การวิเคราะห์แนวทางการพัฒนาการตรวจสอบและแจ้งเตือนการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการด้วยการประยุกต์ใช้โมเดลออโตมาตา

ANALYZING AUDIT DEVELOPMENT GUIDELINES AND NOTIFYING THE OPERATING SYSTEM OF SECURITY MAINTENANCE BY APPLYING THE AUTOMATA MODEL

ทิภาพร ศุภมิตร[1] สุวิทย์ วงศ์คุ้มสิน[2] ชนะธิป ธำรงวิทยภาคย์[3] และ อิฐติศักดิ์ เมืองสง[4]
[1,2,3,4]อาจารย์, สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษมบัณฑิต
60 ถนนร่มเกล้า แขวงมีนบุรี เขตมีนบุรี กรุงเทพฯ 10510,
[1]tipaporn.sup@kbu.ac.th, [2]suwit@kbu.ac.th, [3]chanatip.vv@gmail.com, [4]ittisak.ms@gmail.com

Tipaporn Supamid[1], Suwit Wongkumsin[2], Chanatip Tumrongwittyapak[3]
and Ittisak Muangsong[4]
[1,2,3,4]Lecturer, Department of Computer Engineering, Faculty of Engineering,
Kasem Bundit University, 60 Romklao Rd, Minburi, Bangkok 10510, Thailand,
[1]tipaporn.sup@kbu.ac.th, [2]suwit@kbu.ac.th, [3]chanatip.vv@gmail.com, [4]ittisak.ms@gmail.com

บทคัดย่อ

งานวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาบริบท ปัญหาและสถานการณ์ความมั่นคงปลอดภัยของระบบปฏิบัติการเพื่อพัฒนาวิธีการตรวจสอบ เฝ้าระวัง และแจ้งเตือนระดับความมั่นคงปลอดภัยของระบบปฏิบัติการ โดยเครื่องมือที่ใช้ในการวิจัยคือ การวิเคราะห์ข้อมูล ค่าความถี่ ค่าร้อยละ ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐาน ผลลัพธ์การวิจัยคือ ส่วนที่ 1 การทดสอบและการตรวจสอบของระบบปฏิบัติการ พบว่าการจัดการข้อมูลการทดสอบ 4.98 เปอร์เซ็นต์ ส่วนที่ 2 การวิเคราะห์และการรายงาน 4.93 เปอร์เซ็นต์ ส่วนที่ 3 วิธีการแจ้งเตือน 4.98 เปอร์เซ็นต์ และส่วนที่ 4 การวิเคราะห์แนวทางการพัฒนาการตรวจสอบ และแจ้งเตือนการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการด้วยการประยุกต์ใช้โมเดลออโตมาตา พบว่าอยู่ในระดับที่ดีอย่างมีนัยสำคัญ

คำสำคัญ: การตรวจสอบ, การรักษาความมั่นคงปลอดภัย, ระบบปฏิบัติการ, โมเดลออโตมาตา

ABSTRACT

This study aims to examine the challenges and state of operating system security to develop methods for monitoring, surveillance, and alerting. It uses data analysis techniques, including frequency, percentage, mean, and standard deviation. The findings are as follows: Part 1 shows data management testing at 4.98%. Part 2's analysis and reporting stand at 4.93%. Part 3's alerting methods account for 4.98%. Part 4 discusses developing inspection and alerting methods using automata models, which were found to be at a significantly high level.

KEYWORDS: Inspection, Security, Operating System, Automata Model.

1. บทนำ

การนำเทคโนโลยีทันสมัยมาใช้เพื่อเพิ่มความปลอดภัยของระบบปฏิบัติการเป็นสิ่งสำคัญในยุคดิจิทัล การวิจัยมุ่งเน้นแก้ปัญหาหลักในด้านความปลอดภัย เช่น การปรับปรุงระบบตรวจจับกิจกรรมเสี่ยงให้แม่นยำ เพิ่มความเร็วและประสิทธิภาพโดยไม่กระทบการทำงาน และพัฒนาความแม่นยำในการตรวจสอบเพื่อลดข้อผิดพลาด นอกจากนี้ การออกแบบระบบให้สามารถขยายตามความต้องการ (Scalable) และการใช้เทคโนโลยีการเรียนรู้เชิงลึกในการจัดการข้อมูลเป็นสิ่งสำคัญ เพื่อสร้างระบบปฏิบัติการที่มีความปลอดภัยและประสิทธิภาพสูง การทดสอบและตรวจสอบอย่างเหมาะสมช่วยรับรองความถูกต้องและประสิทธิภาพของระบบในการตรวจสอบความเสี่ยงและการละเมิดความปลอดภัยอย่างมีประสิทธิภาพ ดังนั้นการแก้ไขปัญหาเหล่านี้จะนำไปสู่การพัฒนาระบบปฏิบัติการที่มีความปลอดภัยและประสิทธิภาพสูงขึ้น การทดสอบและการตรวจสอบระบบปฏิบัติการอย่างเหมาะสมเป็นขั้นตอนสำคัญที่ช่วยให้สามารถรับรองความถูกต้องและประสิทธิภาพของระบบในการตรวจสอบและเฝ้าระวังความเสี่ยงและการละเมิดความปลอดภัยได้อย่างมีประสิทธิภาพและเป็นระบบอัตโนมัติมากยิ่งขึ้น

2. ทบทวนวรรณกรรม

2.1 ความมั่นคงปลอดภัยทางไซเบอร์ หรือ Cybersecurity

ความปลอดภัยทางไซเบอร์เป็นกรอบและโครงสร้างพื้นฐานทางเทคโนโลยีที่สร้างขึ้น เพื่อปกป้องข้อมูล เครือข่าย และอุปกรณ์การป้องกันคอมพิวเตอร์ขององค์กรส่วนใหญ่เกิดจากการใช้ระบบข้อมูลส่วนบุคคลและทรัพยากรภายในรวมถึงการปรับใช้ซอฟต์แวร์เพื่อป้องกันการเข้าถึงและการโจมตีโดยไม่ได้รับอนุญาต [1] โดยมุ่งเน้นไปที่การรักษาความปลอดภัยของสภาพแวดล้อมออนไลน์ ความสามารถด้านความปลอดภัยทางไซเบอร์ของพนักงานได้รับการปรับปรุงโดยครอบคลุมการตรวจสอบความท้าทายและอุปสรรคปัจจุบัน ความสามารถด้านความปลอดภัย

ทางไซเบอร์ของพนักงานได้รับการปรับปรุง ควบคู่ไปกับการตรวจสอบประเด็นและอุปสรรคนอกเหนือจากการแสวงหาแก้ไขปัญหาหรืออุปสรรคดังกล่าว โดยมีวัตถุประสงค์เพื่อให้คำแนะนำในการปรับปรุงความสามารถด้านความปลอดภัยทางไซเบอร์ของพนักงานการศึกษานี้ดำเนินการภายในสำนักงานคณะกรรมาธิการความปลอดภัยทางไซเบอร์แห่งชาติ (SCR.)การสอบสวนนี้ใช้วิธีการรวบรวมข้อมูลผ่านเอกสารและการสำรวจที่เกี่ยวข้องกับบุคลากรที่สำคัญ 7 คน แม้ว่าจะมีแนวทางในการเพิ่มทักษะความปลอดภัยทางไซเบอร์ แต่สิ่งสำคัญคือต้องมุ่งเน้นไปที่การศึกษาเพื่อปรับปรุงความเข้าใจและความรู้ในสาขานี้ควรจัดโปรแกรมการฝึกอบรมเพื่อกำหนดเป้าหมายการพัฒนาทักษะความปลอดภัยทางไซเบอร์สำหรับบุคลากรโดยเฉพาะการสนับสนุนและส่งเสริมการพัฒนาทักษะความปลอดภัยทางไซเบอร์ผ่านกิจกรรมต่าง ๆ เป็นสิ่งสำคัญในการจัดหาโอกาสและทรัพยากรที่จำเป็น ความท้าทายและอุปสรรคในการเพิ่มทักษะบุคลากรเป็นหลักมาจากข้อจำกัดทางการเงิน โดยเฉพาะอย่างยิ่งประเด็นเกี่ยวกับบทบัญญัติงบประมาณที่ไม่เพียงพอสำหรับบุคคลที่กระตือรือร้นที่จะพัฒนาความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ ดังนั้นความพร้อมใช้งานของโปรแกรมการศึกษาที่ จำกัด ส่งผลให้ผู้เชี่ยวชาญขาดแคลนเช่นเดียวกับบุคลากรทางปัญญาภาคส่วนนี้โดดเด่นด้วยความขาดแคลนทรัพยากรและความเชี่ยวชาญที่จำเป็นสำหรับการบำรุงความสามารถด้านความปลอดภัยทางไซเบอร์ของบุคลากรที่สนใจ [2] นอกจากนี้การใช้เทคโนโลยีนี้ยังได้รับการยอมรับในขอบเขตของการวิจัยด้านความปลอดภัยของเทคโนโลยีคอมพิวเตอร์ และสาขาเทคโนโลยีวิศวกรรมสารสนเทศอิเล็กทรอนิกส์ยังประสบความสำเร็จในการจัดการกับความท้าทายด้านความปลอดภัยโดยการใช้แนวคิดของพัลส์ที่เหมาะสมบนเวิร์กสเตชัน [3]

2.2 ความปลอดภัยของระบบปฏิบัติการ

การรักษาความปลอดภัยของระบบปฏิบัติการมีบทบาทสำคัญในการปกป้องข้อมูลและทรัพย์สินภายในระบบคอมพิวเตอร์ ดังนั้นความปลอดภัยโดยรวมของระบบข้อมูลองค์กรจึงขึ้นอยู่กับประสิทธิภาพของนโยบายความปลอดภัยที่นำไปใช้ภายในระบบปฏิบัติการเดี่ยว เป็นข้อเท็จจริงที่ได้รับการยอมรับอย่างกว้างขวางว่าระบบปฏิบัติการ Linux (OS) ไม่เพียงพอในฐานะอุปกรณ์รักษาความปลอดภัยที่ครอบคลุมโดยเน้นหลักคือการเสริมสร้างระบบปฏิบัติการจากการละเมิดโดยไม่ได้รับอนุญาต การโจมตีทางไซเบอร์ และการจัดการข้อมูลระบบปฏิบัติการทำหน้าที่เป็นองค์ประกอบสำคัญในการทำงานของคอมพิวเตอร์ [4] รวมถึงการป้องกันระบบคอมพิวเตอร์เป็นหัวใจสำคัญของความน่าเชื่อถือในยุคดิจิทัล ซึ่งครอบคลุมการกำกับดูแลการเข้าถึงและการใช้งานทรัพยากรอย่างเหมาะสม เพื่อปกป้องข้อมูลจากการเข้าถึงหรือการแก้ไขโดยไม่ได้รับอนุญาต [5] มีหลักการสำคัญ 4 ประการในการรักษาความปลอดภัยข้อมูลดังต่อไปนี้ 1) การรักษาความลับ เป็นข้อมูลสามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาต 2) การรักษาความสมบูรณ์ เป็นการรับรองว่า

ข้อมูลไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต 3) ความพร้อมใช้ เป็นข้อมูลและบริการพร้อมใช้งานเมื่อมีความต้องการ 4) การห้ามปฏิเสธความรับผิดชอบ ทั้งผู้ส่งและผู้รับไม่สามารถปฏิเสธการกระทำที่เกี่ยวข้องกับข้อมูล ดังนั้นการควบคุมความปลอดภัยในระบบคอมพิวเตอร์มี 5 ระดับหลักดังต่อไปนี้ 1) Audit เป็นการตรวจสอบว่าใครเป็นผู้ดำเนินการ 2) Integrity เป็นการกำหนดผู้ที่สามารถแก้ไขข้อมูล 3) Encryption เป็นการกำหนดผู้ที่สามารถดูข้อมูล 4) Authorization เป็นการกำหนดผู้ที่ได้รับอนุญาตเข้าถึงข้อมูล 5) Authentication เป็นการยืนยันตัวตนของผู้ใช้ ซึ่งการรวมกันของหลักการเหล่านี้สร้างระบบคอมพิวเตอร์ที่ปลอดภัยและเชื่อถือได้ โดยป้องกันการเข้าถึงและการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต และรักษาความลับข้อมูลให้สูงสุด รวมถึงการปรับใช้และการบำรุงรักษามาตรการความปลอดภัยเหล่านี้ต้องดำเนินการอย่างต่อเนื่องเพื่อรับมือกับภัยคุกคามในโลกดิจิตอลที่เปลี่ยนแปลงไปอย่างรวดเร็ว [6]

2.3 ระบบปฏิบัติการ

ระบบปฏิบัติการ เป็นระบบซอฟต์แวร์ที่ทำหน้าที่จัดการอุปกรณ์ภายในเครื่องคอมพิวเตอร์และเป็นแหล่งซอฟต์แวร์ และบริการทางด้านโปรแกรมคอมพิวเตอร์ แม้ว่าฟังก์ชั่นหลักที่ระบบปฏิบัติการถือว่าจำเป็นเกี่ยวข้องกับการกระจายทรัพยากรทั่วคอมพิวเตอร์เพื่อวัตถุประสงค์ในการให้บริการที่เกี่ยวข้องกับแอพพลิเคชั่นซอฟต์แวร์ที่เกี่ยวข้องกับการส่งข้อมูลและการจัดเก็บข้อมูลควบคู่ไปกับฮาร์ดแวร์ภาพประกอบของสิ่งนี้คือการส่งข้อมูลจากไฟล์ภาพเพื่อแสดงบนหน้าจอการถ่ายโอนข้อมูลไปยังและจากฮาร์ดดิสก์และการถ่ายทอดข้อมูลทั่วระบบตลอดจนกิจกรรมเครือข่ายเอาต์พุตเสียงไปยังลำโพงและการจัดสรรพื้นที่หน่วยความจำเพื่อตอบสนองต่อคำขอซอฟต์แวร์ ซึ่งการจัดสรรเวลาสำหรับการใช้โปรเซสเซอร์และการดำเนินการพร้อมกันของซอฟต์แวร์แอพพลิเคชั่นหลายโปรแกรมปัจจัยต่าง ๆ มีอิทธิพลต่อการรับรู้และการใช้ระบบรักษาความปลอดภัยคอมพิวเตอร์ของพนักงานภายในองค์กรผลการวิจัยถูกนำมาใช้เพื่อให้ความรู้แก่พนักงานเกี่ยวกับการใช้ระบบคอมพิวเตอร์ที่ปลอดภัยและเพื่อกำหนดมาตรการป้องกันภัยคุกคามตัวอย่างการศึกษาประกอบด้วยผู้ปฏิบัติงานคอมพิวเตอร์ 327 คนจากกลุ่มไทยราษฎร์ โดยใช้วิธีการสุ่มแบบแบ่งชั้น ซึ่งข้อมูลที่ได้รับการตรวจสอบผ่านการประยุกต์ใช้สถิติเชิงพรรณนาครอบคลุมความถี่ เปอร์เซ็นต์ ค่าเฉลี่ย และความเบี่ยงเบนมาตรฐาน ตลอดจนสถิติเชิงอนุมาน ซึ่งรวมถึงการทดสอบ t-test, One-way ANOVA, LSD, และ Pearson's Correlation ตามเกณฑ์ที่มีนัยสำคัญทางสถิติอยู่ที่ 0.05 โดยการวิจัยระบุว่าผู้เข้าร่วมส่วนใหญ่ระบุว่าการทำงานในกองบรรณาธิการข่าวแม้จะได้รับการยอมรับอย่างเห็นได้ชัดในความเชี่ยวชาญที่เกี่ยวข้องกับความปลอดภัยของระบบคอมพิวเตอร์ [7] อย่างไรก็ตามนวัตกรรมด้านความปลอดภัยของระบบปฏิบัติการเป็นการมุ่งเน้นไปที่การเพิ่มขีดความสามารถในด้านต่างๆ เช่น สภาพแวดล้อมการดำเนินการที่เชื่อถือได้ (TEE) ความปลอดภัยการจำลองเสมือน การออกแบบไมโครเคอร์เนล

สำหรับความปลอดภัยของเคอร์เนล และความปลอดภัยของแอปพลิเคชันแบบกระจาย นวัตกรรมเหล่านี้ รวมถึง Penglai, CloudVisor, ChCore และ PiXiu ใช้ประโยชน์จากการออกแบบร่วมกันของฮาร์ดแวร์และซอฟต์แวร์ เพื่อให้การป้องกันที่แข็งแกร่งต่อภัยคุกคามความปลอดภัยที่หลากหลาย บทความนี้ยังทบทวนผลงานทางวิชาการที่สำคัญในแต่ละด้าน โดยนำเสนอภาพรวมที่ครอบคลุมเกี่ยวกับความก้าวหน้าในเทคโนโลยีความปลอดภัยของระบบปฏิบัติการ [8]

2.4 ออโตมาตา

ออโตมาตา (Automata) เป็นแบบจำลองทางคณิตศาสตร์ที่ใช้ในการอธิบายขั้นตอนการทำงานของเครื่องจักร มีการแบ่งออโตมาตาออกเป็น 2 ประเภทหลัก คือ ออโตมาตาจำกัดเชิงกำหนด (Deterministic Finite Automata) และ ออโตมาตาจำกัดเชิงไม่กำหนด (Non-Deterministic Finite Automata) [9] โดยมีลักษณะการทำงานดังนี้ 1) ออโตมาตาจำกัดเชิงกำหนด (DFA): สามารถรับสัญลักษณ์ตัวหนึ่งและเปลี่ยนสถานะไปยังสถานะที่กำหนดไว้ล่วงหน้าได้ 2) ออโตมาตาจำกัดเชิงไม่กำหนด (NFA): สามารถมีทางเลือกในการเปลี่ยนสถานะ และมีสถานะมากกว่าหนึ่งตัวเลือกความสามารถในการตัดสินใจถึงทางเลือกที่จะทำให้เครื่องทำงานจนจบและเลือกเปลี่ยนสถานะไปยังทางนั้น ดังนั้นการตัดสินใจแบบนี้ที่เกี่ยวข้องกับการเปลี่ยนสถานะเชิงไม่กำหนด (Nondeterministic State Transition) ทำให้ NFA สามารถทำงานได้ตลอดจนจบโดยที่สามารถตัดสินใจในการเปลี่ยนสถานะได้หลายทางเลือก ซึ่งมีความยืดหยุ่นที่แตกต่างจาก DFA ที่มีการกำหนดทางเดียวในการเปลี่ยนสถานะ เพื่อการใช้งานออโตมาตาเชิงชนิดตัวเลขในรูปแบบต่าง ๆ สามารถช่วยในการแก้ปัญหาและวิเคราะห์การทำงานของระบบที่มีลักษณะการเคลื่อนไหวตามขั้นตอนที่แน่นอนหรือไม่แน่นอนตามลำดับขั้นตอนที่กำหนด [10] อย่างไรก็ตามการปฏิบัติงานทางด้านองค์กรและเทคโนโลยีมีความเกี่ยวข้องกับการพัฒนาซอฟต์แวร์เพื่อใช้ในการจัดการและปฏิบัติการปฏิบัติงานทั้งหมดขององค์กร ขั้นตอนทางด้านซอฟต์แวร์มีความสำคัญในการให้บริการและผลิตภัณฑ์ เพื่อตอบสนองต่อความต้องการและความพึงพอใจของผู้ใช้งาน การนำเครื่องมือทางซอฟต์แวร์มาใช้ในกระบวนการพัฒนาและทดสอบซอฟต์แวร์เป็นส่วนสำคัญในการเพิ่มประสิทธิภาพและความเสถียรของระบบที่สร้างขึ้น ดังนั้นการศึกษาที่ใช้การทดสอบอัตโนมัติบนซอฟต์แวร์เว็บแอปพลิเคชันได้เป็นที่น่าสนใจ เนื่องจากมีผลกระทบที่มีนัยสำคัญต่อกระบวนการพัฒนา การใช้การทดสอบอัตโนมัติช่วยลดระยะเวลาทดสอบ ลดทรัพยากรที่ใช้ (เช่น แรงงานคน) และลดความผิดพลาดที่เกิดจากการทดสอบด้วยมือ ผลลัพธ์ยังพบว่าเวลาที่ใช้ในการทดสอบอัตโนมัติน้อยกว่าเวลาที่ใช้ในการทดสอบด้วยมือ ซึ่งช่วยเพิ่มประสิทธิภาพในกระบวนการทดสอบ ซึ่งการใช้การทดสอบอัตโนมัติมีประโยชน์มากยิ่งในกรณีที่ต้องทำซ้ำการทดสอบหลายครั้ง นอกจากนี้ การรายงานผลการทดสอบที่ได้รับผลลัพธ์ถูกต้องและรวดเร็ว

ช่วยให้ทีมพัฒนามีข้อมูลที่น่าเชื่อถือในการติดตามว่าซอฟต์แวร์ทำงานถูกต้องและครบถ้วนตามข้อกำหนดหรือไม่

3. วิธีการดำเนินงานวิจัย

การศึกษาครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยผู้วิจัยศึกษา และรวบรวมข้อมูลจาก 2 แหล่งหลัก [11, 12] โดยมีขั้นตอนการดำเนินงานวิจัยดังต่อไปนี้

3.1 การเตรียมข้อมูล

1) การเตรียมข้อมูล เป็นรวบรวมข้อมูลที่เกี่ยวข้องกับความปลอดภัยของระบบปฏิบัติการของชนิดของข้อมูลที่บันทึก (เวลาและวันที่เกิดเหตุการณ์, ประเภทของกิจกรรม (เช่น เข้าสู่ระบบ, เปลี่ยนแปลงไฟล์, การเชื่อมต่อเครือข่าย) ผู้ใช้หรือแอปพลิเคชันที่ทำกิจกรรม, ที่มาของกิจกรรม (IP address, ชื่อเครื่องคอมพิวเตอร์) เช่น บันทึกการเข้าถึงระบบ (บันทึกเป็นไฟล์ log ที่สามารถอ่านได้ง่าย และเป็นไฟล์ที่มีโครงสร้างที่ชัดเจน, ใช้รูปแบบที่สามารถนำเข้าสู่ระบบการจัดการ log อัตโนมัติได้ เป็นต้น) การกำหนดการใช้งานที่ผิดปกติ (anomalies) หรือการโจมตีที่เป็นไปได้ และทำการจัดรูปแบบข้อมูลและทำความสะอาดข้อมูลเพื่อให้มีความเหมาะสมสำหรับการนำเข้าเข้าสู่โมเดล รวมถึงการรวบรวมข้อมูลการใช้งานที่ผิดปกติ (Anomaly Detection) วัตถุประสงค์เพื่อการตรวจจับและรายงานเหตุการณ์ที่อาจเป็นสัญญาณของการโจมตีหรือกิจกรรมที่ไม่ปกติ

2) การเลือกและสร้างโมเดล เป็นการเลือกและออกแบบโมเดลที่เหมาะสมสำหรับการตรวจสอบและเฝ้าระวังความปลอดภัย โดยการใช้วิธีการตรวจจับการทำฝั่ง (Intrusion Detection Systems - IDS) ในรูปแบบ Deep Neural Networks (DNNs) เพื่อเป็นการใช้ในการสร้างระบบตรวจจับการทำฝั่งที่มีความสามารถในการตรวจจับภัยคุกคามที่ซับซ้อนมากขึ้น เช่น การโจมตีด้วยการทำซ้ำๆ (replay attacks) หรือการโจมตีแบบไม่ทราบชื่อ (zero-day attacks) โดยใช้โครงข่ายประสาทเทียมที่มีความลึกมากเพื่อจดจำและตรวจจับลักษณะการโจมตีที่ไม่เคยเห็นมาก่อนได้

3) การฝึกโมเดล เป็นการใช้ข้อมูลที่เตรียมไว้เพื่อฝึกโมเดลออโตมาต้า โดยการใช้เทคโนโลยีการเรียนรู้เชิงลึก โดยผู้วิจัยใช้ข้อมูลทั้งหมด 5 ชุด โดยผู้วิจัยได้ทำการวิเคราะห์ข้อมูลดังต่อไปนี้

- ชุดฝึกข้อมูลการสร้างโมเดลที่เรียนรู้จากข้อมูล (Supervised Learning) 5 ชุด จากชุดข้อมูลทั้งหมด (เช่น 100% ของข้อมูล)

- ชุดฝึกโมเดลเป็นลำดับเวลา (Time Series Training) 2 ชุด แบ่งข้อมูลชุดทดสอบจะถูกแบ่งออกเป็นส่วนย่อย 2 ใน 3 ของแต่ละชุดฝึก

```python
from sklearn.model_selection import train_test_split

# ข้อมูลที่จะแบ่งเป็นชุดทดสอบและชุดฝึก
X_all = your_data
y_all = your_targets

# แบ่งชุดทั้งหมดเป็น 5 ชุด
X_train_all, X_test_all, y_train_all, y_test_all = train_test_split(X_all, y_all, test_siz

# วนลูปเพื่อแบ่งแต่ละชุดทดสอบเป็น 3 ใน 2
for X_test, y_test in zip(X_test_all, y_test_all):
    X_test_split1, X_test_split2, y_test_split1, y_test_split2 = train_test_split(X_test,

    # X_test_split2, y_test_split2 คือชุดทดสอบ
    # X_test_split1, y_test_split1 คือชุดฝึก
```

รูปที่ 1 โปรแกรมแสดงการแบ่งชุดฝึกข้อมูล

จากรูปที่ 1 โปรแกรมแสดงการแบ่งชุดฝึกข้อมูล กล่าวคือ เมื่อ train_test_split ใช้ในการแบ่งชุดข้อมูลทั้งหมด (X_all, y_all) เป็น X_train_all, X_test_all, y_train_all, y_test_all ซึ่งจะได้ชุดที่แบ่งไว้สำหรับทดสอบและฝึกทั้งหมด (5 ชุด) และรวมถึงการวนลูป for จะทำการแบ่งแต่ละชุดทดสอบ (X_test, y_test) เป็น 2 ใน 3 ของชุดทดสอบ (X_test_split2, y_test_split2) และส่วนที่เหลือเป็นชุดฝึก (X_test_split1, y_test_split1)

4) การประเมินและปรับปรุง เป็นทดสอบโมเดลที่ได้ฝึกแล้วโดยใช้ชุดข้อมูลที่ไม่เคยเห็นมาก่อน (Test Data) เพื่อประเมินประสิทธิภาพของโมเดล และปรับปรุงโมเดลตามผลการประเมินเพื่อให้มีประสิทธิภาพและความแม่นยำมากยิ่งขึ้น โดยใช้โปรแกรมแจกแจงรายละเอียดดังต่อไปนี้

```python
# แปลงข้อมูลเป็น DataFrame
df = pd.DataFrame(data)

# คำนวณค่าความถี่ (Frequency)
frequency = df['value'].value_counts()

# คำนวณค่าร้อยละ (Percentage)
percentage = df['value'].value_counts(normalize=True) * 100

# คำนวณค่าเฉลี่ย (Mean)
mean_value = np.mean(df['value'])
```

```python
# คำนวณค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)
std_deviation = np.std(df['value'])

# แสดงผลลัพธ์
print("ค่าความถี่:")
print(frequency)
print("\nค่าร้อยละ:")
print(percentage)
print("\nค่าเฉลี่ย:")
print(mean_value)
print("\nค่าส่วนเบี่ยงเบนมาตรฐาน:")
```

รูปที่ 2 โปรแกรมแสดงการการประเมินและปรับปรุง

จากรูปที่ 2 โปรแกรมแสดงการการประเมินและปรับปรุงสามารถแยกชิ้นส่วนได้ดังนี้ (1) value_counts() ใช้สำหรับคำนวณค่าความถี่ของข้อมูลในคอลัมน์ของค่า value ใน DataFrame `df` (2) normalize=True ใน value_counts() จะทำให้ได้ค่าร้อยละ (3) np.mean() ใช้ในการคำนวณ

ค่าเฉลี่ยของข้อมูลในคอลัมน์ของ value (4) np.std() ใช้ในการคำนวณค่าส่วนเบี่ยงเบนมาตรฐานของข้อมูลในคอลัมน์ของ value

5) การทดสอบและการนำไปใช้งาน เป็นการทดสอบโมเดลที่ปรับปรุงแล้วในระบบจริง เพื่อตรวจสอบว่ามันสามารถทำงานได้ตามที่ต้องการหรือไม่ และการตรวจสอบความเรียบร้อยของการตรวจสอบและการแจ้งเตือน

6) การบำรุงรักษาและการอัพเดต เป็นการปรับปรุงและอัพเดตโมเดลออโตมาต้าอย่างสม่ำเสมอเพื่อให้สามารถรับมือกับความเปลี่ยนแปลงในสภาพแวดล้อมและการโจมตีที่เปลี่ยนไปได้

3.2 เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการวิจัย คือ การวิเคราะห์ข้อมูลในการวิจัยในครั้งนี้ เพื่อเป็นการตอบวัตถุประสงค์และทดสอบสมมุติฐานการวิจัยคือ การวิเคราะห์ระดับความพร้อมด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ และด้านความมั่นคงปลอดภัยทางด้านสารสนเทศในศูนย์ไซเบอร์ซีคิวริตี้ ดังนั้นสถิติที่ใช้ในการวิเคราะห์ข้อมูลจะประกอบด้วยสมการดังต่อไปนี้

ค่าความถี่ (Frequency) โดยใช้สูตร

$$f = \frac{n}{T} \tag{1}$$

โดยที่ f คือ ค่าความถี่ (frequency) n คือ จำนวนครั้งที่เหตุการณ์เกิดขึ้น และ T คือ ช่วงเวลาหรือจำนวนทั้งหมดของเหตุการณ์ที่ถูกนับ

ค่าร้อยละ (Percentage) โดยใช้สูตร

$$\text{Percentage} = \frac{\text{ส่วนหนึ่ง}}{\text{จำนวนทั้งหมด}} \text{ X } 100 \tag{2}$$

ค่าเฉลี่ย (Mean) โดยใช้สูตร

$$\text{Mean} = \frac{\sum \text{data}}{n} \tag{3}$$

โดยที่ $\sum$data หมายถึง ผลรวมของข้อมูลทั้งหมด และ n หมายถึง จำนวนข้อมูลทั้งหมด

ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) โดยใช้สูตร

$$\text{Varience} = \frac{\sum\left(x_i - \text{Mean}\right)^2}{N} \quad (4)$$

โดยที่ x_i คือ ค่าข้อมูลแต่ละตัวในชุดข้อมูล และ Mean คือ ค่าเฉลี่ยของชุดข้อมูล และ N คือ จำนวนข้อมูลทั้งหมด

3.3 สถิติที่ใช้ในการวิเคราะห์ข้อมูล

งานวิจัยนี้มีการดำเนินการโดยใช้เครื่องมือดังต่อไปนี้ SPSS, MATLAB, และ WE-KA เพื่อวิเคราะห์ค่าทางสถิติและความสัมพันธ์ทางสถิติด้วยระดับความเชื่อมั่น 95% และความคลาดเคลื่อนที่ยอมรับได้ 0.05% สำหรับการตัดสินใจยอมรับหรือปฏิเสธสมมติฐานของการศึกษา ดังนั้นกระบวนการวิจัยประกอบด้วยการออกแบบการวิจัย, ขั้นตอนการวิจัย, เครื่องมือและอุปกรณ์, กลุ่มตัวอย่าง, การเก็บข้อมูล, การวิเคราะห์ข้อมูล, และการกำหนดเกณฑ์การประเมิน พร้อมนำเสนอวิธีการประเมินข้อมูล [13-15]

3.4 การวิเคราะห์ข้อมูล

การเก็บรวบรวมข้อมูลทางการพัฒนาการตรวจสอบ และแจ้งเตือนการรักษาความมั่นคงปลอดภัย มีขั้นตอนที่สำคัญ คือ การรวบรวมข้อมูลจากแหล่งต่าง ๆ เช่น logs และ reports, การวิเคราะห์ข้อมูลเชิงเนื้อหาเพื่อค้นหาแนวโน้มและปัญหาที่เกิดขึ้น, และการสร้างรายงานเพื่อการแจ้งเตือนและตัดสินใจทางธุรกิจอย่างมีประสิทธิภาพ. ขั้นตอนนี้ช่วยเพิ่มความมั่นใจในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและเทคโนโลยีขององค์กรได้ดีขึ้น

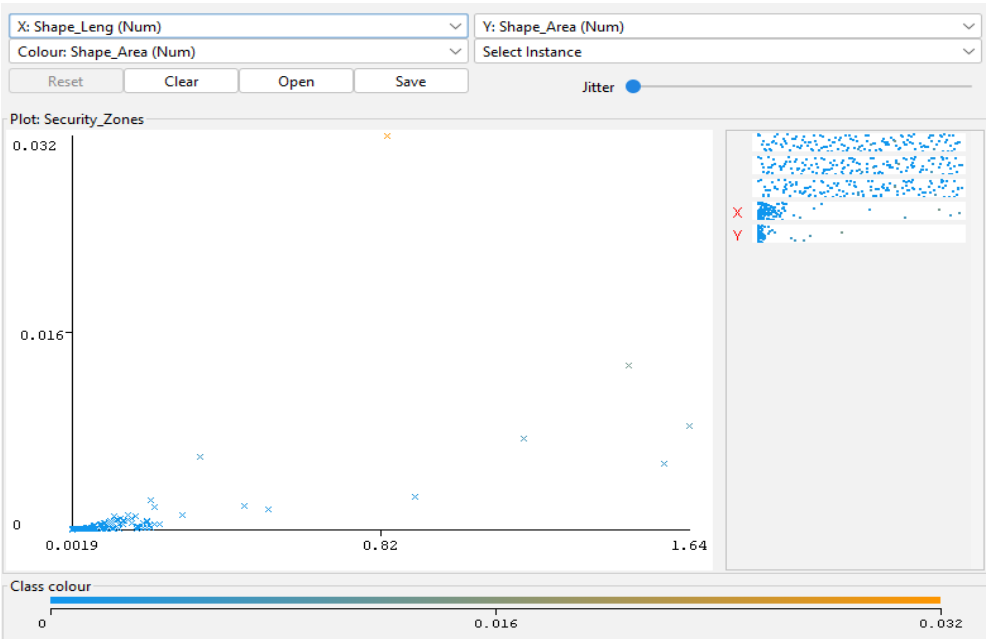
4. ผลการวิจัย

งานวิจัยครั้งนี้มีวัตถุประสงค์เพื่อการทดสอบและการตรวจสอบระบบปฏิบัติการ เพื่อการรับรองการทำงานได้ตามที่กำหนดไว้ และการตรวจสอบความเรียบร้อยของการตรวจสอบ และการแจ้งเตือนของระบบปฏิบัติการได้อย่างถูกต้อง โดยสามารถสรุปผลการวิจัยออกเป็น 4 ส่วน ดังต่อไปนี้

ส่วนที่ 1: การทดสอบและการตรวจสอบของระบบปฏิบัติการ

กระบวนการที่ใช้ในการตรวจสอบความถูกต้องและประสิทธิภาพของระบบปฏิบัติการ โดยใช้โปรแกรม WE-KA เพื่อทำการวิเคราะห์ข้อมูล [15] เพื่อมุ่งเน้นเกี่ยวกับการทดสอบฟังก์ชันต่าง ๆ

ตามรายละเอียดของการทดสอบระบบปฏิบัติการ ดังต่อไปนี้ การวางแผนและการออกแบบการทดสอบ, การเลือกเครื่องมือและเทคโนโลยีที่เหมาะสม,การจัดการข้อมูลการทดสอบ, การทำงานและการประเมินผล, การจัดการการแจ้งเตือนและการแก้ไขข้อผิดพลาดและการเรียนรู้และการพัฒนา สามารถสรุปผลการทดสอบได้ตามรูปที่ 3



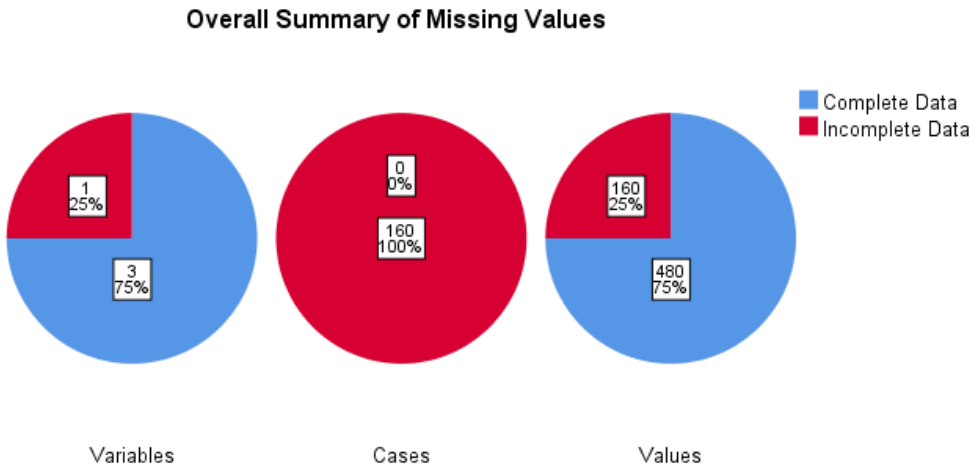
รูปที่ 3 การทดสอบและการตรวจสอบของระบบปฏิบัติการ เพื่อการรับรองการทำงานได้ตามที่กำหนดไว้

จากรูปที่ 3 การทดสอบและการตรวจสอบของระบบปฏิบัติการ เพื่อการรับรองการทำงานได้ตามที่กำหนดไว้ พบว่า การวางแผนและการออกแบบการทดสอบ 4.54 เปอร์เซ็นต์ เนื่องจากการวางแผนการทดสอบอย่างรอบคอบและมีระเบียบ รวมถึงการกำหนดวัตถุประสงค์ของการทดสอบ เช่น การทดสอบฟังก์ชันเฉพาะหรือการทดสอบอินทิเกรตแบบทั่วไป การวางแผนที่เหมาะสมจะช่วยให้การทดสอบเป็นไปอย่างราบรื่นและมีประสิทธิภาพมากขึ้น ขณะที่ การเลือกเครื่องมือและเทคโนโลยีที่เหมาะสม 4.85 เปอร์เซ็นต์ เนื่องจากการเลือกเครื่องมือและเทคโนโลยีที่เหมาะสมสำหรับการทดสอบเป็นสิ่งสำคัญ เช่น เครื่องมือที่ช่วยในการสร้างการทดสอบอัตโนมัติหรือเทคโนโลยีที่ช่วยในการจำลองสภาพแวดล้อมที่ต่างจากการใช้งานได้อย่างปกติมากยิ่งขึ้น ในขณะที่ การจัดการข้อมูลการทดสอบ 4.98 เปอร์เซ็นต์ เนื่องจากการจัดการข้อมูลการทดสอบอย่างเหมาะสมเป็นสิ่งสำคัญ เพื่อให้สามารถเก็บรวบรวมผลลัพธ์การทดสอบได้อย่างเรียบร้อยและ

สามารถใช้ข้อมูลเหล่านั้นในการประเมินและปรับปรุงระบบต่อไป ในขณะที่การทำงานและการประเมินผล 4.77 เปอร์เซ็นต์ เนื่องจาก การทำงานร่วมกับทีมพัฒนาและทีมทดสอบเพื่อให้แน่ใจว่ากระบวนการการทดสอบถูกต้องและเป็นไปตามแผน เรียกใช้ข้อมูลที่ได้รับจากการทดสอบเพื่อประเมินความสมบูรณ์และความพร้อมใช้งานของระบบได้ดีมากยิ่งขึ้น และการจัดการการแจ้งเตือนและการแก้ไขข้อผิดพลาด 4.85 เปอร์เซ็นต์ เนื่องจากการจัดการการแจ้งเตือนและการจัดการข้อผิดพลาดในระหว่างการทดสอบและการดำเนินการเป็นสิ่งสำคัญ เพื่อให้สามารถแก้ไขปัญหาที่พบอย่างรวดเร็วและมีประสิทธิภาพ อย่างไรก็ตามการเรียนรู้และการพัฒนา 4.56 เปอร์เซ็นต์ เนื่องจากการใช้ประสบการณ์จากการทดลองและการประเมินผลเพื่อปรับปรุงกระบวนการการทดสอบในอนาคต โดยการปรับปรุงเทคนิคการทดสอบและการใช้เครื่องมือเพื่อเพิ่มประสิทธิภาพในการทำงาน

ส่วนที่ 2: การตรวจสอบความเรียบร้อยของการตรวจสอบ

การตรวจสอบความเรียบร้อยของการตรวจสอบ เป็นกระบวนการที่มุ่งเน้นการตรวจสอบและยืนยันว่ากระบวนการตรวจสอบเองถูกดำเนินการอย่างถูกต้องและเป็นประสิทธิภาพตามที่กำหนดไว้หรือไม่ เช่นเดียวกับกระบวนการการทดสอบและการตรวจสอบระบบปฏิบัติการที่ได้กล่าวไว้ตามส่วนที่ 1 ซึ่งการตรวจสอบมีดังต่อไปนี้ การเปรียบเทียบผลลัพธ์, การตรวจสอบเงื่อนไขการทดสอบ, การตรวจสอบข้อมูลเข้าระบบ, การวิเคราะห์และการรายงาน และการตรวจสอบข้อกำหนดและมาตรฐาน โดยสามารถสรุปผลการทดสอบได้ตามรูปที่ 4

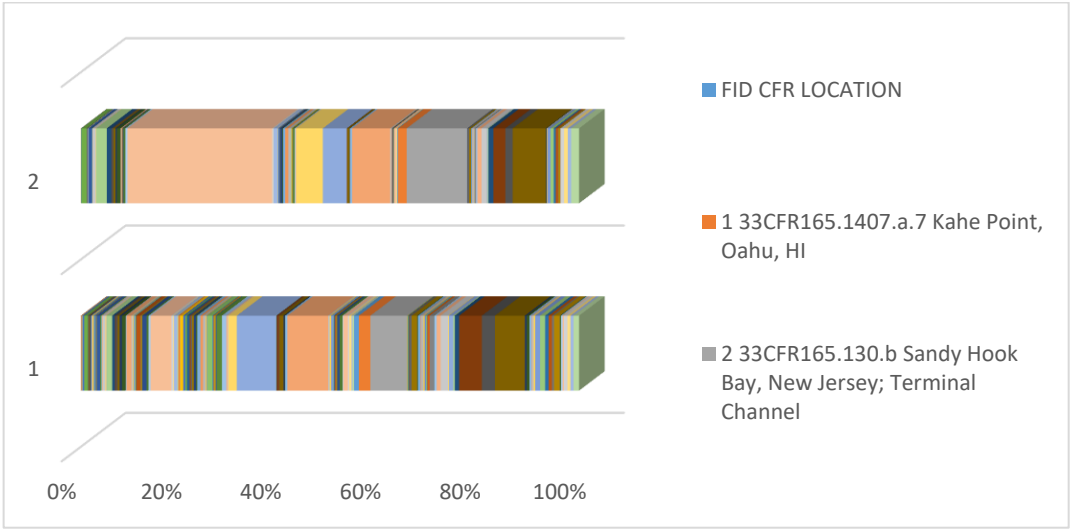


รูปที่ 4 การตรวจสอบความเรียบร้อยของการตรวจสอบ

จากรูปที่ 4 การตรวจสอบความเรียบร้อยของการตรวจสอบ พบว่า การตรวจสอบความเรียบร้อยของระบบประกอบด้วยหลายขั้นตอนที่สำคัญ เพื่อให้แน่ใจว่าระบบทำงานตามมาตรฐานและความคาดหวังที่กำหนดไว้ดังต่อไปนี้ การเปรียบเทียบผลลัพธ์ 4.87% ชี้ให้เห็นถึงความจำเป็นในการเปรียบเทียบผลลัพธ์จากการตรวจสอบกับผลลัพธ์ที่คาดหวัง เพื่อยืนยันความสอดคล้องและความถูกต้อง ตามด้วยการตรวจสอบเงื่อนไขการทดสอบที่ 4.64% ซึ่งเน้นการตั้งเงื่อนไขทดสอบให้เหมาะสมและครอบคลุมทุกแง่มุมที่จำเป็น การตรวจสอบข้อมูลเข้าระบบที่ 4.78% ยืนยันว่าข้อมูลที่ใช้ในการทดสอบถูกต้องและเกี่ยวข้อง ขณะที่การวิเคราะห์และการรายงานที่ 4.93% คือการตรวจสอบและวิเคราะห์ผลลัพธ์เพื่อระบุและแก้ไขปัญหาที่พบ และการตรวจสอบข้อกำหนดและมาตรฐานที่ 4.82% เพื่อยืนยันว่าการทดสอบปฏิบัติตามแนวทางและมาตรฐานที่กำหนดไว้ เหล่านี้รวมกันช่วยให้มั่นใจว่าระบบที่ตรวจสอบมีความน่าเชื่อถือและตรงตามความต้องการที่กำหนดไว้

ส่วนที่ 3: การแจ้งเตือนของระบบปฏิบัติการ

การแจ้งเตือนของระบบปฏิบัติการ เป็นข้อความหรือสัญญาณที่ระบบปฏิบัติการสร้างขึ้นเพื่อแจ้งเตือนผู้ใช้เกี่ยวกับเหตุการณ์หรือสถานะต่าง ๆ ที่เกิดขึ้นในระบบ ซึ่งอาจเป็นข้อมูลที่มีความสำคัญหรือการแจ้งเตือนเกี่ยวกับปัญหาที่ต้องการให้ผู้ใช้รับทราบและดำเนินการต่อไป ประเภทของการแจ้งเตือน, ระดับความสำคัญของการแจ้งเตือน, วิธีการแจ้งเตือน, การปรับแต่งการแจ้งเตือน, การบันทึกประวัติการแจ้งเตือน และการตรวจสอบความเรียบร้อยของการแจ้งเตือน โดยสามารถสรุปผลการทดสอบได้ตามรูปที่ 5

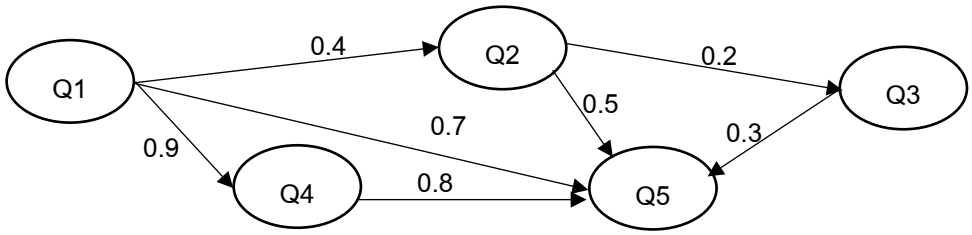


รูปที่ 5 การแจ้งเตือนของระบบปฏิบัติการ

จากรูปที่ 5 การแจ้งเตือนของระบบปฏิบัติการ พบว่า ประเภทของการแจ้งเตือน (4.76%) เป็นการแจ้งเตือนมีหลายประเภทตั้งแต่ข้อผิดพลาดของระบบ, การแจ้งเตือนสถานะปกติ รวมถึงการแจ้งเตือนกิจกรรมเฉพาะ เช่น การเข้าสู่ระบบ ขณะที่ระดับความสำคัญของการแจ้งเตือน (4.87%) เป็นการแจ้งเตือนมีระดับความสำคัญที่แตกต่างกัน ตั้งแต่ระดับสูงสุดสำหรับเหตุการณ์สำคัญมาก ไปจนถึงระดับต่ำสำหรับเหตุการณ์ที่ไม่เป็นไปตามปกติ ในขณะที่วิธีการแจ้งเตือน (4.98%) มีหลากหลายวิธีในการแจ้งเตือน ไม่ว่าจะเป็นการแสดงข้อความบนหน้าจอ, การส่งอีเมล์หรือ SMS, การเปิดเสียงเตือน, หรือการใช้แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ในขณะที่การปรับแต่งการแจ้งเตือน (4.85%) ซึ่งผู้ใช้สามารถปรับแต่งการแจ้งเตือนได้ตามความต้องการ เพื่อให้เหมาะสมกับการใช้งานและความสำคัญของแต่ละเหตุการณ์ ในขณะที่การบันทึกประวัติการแจ้งเตือน (4.79%) เป็นระบบสามารถบันทึกประวัติการแจ้งเตือนไว้เพื่อการตรวจสอบและวิเคราะห์ในอนาคต ช่วยในการเรียนรู้และการปรับปรุงระบบแจ้งเตือน และในขณะที่การตรวจสอบความเรียบร้อยของการแจ้งเตือน (4.83%) มีการตรวจสอบการทำงานของระบบแจ้งเตือนเพื่อให้แน่ใจว่ามีการแจ้งเตือนทุกเหตุการณ์ตามที่กำหนดและป้องกันข้อผิดพลาดที่อาจเกิดขึ้น ซึ่งการวิเคราะห์นี้ช่วยให้เข้าใจถึงแง่มุมต่างๆ ของการแจ้งเตือนในระบบปฏิบัติการ และความสำคัญของการมีระบบแจ้งเตือนที่มีประสิทธิภาพ ซึ่งสามารถปรับแต่งได้ตามความต้องการของผู้ใช้ และสามารถบันทึกประวัติไว้เพื่อการวิเคราะห์และการปรับปรุงในอนาคต

ส่วนที่ 4: การวิเคราะห์แนวทางการพัฒนาการตรวจสอบ และแจ้งเตือนการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการด้วยการประยุกต์ใช้โมเดลออโตมาตา

ในบริบทของ automata (หรือ finite automata) เป็นโครงสร้างทางคณิตศาสตร์ที่ใช้ในการศึกษาการคำนวณและการรู้จำรูปแบบ (pattern recognition) คำว่า "node" หมายถึง "state" หรือสถานะภายใน automaton ประกอบด้วย 1) States (Nodes) คือจุดในกราฟที่แสดงถึงสถานะต่างๆ ของระบบ ซึ่งรวมถึงสถานะเริ่มต้น (initial state) และสถานะสิ้นสุด (accepting/final state) 2) Alphabet ก็คือชุดของสัญลักษณ์ที่ automaton สามารถประมวลผลได้ 3) Transition Function คือฟังก์ชันที่ระบุวิธีการเปลี่ยนแปลงจากสถานะหนึ่งไปยังสถานะหนึ่งไปตามสัญลักษณ์ที่ได้รับ 4) Initial State คือสถานะที่ automaton เริ่มต้นการประมวลผล 5) Accepting States คือสถานะที่ถ้า automaton หยุดที่สถานะนั้น จะถือว่าได้รู้จำสัญลักษณ์ (input) สำเร็จ โดยผู้วิจัยศึกษาแนวคิดเพื่อนำมาใช้ในการพัฒนาระบบปฏิบัติการที่มีความสามารถในการทำงานแบบอัตโนมัติและสามารถประสานงานกับอุปกรณ์และทรัพยากรต่าง ๆ โดยที่มีการนำเทคโนโลยีอัจฉริยะมาใช้งานเพื่อเพิ่มประสิทธิภาพและความสะดวกสบายในการใช้งานสำหรับผู้ใช้งาน อย่างไรก็ตามจากการทดสอบการทำงานของโมเดลออกโตมาตาได้ดังตามรูปที่ 6



รูปที่ 6 การวิเคราะห์แนวทางการพัฒนาการตรวจสอบ และแจ้งเตือนการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการด้วยการประยุกต์ใช้โมเดลออโตมาตา

จากรูปที่ 6 การวิเคราะห์แนวทางการพัฒนาการตรวจสอบ และแจ้งเตือนการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการด้วยการประยุกต์ใช้โมเดลออโตมาตา พบว่า การวิเคราะห์ข้อมูลสัมพันธ์กับการสร้างโมเดลออโตมาตามีค่าความสัมพันธ์อยู่ที่ 0.7 เปอร์เซ็นต์ ซึ่งอยู่ในระดับมากอย่างมีนัยสำคัญ การวิเคราะห์ข้อมูลช่วยให้เข้าใจความสัมพันธ์ระหว่างข้อมูลและใช้ปัญญาประดิษฐ์ในการสร้างโมเดลออโตมาตาที่มีประสิทธิภาพ ส่วนการตรวจสอบและวิเคราะห์สัมพันธ์กับการแจ้งเตือนมีความสอดคล้องกับการประเมินความเสี่ยงและการปรับปรุงเรียนรู้ โดยมีค่าความสัมพันธ์อยู่ที่ 0.9 เปอร์เซ็นต์ ซึ่งอยู่ในระดับมากอย่างมีนัยสำคัญ การตรวจสอบและแจ้งเตือนช่วยให้ผู้ใช้สามารถตัดสินใจได้อย่างมีประสิทธิภาพ

5. สรุปผลการวิจัย

การศึกษาและวิจัยที่นำเสนอเป็นการวิเคราะห์แนวทางการพัฒนาการตรวจสอบ เฝ้าระวัง และแจ้งเตือนการรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการด้วยการประยุกต์ใช้โมเดลออโตมาตา (Automata) ซึ่งมีวัตถุประสงค์หลักที่ชัดเจนดังนี้ 1) ศึกษาบริบท ปัญหาและสถานการณ์ความมั่นคงปลอดภัยของระบบปฏิบัติการ เป็นการวิจัยมุ่งเน้นการวิเคราะห์และทำความเข้าใจเกี่ยวกับสภาพแวดล้อมที่ระบบปฏิบัติการต้องเผชิญ ปัญหาที่อาจเกิดขึ้น และวิธีการที่เหมาะสมในการดำเนินการเพื่อรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการ 2) พัฒนาวิธีการตรวจสอบ เฝ้าระวังและแจ้งเตือนระดับความมั่นคงปลอดภัย เป็นการวิจัยมุ่งเน้นการพัฒนาเครื่องมือและเทคโนโลยีที่ใช้ในการตรวจสอบระบบปฏิบัติการ เช่น โมเดลออโตมาตาที่สามารถตรวจจับและป้องกันการละเมิดความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ 3) การประเมินระบบตรวจสอบ เฝ้าระวัง และแจ้งเตือน เป็นการวิจัยมุ่งเน้นการทดสอบและประเมินประสิทธิภาพของระบบตรวจสอบและแจ้งเตือนในการควบคุมและรักษาความมั่นคงปลอดภัยของระบบปฏิบัติการ โดยมีผลการวิจัยแสดงให้เห็นถึงความสำเร็จในหลายด้านดังต่อไปนี้ การทดสอบและการตรวจสอบระบบปฏิบัติการ พบว่าการจัดการข้อมูลการทดสอบและการเลือกเครื่องมือที่เหมาะสมมีความสำเร็จสูง ซึ่งช่วยให้มีโมเดลที่มีประสิทธิภาพในการตรวจสอบและเฝ้าระวังความปลอดภัย และการตรวจสอบความเรียบร้อย

ของการตรวจสอบ พบว่า การวิเคราะห์และการรายงานรวมถึงการตรวจสอบข้อกำหนดและมาตรฐานแสดงให้เห็นถึงความเรียบร้อยของการตรวจสอบที่ทำให้ระบบได้รับการปรับปรุงและพัฒนาอย่างต่อเนื่อง และการแจ้งเตือนของระบบปฏิบัติการ พบว่ามีวิธีการแจ้งเตือนและการปรับแต่งได้รับคะแนนสูงเนื่องจากสามารถส่งข้อมูลและแจ้งเตือนเหตุการณ์ที่เกิดขึ้นในระบบได้อย่างมีประสิทธิภาพ และการวิเคราะห์แนวทางการพัฒนา พบว่า การทำความเข้าใจและการสร้างโมเดลออโตมาตาที่สามารถตรวจจับและป้องกันการละเมิดความมั่นคงปลอดภัยของระบบปฏิบัติการ พร้อมทั้งการอัพเดตและการเสริมความมั่นคงปลอดภัยของระบบตามความเสี่ยงและภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งผลการวิจัยนี้ช่วยให้นักวิจัยและผู้ดูแลระบบปฏิบัติการเข้าใจและจัดการกับความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ และเพื่อพัฒนาวิธีการป้องกันที่มีความมั่นคงปลอดภัยและคุ้มค่าต่อการใช้งานของระบบปฏิบัติการในอนาคต

References

[1] Molina-Granja F, Molina L, Velasco D, Allauca G, Senthikumar G, Swaminathan N. Demand and employability for the career of engineering in computer security. Inventive Communication and Computational Technologies Conference 2022;383:533-42.

[2] Plerdplern W. The cybersecurity skills development of national cyber security agency [Master of Public Administration]. Bangkok, Thailand: Ramkhamhaeng University; 2022. (In Thai)

[3] Lin J. Research on the security of the application of computer technology and electronic information engineering technology. Journal of Physics Conference Series 2021;1744(3): 032126. doi:10.1088/1742-6596/1744/3/032126.

[4] Zhigalov K, Guzueva E, Polovneva S. Automation security in a machine-building plant. IOP Conference Series: Materials Science and Engineering 2021;1111:012067. doi: 10.1088/ 1757-899X/1111/1/012067

[5] Molisakulmongkol P, Praneetpolgrang P, Soonthornsaratul M, Weerakulwattana S, Wuttipornpong A. Operating systems. Bangkok, Thailand: Duangkamonsamai; 2002. (In Thai)

[6] Jungsamarn S, Pangsuk P. Development of surgical safety checklist in operating room in Surin hospital. Udonthani Hospital Medical Journal 2020;28(2):130-42. (In Thai)

[7] Nilmanee P. The relationship between the perception and the use of computer information security systems: a case study of Thairath group [master of business administration]. Pathumthani, Thailand: Rajamangala University of Technology Thanyaburi; 2018. (In Thai)

[8] Gu J, Hua Z, Li M, Chen H. Innovations and applications of operating system security with a hardware-software co-design. Chineses Science Bulletin 2022;67(32):3862-71.

[9] Sipser M. Introduction to the theory of computation. 3rd ed. Boston, USA: Cengage Learning; 2012.

[10] Imsuwan S, Vorarat S. Using automation testing test the software web application: case study of information and communication technology company. DPU Graduate Studies Journal 2018;7(1):1186-97. (In Thai)

[11] Dataset.world. Cyber security (performance measure 5.12) [Internet]. 2020 [cited 2024 January 20]. Available from: https://data.world/datasets/performance-measures

[12] Rohini N, Sharmila B. RT-IoT2022 [Internet]. 2024 [cited 2024 January 20]. Available from: https://archive.ics.uci.edu/dataset/942/rt-iot2022.

[13] Wikipedia. SPSS statistics [Internet]. 1968 [cited 2024 January 20]. Available from: https://en.wikipedia.org/wiki/SPSS

[14] Wikipedia. MATLAB programming language. [Internet]. 1970s [cited 2024 January 20]. Available from: https://en.wikipedia.org/wiki/MATLAB

[15] Wikipedia. Waikato Environment for Knowledge Analysis (WEKA) [Internet]. 2022 [cited 2024 January 20]. Available from: https://en.wikipedia.org/wiki/Weka_(software)

ประวัติผู้เขียนบทความ

ทิภาพร ศุภมิตร อาจารย์สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษมบัณฑิต เลขที่ 60 ถนนร่มเกล้า แขวงมีนบุรี เขตมีนบุรี กรุงเทพฯ 10510 E-mail: tipaporn.sup@kbu.ac.th สนใจงานวิจัยด้านสมาร์ทซิตี้/สมาร์ทคอมมูนิตี้ วิศวกรรมซอฟต์แวร์ ดาต้าไมนิ่ง ระบบปฏิบัติการ ระบบเทคโนโลยีสารสนเทศ

สุวิทย์ วงศ์คุ้มสิน อาจารย์สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษมบัณฑิต เลขที่ 60 ถนนร่มเกล้า แขวงมีนบุรี เขตมีนบุรี กรุงเทพฯ 10510 E-mail: suwit@kbu.ac.th
สนใจงานวิจัยด้านระบบฐานข้อมูล การพัฒนาเว็บแอปพลิเคชัน แอปพลิเคชันบนสมาร์ทโฟน

ชนะธิป ธำรงวิทยภาคย์ อาจารย์สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษมบัณฑิต เลขที่ 60 ถนนร่มเกล้า แขวงมีนบุรี เขตมีนบุรี กรุงเทพฯ 10510 E-mail: chanatip.vv@gmail.com
สนใจงานวิจัยด้านระบบเครือข่ายคอมพิวเตอร์ เครือข่ายเซนเซอร์ไร้สาย

อิฐติศักดิ์ เมืองสง อาจารย์สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษมบัณฑิต เลขที่ 60 ถนนร่มเกล้า แขวงมีนบุรี เขตมีนบุรี กรุงเทพฯ 10510 E-mail: ittisak.ms@gmail.com
สนใจงานวิจัยด้านความปลอดภัยในระบบเครือข่ายคอมพิวเตอร์ เครือข่ายเซนเซอร์ไร้สาย

Article History:
Received: February 21, 2024
Revised: August 1, 2024
Accepted: August 21, 2024