ตัวแบบทำนายการบุกรุกทางไซเบอร์แบบอัตโนมัติด้วยการเรียนรู้เชิงลึก เพื่อรับมือกับภัยคุกคามทางไซเบอร์สำหรับกองทัพอากาศไทย
An Automated Cyber Intrusion Prediction Model Using Deep Learning to Resilient in Cyber Threat for the Royal Thai Air Force

สมบูรณ์ อุดนัน (Somboon Udnan)*, ประสงค์ ปราณีตพลกรัง (Prasong Praneetpolgrang)**,
และพายัพ ศิรินาม (Payap Sirinam)**

Received: October 31, 2023
Revised: February 21, 2024
Accepted: May 29, 2024

* ผู้นิพนธ์ประสานงาน: สมบูรณ์ อุดนัน (Somboon Udnan) อีเมล: vit.peksayfa@gmail.com

DOI:10.14416/j.it.2025.v1.005

บทคัดย่อ

กองทัพอากาศไทยเป็นหนึ่งในหน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศของประเทศ และมีสถิติการบุกรุกทางไซเบอร์อย่างต่อเนื่องตลอดทั้งปี ผู้วิจัยจึงได้นำเสนอตัวแบบทำนายการบุกรุกทางไซเบอร์รูปแบบใหม่ที่ทำงานอย่างอัตโนมัติด้วยการเรียนรู้เชิงลึก งานวิจัยนี้ เป็นการพัฒนาต่อยอดจากอัลกอริทึมมองย้อนกลับ ทั้งนี้ ได้พัฒนาตัวแบบการทำนายให้มีความแม่นยำมากขึ้น มีการใช้ชุดข้อมูลการบุกรุกทางไซเบอร์ของกองทัพอากาศในห้วงเวลาตั้งแต่ มกราคม 2564 ถึงธันวาคม 2564 จำนวน 241,148 ข้อมูล โดยใช้อัลกอริทึมการเรียนรู้เชิงลึกที่ชื่อว่า MLP, RNN, LSTM, GRU และ Bi-LSTM ผู้วิจัยได้พัฒนาตัวแบบทำนายการบุกรุกทางไซเบอร์ตัวใหม่ที่ชื่อว่า Bi-LSTM Looking Back Risk: Bi-LSTM-LBR อย่างไรก็ตาม ตัวแบบที่สร้างขึ้นมาใหม่นี้มีความแม่นยำมากเมื่อเปรียบเทียบกับตัวแบบทำนายทั้งหมดที่นำมาทำการวิจัยและทดสอบ ซึ่งผลการทำนายมีค่าความคลาดเคลื่อนสัมบูรณ์เฉลี่ยของการทำนาย (Mean Absolute Error: MAE) อยู่ที่ 0.038 มีค่าความคลาดเคลื่อนเฉลี่ย (Mean Square Error: MSE) อยู่ที่ 0.010 และค่าความคลาดเคลื่อนกำลังสองเฉลี่ย (Root Mean Square Error: RMSE) อยู่ที่ 0.102

คำสำคัญ: การทำนาย การบุกรุกทางไซเบอร์ การเรียนรู้เชิงลึก

Abstract

The Royal Thai Air Force was one of the nation's Critical Information Infrastructure (CII) Organizations and has a record of cyber intrusions continue throughout the year. Therefore, researchers presented a new automated cyber intrusion prediction model using deep learning to resilient in cyber threat for the Royal Thai Air Force. It was an extension of the Looking Back Algorithm to increase the accuracy of the predictive model. In order to predict the future of the Air Force's cyber threat patterns, researchers used cyber intrusion datasets from the Air Force that ranging from January 2021 to December 2021 with a total of 241,148 entries. We applied techniques such as RNN, LSTM, GRU, Bi-LSTM Deep Learning (DL). We developed the new cyber intrusion prediction model with name Bi-LSTM Looking Back Risk: Bi-LSTM-LBR. However, the developed model had high accurate result on test dataset that compared to other predictive models. In addition, prediction results had a Mean Absolute Error (MAE) was 0.038, a Mean Square Error (MSE) was 0.010 and a Root Mean Square Error (RMSE) was at 0.102.

Keywords: Prediction, Cyber Intrusion, Deep Learning.

1. บทนำ

การทำนายการบุกรุกทางไซเบอร์มีบทบาทอย่างมากในการสนับสนุนการตัดสินใจเพื่อดำเนินกลยุทธ์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรทางทหาร การทำนายการบุกรุกทางไซเบอร์ในปัจจุบันทำได้ยาก อันเนื่องมาจากปัจจัยของข้อมูลที่ถูกส่งเข้ามาประมวลผลมีปริมาณมากเป็นรายวินาที

* สาขาวิชาเทคโนโลยีป้องกันประเทศ สำนักบัณฑิตศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช
* Defense Technology Program, The Graduate School of Navaminda Kasatriyadhiraj Royal Air Force Academy.
** กองการศึกษา โรงเรียนนายเรืออากาศนวมินทกษัตริยาธิราช
** Academic Faculty, Navaminda Kasatriyadhiraj Royal Air Force Academy.

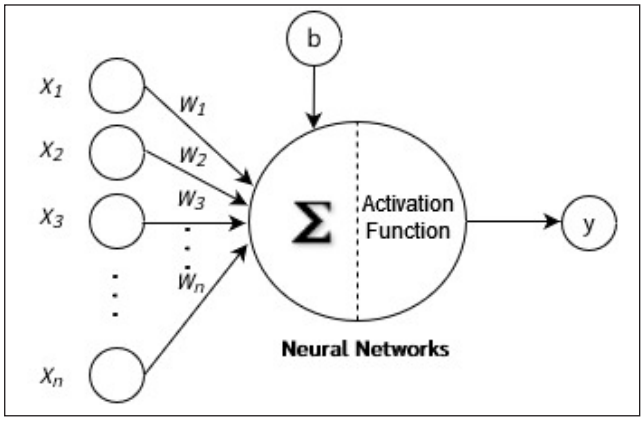
ทำให้หลายหน่วยงานมีการนำเทคโนโลยีการเรียนรู้ของเครื่อง (Machine Learning: ML) มาใช้ในทำนายภัยคุกคามทางไซเบอร์ อีกทั้งยังมีการนำอัลกอริทึม (Algorithm) การเรียนรู้เชิงลึก (Deep Learning: DL) มาใช้วิเคราะห์พฤติกรรมของผู้บุกรุกทางไซเบอร์ [1] เทคโนโลยีดังกล่าวสามารถดำเนินการได้อย่างรวดเร็ว และรองรับความซับซ้อนของรูปแบบการโจมตีทางไซเบอร์ได้เป็นอย่างดี

ปัจจุบันกองทัพอากาศมีระบบการตรวจจับการบุกรุกทางไซเบอร์ (Intrusion Detection Systems: IDS) เป็นเครื่องมือตรวจจับการบุกรุกที่เกิดขึ้นในเวลาปัจจุบันเท่านั้น ไม่อาจจะทำนายแนวโน้มของการโจมตีทางไซเบอร์ที่อาจจะเกิดขึ้นในอนาคตได้ ดังนั้น ผู้วิจัยจึงได้ศึกษาค้นคว้าเกี่ยวกับเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ที่เป็นการเรียนรู้เชิงลึก การนำอัลกอริทึมเกี่ยวกับปัญญาประดิษฐ์มาปรับใช้เพื่อทำนายภัยคุกคามทางไซเบอร์ของกองทัพอากาศ ในหลาย ๆ ด้าน เช่น การตรวจจับการบุกรุก [2] การตรวจสอบมัลแวร์ [3], [4] และการตรวจสอบช่องโหว่ของระบบคอมพิวเตอร์ [5] ซึ่งได้ผลลัพธ์ค่อนข้างแม่นยำ ดังนั้น งานวิจัยนี้ผู้วิจัยได้เลือกใช้ความสามารถของการเรียนรู้เชิงลึก ผลลัพธ์ที่ได้จะทำให้กองทัพอากาศมีระบบตรวจจับที่จะทำนายพฤติกรรมการบุกรุกทางไซเบอร์ที่เป็นอันตรายหรือหาแนวทางป้องกันแก้ไขได้อย่างทันท่วงที

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ตัวแบบทำนายการบุกรุกทางไซเบอร์

ตัวแบบทำนายที่ผู้วิจัยนำมาทำการทดสอบ คือโครงข่ายประสาทเทียมหรือแบบจำลองทางคณิตศาสตร์ที่ถูกพัฒนาขึ้นเพื่อใช้จำลองการทำงานของโครงข่ายประสาทในสมองมนุษย์ มีกระบวนการทำงาน ดังภาพที่ 1



ภาพที่ 1 *การทำงานของโครงข่ายประสาทเทียม 1 หน่วย [6]*

โครงข่ายประสาทเทียมมีคุณลักษณะคล้ายกับการส่งผ่านสัญญาณประสาทในสมองของมนุษย์ มีความสามารถในการรวบรวมองค์ความรู้ (Knowledge) ผ่านกระบวนการเรียนรู้ (Learning Process) อันความรู้เหล่านี้จะถูกจัดเก็บอยู่ในโครงข่ายในรูปของค่าน้ำหนัก ที่เปลี่ยนแปลงค่าได้เมื่อมีการเรียนรู้สิ่งใหม่ ๆ เข้าไป โดยการประมวลผลต่าง ๆ ที่เกิดขึ้นในหน่วยประมวลผลย่อยจะถูกเรียกว่าโหนด (Node) [6] การประมวลผลของโครงข่ายประสาทเทียม สามารถเขียนให้อยู่ในภาพของสมการที่ (1) ได้ ดังนี้

$$y = f\left(\sum_{i=1}^{n} x_i w_i + b\right) \qquad (1)$$

โดยที่

- y คือ ค่าเอาต์พุตของโครงข่ายประสาทเทียม
- f คือ Activation Function
- n คือ จำนวนข้อมูลที่ใช้
- i คือ จำนวนเริ่มต้น มีค่าตั้งแต่ 1 ถึง n
- x_i คือ ค่าข้อมูลอินพุตเข้าไปตามลำดับที่ i
- w_i คือ ค่าน้ำหนักของนิวรอนเน็ตเวิร์กตัวที่ i
- b คือ ค่าความโน้มเอียง (Bias)

2.1.1 ตัวแบบทำนายการบุกรุกทางไซเบอร์ การวิเคราะห์ภัยคุกคามทางไซเบอร์มักจะเป็นการแก้ไขปัญหาการแยกประเภทของข้อมูล (Classification) ด้วยการแบ่งข้อมูลออกเป็นสองกลุ่มหรือหลายกลุ่มได้ด้วยสมการเส้นตรงผ่านคุณสมบัติของนิวรอนเน็ตเวิร์ก (Neural Networks) แบบชั้นเดียว (Single Layer) [7] แต่ในปัญหาบางประเภทที่ต้องใช้เส้นโค้งในการแบ่งข้อมูล เช่น ข้อมูลที่ซ้อนทับกัน จะไม่สามารถใช้สมการเส้นตรงในการแบ่งข้อมูลได้ ในการแก้ไขปัญหาด้วยอัลกอริทึมการเรียนรู้เชิงลึก จะใช้อัลกอริทึมแบบหลายชั้น เช่น Multi-Layer Perceptron (MLP) [8], [9] ในการแก้ไขปัญหาโดยจะมีการเชื่อมต่อกันเป็นโครงข่ายประสาทเทียมที่ประกอบด้วย 3 Layer คือ Input Layer ทำหน้าที่รับข้อมูลเข้าสู่โครงข่ายประสาทเทียม Hidden Layer ทำหน้าที่จำแนกรูปแบบข้อมูลออกเป็นรายละเอียดย่อย ๆ ที่มีได้หลาย Layer ยิ่งมีจำนวน Layer มากเท่าใด ก็ยิ่งจำแนกได้ละเอียดมากขึ้นเท่านั้น และ Output Layer ทำหน้าที่รวมผลลัพธ์ของข้อมูล [10] แต่สำหรับปัญหาที่ต้องการทราบเหตุการณ์ที่มีการเกิดขึ้นอย่างต่อเนื่องเป็นอนุกรมเวลา (Time-Series) [11] ก็จะใช้ตัวแบบทำนายอีกรูปแบบหนึ่งในการแก้ไขปัญหา ดังหัวข้อต่อไป

2.1.2 ตัวแบบทำนาย Recurrent Neural Network (RNN) เป็นตัวแบบทำนายที่มีการเก็บสถานะข้อมูลไว้ใน Hidden State ด้วยการนำ Hidden State ก่อนหน้า มาใช้ในการคำนวณ Hidden State ปัจจุบัน และใช้ Hidden State ปัจจุบัน ในการคำนวณสถานะของข้อมูลในช่วงเวลาถัดไป RNN จึงเหมาะกับข้อมูลที่เป็นลำดับหรือข้อมูลที่เป็นอนุกรมเวลา ทั้งนี้ RNN สามารถทำงานได้ดีกับข้อมูลที่มีลำดับเวลาห่างกันไม่มาก เพราะจะทำให้ประสบปัญหา Vanishing Gradient ได้ [12]

2.1.3 ตัวแบบทำนาย Long Short-Term Memory (LSTM) จากปัญหา Vanishing Gradient ใน RNN ทำให้มีการพัฒนา LSTM ขึ้นใหม่ มีการใช้ข้อมูล Cell State และ Hidden State ในการเก็บข้อมูล จากนั้นส่งไปประมวลผลในช่วงเวลาถัดไป อาศัยเกต (Gate) ต่างๆ ในการคำนวณว่าควรจะเก็บรักษาข้อมูลที่ประกอบไปด้วย Input Gate, Output Gate, และ Forget Gate ภายใน Cell State และ Hidden State มากน้อยเพียงใด แต่ละ Gate มีหน้าที่ในการตัดสินใจว่าจะให้ข้อมูลผ่านไปหรือไม่ตามค่าความสำคัญของข้อมูล หากมีค่าน้อยก็จะไม่อาจผ่าน Gate ไปได้ จึงช่วยป้องกันการเกิด Vanishing Gradient ได้ [13]

2.1.4 ตัวแบบทำนาย Gated Recurrent Unit (GRU) Kyunghyun Cho และคณะ [14] ได้เสนออัลกอริทึม Gate Recurrent Unit (GRU) พัฒนาต่อยอดจาก LSTM ด้วยการทำให้มีโครงสร้างที่ไม่ซับซ้อน การปรับ Gate ใน LSTM เป็น Reset Gate และ Update Gate ซึ่ง Update Gate ทำหน้าที่พิจารณาว่าควรจะเก็บข้อมูล State ก่อนหน้าไว้มากน้อยเพียงใด ขณะที่ Reset Gate ทำหน้าที่คำนวณว่าจะนำข้อมูลจาก State ก่อนหน้ามาพิจารณาร่วมกับข้อมูล Input ปัจจุบันมากน้อยเพียงใด และด้วยจำนวน Gate ที่น้อยกว่าจึงทำให้ GRU สามารถทำงานได้เร็วกว่า LSTM [14], [15]

2.1.5 ตัวแบบทำนาย Bi-LSTM โครงสร้างของ Bi-LSTM จะคล้ายกับ LSTM เพียงแต่ใช้ Layer ของ LSTM จำนวน 2 ชั้น ขนานกัน ทำหน้าที่ประมวลผลทั้งไปข้างหน้า และย้อนกลับ เหมาะกับการนำมาใช้กับข้อมูลที่เป็นข้อความหรือประโยค ทำให้มีความสามารถในการเก็บข้อมูลจากทางส่วนหัวและส่วนท้ายของประโยคในเวลาเดียวกันได้ หลักการทำงานของ Bi-LSTM คือ ระหว่าง Layer ข้อมูล Input จะถูกประมวลผลพร้อมกันสองทิศทาง ทั้งไปข้างหน้า (Forward) และข้างหลัง (Backward) เพื่อรับข้อมูลสถานะที่ซ่อนอยู่ ขณะที่ข้อมูลจะถูกหลอมรวมกันเพื่อให้ได้ผลลัพธ์ออกที่ Layer Output ทำให้ตัวแบบทำนายสามารถรับข้อมูลได้ทั้งเวลาปัจจุบันและอนาคตจากสถานะย้อนกลับและไปข้างหน้าด้วยกระบวนการของตัวแบบทำนาย แต่ละโหนดจะประกอบด้วย สถานะ Forget Gate หรือ f_t ของ Input Gate หรือ i_t ของ Input Modulation Gate สถานะของเซลล์ หรือ Cell State หรือ $\tilde{C}_t$ และ Output Gate หรือ o_t แต่ละ Gate จะสร้างหมายเลขเอาต์พุตระหว่าง 0 ถึง 1 สำหรับแต่ละหมายเลขในสถานะของโหนดก่อนหน้า h_{t-1} และ C_{t-1} ในขณะเดียวกัน เอาต์พุตของ f_t จะบอกสถานะของโหนดแต่ละโหนดว่าข้อมูลใดควรจะลืม หรือทิ้งด้วยการคูณ 0 เข้าไปในตำแหน่งเมทริกซ์ และหากต้องการให้ผลลัพธ์ของสมการเป็น 1 ก็จะคงสถานะเดิมของโหนดนั้นต่อไป แล้วให้ข้อมูลวิ่งผ่านฟังก์ชัน Sigmoid ข้อมูลจะถูกปรับมิติในชั้นของ Hidden State หรือ h_t เพื่อทำให้โหนดตัวใหม่ได้รับสถานะเวกเตอร์ Hidden State ในเวกเตอร์ Output ณ เวลา t โดย h_t จะเท่ากับผลคูณของค่า w'_1 หรือค่าน้ำหนักของนิวรอนเน็ตเวิร์กแบบไปข้างหน้าของ $\overrightarrow{h}_t$ บวก กับค่าผลคูณของ w'_2 หรือค่าน้ำหนักของนิวรอนเน็ตเวิร์ก แบบย้อนกลับของ $\overleftarrow{h}_t$ และบวกกับค่าความโน้มเอียงของข้อมูล b_h ซึ่งจะได้ผลรวมของข้อมูลทั้งสองทิศทางเพื่อเป็นผลลัพธ์ของตัวแบบทำนายดังสมการที่ (2) [16]

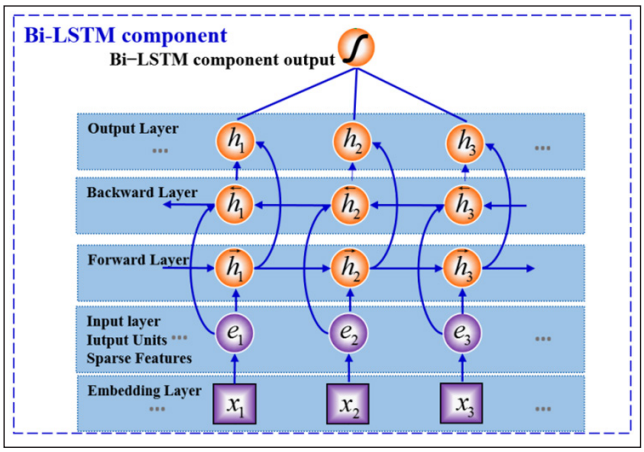
$$
\begin{aligned}
it &= \sigma(w_i[h_{t-1},x_t]b_i), \\
\tilde{C}_t &= \tanh(w_C[h_{t-1},x_t] + b_C), \\
C_t &= (f_t * C_{t-1}) + (i_t * \tilde{C}_t), \\
o_t &= \sigma(w_o[h_{t-1},x_t] + b_o), \\
h_t &= w'_1\,\overrightarrow{h}_t + w'_2\,\overleftarrow{h}_t + b_h
\end{aligned}
\qquad (2)
$$

โดยที่

i_t	คือ	ข้อมูล Input
f_t	คือ	Forget Gate
o_t	คือ	ข้อมูล Output
C_t	คือ	สถานะของเซลล์ หรือ Cell State
h_t	คือ	สถานะของ Hidden State
$\overrightarrow{h}_t$	คือ	สถานะของ Hidden State แบบไปข้างหน้า
$\overleftarrow{h}_t$	คือ	สถานะของ Hidden State แบบย้อนกลับ
σ	คือ	ค่า Activation
b_C	คือ	ค่าความโน้มเอียงของ Cell State
b_f	คือ	ค่าความโน้มเอียงของ Forget Gate
b_i	คือ	ค่าความโน้มเอียงของข้อมูล Input

b_o คือ ค่าความโน้มเอียงของข้อมูล Output
b_h คือ ค่าความโน้มเอียงของข้อมูล Hidden
x_t คือ ข้อมูลอินพุตเข้าไปตามลำดับที่ t
x_i คือ ค่าข้อมูลอินพุตเข้าไปตามลำดับที่ i
w_i คือ ค่าน้ำหนักของนิวรอนเน็ตเวิร์กตัวที่ i
w'_1 คือ ค่าน้ำหนักของนิวรอนเน็ตเวิร์กตัวที่ 1
w'_2 คือ ค่าน้ำหนักของนิวรอนเน็ตเวิร์กตัวที่ 2
t คือ ช่วงเวลา

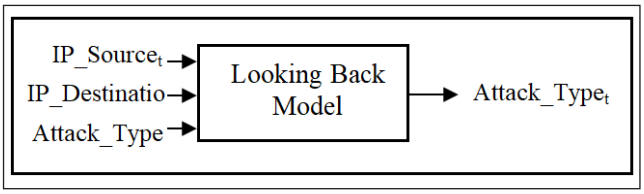
ระบบทำนายที่พัฒนาขึ้นใหม่ มีกระบวนการทำงานและโครงสร้างภายใน ดังภาพที่ 2



ภาพที่ 2 *โครงสร้างภายในของตัวแบบทำนาย Bi-LSTM [16]*

2.2 สถาปัตยกรรมมองย้อนกลับ (Looking Back Model)

เป็นการนำเข้าข้อมูลสู่ตัวแบบทำนายภัยคุกคามทางไซเบอร์รูปแบบหนึ่ง ที่ใช้ข้อมูลหมายเลขไอพีต้นทาง หมายเลขไอพีปลายทาง รวมทั้งรูปแบบการโจมตีที่เคยเกิดขึ้นในอดีตมาเป็นลักษณะข้อมูล (Feature) เพื่อทำนายรูปแบบการโจมตีทางไซเบอร์ที่จะเกิดขึ้น สามารถทำให้ค่า F-Measure สูงขึ้นได้โดยเฉพาะกับตัวแบบทำนายประเภท LSTM [17], [18] มีสถาปัตยกรรมการทำงานดังภาพที่ 3



ภาพที่ 3 *สถาปัตยกรรม Looking Back Model [17]*

2.3 เครื่องมือในการพัฒนา

2.3.1 Anaconda เป็นซอฟต์แวร์ฟรี มีชุดเครื่องมือสนับสนุนที่ออกแบบมาเพื่อการวิจัยและวิทยาศาสตร์โดยเฉพาะ ด้วยการติดตั้ง Anaconda [19] ช่วยให้เข้าถึงสภาพแวดล้อมต่างๆ ของการเขียนโค้ดในภาษา Python หรือภาษา R ได้สะดวกขึ้น ที่เรียกว่าซอฟต์แวร์การพัฒนาแบบบูรณาการ (Integrated Development Environment: IDE) หรือสภาพแวดล้อมการพัฒนาแบบบูรณาการ ซึ่งเป็นแพลตฟอร์มที่ช่วยให้การพัฒนาโค้ดง่ายขึ้นนั้นเอง [20]

2.3.2 Keras เป็น Application Programming Interface (API) สำหรับสร้างนิวรอนเน็ตเวิร์กที่ถูกพัฒนาตามหลักการที่ว่าความสามารถในการเปลี่ยนแนวคิดไปสู่ผลลัพธ์ที่ใช้เวลาน้อยที่สุด อันเป็นกุญแจสำคัญในการทำวิจัยที่ดี [21], [22]

2.3.3 TensorFlow เป็นซอฟต์แวร์โอเพ่นซอร์สที่พัฒนาโดย Google แอปพลิเคชันหลักของ TensorFlow คือการเรียนรู้ของเครื่องและโครงข่ายประสาทเทียมเชิงลึกตามกราฟการไหลของข้อมูล TensorFlow ทำการติดตั้งได้ทั้งบนระบบปฏิบัติการ Ubuntu, macOS และ Windows ทั้งนี้ TensorFlow รองรับการทำงานได้ทั้งใน CPU และ GPU [23], [24]

2.4 การวิเคราะห์ชุดข้อมูลการบุกรุกทางไซเบอร์ของกองทัพอากาศ (RTAF Intrusion Dataset)

ข้อมูลการบุกรุกที่มาจากอุปกรณ์ IDS เป็นผลของการตรวจจับภัยคุกคามทางไซเบอร์จากระบบเครือข่ายคอมพิวเตอร์ภายนอกสู่ระบบเครือข่ายคอมพิวเตอร์ภายในของกองทัพอากาศ มีกระบวนการทั้งหมด 4 ขั้นตอน [25] ดังนี้

ขั้นตอนที่ 1 กระบวนการรวบรวมข้อมูล (Data Acquisition) ผู้วิจัยได้รวบรวมข้อมูล Internal Data ประกอบด้วยข้อมูลการบุกรุกทางไซเบอร์จาก Antivirus ข้อมูลบุกรุกทางไซเบอร์จาก Firewall ภายในกองทัพอากาศ (Palo Auto Firewall) และข้อมูลจากอุปกรณ์ Switch / Router ที่เป็น IDS ภายในของกองทัพอากาศ รวมทั้ง External Data ซึ่งประกอบด้วยข้อมูลการบุกรุกทางไซเบอร์จาก Web App Firewall (Imperva Firewall) มาดำเนินการปรับรูปแบบของข้อมูลให้อยู่ในรูปแบบเดียวกัน แล้วจะได้เป็นชุดข้อมูลการบุกรุกทางไซเบอร์ของกองทัพอากาศสำหรับใช้ในการวิจัยต่อไป

ขั้นตอนที่ 2 การสกัดคุณสมบัติของข้อมูล (Feature Extraction) ผู้วิจัยเลือกลักษณะข้อมูลที่จำเป็นในการทำนายรูปแบบภัยคุกคาม

ทางไซเบอร์ออกมาจากชุดข้อมูล มีลักษณะข้อมูลทั้งหมด 7 ลักษณะข้อมูล ประกอบด้วย id, Alert, Source_IP, Destination_IP, Event_Count, Event_Date, Source_Country, Destination_Country, Cyber Risk, Type_ และ Type สำหรับในกระบวนการนี้จะมีการกำหนดลักษณะข้อมูลที่ต้องการทำนายเป็นฉลากหรือป้าย (Label) ของชุดข้อมูลเอาไว้มีชื่อว่า "Type"

ขั้นตอนที่ 3 การเตรียมข้อมูล (Pre-Processing) ชุดข้อมูล RTAF Intrusion Dataset มีจำนวน 11 แอตทริบิวต์ และ 241,148 เรคคอร์ด โดยมีรายละเอียด ดังตารางที่ 1

ตารางที่ 1 *รายชื่อแอตทริบิวต์และคุณลักษณะข้อมูล (Dataset Properties)*

ลำดับ	ชื่อแอตทริบิวต์	คุณลักษณะข้อมูล (Dataset Properties)
1	Id	Discrete
2	Alert	Discrete
3	Source_IP	Discrete
4	Destination_IP	Discrete
5	Event_Count	Discrete
6	Event_Date	Discrete
7	Source_Country	Discrete
8	Destination_Country	Discrete
9	Risk_Cyber	Discrete
10	Type_	Discrete
11	Type	Discrete

ในการนำข้อมูลเข้าสู่ตัวแบบทำนาย จำเป็นต้องทำให้ข้อมูลอยู่ในรูปของตัวเลขที่อยู่ระหว่าง 0-1 และกำหนดให้ขนาดของข้อมูลเป็นมิติย่อย ๆ เพื่อทำให้ประมวลผลได้ในตัวแบบทำนายการบุกรุกทางไซเบอร์ เริ่มจากการนำลักษณะข้อมูลที่เป็น Label มาทำการเข้ารหัสเป็นตัวเลขด้วยอัลกอริทึม Label-Encoder มีอยู่ใน Library ของ Keras จะได้ผลลัพธ์ออกมาเป็นค่า Index เพื่อใช้สำหรับอ้างอิงแทนรูปแบบภัยคุกคามทางไซเบอร์ในชุดข้อมูล จากนั้นเลือกรูปแบบ Step ของข้อมูลเพื่อใช้กำหนดลำดับของข้อมูล ซึ่งเป็นกระบวนการเตรียมข้อมูล

ตารางที่ 2 *ประเภทของภัยคุกคามทางไซเบอร์*

ประเภทการโจมตี	จำนวน	อัตราส่วน
Probe	56,252	23.73%
Trojan	42,032	17.43%
Cryptojacking	33,508	13.90%
Web Shell	23,321	10.67%
Botnet	22,334	10.26%
Injection	11,619	5.82%
Brute Force Attack	11,308	5.69%
Dropper	4,245	2.76%
Ransomware	1,205	1.50%
R2L	1,086	1.45%
Worm	579	1.42%
DDoS	500	1.21%
Man in the Middle Attacks	194	1.08%
Data leak	87	1.04%
Phishing	58	1.02%
Website Defacement	41	1.02%
Total	241,148	100%

ก่อนการประมวลผลของชุดข้อมูลประเภท Time-Series จากนั้นจึงทำการปรับมิติของข้อมูลให้เหมาะสมกับตัวแบบทำนายการบุกรุกทางไซเบอร์ในแต่ละแบบ จากนั้นทำการแปลงผลลัพธ์ที่ได้ออกมาอยู่ในรูปเมทริกซ์อาเรย์ลิซ (Matrix Arrays List)

ขั้นตอนที่ 4 การเลือกลักษณะข้อมูล (Feature Selection) [26] ผู้วิจัยได้ทำการแบ่งชุดข้อมูลออกเป็น 3 ชุด [27] ประกอบด้วย ชุดข้อมูลสำหรับฝึกสอน (Train Set) 70% ชุดข้อมูลสำหรับการปรับแต่งตัวแบบทำนายการบุกรุกทางไซเบอร์ (Validation Set) 15% และชุดข้อมูลทดสอบ (Test Set) 15% ผู้วิจัยได้ดำเนินการทดลอง ตลอดจนพัฒนาตัวแบบทำนายการบุกรุก

ทางไซเบอร์บนโปรแกรม Anaconda ด้วยภาษา Python เวอร์ชัน 3.8 และใช้ Library ของ Keras กับ Tensor Flow ในการดำเนินการวิจัย

หลังจากดำเนินการแบ่งข้อมูลออกเป็นข้อมูล Train Set, Validation Set และ Test Set เรียบร้อยแล้ว จะได้ปริมาณข้อมูลของแต่ละรูปแบบการโจมตี ดังตารางที่ 3

ตารางที่ 3 *ปริมาณข้อมูลของรูปแบบการโจมตีทางไซเบอร์ในชุดข้อมูลการบุกรุกทางไซเบอร์ของกองทัพอากาศ*

Type	Train 70%	Validation 15%	Test 15%
Probe	39,376	8,438	8,438
Trojan	29,422	6,305	6,305
Cryptojacking	23,456	5,026	5,026
Web Shell	16,325	3,498	3,498
Botnet	15,634	3,350	3,350
Injection	8,133	1,743	1,743
Brute Force Attack	7,916	1,696	1,696
Dropper	2,971	637	637
Ransomware	843	181	181
R2L	760	163	163
Worm	405	87	87
DDoS	350	75	75
Man in the Middle Attacks	136	29	29
Data leak	61	13	13
Phishing	40	9	9
Website Defacement	29	6	6
Total	168,804	36,172	36,172

2.5 การวัดประสิทธิภาพของตัวแบบทำนาย

ในงานวิจัยนี้ ผู้วิจัยได้ใช้อัลกอริทึมนิวรอนเน็ตเวิร์กหลายตัวในการทดลอง ผู้วิจัยได้ทำการทดสอบหาค่าที่เหมาะสมที่สุดในทุก ๆ อัลกอริทึม ทั้งจำนวนโหนด จำนวนชั้น Layer และจำนวนรอบของการ Train [28] จนได้ค่าที่เหมาะสมที่สุดสำหรับการ Train ที่ 50 รอบ จำนวนนิวรอนเน็ตเวิร์กอยู่ที่ 50 ตัว และจำนวนชั้นของ Layer เท่ากัน คือ 2 Layer ในบริบทของการเรียนรู้เชิงลึก ตัวแบบทำนายจะเรียนรู้ที่จะลดฟังก์ชันการสูญเสียหรือฟังก์ชัน Loss เพื่อทำให้ค่าความผิดพลาดเหลือน้อยที่สุดในระหว่างกระบวนการ Training ตัวแบบทำนายจะปรับค่าน้ำหนักและค่าความโน้มเอียง (Bias) ของเครือข่ายในลักษณะที่เป็นการกระจายความน่าจะเป็นที่คาดการไว้ซึ่งจะมีความใกล้เคียงกับการกระจายความน่าจะเป็นที่แท้จริงมากที่สุด

หากผลสุดท้ายของการทำนายมีค่า Error ต่ำ ถือว่ามีความแม่นยำสูง นั่นคือจะใช้เป็นตัวบ่งชี้ว่าตัวแบบทำนายดังกล่าวได้เรียนรู้ข้อมูลที่อินพุตเข้าไปอย่างถูกต้อง ในขณะที่ตัวแบบทำนายจะให้ผลทำนายที่ไม่ใช่ค่าจริงหรือค่าเท็จ แต่จะเป็นค่าความแม่นยำหรือค่าความผิดพลาดห่างจากคำตอบไปในทิศทางบวกหรือลบเท่าใด อย่างไรก็ตาม สมการที่ใช้ในการวัดประสิทธิภาพของตัวแบบทำนายจึงนิยมใช้สมการเพื่อหาค่าความผิดพลาด (Loss) ของการทำนายที่น้อยที่สุด แต่หากมีค่าเพิ่มขึ้นก็จะเป็นการแสดงให้เห็นว่าตัวแบบทำนายดังกล่าวไม่อาจหาคำตอบได้หรือมีค่าความแม่นยำต่ำ

2.5.1 ค่าความคลาดเคลื่อนสัมบูรณ์เฉลี่ย (Mean Absolute Error: MAE) เป็นการวัดความคลาดเคลื่อนที่สามารถบอกถึงขนาดของความคลาดเคลื่อนรวม หากได้ผลลัพธ์ยิ่งน้อยยิ่งแสดงให้เห็นว่าตัวแบบทำนายดังกล่าวมีความแม่นยำมาก ดังสมการที่ (3) [29]

$$MAE = \frac{1}{n}\sum_{t=1}^{n}\left|Y_t - \hat{Y}_t\right| \qquad (3)$$

โดยที่

MAE คือ ค่าความคลาดเคลื่อนสัมบูรณ์เฉลี่ย
n คือ จำนวนข้อมูลที่ใช้
Y_t คือ ค่าจริงที่เวลา t ใด ๆ
$\hat{Y}_t$ คือ ค่าที่ได้จากการทำนายที่เวลา t ใด ๆ

2.5.2 ค่าความคลาดเคลื่อนกำลังสองเฉลี่ย (Mean Squared Error: MSE) เป็นการวัดความคลาดเคลื่อนของการทำนาย จากนั้นนำค่า Error มายกกำลังแล้วหาค่าเฉลี่ยความแม่นยำ ซึ่งผลลัพธ์มีค่ายิ่งน้อยมากเท่าไหร่ ก็ยิ่งแสดงให้เห็นว่าตัวแบบทำนายดังกล่าวมีความแม่นยำมากเท่านั้น ดังสมการที่ (4)

$$MSE = \frac{1}{n}\sum_{t=1}^{n}(Y_t - \hat{Y}_t)^2 \quad (4)$$

โดยที่

MSE คือ ค่าความคลาดเคลื่อนกำลังสองเฉลี่ย

2.5.3 ค่ารากที่สองของค่าความคลาดเคลื่อนกำลังสองเฉลี่ย (Root Mean Squared Error: RMSE) จากการที่ค่า MSE ถูกยกกำลังสองค่า Error ทำให้ค่าเฉลี่ยเปลี่ยนแปลงไป หากต้องการให้ผลการทำนายมีค่า Loss ที่เป็นหน่วยเดียวกับตัวแปร Y จะทำได้ด้วยการทำ Square Root ค่า MSE หรือที่เรียกว่า RMSE ซึ่งจะทำให้เราทราบผลการทำนายค่าเฉลี่ยของตัวแบบทำนายว่าผิดพลาดไปจากค่า Y จริงในทางบวกลบเท่าไหร่ได้ [30] ดังสมการที่ (5)

$$RMSE = \sqrt{\frac{1}{n}\sum_{t=1}^{n}(Y_t - \hat{Y}_t)^2} \quad (5)$$

โดยที่

RMSE คือ ค่ารากที่สองของค่าความคลาดเคลื่อนกำลังสองเฉลี่ย

2.6 งานวิจัยที่เกี่ยวข้อง

Ben Fredj ได้ทำการวิจัยเรื่อง "Cybersecurity Attack Prediction: A Deep Learning Approach" ผลการวิจัยพบว่าการใช้ข้อมูล IP_Source, IP_Destination และ Attack_Typet-1 หรือรูปแบบการบุกรุกทางไซเบอร์ในอดีต มาใช้ในการทำนายรูปแบบการบุกรุกทางไซเบอร์ในปัจจุบัน จะส่งผลทำให้ตัวแบบทำนายมีค่า F-Measure สูงขึ้น เมื่อทำการทดลองกับตัวแบบทำนาย MLP, RNN และ LSTM ซึ่งตัวแบบทำนาย LSTM มีค่าสูงที่สุดกับชุดข้อมูล Called CTF (Defcon Capture the Flag (CTF) Contest)

Xing Fang ได้ทำการวิจัยเรื่อง "Deep Learning Framework for Predicting Cyberattacks Rates" ผลการวิจัยพบว่าการใช้ตัวแบบจำลองและคาดการณ์อัตราการโจมตีทางไซเบอร์ด้วยโครงข่ายประสาทเทียมที่ชื่อ BRNN-LSTM ส่งผลทำให้ประสิทธิภาพความแม่นยำสูงกว่าตัวแบบทำนายพื้นฐานอย่าง ARIMA

Qi Zhang [31] ได้ทำการวิจัยเรื่อง "Multimodel-based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial control Systems" มีการนำเสนอตัวแบบทำนายเกี่ยวกับระบบควบคุมเครื่องปฏิกรณ์เคมีแบบเรียบง่ายใน MATLAB โดยแบ่งออกเป็นสามขั้นตอนคือ การเปิดระบบควบคุมเครื่องปฏิกรณ์เคมี การรวบรวมหลักฐาน การคำนวณความเสี่ยงทางไซเบอร์ทุกนาที ตัวแบบทำนายสามารถทำนายแนวโน้มของเหตุการณ์ความเสี่ยงของ ICSS ซึ่งใช้เป็นแนวทางในการประเมินความเสี่ยงที่เกิดจากการโจมตีทางไซเบอร์ที่ไม่รู้จักมาก่อนได้

3. วิธีดำเนินการวิจัย

ผู้วิจัยได้ศึกษาและรวบรวมข้อมูลเกี่ยวกับรูปแบบภัยคุกคามทางไซเบอร์ของกองทัพอากาศ มีจำนวน 23 รูปแบบ จากนั้น ผู้วิจัยได้คัดเลือกรูปแบบภัยคุกคามที่ระบบตรวจจับการบุกรุกทางไซเบอร์ (IDS) ของกองทัพ อากาศที่ตรวจจับได้ มีจำนวน 17 รูปแบบ ประกอบด้วย ข้อมูลการบุกรุกทางไซเบอร์ทั้งภายใน (Internal Data) และภายนอก (External Data) [32] ที่มีผลกระทบต่อกองทัพอากาศ ตลอดจนดำเนินการตรวจสอบกระบวนการทำงาน ของอัลกอริทึมตัวแบบทำนายการบุกรุกทางไซเบอร์ประเภทการเรียนรู้เชิงลึก เพื่อคัดเลือกตัวแบบทำนายการบุกรุกทางไซเบอร์ที่ดีที่สุดสำหรับทำการทดสอบ โดยมีกรอบแนวคิดในการดำเนินการวิจัย ดังภาพที่ 4

จากภาพที่ 4 กระบวนการพัฒนาตัวแบบทำนายการบุกรุกทางไซเบอร์จะแบ่งออกเป็น 4 ส่วนใหญ่ ๆ คือ 1. Data Acquisition เป็นการรวบรวมข้อมูลภัยคุกคามจากระบบเซนเซอร์ของกองทัพอากาศทั้งภายในและภายนอก 2. Feature Selection เป็นการเลือกข้อมูลและการแบ่งข้อมูลออกเป็นส่วน ๆ เพื่อใช้ในการทดลอง 3. Deep Learning Model เป็นส่วนของตัวแบบทำนาย และ 4. Future Type of Cyber Threats เป็นส่วนแสดงผลการทำนาย โดยกระบวนการทั้งหมดจะทำงานแบบอัตโนมัติ ดังภาพที่ 4

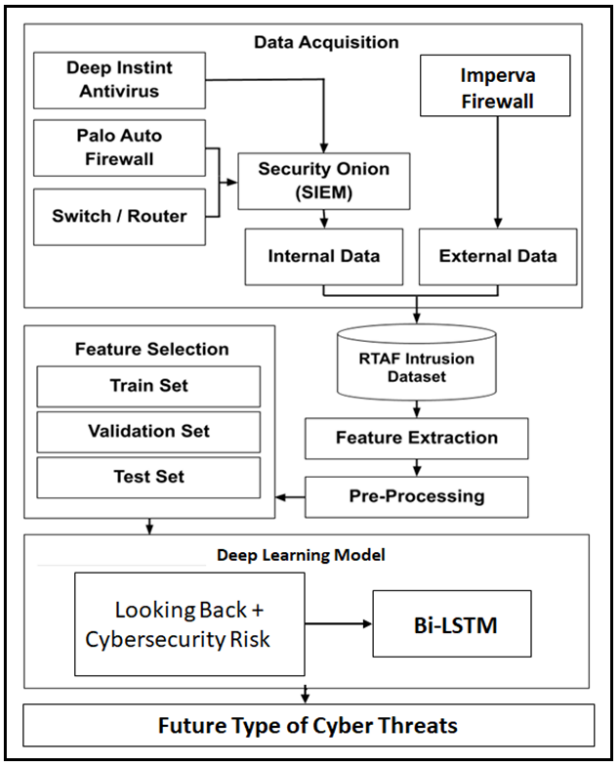
3.1 การคำนวณความเสี่ยงทางไซเบอร์

งานวิจัยนี้ใช้ค่าความเสี่ยงทางไซเบอร์เป็นหนึ่งในค่า Input ของตัวแบบทำนาย สำหรับค่าความเสี่ยงทางไซเบอร์จะเป็นการนำค่าความน่าจะเป็นของรูปแบบภัยคุกคาม (Likelihood) มาคูณกับค่าผลกระทบของรูปแบบภัยคุกคาม (Impact) มีพื้นฐานมาจาก OWASP Risk Rating Methodology Methodology [33] ทั้งนี้จะต้องมีการกำหนดช่วงของอันตรภาคชั้น [34] ของความเสี่ยงระดับของความเสี่ยงจากมากไปน้อย หรือเรียงลำดับเป็นตัวเลข

ขึ้นอยู่กับความต้องการของการกำหนดช่วงความละเอียดในการวัดค่าความเสี่ยง

โดยทั่วไปหน่วยงานต่าง ๆ จะไม่ได้ประเมินความเสี่ยงเพียงแค่ด้านไซเบอร์หรือสารสนเทศเพียงอย่างเดียว แต่จะประเมินความเสี่ยงในทุก ๆ ด้านตามกรอบแนวคิดของ COSO (2012) Risk Assessment in Practice [35] ที่ครอบคลุมในหลายมิติ เช่น ด้านกลยุทธ์ ด้านการเงิน ด้านการบริหาร และด้านกฎหมาย จึงอาจมีการนำเอาเฟรมเวิร์กด้านอื่น ๆ เข้ามาร่วมด้วย เช่น ISO 27005/2018 Information Technology, Security Techniques, Information Security Risk Management (2018) [36] หรือ NIST 800-30 [37] เพื่อให้เข้ากับบริบทความแตกต่างของแต่ละองค์กรด้วยก็ได้ สามารถทำการคำนวณค่าความเสี่ยงทางไซเบอร์ได้ดังสมการที่ (6)

$$Risk = Likelihood \times Impact \quad (6)$$



ภาพที่ 4 *กรอบแนวคิดการพัฒนาตัวแบบทำนายการบุกรุกทางไซเบอร์*

ค่าความเสี่ยงเกิดจากการหาค่า Likelihood ด้วยสมการความน่าจะเป็น (Probability) [38] คูณกับค่า Impact ที่หาจากเทคนิค Analytic Hierarchy Process [39] แล้วจะได้ค่าเฉลี่ยของความเสี่ยงทั้ง 5 ด้าน (การเงิน การดำเนินงาน การกำกับดูแล บุคคลากร ชื่อเสียง) ของภัยคุกคามทางไซเบอร์แต่ละประเภท ดังตารางที่ 4

ตารางที่ 4 *ค่าเฉลี่ยของความเสี่ยงทางไซเบอร์ทั้ง 5 ด้าน*

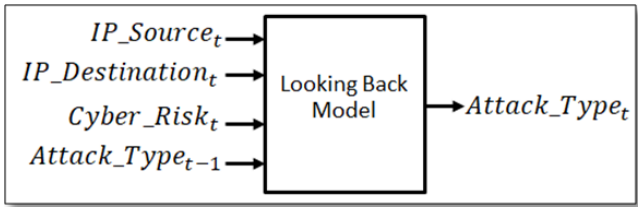
ภัยคุกคามทางไซเบอร์	ค่าเฉลี่ย
Probe	15%
Trojan	12%
Cryptojacking	12%
U2R	12%
Web Shell	9%
Botnet	6%
Injection	6%
Brute force attack	6%
Dropper	6%
Ransomware	3%
R2L	3%
worm	3%
DDoS DoS	3%
Man-in-the-Middle Attacks	3%
Data leak	3%
Phishing	3%
Website Defacement	3%

3.2 สถาปัตยกรรม looking Back + Cyber_Riskt ที่พัฒนาขึ้นใหม่

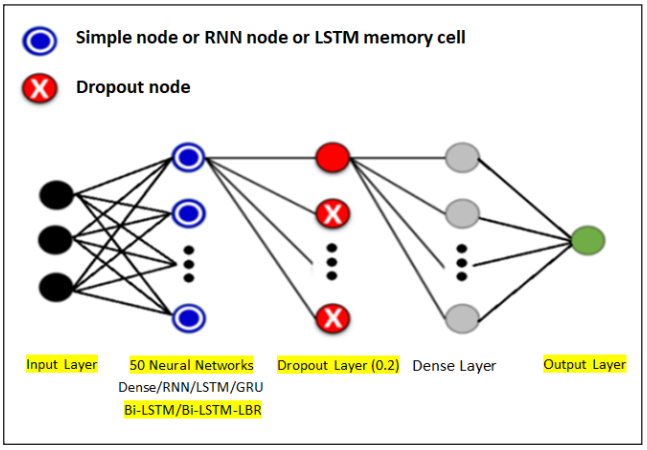
ในสถาปัตยกรรม Looking Back เดิมจะมีนำอินพุตเข้าสู่ตัวแบบทำนายเพียง 3 ลักษณะข้อมูล ประกอบด้วย IP_Sourcet, IP_Destinationt และ Attack Typet แล้วจึงนำเข้าตัวแบบทำนายปกติทั่วไป สำหรับสถาปัตยกรรมใหม่ที่ผู้วิจัยได้พัฒนาขึ้นนั้น จะเพิ่มตัวแปรความเสี่ยงทางไซเบอร์เข้าไปด้วย ทำให้ตัวแบบทำนายมีความแม่นยำสูงขึ้น เนื่องจากมีลักษณะข้อมูลช่วยในการเพิ่มน้ำหนักให้กับผลการทำนาย โดยมีรายละเอียดโครงสร้าง ดังภาพที่ 5

จากภาพที่ 5 พบว่าโครงสร้างสถาปัตยกรรมโครงข่ายประสาทเทียมภายในของตัวแบบทำนายที่ผู้วิจัยพัฒนาขึ้นใหม่เป็นการต่อยอดจากงานวิจัยของ O. Ben Fredj [17]

ด้วยการกำหนดจำนวนนิวรอนเน็ตเวิร์กเป็น 50 มี Dropout Layer ทำหน้าที่สุ่มลดการประมวลผลของ นิวรอนเน็ตเวิร์กเป็น 0.2 และมี Output Layer เพียงหนึ่งตัว เพื่อให้ผลลัพธ์ของการทำนายเป็นรูปแบบภัยคุกคาม (Attack type) เป็นค่าที่ทำให้ตัวแบบทำนายมีความแม่นยำมากที่สุด โดยมีโครงสร้างสถาปัตยกรรมภายในดังภาพที่ 6



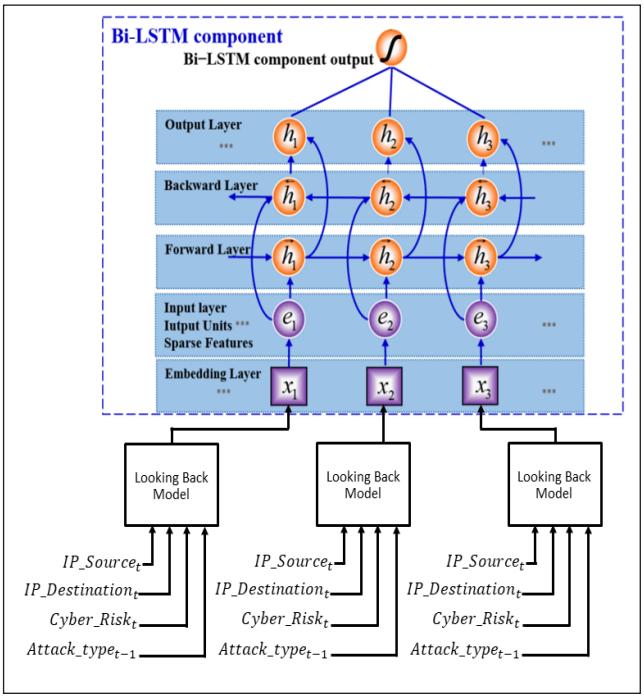
ภาพที่ 5 *สถาปัตยกรรม Looking Back ที่พัฒนาขึ้นใหม่*



ภาพที่ 6 *สถาปัตยกรรมภายในแบบใหม่ของ Looking Back Model ที่ผู้วิจัยพัฒนาขึ้นใหม่*

จากภาพที่ 6 ตัวแบบทำนาย Bi-LSTM ที่มีจุดเด่นในเรื่องของการมองเห็นข้อมูลที่อินพุตเข้ามาได้ครอบคลุมกว่าตัวแบบทำนายอื่น ๆ อีกทั้งสถาปัตยกรรม Looking Back ที่ผ่านการพัฒนาให้ประมวลผลค่าความเสี่ยงทางไซเบอร์ขององค์กรด้วยการอินพุตค่าความเสี่ยงเข้าสู่ตัวแบบทำนายเป็นวิธีการที่ทำให้ประสิทธิภาพตัวแบบทำนายเพิ่มขึ้นได้ ดังนั้น ผู้วิจัยจึงนำอัลกอริทึมทั้งสองรูปแบบมาเชื่อมต่อกัน เพื่อแสดงให้เห็นว่าสถาปัตยกรรม Looking Back เมื่อถูกพัฒนาให้มีคุณสมบัติของข้อมูลค่าความเสี่ยงทางไซเบอร์ของกองทัพอากาศอยู่ในชุดข้อมูลการบุกรุกทางไซเบอร์ของกองทัพอากาศแล้วให้ผลลัพธ์ที่ดีจริงหรือไม่

ผู้วิจัยได้ทำการเปรียบเทียบ กับสถาปัตยกรรมปกติที่มีเพียงลักษณะข้อมูลเป็น IP Address ต้นทาง และ IPAddress ปลายทาง เพื่อใช้ทำนายรูปแบบภัยคุกคามทางไซเบอร์ มีการออกแบบโครงสร้างของสถาปัตยกรรมตัวแบบทำนายใหม่ดังภาพที่ 7



ภาพที่ 7 *ตัวแบบทำนาย Bi-LSTM Looking Back Risk: Bi-LSTM-LBR ที่พัฒนาขึ้นใหม่*

ผลจากการพัฒนาตัวแบบทำนายขึ้นใหม่ จะเห็นได้ว่าสถาปัตยกรรมของตัวแบบทำนาย Bi-LSTM-LBR มีการรับค่าอินพุตเป็นข้อมูล IP_Source, IP_Destination, Attack_Typet-1 และ Cyber Risk ที่เป็นรูปแบบของการ อินพุตข้อมูลแบบ Looking Back Model ที่มีการพัฒนาให้ Dropout Layer ทำการสุ่มหยุดการทำงานของนิวรอนเน็ตเวิร์กลงเพื่อลดการประมวลผลและเพิ่มความเร็วในการประมวลผล รวมทั้งมีโหนดในการรวมผลการทำนายทำหน้าที่รวมข้อมูลทั้งหมดแล้วตัดสินใจว่าจะได้รูปแบบภัยคุกคามทางไซเบอร์เป็นอะไร เพื่อให้ได้เอาต์พุตเป็น 1 โหนด จากนั้น จึงส่งต่อเข้าไปยังตัวแบบทำนาย Bi-LSTM ใน Embedding Layer ณ ตำแหน่ง X1 จนถึง Xn มีส่วนช่วยในกระบวนการรับค่าอินพุตได้กว้างมากขึ้น ทำให้ตัวแบบทำนายเห็นข้อมูลที่ใส่เข้ามาได้กว้างมากขึ้นตามไปด้วย ขณะที่ข้อมูลเมื่อถูกนำเข้าไปประมวลผลในนิวรอนเน็ตเวิร์ก ตัวแบบทำนายก็จะทำการหาค่าน้ำหนักของข้อมูลคล้ายกับตัวแบบทำนาย LSTM แต่จะทำทั้งไปข้างหน้าและย้อนกลับในเวลาเดียวกัน เนื่องจากเป็น Layer ที่ขนานกันอยู่ หลังจากประมวลผลเสร็จแล้วก็จะส่งเป็นเอาต์พุตออกมาที่ Output Layer ที่มีโหนด Activation ทำหน้าที่ตัดสินใจ

ขั้นสุดท้ายก่อนที่จะส่งผลลัพธ์ออกมาเป็นชื่อรูปแบบภัยคุกคามทางไซเบอร์ในอนาคตตามกระบวนการ Training ที่ได้สอนไว้

4. ผลการดำเนินงาน

การที่ Bi-LSTM Looking Back Risk: Bi-LSTM-LBR ที่พัฒนาขึ้นใหม่มีค่าเฉลี่ยความคลาดเคลื่อนกำลังสองน้อยที่สุด แสดงให้เห็นว่าตัวแบบทำนายดังกล่าวมีความแม่นยำสูงที่สุด เรียงลำดับจากค่าความคลาดเคลื่อนต่ำจาก RNN, LSTM, GRU และ Bi-LSTM ที่มีค่าความคลาดเคลื่อนต่ำที่สุด แสดงให้เห็นว่าตัวแบบทำนายที่มีความซับซ้อนสูง จะมีแนวโน้มให้ค่าความคลาดเคลื่อนต่ำ และเมื่อเปรียบเทียบตาราง Looking Back ปกติกับตาราง Looking Back + Cyber_Riskt จะได้ว่าค่า MAE, MSE และ RMSE ลดลงอย่างเห็นได้ชัด ฉะนั้นการเพิ่มค่าความเสี่ยงทางไซเบอร์เข้าไปในตัวแบบทำนายด้วยกระบวนการ Looking Back จะส่งผลทำให้ตัวแบบทำนายมีค่าความคลาดเคลื่อนต่ำลงได้จริง ดังตารางที่ 5 และ 6

ตารางที่ 5 *ผลการทดลองตัวแบบทำนายการบุกรุกทางไซเบอร์*

ตัวแบบทำนาย	MAE	MSE	RMSE
RNN	0.187	0.053	0.231
LSTM	0.053	0.015	0.126
GRU	0.052	0.017	0.133
Bi-LSTM	0.049	0.016	0.127

ตารางที่ 6 *ผลการทดลองตัวแบบทำนายการบุกรุกทางไซเบอร์ Looking Back + Cyber_Riskt*

ตัวแบบทำนาย	MAE	MSE	RMSE
RNN	0.044	0.013	0.115
LSTM	0.039	0.012	0.110
GRU	0.037	0.013	0.113
Bi-LSTM	0.043	0.012	0.107
Bi-LSTM-LBR	0.038	0.010	0.102

ผลการทดลองของตัวแบบทำนายที่ใช้สถาปัตยกรรม Looking Back ปกติดังตารางที่ 5 และสถาปัตยกรรม Looking Back + Cyber_Riskt หรือค่าความเสี่ยงทางไซเบอร์ ซึ่งเป็นการทดสอบตัวแบบทำนายที่พัฒนาขึ้นใหม่ มีผลลัพธ์ ดังตารางที่ 6

จากตารางที่ 6 ตัวแบบทำนาย RNN มีค่า MAE เท่ากับ 0.044 MSE มีค่าเท่ากับ 0.013 RMSE มีค่าเท่ากับ 0.115 ตัวแบบทำนาย LSTM มีค่า MAE เท่ากับ 0.039 MSE มีค่าเท่ากับ 0.012 RMSE มีค่าเท่ากับ 0.110 ตัวแบบทำนาย GRU มีค่า MAE เท่ากับ 0.037 MSE มีค่าเท่ากับ 0.013 RMSE มีค่าเท่ากับ 0.113 ตัวแบบทำนาย Bi-LSTM มีค่า MAE เท่ากับ 0.043 MSE มีค่าเท่ากับ 0.012 RMSE มีค่าเท่ากับ 0.107 และตัวแบบทำนาย Bi-LSTM-LBR ที่พัฒนาขึ้นใหม่ มีค่า MAE เท่ากับ 0.038 MSE มีค่าเท่ากับ 0.010 RMSE มีค่าเท่ากับ 0.102

ตัวแบบทำนายพื้นฐานเช่น RNN, LSTM และ GRU จะมีค่าความคลาดเคลื่อน MAE ที่มีแนวโน้มลดลงเรื่อย ๆ ตามความซับซ้อนของตัวแบบทำนาย ตัวแบบทำนาย RNN มีค่าความคลาดเคลื่อนของการทำนายหรือ MAE อยู่ที่ 0.044 ถือว่ามากที่สุด รองมาคือ Bi-LSTM ตามด้วย LSTM และ GRU ในขณะที่ตัวแบบทำนายที่ทำคะแนนได้ดีที่สุดคือ Bi-LSTM-LBR ที่พัฒนาขึ้นใหม่ มีค่า MAE อยู่ที่ 0.038 ถือว่าน้อยที่สุด แสดงให้เห็นว่าความคลาดเคลื่อนโดยรวมน้อยกว่าทุกตัวแบบทำนาย ขณะที่ค่าความคลาดเคลื่อนเฉลี่ย หรือ MSE ตัวแบบทำนาย RNN กับ GRU ได้ค่า MSE เท่ากัน ขณะที่ LSTM กับ Bi-LSTM ได้ต่ำลงมาเล็กน้อย เช่นเดียวกับตัวแบบทำนายที่พัฒนาขึ้นใหม่ที่ไม่ได้มีค่าห่างจากตัวแบบทำนายพื้นฐานมากนัก ขณะที่ค่า RMSE หรือค่ารากที่สองของค่าความคลาดเคลื่อนกำลังสองเฉลี่ย ที่แสดงให้เห็นว่าตัวแบบทำนายที่ได้ค่านี้น้อยเท่าไหร่ จะหมายความว่าตัวแบบทำนายดังกล่าวมีผลการทำนายที่คลาดเคลื่อนน้อยนั้นเอง แท้จริงแล้วเราจะพบว่าตัวแบบทำนายการบุกรุกทางไซเบอร์ที่พัฒนาขึ้นใหม่มีค่า RMSE น้อยที่สุด คือ 0.102 ตามมาด้วย Bi-LSTM, LSTM, GRU และ RNN ตามลำดับ

5. สรุป

งานวิจัยนี้ ผู้วิจัยได้ทำการพัฒนา ตลอดจนทดสอบตัวแบบทำนายการบุกรุกทางไซเบอร์แบบอัตโนมัติด้วยเทคโนโลยีปัญญาประดิษฐ์ภายใต้การเรียนรู้เชิงลึก สำหรับกองทัพอากาศกับชุดข้อมูลการบุกรุกทางไซเบอร์ของกองทัพอากาศ ซึ่งเป็นข้อมูลการโจมตีต่อระบบข่ายคอมพิวเตอร์ของกองทัพอากาศ ตั้งแต่วันที่ 1 มกราคม 2564 ถึง วันที่ 31 ธันวาคม 2564 ขณะที่ชุดข้อมูลดังกล่าวมีความแตกต่างจากชุดข้อมูลทั่วไป คือมีรูปแบบของการโจมตีทางไซเบอร์ที่เป็นกลุ่มภัยคุกคามทางไซเบอร์ที่มีความเฉพาะด้านของกองทัพอากาศ

จากผลการวิจัยแสดงให้เห็นว่า ผลการพัฒนาอัลกอริทึม Looking Back ด้วยการเพิ่มคุณลักษณะข้อมูลค่าความเสี่ยงทางไซเบอร์ของหน่วยงาน (Looking Back + Cyber_Riskt) และการเพิ่มประสิทธิภาพผลการทำนายด้วยการรวมเข้ากับตัวแบบทำนาย Bi-LSTM ส่งผลให้ตัวแบบทำนายการบุกรุกทางไซเบอร์ที่พัฒนาขึ้นมีค่าความผิดพลาดของการทำนายลดลงได้จริง โดยสาเหตุที่เป็นเช่นนี้สืบเนื่องมาจากอัลกอริทึม Looking Back เป็นเทคนิคในการเพิ่มลักษณะข้อมูล (Feature) ให้กับตัวแบบทำนาย เปรียบได้กับการมีตัวแปรช่วยยืนยันความแม่นยำของข้อมูลที่มีการส่งเข้ามาประมวลผลในนิวรอนเน็ตเวิร์ก ทำให้ค่าน้ำหนักมีความชัดเจนยิ่งขึ้นในแต่ละผลการทำนาย ประกอบกับความสามารถของตัวแบบทำนายกลุ่ม Bidirectional ที่สามารถมองเห็นข้อมูลอินพุตที่เข้ามาประมวลผลได้แบบสองทิศทาง จึงส่งผลทำให้ตัวแบบทำนายที่พัฒนาขึ้นใหม่มีค่าความแม่นยำที่สูงขึ้น ทั้งนี้หากมีการนำเอาความสามารถดังกล่าวมาใช้ในการวิเคราะห์ข้อมูลทั้งในอดีตและแนวโน้มที่จะเกิดขึ้นในอนาคตได้พร้อม ๆ กันผ่านตัวแบบทำนายตัวเดียวได้ก็จะเป็นการเพิ่มประสิทธิภาพให้กับการทำนายการบุกรุกทางไซเบอร์ได้อีกมาก

6. เอกสารอ้างอิง

[1] K. Shaukat, et al. "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade." *IEEE Access,* Vol. 8, pp. 222310-222354, 2020.

[2] C. Liu, et al. "A Hybrid Intrusion Detection System Based on Scalable K-Means+ Random Forest and Deep Learning." *IEEE Access,* Vol. 9, pp. 75729-75740, 2021.

[3] R. Ali, et al. "Deep Learning Methods for Malware and Intrusion Detection: A Systematic Literature Review." *Security and Communication Networks,* Vol. 2022, pp. 1-31, 2022.

[4] M. Husak, et al. "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security." *IEEE Communications Surveys & Tutorials,* Vol. 21, No. 1, pp. 640-660, 2019.

[5] Z. Li, D. Zou, J. Tang, Z. Zhang, M. Sun, and H. Jin. "A Comparative Study of Deep Learning-Based Vulnerability Detection System." *IEEE Access,* Vol. 7, pp. 103184-103197, 2019.

[6] K. Pranomkorn, et al. "Development of a Model and Forecasting of Hourly UV Index Using Artificial Neural Network (ANN) at Songkhla." *RMUTP Research Journal,* Vol. 15, No. 2, pp. 81-82, July-December, 2021.

[7] R. Angela and Borisova. "NEURAL NETWORK FOR CYBERSECURITY." *Proceedings of International Scientific Conference-Defense Technologies DefTech 2023,* Bulgaria, pp. 513-514, 2024.

[8] I. R. Widiasari, L. E. Nugroho, and Widyawan. "Deep Learning Multilayer Perceptron (MLP) for Flood Prediction Model Using Wireless Sensor Network Based Hydrology Time Series Data Mining." *International Conference on Innovative and Creative Information Technology,* Indonesia, pp. 1-2, 2017.

[9] Wei, Yuanyuan, et al. "Ae-mlp: A hybrid deep learning approach for ddos detection and classification." *IEEE Access,* Vol. 9, pp. 146810-146821, 2021.

[10] Y. Javed, et al. "Multi-layer perceptron artificial neural network based IoT botnet traffic classification." *Springer International Publishing, Proceedings of the Future Technologies Conference (FTC),* USA, Vol. 1, 2020.

[11] C. Wang, et al. "A dependable time series analytic framework for cyber-physical systems of IoT-based smart grid." *ACM Transactions on Cyber-Physical Systems,* Vol. 3, No. 1, pp. 1-18, 2018.

[12] X. Fang, M. Xu, S. Xu, and P. Zhao. "A Deep Learning Framework for Predicting Cyber Attacks Rates." *EURASIP Journal on Information Security,* Vol. 2019, No. 1, pp. 3-4, 2019.

[13] H. Ye, et al. "Web Services Classification Based on Wide & Bi-LSTM Model." *IEEE Access,* Vol. 7, pp. 43697-43706, 2019.

[14] K. Cho, B.V. Merrienboer et al. "Learning phrase representations using RNN encoder-decoder for statistical machine translation." *In Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP),* Doha, Qatar, pp. 1724-1734, 2014.

[15] T. Phaladisailoed and Thanisa Numnonda. "Comparison of Learning Models of Various Uniforms for Bitcoin Price Prediction." *Journal of Information Technology Ladkrabang,* No. 1, pp. 4-7, January-June, 2017.

[16] Aldalbahi, A. F. Shahabi, and M. Jasim. "BRNN-LSTM for Initial Access in Millimeter Wave Communications." *Electronics 2021,* Vol. 10, pp. 8-10, 2021.

[17] Ben Fredj, Ouissem, et al. "CyberSecurity attack prediction: a deep learning approach." *13th international conference on security of information and networks, Association for Computing Machinery,* Merkez, Turkey, 2020.

[18] Mihoub, Alaeddine, et al. "Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques." *Computers & Electrical Engineering,* Vol. 98, pp. 3-5, 2022.

[19] D.R. Mérette, et al. "Introduction to Anaconda and Python: Installation and setup." *TEMP, Methods Psychol,* Vol. 16, No. 5, pp. 3-11, 2016.

[20] E. Monday, et al. "Program-Based Construction of Scientific Visualization." *World Journal of Advanced Research and Reviews,* Vol. 11, No. 3, pp. 413-423, 2021.

[21] J. Ott, et al. "A Fortran-Keras Deep Learning Bridge for Scientific Computing." *Scientific Programming,* Vol. 2020, pp. 1-13, 2020.

[22] C. B. Taha and A. B. Sallow. "A comprehensive survey of deep learning models based on Keras framework." *Journal of Soft Computing and Data Minin,* Vol. 2, No. 2, pp. 49-62, July 2021.

[23] M. Abadi, et al. "TensorFlow: A System for Large-Scale Machine Learning." *Proceedings of 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16),* pp. 265-283, 2016.

[24] P. Victor, et al. "Trieste: Efficiently exploring the depths of black-box functions with Tensor Flow." *Ghent University – imec,* Ghent, Belgium, pp. 1-4, 2023.

[25] K. Sraubon. *AI: Deep Learning by Python.* SE-ED Publishing, 2021.

[26] I. A. Kandhro, et al. "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures." *IEEE Access,* Vol. 11, pp. 9136-9148, 2023.

[27] S. Liu, et al. "Model-Free Data Authentication for Cyber Security in Power Systems." *in IEEE Transactions on Smart Grid,* Vol. 11, No. 5, pp. 4565-4568, September, 2020.

[28] M. Uzair and N. Jamil. "Effects of Hidden Layers on the Efficiency of Neural Networks." *IEEE International Multitopic Conference,* Islamabad, Pakistan, pp. 2-6, 2020.

[29] T. Kaewwijit. *The Improvement of Support Vector Regression to Forecast Time Series.* Master Thesis, Computer Engineering, Suranaree University of Technology, 2016.

[30] A. A. Mir. "An Improved Imputation Method for Accurate Prediction of Imputed Dataset Based Radon Time Series." *IEEE Access,* Vol. 10, pp. 6-7, 2022.

[31] Q. Zhang, et al. "Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems." *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* Vol. 46, No. 10, pp. 1429-1444, 2016.

[32] L. Allodi and F. Massacci. "Security Events and Vulnerability Data for Cybersecurity Risk Estimation." *Risk Analysis,* Vol. 37, No. 8, pp. 1606-1627, 2017.

[33] V. Malamas, P. Kotzanikolaou, and C. Douligeris. "Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal." *IEEE Access,* Vol. 9, pp. 40049-40075, 2021.

[34] L. Silanoi and K. Chindaprasert. "The Use of Rating Scale in Quantitative Research on Social Sciences, Humanities, Hotel and Tourism Study." *Journal of Management Science, Ubon Ratchathani University,* Vol. 8, No. 15, pp. 112-126, January-June, 2019.

[35] A. Hemanidhi and S. Chimmanee. "Military-based Cyber Risk Assessment Framework for Supporting Cyber Warfare in Thailand." *Journal of Information and Communication Technology,* Vol. 16, No. 2, pp. 192-222, December, 2017.

[36] S. Ariyani and M. Sudarma. "Implementation of the ISO/IEC 27005 in Risk Security Analysis of Management Information Systems." *Journal of Engineering Research and Application,* Vol. 6, No. 8, pp. 1-6, August, 2016.

[37] M. A. Fikri, et al. "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency." *Procedia Computer Science,* Vol. 161, pp. 1206-1215, 2019.

[38] D. Dudorov, et al. "Probability analysis of cyber attack paths against business and commercial enterprise systems." *IEEE European Intelligence and Security Informatics Conference,* London, United Kingdom, pp. 38-44, 2013.

[39] M.X. He. and X. An. "Information security risk assessment based on analytic hierarchy process." *Indonesian Journal of Electrical Engineering and Computer Science 1.3,* Vol. 1, No. 3, pp. 656-664, March, 2016.