเจนทั้งในนโยบายการควบคุมการเข้าถึงและโครงสร้างขององค์กร ดังนี้

เมื่อผู้ใช้เปลี่ยนตำแหน่งภายในองค์กร การจัดเตรียมสิทธิ์จะง่ายขึ้นโดยการมอบหมายบทบาทที่เหมาะสมให้กับผู้ใช้ แทนการมอบหมายสิทธิ์ทั้งหมดให้กับผู้ใช้

การถอดสิทธิ์ (deprovisioning) จะเป็นอัตโนมัติโดยการลบบทบาทที่ไม่เกี่ยวข้องกับตำแหน่งใหม่ของผู้ใช้ ผู้ดูแลระบบสารสนเทศเพียงแค่ต้องปรับปรุงสิทธิ์ใหม่ให้กับบทบาทที่เหมาะสม และสิทธิ์เหล่านั้นจะถูกส่งต่อไปยังผู้ใช้ที่เกี่ยวข้องทั้งหมดผ่านบทบาท

การตรวจสอบนโยบายการควบคุมการเข้าถึงจะทำได้ง่ายขึ้น เนื่องจากบทบาทต่าง ๆ อาจมีข้อมูลผู้ใช้และสิทธิ์อยู่ในที่เดียวกัน การเข้าใจนโยบายการควบคุมการเข้าถึงที่บังคับใช้ในองค์กรในปัจจุบันเป็นสิ่งสำคัญในการระบุภัยคุกคามด้านความปลอดภัย และอาจช่วยในการรับรองและการตรวจสอบที่กฎหมายกำหนด (Alan C. O'Connor & Ross J. Loomis, 2010)

การสำรวจแนวโน้มการใช้บทบาทและแนวทางนโยบายการควบคุมการเข้าถึง ตามแนวคิด Role-Based Access Control ดังภาพที่ 2



ภาพที่ 2 RBAC Adoption, 1992–2010

หมายเหตุ: สำรวจในอุตสาหกรรมต่าง ๆ ที่ถูกกำหนดโดยรหัส NAICS 2 หลัก ได้แก่ สาธารณูปโภค การผลิต การค้าส่ง การค้าปลีก ข้อมูล การเงินและการประกันภัย บริการด้านวิชาชีพ วิทยาศาสตร์และเทคนิค บริการด้านการศึกษา การดูแลสุขภาพและความช่วยเหลือทางสังคม ศิลปะ ความบันเทิงและสันทนาการ บริการอื่น ๆ และการบริหารสาธารณะ

หมายเหตุ. จาก "2010 Economic Analysis of Role-Based Access Control Final Report", Alan C. O'Connor & Ross J. Loomis, 2010, p. 14 (https://csrc.nist.gov/files/pubs/other/2010/12/19/economic-analysis-of-rbac-final-report/final/docs/20101219_rbac2_final_report.pdf)

ผลการสำรวจระบุว่าการใช้บทบาทมีการเติบโตอย่างต่อเนื่องตั้งแต่ปี 1994 โดยอัตราการนำ RBAC มาใช้เพิ่มขึ้นอย่างรวดเร็วในปี 2004 และอีกครั้งในปี 2008 (Alan C. O'Connor & Ross J. Loomis, 2010)

วิทยานิพนธ์เรื่องการพิสูจน์ตัวจริงอิงบทบาทสำหรับเว็บเซอร์วิสองค์กร พ.ศ. 2558 สรุปผลการวิจัยไว้ว่า บริการพิสูจน์ตัวจริงเป็นสิ่งจำเป็นสำหรับการใช้งานกับบริการต่าง ๆ ที่มีการให้บริการผ่านอินเทอร์เน็ต ไม่ว่าจะเป็นเว็บไซต์ทั่วไป เว็บเซอร์วิส เว็บแอปพลิเคชัน หรือแม้แต่แอปพลิเคชันบนโทรศัพท์มือถือในปัจจุบัน เพื่อใช้เป็นเครื่องมือในการเข้าสู่ระบบสำหรับให้ผู้ใช้งานเข้าถึงบริการที่มีไว้ให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงเท่านั้น อีกส่วนหนึ่งเป็นการรักษาความปลอดภัยของข้อมูลหรือเอกสารต่าง ๆ ซึ่งในงานวิจัยนี้ได้นำแนวคิดการพัฒนาบริการพิสูจน์ตัวจริงอิงบทบาท โดยนำแบบจำลอง Role-Based Access Control เข้ามาเป็นแนวทางในการจัดการการอนุญาตการใช้งานต่าง ๆ ของเว็บเซอร์วิส เพื่อการกำหนดการอนุญาตได้ละเอียดมากขึ้น (ภูวนาถ กอบคำ, 2558)

ในปี 2024 Marquis Yewande Alice ได้ศึกษาเรื่องการประยุกต์ใช้กลยุทธ์การควบคุมการเข้าถึงตามบทบาทอย่างมีประสิทธิภาพเพื่อลดความเสี่ยงจากบุคคลภายใน ในบริบทองค์กรที่หลากหลาย ผลการศึกษาพบว่า Role-Based Access Control (RBAC) มีประสิทธิภาพในการลดการเข้าถึงโดยไม่ได้รับอนุญาตและการรั่วไหลของข้อมูล จึงสามารถลดความเสี่ยงจากภัยคุกคามภายในได้อย่างมีนัยสำคัญ

ในปี 2025 Surendra and Vitla ได้ศึกษาเรื่องการควบคุมการเข้าถึงตามบทบาท (RBAC) และผลกระทบต่อนโยบายความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ผลการศึกษาพบว่า การควบคุมการเข้าถึงตามบทบาท (RBAC) เป็นกลไกที่มีประสิทธิภาพและทรงพลังในการจัดการการเข้าถึงทรัพยากรที่สำคัญภายในองค์กร ช่วยลดความเสี่ยงต่าง ๆ เช่น การเข้าถึงที่ไม่ได้รับอนุญาต ภัยคุกคามจากบุคคลภายใน และการเพิ่มสิทธิ์โดยไม่เหมาะสม โดยการรับรองว่าผู้ใช้จะได้รับสิทธิ์การเข้าถึงเฉพาะที่จำเป็นสำหรับบทบาทของตนเท่านั้น การนำ RBAC มาใช้ช่วยให้องค์กรสามารถจัดการการเข้าถึงได้อย่างมีประสิทธิภาพ รับรองความสอดคล้องกับมาตรฐานทางกฎหมาย และการปรับปรุงด้านความปลอดภัยโดยรวม

สาระสำคัญโดยสรุปของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

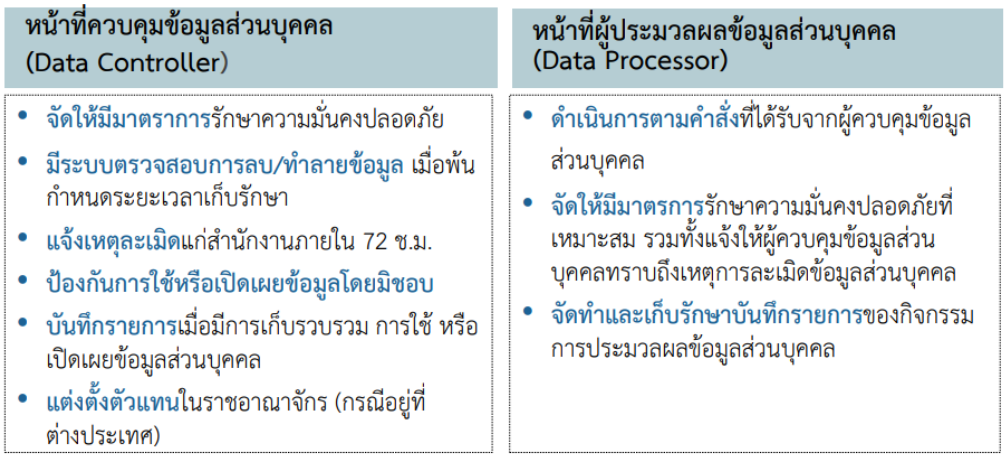
ได้ให้คำจำกัดความข้อมูลส่วนบุคคล (Personal Data) คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว และได้กำหนดบุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลดังนี้ (สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย, 2563)

1) เจ้าของข้อมูลส่วนบุคคล (Data Subject) ตามกฎหมายไม่ได้ให้คำนิยามไว้ แต่โดยหลักการทั่วไปแล้วหมายถึง บุคคลที่ข้อมูลนั้นระบุไปถึง

2) ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) คือ บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เช่น หน่วยงานของรัฐ หรือ เอกชนโดยทั่วไป ที่เก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคลของประชาชนหรือลูกค้าที่มาใช้บริการ

3) ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) คือ บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือ เปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล เช่น บริการ cloud service เป็นต้น

โดยผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) และ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) มีหน้าที่ดังนี้

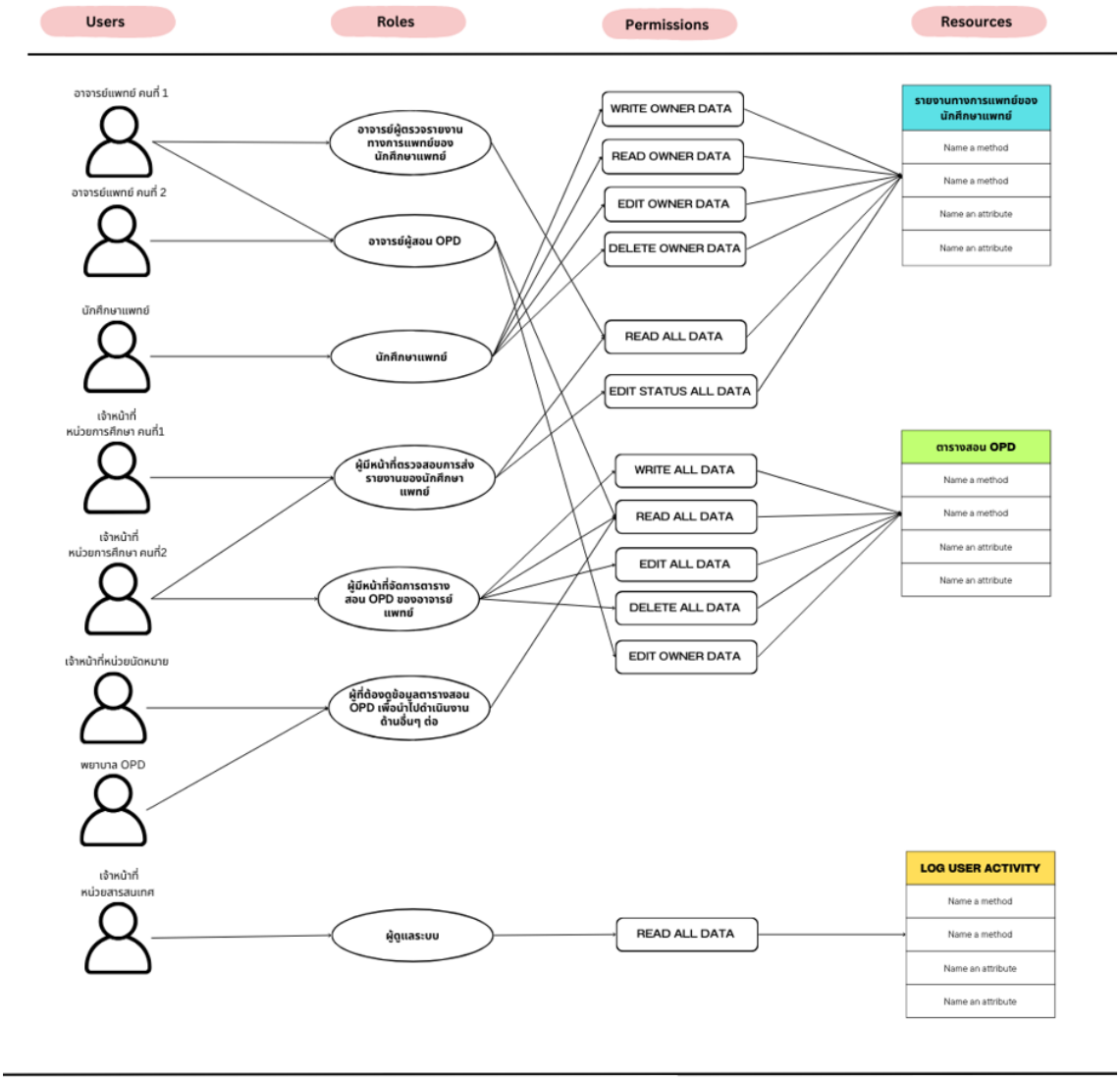


ภาพที่ 3 หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)
และผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)

หมายเหตุ. ดัดแปลงจาก “สรุปสาระสำคัญพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 The Personal Data Protection Act.”, สภาดิจิทัลเพื่อเศรษฐกิจและสังคม, 2564, หน้า 9 (https://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.pdf).

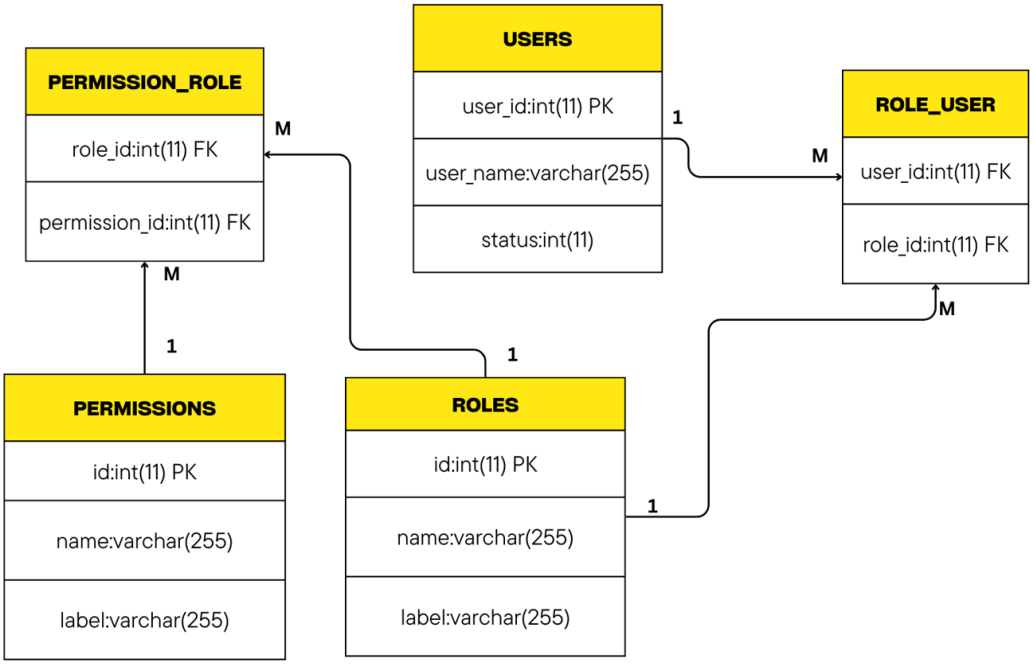
การประยุกต์ใช้แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control) ในการพัฒนาระบบสารสนเทศร่วมกับลาราเวลเฟรมเวิร์ก เวอร์ชั่น 11

การพัฒนาระบบสารสนเทศโดยทั่วไปนั้นจะมีความแตกต่างกันของฐานบทบาทที่ใช้งานตามแต่ละระบบงาน ดังนั้นในขั้นต้นจึงควรมีการจำแนกฐานบทบาทที่จำเป็นต่อการใช้งานออกมาให้ชัดเจน โดยยกตัวอย่างกรณีศึกษาการพัฒนาระบบสารสนเทศ ที่พัฒนาขึ้นเพื่อสนับสนุนพันธกิจในด้านการศึกษา ของภาควิชาอายุรศาสตร์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล โดยเป็นระบบที่ให้บริการการบริหารจัดการการส่งรายงานทางการแพทย์ของนักศึกษาแพทย์ การตรวจสอบติดตามการส่งรายงาน การตรวจรายงานโดยอาจารย์แพทย์และให้บริการการจัดการตารางสอน OPD ของอาจารย์แพทย์ จึงมีผู้ใช้งานที่เกี่ยวข้องกับระบบนี้หลายบทบาท หลายหน้าที่ แต่ละบทบาทถูกกำหนดสิทธิ์ให้มีการเข้าถึงข้อมูลแตกต่างกันออกไป จึงได้นำแนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control) มาประยุกต์ในการวิเคราะห์และออกแบบระบบ และสรุปบทบาท และการกำหนดสิทธิ์การเข้าถึงข้อมูลได้ดังภาพที่ 4



ภาพที่ 4 แสดงข้อกำหนดการควบคุมการเข้าถึงบนฐานบทบาท ของระบบสารสนเทศด้านการศึกษา ของภาควิชาอายุรศาสตร์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

1. การออกแบบโครงสร้างฐานข้อมูลของการควบคุมการเข้าถึงบนฐานบทบาท



ภาพที่ 5 โครงสร้างฐานข้อมูลการควบคุมการเข้าถึงบนฐานบทบาท ของระบบสารสนเทศด้านการศึกษาของภาควิชาอายุรศาสตร์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล

โครงสร้างฐานข้อมูลประกอบด้วยตารางสำหรับเก็บข้อมูล 5 ตาราง ดังนี้

1) ตารางเก็บข้อมูลบทบาท (roles) สำหรับเก็บข้อมูลบทบาททั้งหมดที่ถูกกำหนดให้เข้าถึงข้อมูลในระบบ

2) ตารางเก็บข้อมูลสิทธิ์ (permissions) สำหรับเก็บข้อมูลสิทธิ์ทั้งหมดที่ถูกกำหนดให้เข้าถึงข้อมูลในระบบ

3) ตารางเก็บข้อมูลกำหนดสิทธิ์ให้กับบทบาท (permission role) มีความสัมพันธ์กับตารางเก็บข้อมูลบทบาทโดยอ้างอิงจาก role id และมีความสัมพันธ์กับตารางเก็บข้อมูลสิทธิ์ โดยอ้างอิงจาก permission id

4) ตารางเก็บข้อมูลผู้ใช้งาน (user) สำหรับเก็บข้อมูลผู้ใช้งานระบบ ซึ่งในกรณีศึกษานี้จะไม่มีการเก็บรหัสผ่านของผู้ใช้งาน เนื่องจากการยืนยันตัวตนใช้การเชื่อมโยงข้อมูลกับ API (Application Programming Interface) ระบบที่เก็บข้อมูลบุคลากรของคณะแพทยศาสตร์ศิริราชพยาบาล

5) ตารางเก็บข้อมูลกำหนดบทบาทให้กับผู้ใช้งาน (role user) มีความสัมพันธ์กับตารางเก็บข้อมูลบทบาทโดยอ้างอิงจาก role id และมีความสัมพันธ์กับตารางเก็บข้อมูลผู้ใช้งาน โดยอ้างอิงจาก user id

จากภาพที่ 5 เมื่อสร้างโครงสร้างฐานข้อมูลแล้วให้กำหนดบทบาท (Roles) กำหนดสิทธิ์ (Permissions) แล้วจึงกำหนดสิทธิ์ให้กับบทบาท (permission role) และกำหนดบทบาทให้กับผู้ใช้งาน (role user) ก็จะได้ข้อมูลการควบคุมการเข้าถึงบนฐานบทบาทของผู้ใช้งานระบบทุกคน ระบบจึงสามารถตรวจสอบข้อมูลบทบาทและสิทธิ์ของผู้ใช้งานได้ แล้วนำไปเป็นเงื่อนไขในการควบคุมการเข้าถึงข้อมูลต่าง ๆ ในระบบได้อย่างถูกต้องและสะดวก ตัวอย่างดังภาพที่ 6 และ 7

id	name	label
1	admin_it	เจ้าหน้าที่ดูแลระบบ
2	student	นักศึกษาแพทย์
3	preceptor	อาจารย์ผู้ตรวจรายงาน นศพ.
4	admin_edu_report	เจ้าหน้าที่การศึกษาที่ดูแลการส่งรายงาน
5	admin_edu_manage_preceptc	เจ้าหน้าที่การศึกษาที่ดูแลข้อมูลอาจารย์ preceptor
6	admin_edu_manage_ward	เจ้าหน้าที่การศึกษาที่ดูแลข้อมูลหอผู้ป่วย
7	admin_edu_manage_student	เจ้าหน้าที่การศึกษาที่ดูแลข้อมูลนักศึกษา
8	teacher_opd	อาจารย์สอน OPD

ภาพที่ 6 ตัวอย่างข้อมูลบทบาทในตารางฐานข้อมูลบทบาท (Roles)

id	name	label
1	add_report	บันทึกข้อมูลรายงาน
2	edit_report	แก้ไขข้อมูลรายงาน
3	delete_report	ลบข้อมูลรายงาน
4	view_report	ดูข้อมูลรายงาน

ภาพที่ 7 ตัวอย่างข้อมูลสิทธิ์ในตารางฐานข้อมูลสิทธิ์ (Permissions)

permission_id	role_id
1	2
2	2
3	2
4	2

ภาพที่ 8 ตัวอย่างข้อมูลกำหนดสิทธิ์ให้กับบทบาท (permission_role)

จากภาพที่ 8 คือ การกำหนดสิทธิ์ที่ชื่อ add report, edit report, delete report และ view report ให้กับบทบาทที่ชื่อ student

permission_id	role_id
4	3

ภาพที่ 9 ตัวอย่างข้อมูลกำหนดสิทธิ์ให้กับบทบาท (permission_role)

จากภาพที่ 9 คือ การกำหนดสิทธิ์ที่ชื่อ view_report ให้กับบทบาทที่ชื่อ preceptor

user_id	role_id
4	2
5	2
7	2

ภาพที่ 10 ตัวอย่างข้อมูลกำหนดบทบาทให้กับผู้ใช้งาน (role_user)

จากภาพที่ 10 คือ การกำหนดบทบาทให้กับผู้ใช้งาน หมายเลข 4, 5 และ 7 ให้มีบทบาทที่ชื่อ student

user_id	role_id
132	3
132	8
134	2
137	2
140	3
140	8

ภาพที่ 11 ตัวอย่างข้อมูลกำหนดบทบาทให้กับผู้ใช้งาน (role_user)

จากภาพที่ 11 คือ การกำหนดบทบาทให้กับผู้ใช้งานหมายเลข 132 ให้มี 2 บทบาทคือบทบาทที่ชื่อ preceptor และ teacher_opd เป็นตัวอย่างที่แสดงให้เห็นว่า ผู้ใช้งาน 1 คน สามารถมีบทบาทได้มากกว่า 1 บทบาท

2. การพัฒนาระบบสารสนเทศร่วมกับลาราเวลเฟรมเวิร์ก เวอร์ชั่น 11 โดยใช้คุณลักษณะเรื่องการจัดการสิทธิ์ในการเข้าถึงข้อมูล ร่วมกับโครงสร้างฐานข้อมูลที่ออกแบบโดยประยุกต์ใช้แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control)

ลาราเวลเฟรมเวิร์ก เวอร์ชั่น 11 มีเอกสารที่บ่งชี้ถึงคุณสมบัติที่ใช้ในการจัดการด้านความปลอดภัยของการเข้าถึงระบบสารสนเทศอยู่ 2 วิธี คือ Gates และ Policies ซึ่งอยู่ในหัวข้อความปลอดภัย (Security) หัวข้อย่อยการตรวจสอบสิทธิ์ (Authorization) (Laravel, https://laravel.com/docs/11.x/authorization#introduction) โดยมีหลักการทำงาน คือ สร้างข้อกำหนดก่อนที่จะเข้าถึงเส้นทางและมีตัวควบคุม (controllers) โดย Gate ใช้วิธีการอนุญาตตามสิทธิ์ที่กำหนดใน Gate นั้น ๆ ในขณะที่ policies จะรวมกลุ่มตรรกะทรัพยากรเฉพาะเพื่อสร้างกฎในการควบคุมซึ่งในบทความนี้ได้ใช้แนวทางการตรวจสอบสิทธิ์ (Authorization) ที่ชื่อว่า Gates

Gates เป็นวิธีพื้นฐานของคุณลักษณะการอนุญาตให้เข้าถึงเส้นทาง (Route) ของข้อมูล ใน Laravel Framework โดยให้เขียนโค้ดโปรแกรมที่ไฟล์ AppServiceProvider.php ในฟังก์ชัน boot ดังภาพที่ 12

```
27      public function boot(): void
28      {
29          $permissionGates = Permission::query()->select('name')->get();
30          foreach ($permissionGates as $gate) {
31              Gate::define($gate, fn (User $user) => $user->hasPermission($gate));
32          }
33      }
34
```

ภาพที่ 12 ตัวอย่างการเขียนโค้ดโปรแกรมเพิ่มเติมเพื่อตรวจสอบข้อมูลสิทธิ์ของผู้ใช้งานผ่าน Gates

จากภาพที่ 12 ทุก Http Request ที่เรียกใช้งานผ่านเส้นทาง (Route) ในระบบจะถูกประมวลผลที่ไฟล์ AppServiceProvider.php ในฟังก์ชัน boot เสมอ และ Laravel Framework ได้จัดการส่งข้อมูลผู้ใช้เข้าไปใน Gate ให้อัตโนมัติแล้ว จึงสามารถเขียนโค้ดโปรแกรมเพิ่มเติมเพื่อตรวจสอบข้อมูลสิทธิ์ของผู้ใช้งานได้สะดวก

บรรทัดที่ 31 Gate จะได้รับข้อมูลของผู้ใช้งานระบบที่ผ่านการตรวจสอบตัวตนแล้วเป็นอาร์กิวเมนต์แรกเสมอ จึงสามารถเรียกใช้งานฟังก์ชันใน Class User ได้ ซึ่งตัวอย่างนี้ คือ ฟังก์ชัน hasPermission ดังภาพที่ 13

```
102     public function permissions(): array
103     {
104         return $this->roles()->with( relations: 'permissions')->get()
105             ->map(function ($role) {
106                 return $role->permissions->pluck('name');
107             })->flatten()->values()->unique()->flatten()->toArray();
108     }
        1 usage   new *
109     public function hasPermission(string $permission): bool
110     {
111         return in_array($permission, $this->permissions(), strict: true);
112     }
```

ภาพที่ 13 ตัวอย่างการเขียนโค้ดโปรแกรมฟังก์ชัน hasPermission ใน Class User

จากภาพที่ 13 ฟังก์ชัน hasPermission จะส่งค่าคืนกลับเป็น Boolean (true / false) หลังจากตรวจสอบสิทธิ์การเข้าถึง (Permission) ที่ส่งผ่านเป็นอาร์กิวเมนต์ มาตรวจสอบกับสิทธิ์ที่มีทั้งหมดของผู้ใช้งานคนนี้

จากนั้นใช้ middleware ของ Laravel Framework โดยสามารถเรียกใช้ alias ที่ชื่อว่า can (Laravel, https://laravel.com/docs/11.x/middleware#middleware-aliases) เพื่อตรวจสอบการอนุญาตตามสิทธิ์ที่กำหนดชื่อไว้ก่อนที่คำขอ (Http Request) ที่เข้ามาจะถึงเส้นทาง (Protecting Route) ซึ่ง Laravel Framework จะลงทะเบียนการตรวจสอบสิทธิ์ (Authorized) บนฐานบทบาทตามที่ระบบกำหนดไว้ให้อัตโนมัติ ตัวอย่างเช่น

หากต้องการอนุญาตให้ผู้ใช้งานที่มีสิทธิ์การเข้าถึง (Permission) ที่ชื่อว่า “add_report” เข้าใช้งานเส้นทาง (URL) ที่แสดงการส่งรายงานได้เท่านั้น ก็สามารถใช้ middleware ที่ชื่อว่า can ได้ดังภาพที่ 14

```php
Route::group([
    'prefix' => 'smn/report',
    'as' => 'smn.report.',
    'middleware' => ['auth'],
], function () {

    Route::get('/my-reports',[ReportController::class,'index'])->name('index')->middleware('can:view_report');

    Route::get('/create',[ReportController::class,'create'])->name('create')->middleware('can:add_report');
```

ภาพที่ 14 ตัวอย่างการเขียนโค้ดโปรแกรมด้วยลาราเวลเฟรมเวิร์ก เวอร์ชั่น 11 ในการควบคุมการเข้าถึงบนฐานบทบาท โดยใช้ alias ของ middleware ที่ชื่อ can

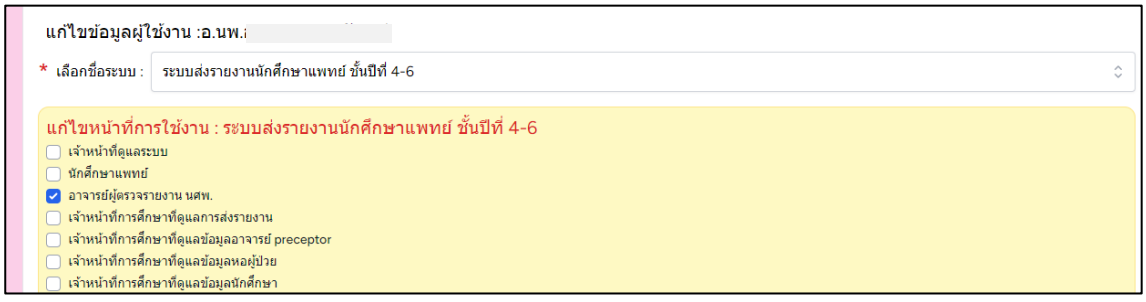
จากภาพที่ 14 ผู้ใช้งานที่มีสิทธิ์เข้าถึงเส้นทาง /create นี้ได้จะต้องมีสิทธิ์ (Permission) ที่ชื่อ add_report โดยใช้ alias ของ middleware ที่ชื่อ can จากตัวอย่างโค้ดโปรแกรมบรรทัดที่ 15

ตัวอย่างเหตุการณ์กรณีที่ผู้ใช้งานระบบสารสนเทศไม่มีสิทธิ์เข้าถึง resource หรือเส้นทางที่ไม่ได้รับอนุญาติในบทบาทของตนเอง เช่น หากผู้ใช้งานเป็นอาจารย์ที่ไม่มีหน้าที่ตรวจรายงานของนักศึกษาแพทย์ แต่ได้รับเส้นทาง URL ของการส่งรายงานมาจากนักศึกษาแพทย์ (https://...../create) เมื่อเข้าไปที่ URL ที่ได้รับมาจะไม่สามารถเข้าใช้งานได้ เพราะระบบจะตรวจสอบบทบาท (Role) และสิทธิ์การเข้าถึง (Permission) ของผู้ใช้งานตามที่กำหนดไว้ในฐานข้อมูลเทียบกับที่กำหนดไว้ที่ middleware (alias ที่ชื่อ can) ของเส้นทาง (Route) นั้น หากไม่ตรงกับสิทธิ์ที่อนุญาตระบบจะแสดงข้อความตัวอย่างดังภาพที่ 15 ให้อัตโนมัติ (HTTP response 403 status code)

ภาพที่ 15 ตัวอย่างหน้าจอเมื่อผู้ใช้งานเข้าไปเส้นทาง (Route) ที่ไม่มีสิทธิ์ในบทบาทของตนเอง

เมื่อมีการปรับเปลี่ยน โยกย้าย แต่งตั้งบุคลากร จำเป็นต้องมีการกำหนดบทบาทให้สิทธิ์ในการเข้าถึงข้อมูลในระบบโดยผู้ดูแลข้อมูลผู้ใช้งาน เช่น ปีการศึกษาใหม่ ประกาศเปลี่ยนรายชื่ออาจารย์แพทย์ที่เป็นอาจารย์ผู้ตรวจรายงานนักศึกษาแพทย์ โดยมีรายชื่อจำนวน 80 รายชื่อ เป็นต้น ผู้ดูแลข้อมูลสิทธิ์การเข้าถึง (Permission) ของผู้ใช้งานระบบสามารถดำเนินการผ่านระบบจัดการสิทธิ์ของผู้ใช้งานระบบ ตัวอย่างหน้าจอ ดังภาพที่ 16 และ 17

ภาพที่ 16 ตัวอย่างหน้าจอการจัดการสิทธิ์และบทบาทของผู้ใช้งานระบบ สำหรับผู้ดูแลระบบใช้งาน



ภาพที่ 17 ตัวอย่างหน้าจอการกำหนดบทบาทให้กับผู้ใช้งานระบบ

ข้อดีของการนำแนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control) มาประยุกต์ใช้

1) เพิ่มความปลอดภัยให้กับข้อมูลในระบบ เนื่องจากผู้ใช้งานแต่ละคนจะถูกกำหนดบทบาทในการเข้าใช้งานระบบและการเข้าถึง แก้ไข เพิ่ม ลบข้อมูล ตามบทบาทหน้าที่ของผู้ใช้งานคนนั้นเท่านั้น

2) เพิ่มความยืดหยุ่นให้กับระบบสารเทศภายในองค์กร เนื่องจากบุคลากรหนึ่งคนอาจมีหลายบทบาท แต่ละบทบาทก็มีหน้าที่ในการจัดการหรือเข้าถึงข้อมูลในระบบแตกต่างกันออกไป อีกทั้งมีการปรับเปลี่ยน โยกย้าย บทบาทของบุคลากรอยู่บ่อยครั้ง ทำให้ดำเนินการได้สะดวกโดยไม่ต้องมีการปรับแก้ไขโค้ดโปรแกรม

ข้อควรระวังของการนำแนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control) มาประยุกต์ใช้

1) การกำหนดบทบาท ควรกำหนดให้ครบถ้วน ครอบคลุมผู้ใช้งานทุกกลุ่มที่สามารถเข้าใช้งานระบบสารสนเทศที่กำลังพัฒนาหรือปรับปรุง ตั้งแต่แรกก่อนนำไปใช้งานจริงจะทำให้การบำรุงรักษาระบบหลังจากใช้งานจริงแล้วทำได้สะดวก

2) ระวังการกำหนดบทบาทที่ซ้ำซ้อนกัน ซึ่งจะทำให้เกิดความเข้าใจคลาดเคลื่อนหรือเข้าใจผิด ในการกำหนดบทบาทต่าง ๆ ให้กับผู้ใช้งานระบบแต่ละคน

บทสรุป

จากการศึกษาและนำแนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control) มาประยุกต์ใช้ในการออกแบบโครงสร้างฐานข้อมูลที่เกี่ยวข้องกับบทบาทและสิทธิ์ร่วมกับการพัฒนาระบบสารสนเทศด้วยลาราเวลเฟรมเวิร์ก ผ่านเครื่องมือที่เรียกว่า Gates ในการควบคุมสิทธิ์การเข้าถึงเส้นทาง (Protecting Route) เพื่อควบคุมสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานระบบสารสนเทศที่มีผู้ใช้งานหลากหลายบทบาท โดยผู้ใช้หนึ่งคนมีหลายบทบาท แต่ละบทบาทมีสิทธิ์การเข้าถึงข้อมูลที่แตกต่างกัน และมีการเปลี่ยนแปลงโยกย้ายผู้ใช้งานไปในบทบาทอื่นอยู่เสมอ พบว่าสามารถทำให้การพัฒนาระบบสารสนเทศด้านการควบคุมการเข้าถึงผ่านการกำหนดสิทธิ์ทำได้สะดวกรวดเร็ว สามารถตรวจสอบสิทธิ์ (Authorization) การเข้าถึงข้อมูลตามฐานบทบาทได้อย่างถูกต้องเป็นไปตามข้อกำหนดของผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เรื่องสิทธิ์การเข้าถึงข้อมูลของระบบงานและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เรื่องการบริหารจัดการสิทธิ์การเข้าถึงตามสิทธิ์ (management of privileged access rights)

แนวคิดการควบคุมการเข้าถึงบนฐานบทบาท (Role-Based Access Control) สามารถนำมาประยุกต์ใช้ในการออกแบบโครงสร้างฐานข้อมูลที่เกี่ยวข้องกับบทบาทและสิทธิ์ แล้วนำไปพัฒนาระบบสารสนเทศได้โดยไม่ขึ้นกับภาษาโปรแกรมหรือเฟรมเวิร์กที่ใช้พัฒนาระบบ ซึ่งหากภาษาโปรแกรมหรือเฟรมเวิร์กที่ใช้ ไม่มีเครื่องมือสำเร็จรูปในการควบคุมสิทธิ์และการตรวจสอบสิทธิ์ นักพัฒนาระบบสามารถเขียนโปรแกรมในส่วนการควบคุมสิทธิ์ และการตรวจสอบสิทธิ์ขึ้นมาเอง

ดังนั้นนักวิเคราะห์ออกแบบและพัฒนาระบบ สามารถนำแนวคิดและวิธีการไปประยุกต์ใช้ในการพัฒนาระบบสารสนเทศของตนเอง เพื่อให้เกิดความยืดหยุ่นต่อการใช้งานกับผู้ที่เป็นผู้ดูแลสิทธิ์และบทบาทของผู้ใช้งานระบบ และรองรับการปรับเปลี่ยนบทบาทของผู้ใช้งานระบบสารสนเทศในอนาคตได้อย่างมีประสิทธิภาพ

กิตติกรรมประกาศ

บทความทางวิชาการฉบับนี้สำเร็จสมบูรณ์ได้จากการสนับสนุนของหน่วยสารสนเทศ และหน่วยการศึกษาก่อนปริญญา ภาควิชาอายุรศาสตร์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล ที่ให้ความสำคัญกับประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 โดยเฉพาะเรื่องการบริหารจัดการสิทธิ์การเข้าถึงตามสิทธิ์ (management of privileged access rights) จนนำไปสู่การค้นคว้าหาแนวคิดและเทคนิคแล้วนำมาประยุกต์ปฏิบัติในการพัฒนาระบบสารสนเทศ เพื่อให้สอดคล้อง

กับประกาศดังกล่าวจนสำเร็จ และขอขอบคุณนายกรมิษฐ์ พิชนาหะรี นักวิชาการคอมพิวเตอร์ ภาควิชาอายุรศาสตร์ คณะแพทยศาสตร์ศิริราชพยาบาล มหาวิทยาลัยมหิดล สำหรับคำแนะนำในการพัฒนาระบบสารสนเทศ

เอกสารอ้างอิง

จิตติภัทร ผสมทรัพย์. (2563). *กรอบงานการควบคุมการเข้าถึงบนฐานบทบาทสำหรับตัวจัดการความมั่นคงไมโครเซอร์วิส* (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย. กรุงเทพฯ. Doi: 10.58837/ CHULA. THE.2020.1024

ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลเรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565. (2565, 20 มิถุนายน). *ราชกิจจานุเบกษา.* เล่ม 139 ตอนพิเศษ 140 ง หน้า 28-31.

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา.* เล่ม 136 ตอน 69 ก, หน้า 52-94.

ภูวนาถ กอบคำ. (2558). *การพิสูจน์ตัวจริงอิงบทบาทสำหรับเว็บเซอร์วิสองค์กร* (วิทยานิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต). จุฬาลงกรณ์มหาวิทยาลัย. กรุงเทพฯ. Doi: 10.58837/CHULA.THE.2015.1140

สภาดิจิทัลเพื่อเศรษฐกิจและสังคม. (2564). สรุปสาระสำคัญพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 The Personal Data Protection Act. สืบค้น 14 สิงหาคม พ.ศ. 2567. จากhttps://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.pdf

Alan C. O'Connor & Ross J. Loomis. (2010). 2010 Economic Analysis of Role-Based Access Control Final Report. *National Institute of Standards and Technology*. Gaithersburg, United States. P2-8. Retrieved August 21, 2024. Retrieved from: https://csrc.nist.gov/files/pubs/other/2010/12/19/economic-analysis-of-rbac-final-report/final/docs/20101219_rbac2_final_report.pdf

David F.Ferraiolo & D. Richard Kuhn. (1992). Role-Base Access Controls. Conference Name: *15th National Computer Security Conference (NCSC)*, 13-16 October 1992, Baltimore, Maryland, United States.

J. Singh, S. Rani 2 and V. Kumar. (2024). Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks. *International Journal of Communication Networks and Information Security*. vol. 16, no. 2, Page. 19-32, Aug. 2024.

Laravel Framework Version 11. Security Authorization. Retrieved June 10, 2024. Retrieved from: https://laravel.com/docs/11.x/authorization

Marquis and Yewande Alice. (2024). "From Theory to Practice: Implementing Effective Role-Based Access Control Strategies to Mitigate Insider Risks in Diverse Organizational Contexts". *Journal of Engineering Research and Reports.* Vol. 26, Issue 5, Page138-154, 2024. Doi: 10.9734/jerr/2024/v26i51141.

Vitra and Surendra. (2025). Role-Based Access Control (RBAC) and its Impact on Organizational Cybersecurity Policies. *SSRN*. Doi: 10.2139/ssrn.5079310