สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวด้วยเทคนิคกฎความสัมพันธ์

ธนกร มีหินกอง*
นักศึกษา คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
ประสงค์ ปราณีตพลกรัง
รองศาสตราจารย์ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม
นิเวศ จิระวิชิตชัย
อาจารย์ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

* ผู้นิพนธ์ประสานงาน โทรศัพท์ 08-6060-4506 อีเมล: thanakorn.phd@gmail.com
รับเมื่อ 1 สิงหาคม 2557 ตอบรับเมื่อ 24 กุมภาพันธ์ 2558 เผยแพร่ออนไลน์ 14 พฤษภาคม 2558
DOI: 10.14416/j.kmutnb.2015.02.003 © 2015 King Mongkut's University of Technology North Bangkok. All Rights Reserved.

บทคัดย่อ

ระบบการตรวจหาการบุกรุกเป็นระบบที่ใช้ตรวจหาผู้ที่บุกรุกเข้ามาในเครือข่ายคอมพิวเตอร์เพื่อมุ่งทำลายระบบหรือขโมยข้อมูลที่สำคัญ ในปัจจุบันพบว่าการบุกรุกมีการพัฒนารูปแบบใหม่เพิ่มขึ้นอย่างต่อเนื่อง จึงทำให้เกิดการศึกษาวิจัยเพื่อปรับปรุงระบบการตรวจหาและวิเคราะห์รูปแบบการบุกรุกให้มีประสิทธิภาพมากยิ่งขึ้น งานวิจัยฉบับนี้ได้ศึกษาและออกแบบสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวใหม่ โดยใช้ตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการพลศึกษาตามมาตรฐาน ISO/IEC 27005 มาตรฐาน ISO/DIS 31000 และมาตรฐาน OCTAVE เพื่อตรวจสอบวัดผลปัจจัยความเสี่ยงด้านต่าง ๆ ควบคู่ไปกับการตรวจสอบจากระบบตรวจหาการบุกรุกแบบปรับตัว ด้วยเทคนิคเหมืองข้อมูลจากการวิเคราะห์ด้วยกฎความสัมพันธ์จากโครงข่ายประสาทเทียม จากผลการทดลองพบว่าระบบตรวจหาการบุกรุกที่ได้พัฒนาขึ้นนี้สามารถรายงานผลได้อย่างรวดเร็วโดยมีค่าความเที่ยงที่ 97.4% และค่าเรียกคืนที่ 92.0% จึงสามารถนำไปใช้วิเคราะห์และทำนายผลการรักษาความมั่นคงปลอดภัยไซเบอร์ได้ต่อไป

คำสำคัญ: สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ระบบตรวจหาการบุกรุกแบบปรับตัว เหมืองข้อมูล

การอ้างอิงบทความ: ธนกร มีหินกอง, ประสงค์ ปราณีตพลกรัง และ นิเวศ จิระวิชิตชัย, "สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวด้วยเทคนิคกฎความสัมพันธ์," *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, ปีที่ 25, ฉบับที่ 2, หน้า 277 - 288, พ.ค. - ส.ค. 2558. http://dx.doi.org/10.14416/j.kmutnb.2015.02.003

Cybersecurity Knowledge Architecture for Supporting the Adaptive Intrusion Detection Systems Using Association Rules

Thanakorn Mehinkong*
Student, School of Information Technology, Sripatum University, Bangkok, Thailand

Prasong Praneetpolgrang
Associate Professor, School of Information Technology, Sripatum University, Bangkok, Thailand

Nivet Chirawichitchai
Lecturer, School of Information Technology, Sripatum University, Bangkok, Thailand

* Corresponding Author, Tel. 08-6060-4506, E-mail: thanakorn.phd@gmail.com
Received 1 August 2014; Accepted 24 February 2015; Published online: 14 May 2015
DOI: 10.14416/j.kmutnb.2015.02.003 © 2015 King Mongkut's University of Technology North Bangkok. All Rights Reserved.

Abstract

The Intrusion Detection Systems are used for detecting and preventing the organizations' computer networks from malicious intruders, who access to destroy or steal crucial information. Nowadays, many new intrusive attacks have been developing continuously. Therefore, many researchers have tried to find out more effective solutions. In this paper, we studied and designed a new Cybersecurity Knowledge Architecture for Supporting the Adaptive Intrusion Detection Systems by using Cybersecurity Risk Assessments Model of Physical Institute of Education according to the standard of ISO/IEC 27005, ISO/DIS 31000, and OCTAVE to measure risk factors. At the same time, we developed the Adaptive Cyber Intrusion Detection System by applying Neural Network with Association rules in Data Mining technique to classify the information of attack computer network. Finally, we have found that our developed detection system is able to report the results promptly and accurately with the precision at 97.4% and the recall at 92.0% which are easy to analyze and predict the results of Cybersecurity.

Keywords: Cybersecurity Knowledge Architecture, Adaptive Intrusion Detection Systems, Data Mining

Please cite this article as: T. Mehinkong, P. Praneetpolgrang and N. Chirawichitchai, "Cybersecurity Knowledge Architecture for Supporting the Adaptive Intrusion Detection Systems Using Association Rules," *J. KMUTNB*, Vol. 25, No. 2, pp. 277 - 288, May. - Aug. 2015 (in Thai). http://dx.doi.org/10.14416/j.kmutnb.2015.02.003

1. บทนำ

การบุกรุกเพื่อหาผลประโยชน์ในระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันมีจำนวนเพิ่มมากขึ้น รวมทั้งมีวิธีหลีกเลี่ยงการตรวจจับจากเครื่องมือต่างๆ และความหลากหลายของรูปแบบการโจมตีที่ซับซ้อนขึ้น เหตุจูงใจส่วนใหญ่มาจากการขยายตัวอย่างรวดเร็วในการประยุกต์ใช้เครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตในองค์กรภาครัฐ ภาคเอกชนและส่วนบุคคลเพื่อทำธุรกรรม ด้านการเงิน ด้านสาธารณูปโภค ด้านการสื่อสาร

ดังนั้น ความสำคัญในการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตรวมถึงข้อมูลที่อยู่ในเครือข่าย จึงเป็นสิ่งจำเป็นที่ทุกองค์กรและทุกคนควรหาแนวทางและวิธีการในการป้องกันอย่างเหมาะสม การนำระบบตรวจหาการบุกรุก (Intrusion Detection Systems: IDS) มาใช้จะช่วยลดปัญหาลงได้บ้างในระยะหนึ่ง เมื่อเวลาผ่านไปการบุกรุกโจมตีก็เกิดขึ้นใหม่ ซึ่งแสดงให้เห็นว่ามีรูปแบบการบุกรุกโจมตีแบบใหม่เกิดขึ้นตลอดเวลา งานวิจัยในด้านนี้มีผู้สนใจศึกษามากขึ้นโดยนำทฤษฎีและวิธีการต่างๆ มากมายมาช่วยในการวิเคราะห์รูปแบบการบุกรุก เช่น การใช้แผนภาพการจัดระเบียบตัวเอง (Self Organizing Map) [1], [2] รวบรวมคุณสมบัติของความถี่ที่เกิดเหตุการณ์บุกรุกการใช้ทฤษฎีการสุ่มเมทริกซ์และระบุผ่านการคำนวณของการวัดความคล้ายกันของเครือข่าย [3] การใช้วิธีวัดความคล้ายกันโดยใช้การจัดกลุ่มด้วยการระบุจำนวนที่เหมาะสมของกลุ่มแบบ Hidden Markov Model [4], [5] การเปรียบเทียบในรายละเอียดย่อยของพฤติกรรมผู้ใช้เครือข่ายแล้วค้นหาองค์ประกอบที่คล้ายกัน

งานวิจัยครั้งนี้จะศึกษาและออกแบบสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวโดยใช้ตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการพลศึกษาตามมาตรฐาน ISO/IEC 27005 [5] มาตรฐาน ISO/DIS 31000 [6] และมาตรฐาน OCTAVE [7] เพื่อตรวจสอบวัดผลปัจจัยความเสี่ยงทางด้านต่างๆ ควบคู่ไปกับการตรวจสอบจากระบบตรวจหาการบุกรุกแบบมีการสอน [8] ด้วยเทคนิคเหมืองข้อมูลจากกฎการวิเคราะห์ความสัมพันธ์ของโครงข่ายประสาทเทียม (Association Rules) เพื่อตรวจจับการโจมตีเครือข่ายคอมพิวเตอร์จากผู้บุกรุก [9], [10]

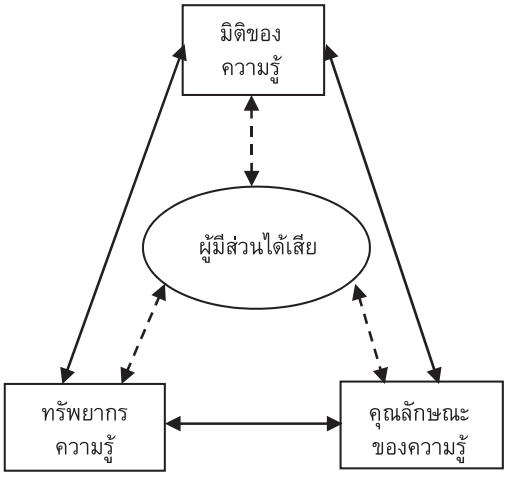
การนำเสนอในส่วนที่เหลือเรียงลำดับดังนี้คือทฤษฎีและงานวิจัยที่เกี่ยวข้อง การดำเนินการวิจัย ผลการวิจัยและอภิปรายผลและสรุป

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การวิจัยครั้งนี้ได้ศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้องด้านสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ด้านระบบตรวจหาการบุกรุก ระบบการเรียนรู้ การวิเคราะห์รูปแบบการบุกรุกและข้อมูลทดสอบระบบตรวจหาการบุกรุก โดยมีรายละเอียดดังนี้

2.1 สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Knowledge Architecture)

สถาปัตยกรรมความรู้หมายถึงสถาปัตยกรรมสารสนเทศและข้อมูลกับสภาพแวดล้อมที่เน้นผลกระทบและความสัมพันธ์ระหว่างมนุษย์กับมนุษย์ มนุษย์กับความรู้ ความรู้กับความรู้ การพัฒนาสถาปัตยกรรมความรู้เป็นการออกแบบโครงสร้างการทำงานขององค์ประกอบต่างๆ ให้ทำงานอย่างสัมพันธ์กัน [11] การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นกลไกในการปกป้องโครงสร้างพื้นฐานไอซีทีขององค์กรโดยมีโครงสร้างสถาปัตยกรรมที่ประกอบด้วยผู้มีส่วนได้เสีย (Stakeholders) ได้แก่ ผู้บริหาร ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต อาจารย์ เจ้าหน้าที่ ด้านมิติองค์ความรู้ (Knowledge Dimensions) เกี่ยวกับการปรับแต่งคอมพิวเตอร์และอุปกรณ์เครือข่าย การใช้โปรแกรมระบบปฏิบัติการและอื่นๆ การวิเคราะห์และแก้ไขปัญหาคอมพิวเตอร์และอุปกรณ์เครือข่าย การแก้ไขเหตุการณ์ที่เป็นภัยคุกคาม ด้านคุณลักษณะความรู้ (Knowledge Characteristics) เกี่ยวกับความต้องการความรู้เพื่อนำไปใช้บำรุงรักษา



รูปที่ 1 องค์ประกอบของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

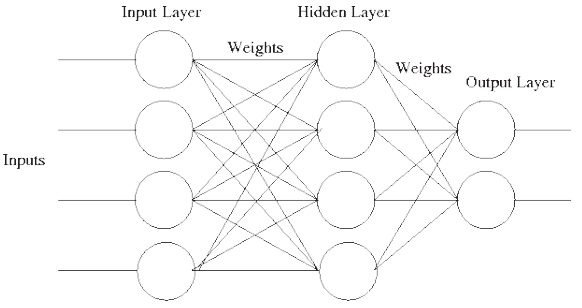
ความมั่นคงปลอดภัยไซเบอร์ ด้านทรัพยากรความรู้ (Knowledge Resources) เกี่ยวกับความรู้ที่มีอยู่ในองค์กร เช่น เอกสาร คู่มือ ตำราหลักสูตรการฝึกอบรมสื่อการสอน วีดีโอ เว็บไซต์แสดงดังรูปที่ 1

2.2 ระบบตรวจหาการบุกรุก (Intrusion Detection Systems)

ระบบตรวจหาการบุกรุก [12] เป็นฮาร์ดแวร์หรือซอฟต์แวร์ที่ติดตามตรวจสอบสัญญาณจราจร (Traffic) ในระบบเครือข่ายคอมพิวเตอร์แล้วแจ้งเตือน (Alert) ให้ผู้รับผิดชอบระบบทราบ ในกรณีมีเหตุการณ์ผิดปกติ (Anomaly) สถาปัตยกรรมระบบตรวจจับการบุกรุกโดยทั่วไปมี 2 ระบบ [13] ดังนี้

ระบบที่ 1 คือระบบตรวจจับการบุกรุกยึดหลักเครือข่าย (Network-based IDS) [14] จะทำงานในเครือข่ายคอมพิวเตอร์ด้วยการติดตามตรวจสอบสัญญาณจราจร (Traffic) ที่อยู่ในรูปของ Packet ข้อมูล โดยตรวจสอบว่า Packet ใดมีลักษณะที่ผิดปกติ

ระบบที่ 2 คือระบบตรวจจับการบุกรุกยึดหลักเครื่องคอมพิวเตอร์ (Host-based IDS) [15] จะทำงานในเครื่องคอมพิวเตอร์ โดยติดตามตรวจสอบสัญญาณ



รูปที่ 2 การทำงานของโครงข่ายประสาทเทียม

จราจร (Traffic) ที่อยู่ในรูปของ Packet ข้อมูล และตรวจสอบการใช้งานโปรแกรมประยุกต์ (Application) ในเครื่องคอมพิวเตอร์ด้วยการใช้ Activity Profiles [16]

งานวิจัยนี้ผู้วิจัยจะใช้ระบบตรวจหาการบุกรุกยึดหลักเครือข่าย (Network-based IDS) ซึ่งสามารถตรวจจับเหตุการณ์ได้ครอบคลุมเครือข่ายมากกว่าระบบตรวจจับการบุกรุกยึดหลักเครื่องคอมพิวเตอร์ (Host-based IDS)

2.3 การเรียนรู้ของโครงข่ายประสาทเทียม (Learning of Neural Network)

โครงข่ายประสาทเทียมเป็นหนึ่งในเทคนิคของการทำเหมืองข้อมูล [17] มีรูปแบบการเรียนรู้โดยทั่วไปมี 2 แบบ คือ

1) การเรียนรู้แบบมีการสอน (Supervised Learning) เป็นการเรียนรู้ที่ต้องมีข้อมูลทั้งข้อมูลอินพุทเข้าระบบและค่าเป้าหมาย ที่เอาท์พุทและใช้ค่าผิดพลาดในการปรับแต่งค่าน้ำหนักหรือพารามิเตอร์ของโครงข่ายหรือโมเดล

2) การเรียนรู้แบบไม่มีการสอน (Unsupervised Learning) เป็นการเรียนรู้ที่ใช้ข้อมูลอินพุทเข้าระบบโดยไม่ต้องกำหนดค่าเป้าหมายที่เอาท์พุท ระบบจะทำการปรับแต่งค่าน้ำหนักหรือพารามิเตอร์ของโครงข่ายหรือโมเดล ตามข้อมูลอินพุท

สำหรับงานวิจัยนี้ จะใช้เทคนิคการทำเหมืองข้อมูลในรูปแบบที่มีการสอนด้วยกฎการวิเคราะห์ความสัมพันธ์เพื่อใช้ประมวลผลข้อมูลเชิงคุณภาพจากรูปแบบการบุกรุกโดยมีรูปแบบโครงข่ายประสาทเทียมแสดงในรูปที่ 2

หลักการทำงานของกฎการวิเคราะห์ความสัมพันธ์เป็นการหาความสัมพันธ์ระหว่างข้อมูลด้วยกันเอง ซึ่งมีพื้นฐานมาจากการเกิดขึ้นร่วมกันหรือพร้อมกันในฐานข้อมูล รูปแบบของการค้นหากฎความสัมพันธ์เป็นรูปแบบทั่วไปของการค้นหากฎความสัมพันธ์คือ

A→B โดยที่ A: เป็นเงื่อนไขหรือ LHS (Left - Hand Side) และ B: เป็นผลลัพธ์ที่เกิดขึ้นหรือ RHS (Right - Hand Side) หรืออยู่ในรูปของ “ถ้า.....แล้ว” (If…… Then….) เช่น

กฎที่ 1: A→B ; if A Then B (1)

กฎที่ 2: B→A ; if B Then A (2)

การประเมินค่าของกฎจะใช้ค่าสนับสนุน (Support) และค่าความเชื่อมั่น (Confidence) โดยที่ค่าสนับสนุนคือเปอร์เซ็นต์ของข้อมูลที่มีเงื่อนไขและผลลัพธ์สอดคล้องตามกฎต่อจำนวนข้อมูลทั้งหมดสามารถเขียนเป็นสมการ (3) ดังนี้

$$\text{ค่าสนับสนุน (A, B)} = \frac{\text{จำนวนของ Transaction (A,B)}}{\text{จำนวน } \textit{Transaction} \text{ ทั้งหมด}} \quad (3)$$

โดยที่ A หมายถึงเหตุการณ์ที่ใช้เป็นเงื่อนไขในการหาผลลัพธ์

B หมายถึงเหตุการณ์ที่เป็นผลลัพธ์

Transaction (A, B) หมายถึงเหตุการณ์ที่ประกอบด้วยเหตุการณ์ A และ B

ค่าความเชื่อมั่นคือเปอร์เซ็นต์ของข้อมูลที่มีเงื่อนไขและผลลัพธ์สอดคล้องตามกฎต่อจำนวนข้อมูลทั้งหมดที่เป็นเงื่อนไขสามารถเขียนเป็นสมการ (4) ดังนี้

$$\text{ค่าความเชื่อมั่น (A, B)} = \frac{\text{จำนวนของ Transaction (A,B)}}{\text{จำนวน } \textit{Transaction (A)}} \quad (4)$$

โดยที่ Transaction (A) หมายถึงเหตุการณ์ที่ประกอบด้วยเหตุการณ์ A อย่างเดียว

สำหรับการเลือกว่าจะใช้กฎใดนั้นจะต้องพิจารณาค่าสนับสนุนและค่าความเชื่อมั่นที่มีค่าสูงกว่าค่าขีดแบ่ง (Threshold) ที่ตั้งไว้นอกจากนี้จะต้องกำหนดค่าสนับสนุนต่ำสุด (Minimum Support) และค่าความเชื่อมั่นต่ำสุด (Minimum Confidence) โดยทั่วไปจะกำหนดค่าสนับสนุนต่ำสุดเป็น 5-10% และค่าความเชื่อมั่นต่ำสุดเป็น 50-100% [18]

ขั้นตอนการทำงานของกฎความสัมพันธ์

เนื่องจากขั้นตอนการทำงานที่ใช้ในการสร้างกฎความสัมพันธ์มีหลากหลายรูปแบบ งานวิจัยนี้จึงเลือกขั้นตอนการทำงานที่นิยมใช้กันแพร่หลายเพื่อนำมาประยุกต์เข้ากับการตรวจหาการบุกรุก โดยผู้วิจัยได้นำรูปแบบขั้นตอนการทำงานแบบอพริโอริ (Apriori Algorithm) [19] ซึ่งเป็นประเภทของการค้นหาความสัมพันธ์แบบตรวจสอบเชิงตรรกะ (Boolean Association Rule) ซึ่งเป็นเทคนิควิธีที่ใช้สำหรับค้นหาสิ่งที่ปรากฏเด่นชัด (Frequent Item Sets) จากฐานข้อมูลที่กำหนด โดยมีหลักการทำงานคือ ขั้นตอนการทำงานแบบอพริโอริจะทำหน้าที่สร้างไอเท็มเซ็ต (Item Set) ที่ต้องการวิเคราะห์ที่เป็นไปได้ทั้งหมดที่มีค่าสนับสนุนมากกว่าค่าสนับสนุนขั้นต่ำโดยจะเริ่มการทำงานในรูปแบบจากล่างขึ้นบน (Bottom up) โดยมีขั้นตอนการทำงานตามรหัสเทียม (Pseudo Codes) ดังนี้

Pseudo Codes for Apriori Algorithm

C_K : Candidate item set of size K

L_K : Frequent item set of size K

L_1 = {Frequent 1 – item set);

For (K = 1; L_K ! = ∅; K++) do

Begin

C_{K+1} = Candidates generated from L_K;

For *each transaction t in database* do

Increment the count of all candidates in

C_{K+1} *that are contained in t*

L_{K+1} = Candidates in C_{K+1} with min_support

End

Return CK LK;

อธิบายขั้นตอนการทำงานตามรหัสเทียม

ขั้นตอนที่ 1 อ่านฐานข้อมูลทั้งหมดและสร้างไอเท็มเซ็ตที่ผ่านค่าสนับสนุนขั้นต่ำความยาว 1 ไอเท็ม (Frequent 1-itemset)

ขั้นตอนที่ 2 สร้างไอเท็มเซ็ตทดสอบ (Candidate Item Set) ที่มีความยาว 2 ไอเท็มจากไอเท็มเซ็ตที่ปรากฏเด่นชัดความยาว 1 ไอเท็มในขั้นตอนแรกและนำไปหาค่าสนับสนุนเพื่อค้นหาไอเท็มเซ็ตที่ปรากฏเด่นชัดความยาว 2 ไอเท็มโดยขั้นตอนการทำงานจะวนรอบทำงานจนกระทั่งไม่พบไอเท็มเซ็ตที่ผ่านค่าสนับสนุนขั้นต่ำจึงจบการทำงานไอเท็มเซ็ตที่ผ่านค่าสนับสนุนขั้นต่ำในแต่ละรอบคือสิ่งที่ปรากฏเด่นชัดจากฐานข้อมูล

2.4 การวิเคราะห์รูปแบบการบุกรุก (Intrusion Analysis)

ระบบตรวจจับการบุกรุกมีวิธีวิเคราะห์รูปแบบการบุกรุกโดยทั่วไป 2 วิธีดังนี้

วิธีที่ 1 เป็นวิธีวิเคราะห์การตรวจจับการใช้งานในทางที่ผิด (Misuse Detection) [20] เป็นการวิเคราะห์พฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายโดยการเปรียบเทียบพฤติกรรมหรือเหตุการณ์ ณ เวลาขณะนั้นกับพฤติกรรมหรือเหตุการณ์ที่เป็นการบุกรุกซึ่งจัดเก็บไว้ในฐานข้อมูลระบบ หากรูปแบบตรงกันแสดงว่าเป็นการบุกรุก

วิธีที่ 2 เป็นวิธีวิเคราะห์การตรวจจับเหตุการณ์ผิดปกติ (Anomaly Detection) [21] เป็นการวิเคราะห์พฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในระบบเครือข่ายโดยการเปรียบเทียบพฤติกรรมหรือเหตุการณ์ ณ เวลาขณะนั้นกับพฤติกรรมหรือเหตุการณ์ที่ปกติซึ่งจัดเก็บไว้ในฐานข้อมูลระบบ หากรูปแบบไม่ตรงกันแสดงว่าเป็นพฤติกรรมหรือเหตุการณ์การบุกรุก วิธีการทำงานของระบบตรวจจับเหตุการณ์ผิดปกติที่นิยมในปัจจุบัน ได้แก่ การตรวจสอบทางเข้า (Threshold Detection) ด้วยการนับจำนวนครั้งของบางเหตุการณ์ที่เกิดขึ้น การวัดด้วยสถิติ (Statistical Measure) เป็นวิธีการวัดการกระจาย คุณสมบัติของโปรไฟล์ที่ใช้วิธีการทางสถิติรวบรวมแล้วสุ่มเหตุการณ์มาเปรียบเทียบกับค่ามาตรฐานที่กำหนดขึ้นเอง หรือเปรียบเทียบกับค่าที่วัดได้จากในอดีต หากเบี่ยงเบนไปจากค่ามาตรฐานที่สร้างไว้ถือว่าผิดปกติ การวัดตามกฎ (Rule-based Measure) เป็นวิธีการวัดโดยกำหนดพฤติกรรมหรือเหตุการณ์ปกติเป็นกฎไว้แล้วนำพฤติกรรมหรือเหตุการณ์ที่เกิดขึ้นในเครือข่าย ณ เวลาในขณะนั้นมาเปรียบเทียบกับกฎ หากไม่ตรงกันแสดงว่าเป็นรูปแบบการบุกรุก แบบผสมผสาน (Hybrid-based IDS) เป็นการวิเคราะห์รูปแบบการโจมตีที่ผสมผสานกันของการตรวจจับการใช้งานในทางที่ผิด (Misuse Detection) และการตรวจจับเหตุการณ์ผิดปกติ (Anomaly Detection) เพื่อเพิ่มประสิทธิภาพในการตรวจจับการบุกรุกโจมตี [16]

ตารางที่ 1 รูปแบบการโจมตี

ที่	กลุ่มการโจมตี 4 กลุ่ม	การโจมตี 22 รูปแบบ
1	Denial of Service (DOS)	Back, Land, Neptune, Pod, Smurt, Teardrop
2	Remote to Local (R2L)	Ftp_write, Guess_passwd, Imap, Multihop, Phf, Spy, Warezclient, Warezmester
3	User to Root (U2R)	Buffer_overflow, Perl, Loadmodule, Rookit
4	Probing	Ipsweep, Nmap, Portsweep, Satan

จากตารางที่ 1 แสดงการแบ่งชุดข้อมูลออกเป็น 4 กลุ่มการโจมตีหลัก คือ DOS, R2L, U2R และ Probe จาก 22 รูปแบบการโจมตีที่แตกต่างกัน

2.5 ชุดข้อมูลทดสอบระบบ

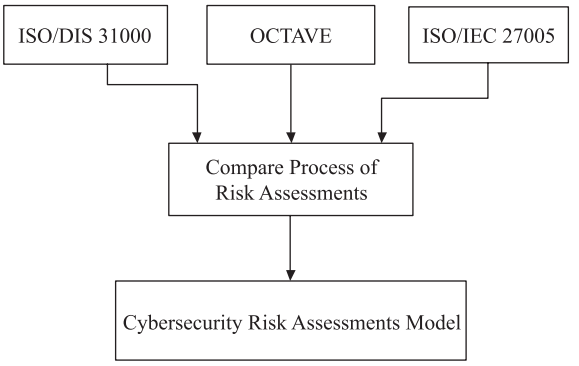
งานวิจัยนี้ใช้ชุดข้อมูล KDD CUP'99 Dataset [22] เป็นฐานข้อมูลในการฝึกและทดสอบประสิทธิภาพ

ของระบบ ซึ่ง KDD CUP'99 Dataset เป็นชุดข้อมูลที่ใช้สำหรับการแข่งขัน The Third International Knowledge Discovery and Data Mining ซึ่งจัดขึ้นร่วมกับ KDD-99 The Fifth International Conference on Knowledge Discovery and Data Mining ซึ่ง KDD CUP'99 dataset ประกอบด้วยข้อมูลขนาดใหญ่มากมีแอทริบิวต์มากถึง 41 แอทริบิวต์ตัวอย่างข้อมูลเช่น 0,tcp,http,SF,174,6345,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,0,0,1,0,0,3,25,5,1,0,0.33,0.02,0,0,0

ข้อมูลเหล่านี้จะถูกแบ่งออกเป็น 2 ชุดคือ 1) ชุดสำหรับใช้สอนระบบให้มีการเรียนรู้รูปแบบการโจมตีและ 2) ชุดสำหรับใช้เป็นข้อมูลสมมติการโจมตีจริงเพื่อวัดผลของระบบที่ได้รับการพัฒนาขึ้นในครั้งนี้

2.6 ตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการพลศึกษาตามมาตรฐาน ISO/IEC 27005 มาตรฐาน ISO/DIS 31000 และมาตรฐาน OCTAVE

ตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในสถาบันการพลศึกษานี้ได้รับการออกแบบและพัฒนาขึ้นจากมาตรฐานการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ คือมาตรฐาน ISO/DIS 31000 [6] มาตรฐาน ISO/IEC 27005 [7] และมาตรฐาน OCTAVE [8] เพื่อใช้สำหรับตรวจสอบและประเมินความเสี่ยงที่ได้จากผลลัพธ์การวิเคราะห์ความสัมพันธ์โดยคำนึงถึงระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ได้แบบประเมินความเสี่ยงที่เหมาะสมกับสถาบันการพลศึกษามากที่สุด ขั้นตอนการพัฒนาตัวแบบประเมินความเสี่ยงดังแสดงในรูปที่ 3



รูปที่ 3 ขั้นตอนการพัฒนาตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

3. การดำเนินการวิจัย

การศึกษาและวิจัยครั้งนี้มีวัตถุประสงค์เพื่อดำเนินการวิเคราะห์และประเมินระดับความพร้อมและสร้างตัวแบบการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์พร้อมทั้งพัฒนาระบบตรวจหาการบุกรุกเชิงเวลาจริงแบบปรับตัวในระบบการรักษาความมั่นคงปลอดภัยไซเบอร์บนพื้นฐานของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีขั้นตอนการดำเนินการวิจัยดังนี้

1) ศึกษาระบบตรวจหาการบุกรุก สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์รวมทั้งกระบวนการและมาตรฐานการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

2) รวบรวมข้อมูลแผนแม่บท โครงสร้างพื้นฐานด้านเทคโนโลยีด้านสารสนเทศและการสื่อสารที่มีอยู่ในปัจจุบันของสถาบันการพลศึกษาที่เป็นกรณีศึกษา

3) สร้างแบบสอบถามเพื่อวิเคราะห์และประเมินระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์พร้อมทั้งหาคุณภาพของแบบสอบถามโดยผู้เชี่ยวชาญและทดลองใช้แบบสอบถามเพื่อให้ได้แบบสอบถามที่มีคุณภาพนำไปเก็บข้อมูลจากกลุ่มตัวอย่างจากนั้นวิเคราะห์ ข้อมูลด้วยค่าทางสถิติเพื่อหาค่าความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์

4) สร้างตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ โดยใช้มาตรฐานการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศคือมาตรฐาน ISO/IEC 27005 มาตรฐาน ISO/DIS 31000 มาตรฐาน OCTAVE และนำระดับความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์มาเป็นเกณฑ์ในการพิจารณาร่วม

5) ออกแบบระบบตรวจหาการบุกรุกบนพื้นฐานสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ด้วยเทคนิคการทำเหมืองข้อมูลด้วยกฎความสัมพันธ์เพื่อให้สามารถตรวจหาและรายงานการบุกรุกได้ทันกับเหตุการณ์การบุกรุกในปัจจุบัน

6) ทดสอบระบบตรวจหาการบุกรุก ด้วยการใช้ข้อมูลทดสอบจาก KDD CUP'99 Dataset โดยการทดสอบและวัดประสิทธิภาพของระบบตรวจหาการบุกรุกที่ได้รับการพัฒนาขึ้นในครั้งนี้ผู้วิจัยจะพิจารณาจากผลลัพธ์ที่ได้จากการวัดค่าความเที่ยง (Precision) และค่าเรียกคืน (Recall)

3.1 การออกแบบระบบ

ระบบตรวจหาการบุกรุกเชิงเวลาจริงแบบปรับตัวบนพื้นฐานของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการออกแบบจะมีความสามารถในการตรวจหาการบุกรุกอย่างถูกต้อง รายงานผลได้เหมาะสมกับสถานการณ์การบุกรุกในปัจจุบันดังแสดงในรูปที่ 4

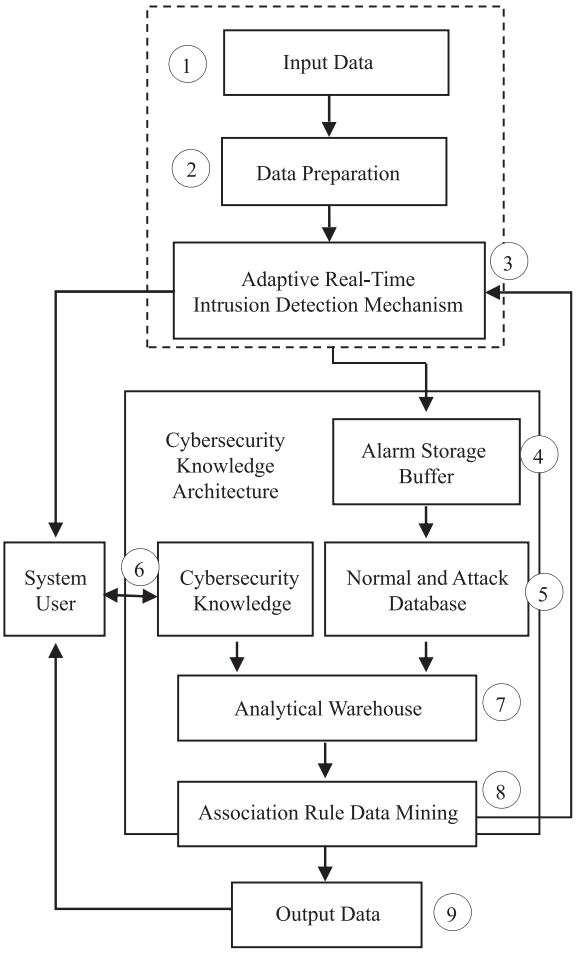
จากรูปที่ 4 แสดงกระบวนการทำงานของสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์อธิบายได้ดังนี้

1) ข้อมูลการบุกรุกจะถูกป้อนเข้าสู่ระบบ (Input Data)

2) ข้อมูลจะถูกจัดเตรียม (Data Preparation) เพื่อเข้าสู่การประมวลผลจากโครงข่ายประสาทเทียมด้วยการทำการนอร์มอลไลเซชัน

3) ข้อมูลที่ผ่านการเตรียมจากกระบวนการที่ 2 จะถูกจัดกลุ่มรูปแบบการบุกรุกทันทีตามเวลาจริง (Real-time) และจะถูกใช้เป็นฐานข้อมูลองค์ความรู้สนับสนุนผู้ดูแลระบบ (System User) ในการแก้ปัญหาเหตุการณ์การบุกรุกและเป็นองค์ความรู้ให้กับผู้ใช้ทั่วไป (User) ได้ศึกษาเพื่อป้องกันความผิดพลาดจากการใช้ระบบและสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยภายในองค์กรให้มีประสิทธิภาพสูงสุด

4) ข้อมูลการบุกรุกที่ถูกปรับแต่ง (Adaptive) จากผู้บริหารระบบ (System Admin) ในกระบวนการที่ 3 จะถูกส่งเข้าฐานพักสัญญาณแจ้งเตือนชั่วคราว (Alarm Buffer) ก่อนส่งเข้าจัดเก็บในฐานข้อมูล



รูปที่ 4 สถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์

5) ข้อมูลจะถูกบันทึกลงฐานข้อมูลสัญญาณเตือนปกติและการโจมตี (Normal and Attacks) เพื่อจัดเก็บข้อมูลในรูปเหตุการณ์ปกติและรูปแบบการบุกรุกโจมตี

6) ฐานข้อมูลความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้จากตัวแบบประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการพลศึกษาตามมาตรฐาน ISO/IEC 27005 มาตรฐาน ISO/DIS 31000 และมาตรฐาน OCTAVE ซึ่งรวบรวมข้อมูลแผนแม่บท โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่มีอยู่ในปัจจุบันมาใช้วิเคราะห์เปรียบเทียบกับข้อมูลบุกรุกที่ตรวจจับได้

7) คลังวิเคราะห์ข้อมูล (Analytical Warehouse) เป็นคลังข้อมูลที่วิเคราะห์และจัดเก็บองค์ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศและข้อมูลเหตุการณ์ปกติและเหตุการณ์ที่เป็นการโจมตี

8) เทคนิคการทำเหมืองข้อมูลด้วยกฎความสัมพันธ์ (Association Rule Data Mining) รับข้อมูลจากคลังวิเคราะห์ข้อมูลมาวิเคราะห์ความสัมพันธ์ด้วยกฎความสัมพันธ์ของรูปแบบการโจมตีกับวิธีดำเนินการแก้ไขเพื่อยุติการโจมตีและป้องกันการโจมตี

9) ข้อมูลออก (Output Data) คือกระบวนการเฝ้าดูสัญญาณเตือนจากระบบตรวจหาการบุกรุกรวมเพื่อรายงานให้ผู้ควบคุมระบบทราบเพื่อดำเนินการปรับปรุงแก้ไขเหตุการณ์ นอกจากนี้ยังเป็นการให้ความรู้เพื่อสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยให้ผู้ใช้งานได้ทราบเพื่อหาวิธีป้องกันที่เหมาะสมต่อไป

4. ผลการวิจัย

การวิจัยครั้งนี้ ผู้วิจัยได้ใช้ชุดข้อมูล KDD CUP'99 Dataset เป็นฐานข้อมูลในการฝึกและทดสอบประสิทธิภาพของระบบ โดยข้อมูลจาก KDD CUP'99 Dataset เหล่านี้จะผ่านกระบวนการนอร์มอลไลเซชันเพื่อปรับค่าให้มีความเหมาะสม หลังจากข้อมูลเหล่านี้ผ่านกระบวนการนอร์มอลไลเซชันแล้ว จะนำเข้ามาประมวลผลด้วยเทคนิคการทำเหมืองข้อมูลแบบใช้กฎความสัมพันธ์โดยรูปแบบการบุกรุกจะถูกตรวจสอบและเปรียบเทียบจากองค์ความรู้ด้านความปลอดภัย เพื่อให้ได้ผลลัพธ์ที่มีความถูกต้องสูง โดยข้อมูลที่จะถูกตรวจจับได้จะถูกเปรียบเทียบจากค่าความเชื่อมั่นและค่าสนับสนุน ดังตารางที่ 2

งานวิจัยครั้งนี้ จะใช้วิธีการประเมินประสิทธิภาพระบบจากการคำนวณหาค่าความเที่ยง (Precision) และค่าเรียกคืน (Recall) โดยที่ค่าความเที่ยงหมายถึงระบบสามารถค้นหารูปแบบการบุกรุกออกมาได้ถูกต้องทั้งหมดและค่าเรียกคืน หมายถึงค่าที่ระบบสามารถค้นหารูปแบบที่เกี่ยวข้องกับการบุกรุกทั้งหมดออกมาได้ดังแสดงในสมการที่ (5) และ (6)

$$\text{ค่าความเที่ยง} = \frac{X}{Y} \quad (5)$$

$$\text{ค่าเรียกคืน} = \frac{X}{Z} \quad (6)$$

โดยที่ X = จำนวนรูปแบบที่เกี่ยวข้องกับการบุกรุกทั้งหมดที่ระบบตรวจสอบและแสดงผลออกมา

Y = จำนวนรูปแบบทั้งหมด (รวมถึงรูปแบบที่ไม่เกี่ยวข้องกับการบุกรุก) ที่ระบบตรวจสอบได้

Z = จำนวนรูปแบบที่เกี่ยวข้องกับการบุกรุกทั้งหมด (รวมถึงจำนวนรูปแบบที่มีอยู่ แต่ระบบไม่สามารถตรวจสอบและแสดงผลออกมา)

ตารางที่ 3 ผลลัพธ์ที่วัดได้จากระบบตรวจจับการบุกรุกด้วยการใช้ข้อมูล KDD CUP'99 ชุดทดสอบ

Exp. no.	Normal Detection	Attack Detection	Precision	Recall
1	56996	228475	97.4%	92.0%
2	57719	229602	94.3%	89.2%
3	59648	166454	95.1%	90.3%
4	59703	166405	91.5%	87.4%

ตารางที่ 2 ตัวอย่างผลการทดสอบความถูกต้องตัวแบบ

ลำดับที่	ความสัมพันธ์	% ค่าความเชื่อมั่นข้อมูลเรียนรู้	% ค่าความเชื่อมั่นข้อมูลตรวจสอบ	% ค่าความถูกต้อง
1	Neptune Port 8088→ DOS attack	93.95	95.00	98.95
2	FTP_Writeport 80 →R2Lattack	100	100	100
3	Buffer OverFlowPort 80 → U2R attempt	82.46	90.00	92.46
4	IPSweep Port 8088 →Probe attempt	89.22	92.35	96.87

อย่างไรก็ดี เมื่อนำมาเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง ซึ่งใช้แผนภาพการจัดระเบียบตัวเอง (Self Organizing Map: SOM) [2] โดยการนำผลการจัดกลุ่มรูปแบบการโจมตีที่ถูกต้อง (Precision) และผลการจัดกลุ่มรูปแบบการโจมตีทั้งหมด (Recall) แทนค่าในสมการที่ (5) และ (6) แสดงในตารางที่ 4

ตารางที่ 4 ผลการเปรียบเทียบระหว่างระบบที่ได้พัฒนาขึ้นกับระบบตรวจจับของงานวิจัยที่เกี่ยวข้อง

Exp. No.	Attack Categories	Association Rules		SOM	
		Precision	Recall	Precision	Recall
1	Denial of Service (DOS)	97.4%	92.0%	95.4%	91.1%
2	User to Root (U2R)	94.3%	89.2%	92.0%	87.5%
3	Remote to Local (R2L)	95.1%	90.3%	93.5%	89.0%
4	Probing (Probe)	91.5%	87.4%	87.0%	83.2%

จากตารางที่ 4 พบว่าระบบที่ได้รับการออกแบบในครั้งนี้ มีความถูกต้องในการประมวลผลลัพธ์ที่มีความถูกต้องสูงกว่า เนื่องจากมีการเรียนรู้รูปแบบจากองค์ความรู้ที่ใช้สอน ทำให้ค่าผลลัพธ์ที่ได้มีความเที่ยงตรง ซึ่งต่างจากงานวิจัยที่เกี่ยวข้องซึ่งใช้การวิเคราะห์ข้อมูลในรูปแบบไม่มีการสอน

5. อภิปรายผลและสรุป

ผู้วิจัยได้ศึกษาสภาพความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันการพลศึกษาตามมาตรฐาน ISO/IEC 27001 ด้านการจัดการเหตุการณ์บุกรุกโจมตี ซึ่งมีความพร้อมน้อยที่สุด ด้านการควบคุมการเข้าถึงข้อมูลและสารสนเทศมีความพร้อมที่รองลงมา เป็นผลให้ความต้องการสารสนเทศในการจัดการเหตุการณ์การบุกรุกมีความต้องการสูง การให้ความรู้และสร้างความตระหนักในการป้องกันตนเองของบุคลากรในสถาบันการพลศึกษาก็มีความต้องการที่รองลงมา ผู้วิจัยจึงได้ออกแบบสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์มาสนับสนุนระบบตรวจหาการบุกรุกแบบปรับตัวที่สามารถแก้ปัญหาด้านความมั่นคงปลอดภัยสารสนเทศกรณีศึกษาของสถาบันการพลศึกษา โดยใช้เทคนิคการทำเหมืองข้อมูลแบบกฎความสัมพันธ์ ซึ่งใช้ในการตรวจหาการบุกรุก เพื่อวิเคราะห์หารูปแบบการบุกรุกและแสดงผลลัพธ์การโจมตีพร้อมทั้งปรับแต่งฐานข้อมูลรูปแบบการบุกรุกโจมตีในสถาปัตยกรรมความมั่นคงปลอดภัยไซเบอร์ให้ใหม่อยู่เสมอ เมื่อระบบรายงานรูปแบบการโจมตี ณ ขณะนั้นแล้วระบบจะแสดงผลวิธีการป้องกันและแก้ไขเหตุการณ์ที่บุกรุกในขณะนั้นจากฐานข้อมูลของสถาปัตยกรรมความรู้มั่นคงปลอดภัยไซเบอร์ให้ผู้ดูแลระบบทราบ รวมทั้งเป็นแหล่งให้ความรู้ผู้ใช้ทั่วไปในการระมัดระวัง สร้างความตระหนัก ป้องกันตัวเองจากอันตรายในเครือข่ายไซเบอร์

จากผลการวิจัยพบว่า ค่าตรวจจับข้อมูลการบุกรุกที่อยู่ในรูปแบบของ DOS ให้ค่าสูงที่สุด โดยมีค่าความเที่ยงที่ 97.4% และค่าเรียกคืนที่ 92.0% เนื่องจากข้อมูลในกลุ่ม DOS นี้มีอยู่ในฐานข้อมูลขององค์ความรู้แม่แบบครบถ้วน จึงทำให้ระบบสามารถวิเคราะห์รายละเอียดของรูปแบบการบุกรุกได้อย่างถูกต้องมากที่สุด ในทางตรงกันข้ามกับรูปแบบการบุกรุกในกลุ่ม PROBE มีกลุ่มข้อมูลที่กระจายแตกต่างกันมากทำให้การนอร์มอลไลเซชันทำได้อย่างจำกัด ระบบจึงไม่สามารถนำมาใช้วิเคราะห์กับฐานข้อมูลขององค์ความรู้แม่แบบได้อย่างถูกต้อง 100% จึงเป็นสาเหตุที่ทำให้ค่าการตรวจหาออกมามีค่าความเที่ยงอยู่ที่ 91.5% และค่าเรียกคืนอยู่ที่ 87.4%

นอกจากนี้ผู้วิจัยพบว่าฐานข้อมูลองค์ความรู้ที่นำมาใช้ตรวจสอบข้อมูลการบุกรุกจำเป็นต้องมีการปรับปรุงให้มีความทันสมัยอยู่ตลอดเวลาเพื่อให้กระบวนการตรวจหาของระบบมีประสิทธิภาพมากยิ่งขึ้นอีกทั้งการตรวจหาด้วยเทคนิคการทำเหมืองข้อมูลแบบกฎความสัมพันธ์ซึ่งเป็นหนึ่งในเทคนิคการทำเหมืองข้อมูลแบบมีการสอนที่ผู้วิจัยได้เลือกมาเป็นระบบต้นแบบเพื่อใช้ในการวิเคราะห์ความสัมพันธ์ข้อมูลการบุกรุกโจมตี หากผู้สนใจที่จะ

ศึกษา วิจัยและพัฒนารูปแบบแนวคิดต่อไป สามารถที่นำทฤษฎี หลักการหรือเทคโนโลยีอื่นๆ มาวิเคราะห์ เช่น Hidden Markov Model (HMM), Fuzzy Logic มาวิจัยและพัฒนาเกี่ยวกับรูปแบบแนวคิดในการพัฒนาตัวแบบสถาปัตยกรรมความรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพื่อสนับสนุนการตรวจหาการบุกรุกเชิงเวลาจริงแบบปรับตัวในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความสามารถและประสิทธิภาพที่แตกต่างในอนาคตต่อไป

เอกสารอ้างอิง

[1] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion detection by machine learning: A review," *Expert Systems with Applications*, vol. 36, no.10, pp. 11994-12000, 2009.

[2] M. K. Albertini and R. F. de Mello, *A Self-Organizing Neural Network Approach Novelty Detection*, IGI GLOBAL, 2010, pp. 49-71.

[3] M. Hassan et al., "A Data Clustering Algorithm based on Single Hidden Markov Model," in *Proceedings of the International Multi conference on Computer Science and Information Technology*, 2006, pp. 57-66.

[4] K. Burbeck and S. Nadjm-Tehrani, "Adaptive real-time anomaly detection with incremental clustering," *Information security technical report*, vol. 12, no. 1, pp. 56-67, 2007.

[5] ISO/IEC FDIS 27001:2005, *Information Technology - Security Management Systems-Requirements*, 2005.

[6] ISO/DIS 31000:2008, *Risk management Principles & guidelines on Implementation*, 2008.

[7] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, *Introduction to the OCTAVE® Approach*, Carnegie Mellon University, Pittsburgh, PA, 2003.

[8] S. S. SivathaSindhu, S. Geetha, and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," *Expert Systems with applications*, vol. 39, no. 1, pp. 129-141, 2012.

[9] D. Brauckhoff, X. Dimitropoulos, A. Wagner, and K. Salamatian, "Anomaly extraction in backbone networks using association rules," *IEEE/ACM Transactions on Networking (TON)*, vol. 20, no.6, pp. 1788-1799, 2012.

[10] A. Chauhan, M. Gaurav, and K. Gulshan, *Survey on data mining techniques in intrusion detection*. Lap Lambert Academic Publ, 2012.

[11] T. Kohonen, "Essentials of the self-organizing map," *Neural Networks*, vol. 37, pp. 52-65, 2013.

[12] S. Kesh and P. Ratnasingam "A Knowledge Architecture for IT Security," *Communications of the ACM*, vol. 50, no. 7, pp. 103-108, 2007.

[13] L. Shahreza et al., "Anomaly detection using a self-organizing map and particle swarm optimization," *ScientiaIranica*, vol. 18, no. 6, pp. 1460-1468, 2011.

[14] P. Garcia-Teodoro, J. Diaz-Verdejo,G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *computers & security*, vol. 28, no. 1, pp. 18-28, 2009.

[15] J. Shun and H. A. Malki, "Network intrusion detection system using neural networks," in *the 4th IEEE International Conference on Natural Computation*, vol. 5, pp. 242-246, 2008.

[16] H.J. Liao, C.H. Richard Lin, Y.C. Lin, and K.Y. Tung, "Intrusion detection system:A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, pp. 16-24, 2013.

[17] Y. H. Hu and J. N. Hwang, *Handbook of neural*

network signal processing, CRC press, 2010.

[18] G. K. Gupta, *Introduction to data mining with case studies*, PHI Learning Pvt. Ltd., 2011.

[19] P. Poncelet and M. Teisseire, *Data mining patterns: new methods and applications*, Information Science Reference, 2008.

[20] A. N. Khan, K. Qureshi, and S. Khan, "An Intelligent Approach of Sniffer Detection," *The International Arab Journal of Information Technology*, vol. 9, no. 1, pp. 9-15, 2012.

[21] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690-1700, 2014.

[22] The UCI KDD Archive Information and Computer Science University of California. (2011, July 16). "KDD CUP 1999 Dataset." [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.htm