โครงงานเลขที่ วศ.คพ. S808-1/2568

เรื่อง

ระบบตรวจจับภัยคุกคามในเทคโนโลยีปฏิบัติการ (OT) สำหรับโรงงานอุตสาหกรรม

โดย

นายธนกฤต บุญยัง รหัส 650612084
นายศุภกร สุวรรณภพ รหัส 650612100
นายอดิศร สันเจริญ รหัส 650612104

โครงงานนี้
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต
ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่
ปีการศึกษา 2568

PROJECT No. CPE S808-1/2568

Anomaly Detection in Operational Technology for Industrial Control Systems

Tanakrit boonyoung 650612084
Suppakorn suwannapop 650612100
Adisorn sancharoen 650612104

A Project Submitted in Partial Fulfillment of Requirements
for the Degree of Bachelor of Engineering
Department of Computer Engineering
Faculty of Engineering
Chiang Mai University
2025

หัวข้อโครงงาน	: ระบบตรวจจับภัยคุกคามในเทคโนโลยีปฏิบัติการ (OT) สำหรับโรงงานอุตสาหกรรม	
	: Anomaly Detection in Operational Technology for Industrial Control Systems	
โดย	: นายธนกฤต บุญยัง	รหัส 650612084
	นายศุภกร สุวรรณภพ	รหัส 650612100
	นายอดิศร สันเจริญ	รหัส 650612104
ภาควิชา	: วิศวกรรมคอมพิวเตอร์	
อาจารย์ที่ปรึกษา	: ผศ.ดร. กำพล วรดิษฐ์	
ปริญญา	: วิศวกรรมศาสตรบัณฑิต	
สาขา	: วิศวกรรมคอมพิวเตอร์	
ปีการศึกษา	: 2568	

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้อนุมัติให้โครงงานนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต (สาขาวิศวกรรมคอมพิวเตอร์)

..... หัวหน้าภาควิชาวิศวกรรมคอมพิวเตอร์
(รศ.ดร. สันติ พิทักษ์กิจนุกูร)

คณะกรรมการสอบโครงงาน

..... ประธานกรรมการ
(ผศ.ดร. กำพล วรดิษฐ์)

..... กรรมการ
(ผศ.ดร. เกษมสิทธิ์ ตียพันธ์)

..... กรรมการ
(อ.นพรุจ ซื่อตรง)

หัวข้อโครงงาน	: ระบบตรวจจับภัยคุกคามในเทคโนโลยีปฏิบัติการ (OT) สำหรับโรงงานอุตสาหกรรม	
	: Anomaly Detection in Operational Technology for Industrial Control Systems	
โดย	: นายธนกฤต บุญยัง	รหัส 650612084
	นายศุภกร สุวรรณภพ	รหัส 650612100
	นายอดิศร สันเจริญ	รหัส 650612104
ภาควิชา	: วิศวกรรมคอมพิวเตอร์	
อาจารย์ที่ปรึกษา	: ผศ.ดร. กำพล วรดิษฐ์	
ปริญญา	: วิศวกรรมศาสตรบัณฑิต	
สาขา	: วิศวกรรมคอมพิวเตอร์	
ปีการศึกษา	: 2568	

บทคัดย่อ

ในยุคอุตสาหกรรม 4.0 โรงงานจำนวนมากได้ปรับใช้ระบบควบคุมอัตโนมัติ (Industrial Control Systems: ICS) ที่เชื่อมโยงกับเทคโนโลยีปฏิบัติการ (Operational Technology: OT) เพื่อตรวจวัดและควบคุมกระบวนการผลิตแบบเรียลไทม์ อย่างไรก็ตาม ความเชื่อมโยงดังกล่าวได้นำมาซึ่งความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจสร้างผล กระทบทั้งในด้านเศรษฐกิจ ความปลอดภัย และสิ่งแวดล้อม โครงงานนี้มีวัตถุประสงค์เพื่อพัฒนา ต้นแบบระบบตรวจจับความผิดปกติ (Intrusion/Anomaly Detection) ที่ใช้เทคนิคการเรียนรู้เชิงลึก (Deep Learning) โดยมุ่งเน้นไปที่การวิเคราะห์ข้อมูลลำดับเวลา (time-series data) ของเซนเซอร์และแอกชูเอเตอร์ในระบบ OT

กระบวนการวิจัยประกอบด้วยการจัดเตรียมและทำความสะอาดข้อมูล (preprocessing) การออกแบบคุณลักษณะ (feature engineering) การสร้างหน้าต่างเวลา (sliding window) และการฝึกโมเดลตรวจจับความผิดปกติ โดยใช้ สถาปัตยกรรม CNN-LSTM แบบหนึ่งมิติ (1D CNN-LSTM) ซึ่งสามารถจับทั้งความสัมพันธ์เชิงเวลาและความสัมพันธ์เชิงลักษณะระหว่างเซนเซอร์ได้ ผลลัพธ์ของโมเดลถูกประเมินด้วยตัวชี้วัด เช่น Accuracy, Precision, Recall และ F1-score เพื่อตรวจสอบประสิทธิภาพในการแยกเหตุการณ์ปกติและเหตุการณ์โจมตี

Project Title	: Anomaly Detection in Operational Technology for Industrial Control Systems	
Name	: Tanakrit boonyoung	650612084
	Suppakorn suwannapop	650612100
	Adisorn sancharoen	650612104
Department	: Computer Engineering	
Project Advisor	: Asst. Prof. Kampol Woradit, Ph.D.	
Degree	: Bachelor of Engineering	
Program	: Computer Engineering	
Academic Year	: 2025	

ABSTRACT

In the era of Industry 4.0, many industrial plants have adopted Industrial Control Systems (ICS) integrated with Operational Technology (OT) to monitor and control production processes in real time. However, this interconnection has also introduced significant cybersecurity risks that may cause severe impacts on economic stability, safety, and the environment. This project aims to develop a prototype anomaly and intrusion detection system leveraging Deep Learning techniques, with a focus on analyzing the time-series data of sensors and actuators within OT environments.

The research process involves several steps: data cleaning and preprocessing, feature engineering, sliding window generation, and training anomaly detection models. A 1D CNN-LSTM architecture is employed to capture both temporal dependencies and cross-sensor feature relationships. The model's performance is evaluated using metrics such as Accuracy, Precision, Recall, and F1-score to assess its ability to distinguish between normal operations and cyberattacks.

สารบัญ

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ที่มาของโครงงาน

ในปัจจุบันโรงงานอุตสาหกรรมจำนวนมากได้ยกระดับกระบวนการผลิตให้มีความเป็นอัตโนมัติสูงขึ้น โดยอาศัยระบบควบคุมอุตสาหกรรม (Industrial Control Systems: ICS) ที่ทำงานร่วมกับระบบเทคโนโลยีปฏิบัติการ (Operational Technology: OT) ซึ่งเชื่อมโยงเซนเซอร์และแอกชูเอเตอร์เข้ากับเครื่องจักรจริง อย่างไรก็ตาม การที่ระบบ OT ถูกเชื่อมต่อเข้ากับเครือข่ายดิจิทัลมากขึ้น ย่อมทำให้ความเสี่ยงจากภัยคุกคามทางไซเบอร์เพิ่มสูงขึ้นตามไปด้วย การโจมตีดังกล่าวอาจทำให้ข้อมูลสูญหายหรือบิดเบือน รวมถึงก่อให้เกิดความเสียหายต่อเครื่องจักร กระบวนการผลิต และความปลอดภัยของบุคลากรได้โดยตรง ดังนั้นโครงงานนี้จึงถูกริเริ่มขึ้นเพื่อพัฒนากลไกการตรวจจับพฤติกรรมที่ผิดปกติในระบบ OT โดยใช้เทคนิคการเรียนรู้ของเครื่อง (Machine Learning) เพื่อเสริมสร้างความปลอดภัยและลดความเสียหายที่อาจเกิดขึ้นในโรงงานอุตสาหกรรม

1.2 วัตถุประสงค์ของโครงงาน

1. ออกแบบและพัฒนาโมเดลตรวจจับความผิดปกติจากข้อมูลเซนเซอร์และแอกชูเอเตอร์ในระบบ OT โดยใช้การวิเคราะห์เชิงเวลา (time-series analysis) ร่วมกับโมเดลเชิงลึก เช่น CNN และ LSTM
2. ระบุเหตุการณ์ที่มีลักษณะเป็นการโจมตีทางไซเบอร์หรือพฤติกรรมที่ผิดปกติในกระบวนการผลิต
3. พัฒนาต้นแบบ (prototype) ที่สามารถนำไปประยุกต์ใช้กับสภาพแวดล้อมในโรงงานจริงได้

1.3 ขอบเขตของโครงงาน

1.3.1 ขอบเขตด้านฮาร์ดแวร์

1. โครงงานนี้ ไม่ได้มุ่งเน้นการพัฒนาหรือใช้งานฮาร์ดแวร์จริง เช่น PLC, ปั๊ม, หรือวาล์ว
2. ส่วนประกอบเหล่านี้ถูก จำลองผ่านข้อมูลจาก SWaT dataset เท่านั้น
3. การดำเนินงานทั้งหมดจึงมุ่งเน้นที่การวิเคราะห์เชิงข้อมูลและการออกแบบโมเดล Machine Learning โดยไม่เกี่ยวข้องกับการสร้างหรือทดสอบระบบฮาร์ดแวร์จริง

1.3.2 ขอบเขตด้านซอฟต์แวร์

การเก็บและใช้ข้อมูล (Data Collection)

1. ใช้ชุดข้อมูล SWaT Dataset (Secure Water Treatment) ซึ่งเป็นข้อมูลจากระบบจำลองโรงงานน้ำประปาที่ใช้กันอย่างแพร่หลายในการศึกษาด้านความปลอดภัยของระบบ ICS/OT
2. ข้อมูลประกอบด้วยค่าการทำงานของเซนเซอร์และแอกชูเอเตอร์ที่มีทั้งสภาวะปกติและสภาวะถูกโจมตี
3. การนำเข้าข้อมูลจะใช้วิธีการอ่านไฟล์ CSV และเตรียมข้อมูลให้อยู่ในรูปแบบที่เหมาะสมต่อการประมวลผล

การตรวจจับและจำแนกความผิดปกติ (Threat Detection and Classification)

1. มุ่งเน้นการตรวจจับเหตุการณ์ที่มีลักษณะผิดปกติ เช่น การเปลี่ยนค่าของเซนเซอร์อย่างผิดธรรมชาติ หรือการสั่งการอุปกรณ์ที่ไม่สอดคล้องกับกระบวนการจริง
2. การจำแนกความผิดปกติออกเป็นสองกลุ่มหลัก ได้แก่
   (a) เหตุการณ์ปกติ (Normal events)
   (b) เหตุการณ์โจมตี/ผิดปกติ (Anomaly/Attack events)
3. การสร้าง Label จะอ้างอิงจากช่วงเวลาที่กำหนดไว้ในเอกสาร SWaT dataset

การประมวลผลและจัดการข้อมูล (Data Implementation)

1. การทำความสะอาดข้อมูล (data preprocessing) เช่น การจัดการค่าที่หายไป, การแทนค่าผิดปกติ, และการ normalize ข้อมูลให้อยู่ในสเกลเดียวกัน
2. การแบ่งข้อมูลออกเป็น Training set, Validation set และ Test set โดยอ้างอิงตามลำดับเวลาเพื่อเลี่ยงการรั่วไหลของข้อมูล (data leakage)
3. การสร้าง sliding windows สำหรับข้อมูลเชิงเวลา (time-series) เพื่อเตรียมให้เป็นอินพุตของโมเดล

การสร้างโมเดลและเปรียบเทียบประสิทธิภาพ (Model Comparison and Performance Evaluation)

1. พัฒนาโมเดลตรวจจับความผิดปกติที่อิงกับ Deep Learning ได้แก่
   (a) Convolutional Neural Network (CNN)
   (b) Long Short-Term Memory (LSTM)
2. ทดสอบโมเดลหลายรูปแบบ เช่น CNN 1D สำหรับจับ pattern ตามลำดับเวลา และ LSTM สำหรับตรวจจับ dependency ระหว่างข้อมูลในช่วงยาว
3. ประเมินผลลัพธ์ด้วยตัวชี้วัดมาตรฐาน
   (a) Accuracy, Precision
   (b) Recall, F1-score
   (c) Confusion Matrix
   (d) AUC-PR/ROC
4. เปรียบเทียบประสิทธิภาพของแต่ละโมเดลเพื่อหาวิธีที่เหมาะสมที่สุดต่อการใช้งาน

ผลลัพธ์ที่คาดว่าจะได้รับ (Expected Outcomes)

1. ได้ต้นแบบ (Prototype) ของระบบตรวจจับความผิดปกติในข้อมูลจากระบบ ICS/OT
2. โมเดลที่พัฒนาแล้วสามารถแยกความแตกต่างระหว่างเหตุการณ์ปกติและเหตุการณ์ผิดปกติได้ในระดับที่แม่นยำ
3. ได้ชุดข้อมูลและโค้ดที่สามารถนำไปปรับใช้หรือต่อยอดในงานวิจัยด้านความปลอดภัยไซเบอร์สำหรับระบบอุตสาหกรรม
4. สนับสนุนการเพิ่มมาตรการด้าน ความมั่นคงปลอดภัยเชิงปฏิบัติการ (Operational Security) ในโรงงานอุตสาหกรรม

1.4 ประโยชน์ที่ได้รับ

ด้านความรู้และความเข้าใจ

1. ได้ความเข้าใจในเชิงลึกเกี่ยวกับประเด็นด้านความมั่นคงปลอดภัยในระบบควบคุมอุตสาหกรรม (OT/ICS)
2. เพิ่มพูนทักษะในการนำ Machine Learning มาประยุกต์ใช้กับข้อมูลเชิงเวลา (time-series)

ด้านการพัฒนาเทคโนโลยี

1. ได้ต้นแบบ (Prototype) ของระบบตรวจจับความผิดปกติที่สามารถนำไปต่อยอดการพัฒนาระบบจริงได้
2. แสดงให้เห็นความเป็นไปได้ของการนำ AI/ML มาใช้แก้ปัญหาความปลอดภัยในภาคอุตสาหกรรม

ด้านการประยุกต์ใช้

1. ผลงานที่ได้สามารถนำไปใช้ตรวจจับการโจมตีหรือพฤติกรรมผิดปกติในโรงงานอุตสาหกรรมจริง
2. ช่วยเพิ่มความปลอดภัยทั้งในด้านข้อมูล เครื่องจักร และบุคลากร ลดความเสี่ยงจากการหยุดชะงักของกระบวนการผลิต

ด้านการวิจัยและการศึกษา

1. สามารถนำองค์ความรู้และผลลัพธ์ไปต่อยอดในเชิงวิจัยด้านความปลอดภัยไซเบอร์สำหรับระบบอุตสาหกรรม
2. เป็นกรณีศึกษาในการบูรณาการ Machine Learning กับความปลอดภัยไซเบอร์ (AI for Cybersecurity)

1.5 เทคโนโลยีและเครื่องมือที่ใช้

1.5.1 เทคโนโลยีด้านฮาร์ดแวร์

Graphics Processing Unit (GPU)

1. ใช้ GPU จากบริการ Google Colab เพื่อเร่งความเร็วในการฝึกโมเดลเชิงลึก (Deep Learning)

1.5.2 เทคโนโลยีด้านซอฟต์แวร์

ภาษาโปรแกรม (Programming Language)

1. ใช้ GPU จากบริการ Google Colab เพื่อเร่งความเร็วในการฝึกโมเดลเชิงลึก (Deep Learning)

เฟรมเวิร์กและไลบรารีสำหรับ Machine Learning (Frameworks and Libraries)

1. Scikit-learn: สำหรับ preprocessing การสร้าง baseline model และการประเมินผลเบื้องต้น
2. TensorFlow และ PyTorch: สำหรับการพัฒนาและฝึกโมเดลเชิงลึก (Deep Learning) เช่น CNN และ LSTM
3. Pandas และ NumPy: สำหรับการจัดการข้อมูลเชิงตารางและการคำนวณเชิงตัวเลข
4. Matplotlib และ Seaborn: สำหรับการสร้าง Visualization วิเคราะห์ข้อมูลและผลลัพธ์ของโมเดล

สภาพแวดล้อมการพัฒนา (Development Environment)

1. Jupyter Notebook และ Google Colab: สำหรับการทดลองเชิงโค้ด การประเมินผล และการรันโมเดลบน GPU
2. GitHub: สำหรับการจัดการซอร์สโค้ดและการทำงานร่วมกัน

1.6 แผนการดำเนินงาน

ขั้นตอนการดำเนินงาน	มิ.ย. 2568	ก.ค. 2568	ส.ค. 2568	ก.ย. 2568	ต.ค. 2568	พ.ย. 2568	ธ.ค. 2568	ม.ค. 2569	ก.พ. 2569
ศึกษาค้นคว้า									
ชิล									
เผา									
ทดสอบ									

1.7 บทบาทและความรับผิดชอบ

อธิบายว่าในการทำงาน นศ. มีการกำหนดบทบาทและแบ่งหน้าที่งานอย่างไรในการทำงาน จำเป็นต้องใช้ความรู้ใดในการทำงานบ้าง

1.8 ผลกระทบด้านสังคม สุขภาพ ความปลอดภัย กฎหมาย และวัฒนธรรม

โครงงานนี้มุ่งเน้นการพัฒนาระบบตรวจจับความผิดปกติในระบบควบคุมอุตสาหกรรม (OT) ซึ่งมีผลกระทบในหลายมิติ ดังนี้

ด้านสังคม

การเพิ่มประสิทธิภาพในการตรวจจับและป้องกันการโจมตีไซเบอร์ในระบบอุตสาหกรรม สามารถลดความเสี่ยงของเหตุการณ์ที่อาจกระทบต่อประชาชน เช่น การปนเปื้อนของระบบน้ำในกรณีศึกษา SWaT dataset หรือการหยุดชะงักของการให้บริการสาธารณะ ซึ่งมีผลโดยตรงต่อคุณภาพชีวิตของสังคม

ด้านสุขภาพและความปลอดภัย

ระบบ OT ที่ถูกรุกรานสามารถส่งผลกระทบต่อความปลอดภัยของพนักงานและชุมชนโดยรอบ เช่น การทำงานผิดพลาดของปั๊ม วาล์ว หรือเซนเซอร์ในกระบวนการผลิตน้ำ หากตรวจจับและตอบสนองได้เร็ว จะช่วยลดความเสี่ยงต่ออุบัติเหตุและผลกระทบต่อสุขภาพของผู้บริโภคและผู้ปฏิบัติงาน

ด้านกฎหมายและมาตรฐาน

อุตสาหกรรมสมัยใหม่ต้องสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Regulations) และมาตรฐานสากล เช่น IEC 62443 และ ISO/IEC 27001 การพัฒนาโครงงานนี้ช่วยสร้างแนวทางที่สอดคล้องกับข้อกำหนดดังกล่าว และสามารถนำไปปรับใช้เพื่อตอบสนองต่อกฎหมายและมาตรการควบคุมของหน่วยงานที่เกี่ยวข้อง

ด้านวัฒนธรรมองค์กร

การนำเทคโนโลยี Machine Learning มาปรับใช้กับระบบ OT ช่วยเสริมสร้างวัฒนธรรมด้าน ความตระหนักรู้ทางไซเบอร์ (Cybersecurity Awareness) ในองค์กร ส่งเสริมให้ผู้ปฏิบัติงานและผู้บริหารเห็นความสำคัญของความปลอดภัยเชิงข้อมูลควบคู่ไปกับความปลอดภัยเชิงกายภาพ

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

การทำโครงงาน เริ่มต้นด้วยการศึกษาค้นคว้า ทฤษฎีที่เกี่ยวข้อง หรือ งานวิจัย/โครงงาน ที่เคยมีผู้นำเสนอไว้แล้ว ซึ่งเนื้อหาในบทนี้ก็จะเกี่ยวกับการอธิบายถึงสิ่งที่เกี่ยวข้องกับโครงงาน เพื่อให้ผู้อ่านเข้าใจเนื้อหาในบทถัดๆ ไปได้ง่ายขึ้น

2.1 Operational Technology (OT) และ Industrial Control Systems (ICS)

Operational Technology (OT) คือเทคโนโลยีที่ใช้สำหรับตรวจสอบและควบคุมกระบวนการทางกายภาพในโรงงานอุตสาหกรรมหรือโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบไฟฟ้า ระบบน้ำมัน และระบบบำบัดน้ำเสีย จุดเด่นของ OT คือการทำงานที่ต้องเน้น ความต่อเนื่อง ความเสถียร และความปลอดภัย มากกว่า IT (Information Technology) ที่มุ่งเน้นการประมวลผลข้อมูลและธุรกรรมเป็นหลัก

Industrial Control Systems (ICS) เป็นกลุ่มของระบบที่ใช้ควบคุมและจัดการการทำงานของ OT โดยมีตัวอย่างที่สำคัญ ได้แก่

1. Supervisory Control and Data Acquisition (SCADA) ใช้สำหรับควบคุมและตรวจสอบระบบขนาดใหญ่ที่กระจายตัว
2. Distributed Control System (DCS) ใช้ควบคุมกระบวนการแบบต่อเนื่อง เช่น โรงกลั่นน้ำมัน
3. Programmable Logic Controller (PLC) ใช้ในกระบวนการที่ต้องการการควบคุมแบบเฉพาะกิจ

2.2 ความมั่นคงปลอดภัยไซเบอร์ในระบบ OT/ICS

ระบบ ICS เดิมถูกออกแบบมาเพื่อเน้นความทนทานและการทำงานอย่างต่อเนื่อง โดยไม่ได้คำนึงถึงการป้องกันภัยไซเบอร์ ทำให้มีช่องโหว่ต่อการโจมตี เช่น:

1. Stuxnet (2010): มัลแวร์ที่แทรกแซงการทำงานของ PLC ในโรงงานนิวเคลียร์อิหร่าน
2. Ukraine Power Grid Attack (2015): การโจมตีระบบไฟฟ้าทำให้เกิดการดับไฟในวงกว้าง

กรณีศึกษาดังกล่าวสะท้อนว่าภัยคุกคามไซเบอร์สามารถสร้างความเสียหายทั้งด้านเศรษฐกิจ ความมั่นคง และความปลอดภัยของประชาชน การพัฒนา ระบบตรวจจับความผิดปกติ (Anomaly Detection) จึงมีความสำคัญอย่างยิ่งใน OT

2.2.1 Anomaly Detection

Anomaly Detection คือกระบวนการระบุข้อมูลที่เบี่ยงเบนไปจากรูปแบบปกติ ซึ่งอาจเกิดจากการโจมตี ความผิดพลาดของอุปกรณ์ หรือความผิดปกติของกระบวนการ โดยทั่วไปแบ่งได้เป็น 3 ประเภท:

1. Point Anomaly: ข้อมูลจุดเดียวที่ผิดปกติ (เช่น ค่า Sensor พุ่งสูงกว่าปกติ)
2. Contextual Anomaly: ข้อมูลที่ปกติในบางบริบท แต่ผิดปกติในอีกบริบทหนึ่ง (เช่น ค่าน้ำสูงในฤดูฝนเป็นเรื่องปกติ แต่สูงในฤดูแล้งถือว่าผิดปกติ)

3. Collective Anomaly: ลำดับข้อมูลหลายจุดที่รวมกันแล้วผิดปกติ (เช่น การทำงานของ Pump และ Valve ที่ไม่สัมพันธ์กัน)

สำหรับระบบ ICS Collective Anomaly มีความสำคัญมาก เนื่องจากข้อมูลจาก Sensor และ Actuator อยู่ในรูปแบบ Time-Series ที่ต้องพิจารณาลำดับเวลา

2.3 Secure Water Treatment (SWaT) Dataset

Secure Water Treatment (SWaT) Dataset เป็นชุดข้อมูลที่สร้างขึ้นจากโรงงานจำลองระบบบำบัดน้ำ (Water Treatment Testbed) โดย iTrust Lab, Singapore University of Technology and Design (SUTD) มีวัตถุประสงค์เพื่อใช้เป็น มาตรฐานกลาง (benchmark) สำหรับการวิจัยด้านความปลอดภัยไซเบอร์ในระบบควบคุมอุตสาหกรรม (ICS/SCADA)

โครงสร้างของระบบ SWaT

โรงงานจำลอง SWaT ออกแบบให้มีลักษณะใกล้เคียงโรงงานจริง โดยแบ่งออกเป็น 6 กระบวนการย่อย (Processes/Stages):

1. P1: Raw Water Supply – ระบบสูบน้ำดิบเข้าสู่ถังเก็บ
2. P2: Pre-treatment – การกรองเบื้องต้น (Ultrafiltration)
3. P3: Chemical Dosing – การเติมสารเคมี เช่น กรด-ด่าง เพื่อปรับค่า pH
4. P4: Membrane-based Ultra-Filtration – การกรองละเอียดด้วยเมมเบรน
5. P5: Dechlorination – การกำจัดคลอรีนที่เหลืออยู่
6. P6: Backwash and Product Storage – การล้างย้อนและการเก็บน้ำสะอาดในถังเก็บสุดท้าย

ในแต่ละกระบวนการจะมีการติดตั้ง เซนเซอร์ (sensors) และ แอกชูเอเตอร์ (actuators) เช่น ปั๊ม (pumps), วาล์ว (valves), และเครื่องวัดระดับน้ำ (level sensors) ซึ่งควบคุมด้วย PLC (Programmable Logic Controllers) และเฝ้าติดตามผ่านระบบ SCADA

ประเภทตัวแปรใน Dataset

ข้อมูลที่บันทึกจาก SWaT เป็น Time-Series รายวินาที (1 sample/second) ครอบคลุมช่วงเวลา 11 วัน รวม 946,722 records และ 51 attributes

ข้อมูลทางกายภาพ (Physical Properties)

1. Sensors (ตัวแปรต่อเนื่อง)
   (a) Flow (อัตราการไหล)
   (b) Level (ระดับน้ำ)
   (c) Pressure (ความดัน)

(d) Conductivity (ค่าการนำไฟฟ้า)

(e) pH (กรด-ด่าง)

(f) ORP (Oxidation-Reduction Potential)

(g) Temperature (อุณหภูมิ)

2. Actuators (ตัวแปรไม่ต่อเนื่อง)

(a) ปั๊ม (Pumps – เปิด/ปิด)

(b) วาล์ว (Motorized Valves – เปิด/ปิด)

(c) Dosing Pumps (สำหรับจ่ายสารเคมี)

สถานการณ์การโจมตี (Attack Scenarios)

ในการทดลอง มีการออกแบบการโจมตีทั้งหมด 36 รูปแบบ แบ่งเป็น:

1. Single Stage Single Point (SSSP) – โจมตีจุดเดียวในกระบวนการเดียว (26 ครั้ง)
2. Single Stage Multi Point (SSMP) – โจมตีหลายจุดในกระบวนการเดียว (4 ครั้ง)
3. Multi Stage Single Point (MSSP) – โจมตี 1 จุด แต่มีผลกระทบหลายกระบวนการ (2 ครั้ง)
4. Multi Stage Multi Point (MSMP) – โจมตีหลายจุดในหลายกระบวนการ (4 ครั้ง)

ตัวอย่าง:

1. ปลอมค่าจาก LIT101 (Level Sensor) ทำให้ระบบเข้าใจผิดว่าน้ำเต็มถัง และสั่งหยุดปั๊ม ส่งผลให้น้ำล้น (Overflow)
2. ปลอมค่าจาก LIT301 ให้แสดงค่าสูงผิดปกติ ส่งผลให้ปั๊มทำงานต่อแม้น้ำหมด และเกิด Underflow และอาจทำให้ปั๊มเสียหาย

2.4 Machine Learning

Machine Learning (ML) เป็นแขนงหนึ่งของปัญญาประดิษฐ์ (Artificial Intelligence: AI) ที่ช่วยให้ระบบสามารถเรียนรู้และปรับปรุงประสิทธิภาพจากข้อมูล โดยไม่ต้องเขียนกฎแบบตายตัวล่วงหน้า การป้อนข้อมูลจำนวนมากที่หลากหลายช่วยให้โมเดลสามารถสกัดรูปแบบ (patterns) และปรับปรุงความแม่นยำได้อย่างต่อเนื่อง

สำหรับโครงการนี้ ML ถูกนำมาใช้ในการตรวจจับความผิดปกติ (Anomaly Detection) ใน ข้อมูลเชิงเวลา (time-series) ที่ได้จาก ระบบควบคุมอุตสาหกรรม (ICS/OT) ซึ่งประกอบด้วยเซนเซอร์และแอกชูเอเตอร์ในระบบบำบัดน้ำ (SWaT dataset)

2.5 Convolutional Neural Network – Long Short-Term Memory (CNN-LSTM)

การตรวจจับความผิดปกติในข้อมูลเชิงเวลา (time-series anomaly detection) จำเป็นต้องอาศัยโมเดลที่สามารถสกัดคุณลักษณะเชิงลึกและในขณะเดียวกันต้องเข้าใจความสัมพันธ์เชิงลำดับเวลา โมเดล CNN-LSTM จึงถูกนำมาใช้เพราะผสานข้อดีของ Convolutional Neural Network (CNN) และ Long Short-Term Memory (LSTM) เข้าด้วยกัน ทำให้สามารถจัดการกับข้อมูลจากระบบควบคุมอุตสาหกรรม (ICS) ที่มีความซับซ้อนสูงได้อย่างมีประสิทธิภาพ โดยเฉพาะข้อมูลจาก SWaT dataset ซึ่งประกอบด้วยข้อมูลจาก sensor และ actuator ที่บันทึกเป็นลำดับเวลา

2.5.1 Convolutional Neural Network (CNN)

CNN เป็นโครงข่ายประสาทเทียมที่พัฒนาขึ้นเพื่อตรวจจับและสกัดคุณลักษณะสำคัญจากข้อมูล โดยอาศัยการทำงานของ convolution filters ที่เลื่อนผ่านข้อมูลเพื่อค้นหารูปแบบซ้ำหรือความเปลี่ยนแปลงที่มีนัยสำคัญ ในบริบทของข้อมูลเชิงเวลา CNN สามารถทำหน้าที่ตรวจสอบการเปลี่ยนแปลงของค่า sensor ในช่วงสั้น ๆ ได้อย่างมีประสิทธิภาพ เช่น การแกว่งของระดับน้ำหรือการเปลี่ยนแปลงค่าความดันอย่างเฉียบพลัน นอกจากนี้ CNN ยังช่วยลดสัญญาณรบกวน (noise) และเน้นคุณลักษณะที่บ่งบอกถึงความผิดปกติได้อย่างชัดเจน

2.5.2 Long Short-Term Memory (LSTM)

LSTM เป็นโครงข่ายประสาทเทียมแบบ Recurrent Neural Network (RNN) ที่ถูกออกแบบมาเพื่อแก้ไขข้อจำกัดด้านการจำข้อมูลระยะยาวของ RNN ทั่วไป โดยใช้โครงสร้างที่มีกลไกสำคัญคือ forget gate, input gate และ output gate เพื่อกำหนดว่าข้อมูลใดควรถูกเก็บรักษาไว้และข้อมูลใดควรถูกลืมไป ทำให้ LSTM สามารถเรียนรู้ความสัมพันธ์ที่ซับซ้อนและยาวนานของข้อมูลเชิงเวลาได้อย่างมีประสิทธิภาพ สำหรับข้อมูลจาก SWaT dataset LSTM สามารถตรวจสอบความเชื่อมโยงของ sensor และ actuator ที่ทำงานต่อเนื่องหลายขั้นตอน เช่น ลำดับการเปิดปิดของปั๊มและวาล์ว ซึ่งอาจเป็นปัจจัยสำคัญที่ทำให้เกิดความผิดปกติในกระบวนการ

2.5.3 CNN-LSTM for Anomaly Detection

การผสมผสาน CNN และ LSTM เข้าไว้ด้วยกันในโมเดล CNN-LSTM ทำให้สามารถใช้ CNN ในการสกัดคุณลักษณะสำคัญจากข้อมูลเชิงเวลาในช่วงสั้น แล้วส่งผลลัพธ์ต่อให้ LSTM เพื่อเรียนรู้ความสัมพันธ์ที่ต่อเนื่องในระยะยาว แนวทางนี้ช่วยให้โมเดลสามารถจับพฤติกรรมผิดปกติที่ซับซ้อนในระบบ ICS ได้ดียิ่งขึ้น เมื่อเปรียบเทียบกับการใช้ CNN หรือ LSTM เพียงอย่างเดียว งานวิจัยจำนวนมากยืนยันว่าโมเดล CNN-LSTM มีประสิทธิภาพในการลดอัตราการตรวจจับผิดพลาด (false positives) และเพิ่มความแม่นยำในการตรวจจับ anomaly ได้ โดยเฉพาะอย่างยิ่งเมื่อใช้กับข้อมูลที่มีลักษณะ time-series แบบหลายตัวแปร (multivariate time-series) เช่นใน SWaT dataset

2.5.4 Dense Layer และ Fully Connected Layer

หลังจากที่ CNN และ LSTM ทำหน้าที่สกัดคุณลักษณะและจับความสัมพันธ์เชิงเวลาแล้ว ผลลัพธ์ที่ได้จะถูกส่งต่อไปยัง Dense Layer หรือ Fully Connected Layer เพื่อทำการรวมข้อมูลและสร้างการ

ตัดสินใจสุดท้าย Dense Layer ทำงานโดยเชื่อมต่อทุกนิวรอนกับนิวรอนในชั้นถัดไป ช่วยให้โมเดลสามารถเรียนรู้การรวมคุณลักษณะที่ซับซ้อนและสร้างการจำแนก (classification) ระหว่างเหตุการณ์ปกติและเหตุการณ์ผิดปกติได้อย่างมีประสิทธิภาพ ในโครงการนี้ Dense Layer ทำหน้าที่แปลง representation ที่ได้จาก CNN-LSTM ให้กลายเป็นค่าความน่าจะเป็น (probability) ของ class เช่น Normal (0) และ Anomaly (1)

2.5.5 Activation Functions

ฟังก์ชันกระตุ้น (Activation Functions) เป็นองค์ประกอบสำคัญของ Dense Layer ซึ่งใช้ในการกำหนดเส้นแบ่งเชิงเส้นหรือไม่เชิงเส้น เช่น:

1. ReLU (Rectified Linear Unit): ใช้ในชั้นซ่อน (hidden layers) ของ CNN และ LSTM เพื่อลดปัญหา vanishing gradient และเร่งการเรียนรู้
2. Sigmoid: เหมาะกับการจำแนกแบบ binary anomaly detection เนื่องจากผลลัพธ์อยู่ระหว่าง 0–1
3. Softmax: ใช้สำหรับ multi-class anomaly detection เมื่อมีความผิดปกติหลายประเภท

2.5.6 Regularization Layers (Dropout และ Batch Normalization)

เพื่อป้องกันการเกิด overfitting จากข้อมูลที่มีความซับซ้อนสูง เช่น SWaT dataset การเพิ่ม Regularization Layers มีความสำคัญมาก ได้แก่:

1. Dropout Layer: ทำการสุ่มปิดบางนิวรอนระหว่างการฝึก เพื่อป้องกันไม่ให้โมเดลจดจำข้อมูลมากเกินไป แต่ช่วยให้เกิดการเรียนรู้ที่ครอบคลุมมากขึ้น
2. Batch Normalization: ช่วยปรับค่าการกระจายของข้อมูลในแต่ละชั้นให้อยู่ในช่วงที่เหมาะสม ทำให้การฝึกโมเดลเสถียรและรวดเร็วขึ้น

2.6 Correlation Matrix

Correlation Matrix เป็นเครื่องมือเชิงสถิติที่ใช้วิเคราะห์ความสัมพันธ์ระหว่างตัวแปรหลายตัวพร้อมกัน โดยจะแสดงค่า Correlation Coefficient ที่มีค่าตั้งแต่ -1 ถึง 1

1. ค่า 1 หมายถึงความสัมพันธ์เชิงบวกอย่างสมบูรณ์ (เมื่อค่าของตัวแปรหนึ่งเพิ่ม อีกตัวก็เพิ่มตาม)
2. ค่า -1 หมายถึงความสัมพันธ์เชิงลบอย่างสมบูรณ์ (เมื่อค่าของตัวแปรหนึ่งเพิ่ม อีกตัวจะลดลง)
3. ค่า 0 หมายถึงไม่มีความสัมพันธ์

สำหรับ SWaT dataset การสร้าง Correlation Matrix มีความสำคัญในหลายประเด็น ได้แก่

1. การทำความเข้าใจความสัมพันธ์ของ Sensor และ Actuator: เช่น ระดับน้ำ (Level) ควรมีความสัมพันธ์กับการทำงานของปั๊ม (Pump) และวาล์ว (Valve)
2. การตรวจหาความผิดปกติ (Anomaly): หาก correlation ระหว่าง sensor และ actuator ไม่เป็นไปตามปกติ เช่น ค่า Flow ไม่สัมพันธ์กับการเปิดปิด Valve อาจบ่งชี้ถึงการโจมตีหรือความผิดปกติในกระบวนการ

3. Feature Selection: การวิเคราะห์ความสัมพันธ์ช่วยคัดเลือกตัวแปรที่สำคัญ และลด multicollinearity เพื่อลด noise ก่อนนำเข้าสู่โมเดล Machine Learning

การใช้ Correlation Matrix จึงเป็นขั้นตอนสำคัญใน Exploratory Data Analysis (EDA) ของโครงการนี้ เพื่อทำให้การออกแบบและฝึกสอนโมเดล anomaly detection มีความถูกต้องและแม่นยำมากขึ้น

2.7 Model Evaluation

การประเมินผลลัพธ์ของโมเดลมีความสำคัญอย่างยิ่ง เนื่องจากเป็นวิธีการตรวจสอบความถูกต้องและความน่าเชื่อถือของโมเดลในการตรวจจับความผิดปกติจากข้อมูลจริง โดยเฉพาะอย่างยิ่งในกรณีของ SWaT dataset ซึ่งมีลักษณะข้อมูล ไม่สมดุล (imbalanced data) กล่าวคือ ข้อมูลเหตุการณ์ปกติ (Normal) มีจำนวนมากกว่าข้อมูลเหตุการณ์ผิดปกติ (Anomaly) อย่างมาก การใช้ตัวชี้วัด (Evaluation Metrics) ที่เหมาะสมจึงมีบทบาทสำคัญในการสะท้อนศักยภาพของโมเดลได้อย่างครบถ้วน
ตัวชี้วัดที่ใช้ประกอบการประเมินในโครงการนี้ ได้แก่:

1. Accuracy
   เป็นสัดส่วนของจำนวนข้อมูลทั้งหมดที่โมเดลสามารถจำแนกได้ถูกต้อง แต่เนื่องจากข้อมูลมีความไม่สมดุล ค่าความแม่นยำ (accuracy) เพียงอย่างเดียวอาจไม่สะท้อนศักยภาพของโมเดลได้อย่างแท้จริง เพราะโมเดลที่ทำนายว่าข้อมูลเป็น “ปกติ” ตลอดเวลาอาจได้ค่า accuracy สูง แต่ไม่สามารถตรวจจับ anomaly ได้เลย
2. Precision
   เป็นตัวชี้วัดความถูกต้องของการทำนาย anomaly หมายถึง ในจำนวนทั้งหมดที่โมเดลทำนายว่า “ผิดปกติ” มีสัดส่วนเท่าใดที่เป็น anomaly จริง Precision ที่สูงบ่งชี้ว่าโมเดลสามารถลดการแจ้งเตือนผิดพลาด (False Positives) ได้
3. Recall (Sensitivity)
   เป็นตัวชี้วัดความสามารถของโมเดลในการตรวจจับ anomaly ได้ครบถ้วน หมายถึงในจำนวน anomaly ทั้งหมดที่มีอยู่โมเดลสามารถตรวจพบได้กี่กรณี Recall จึงมีความสำคัญอย่างยิ่งในงาน ICS/OT anomaly detection เพราะการพลาดการตรวจจับ anomaly เพียงเล็กน้อยอาจก่อให้เกิดผลกระทบต่อความปลอดภัยและการดำเนินงานของระบบ
4. F1-score
   เป็นค่าเฉลี่ยเชิงฮาร์โมนิก (Harmonic Mean) ระหว่าง Precision และ Recall ทำให้สะท้อนสมดุลระหว่างการลดการแจ้งเตือนผิดพลาดและการเพิ่มอัตราการตรวจจับ anomaly ได้อย่างเหมาะสม โดยเฉพาะอย่างยิ่งใน dataset ที่มี class imbalance
5. Confusion Matrix
   เป็นตารางที่แสดงการจำแนกผลลัพธ์ของโมเดลอย่างละเอียดในรูปของ True Positive (TP), True Negative (TN), False Positive (FP) และ False Negative (FN) ช่วยให้สามารถวิเคราะห์ข้อผิดพลาดของโมเดลได้เชิงลึก และชี้ชัดว่าปัญหาของโมเดลอยู่ที่การตรวจจับ anomaly ไม่เพียงพอ (Recall ต่ำ) หรือการแจ้งเตือนผิดพลาดสูง (Precision ต่ำ)

6. ROC-AUC (Receiver Operating Characteristic – Area Under Curve)
   เป็นการประเมินสมรรถนะของโมเดลโดยไม่ขึ้นกับ threshold โดยใช้ค่า True Positive Rate และ False Positive Rate มาวิเคราะห์เส้นโค้ง (ROC Curve) ค่า AUC ที่สูงใกล้ 1 บ่งชี้ว่าโมเดลสามารถจำแนก anomaly ออกจาก normal ได้อย่างมีประสิทธิภาพ

7. PR-AUC (Precision-Recall Area Under Curve)
   เป็นการวัดสมรรถนะที่เหมาะสมอย่างยิ่งสำหรับข้อมูลที่ไม่สมดุล (imbalanced dataset) โดยแสดงความสัมพันธ์ระหว่าง Precision และ Recall ตลอดทุก threshold ค่าที่สูงใกล้ 1 แสดงว่าโมเดลมีความสามารถในการตรวจจับ anomaly ได้ดีแม้ในสภาพที่ anomaly มีสัดส่วนค่อนข้างน้อย

บทที่ 3
โครงสร้างและขั้นตอนการทำงาน

3.1 โครงสร้างทางสถาปัตยกรรม

รูปที่ 3.1: The Walrus and the Carpenter

3.2 การเตรียมข้อมูล (Data Preparation)

3.2.1 การโหลดและอ่านชุดข้อมูล (Data Loading)

ขั้นตอนแรกคือการนำเข้าชุดข้อมูลที่ใช้สำหรับการทดลอง SWaT Dataset ซึ่งเป็นข้อมูลการทำงานของระบบน้ำในอุตสาหกรรมที่บันทึกค่า sensor และ actuator ในรูปแบบ time-series การโหลดข้อมูลอาจใช้เครื่องมืออย่าง Pandas เพื่ออ่านไฟล์ .csv แล้วจัดเก็บให้อยู่ในรูปแบบ DataFrame เพื่อให้สามารถจัดการได้สะดวกในขั้นตอนถัดไป

3.2.2 การจัดการค่าที่หายไป (Missing Value Handling)

ข้อมูลที่ได้จากระบบ OT/ICS มักมีปัญหาค่าที่หายไป (missing values) อันเนื่องมาจากปัญหาของ sensor หรือการบันทึกข้อมูล การจัดการอาจทำได้หลายวิธี เช่น

1. การลบข้อมูลแถวที่หายไป (listwise deletion)
2. การแทนค่าด้วยสถิติพื้นฐาน (เช่น ค่าเฉลี่ย ค่ามัธยฐาน)
3. การแทนค่าด้วยการคำนวณจากข้อมูลรอบข้าง เช่น interpolation ในกรณีข้อมูลเชิงเวลา

3.2.3 การแยกประเภทคุณลักษณะ (Continuous / Discrete Features)

ชุดข้อมูลมักประกอบด้วยคุณลักษณะหลายประเภท เช่น

1. Continuous features: ค่าเซนเซอร์ เช่น ความดัน, อัตราการไหล
2. Discrete features: ค่าสถานะ actuator เช่น เปิด/ปิดวาล์ว, เปิด/ปิดปั๊ม
   การแยกประเภทคุณลักษณะมีความสำคัญเพราะวิธี preprocessing อาจแตกต่างกัน เช่น continuous ต้อง scaling แต่ discrete อาจใช้ encoding

3.2.4 การปรับสเกลข้อมูล (Scaling and Normalization)

ค่าของเซนเซอร์บางตัวอาจอยู่ในช่วงที่ต่างกันมาก เช่น อุณหภูมิ (0–100) กับค่าแรงดัน (0–10,000) หากไม่ปรับสเกล อาจทำให้โมเดลให้ความสำคัญกับตัวแปรที่มีค่ามากเกินไป โดยใช้วิธี

Min-Max Scaling (ปรับให้อยู่ในช่วง [0,1])

3.2.5 การแบ่งชุดข้อมูล (Training / Testing Split)

เพื่อป้องกันการ overfitting ต้องแบ่งข้อมูลออกเป็น training set และ testing set เช่น 70/30 หรือ 80/20 ในงาน time-series อาจต้องใช้ sliding window ในการแบ่ง โดยไม่ทำการ shuffle ข้อมูล เพื่อคงลำดับเวลาให้ถูกต้อง

3.3 การทำ Feature Engineering

3.3.1 การเลือกคุณลักษณะที่เกี่ยวข้อง (Feature Selection)

ไม่ใช่ทุกคุณลักษณะมีความสำคัญต่อการตรวจจับ anomaly การใช้ feature selection จะช่วยลดมิติของข้อมูลและปรับปรุงประสิทธิภาพโมเดล เทคนิคที่ใช้เช่น

1. การวิเคราะห์ Correlation Matrix
2. การใช้ Mutual Information
3. การใช้ Model-based feature selection เช่น Random Forest

3.3.2 การใช้ Sliding Window กับ Time-series Data

เนื่องจากข้อมูล ICS/OT เป็น time-series จำเป็นต้องแปลงข้อมูลให้อยู่ในรูป window-based input เช่น สร้าง sequence ขนาด 30 หรือ 60 วินาที เพื่อใช้ในการเรียนรู้ pattern ของระบบ วิธีนี้ช่วยให้โมเดล CNN/LSTM สามารถตรวจจับลักษณะของ anomaly ที่เกิดขึ้นในช่วงเวลาได้

3.3.3 การสร้างคุณลักษณะใหม่ (Derived Features)

สามารถสร้าง feature เพิ่มเติมจากข้อมูลดิบ เช่น

1. ค่า moving average ของเซนเซอร์
2. ค่าความแตกต่างระหว่างเวลา (Δt)
3. อัตราการเปลี่ยนแปลง (derivatives)
   สิ่งเหล่านี้ช่วยให้โมเดลจับความผิดปกติได้ดีกว่าการใช้ข้อมูลดิบเพียงอย่างเดียว

3.3.4 การตรวจสอบความสัมพันธ์ของคุณลักษณะ (Correlation Analysis)

การวิเคราะห์ความสัมพันธ์ระหว่าง features เช่น การคำนวณ Pearson Correlation หรือ Spearman Rank Correlation เพื่อดูว่าคุณลักษณะใดสัมพันธ์กันมากเกินไป หาก correlation สูง อาจเลือกตัดบาง feature ทิ้งเพื่อลด redundancy

3.4 การออกแบบและพัฒนาโมเดล (Model Design and Development)

3.4.1 การเลือกโมเดลต้นแบบ (CNN Prototype)

เลือกใช้ Convolutional Neural Network (CNN) เพราะสามารถจับ pattern ในข้อมูล time-series ได้คล้ายกับการประมวลผลภาพ โดยมองว่าแต่ละ sequence เป็น “สัญญาณหลายมิติ” จาก sensor และ actuator

3.4.2 สถาปัตยกรรมของโมเดล (Model Architecture)

Input Layer: รับข้อมูล time-series ที่ผ่าน preprocessing แล้ว

1. Input Layer: รับข้อมูล time-series ที่ผ่าน preprocessing แล้ว
2. Convolutional Layer: ดึง pattern ที่ซ่อนอยู่จากข้อมูล เช่น ความเปลี่ยนแปลงของ sensor
3. Pooling Layer: ลดมิติและ noise ทำให้โมเดล generalize ได้ดีขึ้น
4. Fully Connected Layer: รวม feature ที่สกัดมาเพื่อใช้ในการจำแนก anomaly
5. Output Layer: ใช้ softmax/sigmoid เพื่อตัดสินว่าเป็น “ปกติ” หรือ “ผิดปกติ”

3.4.3 การตั้งค่า Hyperparameters

กำหนดค่าเช่น learning rate, batch size, จำนวน epoch, จำนวน filter และ kernel size ใน CNN การเลือกค่าเหล่านี้มีผลโดยตรงต่อความแม่นยำและความเร็วของการเรียนรู้

3.4.4 เครื่องมือและ Framework ที่ใช้ (เช่น TensorFlow / PyTorch)

เช่น TensorFlow, PyTorch, Scikit-learn ใช้ร่วมกับ Google Colab (GPU) เพื่อประมวลผลได้เร็วขึ้น

3.5 การทดสอบและประเมินผล (Experiment and Evaluation)

3.5.1 วิธีการแบ่งชุดข้อมูลสำหรับทดสอบ (Train/Test Strategy)

ใช้ hold-out method (train/test split) หรือ cross-validation สำหรับ time-series อาจใช้ walk-forward validation เพื่อเลียนแบบสถานการณ์จริง

3.5.2 ตัวชี้วัดประสิทธิภาพ (Evaluation Metrics)

1. Accuracy: วัดความถูกต้องโดยรวม
2. Precision, Recall, F1-score: วัดความสามารถในการตรวจจับ anomaly โดยไม่แจ้งเตือนผิดพลาด
3. Detection Rate (DR), False Alarm Rate (FAR): เน้นการประเมินประสิทธิภาพในการตรวจจับโจมตีและลด false positive

3.6 การประยุกต์ใช้งานและข้อจำกัด (Application and Limitations)

3.6.1 ศักยภาพในการนำไปใช้จริง (Practical Applications)

ระบบที่พัฒนาสามารถนำไปใช้ใน โรงงานอุตสาหกรรม เพื่อช่วยตรวจจับพฤติกรรมผิดปกติของเซน-เซอร์หรือ อุปกรณ์ เช่น การโจมตีปั๊มน้ำ หรือการเปิดวาล์วโดยไม่ได้รับอนุญาต

3.6.2 ข้อจำกัดของโครงงาน (Limitations)

1. ใช้ข้อมูลจำลอง (SWaT dataset) แทนข้อมูลจริง
2. ทดสอบในสภาพแวดล้อมจำกัด ไม่ครอบคลุมทุกประเภทของการโจมตี
3. ความแม่นยำอาจลดลงหากนำไปใช้กับ dataset อื่นที่มีลักษณะแตกต่าง

3.6.3 แนวทางการพัฒนาในอนาคต (Future Work)

1. ทดลองใช้โมเดล Hybrid (CNN+LSTM)
2. นำ model ไปใช้ในการทำระบบเตือน โดยผ่าน API หรือ Websocket

บทที่ 4
การทดลองและผลลัพธ์

ในบทนี้จะทดสอบเกี่ยวกับการทำงานในฟังก์ชันหลักๆ

4.1 Objective (วัตถุประสงค์การทดสอบ)

1. ตรวจสอบความสามารถของโมเดล CNN-LSTM ในการ แยกแยะสถานะ normal และ anomaly จาก SWaT dataset
2. วัดประสิทธิภาพของโมเดลตามตัวชี้วัดมาตรฐาน:
   (a) Precision, Recall, F1-score, AUC
   (b) Detection Delay และ Latency สำหรับการทดสอบแบบ real-time
3. ตรวจสอบ robustness ของโมเดลต่อ:
   (a) Noise (sensor fluctuation)
   (b) Missing data
   (c) Concept drift หรือ pattern ใหม่ที่ไม่เคยเห็น
4. เปรียบเทียบ performance กับ baseline models เช่น LSTM, CNN, Autoencoder

4.2 Requirements (ข้อกำหนดการทดสอบ)

4.2.1 Functional Requirements (ข้อกำหนดเชิงฟังก์ชัน)

1. โมเดลต้องสามารถจำแนก Normal vs Anomaly สำหรับข้อมูล time-series
2. สามารถแจ้งเตือน (Alert) เมื่อพบ anomaly ได้แบบ real-time หรือ batch
3. รองรับ input จาก sensor/actuator ตาม SWaT dataset
4. มี visualization/logging ของผลลัพธ์และ reconstruction error (ถ้ามี)

4.2.2 Non-Functional Requirements (ข้อกำหนดไม่เชิงฟังก์ชัน)

1. Accuracy: F1-score $\geq 85\%$ (ตัวอย่าง benchmark)
2. Latency: การทำนาย ≤ 20 ms ต่อ window (real-time)
3. Robustness: Performance degradation $\leq \geq 10\%$ เมื่อมี noise/missing data
4. Scalability: รองรับจำนวน sensor ≥ 50 และ batch size ≥ 64
5. Usability: รายงานผลลัพธ์ในรูปแบบตาราง/กราฟเข้าใจง่าย

4.2.3 Dataset Requirements

1. ใช้ SWaT dataset: Normal logs สำหรับ train, Normal + Attack logs สำหรับ test
2. แบ่งข้อมูลเป็น training/validation/test sets อย่างเหมาะสม
3. Preprocessing: normalization, windowing, imputation for missing data

4.3 Testing Strategy (กลยุทธ์การทดสอบ)

4.3.1 Types of Testing

1. Functional Testing:
   (a) ตรวจสอบว่าโมเดลสามารถระบุ anomaly ใน test set ได้ถูกต้อง
   (b) ตรวจสอบ alert system สำหรับ online detection
2. Performance Testing:
   (a) ประเมิน Precision, Recall, F1-score, AUC
   (b) วัด latency และ throughput
3. Robustness Testing:
   (a) เพิ่ม noise ในข้อมูล sensor
   (b) ลอง missing values (random drop)
   (c) ตรวจสอบ model performance ต่อ concept drift หรือ attack ใหม่
4. Comparison Testing:
   เปรียบเทียบกับ baseline models: LSTM, CNN, Autoencoder

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผล

นศ. ควรสรุปถึงข้อจำกัดของระบบในด้านต่างๆ ที่ระบบมีในเนื้อหาส่วนนี้ด้วย

5.2 ปัญหาที่พบและแนวทางการแก้ไข

ในการทำโครงงานนี้ พบว่าเกิดปัญหาหลักๆ ดังนี้

5.3 ข้อเสนอแนะและแนวทางการพัฒนาต่อ

ข้อเสนอแนะเพื่อพัฒนาโครงงานนี้ต่อไป มีดังนี้

บรรณานุกรม

ภาคผนวก

ภาคผนวก ก

The first appendix

Text for the first appendix goes here.

ก.1 Appendix section

Text for a section in the first appendix goes here.

test ทดสอบฟอนต์ serif ภาษาไทย

test ทดสอบฟอนต์ sans serif ภาษาไทย

`test ทดสอบฟอนต์ teletype ภาษาไทย`

test ทดสอบฟอนต์ teletype ภาษาไทย

ตัวหนา serif ภาษาไทย sans serif ภาษาไทย `teletype ภาษาไทย`

ตัวเอียง serif ภาษาไทย sans serif ภาษาไทย `teletype ภาษาไทย`

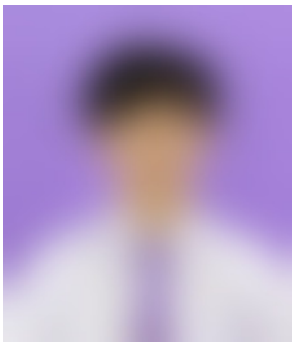
ตัวหนาเอียง serif ภาษาไทย sans serif ภาษาไทย `teletype ภาษาไทย`

https://www.example.com/test_ทดสอบ_url

ภาคผนวก ข
คู่มือการใช้งานระบบ

Manual goes here.

ประวัติผู้เขียน



Your biosketch goes here. Make sure it sits inside the `biosketch` environment.