



การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

นางสาวจิราวรรณ โคประโคน

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ครุศาสตร์อุตสาหกรรมมหาบัณฑิต
สาขาวิชาวิศวกรรมเครื่องกลศึกษา
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก



นางสาวจิราวรรณ โคประโคน

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
ครุศาสตร์อุตสาหกรรมมหาบัณฑิต
สาขาวิชาวิศวกรรมเครื่องกลศึกษา
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567
ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการ
ตรวจจับการบุกรุก

โดย นางสาวจิราวรรณ โคประโคน

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรครุศาสตรบัณฑิต
สาขาวิชาวิศวกรรมเครื่องกลศึกษา

คณบดีคณะครุศาสตรบัณฑิต

(รองศาสตราจารย์ ดร.สมศักดิ์ อรรคทิมากุล)

คณะกรรมการสอบการค้นคว้าอิสระ

ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.นิวัฒน์ ศรีสวัสดิ์)

อาจารย์ที่ปรึกษา

(รองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร)

กรรมการ

(รองศาสตราจารย์ ดร.สันติ หุตะมาน)

ชื่อ : นางสาวจิราวรรณ โคประโคน
ชื่อการค้นคว้าอิสระ : การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก
สาขาวิชา : วิศวกรรมเครื่องกลศึกษา
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : รองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร
ปีการศึกษา : 2567

บทคัดย่อ

ในยุคปัจจุบันเทคโนโลยีปัญญาประดิษฐ์ (AI) มีบทบาทสำคัญในระบบรักษาความปลอดภัย โดยเฉพาะในระบบตรวจจัดการบุกรุกที่ใช้ AI ในการวิเคราะห์ภาพและสัญญาณจากกล้องวงจรปิด และเซ็นเซอร์ต่าง ๆ ซึ่งช่วยเพิ่มความแม่นยำในการตรวจจับและลดความผิดพลาดจากการใช้มนุษย์ การศึกษาในระดับอาชีวศึกษาจึงจำเป็นต้องพัฒนาให้สอดคล้องกับความก้าวหน้าทางเทคโนโลยี AI เพื่อเตรียมความพร้อมให้กับนักเรียนที่ต้องการเข้าสู่อุตสาหกรรมที่เกี่ยวข้อง ปัญหาที่พบในปัจจุบัน คือการเรียนการสอนในระดับอาชีวศึกษาไม่สามารถนำเทคโนโลยี AI มาประยุกต์ใช้ได้อย่างเต็มที่ เนื่องจากขาดสื่อการเรียนรู้ที่เหมาะสมและขาดความเข้าใจในการใช้งาน AI ในระบบรักษาความปลอดภัย ส่งผลให้นักเรียนไม่สามารถพัฒนาทักษะที่จำเป็นในการทำงานในอุตสาหกรรมที่ต้องการเทคโนโลยีเหล่านี้ได้อย่างเต็มที่ งานวิจัยนี้มุ่งเน้นการพัฒนาชุดการเรียนรู้เชิงปฏิบัติที่ใช้ AI ในการตรวจจัดการบุกรุก เพื่อตรวจสอบผลสัมฤทธิ์ทางการเรียน ทักษะการปฏิบัติงาน และทัศนคติของผู้เรียน ผลการศึกษาพบว่าชุดการเรียนรู้ที่พัฒนาขึ้นสามารถทำงานได้อย่างมีประสิทธิภาพ โดยมีความแม่นยำสูงในสภาพแสงปกติ (94.74%) และมีความแม่นยำที่ยอมรับได้ในสภาพแสงน้อย (87.89%) นอกจากนี้ ระบบของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI แสดงให้เห็นถึงความสอดคล้องและเสถียรภาพในการทำงานตามที่ออกแบบไว้ ผลสัมฤทธิ์ทางด้านความรู้ของกลุ่มทดลองที่ใช้ชุดการเรียนรู้สูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$) เช่นเดียวกับทักษะการปฏิบัติงานและทัศนคติของผู้เรียนที่มีทัศนคติเชิงบวกต่อ AI มากขึ้น ซึ่งจะช่วยเสริมสร้างศักยภาพในการแข่งขันและเพิ่มโอกาสในการประกอบอาชีพในยุคที่เทคโนโลยีเป็นปัจจัยสำคัญในการขับเคลื่อนเศรษฐกิจและอุตสาหกรรมระดับโลก

(มีจำนวนทั้งสิ้น 112 หน้า)

คำสำคัญ : ปัญญาประดิษฐ์ในระบบรักษาความปลอดภัย, ชุดการเรียนรู้เชิงปฏิบัติ,
ระบบตรวจจัดการบุกรุก

อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Miss Jirawan Khoprakhon
Independent Study Title : Development of a Practical AI Security System
Learning Kit for Intrusion Detection.
Major Field : Mechanical Engineering Education
King Mongkut's University of Technology North
Bangkok
Independent Study Advisor : Associate Professor Dr. Suppachai Howimanporn
Academic Year : 2024

ABSTRACT

In the current era, artificial intelligence (AI) technology plays an important role in security systems, especially in intrusion detection systems that use AI to analyze images and signals from CCTV cameras and various sensors, which helps increase detection accuracy and reduce human errors. Therefore, vocational education must be developed in line with the advances in AI technology to prepare students who want to enter related industries. The current problem is that vocational education cannot fully apply AI technology due to the lack of appropriate learning media and a lack of understanding of the use of AI in security systems. As a result, students cannot fully develop the skills needed to work in industries that require these technologies. This research focuses on developing a practical learning kit that uses AI for intrusion detection to examine the learning achievements, work skills, and attitudes of learners. The study's results found that the developed learning kit can work efficiently with high accuracy in normal light conditions (94.74%) and acceptable accuracy in low light conditions (87.89%). In addition, the AI security practical learning kit system shows consistency and stability in its design. The knowledge achievement of the experimental group using the learning kit was significantly higher than the control group ($p < 0.05$), as were the learners' work skills and attitudes, which had a more positive attitude towards AI, which will help enhance their competitiveness and increase their career opportunities in an era where technology is a key factor driving the global economy and industry.

(Total 112 Pages)

Keywords: AI in Security Systems, Practical Learning Kit,
Intrusion detection systems.

Advisor

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยดีจากการเสียสละเวลาและอุทิศตนของ
รองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร อาจารย์ที่ปรึกษาสารนิพนธ์ และคำปรึกษาจาก
รองศาสตราจารย์ ดร.ศศิธร ชูแก้ว ในการให้ความรู้ คำปรึกษา คำแนะนำ ข้อคิดเห็นต่าง ๆ ที่เป็น
ประโยชน์ต่อการจัดทำสารนิพนธ์ด้วยความเอาใจใส่ ตลอดระยะเวลาของการวิจัย ทั้งในเวลา
ราชการ ณ คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ และ
นอกเวลาราชการ ณ สมาคมการศึกษาดิจิทัลและวิศวกรรมการเรียนรู้ ผู้วิจัยรู้สึกซาบซึ้งและขอ
กราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอกราบขอบพระคุณคณะผู้บริหาร คณะครูแผนกวิชาช่างอิเล็กทรอนิกส์วิทยาลัยเทคนิค
นครนายก ที่ให้การสนับสนุนในด้านสถานที่ วัสดุอุปกรณ์ และผู้เข้าร่วมการวิจัย เพื่อใช้ในการ
ดำเนินการวิจัย ผู้วิจัยขอกราบขอบพระคุณอย่างสูง

ขอกราบขอบพระคุณผู้เชี่ยวชาญและผู้ทรงคุณวุฒิทุกท่าน ที่ให้ความอนุเคราะห์
เสียสละเวลา ในการประเมินตรวจสอบเครื่องมือที่ใช้ในการวิจัย รวมถึงให้ข้อเสนอแนะที่เป็น
ประโยชน์ต่อการวิจัย ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูง

สุดท้ายนี้ ผู้วิจัยใคร่ขอกราบขอบพระคุณ นายประกอบ โคประโคน (บิดา)
นางเชียร โคประโคน (มารดา) ที่คอยสนับสนุนค่าลงทะเบียนเรียนในหลักสูตร
นางสาวขวัญสิริ กองประโคน ที่ให้การสนับสนุนที่พักรวมถึงให้กำลังใจตลอดระยะเวลาในการศึกษา
และผู้เกี่ยวข้องทุกท่าน ที่คอยให้ความช่วยเหลือ สนับสนุน และเป็นกำลังใจในการทำสารนิพนธ์
จนสำเร็จลุล่วงเป็นอย่างดี ผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

จิราวรรณ โคประโคน

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ข
บทคัดย่อภาษาอังกฤษ	ค
กิตติกรรมประกาศ	ง
สารบัญ	จ
สารบัญตาราง	ช
สารบัญรูปภาพ	ซ
บทที่ 1 บทนำ	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์ของการวิจัย	2
1.3 สมมติฐานในงานวิจัย	2
1.4 ขอบเขตของการวิจัย	2
1.5 นิยามศัพท์เฉพาะ	3
1.6 กรอบแนวคิดของการวิจัย	4
1.7 ประโยชน์ที่คาดว่าจะได้รับ	4
บทที่ 2 เอกสารและงานวิจัยที่เกี่ยวข้อง	5
2.1 แนวทางและหลักสูตรประกาศนียบัตรวิชาชีพ พ.ศ. 2567	5
2.2 ระบบตรวจจับการบุกรุกในสถานที่ (Intrusion Detection Systems - IDS)	7
2.3 การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence) ในระบบรักษาความปลอดภัย	8
2.4 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)	15
2.5 ชุดการเรียนรู้เชิงปฏิบัติ (Practical Learning Kits)	16
2.6 งานวิจัยที่เกี่ยวข้อง	17
บทที่ 3 วิธีดำเนินการวิจัย	19
3.1 การออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก	19
3.2 การสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย	21
3.3 ขั้นตอนเก็บข้อมูลการวิจัย	30
3.4 การวิเคราะห์ข้อมูลการวิจัย	34
บทที่ 4 ผลการวิจัย	37
4.1 ผลการสร้างชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก	37
4.2 ผลการเปรียบเทียบการประเมินด้านความรู้ก่อนเรียนและหลังเรียน	42
4.3 ผลการประเมินทักษะการปฏิบัติงาน	43

สารบัญ (ต่อ)

	หน้า
4.4 ผลการประเมินทัศนคติของผู้เรียนที่มีต่อการนำระบบรักษาความปลอดภัยด้วย ปัญญาประดิษฐ์ ในการตรวจจับการบุกรุกไปใช้งาน	43
4.5 ผลการประเมินความสอดคล้องที่มีต่อแบบประเมินทักษะและแบบประเมิน ทัศนคติจากผู้เชี่ยวชาญ	47
บทที่ 5 สรุป อภิปรายผล และข้อเสนอแนะ	50
5.1 สรุปผลการวิจัย	50
5.2 อภิปรายผล	50
5.3 ข้อเสนอแนะ	51
บรรณานุกรม	52
ภาคผนวก	56
ภาคผนวก ก	57
หนังสือขอความอนุเคราะห์เป็นผู้เชี่ยวชาญ	58
แบบประเมินความสอดคล้องที่มีต่อแบบประเมินความรู้ ทักษะ และ แบบประเมินทัศนคติของผู้เชี่ยวชาญ	63
ภาคผนวก ข	72
ตารางวิเคราะห์การจัดการเรียนรู้	73
แผนการจัดการเรียนรู้	75
แบบทดสอบวัดความรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย ปัญญาประดิษฐ์ในการตรวจจับการบุกรุก	79
ใบปฏิบัติงานและแบบบันทึกผลการประเมินเรื่องระบบรักษาความปลอดภัยที่ ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก	80
แบบสอบถามทัศนคติของผู้เรียนการนำระบบรักษาความปลอดภัยที่ขับเคลื่อน ด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน	88
คู่มือการใช้งาน	89
ภาคผนวก ค	90
หนังสือเชิญเข้าร่วมการประชุม	91
เกียรติบัตรเข้าร่วมนำเสนอบทความทางวิชาการ	92
เกียรติบัตรรางวัลของบทความทางวิชาการ	93
เอกสารเผยแพร่บทความทางวิชาการ	94
ภาคผนวก ง	99
ผลการวิเคราะห์ข้อมูลการวิจัยด้วยโปรแกรม IBM SPSS	100
ประวัติผู้เขียน	101

สารบัญตาราง

ตารางที่	หน้า
3-1 เป้าหมายการเรียนรู้ (Learning Objectives) ทั้งด้านความรู้ ทักษะ และทัศนคติ	20
3-2 อุปกรณ์ที่ใช้ใน Plant	23
3-3 ข้อมูลผู้เชี่ยวชาญในการประเมินความสอดคล้องของเครื่องมือ	29
3-4 โครงสร้างการวิจัย	34
4-1 ผลการทดสอบการทำงานของชุดการเรียนรู้เชิงปฏิบัติ	41
4-2 ผลการประเมินด้านความรู้ก่อนเรียนของกลุ่มทดลอง และกลุ่มควบคุม	42
4-3 ผลการประเมินด้านความรู้หลังเรียนของกลุ่มทดลอง และกลุ่มควบคุม	42
4-4 ผลการประเมินทักษะการปฏิบัติงานของผู้เรียน	43
4-5 ผลการประเมินทัศนคติของผู้เรียนกลุ่มทดลอง	44
4-6 ผลการประเมินทัศนคติของผู้เรียนกลุ่มควบคุม	45
4-7 ผลการเปรียบเทียบทัศนคติของผู้เรียนต่อการใช้ AI ในระบบรักษาความปลอดภัย ในกลุ่มทดลองและกลุ่มควบคุม	46
4-8 การประเมินค่าดัชนีความตรงเชิงเนื้อหา (IOC) สำหรับแบบทดสอบวัดความรู้	47
4-9 การประเมินค่าดัชนีความตรงเชิงเนื้อหา (IOC) สำหรับแบบประเมินทักษะ	48
4-10 การประเมินค่าดัชนีความตรงเชิงเนื้อหา (IOC) สำหรับแบบประเมินทัศนคติ	48

สารบัญรูปภาพ

ภาพที่	หน้า
1-1 กรอบแนวคิดการวิจัย	4
2-1 หลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567 สาขาวิชาอิเล็กทรอนิกส์	6
2-2 Convolutional Neural Network	9
2-3 การทำคอนโวลูชัน	10
2-4 ชั้นพูลลิงโดย Max Pooling และ Average Pooling	11
2-5 ชั้นการเชื่อมโยงเต็มรูปแบบ	11
2-6 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)	15
3-1 ขั้นตอนในออกแบบการออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก	19
3-2 การสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย	21
3-3 ขั้นตอนในสร้างชุดการเรียนรู้เชิงปฏิบัติ	22
3-4 Plant ชุดทดลองระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI ในการตรวจจับการบุกรุกขนาดเล็ก	24
3-5 PCB Layout	25
3-6 การประกอบชุดทดลองระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI ในการตรวจจับการบุกรุกขนาดเล็ก	26
3-7 ตัวอย่างโปรแกรมสำหรับตรวจจับการบุกรุก	27
3-8 คู่มือการใช้งาน	28
3-9 ขั้นตอนการสร้างเครื่องมือสำหรับประเมิน	29
3-10 ผังงานขั้นตอนในการเก็บข้อมูลการวิจัย	31
3-11 เก็บข้อมูลการวิจัยกับผู้เรียนกลุ่มทดลอง	33
3-12 ภาพบรรยากาศเก็บข้อมูลการวิจัย	33
3-13 กระบวนการในการวิเคราะห์ข้อมูลการวิจัย	34
4-1 ชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI ในการตรวจจับการบุกรุกขนาดเล็ก	37
4-2 การทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงปกติ	38
4-3 ผลทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงน้อย	39
4-4 ความสำเร็จในการติดตั้งฮาร์ดแวร์โดยผู้เรียน	39

สารบัญรูปภาพ (ต่อ)

ภาพที่	หน้า
4-5 การทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง	40
ก-1 หนังสือขอความอนุเคราะห์ ผศ. ดร.ปรกรณ์เกียรติ์ เศรษฐเมธิกุล เป็นผู้เชี่ยวชาญ	58
ก-2 หนังสือขอความอนุเคราะห์ ผศ.ชลดา ปานสง เป็นผู้เชี่ยวชาญ	59
ก-3 หนังสือขอความอนุเคราะห์ นายศุภกฤต รongam เป็นผู้เชี่ยวชาญ	60
ก-4 หนังสือขอความอนุเคราะห์ นางกฤษณา เอ็งฉุน เป็นผู้เชี่ยวชาญ	61
ก-5 หนังสือขอความอนุเคราะห์ นายยงยุทธ จันทรัตน์ เป็นผู้เชี่ยวชาญ	62
ข-1 แบบทดสอบวัดความรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก	79
ข-2 แบบสอบถามทัศนคติของผู้เรียน	88
ข-3 แบบสอบถามทัศนคติของผู้เรียนการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน	89
ค-1 หนังสือเชิญเข้าร่วมการประชุม	91
ค-2 เกียรติบัตรเข้าร่วมนำเสนอบทความทางวิชาการ	92
ค-3 เกียรติบัตรรางวัลของบทความทางวิชาการ	93
ง-1 ผลการวิเคราะห์ข้อมูลการวิจัยด้วยโปรแกรม IBM SPSS	100

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในยุคปัจจุบันเทคโนโลยีและปัญญาประดิษฐ์ (AI) มีบทบาทสำคัญในชีวิตประจำวัน หนึ่งในนั้นคือระบบรักษาความปลอดภัยทรัพย์สินและข้อมูล การนำ AI ใช้ในการตรวจจับการบุกรุกทำให้ระบบมีความแม่นยำและมีประสิทธิภาพสูงขึ้น การศึกษาในระดับอาชีวศึกษาจึงจำเป็นต้องปรับปรุงหลักสูตรและการเรียนการสอนให้สอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยี เพื่อให้นักเรียนมีทักษะและความรู้ที่ทันสมัย (Kwon & Park, 2022).

ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI ได้รับความนิยมเพิ่มมากขึ้นทั้งในภาคธุรกิจและที่อยู่อาศัย การตรวจจับการบุกรุกด้วย AI มีความสามารถในการวิเคราะห์ภาพจากกล้องวงจรปิดและสัญญาณอื่น ๆ ได้อย่างแม่นยำ ช่วยลดอัตราความผิดพลาดที่เกิดจากมนุษย์และเพิ่มความปลอดภัยให้กับสถานที่ที่มีการติดตั้งระบบดังกล่าว (Zhou et al., 2021).

การนำเทคโนโลยี AI มาใช้ในระบบรักษาความปลอดภัยจึงกลายเป็นทักษะที่สำคัญที่นักเรียนอาชีวศึกษาจำเป็นต้องมี การพัฒนาชุดการเรียนรู้เชิงปฏิบัติที่เน้นการใช้ AI ในการตรวจจับการบุกรุกจะช่วยให้นักเรียนมีความเข้าใจและสามารถนำความรู้ไปใช้ในทางปฏิบัติได้จริง ทำให้นักเรียนสามารถตอบสนองต่อความต้องการของตลาดแรงงานได้ดีขึ้น (Lee, 2020).

จากการศึกษาในหลักสูตรประกาศนียบัตรวิชาชีพ พ.ศ. 2567 สาขาอิเล็กทรอนิกส์ มีการระบุถึงความจำเป็นในการใช้เทคโนโลยีสมัยใหม่ในการเรียนการสอน รวมถึงการพัฒนาชุดการเรียนรู้เชิงปฏิบัติที่ตอบสนองต่อความต้องการของตลาดแรงงานและสถานประกอบการ หลักสูตรดังกล่าวเน้นให้ผู้เรียนมีความรู้และทักษะที่สามารถประยุกต์ใช้ได้จริงในการทำงาน (Ministry of Education, 2024).

ปัญหาที่พบในปัจจุบันคือการเรียนการสอนในระดับอาชีวศึกษายังไม่สามารถนำเทคโนโลยี AI มาประยุกต์ใช้ได้อย่างเต็มที่ เนื่องจากขาดสื่อการเรียนรู้ที่เหมาะสมและขาดความเข้าใจในการใช้งาน AI ในระบบรักษาความปลอดภัย ส่งผลให้นักเรียนไม่สามารถพัฒนาทักษะที่จำเป็นในการทำงานในอุตสาหกรรมที่ต้องการเทคโนโลยีเหล่านี้ได้อย่างเต็มที่ (Smith & Taylor, 2023).

การพัฒนาชุดการเรียนรู้เชิงปฏิบัติที่เน้นการใช้ AI ในการตรวจจับการบุกรุกจะช่วยเสริมสร้างทักษะและความรู้ให้กับนักเรียนอาชีวศึกษา โดยสามารถนำความรู้ที่ได้ไปประยุกต์ใช้ในสถานประกอบการจริงได้อย่างมีประสิทธิภาพ ซึ่งจะทำให้นักเรียนมีความพร้อมในการทำงานในสาขาอาชีพที่เกี่ยวข้องกับการรักษาความปลอดภัยและเทคโนโลยี AI (Johnson & Wong, 2023).

การวิจัยและพัฒนาชุดการเรียนรู้ดังกล่าวจำเป็นต้องคำนึงถึงการออกแบบเนื้อหาที่สามารถเข้าใจได้ง่ายและมีความน่าสนใจ รวมถึงการใช้เทคโนโลยีและอุปกรณ์ที่ทันสมัย เพื่อให้นักเรียนมีประสบการณ์ในการใช้งานจริงและสามารถนำไปประยุกต์ใช้ในอาชีพได้ ชุดการเรียนรู้ที่พัฒนาขึ้น

จะต้องสามารถนำไปใช้ในการเรียนการสอนและประยุกต์ใช้ในสถานประกอบการได้จริง (Chen & Liu, 2022).

ดังนั้นการพัฒนาชุดการเรียนรู้เชิงปฏิบัติที่ใช้ AI ในการตรวจจับการบุกรุกจะช่วยเสริมสร้างศักยภาพของนักเรียนอาชีวศึกษาในสาขาอิเล็กทรอนิกส์ให้มีความสามารถที่สอดคล้องกับความต้องการของตลาดแรงงาน ช่วยเพิ่มโอกาสในการประกอบอาชีพและส่งเสริมการพัฒนาประเทศในด้านเทคโนโลยีและนวัตกรรม การลงทุนในทรัพยากรมนุษย์จึงเป็นการส่งเสริมให้ประเทศสามารถพัฒนาต่อไปในอนาคตได้อย่างยั่งยืน (Nguyen & Tran, 2021)

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.2.2 เพื่อประเมินผลสัมฤทธิ์ด้านความรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.2.3 เพื่อประเมินทักษะการปฏิบัติงานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.2.4 เพื่อประเมินทัศนคติของผู้เรียนต่อการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน

1.3 สมมติฐานในงานวิจัย

1.3.1 ผลสัมฤทธิ์ทางด้านความรู้ของกลุ่มทดลองที่ใช้ชุดการเรียนรู้สูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญทางสถิติ

1.3.2 ทักษะการปฏิบัติงานของผู้เรียนที่ใช้ชุดการเรียนรู้เชิงปฏิบัติที่พัฒนาขึ้นสูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญทางสถิติ

1.3.3 ทัศนคติของผู้เรียนที่มีต่อการนำระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งานของกลุ่มทดลองเป็นไปในเชิงบวกมากกว่ากลุ่มควบคุม

1.4 ขอบเขตของการวิจัย

1.4.1 ด้านเนื้อหา ศึกษาเกี่ยวกับการเชื่อมต่ออุปกรณ์ในระบบการตรวจจับการบุกรุก ดังนี้

1.4.1.1 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)

1.4.1.2 ไมโครคอนโทรลเลอร์

1.4.1.3 Servomotor

1.4.1.4 Buzzer

1.4.1.5 LED

1.4.2 กลุ่มผู้เข้าร่วมการวิจัย คือ ผู้เรียนในระดับประกาศนียบัตรวิชาชีพ (ปวช.) ชั้นปีที่ 3 แผนกวิชาอิเล็กทรอนิกส์ วิทยาลัยเทคนิคนครนายก ที่ลงทะเบียนเรียนในรายวิชาอุปกรณ์อิเล็กทรอนิกส์ในระบบรักษาความปลอดภัย รหัสวิชา 20105-2025 จำนวน 40 คน โดยใช้วิธีเลือกผู้เข้าร่วมการวิจัยแบบเจาะจง

1.4.3 ผู้เชี่ยวชาญในการประเมินคุณภาพเครื่องมือ โดยมีคุณสมบัติเป็นผู้ที่มีความเชี่ยวชาญหรือ ผู้ที่มีประสบการณ์สอนไม่ต่ำกว่า 3 ปี จำนวน 5 ท่าน

1.4.4 เครื่องมือที่ใช้ในงานวิจัย

1.4.4.1 ชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.4.4.2 แบบทดสอบวัดความรู้เรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.4.4.3 แบบทดสอบวัดทักษะการปฏิบัติงานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.4.4.4 แบบสอบถามเพื่อสำรวจทัศนคติของผู้เรียนต่อการนำไปใช้งาน

1.4.5 การวิจัยแบบ Quasi-Experimental Design โดยใช้การวิจัยแบบแผนการทดลอง 2 กลุ่ม คือกลุ่มทดลองและกลุ่มควบคุม

1.5 นิยามศัพท์เฉพาะ

1.5.1 ปัญญาประดิษฐ์ในระบบรักษาความปลอดภัย หมายถึง การประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ในการวิเคราะห์ ตรวจจับ และตอบสนองต่อภัยคุกคามในระบบรักษาความปลอดภัย โดยใช้เทคนิคต่างๆ เช่น การจดจำใบหน้า การวิเคราะห์พฤติกรรม และการเรียนรู้ของเครื่อง (Machine Learning) เพื่อเพิ่มประสิทธิภาพในการป้องกันและแจ้งเตือนอัตโนมัติ

1.5.2 ชุดการเรียนรู้เชิงปฏิบัติ หมายถึง สื่อการเรียนรู้ที่ออกแบบมาเพื่อให้ผู้เรียนได้ลงมือปฏิบัติจริง โดยมุ่งเน้นการทดลอง ทดสอบ และแก้ไขปัญหาในสถานการณ์จริง เพื่อพัฒนาทักษะและความเข้าใจในเนื้อหา

1.5.3 ระบบตรวจจับการบุกรุก หมายถึง ระบบที่ใช้เพื่อตรวจสอบและแจ้งเตือนเมื่อมีการเข้าถึงที่ไม่ได้รับอนุญาตหรือกิจกรรมที่น่าสงสัยในพื้นที่

1.5.4 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) หมายถึง อุปกรณ์ประมวลผลภาพที่มีปัญญาประดิษฐ์ (AI) ในตัว สามารถเรียนรู้และจดจำวัตถุ ใบหน้า ป้ายข้อความ และลักษณะเฉพาะต่างๆ ได้โดยอัตโนมัติ ใช้ในการพัฒนาแอปพลิเคชันที่เกี่ยวข้องกับการตรวจจับวัตถุ การควบคุมด้วยภาพ และระบบรักษาความปลอดภัย

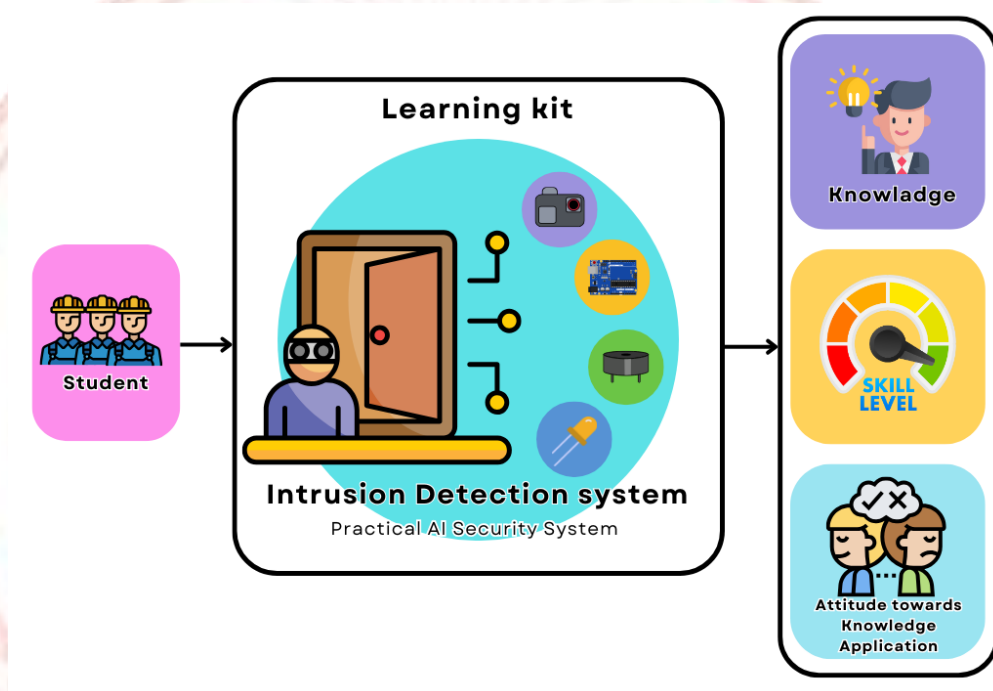
1.6 กรอบแนวคิดของการวิจัย

1.6.1 ตัวแปรที่ศึกษา

1.6.1.1 ตัวแปรต้น ได้แก่ ชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.6.1.2 ตัวแปรตาม คือ ความรู้ ทักษะการปฏิบัติงาน และทัศนคติต่อการเรียนรู้ของผู้เรียนต่อการนำไปใช้งาน

โดยกรอบแนวคิดการวิจัย แสดงดังภาพที่ 1-1



ภาพที่ 1-1 กรอบแนวคิดการวิจัย

1.7 ประโยชน์ที่คาดว่าจะได้รับ

1.7.1 ได้ชุดการเรียนรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.7.2 ผู้เรียนมีทักษะในการประยุกต์ใช้อุปกรณ์และปฏิบัติงานในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

1.7.3 ได้เครื่องมือสำคัญในการปรับปรุงและพัฒนาการศึกษาให้มีคุณภาพสูงขึ้นสอดคล้องกับความต้องการของผู้เรียนและตลาดแรงงานในปัจจุบัน

บทที่ 2

เอกสารและงานวิจัยที่เกี่ยวข้อง

การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ ในการตรวจจับการบุกรุก ในครั้งนี้ ผู้วิจัยได้มีการศึกษาทฤษฎีต่าง ๆ รวมถึงเอกสาร และงานวิจัยที่เกี่ยวข้อง ดังนี้

- 2.1 แนวทางและหลักสูตรประกาศนียบัตรวิชาชีพ พ.ศ. 2567
- 2.2 ระบบตรวจจับการบุกรุกในสถานที่ (Intrusion Detection Systems - IDS)
- 2.3 การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence) ในระบบรักษาความปลอดภัย
- 2.4 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)
- 2.5 ชุดการเรียนรู้เชิงปฏิบัติ (Practical Learning Kits)
- 2.6 การวิจัยที่เกี่ยวข้อง

2.1 แนวทางและหลักสูตรประกาศนียบัตรวิชาชีพ พ.ศ. 2567

หลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567 มุ่งพัฒนาผู้เรียนให้มีสมรรถนะด้านวิชาชีพที่สอดคล้องกับกรอบคุณวุฒิแห่งชาติ มาตรฐานสากล และความต้องการของตลาดแรงงาน โดยเน้นการเรียนรู้ผ่านการปฏิบัติจริง เพื่อเสริมสร้างทักษะด้านฝีมือ คุณธรรม จริยธรรม และจรรยาบรรณวิชาชีพ หลักสูตรมีความยืดหยุ่น เปิดโอกาสให้ผู้เรียนเลือกแนวทางการศึกษาที่เหมาะสม พร้อมรองรับการเทียบโอนผลการเรียน ความรู้ และประสบการณ์ตามมาตรฐานอาชีพ อีกทั้งยังสนับสนุนการเรียนรู้ตลอดชีวิต การพัฒนาหลักสูตรร่วมกับชุมชนและสถานประกอบการ ตลอดจนการสร้างความร่วมมือระหว่างหน่วยงานทั้งในและต่างประเทศ เพื่อเพิ่มศักยภาพในการแข่งขันในระดับโลกอย่างยั่งยืน

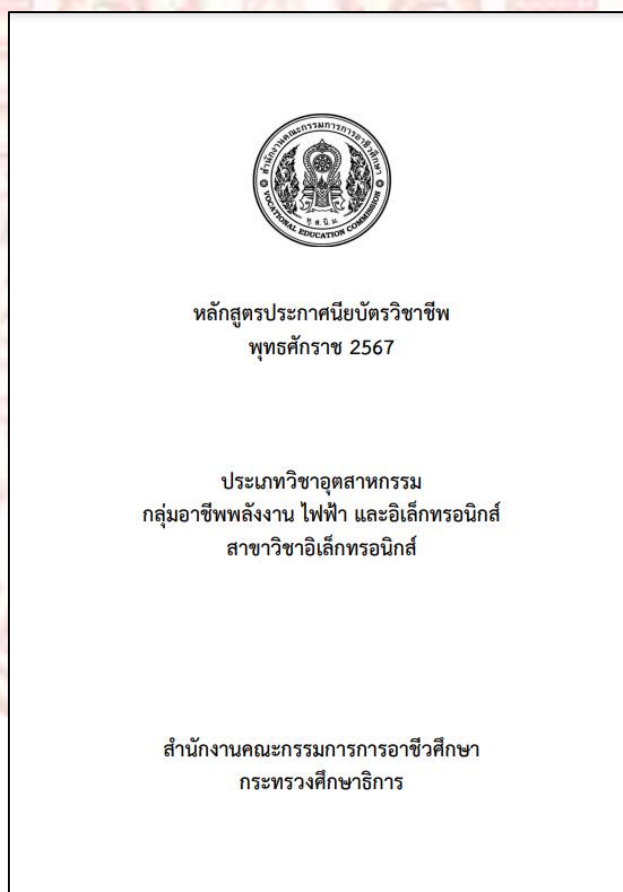
จุดหมายของหลักสูตรคือการสร้างบุคลากรที่มีคุณลักษณะและพฤติกรรมที่ดี มีจรรยาบรรณวิชาชีพ ความรับผิดชอบต่อสังคม และจิตสำนึกอนุรักษ์สิ่งแวดล้อม พร้อมทั้งพัฒนาความรู้ในด้านข้อเท็จจริง หลักการ ทฤษฎี และแนวปฏิบัติที่เกี่ยวข้องกับงานอาชีพ โดยมุ่งเสริมทักษะการสื่อสาร การใช้เทคโนโลยีดิจิทัล การคิดวิเคราะห์ การแก้ปัญหา และการเรียนรู้ตลอดชีวิต รวมถึงการปรับตัวต่อการเปลี่ยนแปลงในงานอาชีพ อีกทั้งยังปลูกฝังความตระหนักรู้ในปัญหาเศรษฐกิจ สังคม และสิ่งแวดล้อม ตลอดจนการมีส่วนร่วมในการพัฒนาชาติให้มั่นคงและยั่งยืน มุ่งเน้นการสร้างผู้เรียนที่พร้อมด้วยความรู้ ทักษะ และจิตสำนึกที่ดี เพื่อเป็นกำลังสำคัญในการพัฒนาประเทศอย่างยั่งยืนในอนาคต

โดยหลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567 ประเภทวิชาอุตสาหกรรม กลุ่มอาชีพ พลังงาน ไฟฟ้า และอิเล็กทรอนิกส์ สาขาวิชาอิเล็กทรอนิกส์มุ่งเน้นการพัฒนาผู้เรียนให้มีความรู้และ

ทักษะด้านอิเล็กทรอนิกส์ที่ตอบสนองความต้องการของตลาดแรงงานในอุตสาหกรรมพลังงาน ไฟฟ้า และอิเล็กทรอนิกส์ โดยเน้นการเรียนรู้ผ่านการปฏิบัติจริง เพื่อสร้างสมรรถนะในงานวิชาชีพเฉพาะทาง เช่น การออกแบบ การติดตั้ง การบำรุงรักษา และการแก้ไขปัญหาาระบบอิเล็กทรอนิกส์ ตลอดจน การบูรณาการเทคโนโลยีดิจิทัลและการสื่อสารเพื่อเพิ่มประสิทธิภาพในการทำงาน

หลักสูตรยังให้ความสำคัญกับการพัฒนาทักษะด้านการคิดวิเคราะห์ การแก้ปัญหา และการทำงานร่วมกันในรูปแบบทีม พร้อมปลูกฝังจริยธรรม จรรยาบรรณวิชาชีพ ความรับผิดชอบต่อสังคม และจิตสำนึกในการอนุรักษ์พลังงานและสิ่งแวดล้อม

นอกจากนี้ ผู้เรียนจะได้รับโอกาสในการฝึกประสบการณ์วิชาชีพในสถานประกอบการจริง โดยร่วมมือกับหน่วยงานภาครัฐและเอกชน เพื่อเตรียมความพร้อมสำหรับการเข้าสู่อาชีพในสายงาน อิเล็กทรอนิกส์หรือการประกอบอาชีพอิสระอย่างมั่นคงและยั่งยืน ทั้งนี้ หลักสูตรได้ออกแบบให้ สอดคล้องกับมาตรฐานอาชีพและกรอบคุณวุฒิแห่งชาติ เพื่อสร้างบุคลากรที่มีสมรรถนะสูงและมี ศักยภาพในการแข่งขันในระดับสากล (หลักสูตร ประกาศนียบัตรวิชาชีพ พุทธศักราช 2567, 2567)



ภาพที่ 2-1 หลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567 สาขาวิชาอิเล็กทรอนิกส์
(หลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567, 2567)

2.2 ระบบตรวจจับการบุกรุกในสถานที่ (Intrusion Detection Systems - IDS)

2.2.1 แนวคิดและความสำคัญของระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก (Intrusion Detection Systems - IDS) คือระบบที่ออกแบบมาเพื่อตรวจสอบกิจกรรมที่ผิดปกติหรือพฤติกรรมที่เข้าข่ายการบุกรุกในสถานที่เป้าหมาย เช่น อาคารสำนักงาน บ้าน หรือพื้นที่เฉพาะอื่นๆ โดยมีวัตถุประสงค์ในการเพิ่มความปลอดภัยและลดความเสี่ยงจากการโจรกรรมหรือเหตุการณ์ที่ไม่พึงประสงค์ (Hasan et al., 2022) ระบบ IDS สามารถแบ่งออกเป็นสองประเภทหลัก ได้แก่

2.2.1.1 ระบบตรวจจับเชิงรับ (Passive IDS): ทำหน้าที่แจ้งเตือนเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น

2.2.1.2 ระบบตรวจจับเชิงรุก (Active IDS): มีฟังก์ชันในการตอบสนองอัตโนมัติเพื่อป้องกันหรือจำกัดการเข้าถึง (Rahman & Chen, 2021)

2.2.2 องค์ประกอบหลักของระบบตรวจจับการบุกรุก

2.2.2.1 ตัวเซ็นเซอร์ (Sensors): ใช้สำหรับตรวจจับการเปลี่ยนแปลงหรือพฤติกรรมที่น่าสงสัย เช่น เซ็นเซอร์ตรวจจับการเคลื่อนไหว (Motion Sensors) และเซ็นเซอร์อุณหภูมิ (Temperature Sensors)

2.2.2.2 ตัวประมวลผล (Processor): ใช้สำหรับวิเคราะห์ข้อมูลที่ได้รับจากเซ็นเซอร์ โดยอาจใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) หรือ Machine Learning (ML) เพื่อเพิ่มความแม่นยำ (Li et al., 2023)

2.2.2.3 ระบบการแจ้งเตือน (Alert System): อาจใช้สัญญาณเสียง ไฟแจ้งเตือน หรือการส่งการแจ้งเตือนผ่านแอปพลิเคชันมือถือ

2.2.2.4 ระบบควบคุม (Control System): สามารถทำงานร่วมกับระบบล็อกอิเล็กทรอนิกส์หรือระบบอื่นๆ เพื่อเพิ่มความปลอดภัย

2.2.3 การประยุกต์ใช้ระบบตรวจจับการบุกรุกในสถานการณ์จริง

ในปัจจุบัน ระบบ IDS ถูกนำมาใช้อย่างแพร่หลายในหลากหลายอุตสาหกรรม เช่น การรักษาความปลอดภัยในบ้านอัจฉริยะ (Smart Home Security), การป้องกันข้อมูลในศูนย์ข้อมูล (Data Centers), และการเฝ้าระวังในพื้นที่สาธารณะ (Public Spaces Monitoring) โดยระบบที่ทันสมัยสามารถทำงานร่วมกับ IoT และระบบคลาวด์เพื่อเพิ่มประสิทธิภาพการเฝ้าระวังและการจัดการข้อมูล (Ahmed et al., 2021)

2.2.4 การพัฒนาระบบตรวจจับการบุกรุกด้วย AI และ IoT

การใช้ AI และ IoT ได้ปรับปรุงระบบ IDS ให้สามารถเรียนรู้จากข้อมูลในอดีตและระบุความเสี่ยงได้อย่างแม่นยำยิ่งขึ้น ตัวอย่างเช่น การใช้โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) ในการตรวจจับใบหน้าเพื่อควบคุมการเข้าถึง หรือการใช้ ESP32 สำหรับการสื่อสาร

ผ่านเครือข่าย Wi-Fi (Kim et al., 2023) เทคโนโลยีเหล่านี้ช่วยเพิ่มความปลอดภัยและลดโอกาสที่ผู้บุกรุกจะสามารถเข้าถึงพื้นที่ได้

2.3 การประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence) ในระบบรักษาความปลอดภัย

2.3.1 แนวคิดและบทบาทของปัญญาประดิษฐ์ในระบบรักษาความปลอดภัย

ปัญญาประดิษฐ์ (Artificial Intelligence: AI) ได้เข้ามามีบทบาทสำคัญในระบบรักษาความปลอดภัย เนื่องจากความสามารถในการวิเคราะห์ข้อมูลขนาดใหญ่ ประมวลผลอย่างรวดเร็ว และตัดสินใจได้อย่างแม่นยำ AI ถูกนำมาใช้ในการพัฒนาระบบรักษาความปลอดภัยเพื่อเพิ่มประสิทธิภาพการตรวจจับภัยคุกคามและลดความผิดพลาดจากมนุษย์ (Chen et al., 2022) เทคโนโลยี AI ยังสามารถเรียนรู้พฤติกรรมปกติและพฤติกรรมที่ผิดปกติในสภาพแวดล้อมต่างๆ เพื่อช่วยป้องกันเหตุการณ์ที่ไม่พึงประสงค์ได้อย่างทันท่วงที (Zhang et al., 2023)

2.3.2 การนำ AI มาใช้ในระบบรักษาความปลอดภัย

2.3.2.1 การวิเคราะห์ภาพและวิดีโอ

AI ถูกนำมาใช้ในการวิเคราะห์ภาพและวิดีโอจากกล้องวงจรปิด (CCTV) เพื่อระบุบุคคลต้องสงสัย การตรวจจับการเคลื่อนไหวที่ผิดปกติ หรือการจดจำใบหน้า (Facial Recognition) ซึ่งช่วยให้สามารถเฝ้าระวังพื้นที่ได้อย่างมีประสิทธิภาพมากขึ้น โดยเฉพาะ โครงข่ายประสาทเทียมแบบคอนโวลูชัน (Convolutional Neural Network - CNN) ซึ่งเป็นเทคนิค Deep Learning ที่สามารถเรียนรู้และจดจำลักษณะเฉพาะของใบหน้าและวัตถุได้อย่างแม่นยำ (Li et al., 2021) ระบบเฝ้าระวังอัตโนมัติที่ใช้ CNN สามารถวิเคราะห์ข้อมูลจากกล้อง CCTV ได้แบบเรียลไทม์ และลดอัตราการแจ้งเตือนที่ผิดพลาดเมื่อเทียบกับเทคนิคแบบดั้งเดิม

2.3.2.2 การตรวจจับการบุกรุก (Intrusion Detection)

ด้วยการใช้เทคโนโลยี Machine Learning (ML) และ Deep Learning ระบบสามารถเรียนรู้และวิเคราะห์รูปแบบพฤติกรรมเพื่อระบุภัยคุกคาม เช่น การตรวจจับการพยายามเข้าถึงพื้นที่ที่ไม่ได้รับอนุญาต โดย CNN มีบทบาทสำคัญในการวิเคราะห์ภาพเพื่อตรวจจับบุคคลที่บุกรุกผ่านการแยกแยะลักษณะของภาพ เช่น ท่าทาง การเคลื่อนไหว และตำแหน่งของบุคคล (Khan et al., 2020) นอกจากนี้ โมเดล YOLO (You Only Look Once) ซึ่งเป็นสถาปัตยกรรม CNN ที่มีความเร็วสูง ยังถูกใช้ในการตรวจจับและติดตามวัตถุในระบบรักษาความปลอดภัยเพื่อลดระยะเวลาการตอบสนองต่อเหตุการณ์ที่ผิดปกติ

2.3.2.3 ระบบการยืนยันตัวตน (Authentication Systems)

AI ช่วยเพิ่มความปลอดภัยให้กับระบบยืนยันตัวตนผ่านการวิเคราะห์ลักษณะทางชีวมิติ เช่น ลายนิ้วมือ การสแกนม่านตา และการวิเคราะห์เสียง ซึ่งช่วยลดโอกาสการปลอมแปลงตัวตน CNN ถูกนำมาใช้ใน FaceNet และ DeepFace ซึ่งเป็นโมเดลที่ใช้ในระบบการจดจำใบหน้าด้วยความแม่นยำสูง ระบบเหล่านี้สามารถเรียนรู้คุณลักษณะของใบหน้าจากฐานข้อมูลขนาดใหญ่และ

สามารถตรวจจับความพยายามในการปลอมแปลงตัวตน เช่น การใช้ภาพถ่ายหรือวิดีโอเพื่อแอบอ้างตัวตน (Rahman & Ahmed, 2023)

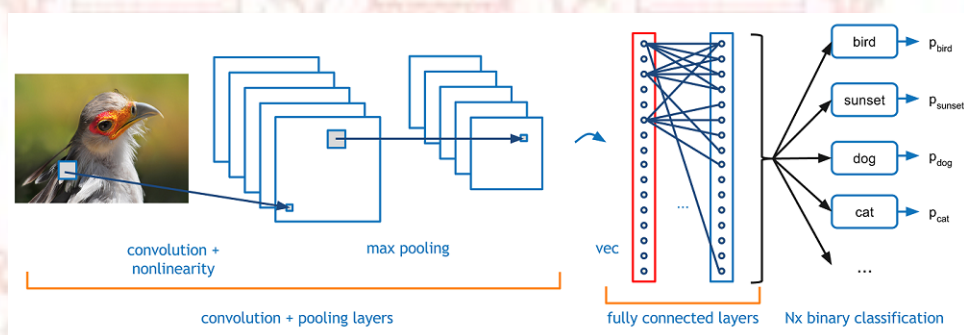
2.3.2.4 การประมวลผลเหตุการณ์แบบเรียลไทม์

ระบบ AI สามารถประมวลผลข้อมูลที่ได้รับจากเซ็นเซอร์ต่างๆ และแจ้งเตือนเมื่อพบเหตุการณ์ที่ผิดปกติ เช่น การตรวจจับเสียงผิดปกติ หรืออุณหภูมิที่เพิ่มขึ้นในพื้นที่เฉพาะ โดย CNN มีบทบาทสำคัญในการช่วยแยกแยะประเภทของวัตถุหรือเหตุการณ์จากกล้องวงจรปิดได้อย่างรวดเร็ว ตัวอย่างเช่น ResNet และ MobileNet ถูกนำมาใช้ในอุปกรณ์ IoT เพื่อประมวลผลเหตุการณ์แบบเรียลไทม์โดยใช้พลังงานต่ำ (Huang et al., 2022)

การนำ CNN และ Deep Learning มาใช้ในระบบรักษาความปลอดภัยทำให้สามารถวิเคราะห์ภาพและวิดีโอได้อย่างแม่นยำ ลดข้อผิดพลาดในการตรวจจับ และเพิ่มประสิทธิภาพในการเฝ้าระวังและตอบสนองต่อภัยคุกคามแบบเรียลไทม์

2.3.3 โครงข่ายประสาทเทียมแบบคอนโวลูชัน (Convolutional Neural Network - CNN)

โครงข่ายประสาทเทียมแบบคอนโวลูชันเป็นสถาปัตยกรรมหนึ่งของ Deep Learning ที่ถูกออกแบบมาเพื่อประมวลผลข้อมูลที่มีโครงสร้างแบบกริด เช่น ภาพสองมิติ โดยเฉพาะอย่างยิ่งในการวิเคราะห์และจดจำลักษณะเฉพาะของภาพ



ภาพที่ 2-2 Convolutional Neural Network (Deshpande, A., 2016)

หลักการทำงานของโครงข่ายประสาทเทียมแบบคอนโวลูชัน CNN มีลักษณะเด่นคือความสามารถในการเรียนรู้คุณลักษณะ (features) จากข้อมูลภาพโดยอัตโนมัติผ่านกระบวนการที่เรียกว่า การคอนโวลูชัน (convolution) การลดทอนขนาด (pooling) และการเชื่อมต่อแบบเต็มรูปแบบ (fully connected) โดยมีองค์ประกอบหลักดังนี้

2.3.3.1 ชั้นคอนโวลูชัน (Convolutional Layer) ชั้นคอนโวลูชันทำหน้าที่สกัดคุณลักษณะจากภาพนำเข้าโดยใช้ตัวกรอง (filter หรือ kernel) ซึ่งเป็นเมทริกซ์น้ำหนักที่เรียนรู้ได้ ตัวกรองจะเลื่อนไปบนภาพนำเข้าและคำนวณผลคูณจุด (dot product) ระหว่างค่าพิกเซลของภาพ

กับค่าน้ำหนักในตัวกรอง ผลลัพธ์ที่ได้เรียกว่า feature map ซึ่งแสดงถึงการตรวจจับคุณลักษณะต่างๆ เช่น ขอบ เส้น หรือรูปร่างในภาพ สมการของการคอนโวลูชันสามารถแสดงได้ดังนี้

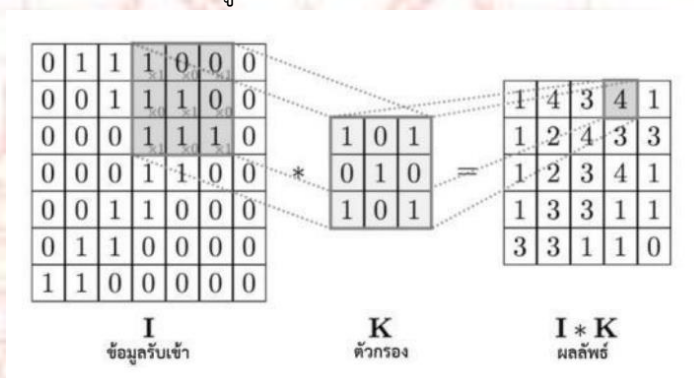
$$(I * K)(i,j) = \sum_m \sum_n I(i+m,j+n) \cdot K(m,n) \quad (2-1)$$

โดยที่:

I คือภาพนำเข้า

K คือตัวกรอง (kernel)

* แทนการดำเนินการคอนโวลูชัน

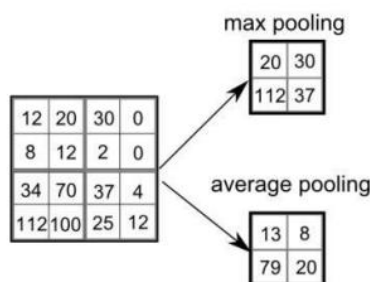


ภาพที่ 2-3 การทำคอนโวลูชัน (ธนภัทร์ คุ่มสุภา, 2559)

2.3.3.2 ฟังก์ชันกระตุ้น (Activation Function) หลังจากการคอนโวลูชัน จะมีการใช้ฟังก์ชันกระตุ้นที่ไม่เชิงเส้น (non-linear activation function) เช่น ReLU (Rectified Linear Unit) เพื่อเพิ่มความสามารถในการเรียนรู้ความสัมพันธ์ที่ซับซ้อน ฟังก์ชัน ReLU จะแปลงค่าที่น้อยกว่าศูนย์เป็นศูนย์ และคงค่าที่มากกว่าหรือเท่ากับศูนย์ไว้เหมือนเดิม

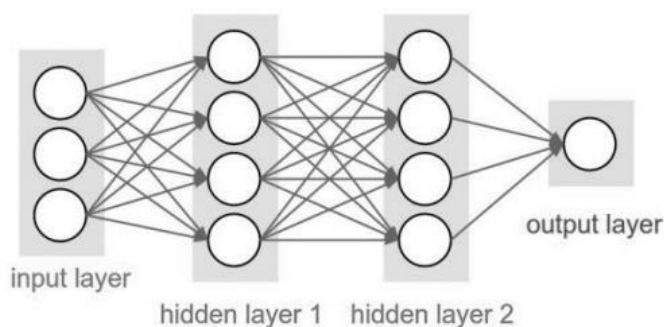
$$f(x) = \max(0, x) \quad (2-2)$$

2.3.3.3 ชั้นพูลลิง (Pooling Layer) ชั้นพูลลิงทำหน้าที่ลดขนาดของ feature map เพื่อลดจำนวนพารามิเตอร์และการคำนวณในโมเดล นอกจากนี้ยังช่วยให้โมเดลมีความทนทานต่อการเปลี่ยนตำแหน่งเล็กน้อยของวัตถุในภาพ (translation invariance) วิธีพูลลิงที่นิยมใช้ ได้แก่ Max Pooling เป็นการเลือกค่าสูงสุดในหน้าต่างที่กำหนดและ Average Pooling การคำนวณค่าเฉลี่ยของค่าในหน้าต่างที่กำหนด



ภาพที่ 2-4 ชั้นพูลลิงโดย Max Pooling และ Average Pooling (ธนภัทร์ คุ้มสุภา, 2559)

2.3.3.4 ชั้นเชื่อมต่อแบบเต็มรูปแบบ (Fully Connected Layer) หลังจากผ่านชั้นคอนโวลูชันและชั้นพูลลิงหลายชั้นแล้ว feature map จะถูกแปลงเป็นเวกเตอร์แบบหนึ่งมิติและส่งไปยังชั้นเชื่อมต่อแบบเต็มรูปแบบ ซึ่งทำหน้าที่เหมือนโครงข่ายประสาทเทียมแบบดั้งเดิม (traditional neural network) เพื่อทำการจำแนกประเภทหรือการทำนาย



ภาพที่ 2-5 ชั้นการเชื่อมโยงเต็มรูปแบบ (ธนภัทร์ คุ้มสุภา, 2559)

2.3.3.5 ชั้นผลลัพธ์ (Output Layer) ชั้นสุดท้ายของ CNN จะใช้ฟังก์ชัน SoftMax เพื่อแปลงผลลัพธ์เป็นความน่าจะเป็นของแต่ละคลาสในงานการจำแนกประเภท

2.3.3.6 สถาปัตยกรรม CNN ที่สำคัญ ตลอดระยะเวลาที่ผ่านมา มีการพัฒนาสถาปัตยกรรม CNN หลากหลายรูปแบบ โดยแต่ละรูปแบบมีนวัตกรรมและข้อดีที่แตกต่างกัน สถาปัตยกรรมที่สำคัญมีดังนี้

2.3.3.6.1 LeNet-5 พัฒนาโดย Yann LeCun และคณะในปี 1998 เป็นหนึ่งในสถาปัตยกรรม CNN ยุคแรกที่ใช้สำหรับการรู้จำตัวเลขลายมือ (MNIST dataset) ประกอบด้วยชั้นคอนโวลูชัน 2 ชั้น ชั้นพูลลิง 2 ชั้น และชั้นเชื่อมต่อแบบเต็มรูปแบบ 3 ชั้น (LeCun et al., 1998)

2.3.3.6.2 AlexNet พัฒนาโดย Alex Krizhevsky และคณะในปี 2012 มีโครงสร้างที่ลึกกว่า LeNet โดยประกอบด้วยชั้นคอนโวลูชัน 5 ชั้น และชั้นเชื่อมต่อแบบเต็มรูปแบบ

3 ชั้น นอกจากนี้ยังมีการใช้เทคนิค Dropout เพื่อลดปัญหา Overfitting และใช้ GPU ในการฝึกสอนโมเดล (Krizhevsky et al., 2012)

2.3.3.6.3 VGGNet พัฒนาโดย Visual Geometry Group จาก University of Oxford ในปี 2014 มีจุดเด่นคือใช้ตัวกรองขนาด 3x3 ทั้งหมดในชั้นคอนโวลูชัน และมีโครงสร้างที่เรียบง่ายแต่ลึกมาก (16-19 ชั้น) ทำให้สามารถเรียนรู้คุณลักษณะที่ซับซ้อนได้ดี (Simonyan & Zisserman, 2014)

2.3.3.6.4 GoogLeNet พัฒนาโดยทีมวิจัยของ Google ในปี 2014 มีการใช้โมดูล Inception ซึ่งประกอบด้วยตัวกรองหลายขนาด (1x1, 3x3, 5x5) ทำงานขนานกัน ช่วยให้โมเดลสามารถจับคุณลักษณะในหลายระดับพร้อมกัน และลดจำนวนพารามิเตอร์ลงอย่างมาก (Szegedy et al., 2015)

2.3.3.6.5 ResNet (Residual Network) พัฒนาโดยทีมวิจัยของ Microsoft Research ในปี 2015 มีการใช้ "skip connections" หรือ "residual connections" เพื่อแก้ปัญหา vanishing gradient ในโครงข่ายที่ลึกมาก ทำให้สามารถสร้างโมเดลที่มีความลึกถึง 152 ชั้นได้ (He et al., 2016)

2.3.3.7 การประยุกต์ใช้งาน CNN ได้รับการประยุกต์ใช้ในงานหลากหลายด้าน โดยเฉพาะงานที่เกี่ยวข้องกับการประมวลผลภาพและวิดีโอ

2.3.3.7.1 การจำแนกภาพ (Image Classification) CNN ถูกใช้อย่างแพร่หลายในการจำแนกวัตถุในภาพ เช่น การแยกประเภทสัตว์ พืช ยานพาหนะ หรือวัตถุอื่นๆ โดยโมเดลจะเรียนรู้คุณลักษณะเฉพาะของแต่ละคลาสเพื่อทำนายป้ายกำกับ (label) ที่ถูกต้อง (Russakovsky et al., 2015)

2.3.3.7.2 การตรวจจับวัตถุ (Object Detection) CNN สามารถระบุตำแหน่งและประเภทของวัตถุหลายชิ้นในภาพเดียวกันได้ โดยใช้เทคนิคเช่น R-CNN, Fast R-CNN, Faster R-CNN และ YOLO (You Only Look Once) ซึ่งมีประสิทธิภาพสูงในการตรวจจับวัตถุแบบเรียลไทม์ (Girshick et al., 2014; Redmon et al., 2016)

2.3.3.7.3 การแบ่งส่วนภาพ (Image Segmentation) การแบ่งส่วนภาพเป็นการระบุพิกเซลแต่ละพิกเซลว่าเป็นส่วนของวัตถุใด โดย CNN ที่นิยมใช้ในงานนี้ได้แก่ Fully Convolutional Networks (FCN), U-Net และ Mask R-CNN (Long et al., 2015; Ronneberger et al., 2015; He et al., 2017)

2.3.3.7.4 การรู้จำใบหน้า (Face Recognition) CNN สามารถใช้ในการตรวจจับและรู้จำใบหน้าบุคคลโดยเรียนรู้คุณลักษณะเฉพาะของใบหน้าแต่ละคน ซึ่งนำไปประยุกต์ใช้ในระบบรักษาความปลอดภัย การยืนยันตัวตน และแอปพลิเคชันโซเชียลมีเดีย (Taigman et al., 2014)

2.3.3.7.5 การประมวลผลภาษาธรรมชาติ (Natural Language Processing)

แม้ว่า CNN จะถูกพัฒนาขึ้นมาเพื่อการประมวลผลภาพเป็นหลัก แต่ก็สามารถประยุกต์ใช้กับข้อมูลเชิงลำดับ เช่น ข้อความ โดยการแปลงข้อความเป็นเมทริกซ์และใช้การคอนโวลูชันแบบ 1 มิติ (Kim, 2014)

2.3.3.8 ข้อดีและข้อจำกัดของ CNN

2.3.3.8.1 ข้อดี CNN ใช้แนวคิดการแบ่งปันพารามิเตอร์ (parameter sharing) ทำให้จำนวนพารามิเตอร์ที่ต้องเรียนรู้้น้อยกว่าโครงข่ายประสาทเทียมแบบเชื่อมต่อเต็มรูปแบบ สามารถเรียนรู้คุณลักษณะจากข้อมูลโดยอัตโนมัติ ไม่จำเป็นต้องกำหนดคุณลักษณะเองแบบวิธีการดั้งเดิมมีความทนทานต่อการเปลี่ยนแปลงตำแหน่ง การหมุน และการปรับขนาดของวัตถุในภาพและให้ผลลัพธ์ที่แม่นยำในงานการประมวลผลภาพและวิดีโอ

2.3.3.8.2 ข้อจำกัด CNN มักต้องการข้อมูลฝึกสอนในปริมาณมากเพื่อให้ได้ผลลัพธ์ที่ดี การฝึกสอน CNN ที่มีความลึกมากต้องใช้ทรัพยากรการคำนวณสูงและเวลานาน CNN มักถูกมองว่าเป็น "black box" เนื่องจากยากที่จะอธิบายว่าโมเดลตัดสินใจอย่างไรและ CNN อาจไวต่อการเปลี่ยนแปลงของข้อมูล เช่น ความผิดเพี้ยนของภาพ หรือตัวอย่างที่ถูกออกแบบมาเพื่อหลอกโมเดล (adversarial examples)

2.3.4 Deep Learning

Deep Learning เป็นสาขาหนึ่งของปัญญาประดิษฐ์ (Artificial Intelligence: AI) และการเรียนรู้ของเครื่อง (Machine Learning: ML) ซึ่งใช้โครงข่ายประสาทเทียมที่มีหลายชั้น (Multi-layer Neural Networks) เพื่อเรียนรู้รูปแบบข้อมูลที่ซับซ้อน (LeCun et al., 2015) โดยอัลกอริทึมของ Deep Learning สามารถดึงคุณลักษณะของข้อมูลได้อัตโนมัติโดยไม่ต้องพึ่งพาการออกแบบฟีเจอร์แบบดั้งเดิม (Goodfellow et al., 2016) ทำให้ได้รับความนิยมในการใช้งานหลากหลาย เช่น การรู้จำภาพ การประมวลผลภาษาธรรมชาติ และการขับเคลื่อนด้วยตนเอง

2.3.4.1 โครงสร้างของ Deep Learning ประกอบด้วยโครงข่ายประสาทเทียมที่มีหลายชั้น โดยมีองค์ประกอบหลักดังนี้

2.3.4.1.1 ชั้นอินพุต (Input Layer) รับข้อมูลดิบจากแหล่งต่าง ๆ เช่น ภาพ เสียง หรือข้อความ

2.3.4.1.2 ชั้นซ่อน (Hidden Layers) ประมวลผลข้อมูลผ่านนิวรอนโดยใช้ฟังก์ชันการกระตุ้น (Activation Function) เช่น ReLU, Sigmoid และ Tanh (Nair & Hinton, 2010)

2.3.4.1.3 ชั้นเอาต์พุต (Output Layer) สร้างผลลัพธ์ตามประเภทของปัญหา เช่น การจำแนกประเภท หรือการทำนายค่าเชิงตัวเลข

2.3.4.2 อัลกอริทึมที่สำคัญใน Deep Learning มีอัลกอริทึมที่สำคัญหลายแบบ ซึ่งแต่ละแบบมีการนำไปใช้ที่แตกต่างกัน ได้แก่

2.3.4.2.1 Convolutional Neural Networks (CNNs) ใช้สำหรับการประมวลผลภาพโดยใช้การกรองเชิงพื้นที่เพื่อลดความซับซ้อนของข้อมูล (Krizhevsky et al., 2012)

2.3.4.2.2 Recurrent Neural Networks (RNNs) เหมาะสำหรับข้อมูลลำดับ เช่น ข้อความและเสียง โดยสามารถเก็บข้อมูลจากอดีตเพื่อพยากรณ์อนาคตได้ (Hochreiter & Schmidhuber, 1997)

2.3.4.2.3 Generative Adversarial Networks (GANs): ใช้สำหรับการสร้างข้อมูลใหม่ที่คล้ายกับข้อมูลต้นแบบ โดยมีการต่อสู้ระหว่างตัวสร้าง (Generator) และตัวแยกแยะ (Discriminator) (Goodfellow et al., 2014)

2.3.4.3 การประยุกต์ใช้ Deep Learning ถูกนำไปใช้ในหลากหลายสาขา เช่น

2.3.4.3.1 การรู้จำภาพ (Image Recognition) ใช้ในระบบรู้จำใบหน้าและการวิเคราะห์ทางการแพทย์ เช่น การตรวจจับมะเร็ง (Litjens et al., 2017)

2.3.4.3.2 การประมวลผลภาษาธรรมชาติ (Natural Language Processing - NLP) ใช้ในแชทบอท การแปลภาษา และการสังเคราะห์เสียงพูด (Devlin et al., 2019)

2.3.4.3.3 ยานยนต์ขับเคลื่อนอัตโนมัติ (Autonomous Vehicles) ใช้ในการวิเคราะห์ภาพจากกล้องและเซ็นเซอร์เพื่อนำทาง (Bojarski et al., 2016)

Deep Learning เป็นเทคนิคที่มีศักยภาพสูงในปัจจุบัน โดยใช้โครงข่ายประสาทเทียมที่มีหลายชั้นเพื่อเรียนรู้ข้อมูลที่ซับซ้อน โดยมีการนำไปใช้ในหลากหลายด้าน เช่น การรู้จำภาพ การประมวลผลภาษาธรรมชาติ และยานยนต์อัตโนมัติ การพัฒนาเทคนิคใหม่นี้ยังคงเป็นที่สนใจของนักวิจัยและอุตสาหกรรมต่าง ๆ อย่างต่อเนื่อง

2.3.5 ความก้าวหน้าของ AI ในระบบรักษาความปลอดภัย

ในช่วง 5 ปีที่ผ่านมา การพัฒนาเทคโนโลยี AI ทำให้ระบบรักษาความปลอดภัยมีความแม่นยำและความชาญฉลาดเพิ่มขึ้น ตัวอย่างเช่น การใช้ AI ในระบบบ้านอัจฉริยะ (Smart Home) ที่สามารถตรวจจับและตอบสนองต่อสถานการณ์ได้อัตโนมัติ หรือการใช้ AI เพื่อวิเคราะห์ข้อมูลจากอุปกรณ์ IoT เพื่อป้องกันการโจมตีทางไซเบอร์ (Ahmed et al., 2023)

2.3.5 ความท้าทายในการใช้ AI

แม้ว่า AI จะมีศักยภาพสูง แต่การใช้งานยังคงเผชิญกับความท้าทาย เช่น ความเป็นส่วนตัวของข้อมูล (Data Privacy) และความปลอดภัยในการป้องกันการโจมตีจากแฮกเกอร์ (Cybersecurity Threats) การพัฒนาระบบที่สามารถจัดการกับปัญหาเหล่านี้ได้ยังคงเป็นหัวข้อวิจัยที่สำคัญ (Chen et al., 2022)

2.4 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)



ภาพที่ 2-6 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)

2.4.1 แนวคิดและความสำคัญของโมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)

โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) เป็นอุปกรณ์เซ็นเซอร์อัจฉริยะที่ใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในการประมวลผลภาพและจดจำวัตถุ เช่น ใบหน้า ป้ายข้อความ และรูปร่างของวัตถุแบบเรียลไทม์ โดยมีความสามารถในการเรียนรู้แบบ Machine Learning ในตัว ซึ่งช่วยเพิ่มความสะดวกและประสิทธิภาพในการพัฒนาระบบตรวจจับใบหน้าและการควบคุมความปลอดภัย (Wang et al., 2021)

โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) มาพร้อมกับอัลกอริทึม AI ที่สามารถทำงานได้ทันทีโดยไม่ต้องเขียนโค้ดเพิ่มเติมมากมาย และรองรับการเชื่อมต่อกับไมโครคอนโทรลเลอร์ เช่น Arduino, ESP32, และ Raspberry Pi ทำให้เหมาะสมสำหรับการออกแบบระบบรักษาความปลอดภัยในสถานที่ต่างๆ (Chen et al., 2022)

2.4.2 การใช้โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) ในการตรวจจับใบหน้า

HuskyLens ถูกนำมาใช้ในการตรวจจับและจดจำใบหน้าในระบบรักษาความปลอดภัยเพื่อเพิ่มความแม่นยำและลดข้อผิดพลาดของระบบ ตัวอย่างการใช้งาน เช่น

การตรวจจับและยืนยันตัวตน HuskyLens สามารถตรวจจับใบหน้าและเปรียบเทียบกับฐานข้อมูลที่เก็บไว้ เพื่อยืนยันตัวตนของผู้ใช้งาน ทำให้สามารถใช้เป็นระบบยืนยันตัวตนในสถานที่ที่ต้องการความปลอดภัยสูง เช่น ห้องเซิร์ฟเวอร์หรือสำนักงาน (Zhao et al., 2023)

การเฝ้าระวังและแจ้งเตือน ด้วยการวิเคราะห์ใบหน้าแบบเรียลไทม์ HuskyLens สามารถแจ้งเตือนเมื่อมีการตรวจพบบุคคลที่ไม่ได้รับอนุญาตในพื้นที่ เช่น การใช้งานในบ้านอัจฉริยะหรืออาคารสำนักงาน (Liu et al., 2021)

2.4.3 การควบคุมระบบรักษาความปลอดภัยด้วย โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)

HuskyLens สามารถทำงานร่วมกับระบบควบคุมต่างๆ เพื่อสร้างระบบรักษาความปลอดภัยที่ชาญฉลาด เช่น การควบคุมประตูอัตโนมัติ HuskyLens ถูกใช้ร่วมกับไมโครคอนโทรลเลอร์และมอเตอร์เซอร์โว (Servo Motor) เพื่อควบคุมการเปิด-ปิดประตู โดยอนุญาตเฉพาะบุคคลที่ได้รับ

การยืนยันตัวตน (Li et al., 2022) การแจ้งเตือนผ่าน IoT ระบบสามารถส่งการแจ้งเตือนไปยังอุปกรณ์เคลื่อนที่ของผู้ใช้งานผ่านเครือข่าย IoT เมื่อพบการบุกรุก หรือเมื่อมีบุคคลแปลกหน้าพยายามเข้าถึงพื้นที่ (Huang et al., 2023)

2.4.4 ความก้าวหน้าของโมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens)ในระบบรักษาความปลอดภัย

ในช่วงไม่กี่ปีที่ผ่านมา HuskyLens ได้รับการพัฒนาให้สามารถประมวลผลภาพได้อย่างรวดเร็วและแม่นยำยิ่งขึ้น พร้อมทั้งรองรับการใช้งานในสถานการณ์ที่ซับซ้อน เช่น สภาพแสงน้อยหรือมีสิ่งกีดขวาง นอกจากนี้ การเชื่อมต่อกับเทคโนโลยีอื่นๆ เช่น ESP32 และระบบคลาวด์ ยังช่วยเพิ่มขีดความสามารถของระบบในการทำงานระยะไกลและการจัดการข้อมูลขนาดใหญ่ (Wang et al., 2023)

2.5 ชุดการเรียนรู้เชิงปฏิบัติ (Practical Learning Kits)

ชุดการเรียนรู้เชิงปฏิบัติ (Practical Learning Kits) เป็นเครื่องมือที่ถูกออกแบบมาเพื่อให้ นักเรียนหรือผู้เรียนได้ลงมือปฏิบัติจริง ชุดการเรียนรู้เหล่านี้มีบทบาทสำคัญในการพัฒนาทักษะทางวิชาชีพ การแก้ปัญหา และการเรียนรู้เชิงประยุกต์ โดยเฉพาะในสาขาวิชาที่เกี่ยวข้องกับเทคโนโลยี เช่น วิศวกรรมศาสตร์ อิเล็กทรอนิกส์ และระบบสมองกลฝังตัว (Huang et al., 2022)

2.5.1 ประเภทของชุดการเรียนรู้เชิงปฏิบัติ

2.5.1.1 ชุดการเรียนรู้การเขียนโปรแกรมและควบคุมระบบ (Programming and Control Kits) ตัวอย่างเช่น Arduino Kits, Raspberry Pi Kits หรือ ESP32 Kits ซึ่งช่วยให้ผู้เรียนได้ทดลองเขียนโปรแกรมเพื่อควบคุมอุปกรณ์ เช่น มอเตอร์ เซ็นเซอร์ และไฟ LED นอกจากนี้ยังสามารถใช้ชุดเหล่านี้ในการพัฒนาระบบ IoT ได้ (Chen et al., 2023)

2.5.1.2 ชุดการเรียนรู้ด้านหุ่นยนต์ (Robotics Kits) ชุดการเรียนรู้ประเภทนี้ เช่น LEGO Mindstorms หรือ KidBright Robot Kits ถูกใช้เพื่อให้ผู้เรียนพัฒนาทักษะการเขียนโปรแกรมและการออกแบบระบบหุ่นยนต์ ชุดเหล่านี้ช่วยให้ผู้เรียนสามารถทดลองสร้างและควบคุมหุ่นยนต์ในรูปแบบต่างๆ เช่น หุ่นยนต์เดินตามเส้นหรือหุ่นยนต์หลีกเลี่ยงสิ่งกีดขวาง (Li et al., 2022)

2.5.1.3 ชุดการเรียนรู้ด้านระบบสมองกลฝังตัว (Embedded System Kits) ชุดการเรียนรู้ที่เน้นการพัฒนาระบบสมองกลฝังตัว เช่น การใช้ Arduino หรือ STM32 ในการสร้างระบบควบคุม เช่น ระบบควบคุมอุณหภูมิหรือระบบแจ้งเตือนภัย ชุดเหล่านี้ช่วยพัฒนาทักษะที่สามารถนำไปประยุกต์ใช้ในอุตสาหกรรม (Zhao et al., 2021)

2.5.1.4 ชุดการเรียนรู้ด้านปัญญาประดิษฐ์ (AI Learning Kits) ตัวอย่างเช่น HuskyLens Learning Kits ที่ช่วยให้ผู้เรียนได้ทดลองการพัฒนาระบบตรวจจับใบหน้า การจดจำวัตถุ และการประมวลผลภาพ ชุดนี้เหมาะสำหรับการพัฒนาโครงการที่ใช้ AI ในการควบคุมระบบรักษาความปลอดภัย (Wang et al., 2023)

2.5.1.5 ชุดการเรียนรู้การสร้างต้นแบบระบบ IoT (IoT Prototyping Kits) ชุด IoT เช่น ESP32 DevKit หรือ NodeMCU ถูกใช้ในการพัฒนาโครงการเชิงปฏิบัติ เช่น ระบบสมาร์ทโฮม หรือระบบควบคุมอุปกรณ์ระยะไกล ชุดเหล่านี้ช่วยให้นักเรียนเข้าใจการเชื่อมต่อเครือข่ายและการส่งข้อมูลผ่านระบบ IoT (Ahmed et al., 2023)

2.5.2 ประโยชน์ของชุดการเรียนรู้เชิงปฏิบัติ

การพัฒนาทักษะการแก้ปัญหาโดยผู้เรียนสามารถทดลองและพัฒนาทักษะผ่านสถานการณ์จำลอง การเรียนรู้เชิงประยุกต์ซึ่งชุดการเรียนรู้เชิงปฏิบัติช่วยให้ผู้เรียนสามารถเชื่อมโยงแนวคิดเชิงทฤษฎีกับการใช้งานจริง และการพัฒนานวัตกรรม ชุดเหล่านี้ช่วยกระตุ้นความคิดสร้างสรรค์ในการพัฒนาโซลูชันใหม่

2.5.3 การประยุกต์ใช้ในระบบการศึกษา

ชุดการเรียนรู้เชิงปฏิบัติถูกนำมาใช้ในโรงเรียนและสถาบันการศึกษาเพื่อเสริมสร้างการเรียนรู้ที่มีความน่าสนใจและท้าทาย ตัวอย่างเช่น การใช้ชุด โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) เพื่อพัฒนาโครงการด้านความปลอดภัย หรือการใช้ Arduino ในการสร้างระบบควบคุมอัตโนมัติในวิชาวิศวกรรม (Huang et al., 2022)

2.6 งานวิจัยที่เกี่ยวข้อง

Kwon, J., & Park, S. (2022). ได้ศึกษาการนำเทคโนโลยี AI มาใช้ในระบบรักษาความปลอดภัยที่ทันสมัย โดยเฉพาะการตรวจจับภัยคุกคามและการวิเคราะห์ข้อมูลแบบเรียลไทม์ ผลการวิจัยพบว่า AI ช่วยเพิ่มความสามารถในการตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพถึง 95% โดยสามารถตรวจสอบข้อมูลที่มีความซับซ้อนและวิเคราะห์พฤติกรรมผิดปกติได้อย่างรวดเร็ว ระบบที่ขับเคลื่อนด้วย AI ช่วยลดระยะเวลาในการตอบสนองต่อภัยคุกคามและเพิ่มความปลอดภัยให้กับระบบเครือข่าย นอกจากนี้ยังเป็นตัวช่วยสำคัญในการลดข้อผิดพลาดที่เกิดจากมนุษย์ในการตรวจจับภัยคุกคาม

Zhou, H., et al. (2021). ได้เปรียบเทียบประสิทธิภาพของระบบตรวจจับการบุกรุก (IDS) ระหว่างโมเดล Machine Learning และ Deep Learning ผลการวิจัยพบว่าโมเดล Deep Learning มีความแม่นยำสูงสุดถึง 97% ในการตรวจจับการบุกรุกที่มีรูปแบบซับซ้อน อย่างไรก็ตาม โมเดลนี้มีข้อเสียในแง่ของการใช้ทรัพยากรระบบที่สูงกว่า เช่น การประมวลผลและการจัดเก็บข้อมูล ระบบที่ใช้ AI เหล่านี้เหมาะสมสำหรับการใช้งานในสถานการณ์ที่ต้องการความแม่นยำสูง เช่น การรักษาความปลอดภัยของข้อมูลในองค์กรขนาดใหญ่

Lee, C. (2020). ได้ศึกษาการประยุกต์ใช้ AI ในการเรียนการสอนสายอาชีพผ่านกิจกรรมปฏิบัติที่ออกแบบเพื่อเสริมสร้างความเข้าใจในเทคโนโลยี AI ผลการวิจัยแสดงว่านักเรียนที่ใช้โมดูลการเรียนรู้ AI มีความเข้าใจในเทคโนโลยี AI เพิ่มขึ้นถึง 85% และสามารถนำความรู้ไปประยุกต์ใช้ในโครงการปฏิบัติจริงได้อย่างมีประสิทธิภาพ การใช้ AI ในกระบวนการเรียนการสอนยังช่วยให้นักเรียนมีความมั่นใจในทักษะที่ได้รับ และสามารถปรับตัวต่อการเปลี่ยนแปลงของเทคโนโลยีในสายงานอาชีพ

Smith, A., & Taylor, B. (2023). ได้วิเคราะห์ความท้าทายในการบูรณาการ AI ในการฝึกอบรมสายอาชีพ เช่น ความพร้อมของครูผู้สอน ข้อจำกัดของทรัพยากร และการออกแบบหลักสูตรที่เหมาะสม ผลการวิจัยพบว่าการฝึกอบรมครูผู้สอนในด้านเทคโนโลยี AI สามารถลดช่องว่างของความรู้ได้ถึง 70% ซึ่งส่งผลต่อการเพิ่มประสิทธิภาพในการจัดการเรียนการสอนที่เกี่ยวข้องกับ AI การพัฒนาทรัพยากรและการสนับสนุนที่เหมาะสมยังช่วยให้การเรียนการสอนสามารถรองรับความต้องการของอุตสาหกรรมในยุคดิจิทัลได้ดียิ่งขึ้น

Johnson, M., & Wong, Y. (2023). ได้ศึกษาการใช้โมดูลการเรียนรู้ที่ขับเคลื่อนด้วย AI ในการพัฒนาทักษะปฏิบัติของนักเรียนในสายอาชีพ โดยการทดลองเปรียบเทียบระหว่างกลุ่มนักเรียนที่ใช้โมดูล AI และกลุ่มที่ไม่ได้ใช้ ผลการวิจัยแสดงให้เห็นว่านักเรียนที่ใช้โมดูล AI มีพัฒนาการในด้านทักษะปฏิบัติสูงขึ้นอย่างมีนัยสำคัญ โดยคะแนนเฉลี่ยเพิ่มขึ้น 25% เมื่อเทียบกับกลุ่มควบคุม นอกจากนี้ นักเรียนยังรายงานว่าการเรียนรู้ผ่านโมดูล AI ช่วยเพิ่มความเข้าใจในกระบวนการทำงานที่ซับซ้อน และสามารถนำไปปรับใช้ในสถานการณ์จริงได้อย่างมีประสิทธิภาพ

Chen, J., & Liu, S. (2022). ได้ออกแบบและพัฒนา AI Learning Kits ที่เน้นการใช้งานง่ายและราคาประหยัด โดยมุ่งหวังให้นักเรียนสามารถเข้าใจแนวคิดพื้นฐานและการประยุกต์ใช้ AI ในงานปฏิบัติ ผลการทดสอบกับกลุ่มนักเรียนแสดงให้เห็นว่า Learning Kits ช่วยเพิ่มความเข้าใจในเทคโนโลยี AI ได้อย่างชัดเจน พร้อมทั้งได้รับคะแนนความพึงพอใจสูงถึง 92% จากนักเรียน การใช้งาน Learning Kits ยังแสดงให้เห็นถึงศักยภาพในการนำไปพัฒนาเป็นสื่อการเรียนรู้ที่มีประสิทธิภาพและเหมาะสมกับการศึกษาสายอาชีพ

Nguyen, T., & Tran, L. (2021). ได้สำรวจแนวโน้มการฝึกอบรมสายอาชีพที่นำ AI เข้ามาประยุกต์ใช้ โดยเน้นการปรับปรุงการเรียนรู้เชิงปฏิบัติให้ทันสมัยและมีความยืดหยุ่น ผลการสำรวจแสดงให้เห็นว่า AI ช่วยลดช่องว่างระหว่างความรู้ทฤษฎีและการปฏิบัติในสายอาชีพได้ถึง 60% พร้อมทั้งสร้างโอกาสในการพัฒนาทักษะใหม่ที่สำคัญสำหรับการทำงานในอุตสาหกรรม 4.0 งานวิจัยยังเน้นย้ำถึงความสำคัญของการผสมผสาน AI ในระบบการศึกษาเพื่อส่งเสริมการเรียนรู้ตลอดชีวิตและการพัฒนาศักยภาพบุคลากรในอนาคต

Smith, J., & Brown, K. (2023). ได้ศึกษาประสิทธิภาพของการใช้ Gamification ในการเรียนรู้ออนไลน์ โดยมุ่งเน้นผลกระทบต่อ ทักษะคิดและการมีส่วนร่วมของผู้เรียน ผลการวิจัยพบว่ากลุ่มทดลองที่เรียนรู้ผ่านเกมมีพิเคชันมีทักษะคิดเชิงบวกสูงกว่ากลุ่มควบคุม อย่างมีนัยสำคัญ นอกจากนี้ การใช้ องค์ประกอบของเกม เช่น คะแนน บัตรรางวัล และกระดานผู้นำ ยังช่วยเพิ่มแรงจูงใจในการเรียนรู้ถึง 70% งานวิจัยชี้ให้เห็นว่าการออกแบบ Gamification อย่างมีระบบสามารถ ลดอัตราการเรียนกลางคันและเพิ่มความพึงพอใจของผู้เรียน ได้อย่างมีประสิทธิภาพ อีกทั้งยังสนับสนุนให้สถาบันการศึกษา ประยุกต์ใช้ Gamification อย่างเหมาะสมเพื่อพัฒนาการเรียนรู้ในยุคดิจิทัล

บทที่ 3

วิธีดำเนินการวิจัย

การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก เป็นการวิจัยที่บูรณาการเรียนรู้จากรายวิชาอุปกรณ์อิเล็กทรอนิกส์ในระบบรักษาความปลอดภัย เพื่อพัฒนาชุดการเรียนรู้แบบปฏิบัติการของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก และประเมินผลสัมฤทธิ์ความรู้ ทักษะและทัศนคติของผู้เรียนต่อการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน ดังนั้นผู้วิจัยจึงได้ออกแบบวิธีการดำเนินงานวิจัย ซึ่งมีรายละเอียด ดังนี้

3.1 การออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

3.2 การสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย

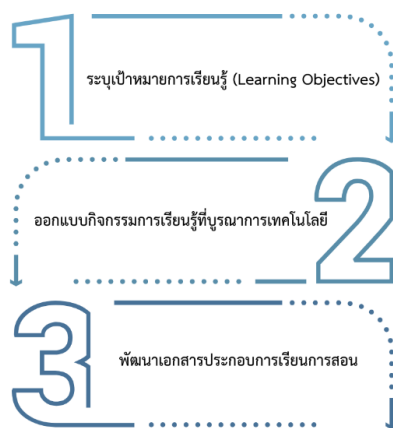
3.3 ขั้นตอนดำเนินการเก็บข้อมูลการวิจัย

3.4 การวิเคราะห์ข้อมูลการวิจัย

3.1 การออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

ผู้วิจัยกำหนดลำดับขั้นตอนในออกแบบการออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก ดังภาพที่ 3-1

การออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัย
ด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก



ภาพที่ 3-1 ขั้นตอนในออกแบบการออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

3.1.1 ระบุเป้าหมายการเรียนรู้ (Learning Objectives) ทั้งด้านความรู้ ทักษะ และทัศนคติ
โดยผู้วิจัยได้ระบุเป้าหมายการเรียนรู้ไว้ดังนี้

ตารางที่ 3-1 เป้าหมายการเรียนรู้ (Learning Objectives) ทั้งด้านความรู้ ทักษะ และทัศนคติ

ด้าน	เป้าหมายการเรียนรู้
ความรู้ (Knowledge)	1. บอกความหมายของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ 2. อธิบายความสำคัญของปัญญาประดิษฐ์ในการตรวจจับการบุกรุก 3. บอกส่วนประกอบสำคัญในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ 4. อธิบายเกี่ยวกับ Machine Learning ในการจดจำบุคคล 5. อธิบายหลักการของระบบ IoT ที่ใช้ในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ 6. อธิบายการทำงานของ AI ในการตรวจจับพฤติกรรมผิดปกติในพื้นที่สาธารณะ 7. อธิบายบทบาทของ Machine Learning และ IoT ในการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ 8. อธิบายปัจจัยที่ส่งผลต่อความแม่นยำของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ AI 9. อธิบายความสำคัญของ Deep Learning ในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ 10. อธิบายความหมายของ Convolutional Neural Networks (CNN) 11. อธิบายหลักการทำงานของ Convolutional Neural Networks (CNN) 12. บอกตัวอย่างสถานการณ์ที่ใช้ AI ในการรักษาความปลอดภัย 13. เปรียบเทียบข้อดีของการใช้ AI กับการใช้มนุษย์ในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์
ทักษะ (Skill)	1. ติดตั้งและเชื่อมต่ออุปกรณ์ในงานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ 2. เขียนโปรแกรมพื้นฐานในงานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สำหรับการตรวจจับการบุกรุก 3. ทดสอบและปรับปรุงระบบรักษาความปลอดภัยให้มีประสิทธิภาพ 4. ปรับแต่งโปรแกรมให้ตอบสนองตามความต้องการ
ทัศนคติ (Attitude)	1. มีทัศนคติเชิงบวกต่อการใช้ AI ในการพัฒนาระบบรักษาความปลอดภัย 2. เห็นคุณค่าและความสำคัญของเทคโนโลยี AI ในการรักษาความปลอดภัย 3. มีความมุ่งมั่นที่จะพัฒนาทักษะในการใช้ AI และเทคโนโลยีที่เกี่ยวข้อง

3.1.2 ออกแบบกิจกรรมการเรียนรู้ที่บูรณาการเทคโนโลยี ผู้วิจัยได้ออกแบบกิจกรรมการเรียนรู้ที่บูรณาการเทคโนโลยีโดยเลือกใช้โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) ในการตรวจจับบุคคล การควบคุมเซอร์โวมอเตอร์เพื่อเปิด-ปิดประตู และการส่งสัญญาณเสียงและแสงเตือน (Buzzer และ LED) รายละเอียดดังนี้

3.1.2.1 โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) สำหรับตรวจจับใบหน้า

3.1.2.2 Microcontroller (Arduino Nano) สำหรับควบคุมระบบ

3.1.2.3 Servomotors สำหรับการควบคุมประตูหรืออุปกรณ์เคลื่อนที่

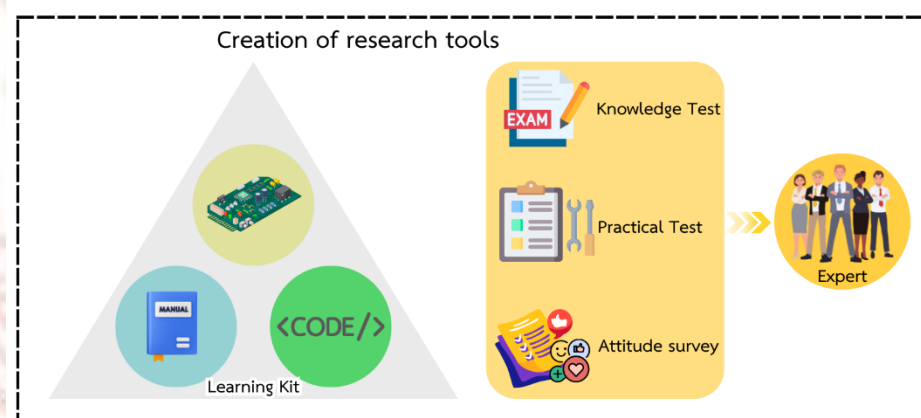
3.1.2.4 Buzzer และ LED สำหรับส่งสัญญาณเตือน

3.1.2.5 โมดูล Wi-Fi (ESP01) สำหรับส่งการแจ้งเตือน

3.1.3 พัฒนาเอกสารประกอบการเรียนการสอน เช่น คู่มือการใช้งาน แผนการจัดการเรียนรู้

3.2 การสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย

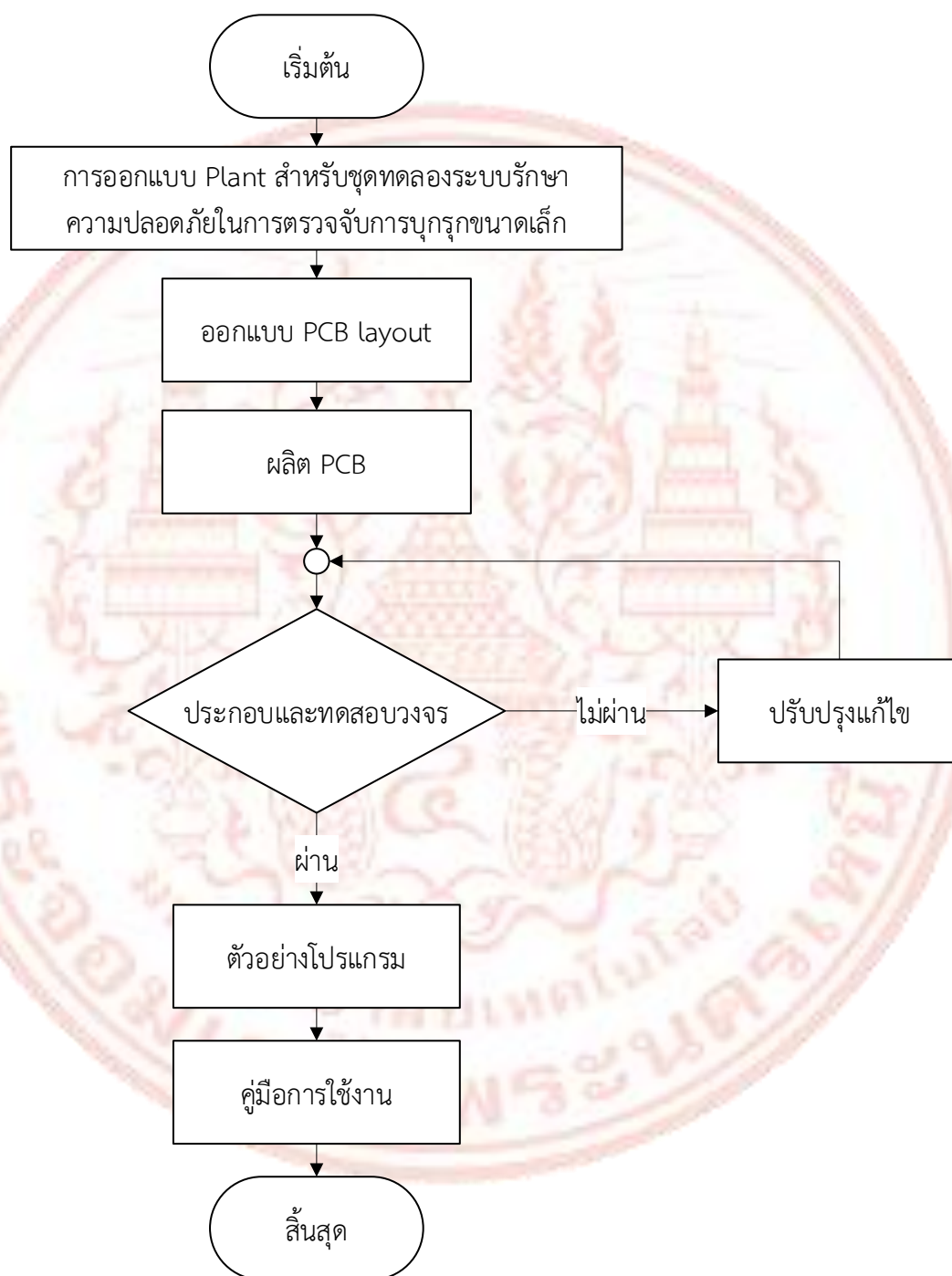
ผู้วิจัยได้ออกแบบชุดการเรียนรู้ขั้นตอนต่อมาเป็นการการสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย โดยผู้วิจัยได้มีการกำหนดลำดับขั้นตอนในการสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัยดังภาพที่ 3-2



ภาพที่ 3-2 การสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย

3.2.1 ชุดการเรียนรู้เชิงปฏิบัติ ผู้วิจัยได้ออกแบบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกจากข้อมูลที่ได้วิเคราะห์ถึงเป้าหมายในการเรียนรู้ (Learning Objectives) ทั้งด้านความรู้ ทักษะ และทัศนคติรวมถึงการเรียนรู้ที่บูรณาการเทคโนโลยีนำมาซึ่งการสร้างชุดการเรียนรู้เชิงปฏิบัติเพื่อให้ผู้เรียนได้รับประสบการณ์ตรง ในชุดการเรียนรู้เชิงปฏิบัติประกอบไปด้วย ชุดการเรียนรู้ที่ประกอบด้วยชุดการทดลอง (Learning Kit)

คู่มือการใช้งาน และตัวอย่างโปรแกรมสำหรับการตรวจจับการบุกรุกโดยผู้วิจัยมีขั้นตอนในการพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยในการตรวจจับการบุกรุก ดังนี้



ภาพที่ 3-3 ขั้นตอนในสร้างชุดการเรียนรู้เชิงปฏิบัติ

จากภาพที่ 3-3 ขั้นตอนในสร้างชุดการเรียนรู้เชิงปฏิบัติ ในส่วนของการออกแบบ โครงสร้างชุดการเรียนรู้ต้องสอดคล้องกับเป้าหมายการเรียนรู้ เช่น บทเรียนทฤษฎีพื้นฐาน (Introduction and Theory) การติดตั้งและเชื่อมต่ออุปกรณ์ (Hardware Setup) การเขียน โปรแกรมควบคุม (Programming) และการทดสอบและปรับปรุงระบบ (Testing and Refinement) ดังนั้นผู้วิจัยจึงเลือกที่จะสร้างชุดการเรียนรู้เชิงปฏิบัติ ที่ประกอบไปด้วย ชุดสำหรับการทดลอง ตัวอย่างโปรแกรมสำหรับการตรวจนับการบุกรุกและคู่มือการใช้งาน

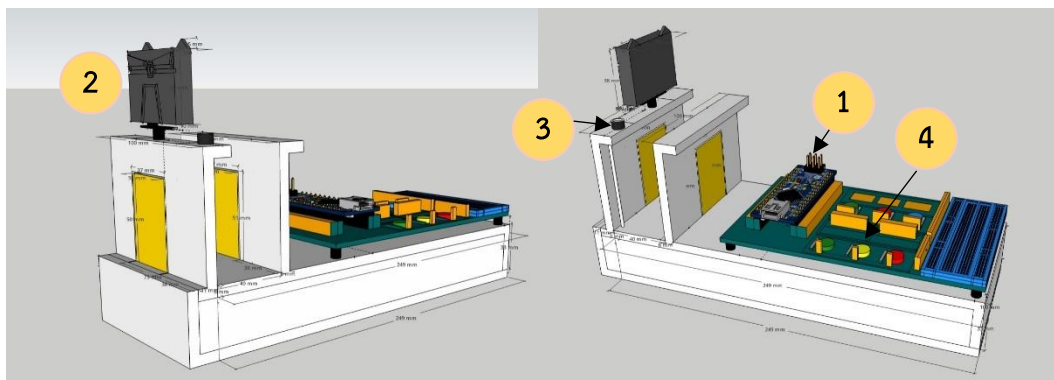
ผู้วิจัยเริ่มต้นจากการออกแบบ Plant สำหรับชุดทดลองระบบรักษาความปลอดภัยในการตรวจนับการบุกรุกขนาดเล็กโดยมี วัตถุประสงค์ของการออกแบบ คือ สร้างชุดทดลองที่สามารถ ใช้ศึกษาการทำงานของระบบรักษาความปลอดภัยที่ตรวจนับการบุกรุก ออกแบบให้มีขนาดกะทัดรัด สามารถเคลื่อนย้ายและติดตั้งได้ง่าย ใช้เซนเซอร์และอุปกรณ์ที่หาได้ง่ายหรือมีอยู่แล้วและมีต้นทุนต่ำ มาประยุกต์ใช้ และรองรับการพัฒนาปรับแต่งซอฟต์แวร์เพื่อทดลองอัลกอริธึมต่าง ๆ

องค์ประกอบของ Plant โดยโครงสร้างทางกายภาพ ผู้วิจัยเลือกใช้แผ่นพลาสติก (Plaswood) เป็นฐานรองอุปกรณ์ ติดตั้งแผ่น PCB ที่ออกแบบเพื่อความสะดวกในการใช้งาน มีพื้นที่ ติดตั้งเซนเซอร์ในตำแหน่งที่เหมาะสมและมีช่องสำหรับเชื่อมต่อสายไฟและพอร์ตสื่อสารและ อุปกรณ์ ที่ใช้ใน Plant ดังแสดงในตารางที่ 3-2

ตารางที่ 3-2 อุปกรณ์ที่ใช้ใน Plant

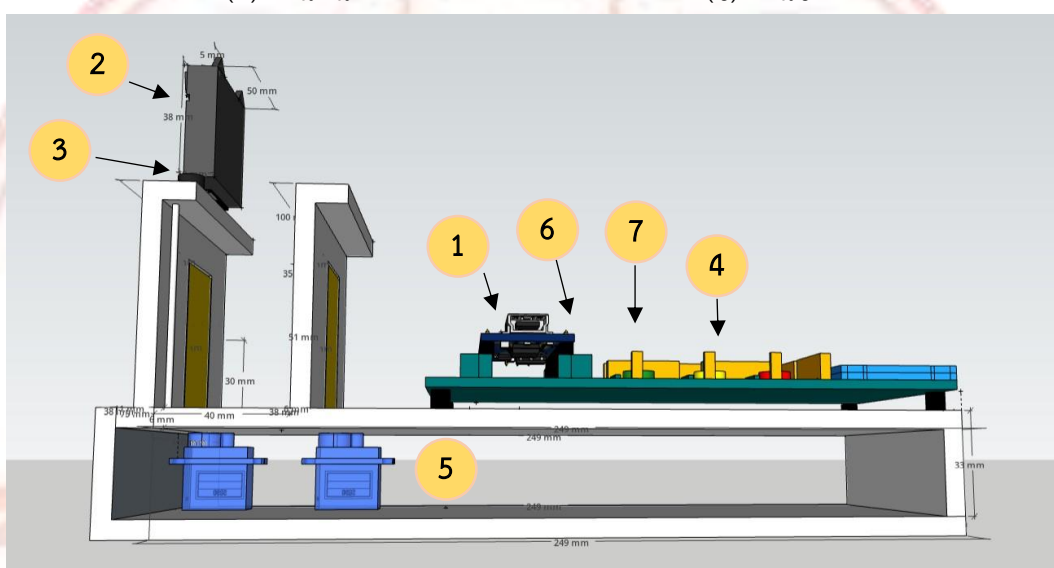
หมายเลข	หมวดหมู่	อุปกรณ์ที่ใช้	ฟังก์ชัน
1	หน่วยประมวลผล	Arduino Nano	บอร์ดควบคุมการทำงาน
2	เซนเซอร์ตรวจจับ	HuskyLens	ตรวจจับใบหน้าหรือวัตถุ
3	ระบบแจ้งเตือน	Buzzer	ส่งเสียงเตือนเมื่อพบการบุกรุก
4	ระบบแจ้งเตือน	LED	แสดงสถานะระบบ
5	ระบบควบคุมการเข้าถึง	Servomotor	ควบคุมการเปิด-ปิดประตู
6	การเชื่อมต่อ	Module Wi-Fi (ESP01)	ส่งข้อมูลไปยัง Dashboard หรือ Cloud
7	แหล่งพลังงาน	Power Supply	จ่ายไฟให้กับอุปกรณ์ 6-9V

จากวัตถุประสงค์และองค์ประกอบต่างๆของ Plant ผู้วิจัยได้ทำการออกแบบด้วย โปรแกรม Sketup online ดังแสดงในภาพที่ 3-4



(ก) ด้านหน้า

(ข) ด้านข้าง



(ค) โครงสร้างภายใน

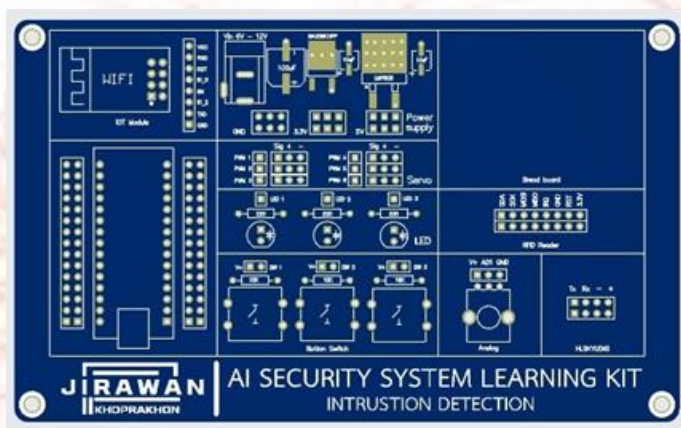
ภาพที่ 3-4 Planชุดทดลองระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI ในการตรวจจับการบุกรุกขนาดเล็ก

ต่อมาผู้วิจัยได้ออกแบบแผ่นวงจรพิมพ์ (Printed Circuit Board - PCB) สำหรับชุดการทดลอง การออกแบบ PCB สำหรับชุดการทดลองเป็นขั้นตอนสำคัญในการพัฒนาชุดทดลองที่พร้อมใช้งาน เพื่อให้ผู้เรียนสามารถประกอบและใช้งานได้อย่างสะดวก รวมถึงเพิ่มความน่าสนใจในการเรียนรู้เกี่ยวกับระบบอิเล็กทรอนิกส์และปัญญาประดิษฐ์ (AI) โดยกระบวนการออกแบบและสร้าง PCB สามารถอธิบายได้ดังนี้

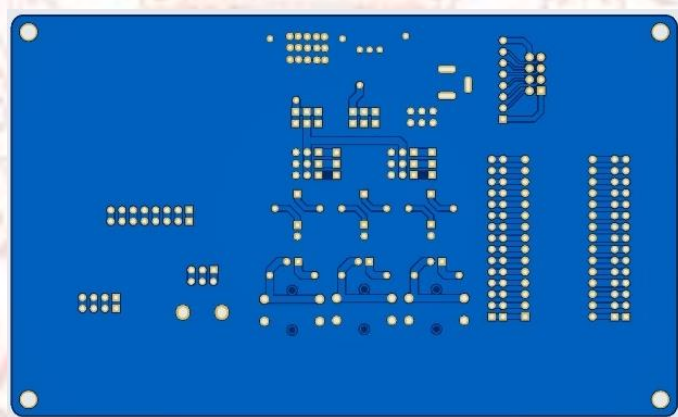
กำหนดเป้าหมายและข้อกำหนดของ PCB โดยเป้าหมายคือการออกแบบ PCB ที่รองรับการใช้งานร่วมกับ โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens), Arduino Nano เซ็นเซอร์, และอุปกรณ์เสริม เช่น เซอร์โวมอเตอร์, Buzzer, และ LED ข้อกำหนด คือ ขนาดต้องเหมาะสมกับ

พื้นที่การใช้งาน รองรับการเชื่อมต่ออุปกรณ์ผ่าน Header Pins หรือ Connector รองรับการจ่ายไฟจาก USB หรือ Power Supply และต้องออกแบบวงจรให้ปลอดภัยต่อการใช้งานของผู้เรียน

การออกแบบ PCB Layout ในการจัดวางองค์ประกอบ ของ PCB วาง Arduino และ โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) ในตำแหน่งที่สะดวกต่อการต่ออุปกรณ์ เว้นระยะห่างระหว่างเส้นลายวงจรให้เพียงพอ ใช้สายไฟขนาดใหญ่สำหรับการจ่ายไฟและสายกราวด์ และเลือกเส้นทางสายสัญญาณให้สั้นที่สุดสำหรับสัญญาณที่ไวต่อการรบกวน โดย Layout เป็นไปดัง ภาพที่ 3-5



(ก) ด้านหน้า PCB

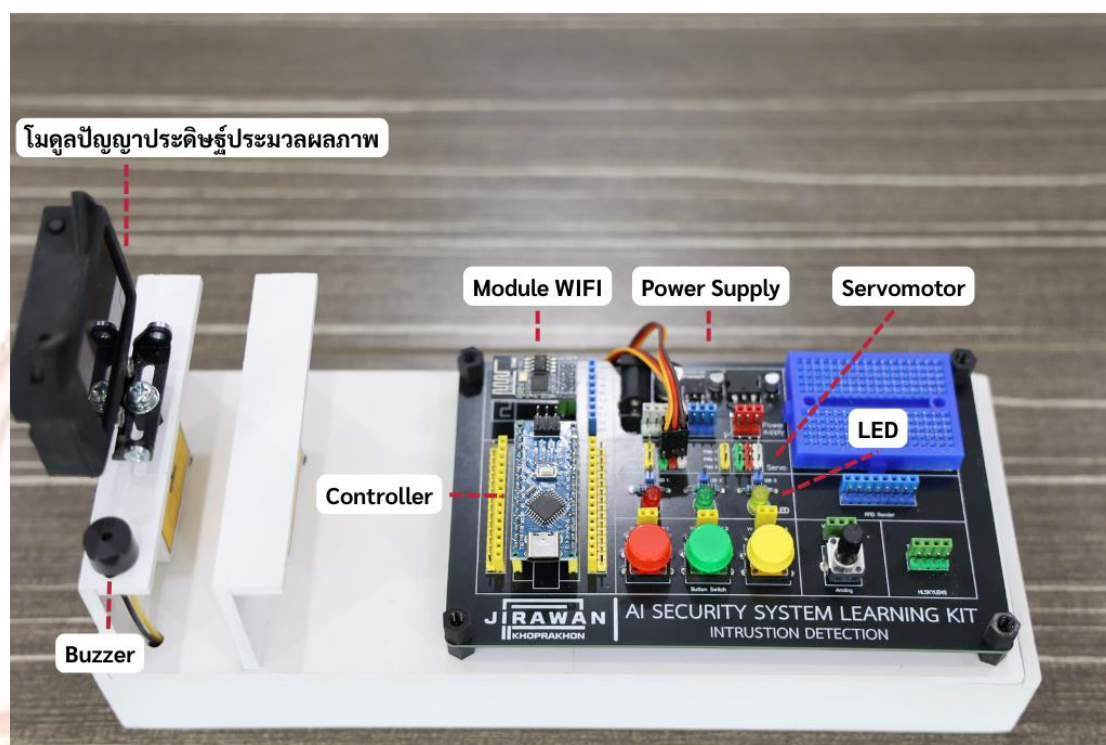


(ข) ด้านหลัง PCB

ภาพที่ 3-5 PCB Layout

ในการผลิต PCB ผู้วิจัยได้สร้าง Gerber File สร้างไฟล์ที่จำเป็นสำหรับการผลิต PCB และสั่งผลิต PCB โดยเลือกผู้ผลิต PCB ที่สามารถผลิตในขนาดเล็กสำหรับชุดการเรียนรู้

การประกอบและทดสอบ ประกอบและบัดกรีอุปกรณ์ทั้งหมดบน PCB และตรวจสอบความถูกต้องของการเชื่อมต่อ โดยทดสอบการจ่ายไฟและการทำงานของวงจร และตรวจสอบการเชื่อมต่อกับ โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens), Arduino, และเซ็นเซอร์



ภาพที่ 3-6 การประกอบชุดทดลองระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกขนาดเล็ก

ผู้วิจัยได้ทดสอบชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกสำเร็จและทำการทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ความสำเร็จในการติดตั้งฮาร์ดแวร์โดยผู้เรียน และความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง

ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI สามารถอ้างอิงได้จากงานของ Kwon, J., & Park, S. (2022) ที่ศึกษาการใช้ AI ในระบบรักษาความปลอดภัย โดยเน้นการวิเคราะห์ความแม่นยำในการตรวจจับการบุกรุก ซึ่งระบบ AI ใช้เกณฑ์ความแม่นยำ (Accuracy) ในการประเมินผลโดยใช้สูตรดังนี้

$$\text{Accuracy (\%)} = \frac{\text{จำนวนการตรวจจับที่ถูกต้อง}}{\text{จำนวนการตรวจจับทั้งหมด}} \times 100 \quad (3-1)$$

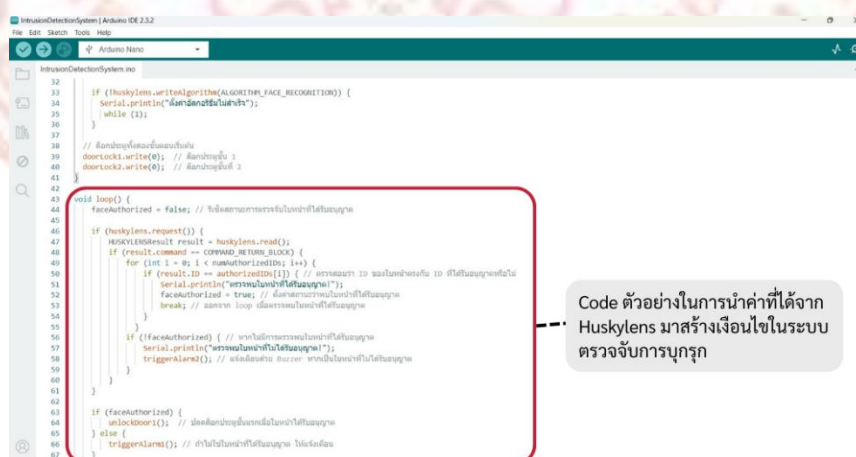
ความสำเร็จในการติดตั้งฮาร์ดแวร์ของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI โดยนักศึกษา สามารถอ้างอิงได้จากงานวิจัยของ Johnson, M., & Wong, Y. (2023) ที่ศึกษาการพัฒนาทักษะปฏิบัติของนักเรียนผ่านโมดูลการเรียนรู้ AI โดยเน้นการประเมินผลจากความสำเร็จในการปฏิบัติจริง เช่น การติดตั้งอุปกรณ์ โดยใช้สูตรดังนี้

$$\text{Success Rate} = \frac{\text{จำนวนผู้ที่ติดตั้งสำเร็จจำนวนผู้เข้าร่วมทั้งหมด}}{\text{จำนวนผู้เข้าร่วมทั้งหมด}} \times 100 \quad (3-2)$$

ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง สามารถอ้างอิงได้จากงานของ Nguyen, T., & Tran, L. (2021) ที่สำรวจการใช้งาน AI ในสถานการณ์จำลองเพื่อวัดความแม่นยำของระบบในสถานการณ์ต่าง ๆ ที่จำลองสภาพแวดล้อมจริง โดยใช้สูตรดังนี้

$$\text{Scenario Accuracy} = \frac{\text{จำนวนการทำงานที่ถูกต้องในสถานการณ์}}{\text{จำนวนการทดลองทั้งหมด}} \times 100 \quad (3-3)$$

หลังจากการทดสอบแล้ว ผู้วิจัยได้สร้างตัวอย่างโปรแกรมสำหรับการตรวจจับการบุกรุกขึ้นดังภาพที่ 3-7 ที่เป็นโค้ดตัวอย่างในการนำค่าที่ได้จากโมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens) มาสร้างเงื่อนไขในระบบ



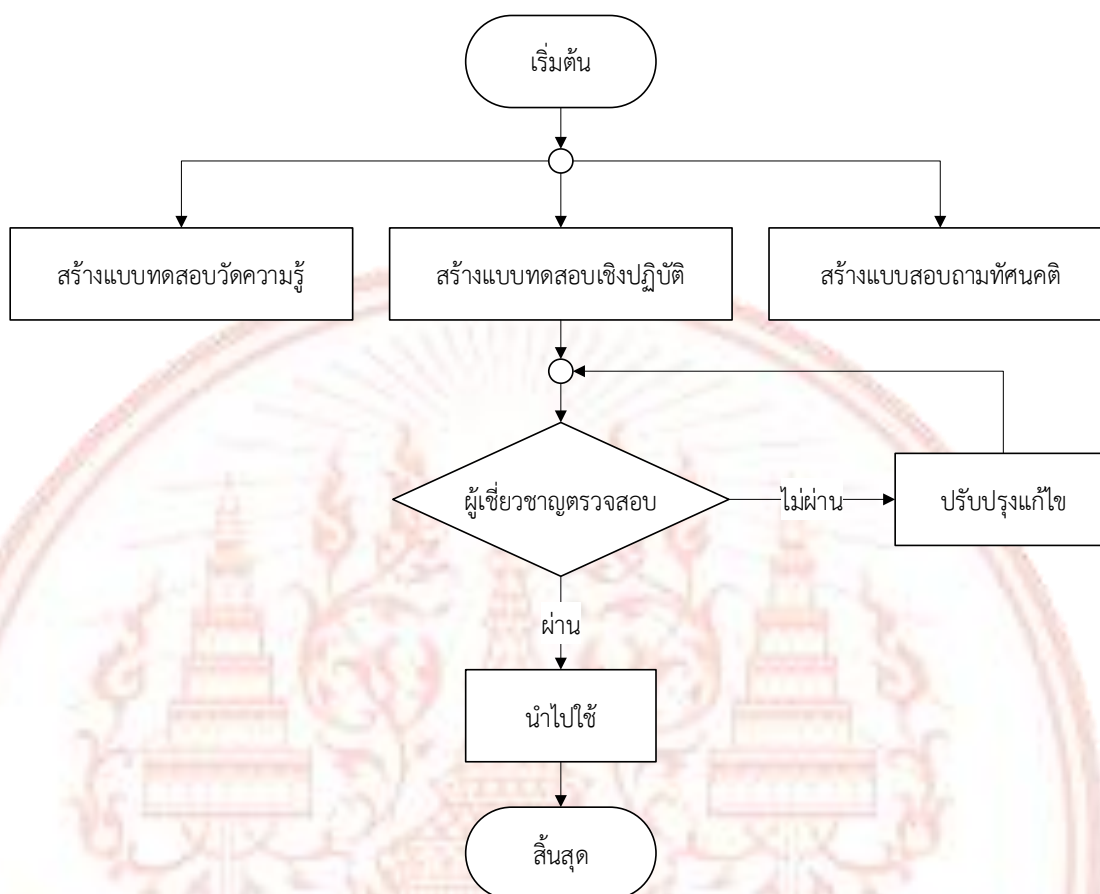
ภาพที่ 3-7 ตัวอย่างโปรแกรมสำหรับการตรวจจับการบุกรุก

ขั้นตอนต่อมาผู้วิจัยได้จัดทำคู่มือการใช้งานชุดการเรียนรู้เชิงปฏิบัติของระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก ดังภาพที่ 3-8



ภาพที่ 3-8 คู่มือการใช้งาน

ผู้วิจัยได้ออกแบบชุดการเรียนรู้แล้วเสร็จแล้วนั้น ขั้นตอนต่อมาเป็นการสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัย โดยผู้วิจัยได้มีการกำหนดลำดับขั้นตอนในการสร้างและการตรวจสอบคุณภาพของเครื่องมือที่ใช้ในการวิจัยดังภาพที่ 3-9



ภาพที่ 3-9 ขั้นตอนการสร้างเครื่องมือสำหรับการประเมิน

โดยเครื่องมือสำหรับการประเมินทั้งหมด ผู้วิจัยได้ทำหนังสือขอความอนุเคราะห์ผู้เชี่ยวชาญในการประเมินเครื่องมือ ผู้วิจัยได้กำหนดคุณสมบัติของผู้ที่จะมาประเมิน โดยต้องมีคุณสมบัติเป็นผู้ที่มีความเชี่ยวชาญ หรือ มีประสบการณ์สอนในเรื่องที่เกี่ยวข้อง ไม่น้อยกว่า 3 ปี จำนวน 5 ท่าน มีรายชื่อดังตารางที่ 3-3

ตารางที่ 3-3 ข้อมูลผู้เชี่ยวชาญในการประเมินความสอดคล้องของเครื่องมือสำหรับการประเมิน

ลำดับ	ชื่อ-สกุล	ตำแหน่ง	สังกัด
1	ผศ.ดร.ปรกรณ์เกียรติ์ เสวตเมธิกุล	อาจารย์ประจำ ภาควิชา ครุศาสตร์ อุตสาหกรรม	ภาควิชาครุศาสตร์อุตสาหกรรม คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีราชมงคล ธัญบุรี
2	ผศ.ชลดา ปานสง		

ลำดับ	ชื่อ-สกุล	ตำแหน่ง	สังกัด
3	นายศุภกฤต รื่องาม	อาจารย์	สำนักงานห้องเรียนวิศว์-วิทย์ สถาบันการเรียนรู้ มหาวิทยาลัย เทคโนโลยีพระจอมเกล้าธนบุรี
4	นางกฤษณา เอ็งฉุน	ครู วิทยฐานะครู ชำนาญการพิเศษ	วิทยาลัยเทคนิคนครนายก
5	นายยงยุทธ จันทรัตน์	ครู วิทยฐานะครู ชำนาญการพิเศษ	วิทยาลัยเทคนิคสระบุรี

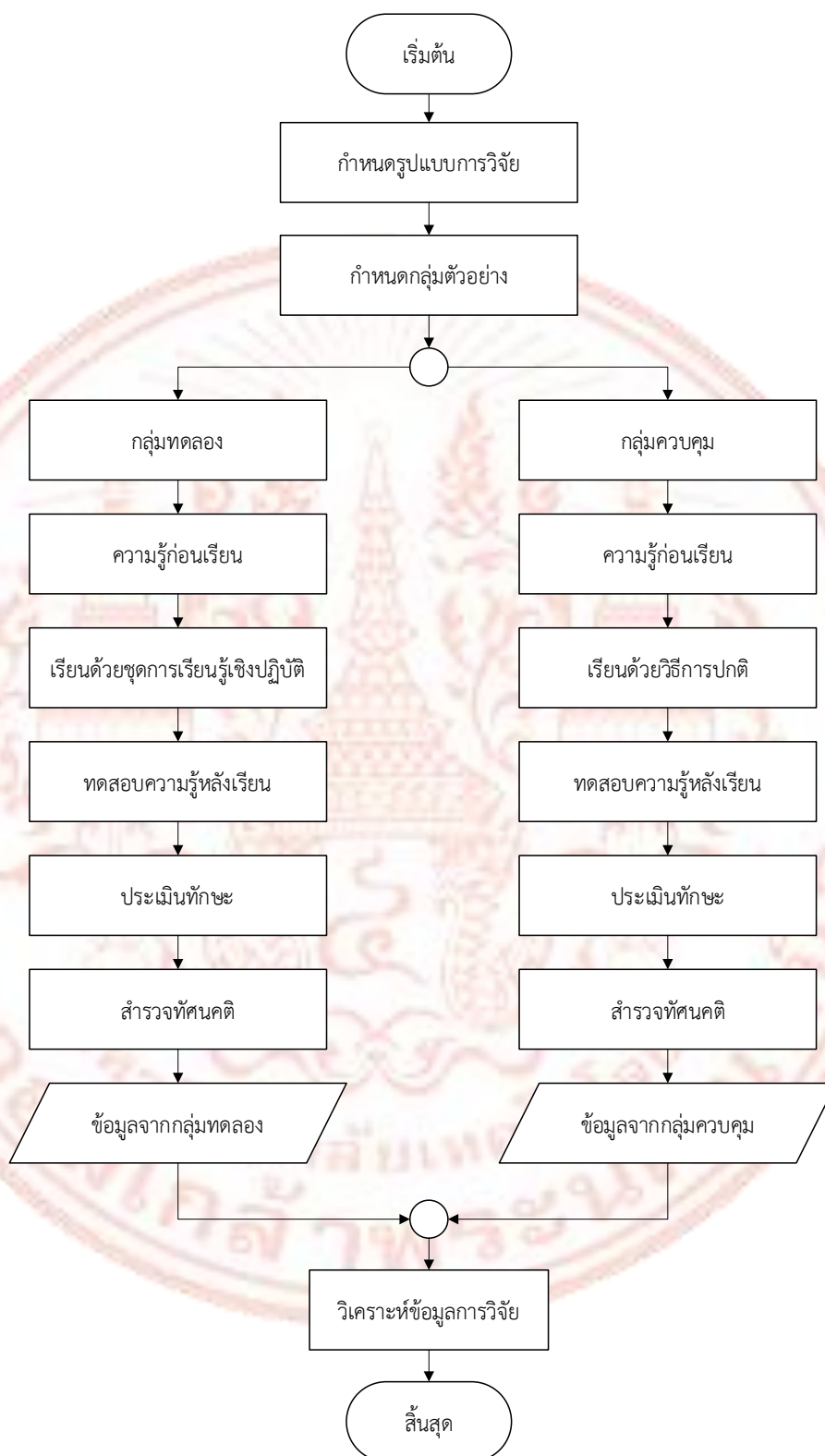
3.2.2 แบบทดสอบวัดความรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก ในการวิจัยครั้งนี้ ผู้วิจัยได้พัฒนาแบบทดสอบชนิดเลือกตอบ 4 ตัวเลือก จำนวน 20 ข้อ เพื่อวัดความรู้ของผู้เรียนให้สอดคล้องกับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้ หลังจากสร้างแบบทดสอบเสร็จสิ้น ได้ดำเนินการขอความอนุเคราะห์จากผู้เชี่ยวชาญเพื่อประเมินค่าความสอดคล้องของข้อคำถาม

3.2.3 แบบทดสอบเชิงปฏิบัติระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก เป็นแบบทดสอบเชิงปฏิบัติ (Practical Test) โดยมีวัตถุประสงค์เพื่อวัดทักษะการปฏิบัติงานในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก ซึ่งเน้นการปฏิบัติจริง เช่น การตั้งค่าฮาร์ดแวร์ การพัฒนาและปรับปรุงโปรแกรม การทดสอบในสถานการณ์ต่าง ๆ และการแก้ไขปัญหาเพื่อเพิ่มประสิทธิภาพของระบบ แบบประเมินผลใช้รูปแบบรูบริก (Rubric Score) ในการประเมินโดยแบ่งเป็น 5 ระดับในการประเมิน โดยมีรายละเอียดการประเมินจากวัตถุประสงค์เชิงพฤติกรรมที่สอดคล้องกับการทำแบบปฏิบัติงานที่ผู้สอนกำหนดให้ และการตรวจผลการประเมินด้านทักษะการปฏิบัติงานของผู้เรียนในลักษณะแบบรายการตรวจสอบ (Checklist)

3.2.4 แบบสอบถามทัศนคติของผู้เรียนการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุกไปใช้งาน เป็นรูปแบบสอบถามระดับความเห็นแบ่งออกเป็น 5 ระดับในการประเมิน โดยแบ่งการประเมินออกเป็น 3 ด้าน คือ 1. ด้านทัศนคติเชิงบวกต่อการใช้ AI ในการพัฒนาระบบรักษาความปลอดภัย 2. คุณค่าและความสำคัญของเทคโนโลยี AI ในการรักษาความปลอดภัย และ 3. ความมุ่งมั่นที่จะพัฒนาทักษะในการใช้ AI และเทคโนโลยีที่เกี่ยวข้อง

3.3 ขั้นตอนดำเนินการเก็บข้อมูลการวิจัย

เมื่อผู้วิจัยสร้างเครื่องมือวิจัย ที่ผ่านการตรวจสอบคุณภาพจากผู้เชี่ยวชาญ และได้เครื่องมือที่ใช้ในการวิจัยที่สมบูรณ์แล้ว ผู้วิจัยได้ดำเนินการเก็บข้อมูลการวิจัย โดยได้มีการกำหนดลำดับขั้นตอนในการเก็บข้อมูล ดังภาพที่ 3-10 พร้อมทั้งอธิบายรายละเอียดดังนี้



ภาพที่ 3-10 ผังงานขั้นตอนในการเก็บข้อมูลการวิจัย

3.3.1 กำหนดรูปแบบการวิจัย

ผู้วิจัยได้กำหนดรูปแบบการวิจัยแบบ Quasi-Experimental Design โดยใช้ Modified Pretest-Posttest Control Group Design เป็นการดัดแปลงแนวคิดมาจาก Campbell & Stanley (1963) และพัฒนาโดย Shadish, Cook, & Campbell (2002) ในงานวิจัยด้าน Quasi-Experimental Research เพื่อให้เหมาะสมกับงานวิจัยที่ไม่สามารถวัดบางตัวแปรก่อนเรียนและวัดเฉพาะบางตัวแปรหลังเรียนเท่านั้น

E	O1	X	O2
C	O1		O2

โดย

E หมายถึง กลุ่มทดลอง (Experimental Group) เรียนด้วยชุดการเรียนรู้เชิงปฏิบัติ

C หมายถึง กลุ่มควบคุม (Control Group) เรียนด้วยการสอนแบบปกติ

X หมายถึง ใช้ชุดการเรียนรู้ที่พัฒนาขึ้น

O1 หมายถึง การวัดผลก่อนเรียน (Pretest) เฉพาะด้านความรู้

O2 หมายถึง การวัดผลหลังเรียน (Posttest) ด้านความรู้ ทักษะการปฏิบัติงาน และ

ทัศนคติ

3.3.2 ผู้เข้าร่วมการวิจัย

การดำเนินการวิจัย ผู้วิจัยเลือกใช้ผู้เข้าร่วมการวิจัยคือ นักศึกษาระดับประกาศนียบัตรวิชาชีพ (ปวช.) ชั้นปีที่ 3 สาขาอิเล็กทรอนิกส์ จำนวน 40 คน ที่ลงทะเบียนเรียนในรหัสวิชา 20105-2025 รายวิชาอุปกรณ์อิเล็กทรอนิกส์ในระบบรักษาความปลอดภัย โดยแบ่งออกเป็น 2 ประเภทคือ

3.3.1 กลุ่มทดลอง โดยมีจำนวน 20 คน จะใช้วิธีการเรียนการสอนโดยใช้ชุดการเรียนรู้เชิงปฏิบัติ แล้วทำการทดสอบผลสัมฤทธิ์ทางการเรียนจากการวัดความรู้ ทักษะการปฏิบัติตามโจทย์ที่ผู้สอนกำหนด และทัศนคติโดยใช้เกณฑ์การประเมินแบบตรวจสอบรายการและการประเมินทัศนคติของผู้เรียน

3.3.2 กลุ่มควบคุม จำนวน 20 คน จะใช้วิธีการเรียนการสอนในรูปแบบทั่วไป คือการบรรยาย โดยเก็บข้อมูลจากการทดสอบผลสัมฤทธิ์ทางการเรียนจากการวัดความรู้ ทักษะการปฏิบัติตามโจทย์ที่ผู้สอนกำหนด และทัศนคติโดยใช้เกณฑ์การประเมินแบบตรวจสอบรายการและการประเมินทัศนคติของผู้เรียน

3.3.3 การเก็บข้อมูลวิจัย

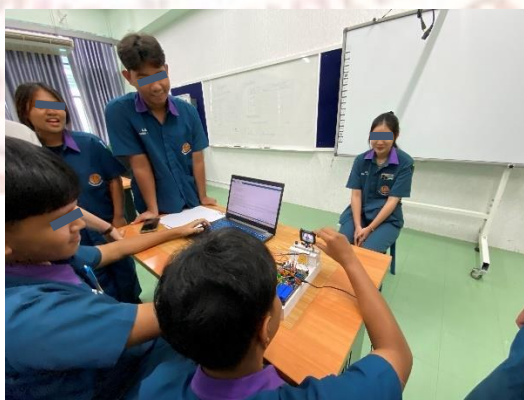
3.3.3.1 เก็บข้อมูลการวิจัยกับผู้เรียนกลุ่มทดลอง แบ่งออกเป็น 2 ขั้นตอน โดยขั้นตอนที่ 1 ผู้วิจัยได้ทำการทดสอบความรู้ก่อนการเรียน หลังจากนั้นแนะนำการใช้งานชุดการเรียนรู้

เชิงปฏิบัติ เรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกให้กับผู้เรียนกลุ่มทดลอง แสดงดังภาพที่ 3-11



ภาพที่ 3-11 เก็บข้อมูลการวิจัยกับผู้เรียนกลุ่มทดลอง

ผู้วิจัยกำหนดเวลา 180 นาที ตามแผนการสอนในการให้ความรู้แก่ผู้เรียนกลุ่มทดลอง โดยการใช้ชุดการเรียนรู้ เริ่มจากการให้ความรู้เรื่องหลักการทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ การปฏิบัติงานตั้งแต่การติดตั้งระบบ และการเขียนโปรแกรมควบคุม ปรับปรุงการทำงานของระบบ ตามใบงานการทดลองประกอบการเรียนรู้เมื่อเสร็จสิ้นกระบวนการ ทำแบบวัดความรู้ (ทดสอบหลังเรียน) ต่อไปคือกระบวนการในการทดสอบทักษะ โดยใช้แบบทดสอบเชิงปฏิบัติ และประเมินคะแนนแบบรูปลิก และทำแบบสอบถามด้านทัศนคติในการนำระบบความปลอดภัยไปงานภาพบรรยากาศการเก็บข้อมูลการวิจัย แสดงดังภาพที่ 3-11 และภาพที่ 3-12



ภาพที่ 3-12 ภาพบรรยากาศการเก็บข้อมูลการวิจัย

3.3.3.2 เก็บข้อมูลการวิจัยกับผู้เรียนกลุ่มควบคุม ในส่วนนี้ผู้วิจัยใช้วิธีการจัดการเรียนการสอนแบบปกติ โดยมีลักษณะคล้ายกับกลุ่มทดลอง เริ่มจากการให้ผู้เรียนกลุ่มควบคุมทำแบบวัดความรู้ (ทดสอบก่อนเรียน) บรรยายเนื้อหาในชั้นเรียน และทำแบบวัดความรู้ (ทดสอบหลังเรียน) และทำการทดสอบทักษะโดยใช้แบบทดสอบเชิงปฏิบัติ และประเมินคะแนนแบบรูปลิก และทำแบบสอบถามด้านทัศนคติในการนำระบบความปลอดภัยไปงาน

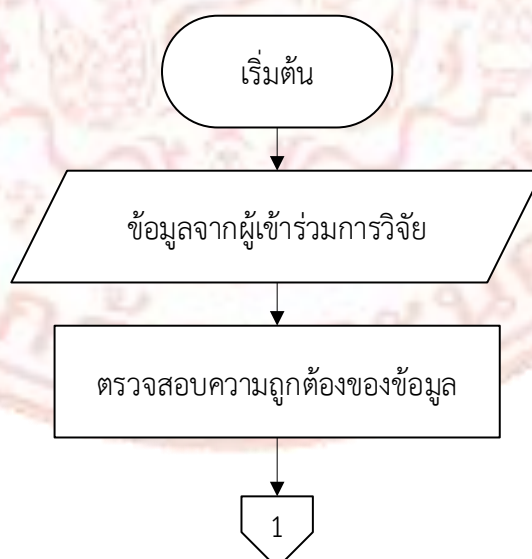
จากขั้นตอนดำเนินการเก็บข้อมูลการวิจัยโดยสรุปแล้วสามารถเข้าใจโครงสร้างการวิจัยเป็นไปตามตารางที่ 3-4

ตารางที่ 3-4 สรุปโครงสร้างการวิจัย

ด้าน	Pretest (ก่อนเรียน)	Posttest (หลังเรียน)	ผู้เข้าร่วมการวิจัย
ความรู้	วัด	วัด	ทั้งกลุ่มทดลองและควบคุม
ทักษะการปฏิบัติ	ไม่วัด	วัด	ทั้งกลุ่มทดลองและควบคุม
ทัศนคติ	ไม่วัด	วัด	ทั้งกลุ่มทดลองและควบคุม

3.4 การวิเคราะห์ข้อมูลการวิจัย

หลังจากที่ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลการวิจัยเกี่ยวกับการพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกเสร็จสิ้น ผู้วิจัยได้นำข้อมูลที่รวบรวมมาเข้าสู่กระบวนการวิเคราะห์ข้อมูลการวิจัยตามลำดับขั้นตอนดังภาพที่ 3-13



ภาพที่ 3-13 กระบวนการวิเคราะห์ข้อมูลการวิจัย



จากภาพที่ 3-13 เป็นกระบวนการวิเคราะห์ข้อมูลการวิจัย โดยมีขั้นตอนต่างๆดังรายละเอียดดังนี้

3.2.1 ตรวจสอบความถูกต้องของข้อมูล ผู้วิจัยเริ่มต้นด้วยการตรวจสอบข้อมูลที่ได้จากการเก็บรวบรวม เพื่อให้แน่ใจว่าข้อมูลครบถ้วนและถูกต้อง ไม่มีข้อผิดพลาดหรือข้อมูลสูญหาย ทั้งในส่วน

ของผลการทดสอบประสิทธิภาพของชุดการเรียนรู้และข้อมูลการประเมินจากผู้เข้าร่วมการวิจัย เช่น แบบทดสอบก่อนเรียน-หลังเรียน แบบประเมินทักษะ และแบบประเมินทัศนคติของผู้เรียน

3.2.2 การจัดหมวดหมู่ข้อมูล ข้อมูลถูกจัดหมวดหมู่ตามหัวข้อหลักที่เกี่ยวข้อง เช่น ผลการสร้างชุดการเรียนรู้ ผลการทดสอบความรู้ก่อนและหลังเรียน ทักษะการปฏิบัติงาน และทัศนคติของผู้เรียน เพื่อให้ง่ายต่อการนำไปวิเคราะห์เชิงสถิติ

3.2.3 วิเคราะห์ข้อมูลเชิงพรรณนา (Descriptive Statistics) ผู้วิจัยคำนวณสถิติพื้นฐาน เช่น ค่าเฉลี่ย (Mean), ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) และเปอร์เซ็นต์ เพื่อสรุปผลการประเมินประสิทธิภาพของชุดการเรียนรู้ เช่น ความแม่นยำของ โมดูลปัญญาประดิษฐ์ประมวลผลภาพ (HuskyLens), เวลาตอบสนองของเซอร์โวมอเตอร์ และอัตราความสำเร็จในการติดตั้งอุปกรณ์โดยผู้เรียน

3.2.4 วิเคราะห์ความแตกต่างเชิงสถิติ (Inferential Statistics) ผู้วิจัยใช้การทดสอบทางสถิติที่เหมาะสม เช่น

3.2.4.1. Mann-Whitney U Test ใช้ในการเปรียบเทียบคะแนนความรู้และทักษะของกลุ่มทดลองและกลุ่มควบคุม เพื่อพิจารณาความแตกต่างอย่างมีนัยสำคัญทางสถิติระหว่างสองกลุ่ม

3.2.4.2. การคำนวณค่า IOC (Index of Item-Objective Congruence) ตามแนวทางของ Rovinelli & Hambleton (1976) ใช้ในการประเมินความสอดคล้องของแบบประเมินความรู้ ทักษะ และทัศนคติกับวัตถุประสงค์ของการวิจัย

3.2.5 วิเคราะห์และแปลผลข้อมูลเชิงคุณภาพ (Qualitative Data Analysis) สำหรับความคิดเห็นเพิ่มเติมจากผู้เรียนและผู้เชี่ยวชาญ ผู้วิจัยนำข้อมูลเหล่านี้มาวิเคราะห์เชิงคุณภาพเพื่อระบุจุดเด่น จุดที่ต้องปรับปรุง และข้อเสนอแนะในการพัฒนาชุดการเรียนรู้ต่อไป

3.2.6 สรุปผลการวิเคราะห์ ผู้วิจัยจัดทำสรุปผลการวิเคราะห์ในรูปแบบตาราง กราฟ และข้อความบรรยาย เพื่อแสดงผลการวิจัยอย่างชัดเจน เช่น การแสดงตารางเปรียบเทียบคะแนนความรู้ก่อนและหลังเรียนของกลุ่มทดลองและกลุ่มควบคุม รวมถึงผลการประเมินทัศนคติ

3.2.7 อภิปรายผลการวิจัย ผู้วิจัยนำผลการวิเคราะห์ที่ได้มาเปรียบเทียบกับงานวิจัยก่อนหน้า พร้อมทั้งอภิปรายถึงความสำคัญของผลการวิจัยต่อการพัฒนาการเรียนรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์

3.2.8 ข้อเสนอแนะสำหรับการวิจัยในอนาคต จากข้อมูลที่วิเคราะห์ ผู้วิจัยสรุปข้อเสนอแนะสำหรับการนำผลการวิจัยไปประยุกต์ใช้ และแนะนำประเด็นการวิจัยเพิ่มเติมที่เกี่ยวข้อง

บทที่ 4

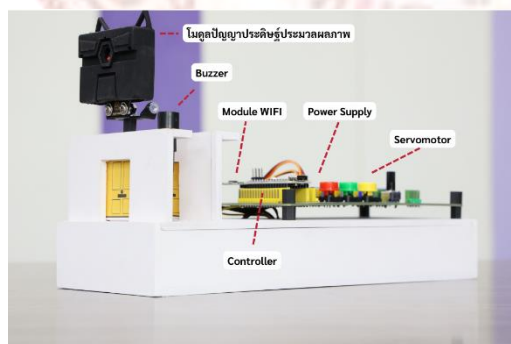
ผลการวิจัย

การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก เป็นการวิจัยที่บูรณาการเรียนรู้จากรายวิชาอุปกรณ์อิเล็กทรอนิกส์ในระบบรักษาความปลอดภัย เพื่อพัฒนาชุดการเรียนรู้แบบปฏิบัติการของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก และประเมินผลสัมฤทธิ์ความรู้ ทักษะและทัศนคติของผู้เรียนต่อการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน โดยที่ผลการวิเคราะห์ออกเป็นหัวข้อดังนี้

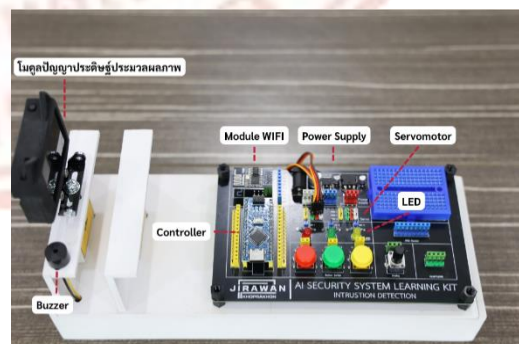
- 4.1 ผลการสร้างชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก
- 4.2 ผลการเปรียบเทียบผลการประเมินด้านความรู้ก่อนเรียนและหลังเรียน
- 4.3 ผลการประเมินทักษะการปฏิบัติงานของผู้เรียนของกลุ่มทดลองและกลุ่มควบคุม
- 4.4 ผลการประเมินทัศนคติของผู้เรียนที่มีต่อการนำระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ ในการตรวจจับการบุกรุกไปใช้งาน
- 4.5 ผลการประเมินความสอดคล้องที่มีต่อแบบประเมินความรู้ ทักษะ และแบบประเมินทัศนคติจากผู้เชี่ยวชาญ

4.1 ผลการสร้างชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

ผู้วิจัยได้พัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกสำเร็จดังรูปที่ 4-1



(ก) ด้านหน้า

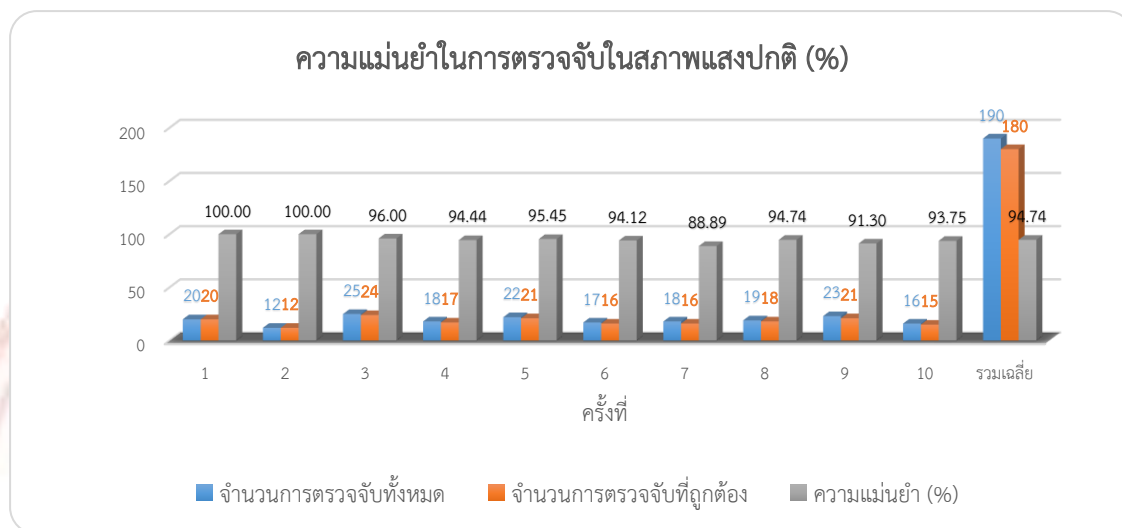


(ข) ด้านข้าง

ภาพที่ 4-1 ชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในการตรวจจับการบุกรุกขนาดเล็ก

และผู้วิจัยได้ทำการทดสอบตามหัวข้อต่างๆโดยมีผลการทำงานของชุดการเรียนรู้เชิงปฏิบัติดังรายการต่อไปนี้

4.1.1 การทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงปกติ (200-400 lux)



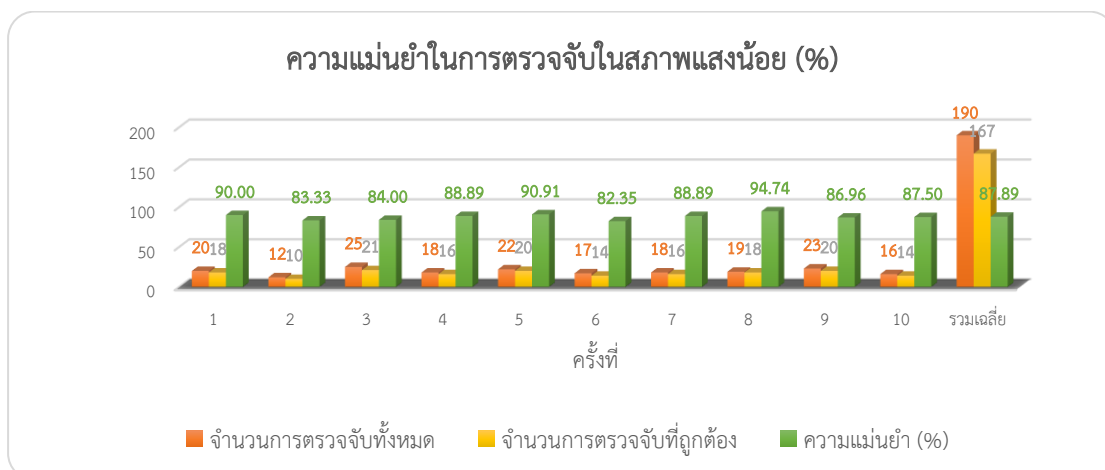
ภาพที่ 4-2 การทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงปกติ

จากรูปภาพที่ 4-2 แสดงผลการทดสอบความแม่นยำของการตรวจจับในสภาพแสงปกติ โดยมีการทดสอบทั้งหมด 10 ครั้ง ผลการทดสอบแสดงให้เห็นว่า ในครั้งที่ 1 และ 2 ระบบมีความแม่นยำ 100% โดยประมวลผลข้อมูลได้อย่างถูกต้องทั้งหมด ในครั้งที่ 3 ถึง 10 ความแม่นยำลดลงเล็กน้อย แต่ยังคงอยู่ในระดับที่น่าพอใจ โดยความแม่นยำอยู่ในช่วง 88.89% ถึง 96.00% ผลรวมเฉลี่ยแสดงให้เห็นว่าระบบมีความแม่นยำโดยรวมอยู่ที่ 94.74% ซึ่งถือว่าอยู่ในเกณฑ์ที่ดี

ข้อสังเกตได้ว่าความแม่นยำในการตรวจจับค่อนข้างสูงในครั้งแรกๆ และลดลงเล็กน้อยในครั้งหลังๆ ซึ่งอาจเกิดจากปัจจัยต่างๆ เช่น ความแตกต่างของข้อมูลที่ใช้ในการทดสอบ, การเปลี่ยนแปลงของสภาพแสงเล็กน้อย, หรือข้อจำกัดของระบบเอง นอกจากนี้ ค่าของข้อมูลที่น่ามาประมวลผลในแต่ละครั้งมีจำนวนที่ไม่เท่ากัน

โดยรวมแล้ว ระบบมีการตรวจจับที่ดีในสภาพแสงปกติ โดยมีค่าเฉลี่ยความแม่นยำอยู่ที่ 94.74% อย่างไรก็ตาม ควรมีการวิเคราะห์เพิ่มเติมเพื่อหาสาเหตุของความแตกต่างของความแม่นยำในแต่ละครั้ง และปรับปรุงระบบให้มีความแม่นยำยิ่งขึ้น

4.1.2 การทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงน้อย (< 100 lux)



ภาพที่ 4-3 ผลทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงน้อย

จากภาพที่ 4-3 แสดงผลการทดสอบความแม่นยำของระบบตรวจจับในสภาพแสงน้อย โดยทำการทดสอบทั้งหมด 10 ครั้ง และแสดงค่าเฉลี่ยรวมในแต่ละครั้งของการทดสอบ จะเห็นได้ว่าความแม่นยำในการตรวจจับของระบบนั้นค่อนข้างแตกต่างกันไปในแต่ละครั้งของการทดสอบ โดยครั้งที่ 8 มีความแม่นยำสูงสุดอยู่ที่ 94.74% ในขณะที่ครั้งที่ 6 มีความแม่นยำต่ำสุดอยู่ที่ 82.35% ค่าเฉลี่ยความแม่นยำโดยรวมของการทดสอบทั้ง 10 ครั้งอยู่ที่ 87.89% ซึ่งถือว่าอยู่ในระดับที่ค่อนข้างดีสำหรับการตรวจจับในสภาพแสงน้อย นอกจากนี้ ยังแสดงให้เห็นถึงจำนวนครั้งที่ระบบตรวจจับผิดพลาดและถูกต้องในแต่ละครั้งของการทดสอบ ซึ่งช่วยให้เห็นภาพรวมของการทำงานของระบบได้ชัดเจนยิ่งขึ้น เราสามารถสรุปได้ว่าระบบตรวจจับมีความสามารถในการทำงานได้ดีในสภาพแสงน้อยโดยมีค่าเฉลี่ยความแม่นยำอยู่ที่ 87.89%

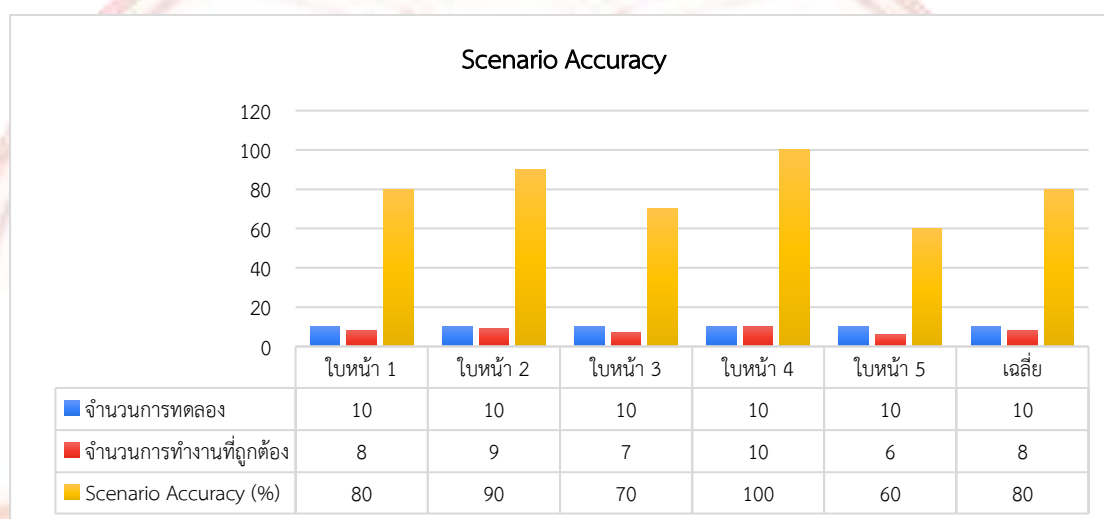
4.1.3 ความสำเร็จในการติดตั้งฮาร์ดแวร์ของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI โดยผู้เรียน



ภาพที่ 4-4 ความสำเร็จในการติดตั้งฮาร์ดแวร์โดยผู้เรียน

จากภาพที่ 4-4 ผลลัพธ์ของความสำเร็จในการติดตั้งฮาร์ดแวร์โดยผู้เรียน จะเห็นได้ว่าส่วนใหญ่ของผู้เรียนคิดเป็น 90% สามารถติดตั้งฮาร์ดแวร์ได้สำเร็จ ในขณะที่ผู้เรียนเพียง 10% เท่านั้นที่ไม่สามารถติดตั้งฮาร์ดแวร์ได้สำเร็จ ข้อมูลนี้แสดงให้เห็นว่าผู้เรียนส่วนใหญ่มีความเข้าใจและสามารถปฏิบัติงานในการติดตั้งฮาร์ดแวร์ได้เป็นอย่างดี โดยมีอัตราความสำเร็จที่ค่อนข้างสูง

4.1.4 ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง



ภาพที่ 4-5 ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง

จากภาพที่ 4-5 แสดงผลการทดสอบความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง (Scenario Accuracy) ในการตรวจจับใบหน้า 5 ใบหน้า โดยแต่ละใบหน้ามีการทดสอบทั้งหมด 10 ครั้ง โดยใบหน้า 1 มีการทำงานที่ถูกต้อง 8 ครั้งจาก 10 ครั้ง คิดเป็นความแม่นยำ 80% ใบหน้า 2 มีการทำงานที่ถูกต้อง 9 ครั้งจาก 10 ครั้ง คิดเป็นความแม่นยำ 90% ใบหน้า 3 มีการทำงานที่ถูกต้อง 7 ครั้งจาก 10 ครั้ง คิดเป็นความแม่นยำ 70% ใบหน้า 4 มีการทำงานที่ถูกต้อง 10 ครั้งจาก 10 ครั้ง คิดเป็นความแม่นยำ 100% ใบหน้า 5 มีการทำงานที่ถูกต้อง 6 ครั้งจาก 10 ครั้ง คิดเป็นความแม่นยำ 60% จากข้อมูลจะเห็นได้ว่าความแม่นยำในการตรวจจับใบหน้าแตกต่างกันไปในแต่ละใบหน้า โดยใบหน้า 4 มีความแม่นยำสูงสุด (100%) และใบหน้า 5 มีความแม่นยำต่ำสุด (60%) เฉลี่ยมีความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลองเป็น 80%

จากที่ผู้วิจัยได้ทำการทดสอบตามหัวข้อต่างๆโดยมีผลการทำงานของชุดการเรียนรู้เชิงปฏิบัติในรายการต่างๆข้างต้นนั้น สามารถสรุปผลการทดสอบการทำงานของชุดการเรียนรู้เชิงปฏิบัติได้ดังตารางที่ 4-1

ตารางที่ 4-1 ผลการทดสอบการทำงานของชุดการเรียนรู้เชิงปฏิบัติ

การทดสอบ	วิธีการทดสอบ	ผลลัพธ์	หมายเหตุ
ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงปกติ (200-400 lux)	ทดสอบความแม่นยำในการตรวจจับในสภาพแสงปกติ 10 ครั้ง	94.74%	มีความแม่นยำสูงในสภาพแสงปกติ
ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสภาพแสงน้อย (<100 lux)	ทดสอบความแม่นยำในการตรวจจับในสภาพแสงน้อย 10 ครั้ง	87.89%	ความแม่นยำลดลงเล็กน้อยในสภาพแสงน้อย
ความสำเร็จในการติดตั้งฮาร์ดแวร์ของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI โดยผู้เรียน	ประเมินความสำเร็จในการติดตั้งฮาร์ดแวร์	90%	ผู้เรียนส่วนใหญ่ติดตั้งได้สำเร็จ
ความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI ในสถานการณ์จำลอง	ทดสอบความแม่นยำในการตรวจจับใบหน้า 5 ใบหน้า (10 ครั้ง/ใบหน้า)	80%	ระบบทำงานได้ดีในสถานการณ์จำลอง

จากตารางที่ 4-1 พบว่าจากการทดลองใช้งานชุดการทดลองที่พัฒนาขึ้นสำหรับระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก พบว่าชุดการทดลองมีประสิทธิภาพและเหมาะสมสำหรับการนำไปใช้ในการเรียนรู้เชิงปฏิบัติในด้านต่าง ๆ ดังนี้ ในด้านความแม่นยำของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI พบว่าความแม่นยำในการทำงานในสภาพแสงปกติอยู่ที่ร้อยละ 94.74 ซึ่งถือว่าเป็นระดับที่สูงและสามารถรองรับการใช้งานในสถานการณ์ปกติได้เป็นอย่างดี ส่วนในสภาพแสงน้อย ความแม่นยำลดลงเล็กน้อยเหลือร้อยละ 87.89 แต่ยังคงอยู่ในระดับที่ยอมรับได้ แสดงให้เห็นถึงความสามารถของอุปกรณ์ในการทำงานภายใต้สภาพแวดล้อมที่หลากหลาย ในด้านการใช้งานชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI นักศึกษา

ร้อยละ 90 สามารถติดตั้งและเชื่อมต่ออุปกรณ์ทั้งหมดได้สำเร็จภายในเวลาที่กำหนด แสดงให้เห็นว่าชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วย AI มีการออกแบบที่เหมาะสม ใช้งานง่าย และเป็นมิตรต่อผู้ใช้ อีกทั้งในการทดลองสถานการณ์จำลอง ระบบมีความแม่นยำในการทำงานถึงร้อยละ 80 ซึ่งแสดงถึงความสามารถของระบบในการรองรับสถานการณ์ที่ซับซ้อนและการตรวจจับที่มีประสิทธิภาพ

4.2 ผลการเปรียบเทียบผลการประเมินด้านความรู้ก่อนเรียนและหลังเรียน

ผลการเปรียบเทียบการประเมินก่อนเรียนและหลังเรียนของผู้เรียนได้นำไปใช้กับผู้เรียน 2 กลุ่ม ทั้งกลุ่มทดลอง จำนวน 20 คน และกลุ่มควบคุม 20 คน คะแนนเต็ม 20 คะแนน จึงมีผลการเปรียบเทียบดังตารางที่ 4-2 และ 4-3

ตารางที่ 4-2 ผลการประเมินด้านความรู้ก่อนเรียนของกลุ่มทดลอง และกลุ่มควบคุม

กลุ่ม	จำนวน (N)	ค่าเฉลี่ยลำดับ (Mean Rank)	ผลรวมของอันดับ (Sum of Ranks)	U	Z	p-value
กลุ่มทดลอง	20	21.70	434.00	176.00	-0.666	0.505
กลุ่มควบคุม	20	19.30	386.00			

จากตารางที่ 4-2 จากการทดสอบ Mann-Whitney U Test พบว่าแม้ว่าคะแนนก่อนเรียนของกลุ่มทดลองจะมีแนวโน้มสูงกว่ากลุ่มควบคุม แต่ไม่มีความแตกต่างอย่างมีนัยสำคัญทางสถิติ ($p > 0.05$) ซึ่งแสดงให้เห็นว่า ก่อนการเรียนรู้ ทั้งสองกลุ่มมีความสามารถพื้นฐานที่ใกล้เคียงกัน ดังนั้นการเรียนรู้ในกลุ่มทดลองไม่ได้เริ่มต้นด้วยความแตกต่างทางสถิติจากกลุ่มควบคุม ซึ่งหมายความว่าหากมีความแตกต่างในการพัฒนาผลสัมฤทธิ์หลังเรียน ก็สามารถสันนิษฐานได้ว่าเป็นผลจากชุดการเรียนรู้ที่ใช้ในกลุ่มทดลอง

ตารางที่ 4-3 ผลการประเมินด้านความรู้หลังเรียนของกลุ่มทดลอง และกลุ่มควบคุม

กลุ่ม	จำนวน (N)	ค่าเฉลี่ยลำดับ (Mean Rank)	ผลรวมของอันดับ (Sum of Ranks)	U	Z	p-value
กลุ่มทดลอง	20	29.55	591.00	19.00	-4.946	0.000
กลุ่มควบคุม	20	11.45	229.00			

จากตารางที่ 4-3 จากผลการทดสอบ Mann-Whitney U Test พบว่า กลุ่มทดลองมีคะแนนทักษะสูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$) ซึ่งหมายความว่า การใช้ชุดการเรียนรู้ที่พัฒนาขึ้นช่วยเสริมสร้างทักษะของผู้เรียนได้อย่างชัดเจน และสามารถนำไปใช้เป็นแนวทางในการพัฒนาสื่อการสอนในอนาคตได้

4.3 ผลการประเมินทักษะการปฏิบัติงาน

ผลการการประเมินทักษะการปฏิบัติงานของผู้เรียนเรื่องระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก โดยนำไปใช้กับผู้เรียน 2 กลุ่มคือ กลุ่มทดลอง และกลุ่มควบคุม จำนวนกลุ่มละ 20 คน ด้วยวิธีการใช้การประเมินรายการตรวจสอบ (Checklist) จำนวน 20 ข้อ คะแนนเต็ม 80 คะแนน ซึ่งผลการประเมินได้มาจากครูผู้สอนเป็นผู้ประเมิน เมื่อนำผลการประเมินทักษะการปฏิบัติงานมาเปรียบเทียบระหว่าง 2 กลุ่มผู้เรียน จะได้ผลดังตารางที่ 4-4

ตารางที่ 4-4 ผลการประเมินทักษะการปฏิบัติงานของผู้เรียน

กลุ่ม	จำนวน (N)	ค่าเฉลี่ยลำดับ (Mean Rank)	ผลรวมของอันดับ (Sum of Ranks)	U	Z	p-value
กลุ่มทดลอง	20	30.25	605.00	5.00	-5.30	0.00
กลุ่มควบคุม	20	10.75	215.00			

จากผลการวิเคราะห์ในตารางที่ 4.4 พบว่าการศึกษานี้ใช้สถิติ Mann-Whitney U Test เพื่อเปรียบเทียบผลสัมฤทธิ์ทางการเรียนระหว่างสองกลุ่ม ได้แก่ กลุ่มทดลองที่เรียนรู้ผ่านชุดการเรียนรู้ที่พัฒนาขึ้น และกลุ่มควบคุมที่ใช้วิธีการสอนแบบดั้งเดิม ผลการทดสอบชี้ให้เห็นว่ากลุ่มทดลองมีผลสัมฤทธิ์ทางการเรียนสูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญ โดยค่าเฉลี่ยของอันดับ (Mean Rank) ของกลุ่มทดลองอยู่ที่ 30.25 ขณะที่กลุ่มควบคุมมีค่าเฉลี่ยเพียง 10.75 นอกจากนี้ ผลรวมของอันดับ (Sum of Ranks) ของกลุ่มทดลองมีค่า 605.00 ซึ่งสูงกว่ากลุ่มควบคุมที่มีค่า 215.00 อย่างมีนัยสำคัญ ค่า p-value จากการทดสอบเท่ากับ 0.00 ซึ่งต่ำกว่าระดับนัยสำคัญที่ 0.05 แสดงให้เห็นว่าผลสัมฤทธิ์ทางการเรียนของทั้งสองกลุ่มแตกต่างกันอย่างมีนัยสำคัญทางสถิติ โดยกลุ่มทดลองมีผลลัพธ์ที่ดีกว่ากลุ่มควบคุม

4.4 ผลการประเมินทัศนคติของผู้เรียนที่มีต่อการนำระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน

4.4.1 ผลการประเมินทัศนคติของผู้เรียน โดยทดสอบกับผู้เรียนกลุ่มทดลองและกลุ่มควบคุม

การเก็บข้อมูลจากแบบประเมินทัศนคติของผู้เรียนโดยแบ่งรายการประเมินออกเป็น 3 ด้าน รวม 15 ข้อ คือ ด้านที่ 1. ด้านทัศนคติเชิงบวกต่อการใช้ AI ในการพัฒนาระบบรักษาความปลอดภัย ด้านที่ 2. ด้านคุณค่าและความสำคัญของเทคโนโลยี AI ในการรักษาความปลอดภัย และด้านที่ 3. ด้านความมุ่งมั่นที่จะพัฒนาทักษะในการใช้ AI และเทคโนโลยีที่เกี่ยวข้อง ผู้วิจัยได้สรุปผลการประเมินทัศนคติของผู้เรียนที่มีต่อการนำระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน มีผลดังตารางที่ 4-5 และ ตารางที่ 4-6

ตารางที่ 4-5 ผลการประเมินทัศนคติของผู้เรียนกลุ่มทดลอง

รายการประเมิน	Σx	$\bar{x}$	S.D.	แปลความ
ด้านทัศนคติเชิงบวกต่อการใช้ AI ในการพัฒนาระบบรักษาความปลอดภัย				
ข้อที่ 1 ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สามารถช่วยเพิ่มความปลอดภัยในชีวิตประจำวันได้	93	4.65	0.49	เห็นด้วยมาก
ข้อที่ 2 การใช้ระบบ AI ในการตรวจจับการบุกรุกมีความน่าเชื่อถือ	98	4.90	0.30	เห็นด้วยมาก
ข้อที่ 3 ระบบ AI ที่ใช้ในการตรวจจับการบุกรุกสามารถป้องกันเหตุการณ์ไม่พึงประสงค์ได้ดี	91	4.55	0.51	เห็นด้วยมาก
ข้อที่ 4 ระบบ AI สามารถปรับปรุงประสิทธิภาพการตรวจจับการบุกรุกได้ดีกว่าระบบเดิม	94	4.70	0.47	เห็นด้วยมาก
ข้อที่ 5 การใช้ AI ในระบบรักษาความปลอดภัยทำให้การทำงานของเจ้าหน้าที่รักษาความปลอดภัยง่ายขึ้น	93	4.65	0.49	เห็นด้วยมาก
ข้อที่ 6 การใช้ระบบ AI ในการตรวจจับการบุกรุกสามารถลดอัตราการเกิดเหตุร้ายในชุมชนของคุณได้	94	4.70	0.47	เห็นด้วยมาก
ข้อที่ 7 การใช้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI สามารถช่วยลดภาระงานของเจ้าหน้าที่รักษาความปลอดภัยในสถานที่สาธารณะได้	95	4.75	0.44	เห็นด้วยมาก
ด้านคุณค่าและความสำคัญของเทคโนโลยี AI ในการรักษาความปลอดภัย				
ข้อที่ 8 การเรียนรู้เกี่ยวกับระบบ AI ที่ใช้ในการตรวจจับการบุกรุกมีประโยชน์ต่อการพัฒนาทักษะของคุณ	94	4.70	0.47	สำคัญมาก
ข้อที่ 9 การใช้ชุดการเรียนรู้เชิงปฏิบัติทำให้คุณเข้าใจการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มากขึ้น	96	4.80	0.41	สำคัญมาก
ข้อที่ 10 ระบบ AI ที่ใช้ในการตรวจจับการบุกรุกสามารถปรับปรุงและพัฒนาได้ในอนาคต	92	4.60	0.50	สำคัญมาก
ข้อที่ 11 ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI สามารถนำไปใช้ในบ้านเรือนของคุณ	91	4.55	0.51	สำคัญมาก
ข้อที่ 12 ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มีค่าใช้จ่ายที่คุ้มค่า	91	4.55	0.51	สำคัญมาก
ข้อที่ 13 ปัจจุบันมีระบบ AI ความจำเป็นที่นำมาใช้ในการรักษาความปลอดภัยในโรงเรียนหรือสถานที่ทำงาน	87	4.35	0.49	สำคัญมาก
ด้านความมุ่งมั่นที่จะพัฒนาทักษะในการใช้ AI และเทคโนโลยีที่เกี่ยวข้อง				
ข้อที่ 14 คุณมีความสนใจที่จะศึกษาเพิ่มเติมเกี่ยวกับการใช้ AI ในระบบรักษาความปลอดภัย	85	4.25	0.44	มีแรงจูงใจมาก
ข้อที่ 15 คุณมีความกังวลเกี่ยวกับความเป็นส่วนตัวในการใช้ระบบ AI ในการตรวจจับการบุกรุก	85	4.25	0.55	มีแรงจูงใจมาก
ผลเฉลี่ยรวมของการประเมินทัศนคติ	1379	68.95	3.47	

จากตารางที่ 4-5 พบว่าผลการประเมินทัศนคติของผู้เรียนมีทัศนคติเชิงบวกต่อการใช้ AI ในระบบรักษาความปลอดภัย โดยมีค่าเฉลี่ยรวมของการประเมินทัศนคติอยู่ที่ 68.95 ซึ่งบ่งชี้ถึงความเห็นด้วยในระดับสูง โดยเฉพาะในการใช้ระบบ AI ในการตรวจจับการบุกรุกมีความน่าเชื่อถือ ด้านคุณค่าและความสำคัญของ AI ผู้เรียนเห็นว่าการใช้ชุดการเรียนรู้เชิงปฏิบัติทำให้คุณเข้าใจการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มากขึ้น (ค่าเฉลี่ย 4.80) ผู้เรียนมีแรงจูงใจสูงในการศึกษาต่อยอดเทคโนโลยี AI (ค่าเฉลี่ย 4.25) อย่างไรก็ตาม ยังคงมีข้อกังวลเกี่ยวกับความเป็นส่วนตัวในการใช้งาน AI ซึ่งควรได้รับการพิจารณาเพื่อสร้างความมั่นใจในการใช้งานใน

อนาคต โดยสรุปผู้เรียนมีมุมมองเชิงบวกต่อ AI และตระหนักถึงคุณค่าของการเรียนรู้เทคโนโลยีนี้ พร้อมทั้งจะพัฒนาทักษะและนำ AI ไปประยุกต์ใช้ในชีวิตจริงต่อไป

ตารางที่ 4-6 ผลการประเมินทัศนคติของผู้เรียนกลุ่มควบคุม

รายการประเมิน	Σx	$\bar{x}$	S.D.	แปลความ
ด้านทัศนคติเชิงบวกต่อการใช้ AI ในการพัฒนาระบบรักษาความปลอดภัย				
ข้อที่ 1 ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สามารถช่วยเพิ่มความปลอดภัยในชีวิตประจำวันได้	80	4.00	0.00	เห็นด้วยมาก
ข้อที่ 2 การใช้ระบบ AI ในการตรวจจับการบุกรุกมีความน่าเชื่อถือ	77	3.85	0.37	เห็นด้วยมาก
ข้อที่ 3 ระบบ AI ที่ใช้ในการตรวจจับการบุกรุกสามารถป้องกันเหตุการณ์ไม่พึงประสงค์ได้ดี	77	3.85	0.49	เห็นด้วยมาก
ข้อที่ 4 ระบบ AI สามารถปรับปรุงประสิทธิภาพการตรวจจับการบุกรุกได้ดีกว่าระบบเดิม	78	3.90	0.45	เห็นด้วยมาก
ข้อที่ 5 การใช้ AI ในระบบรักษาความปลอดภัยทำให้การทำงานของเจ้าหน้าที่รักษาความปลอดภัยง่ายขึ้น	78	3.90	0.45	เห็นด้วยมาก
ข้อที่ 6 การใช้ระบบ AI ในการตรวจจับการบุกรุกสามารถลดอัตราการเกิดเหตุร้ายในชุมชนของคุณได้	76	3.80	0.41	เห็นด้วยมาก
ข้อที่ 7 การใช้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI สามารถช่วยลดภาระงานของเจ้าหน้าที่รักษาความปลอดภัยในสถานที่สาธารณะได้	76	3.80	0.52	เห็นด้วยมาก
ด้านคุณค่าและความสำคัญของเทคโนโลยี AI ในการรักษาความปลอดภัย				
ข้อที่ 8 การเรียนรู้เกี่ยวกับระบบ AI ที่ใช้ในการตรวจจับการบุกรุกมีประโยชน์ต่อการพัฒนาทักษะของคุณ	76	3.80	0.52	สำคัญมาก
ข้อที่ 9 การใช้ชุดการเรียนรู้เชิงปฏิบัติทำให้คุณเข้าใจการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มากขึ้น	78	3.90	0.45	สำคัญมาก
ข้อที่ 10 ระบบ AI ที่ใช้ในการตรวจจับการบุกรุกสามารถปรับปรุงและพัฒนาได้ในอนาคต	78	3.90	0.31	สำคัญมาก
ข้อที่ 11 ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI สามารถนำไปใช้ในบ้านเรือนของคุณ	77	3.85	0.37	สำคัญมาก
ข้อที่ 12 ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มีค่าใช้จ่ายที่คุ้มค่า	78	3.90	0.45	สำคัญมาก
ข้อที่ 13 ปัจจุบันมีระบบ AI ความจำเป็นที่นำมาใช้ในการรักษาความปลอดภัยในโรงเรียนหรือสถานที่ทำงาน	79	3.95	0.22	สำคัญมาก
ด้านความมุ่งมั่นที่จะพัฒนาทักษะในการใช้ AI และเทคโนโลยีที่เกี่ยวข้อง				
ข้อที่ 14 คุณมีความสนใจที่จะศึกษาเพิ่มเติมเกี่ยวกับการใช้ AI ในระบบรักษาความปลอดภัย	83	4.15	0.37	แรงจูงใจมาก
ข้อที่ 15 คุณมีความกังวลเกี่ยวกับความเป็นส่วนตัวในการใช้ระบบ AI ในการตรวจจับการบุกรุก	81	4.05	0.22	แรงจูงใจมาก
ผลเฉลี่ยรวมของการประเมินทัศนคติ	1172	58.60	3.23	

จากตารางที่ 4-6 พบว่าผลการประเมินทัศนคติของผู้เรียนต่อการใช้ AI ในระบบรักษาความปลอดภัย พบว่าผู้เรียนมีทัศนคติเชิงบวกในระดับเห็นด้วยอย่างมาก กับระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สามารถช่วยเพิ่มความปลอดภัยในชีวิตประจำวันได้โดยมีค่าเฉลี่ยรวมอยู่ที่ 4.00 ซึ่งสะท้อนถึงความเชื่อมั่นในประสิทธิภาพของ AI ในการช่วยเพิ่ม

ความปลอดภัยและลดภาระงานของเจ้าหน้าที่ ด้านคุณค่าและความสำคัญของ AI ผู้เรียนมองว่า AI มีบทบาทสำคัญในการพัฒนาทักษะและสามารถนำไปประยุกต์ใช้ในบ้านเรือนและสถานที่ทำงานได้ (ค่าเฉลี่ย 3.90) อย่างไรก็ตามในด้านความมุ่งมั่นในการศึกษาต่อยอด AI พบว่าผู้เรียนมีระดับแรงจูงใจมาก (ค่าเฉลี่ย 4.15) และยังมีข้อกังวลเกี่ยวกับความเป็นส่วนตัว สรุปได้ว่า ผู้เรียนมีมุมมองเชิงบวกต่อ AI และเห็นถึงคุณค่าของเทคโนโลยีนี้ แต่ยังต้องการข้อมูลเพิ่มเติมเพื่อสร้างความมั่นใจในการใช้งาน

4.4.2 การเปรียบเทียบทัศนคติของผู้เรียนต่อการใช้ AI ในระบบรักษาความปลอดภัย ในกลุ่มทดลองและกลุ่มควบคุม

ตารางที่ 4-7 ผลการเปรียบเทียบทัศนคติของผู้เรียนต่อการใช้ AI ในระบบรักษาความปลอดภัย

กลุ่ม	จำนวน (N)	ค่าเฉลี่ยลำดับ (Mean Rank)	ผลรวมของอันดับ (Sum of Ranks)	U	Z	p-value
กลุ่มทดลอง	20	30.28	605.50	4.50	-5.3	0.00
กลุ่มควบคุม	20	10.73	214.50			

จากตารางที่ 4-7 จากการวิเคราะห์ผลด้วย Mann-Whitney U Test ($p = 0.00$, $p < 0.05$) พบว่ามีความแตกต่างอย่างมีนัยสำคัญทางสถิติระหว่างทัศนคติของผู้เรียนในกลุ่มทดลองและกลุ่มควบคุม โดยค่าเฉลี่ยลำดับ (Mean Rank) ของกลุ่มทดลองสูงกว่ากลุ่มควบคุมอย่างชัดเจน (30.28 เมื่อเทียบกับ 10.73) นอกจากนี้ ผลรวมลำดับ (Sum of Ranks) ของกลุ่มทดลองอยู่ที่ 605.50 ในขณะที่กลุ่มควบคุมมีค่าเพียง 214.50 ซึ่งสะท้อนให้เห็นว่าผู้เรียนในกลุ่มทดลองมีมุมมองที่ดีต่อการใช้ AI ในระบบรักษาความปลอดภัยมากกว่าอย่างมีนัยสำคัญ ชุดการเรียนรู้ที่พัฒนาขึ้นสามารถส่งเสริมให้ผู้เรียนเกิดทัศนคติเชิงบวกต่อเทคโนโลยี AI และทำให้พวกเขาเข้าใจถึงความสำคัญและบทบาทของ AI ในการเสริมสร้างความปลอดภัยได้อย่างชัดเจนและมีประสิทธิภาพยิ่งขึ้น

4.5 ผลการประเมินความสอดคล้องที่มีต่อแบบประเมินความรู้ ทักษะ และแบบประเมินทัศนคติของผู้เชี่ยวชาญ

ผู้วิจัยได้ทำการออกแบบแบบประเมินสำหรับผู้เรียนในด้านความรู้ ทักษะการปฏิบัติงาน และด้านทัศนคติของผู้เรียน โดยผู้เชี่ยวชาญ ซึ่งผู้วิจัยได้จัดทำหนังสือขอความอนุเคราะห์ผู้เชี่ยวชาญประเมินแบบทดสอบจำนวน 5 ท่าน โดยใช้สัญลักษณ์ (☒ = 1, ☐ = 0, ☒ = -1) เพื่อให้ง่ายต่อการแสดงข้อมูลมีผลการประเมินดังนี้

4.5.1 การประเมินแบบทดสอบวัดความรู้เกี่ยวกับระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก ดำเนินการโดยผู้เชี่ยวชาญ เพื่อพิจารณาความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์เชิงพฤติกรรมที่กำหนด ซึ่งประกอบด้วย 13 วัตถุประสงค์เชิงพฤติกรรม และ 20 ข้อคำถาม ผลการประเมินค่าดัชนีความตรงเชิงเนื้อหา (Index of Item-

Objective Congruence: IOC) แสดงไว้ในตารางที่ 4-8 ซึ่งระบุค่าความสอดคล้องของแต่ละข้อคำถาม โดยมีเกณฑ์พิจารณา ดังนี้

ค่าดัชนี IOC ตั้งแต่ 0.5 ขึ้นไป หมายถึง ข้อคำถามสามารถนำไปใช้ได้

ค่าดัชนี IOC ต่ำกว่า 0.5 หมายถึง ควรปรับปรุงข้อคำถามก่อนนำไปใช้

ตารางที่ 4-8 การประเมินค่าดัชนีความตรงเชิงเนื้อหา (IOC) สำหรับแบบทดสอบวัดความรู้ของผู้เรียน

ข้อ	การให้คะแนนของผู้เชี่ยวชาญ	ค่า IOC	ผลการพิจารณา
1	○○□□□	0.6	นำไปใช้ได้
2	○□□□□	0.8	นำไปใช้ได้
3	○□○□□	0.6	นำไปใช้ได้
4	×□□□□	0.8	นำไปใช้ได้
5	□□□□□	1.0	นำไปใช้ได้
6	□□□○□	0.8	นำไปใช้ได้
7	×○□□□	0.6	นำไปใช้ได้
8	□○□□□	0.8	นำไปใช้ได้
9	□□□□□	1.0	นำไปใช้ได้
10	□○□□□	0.8	นำไปใช้ได้
11	○○□□□	0.6	นำไปใช้ได้
12	□○□□□	0.8	นำไปใช้ได้
13	□○○□□	0.6	นำไปใช้ได้
14	○○□□□	0.6	นำไปใช้ได้
15	○○□□□	0.6	นำไปใช้ได้
16	□×□□□	0.6	นำไปใช้ได้
17	□×□□□	0.6	นำไปใช้ได้
18	□○□□□	0.8	นำไปใช้ได้
19	○□□○□	0.6	นำไปใช้ได้
20	□○□□□	0.8	นำไปใช้ได้

จากตารางที่ 4-8 ผลการวิเคราะห์พบว่าข้อคำถามทั้งหมดมีค่าความสอดคล้อง IOC ตั้งแต่ 0.6 ขึ้นไป ซึ่งอยู่ในระดับที่สามารถนำไปใช้ได้ โดยไม่มีข้อคำถามใดที่ต่ำกว่าค่ามาตรฐาน (0.5) ทั้งนี้ ข้อคำถามที่ได้ค่าความสอดคล้องต่ำกว่า 1.0 อาจได้รับข้อเสนอแนะให้ปรับปรุงเพื่อเพิ่มความชัดเจน และลดความคลุมเครือ ก่อนนำไปใช้ในขั้นตอนต่อไป

4.5.2 การประเมินแบบประเมินทักษะในงานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก ได้รับการวิเคราะห์โดยผู้เชี่ยวชาญ เพื่อพิจารณาความสอดคล้องระหว่างข้อคำถามและวัตถุประสงค์เชิงพฤติกรรม ซึ่งประกอบด้วย 7 วัตถุประสงค์เชิงพฤติกรรม และ 7 ข้อคำถาม ผลการประเมินค่าดัชนีความตรงเชิงเนื้อหา (Index of Item-Objective Congruence: IOC) สรุปไว้ในตารางที่ 4-9

ตารางที่ 4-9 การประเมินค่าดัชนีความตรงเชิงเนื้อหา (IOC) สำหรับแบบประเมินทักษะของผู้เรียน

ข้อ	การให้คะแนนของผู้เชี่ยวชาญ	ค่า IOC	ผลการพิจารณา
1	☑☑☑☑☑	1.0	นำไปใช้ได้
2	☑☑☑☑☑	1.0	นำไปใช้ได้
3	☑☑☒☑☑	0.6	นำไปใช้ได้
4	☑☑☑☑○	0.8	นำไปใช้ได้
5	☑☑☑☑☑	1.0	นำไปใช้ได้
6	☑☑☑☑☑	1.0	นำไปใช้ได้
7	☑☑☑☑☑	1.0	นำไปใช้ได้

จากตารางที่ 4-9 พบว่าข้อคำถามทั้งหมดมีค่าดัชนีความสอดคล้อง (IOC) ตั้งแต่ 0.6 ขึ้นไป ซึ่งหมายความว่าสามารถนำไปใช้ในการประเมินผู้เรียนได้ อย่างไรก็ตาม ข้อคำถามบางส่วนได้รับข้อเสนอแนะให้มีการปรับปรุงความชัดเจนและความครอบคลุมของเนื้อหา เพื่อให้แน่ใจว่าแบบประเมินสามารถวัดทักษะของผู้เรียนได้อย่างมีประสิทธิภาพ ก่อนนำไปใช้ในการทดสอบจริง

4.5.3 การประเมินแบบประเมินทัศนคติของผู้เรียนที่มีต่อการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สำหรับการตรวจจับการบุกรุกไปใช้งาน ได้รับการวิเคราะห์โดยผู้เชี่ยวชาญ เพื่อพิจารณาความสอดคล้องระหว่างข้อคำถามกับพฤติกรรมที่ต้องการวัด โดยแบ่งการประเมินออกเป็น 3 ด้าน รวมทั้งหมด 15 ข้อ ผลการประเมินค่าดัชนีความตรงเชิงเนื้อหา (Index of Item-Objective Congruence: IOC) สรุปไว้ในตารางที่ 4-10 ซึ่งแสดงระดับความสอดคล้องของข้อคำถามกับวัตถุประสงค์ของการประเมิน เพื่อให้มั่นใจว่าแบบประเมินมีความเหมาะสม ครอบคลุม และสามารถสะท้อนทัศนคติของผู้เรียนได้อย่างถูกต้องและชัดเจน

ตารางที่ 4-10 การประเมินค่าดัชนีความตรงเชิงเนื้อหา (IOC) สำหรับแบบประเมินทัศนคติของผู้เรียน

ข้อ	การให้คะแนนของผู้เชี่ยวชาญ	ค่า IOC	ผลการพิจารณา
1	☑☑☑☑☑	1.0	นำไปใช้ได้
2	☑☑☑☑☑	1.0	นำไปใช้ได้

ตารางที่ 4-10 (ต่อ)

ข้อ	การให้คะแนนของผู้เชี่ยวชาญ	ค่า IOC	ผลการพิจารณา
3	☑☑○☑○	0.6	นำไปใช้ได้
4	☑☑☑☑○	0.8	นำไปใช้ได้
5	☑☑☑○○	0.6	นำไปใช้ได้
6	○☑☑☑○	0.6	นำไปใช้ได้
7	☑☑☑☑○	0.8	นำไปใช้ได้
8	☑☑☑☑○	0.8	นำไปใช้ได้
9	☑☑☑☑○	0.8	นำไปใช้ได้
10	☑☑☑☑○	0.8	นำไปใช้ได้
11	☑☑☑☑○	0.8	นำไปใช้ได้
12	☑☑☑○○	0.6	นำไปใช้ได้
13	☑☑○☑○	0.6	นำไปใช้ได้
14	☑☑☑☑○	0.8	นำไปใช้ได้
15	☑☑☑☑○	0.8	นำไปใช้ได้

จากตารางที่ 4-10 พบว่าแบบประเมินมีค่าดัชนีความสอดคล้อง (IOC) ตั้งแต่ 0.6 ขึ้นไป ซึ่งหมายความว่าสามารถนำไปใช้ในการประเมินทัศนคติของผู้เรียนได้ อย่างไรก็ตาม ข้อคำถามบางข้อได้รับข้อเสนอแนะให้ปรับปรุงเพื่อเพิ่มความชัดเจน ความครอบคลุม และลดความคลุมเครือของเนื้อหา ก่อนนำไปใช้จริงในการประเมินกับผู้เรียน เพื่อให้สามารถสะท้อนทัศนคติของผู้เรียนได้อย่างถูกต้องและแม่นยำมากขึ้น

บทที่ 5

สรุป อภิปรายผล และข้อเสนอแนะ

5.1 สรุปผลการวิจัย

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อพัฒนาชุดการเรียนรู้เชิงปฏิบัติสำหรับระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก โดยทดสอบผลสัมฤทธิ์ทางด้านความรู้ ทักษะการปฏิบัติงาน และทัศนคติของผู้เรียน ผลการวิจัยสรุปได้ดังนี้:

5.1.1 การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก โดยชุดการเรียนรู้ที่พัฒนาขึ้นสามารถทำงานได้อย่างมีประสิทธิภาพ โดยมีความแม่นยำสูงในสภาพแสงปกติ (94.74%) และมีความแม่นยำที่ยอมรับได้ในสภาพแสงน้อย (87.89%) ระบบการทำงานโดยรวมของชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์แสดงให้เห็นถึงความสอดคล้องและเสถียรภาพในการทำงานตามที่ออกแบบไว้

5.1.2 ผลสัมฤทธิ์ทางด้านความรู้ ผลการทดสอบความรู้ก่อนและหลังการเรียนรู้ระหว่างกลุ่มทดลองและกลุ่มควบคุม แสดงให้เห็นว่าผู้เรียนในกลุ่มทดลองที่ได้ใช้ชุดการเรียนรู้มีคะแนนสูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$). แสดงให้เห็นว่าชุดการเรียนรู้ที่พัฒนาขึ้นสามารถช่วยเสริมสร้างความรู้ของผู้เรียนได้อย่างชัดเจน

5.1.3 ทักษะการปฏิบัติงาน การประเมินทักษะการปฏิบัติงานของผู้เรียนระหว่างสองกลุ่ม แสดงให้เห็นว่ากลุ่มทดลองมีทักษะการปฏิบัติงานที่ดีกว่ากลุ่มควบคุม โดยมีคะแนนสูงกว่าอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$)

5.1.4 ทัศนคติของผู้เรียน ผู้เรียนในกลุ่มทดลองมีทัศนคติเชิงบวกต่อการใช้เทคโนโลยี AI ในระบบรักษาความปลอดภัยสูงกว่ากลุ่มควบคุมอย่างมีนัยสำคัญทางสถิติ ($p < 0.05$) ผู้เรียนเห็นว่าการใช้ AI มีประโยชน์ในการเพิ่มความปลอดภัยและสามารถนำไปประยุกต์ใช้ในชีวิตประจำวันได้

5.2 อภิปรายผล

ผลการวิจัยชี้ให้เห็นว่าการใช้ชุดการเรียนรู้ที่พัฒนาขึ้นสามารถเสริมสร้างความรู้และทักษะการปฏิบัติงานของผู้เรียนได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับหลักการเรียนรู้แบบลงมือปฏิบัติที่เน้นการสร้างประสบการณ์จริงและการเรียนรู้ผ่านการทำงานในสถานการณ์จริง นอกจากนี้ การใช้ AI ในระบบรักษาความปลอดภัยยังช่วยให้ผู้เรียนเห็นความสำคัญและประโยชน์ของเทคโนโลยีในการแก้ปัญหาทางสังคม เช่น การป้องกันการบุกรุกและเพิ่มความปลอดภัยในชีวิตประจำวัน

อย่างไรก็ตาม ควรมีการพิจารณาเพิ่มเติมในเรื่องของการเพิ่มประสิทธิภาพในสภาพแสงน้อยและความเสถียรของระบบในสภาพแวดล้อมที่แตกต่างกัน นอกจากนี้ ควรให้ความสำคัญกับการสร้างความเชื่อมั่นและการให้ข้อมูลเกี่ยวกับความเป็นส่วนตัวในการใช้งาน AI

5.3 ข้อเสนอแนะ

5.3.1 ข้อเสนอแนะในการนำผลการวิจัยไปใช้

5.3.1.1 ชุดการเรียนรู้สามารถนำไปประยุกต์ใช้ในรายวิชาที่เกี่ยวข้องกับระบบรักษาความปลอดภัยและการประยุกต์เทคโนโลยี AI เพื่อเสริมสร้างทักษะการเรียนรู้ที่สอดคล้องกับความต้องการของอุตสาหกรรม

5.3.1.2 สถานศึกษาอาจพิจารณาจัดกิจกรรมการเรียนรู้เพิ่มเติม เช่น การจำลองสถานการณ์ในชีวิตจริง เพื่อให้ผู้เรียนได้พัฒนาทักษะการแก้ไขปัญหาและการตัดสินใจ

5.3.2 ข้อเสนอแนะสำหรับการวิจัยในอนาคต

5.3.2.1 ควรพัฒนาชุดการเรียนรู้ที่ครอบคลุมการทำงานในสภาพแวดล้อมที่หลากหลาย เช่น สภาพแสงที่เปลี่ยนแปลง หรือการตรวจจับวัตถุที่ซับซ้อนมากขึ้น

5.3.2.2 ควรศึกษาเพิ่มเติมเกี่ยวกับการปรับปรุงระบบ AI เพื่อเพิ่มความแม่นยำ และลดข้อจำกัดของอุปกรณ์ เช่น การประมวลผลในสภาพแสงน้อย

5.3.2.3 ควรขยายผู้เข้าร่วมการวิจัยให้หลากหลายและครอบคลุมกลุ่มเป้าหมายในระดับอื่น ๆ เช่น ระดับอาชีวศึกษาตอนต้นหรือระดับมหาวิทยาลัย เพื่อเปรียบเทียบผลลัพธ์ในมิติต่าง

บรรณานุกรม

ภาษาไทย

- คุ้มสุภา, ธ. (2559). การประมวลผลภาพดิจิทัลด้วยโครงข่ายประสาทเทียมแบบคอนโวลูชัน. *วารสารวิชาการและวิจัย มทร.พระนคร*, 10(2), 159-169.
- สำนักงานคณะกรรมการการอาชีวศึกษา. (2567). [ออนไลน์]. *หลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567*. [สืบค้นวันที่ 22 ตุลาคม 2567]. สืบค้นจาก <https://bsq.vec.go.th>

ภาษาอังกฤษ

- Ahmed, A., Nain, N., Vijayaraghavan, P., & Sajjan, S. (2021). The role of IoT in enhancing intrusion detection systems. *Journal of IoT Applications*, 23(4), 145-157.
- Bojarski, M., Del Testa, D., Dworakowski, D., Firner, B., Flepp, B., Goyal, P., Jackel, L. D., Monfort, M., Muller, U., Zhang, J., Zhang, X., Zhao, J., & Zieba, K. (2016). End to end learning for self-driving cars. *arXiv preprint arXiv:1604.07316*.
- Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi-experimental designs for research*. Rand McNally.
- Chen, J., & Liu, S. (2022). Design and implementation of AI learning kits. *Technology in Education*, 17(4), 101-115.
- Deshpande, A. (2016). [online]. "A beginner's guide to understanding convolutional neural networks." [cited 2024 Apr. 1]. Available from : URL : <https://adeshpande3.github.io/A-Beginner%27s-Guide-To-Understanding-Convolutional-Neural-Networks/>
- Devlin, J., Chang, M. W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, 4171-4186.
- Girshick, R., Donahue, J., Darrell, T., & Malik, J. (2014). Rich feature hierarchies for accurate object detection and semantic segmentation. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 580-587).
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 27.
- Hasan, R., Husain, M., & Amjad, K. (2022). Intrusion detection systems: Enhancing security through AI. *Journal of Security Studies*, 34(2), 87-103.
- He, K., Gkioxari, G., Dollár, P., & Girshick, R. (2017). Mask R-CNN. In *Proceedings of the IEEE international conference on computer vision* (pp. 2961-2969).
- He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 770-778).
- Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735-1780.
- Huang, L., Zhang, Y., & Wang, R. (2022). Practical learning kits: A new approach to vocational education. *Journal of Engineering Education*, 54(1), 123-134.
- Johnson, M., & Wong, Y. (2023). Enhancing practical skills through AI-based learning modules. *Journal of Vocational Education*, 22(3), 59-72.
- Khan, M., Ahmed, S., & Rahman, N. (2020). Machine learning in intrusion detection: A comprehensive review. *Cybersecurity Journal*, 48(5), 201-215.
- Kim, S., Park, J., & Lee, H. (2023). Integrating ESP32 and AI for smart security systems. *Journal of IoT Innovations*, 12(6), 99-111.
- Kim, Y. (2014). Convolutional neural networks for sentence classification. In *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)* (pp. 1746-1751).
- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. In *Advances in neural information processing systems* (pp. 1097-1105).
- Kwon, J., & Park, S. (2022). Application of AI in modern security systems. *Journal of Security Technology*, 15(3), 45-57.
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
- LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11), 2278-2324.
- Lee, C. (2020). Practical implementation of AI in vocational education. *Educational Technology Journal*, 10(2), 78-89.

- Li, T., Zhang, X., & Chen, K. (2023). AI-driven intrusion detection systems: An overview. *Journal of Artificial Intelligence Research*, 47(7), 321-344.
- Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., van der Laak, J. A., van Ginneken, B., & Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, 42, 60-88.
- Liu, Z., Wang, J., & Chen, Y. (2021). The application of HuskyLens in real-time face detection. *Applied AI Technologies*, 15(4), 78-88.
- Long, J., Shelhamer, E., & Darrell, T. (2015). Fully convolutional networks for semantic segmentation. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 3431-3440).
- Nair, V., & Hinton, G. E. (2010). Rectified linear units improve restricted Boltzmann machines. *Proceedings of the 27th International Conference on Machine Learning (ICML-10)*, 807-814.
- Nguyen, T., & Tran, L. (2021). Future directions in AI-driven vocational training. *Asian Journal of Technical Education*, 14(2), 88-97.
- Rahman, A., & Chen, H. (2021). Active and passive intrusion detection systems: Comparative analysis. *Journal of Cybersecurity Research*, 19(2), 99-113.
- Rahman, T., & Ahmed, J. (2023). Biometrics and AI in authentication systems. *Journal of Advanced Security Systems*, 24(5), 345-367.
- Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You only look once: Unified, real-time object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 779-788).
- Ronneberger, O., Fischer, P., & Brox, T. (2015). U-net: Convolutional networks for biomedical image segmentation. In *International Conference on Medical image computing and computer-assisted intervention* (pp. 234-241).
- Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., Berg, A. C., & Fei-Fei, L. (2015). ImageNet large scale visual recognition challenge. *International Journal of Computer Vision*, 115(3), 211-252.
- Shadish, W. R., Cook, T. D., & Campbell, D. T. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Houghton Mifflin.
- Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

- Smith, A., & Taylor, B. (2023). Challenges in integrating AI in vocational training. *Vocational Studies Review*, 18(1), 34-47.
- Smith, J., & Brown, K. (2023). The effectiveness of gamification in online learning: Impact on students' attitudes and engagement. *ResearchGate*. Retrieved from <https://www.researchgate.net/publication/378301328>
- Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V., & Rabinovich, A. (2015). Going deeper with convolutions. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 1–9). IEEE. <https://doi.org/10.1109/CVPR.2015.7298594>
- Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1701-1708).
- Wang, H., Li, J., & Zhang, M. (2023). Advances in HuskyLens technology for security applications. *Journal of AI and Computer Vision*, 3(4), 120-132.
- Zhang, P., Yang, L., & Zhao, D. (2023). Enhancing threat detection with AI: A review. *Journal of Advanced Security Studies*, 28(5), 205-223.
- Zhao, K., Wang, Q., & Liu, C. (2023). Real-time face recognition with HuskyLens in IoT systems. *Journal of Embedded Systems*, 18(7), 89-104.
- Zhou, H., Liu, Y., & Zhang, W. (2021). AI-driven intrusion detection systems: Efficiency and accuracy. *International Journal of AI Research*, 20(4), 123-135.

Click or tap here to enter text.

ภาคผนวก



ภาคผนวก ก

- หนังสือขอความอนุเคราะห์เป็นผู้เชี่ยวชาญ
- แบบประเมินความสอดคล้องที่มีต่อแบบประเมินความรู้ ทักษะ และแบบประเมินทัศนคติของผู้เชี่ยวชาญ





ที่ อว 7104.1/104

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
1518 ถนนประชากราษฎร์ 1 แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพฯ 10800

16 มกราคม 2568

เรื่อง ขอบความอนุเคราะห์ให้บุคลากรภายในสังกัดเป็นผู้เชี่ยวชาญ

เรียน หัวหน้าภาควิชาครุศาสตร์อุตสาหกรรม

คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ด้วยนางสาวจิราวรรณ โคประโคน รหัสประจำตัว 66-020178-5802-5 เป็นนักศึกษาระดับปริญญาโท หลักสูตรครุศาสตร์อุตสาหกรรมมหาบัณฑิต สาขาวิชาวิศวกรรมเครื่องกลศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ได้ทำสารนิพนธ์เรื่อง “การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก” โดยมีรองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร เป็นอาจารย์ที่ปรึกษาสารนิพนธ์

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พิจารณาเห็นว่าบุคลากรภายในหน่วยงานของท่านเป็นผู้มีความรู้ความสามารถและมีประสบการณ์เป็นอย่างดี จึงขอความอนุเคราะห์ให้ ผู้ช่วยศาสตราจารย์ ดร.ปกรณ์เกียรติ์ เสวตเมธิกุล ตำแหน่งอาจารย์ประจำภาควิชาครุศาสตร์อุตสาหกรรม ภาควิชาครุศาสตร์อุตสาหกรรม คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เป็นผู้เชี่ยวชาญ เพื่อประเมินความสอดคล้องของแบบทดสอบวัดผลสัมฤทธิ์ด้านความรู้และทักษะการปฏิบัติงาน รวมถึงแบบประเมินทัศนคติของผู้เรียนในเรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก เพื่อนำมาปรับปรุงแก้ไขให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

โดยขอให้ท่านได้โปรดประเมิน ให้คำแนะนำ และข้อเสนอแนะ เพื่อเป็นข้อมูลในการจัดทำสารนิพนธ์เรื่องดังกล่าว และขอขอบพระคุณท่านที่ได้ให้ความอนุเคราะห์เป็นอย่างสูงมา ณ โอกาสนี้ ทั้งนี้เพื่อประโยชน์สูงสุดของนักศึกษา

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ


(รองศาสตราจารย์ ดร.กิตติวัฒน์ สุทธิโรจน์)
หัวหน้าภาควิชาครุศาสตร์เครื่องกล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาควิชาครุศาสตร์เครื่องกล

โทรศัพท์ 02-555-2000 ต่อ 3207

ผู้จัดทำสารนิพนธ์ 082-483-0821 (นางสาวจิราวรรณ โคประโคน)

ภาพที่ ก-1 หนังสือขอความอนุเคราะห์ ผศ. ดร. ปกรณ์เกียรติ์ เสวตเมธิกุลเป็นผู้เชี่ยวชาญ



ที่ อว 7104.1/105

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
1518 ถนนประชากราษฎร์ 1 แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพฯ 10800

16 มกราคม 2568

เรื่อง ขอบความอนุเคราะห์ให้บุคลากรภายในสังกัดเป็นผู้เชี่ยวชาญ

เรียน หัวหน้าภาควิชาครุศาสตร์อุตสาหกรรม

คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ด้วยนางสาวจิราวรรณ โคประโคน รหัสประจำตัว 66-020178-5802-5 เป็นนักศึกษาระดับปริญญาโท หลักสูตรครุศาสตร์อุตสาหกรรมมหาบัณฑิต สาขาวิชาวิศวกรรมเครื่องกลศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ได้ทำสารนิพนธ์เรื่อง “การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก” โดยมีรองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร เป็นอาจารย์ที่ปรึกษาสารนิพนธ์

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พิจารณาเห็นว่าบุคลากรภายในหน่วยงานของท่านเป็นผู้มีความรู้ความสามารถและมีประสบการณ์เป็นอย่างดี จึงขอความอนุเคราะห์ให้ ผู้ช่วยศาสตราจารย์ ชลดา ปานสง ตำแหน่งอาจารย์ประจำภาควิชาครุศาสตร์อุตสาหกรรม ภาควิชาครุศาสตร์อุตสาหกรรม คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เป็นผู้เชี่ยวชาญ เพื่อประเมินความสอดคล้องของแบบทดสอบวัดผลสัมฤทธิ์ด้านความรู้และทักษะการปฏิบัติงาน รวมถึงแบบประเมินทัศนคติของผู้เรียนในเรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก เพื่อนำมาปรับปรุงแก้ไขให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

โดยขอให้ท่านได้โปรดประเมิน ให้คำแนะนำ และข้อเสนอแนะ เพื่อเป็นข้อมูลในการจัดทำสารนิพนธ์เรื่องดังกล่าว และขอขอบพระคุณท่านที่ได้ให้ความอนุเคราะห์เป็นอย่างสูงมา ณ โอกาสนี้ ทั้งนี้เพื่อประโยชน์สูงสุดของนักศึกษา

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ

(รองศาสตราจารย์ ดร.กิตติวุฒิ สุทธิโรจน์)

หัวหน้าภาควิชาครุศาสตร์เครื่องกล

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาควิชาครุศาสตร์เครื่องกล

โทรศัพท์ 02-555-2000 ต่อ 3207

ผู้จัดทำสารนิพนธ์ 082-483-0821 (นางสาวจิราวรรณ โคประโคน)

ภาพที่ ก-2 หนังสือขอความอนุเคราะห์ ผศ. ชลดา ปานสง เป็นผู้เชี่ยวชาญ



ที่ อว 7104.1/106

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
1518 ถนนประชากรราษฎร์ 1 แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพฯ 10800

16 มกราคม 2568

เรื่อง ขอบความอนุเคราะห์ให้บุคลากรภายในสังกัดเป็นผู้เชี่ยวชาญ

เรียน ผู้อำนวยการสำนักงานห้องเรียนวิศว์-วิทย์ สถาบันการเรียนรู้ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

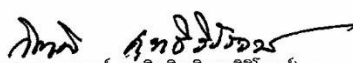
ด้วยนางสาวจิราวรรณ โคประโคน รหัสประจำตัว 66-020178-5802-5 เป็นนักศึกษาระดับปริญญาโท หลักสูตรครุศาสตร์อุตสาหกรรมมหาบัณฑิต สาขาวิชาวิศวกรรมเครื่องกลศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ได้ทำสารนิพนธ์เรื่อง “การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก” โดยมีรองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร เป็นอาจารย์ที่ปรึกษาสารนิพนธ์

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พิจารณาเห็นว่าบุคลากรภายในหน่วยงานของท่านเป็นผู้มีความรู้ความสามารถและมีประสบการณ์เป็นอย่างดี จึงขอความอนุเคราะห์ให้ นายศุภกฤต รongam ตำแหน่งอาจารย์ประจำสำนักงานห้องเรียนวิศว์-วิทย์ สถาบันการเรียนรู้ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี เป็นผู้เชี่ยวชาญ เพื่อประเมินความสอดคล้องของแบบทดสอบวัดผลสัมฤทธิ์ด้านความรู้และทักษะการปฏิบัติงาน รวมถึงแบบประเมินทัศนคติของผู้เรียนในเรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจัดการบุกรุก เพื่อนำมาปรับปรุงแก้ไขให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

โดยขอให้ท่านได้โปรดประเมิน ให้คำแนะนำ และข้อเสนอแนะ เพื่อเป็นข้อมูลในการจัดทำสารนิพนธ์เรื่องดังกล่าว และขอขอบพระคุณท่านที่ได้ให้ความอนุเคราะห์เป็นอย่างสูงมา ณ โอกาสนี้ ทั้งนี้เพื่อประโยชน์สูงสุดของนักศึกษา

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ


(รองศาสตราจารย์ ดร.กิตติวุฒิ สุทธิวิโรจน์)

หัวหน้าภาควิชาครุศาสตร์เครื่องกล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาควิชาครุศาสตร์เครื่องกล

โทรศัพท์ 02-555-2000 ต่อ 3207

ผู้จัดทำสารนิพนธ์ 082-483-0821 (นางสาวจิราวรรณ โคประโคน)

ภาพที่ ก-3 หนังสือขอความอนุเคราะห์ นายศุภกฤต รongam เป็นผู้เชี่ยวชาญ



ที่ อว 7104.1/107

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
1518 ถนนประชากราษฎร์ 1 แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพฯ 10800

16 มกราคม 2568

เรื่อง ขอความอนุเคราะห์ให้บุคลากรภายในสังกัดเป็นผู้เชี่ยวชาญ

เรียน ผู้อำนวยการวิทยาลัยเทคนิคนครนายก

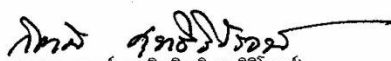
ด้วยนางสาวจิราวรรณ โคประโคน รหัสประจำตัว 66-020178-5802-5 เป็นนักศึกษาระดับปริญญาโท หลักสูตรครุศาสตร์อุตสาหกรรมมหาบัณฑิต สาขาวิชาวิศวกรรมเครื่องกลศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ได้ทำสารนิพนธ์เรื่อง “การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจบบักรุก” โดยมีรองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร เป็นอาจารย์ที่ปรึกษาสารนิพนธ์

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พิจารณาเห็นว่าบุคลากรภายในหน่วยงานของท่านเป็นผู้มีความรู้ความสามารถและมีประสบการณ์เป็นอย่างดี จึงขอความอนุเคราะห์ให้ นางกฤษณา เอ็งฉุน ตำแหน่งครู วิทยฐานะครูชำนาญการพิเศษ แผนกวิชาอิเล็กทรอนิกส์ วิทยาลัยเทคนิคนครนายก เป็นผู้เชี่ยวชาญ เพื่อประเมินความสอดคล้องของแบบทดสอบวัดผลสัมฤทธิ์ด้านความรู้และทักษะการปฏิบัติงาน รวมถึงแบบประเมินทัศนคติของผู้เรียนในเรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจบบักรุก เพื่อนำมาปรับปรุงแก้ไขให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

โดยขอให้ท่านได้โปรดประเมิน ให้คำแนะนำ และข้อเสนอแนะ เพื่อเป็นข้อมูลในการจัดทำสารนิพนธ์เรื่องดังกล่าว และขอขอบพระคุณท่านที่ได้ให้ความอนุเคราะห์เป็นอย่างสูงมา ณ โอกาสนี้ ทั้งนี้เพื่อประโยชน์สูงสุดของนักศึกษา

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ


(รองศาสตราจารย์ ดร.กิตติวุฒิ สุทธิวิโรจน์)

หัวหน้าภาควิชาครุศาสตร์เครื่องกล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาควิชาครุศาสตร์เครื่องกล

โทรศัพท์ 02-555-2000 ต่อ 3207

ผู้จัดทำสารนิพนธ์ 082-483-0821 (นางสาวจิราวรรณ โคประโคน)

ภาพที่ ก-4 หนังสือขอความอนุเคราะห์ นางกฤษณา เอ็งฉุน เป็นผู้เชี่ยวชาญ



ที่ อว 7104.1/108

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
1518 ถนนประชากรราษฎร์ 1 แขวงวงศ์สว่าง
เขตบางซื่อ กรุงเทพฯ 10800

16 มกราคม 2568

เรื่อง ขอความอนุเคราะห์ให้บุคลากรภายในสังกัดเป็นผู้เชี่ยวชาญ

เรียน ผู้อำนวยการวิทยาลัยเทคนิคสระบุรี

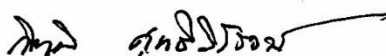
ด้วยนางสาวจิราวรรณ โคประโคน รหัสประจำตัว 66-020178-5802-5 เป็นนักศึกษาระดับปริญญาโท หลักสูตรครุศาสตร์อุตสาหกรรมมหาบัณฑิต สาขาวิชาวิศวกรรมเครื่องกลศึกษา คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ได้ทำสารนิพนธ์เรื่อง “การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก” โดยมีรองศาสตราจารย์ ดร.ศุภชัย หอวิมานพร เป็นอาจารย์ที่ปรึกษาสารนิพนธ์

ภาควิชาครุศาสตร์เครื่องกล คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พิจารณาเห็นว่าบุคลากรภายในหน่วยงานของท่านเป็นผู้มีความรู้ความสามารถและมีประสบการณ์เป็นอย่างดี จึงขอความอนุเคราะห์ให้ นายยงยุทธ จันทรัตน์ ตำแหน่งครู วิทยฐานะครูชำนาญการพิเศษ แผนกวิชาอิเล็กทรอนิกส์ วิทยาลัยเทคนิคสระบุรี เป็นผู้เชี่ยวชาญ เพื่อประเมินความสอดคล้องของแบบทดสอบวัดผลสัมฤทธิ์ด้านความรู้และทักษะการปฏิบัติงาน รวมถึงแบบประเมินทัศนคติของผู้เรียนในเรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก เพื่อนำมาปรับปรุงแก้ไขให้มีความสมบูรณ์ยิ่งขึ้นต่อไป

โดยขอให้ท่านได้โปรดประเมิน ให้คำแนะนำ และข้อเสนอแนะ เพื่อเป็นข้อมูลในการจัดทำสารนิพนธ์เรื่องดังกล่าว และขอขอบพระคุณท่านที่ได้ให้ความอนุเคราะห์เป็นอย่างสูงมา ณ โอกาสนี้ ทั้งนี้เพื่อประโยชน์สูงสุดของนักศึกษา

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ด้วย จะเป็นพระคุณยิ่ง

ขอแสดงความนับถือ


(รองศาสตราจารย์ ดร.กิตติวดี สุทธิโรจน์)

หัวหน้าภาควิชาครุศาสตร์เครื่องกล
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาควิชาครุศาสตร์เครื่องกล

โทรศัพท์ 02-555-2000 ต่อ 3207

ผู้จัดทำสารนิพนธ์ 082-483-0821 (นางสาวจิราวรรณ โคประโคน)

ภาพที่ ก-5 หนังสือขอความอนุเคราะห์ นายยงยุทธ จันทรัตน์ เป็นผู้เชี่ยวชาญ



**แบบประเมินความสอดคล้องระหว่างวัตถุประสงค์เชิงพฤติกรรมกับแบบทดสอบความรู้
ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก**

คำชี้แจง ให้ท่านพิจารณาว่าแบบวัดความเข้าใจที่สร้างขึ้น มีความสอดคล้องกับวัตถุประสงค์เชิง พฤติกรรมที่กำหนดไว้หรือไม่ โดยการพิจารณาให้น้ำหนักความสอดคล้อง ดังนี้

- 1 คือ ไม่สนใจ ว่าแบบทดสอบข้อนั้น ไม่สอดคล้อง กับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้
- 0 คือ ไม่แน่ใจ ว่าแบบทดสอบข้อนั้น สอดคล้อง กับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้ หรือไม่
- +1 คือ เน้นใจ ว่าแบบทดสอบข้อนั้น สอดคล้อง กับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้

วัตถุประสงค์เชิงพฤติกรรม	ข้อสอบ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
1. บอกความหมายของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้	1. ความหมายของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์คือข้อใด ก. ระบบที่พึ่งพามนุษย์ในการวิเคราะห์ข้อมูลตลอดเวลา ☒ ข. ระบบที่ใช้ AI เพื่อวิเคราะห์และตอบสนองต่อภัยคุกคาม ค. ระบบที่ใช้เซ็นเซอร์เสียงเท่านั้น ง. ระบบที่ทำงานเฉพาะในช่วงเวลากลางคืน				
2. อธิบายความสำคัญของ AI ในการตรวจจับการบุกรุกได้	2. AI มีสำคัญอย่างไรในการตรวจจับการบุกรุก ก. แจ้งเตือนเมื่อพบการเปลี่ยนแปลงสภาพแวดล้อม ข. ควบคุมระบบไฟฟ้าในอาคารทั้งหมด ☒ ค. วิเคราะห์ข้อมูลและแจ้งเตือนทันทีเมื่อพบความผิดปกติ ง. ทำงานเฉพาะกับกล้องวงจรปิด				
3. บอกส่วนประกอบสำคัญในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้	3. ส่วนประกอบใดที่ทำหน้าที่ในการรวบรวมข้อมูลจากสภาพแวดล้อมเพื่อนำมาวิเคราะห์โดย AI ก. อัลกอริทึม AI ข. ฐานข้อมูล ☒ ค. เซ็นเซอร์และกล้อง ง. ระบบแจ้งเตือน				
	4. ส่วนประกอบใดที่ทำหน้าที่ในการประมวลผลข้อมูลและตัดสินใจในการตอบสนองต่อภัยคุกคาม ก. เซ็นเซอร์ ข. ฐานข้อมูล ☒ ค. อัลกอริทึม AI ง. ระบบแจ้งเตือน				

วัตถุประสงค์เชิง พฤติกรรม	ข้อสอบ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
4. อธิบายเกี่ยวกับ Machine Learning ในการจดจำบุคคลได้	5. ขั้นตอนที่สำคัญในการฝึกฝนโมเดล Machine Learning สำหรับการจดจำใบหน้า ก. การรวบรวมข้อมูลใบหน้าจำนวนน้อย ข. การใช้ข้อมูลใบหน้าที่มีความหลากหลาย ค. การใช้ข้อมูลใบหน้าที่มีคุณภาพต่ำ ง. การฝึกฝนโมเดลด้วยข้อมูลใบหน้าจากบุคคลเดียว				
	6. ข้อใดอธิบายการทำงานของ Machine Learning ในการจดจำใบหน้าได้ถูกต้องที่สุด ก. Machine Learning ทำงานเฉพาะในช่วงกลางคืนเพื่อป้องกันการบันทึกข้อมูลผิดพลาด ข. Machine Learning ลดขนาดข้อมูลภาพเพื่อประหยัดพื้นที่จัดเก็บ ค. Machine Learning ใช้สร้างเครือข่ายการเชื่อมต่อระหว่างกล้องวงจรปิดในพื้นที่ ง. Machine Learning ใช้เปรียบเทียบข้อมูลใบหน้ากับฐานข้อมูลเพื่อยืนยันตัวบุคคล				
5. อธิบายหลักการของ ระบบ IoT ที่ใช้ใน ระบบรักษาความ ปลอดภัยที่ขับเคลื่อน ด้วยปัญญาประดิษฐ์	7. การใช้ IoT ในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ที่ถูกต้องที่สุดคือข้อใด ก. การตั้งค่าการแจ้งเตือนเสียงในบ้านโดยใช้อุปกรณ์ IoT ข. การสื่อสารระหว่างกล้องอัจฉริยะและเซ็นเซอร์การเคลื่อนไหวเพื่อตรวจจับภัยคุกคาม ค. การควบคุมการเปิดปิดไฟในอาคารอัตโนมัติโดยใช้ระบบ IoT เพื่อเพิ่มความปลอดภัย ง. การใช้ Wi-Fi เพื่อตรวจจับภัยคุกคามในพื้นที่โดยตรง				
	8. การใช้ IoT ร่วมกับ AI ในระบบรักษาความปลอดภัยมีลักษณะอย่างไร ก. การแจ้งเตือนผ่านแอปพลิเคชันเมื่อพบภัยคุกคามโดยการวิเคราะห์ข้อมูลจากอุปกรณ์ IoT ด้วย AI ข. การควบคุมอุปกรณ์ไฟฟ้าภายในบ้านทั้งหมดแบบระบบปิดโดยไม่มีการเชื่อมต่อกับภายนอก ค. การติดตั้งกล้องวงจรปิดโดยไม่เชื่อมต่อเครือข่ายและไม่มีการวิเคราะห์ข้อมูล ง. การตรวจสอบเสียงเท่านั้น โดยไม่มีการวิเคราะห์ข้อมูลอื่น ๆ และไม่มีการแจ้งเตือน				
6. อธิบายการทำงานของ AI ในการตรวจจับ พฤติกรรมผิดปกติใน พื้นที่สาธารณะได้	9. AI ทำงานอย่างไรในการตรวจจับพฤติกรรมผิดปกติในพื้นที่สาธารณะ ก. ใช้ข้อมูลจากเซ็นเซอร์เสียงเพียงอย่างเดียว ข. ตรวจจับภัยคุกคามเฉพาะในเวลากลางวัน				

วัตถุประสงค์เชิง พฤติกรรม	ข้อสอบ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
	ก) วิเคราะห์ภาพจากกล้องวงจรปิดและระบุการเคลื่อนไหวผิดปกติและแสดงผล ง. แจ้งเตือนเฉพาะเมื่อมีการเปลี่ยนแปลงอินเทอร์เนต				
7. อธิบายบทบาทของ Machine Learning และ IoT ในการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้	10. ข้อใดเปรียบเทียบบทบาทของ Machine Learning และ IoT ในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้ถูกต้องที่สุด ก) Machine Learning ใช้ในการวิเคราะห์และจดจำรูปแบบ เช่น ใบหน้า ขณะที่ IoT เชื่อมต่ออุปกรณ์ต่าง ๆ ข. Machine Learning ทำหน้าที่เชื่อมต่ออุปกรณ์ในระบบ ขณะที่ IoT ใช้ในการจดจำพฤติกรรมของบุคคล ค. Machine Learning และ IoT มีบทบาทเหมือนกันในการตรวจจับการเคลื่อนไหวผิดปกติ ง. Machine Learning และ IoT ใช้ในการแจ้งเตือนเท่านั้น				
8. อธิบายปัจจัยที่ส่งผลต่อความแม่นยำของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้	11. ปัจจัยสำคัญที่ส่งผลต่อความแม่นยำของ AI ในการรักษาความปลอดภัยมากที่สุด ก. ความเร็วในการประมวลผลของฮาร์ดแวร์ ข) คุณภาพของข้อมูลที่ใช้ในการฝึกโมเดล AI ค. จำนวนกล้องวงจรปิดที่ติดตั้ง ง. ความซับซ้อนของอัลกอริทึม AI				
	12. การกำกับดูแลของมนุษย์มีผลต่อความแม่นยำของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์อย่างไร ก. ช่วยเพิ่มความเร็วในการประมวลผลของ AI ข. ช่วยลดต้นทุนในการพัฒนาระบบ AI ค) ช่วยตรวจสอบและแก้ไขข้อผิดพลาดของ AI ง. ช่วยเพิ่มจำนวนกล้องวงจรปิดที่ระบบ AI รองรับ				
9. อธิบายความสำคัญของ Deep Learning ในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้	13. Deep Learning มีความสำคัญต่อระบบรักษาความปลอดภัยอย่างไร ก) ช่วยวิเคราะห์ภาพและเสียงที่ซับซ้อนได้แม่นยำ ข. ลดจำนวนข้อมูลที่ต้องจัดเก็บในระบบ ค. ใช้เฉพาะในระบบการจดจำเสียง ง. ทำงานเฉพาะกับข้อมูลภาพนิ่ง				
	ข้อ 14. Deep Learning มีความสำคัญอย่างไรในการยกระดับระบบรักษาความปลอดภัย ก. ลดระยะเวลาที่ใช้ในการประมวลผลและจัดการข้อมูลจำนวนมาก ทำให้ระบบตอบสนองต่อภัยคุกคามได้รวดเร็วยิ่งขึ้น				

วัตถุประสงค์เชิง พฤติกรรม	ข้อสอบ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
	ข. เพิ่มประสิทธิภาพในการวิเคราะห์ข้อมูลเสียง โดยสามารถแยกแยะและจดจำเสียงที่เกี่ยวข้องกับภัยคุกคามได้อย่างแม่นยำ ค. ลดปริมาณข้อมูลที่ต้องส่งจากเซ็นเซอร์ไปยังระบบประมวลผล ทำให้ประหยัดพลังงานและแบนด์วิดท์ในการสื่อสาร ง. วิเคราะห์ข้อมูลภาพและเสียงที่มีความซับซ้อนสูงได้อย่างละเอียดและแม่นยำ ทำให้สามารถตรวจจับและระบุภัยคุกคามที่ซับซ้อนได้				
10. อธิบายความหมายของ Convolutional Neural Networks (CNN) ได้	ข้อ 15. ข้อใดอธิบายความหมายของ Convolutional Neural Networks (CNN) ในบริบทของระบบรักษาความปลอดภัยได้ชัดเจนที่สุด ก. CNN เป็นเทคนิคการบีบอัดข้อมูลภาพเพื่อลดขนาดไฟล์ ทำให้สามารถจัดเก็บและส่งข้อมูลภาพได้ง่ายขึ้นในระบบรักษาความปลอดภัย ข. CNN เป็นโครงข่ายประสาทเทียมที่ออกแบบมาเพื่อวิเคราะห์และจัดจํารูปแบบในข้อมูลภาพ โดยใช้ในการตรวจจับใบหน้า วัตถุ หรือเหตุการณ์ผิดปกติในระบบรักษาความปลอดภัย ค. CNN เป็นอัลกอริทึมที่ใช้ในการวิเคราะห์ข้อมูลเสียงเพื่อตรวจจับเสียงผิดปกติ เช่น เสียงการบุกรุกหรือเสียงเตือนภัยในระบบรักษาความปลอดภัย ง. CNN เป็นระบบอัตโนมัติที่ใช้ในการควบคุมและสั่งการอุปกรณ์รักษาความปลอดภัย เช่น กล้องวงจรปิดหรือระบบล็อกประตู				
11. อธิบายหลักการการทำงานของ Convolutional Neural Networks (CNN) ได้	16. หลักการทำงานของ Convolutional Neural Networks (CNN) คืออะไร ก. วิเคราะห์ข้อมูลที่ไม่มีรูปแบบเฉพาะ ข. ตรวจจับเสียงที่ซับซ้อนและมีลำดับเวลา ค. แบ่งภาพออกเป็นส่วนเล็ก ๆ และวิเคราะห์คุณลักษณะ ง. ลดความละเอียดของภาพเพื่อเพิ่มความเร็ว				
12. บอกตัวอย่างสถานการณ์ที่ใช้ AI ในการรักษาความปลอดภัยได้	17. ตัวอย่างสถานการณ์ที่ใช้ AI ในการรักษาความปลอดภัยคือข้อใด ก. การวิเคราะห์ข้อมูลการจราจร ข. การตรวจสอบข้อมูลย้อนหลังในพื้นที่สาธารณะ ค. การลดปริมาณข้อมูลในกล้องวงจรปิด ง. การแจ้งเตือนเมื่อมีผู้บุกรุกในบ้าน 18. ข้อใดแสดงถึงระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ได้อย่างมีประสิทธิภาพสูงสุด				

วัตถุประสงค์เชิง พฤติกรรม	ข้อสอบ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
	ก. ระบบที่ตรวจจับผู้บุกรุกและแจ้งเตือนอัตโนมัติแบบเรียลไทม์ ปรับปรุงความแม่นยำในการตรวจจับจากการเรียนรู้ข้อมูลอย่างต่อเนื่อง ข. ระบบรักษาความปลอดภัย AI ที่เน้นการทำงานเฉพาะในเวลากลางคืนเพื่อลดการใช้พลังงาน โดยจะปิดการทำงานในช่วงเวลากลางวันเพื่อประหยัดพลังงาน ค. ระบบรักษาความปลอดภัย AI ที่ลดการใช้ข้อมูลโดยการไม่ตรวจจับพฤติกรรมที่ผิดปกติ เพื่อลดความซับซ้อนในการประมวลผล ง. ระบบรักษาความปลอดภัย AI ที่ลดต้นทุนโดยไม่ใช้กล้องวงจรปิด แต่จะใช้เซ็นเซอร์ตรวจจับความเคลื่อนไหวและเสียงเท่านั้น				
13. เปรียบเทียบข้อดีของการใช้ AI กับการใช้มนุษย์ในระบบรักษาความปลอดภัยได้	19. ข้อใดแสดงถึงการเปรียบเทียบข้อดีของ AI กับมนุษย์ได้เหมาะสมที่สุด ก. AI ทำงานได้ดีกว่ามนุษย์ในทุกกรณี ข. AI แม่นยำและทำงานได้ตลอด 24 ชั่วโมง ค. มนุษย์ไม่มีข้อจำกัดในการตรวจจับภัยคุกคาม ง. AI ไม่สามารถทำงานแบบเรียลไทม์ได้				
	20. ข้อดีของ AI ที่เหนือกว่ามนุษย์ในระบบรักษาความปลอดภัยคือข้อใด ก. AI ต้องการการปรับแต่งตลอดเวลา ข. AI มีต้นทุนการบำรุงรักษาสูงกว่า ค. AI ทำงานเฉพาะในสภาพแสงปกติ ง. AI ไม่มีความเหนื่อยล้าและทำงานได้ตลอดเวลา				

ลงชื่อ.....

()

ผู้เชี่ยวชาญ



แบบประเมินความสอดคล้องระหว่างวัตถุประสงค์เชิงพฤติกรรมกับแบบทดสอบเชิงปฏิบัติ (Practical Test)
ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

คำชี้แจง ให้ท่านพิจารณาว่าแบบวัดความเข้าใจที่สร้างขึ้น มีความสอดคล้องกับวัตถุประสงค์เชิง พฤติกรรมที่กำหนดไว้หรือไม่ โดยการพิจารณาให้น้ำหนักความสอดคล้อง ดังนี้

- 1 คือ แน่ใจ ว่าแบบทดสอบข้อนั้น ไม่สอดคล้อง กับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้
- 0 คือ ไม่แน่ใจ ว่าแบบทดสอบข้อนั้น สอดคล้อง กับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้ หรือไม่
- +1 คือ แน่ใจ ว่าแบบทดสอบข้อนั้น สอดคล้อง กับวัตถุประสงค์เชิงพฤติกรรมที่กำหนดไว้

วัตถุประสงค์เชิงพฤติกรรม	รายละเอียดการประเมินด้านทักษะ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
1. ติดตั้งและเชื่อมต่อ HuskyLens กับ ไมโครคอนโทรลเลอร์ ได้	ข้อ 1: ตั้งค่าและเชื่อมต่อ HuskyLens เพื่อใช้ในการตรวจจับภาพและวิเคราะห์การบุกรุก 1.1 เชื่อมต่อ HuskyLens กับ Arduino ผ่านพอร์ต RX และ TX 1.2 ตั้งค่า Face Recognition Algorithm ใน HuskyLens				
2. ตั้งค่าการทำงานของ AI ใน HuskyLens เพื่อควบคุมอุปกรณ์อื่น ๆ ในระบบรักษาความปลอดภัย	ข้อ 2: ตั้งค่า AI ใน HuskyLens เพื่อสั่งการควบคุมอุปกรณ์ในระบบรักษาความปลอดภัย 2.1 ตั้งค่าให้ HuskyLens สั่งงาน Servo Motor ให้ปลดล็อกเมื่อพบใบหน้าที่ได้รับอนุญาต 2.2 ตั้งค่าให้ HuskyLens สั่งงาน Buzzer และ LED แจ้งเตือนเมื่อพบใบหน้าที่ไม่ได้รับอนุญาต				
3. เขียนโปรแกรมเพื่อควบคุมการทำงานของ HuskyLens และ ไมโครคอนโทรลเลอร์ ในระบบรักษาความปลอดภัย	ข้อ 3: ทดสอบความถูกต้องและประสิทธิภาพของโปรแกรม 3.1 ทดสอบการตรวจจับใบหน้าที่ได้รับอนุญาต (True Positive) 3.2 ทดสอบการแจ้งเตือนใบหน้าที่ไม่ได้รับอนุญาต (False Positive)				
4. ปรับแต่งโปรแกรม ให้ AI ใน HuskyLens สามารถทำงานได้อย่างแม่นยำและมีประสิทธิภาพมากขึ้น	ข้อ 4: ปรับแต่งโปรแกรม AI เพื่อเพิ่มประสิทธิภาพในการตรวจจับ 4.1 ปรับปรุงเพื่อลด False Positive และ False Negative 4.2 เพิ่มความแม่นยำของระบบ $\geq 10\%$				

วัตถุประสงค์เชิง พฤติกรรม	รายละเอียดการประเมินด้านทักษะ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
5. ทดสอบระบบรักษา ความปลอดภัยที่ ขับเคลื่อนด้วย AI และ ระบุข้อผิดพลาดที่ เกิดขึ้นได้	ข้อ 5: ทดสอบระบบในสถานการณ์จำลอง 5.1 ทดสอบระบบในสภาพแสงปกติ 5.2 ทดสอบระบบในสภาพแสงน้อย 5.3 ทดสอบระบบในการตรวจจับหลายเป้าหมาย พร้อมกัน				
6. ระบุข้อผิดพลาดที่ เกิดขึ้นในกระบวนการ ทำงานของ AI และ แก้ไขปัญหานั้นได้	ข้อ 6: วิเคราะห์ข้อผิดพลาดและแก้ไขโปรแกรม 6.1 วิเคราะห์ข้อผิดพลาด เช่น False Positive และ False Negative 6.2 แก้ไขข้อผิดพลาดและปรับปรุงระบบ				
7. ปรับแต่งโปรแกรม และการทำงานของ AI ใน HuskyLens เพื่อให้ ระบบรักษาความ ปลอดภัยทำงานได้ อย่างมีประสิทธิภาพใน ทุกสถานการณ์	ข้อ 7: ปรับแต่งโปรแกรมให้ระบบตอบสนองใน สถานการณ์หลากหลาย 7.1 ปรับโปรแกรมให้ตอบสนองในสถานการณ์แสง น้อย 7.2 ปรับโปรแกรมให้รองรับการตรวจจับหลาย เป้าหมายพร้อมกัน				

ลงชื่อ.....

()

ผู้เชี่ยวชาญ



**แบบประเมินความสอดคล้องของแบบสอบถามทัศนคติของผู้เรียน
การนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน**

คำชี้แจง โปรดพิจารณาความสอดคล้องของประเด็นข้อคำถามเพื่อใช้ในแบบประเมินทัศนคติของผู้เรียน โดยพิจารณาแต่ละข้อว่ามีความสอดคล้องหรือไม่ โดยการพิจารณาให้น้ำหนักความสอดคล้อง ดังนี้

-1 คือ ไม่สอดคล้อง
0 คือ ไม่แน่ใจ
+1 คือ สอดคล้อง

ด้านที่ 1 ทัศนคติเชิงบวกต่อการใช้ AI ในการพัฒนาระบบรักษาความปลอดภัย

ข้อที่	ข้อคำถาม	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
1	ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์สามารถช่วยเพิ่มความปลอดภัยในชีวิตประจำวันได้				
2	การใช้ระบบ AI ทำให้การตรวจจับการบุกรุกมีความน่าเชื่อถือ				
3	ระบบ AI ที่ใช้ในการตรวจจับการบุกรุกสามารถป้องกันเหตุการณ์ไม่พึงประสงค์ได้				
4	ระบบ AI สามารถปรับปรุงประสิทธิภาพการตรวจจับการบุกรุกได้ดีกว่าระบบเดิม				
5	การใช้ AI ในระบบรักษาความปลอดภัยทำให้การทำงานของเจ้าหน้าที่รักษาความปลอดภัยง่ายขึ้น				
6	การใช้ระบบ AI ในการตรวจจับการบุกรุกสามารถลดอัตราการเกิดเหตุร้ายในชุมชนของคุณได้				
7	การใช้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI สามารถช่วยลดภาระงานของเจ้าหน้าที่รักษาความปลอดภัยในสถานที่สาธารณะได้				

ด้านที่ 2 คุณค่าและความสำคัญของเทคโนโลยี AI ในการรักษาความปลอดภัย

ข้อที่	ข้อคำถาม	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
8	การเรียนรู้เกี่ยวกับระบบ AI ที่ใช้ในการตรวจจับการบุกรุกมีประโยชน์ต่อการพัฒนาทักษะของคุณ				
9	การใช้ชุดการเรียนรู้เชิงปฏิบัติทำให้คุณเข้าใจการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มากขึ้น				
10	ระบบ AI ที่ใช้ในการตรวจจับการบุกรุกสามารถปรับปรุงและพัฒนาได้ในอนาคต				
11	ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI สามารถนำไปใช้ในบ้านเรือนของคุณได้				
12	ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI มีค่าใช้จ่ายที่คุ้มค่า				
13	ปัจจุบันมีระบบ AI ความจำเป็นที่นำมาใช้ในการรักษาความปลอดภัยในโรงเรียนหรือสถานที่ทำงาน				

ด้านที่ 3 ความมุ่งมั่นที่จะพัฒนาทักษะในการใช้ AI และเทคโนโลยีที่เกี่ยวข้อง

ข้อที่	ข้อความ	น้ำหนักความสอดคล้อง			ข้อเสนอแนะ
		-1	0	+1	
14	คุณมีความสนใจที่จะศึกษาเพิ่มเติมเกี่ยวกับการใช้ AI ในระบบรักษาความปลอดภัย				
15	คุณมีความกังวลเกี่ยวกับความเป็นส่วนตัวในการใช้ระบบ AI ในการตรวจจับการบุกรุก				

ลงชื่อ.....

()

ผู้เชี่ยวชาญ

ภาคผนวก ข

- ตารางวิเคราะห์การจัดการเรียนรู้
- แผนการจัดการเรียนรู้
- แบบทดสอบวัดความรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก
- ใบปฏิบัติงานและแบบบันทึกผลการประเมินเรื่องระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก
- แบบสอบถามทัศนคติของผู้เรียนการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน
- คู่มือการใช้งาน

ตารางวิเคราะห์การจัดการเรียนรู้เรื่อง: ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการทุจริต

หัวข้อที่	หัวข้อการเรียนรู้	เนื้อหา	วัตถุประสงค์	หัวข้อรายการประเมินที่เกี่ยวกับทักษะทางด้าน AI
1	บทนำและทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วย AI	1. บทนำและความสำคัญของระบบรักษาความปลอดภัยด้วย AI 2. ทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วย AI 3. คุณสมบัติของระบบรักษาความปลอดภัยด้วย AI	1.1 บอกความหมายของระบบรักษาความปลอดภัยด้วย AI ได้ 1.2 บอกบทบาทของ AI ในการตรวจจับการทุจริตได้ 1.3 อธิบายความสำคัญของการตอบสนองแบบเรียลไทม์ในระบบรักษาความปลอดภัยด้วย AI ได้ 2.1 บอกส่วนประกอบสำคัญของระบบรักษาความปลอดภัยได้ 2.2 ระบุจุดให้ความรู้เกี่ยวกับ Machine Learning เพื่ออธิบายการวิเคราะห์ข้อมูลในหน้าที่ AI ที่ใช้ในการตรวจจับทุจริตได้ 2.3 อธิบายตัวอย่างของระบบ IoT ที่ใช้ในระบบรักษาความปลอดภัย 3.1 อธิบายการทำงานของ AI ในการตรวจจับพฤติกรรมผิดปกติในพื้นที่สาธารณะได้ 3.2 แยกแยะบทบาทของ AI, Machine Learning และ IoT ในการทำงานของระบบรักษาความปลอดภัยได้ 3.3 วิเคราะห์ปัจจัยที่ส่งผลต่อความแม่นยำของระบบรักษาความปลอดภัย AI ได้ 3.4 อธิบายแนวคิดพื้นฐานของ Deep Learning ในระบบรักษาความปลอดภัยได้ 3.5 ระบุบทบาทของ Convolutional Neural Networks (CNN) ในการตรวจจับใบหน้าและตรวจจับวัตถุได้	-
2.	การติดตั้งและเชื่อมต่อบุคลากรในระบบรักษาความปลอดภัย	4. ตัวอย่างและการประยุกต์ใช้งานจริงของระบบรักษาความปลอดภัยด้วย AI 5. ประโยชน์และข้อจำกัดของระบบรักษาความปลอดภัยด้วย AI 1. การติดตั้งและเชื่อมต่อ HuskyLens ซึ่งเป็นการบูรณาการ AI ในตัว 2. การเชื่อมต่อและติดตั้งการทำงานของ AI ใน HuskyLens เพื่อให้ทำงานร่วมกับเทอร์โมโมเตอร์, Buzzer, LED	4.1 ออกแบบระบบด้วยสถานการณ์ที่ใช้ AI ในการรักษาความปลอดภัยได้ 5.1 เปรียบเทียบข้อดีของการใช้ AI กับการใช้มนุษย์ในระบบรักษาความปลอดภัยได้ ติดตั้งและเชื่อมต่อ HuskyLens กับไมโครคอนโทรลเลอร์ได้อย่างถูกต้อง ติดตั้งการทำงานของ AI ใน HuskyLens เพื่อควบคุมอุปกรณ์อื่น ๆ ในระบบรักษาความปลอดภัย	ความสามารถในการตั้งค่าและเชื่อมต่อ HuskyLens เพื่อใช้ในการตรวจจับภาพและวิเคราะห์การทุจริต ความสามารถในการตั้งค่า AI ใน HuskyLens เพื่อสั่งการควบคุมอุปกรณ์ต่าง ๆ ในระบบรักษาความปลอดภัย



หัวข้อที่	หัวข้อการเรียนรู้	เนื้อหา	วัตถุประสงค์	หัวข้อการประเมินที่เกี่ยวกับทักษะด้าน AI
3.	การเขียนโปรแกรมเพื่อควบคุมระบบรักษาความปลอดภัยด้วย AI	1. การเขียนโปรแกรมเพื่อสั่งการ HuskyLens ให้สามารถตรวจจับการบุกรุกและสั่งการอุปกรณ์อื่น ๆ 2. การปรับแต่งโปรแกรมเพื่อเพิ่มความแม่นยำและประสิทธิภาพของ AI ในการตรวจจับการบุกรุก	เขียนโปรแกรมเพื่อควบคุมการทำงานของ HuskyLens และไมโครคอนโทรลเลอร์ในระบบรักษาความปลอดภัย ปรับแต่งโปรแกรมให้ AI ใน HuskyLens สามารถทำงานได้อย่างแม่นยำและมีประสิทธิภาพมากขึ้น	ความถูกต้องและประสิทธิภาพของโปรแกรมในการควบคุมการทำงานของ AI สำหรับการตรวจจับและป้องกันการบุกรุก
4.	การทดสอบและปรับปรุงระบบรักษาความปลอดภัย	1. การทดสอบการทำงานของระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI รวมถึงการตรวจจับการบุกรุกและการตอบสนองของอุปกรณ์ต่าง ๆ 2. การวิเคราะห์และแก้ไขข้อผิดพลาดในการทำงานของ AI และปรับปรุงโปรแกรมให้ประสิทธิภาพมากขึ้น 3. การปรับแต่งและปรับปรุงการทำงานของ AI ใน HuskyLens ให้สามารถตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพในสถานการณ์ต่าง ๆ	ทดสอบระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI และระบุข้อผิดพลาดที่เกิดขึ้นได้ ระบุข้อผิดพลาดที่เกิดขึ้นในกระบวนการทำงานของ AI และแก้ไขปัญหานั้นได้ ปรับแต่งโปรแกรมและการทำงานของ AI ใน HuskyLens เพื่อให้ระบบรักษาความปลอดภัยทำงานได้อย่างมีประสิทธิภาพในทุกสถานการณ์	ความสามารถในการวิเคราะห์ข้อผิดพลาดของ AI และการปรับปรุงโปรแกรมเพื่อเพิ่มประสิทธิภาพในการตรวจจับการบุกรุก ความสามารถในการปรับแต่งโปรแกรม AI เพื่อให้ระบบรักษาความปลอดภัยสามารถตอบสนองต่อการบุกรุกในสถานการณ์ที่หลากหลาย

แผนการจัดการเรียนรู้

ชื่อวิชา อุปกรณ์อิเล็กทรอนิกส์ในระบบรักษาความปลอดภัย

รหัส 20105-2025

ชื่อหน่วย บูรณาการระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์กับระบบควบคุม

ชื่อเรื่อง ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก เวลา 4 ชั่วโมง

หัวข้อเรื่อง

1. ทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ (Introduction and Theory)
2. การติดตั้งและเชื่อมต่ออุปกรณ์
3. การเขียนโปรแกรมเพื่อควบคุมการตรวจจับการบุกรุก
4. การทดสอบและการปรับปรุงระบบ
5. การประยุกต์ใช้ระบบรักษาความปลอดภัยในสถานการณ์จริง

สาระสำคัญ

ระบบรักษาความปลอดภัยเป็นส่วนสำคัญในการปกป้องทรัพย์สินและบุคคลจากอันตรายและการบุกรุก ซึ่งในปัจจุบันเทคโนโลยีปัญญาประดิษฐ์ (AI) ได้เข้ามามีบทบาทสำคัญในการพัฒนาระบบรักษาความปลอดภัยให้มีความแม่นยำและประสิทธิภาพสูงขึ้น AI สามารถช่วยตรวจจับสิ่งผิดปกติได้อย่างรวดเร็วและแม่นยำ ด้วยการเรียนรู้และประมวลผลข้อมูลจากอุปกรณ์ต่างๆ ในระบบ เช่น กล้องตรวจจับใบหน้า, เซ็นเซอร์ตรวจจับการเคลื่อนไหว และการวิเคราะห์พฤติกรรมของบุคคลในพื้นที่ที่กำหนด

หนึ่งในอุปกรณ์ที่มีความสำคัญในระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI คือ HuskyLens ซึ่งเป็นกล้อง AI ที่สามารถตรวจจับและจดจำใบหน้า รวมถึงการเคลื่อนไหวได้อย่างแม่นยำ เมื่อทำงานร่วมกับไมโครคอนโทรลเลอร์ เช่น Arduino และอุปกรณ์เสริมต่างๆ อย่างเซอร์โวมอเตอร์และ Buzzer ระบบนี้สามารถสร้างระบบการเตือนภัยอัตโนมัติที่ตรวจจับการบุกรุกได้อย่างรวดเร็ว ระบบจะสามารถตอบสนองได้ทันทีเมื่อมีบุคคลที่ไม่รู้จักเข้ามาในพื้นที่ ระบบสามารถปลดล็อกหรือแจ้งเตือนเมื่อบุคคลที่รู้จักเข้าใช้งานได้ตามปกติ

การเขียนโปรแกรมเพื่อควบคุมการทำงานของระบบนี้ยังเป็นส่วนสำคัญที่ช่วยให้ระบบสามารถทำงานได้อย่างราบรื่น โดยการใช้ภาษาการเขียนโปรแกรมเพื่อสั่งงาน HuskyLens ในการตรวจจับการบุกรุก AI ช่วยวิเคราะห์สถานการณ์และทำการแจ้งเตือนเมื่อพบความผิดปกติ ทำให้งานรักษาความปลอดภัยมีความรวดเร็วและมีประสิทธิภาพมากขึ้น

นอกจากนี้ การทดสอบและปรับปรุงระบบยังเป็นขั้นตอนสำคัญเพื่อให้แน่ใจว่าระบบสามารถทำงานได้อย่างเหมาะสมในสถานการณ์ต่างๆ การปรับแต่งระบบให้สามารถตอบสนองตามสถานการณ์จริง จะช่วยเพิ่มความแม่นยำในการตรวจจับการบุกรุกได้ดียิ่งขึ้น

ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์จึงเป็นเทคโนโลยีที่มีศักยภาพสูงในการปกป้องชีวิตและทรัพย์สิน โดยเฉพาะในยุคที่เทคโนโลยีการตรวจจับและการแจ้งเตือนที่แม่นยำมีความสำคัญมากขึ้น

วัตถุประสงค์การเรียนรู้

1. สามารถอธิบายหลักการทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ได้
2. นักเรียนสามารถติดตั้งและเชื่อมต่ออุปกรณ์ในระบบรักษาความปลอดภัยได้
3. นักเรียนสามารถเขียนโปรแกรมพื้นฐานสำหรับการตรวจจับการบุกรุกโดยใช้ HuskyLens และไมโครคอนโทรลเลอร์ได้
4. นักเรียนสามารถทดสอบและปรับปรุงระบบให้ทำงานได้อย่างมีประสิทธิภาพ

ผลลัพธ์ที่คาดหวัง

หลังจากการเรียนรู้ ผู้เรียนจะมีความรู้พื้นฐานเกี่ยวกับระบบรักษาความปลอดภัยด้วย AI สามารถนำความรู้ไปใช้ในการพัฒนาหรือศึกษาระบบ AI ที่ซับซ้อนมากขึ้นเพื่อเพิ่มประสิทธิภาพในการทำงานและความปลอดภัยในระดับสูงสุดในบริบทต่างๆ ได้

เวลา	เรื่อง	วัตถุประสงค์	กิจกรรม
30 น.	ทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ (Introduction and Theory) 1. บทนำและความสำคัญของระบบรักษาความปลอดภัยด้วย AI	1.1 บอกความหมายของระบบรักษาความปลอดภัยด้วย AI ได้ 1.2 บอกบทบาทของ AI ในการตรวจจับการบุกรุกได้ 1.3 อธิบายความสำคัญของการตอบสนองแบบเรียลไทม์ในระบบรักษาความปลอดภัยด้วย AI ได้	- ทดสอบก่อนเรียน - บรรยายเรื่องความสำคัญของ AI และทฤษฎีพื้นฐานของระบบรักษาความปลอดภัย - แนะนำชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก - คุณสมบัติของระบบรักษาความปลอดภัยด้วย AI - ตัวอย่างและการประยุกต์ใช้งานจริงของระบบรักษาความปลอดภัยด้วย AI - ประโยชน์และข้อจำกัดของระบบรักษาความปลอดภัยด้วย AI
	2. ทฤษฎีพื้นฐานของระบบรักษาความปลอดภัยด้วย AI	2.1 บอกส่วนประกอบสำคัญในระบบรักษาความปลอดภัยได้ 2.2 ประยุกต์ใช้ความรู้เกี่ยวกับ Machine Learning เพื่ออธิบายการวิเคราะห์ข้อมูลใบหน้าที่ AI ใช้ในการจดจำบุคคลได้ 2.3 อธิบายตัวอย่างของระบบ IoT ที่ใช้ในระบบรักษาความปลอดภัย	
	3. คุณสมบัติของระบบรักษาความปลอดภัยด้วย AI	3.1 อธิบายการทำงานของ AI ในการตรวจจับพฤติกรรมผิดปกติในพื้นที่สาธารณะได้ 3.2 แยกแยะบทบาทของ AI, Machine Learning และ IoT ในการทำงานของระบบรักษาความปลอดภัยได้ 3.3 วิเคราะห์ปัจจัยที่ส่งผลกระทบต่อความแม่นยำของระบบรักษาความปลอดภัย AI ได้	

เวลา	เรื่อง	วัตถุประสงค์	กิจกรรม
		3.4 อธิบายแนวคิดพื้นฐานของ Deep Learning ในระบบรักษาความปลอดภัยได้ 3.5 ระบุบทบาทของ Convolutional Neural Networks (CNN) ในการจดจำใบหน้าและตรวจจับวัตถุได้	
	4. ตัวอย่างและการประยุกต์ใช้งานจริงของระบบรักษาความปลอดภัยด้วย AI	4.1 ออกแบบตัวอย่างสถานการณ์ที่ใช้ AI ในการรักษาความปลอดภัยได้	
	5. ประโยชน์และข้อจำกัดของระบบรักษาความปลอดภัยด้วย AI	5.1 เปรียบเทียบข้อดีของการใช้ AI กับการใช้มนุษย์ในระบบรักษาความปลอดภัยได้	
30 น.	การติดตั้งและเชื่อมต่ออุปกรณ์ (Hardware Setup and Connection)	นักเรียนสามารถติดตั้งและเชื่อมต่ออุปกรณ์ในระบบรักษาความปลอดภัยได้	- การสาธิตวิธีการเชื่อมต่อ HuskyLens กับ ไมโครคอนโทรลเลอร์และอุปกรณ์อื่นๆ - นักเรียนลงมือปฏิบัติติดตั้งและเชื่อมต่ออุปกรณ์ตามคำแนะนำ - การทดสอบการเชื่อมต่อเบื้องต้นของอุปกรณ์
1 ชม.	การเขียนโปรแกรมสำหรับการตรวจจับการบุกรุก (Programming for Intrusion Detection)	นักเรียนสามารถเขียนโปรแกรมพื้นฐานเพื่อควบคุมระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI	- การแนะนำโค้ดตัวอย่างสำหรับการเขียนโปรแกรมเพื่อใช้ HuskyLens ตรวจจับการบุกรุก - นักเรียนลงมือเขียนโปรแกรมและทดสอบการทำงานของระบบ - การปรับแต่งโปรแกรมให้ตอบสนองตามการทำงานที่ต้องการ

เวลา	เรื่อง	วัตถุประสงค์	กิจกรรม
1 ชม.	การทดสอบและปรับปรุงระบบ (Testing and System Refinement)	นักเรียนสามารถทดสอบและปรับปรุงระบบรักษาความปลอดภัยให้ทำงานได้อย่างมีประสิทธิภาพ	- นักเรียนทดสอบระบบที่ได้พัฒนาในสถานการณ์ต่างๆ - การวิเคราะห์ผลลัพธ์และการแก้ไขข้อผิดพลาดที่พบ - การอภิปรายและแลกเปลี่ยนความคิดเห็นเกี่ยวกับการปรับแต่งและปรับปรุงการทำงานของ AI ให้สามารถตรวจจับการบุกรุกได้อย่างมีประสิทธิภาพในสถานการณ์ต่าง ๆ - ทดสอบหลังเรียน
1 ชม.	ประเมินผลการปฏิบัติงาน	เพื่อประเมินผลทักษะในการปฏิบัติงาน	- สอบปฏิบัติ

การประเมินผล

- การทดสอบก่อนและหลังการเรียนรู้ (Pre-Test/Post-Test): ประเมินความรู้พื้นฐานและความเข้าใจของนักเรียน
- ประเมินผลการปฏิบัติงาน (Performance Assessment)
- การสำรวจความคิดเห็น (Feedback Survey) : สำรวจทัศนคตินักเรียนต่อการเรียนรู้

ทรัพยากรที่ใช้

- อุปกรณ์ : ชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก
- ซอฟต์แวร์ : Arduino IDE หรือซอฟต์แวร์อื่นๆ สำหรับการเขียนโค้ด
- สื่อการเรียนรู้ : สไลด์ประกอบการสอน, คู่มือการใช้งานอุปกรณ์



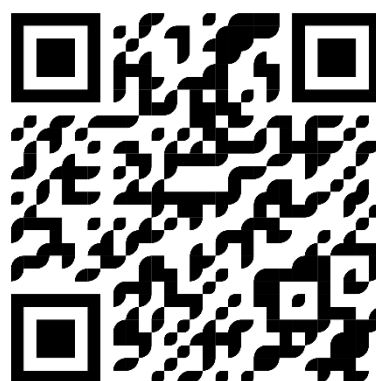
KNOWLEDGE TEST

แบบทดสอบวัดความรู้
ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

* ระบุว่าเป็นคำถามที่จำเป็น

ชื่อ *

คำตอบของคุณ



ภาพที่ ข-1 แบบทดสอบวัดความรู้ระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์
ในการตรวจจับการบุกรุก

ใบปฏิบัติงานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก
เรื่อง งานระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก **เวลา 60 นาที**
รหัสวิชา 20105-2125 วิชาอุปกรณ์อิเล็กทรอนิกส์ในระบบรักษาความปลอดภัย ระดับ ปวช.3

ชื่อ – นามสกุล **เลขที่** **กลุ่มที่.....**

จุดประสงค์เชิงพฤติกรรม เมื่อทดลองนี้จบแล้ว ผู้เรียนสามารถ

1. ผู้เรียนสามารถติดตั้งและเชื่อมต่อ HuskyLens กับไมโครคอนโทรลเลอร์ได้อย่างถูกต้อง
2. ผู้เรียนสามารถตั้งค่าการทำงานของ AI ใน HuskyLens เพื่อควบคุมอุปกรณ์อื่น ๆ ในระบบรักษาความปลอดภัย
3. ผู้เรียนสามารถเขียนโปรแกรมเพื่อควบคุมการทำงานของ HuskyLens และไมโครคอนโทรลเลอร์ในระบบรักษาความปลอดภัย
4. ผู้เรียนสามารถปรับแต่งโปรแกรมให้ AI ใน HuskyLens สามารถทำงานได้อย่างแม่นยำและมีประสิทธิภาพมากขึ้น
5. ผู้เรียนสามารถทดสอบระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วย AI และระบุข้อผิดพลาดที่เกิดขึ้นได้
6. ผู้เรียนสามารถระบุข้อผิดพลาดที่เกิดขึ้นในกระบวนการทำงานของ AI และแก้ไขปัญหาเหล่านั้นได้
7. ผู้เรียนสามารถปรับแต่งโปรแกรมและการทำงานของ AI ใน HuskyLens เพื่อให้ระบบรักษาความปลอดภัยทำงานได้อย่างมีประสิทธิภาพในทุกสถานการณ์

เครื่องมือและอุปกรณ์

AI Security System Learning Kit Intrusion detection

ขั้นตอนการปฏิบัติงาน

ขั้นตอนที่ 1 การเตรียมอุปกรณ์และการเชื่อมต่อวงจร

- 1.1 เชื่อมต่อ เซอร์ไวโมเตอร์ ตัวที่ 1 กับพอร์ตดิจิทัล 5 และตัวที่ 2 กับพอร์ตดิจิทัล 6 ของ Arduino
- 1.2 เชื่อมต่อ HuskyLens ที่พอร์ต RX = 10 และ TX = 11 ของ Arduino
- 1.3 ตั้งค่า Face Recognition Algorithm ใน HuskyLens
- 1.4 เชื่อมต่อ LED ที่พอร์ตดิจิทัล 3 และ Buzzer ที่พอร์ตดิจิทัล 8
- 1.5 เชื่อมต่อ สวิตช์ ที่พอร์ตดิจิทัล 4 พร้อมใช้ Pullup Resistor

ขั้นตอนที่ 2 การติดตั้งและเขียนโปรแกรม

2.1 เปิดโปรแกรม Arduino IDE และทำการติดตั้งไลบรารีที่จำเป็น ได้แก่

- ไลบรารีสำหรับ HuskyLens (ใช้ Library Manager เพื่อติดตั้ง)
- ไลบรารีสำหรับ Servo (ใช้ Library Manager เพื่อติดตั้ง)

2.2 เปิดไฟล์โปรแกรมจากโค้ดที่ให้มาในใบปฏิบัติงานนี้ แล้วทำการคัดลอกลงใน Arduino IDE ของคุณ

2.3 ตั้งค่า AI ใน HuskyLens เพื่อสั่งการควบคุมอุปกรณ์ในระบบรักษาความปลอดภัย

- ตั้งค่าให้ HuskyLens สั่งงาน Servo Motor ให้ปลดล็อกเมื่อพบใบหน้าที่ได้รับอนุญาต

- ตั้งค่าให้ HuskyLens สั่งงาน Buzzer และ LED แจ้งเตือนเมื่อพบใบหน้าที่ไม่ได้

รับอนุญาต

ขั้นตอนที่ 3 การตรวจสอบโปรแกรม

3.1 ตรวจสอบความถูกต้องของโค้ดและเลือกบอร์ดที่ใช้งาน (Arduino Nano)

3.2 กด Verify เพื่อตรวจสอบความถูกต้องของโปรแกรม

3.3 หากโค้ดไม่มีข้อผิดพลาด ให้กด Upload เพื่ออัปโหลดโค้ดลงบอร์ด

ตัวอย่างโปรแกรมที่ 5.2.1

```
#include <SoftwareSerial.h>
#include "HUSKYLENS.h"
#include <Servo.h>

// กำหนดพอร์ต RX และ TX สำหรับ HuskyLens
SoftwareSerial huskySerial(10, 11); // RX = 10, TX = 11
HUSKYLENS huskylens;

Servo doorLock1; // Servo สำหรับประตูชั้นที่ 1
Servo doorLock2; // Servo สำหรับประตูชั้นที่ 2

const int outputPin = 3; // พอร์ตดิจิทัลสำหรับเอาต์พุต เช่น LED
const int switchPin = 4; // พอร์ตดิจิทัลสำหรับสวิตช์
int switchState; // ประกาศตัวแปร switchState

const int servoPin1 = 5; // พอร์ตดิจิทัลสำหรับเซอร์โวมอเตอร์ตัวแรก
const int servoPin2 = 6; // พอร์ตดิจิทัลสำหรับเซอร์โวมอเตอร์ตัวที่สอง
const int buzzerPin = 8; // พอร์ตดิจิทัลสำหรับ Buzzer

const int authorizedIDs[] = {1, 2, 3, 4, 5}; // อาร์เรย์ของ ID ผู้ใช้ที่ได้รับอนุญาต
const int numAuthorizedIDs = sizeof(authorizedIDs) / sizeof(authorizedIDs[0]); //
จำนวน ID ที่ได้รับอนุญาต
```

```

bool faceAuthorized = false; // สถานะการตรวจจับใบหน้าที่ได้รับอนุญาต

void setup() {
  Serial.begin(9600);          // เริ่มต้น Serial สำหรับการ debug
  huskySerial.begin(9600);     // เริ่มต้น HuskyLens ผ่าน UART
  huskylens.begin(huskySerial);
  doorLock1.attach(servoPin1); // Servo ประตูล็อก 1 เชื่อมต่อที่พอร์ตดิจิตอล 5
  doorLock2.attach(servoPin2); // Servo ประตูล็อก 2 เชื่อมต่อที่พอร์ตดิจิตอล 6

  pinMode(switchPin, INPUT_PULLUP); // ตั้งค่าให้สวิตช์เป็น input แบบ Pullup (พอร์ต
  ดิจิตอล 4)
  pinMode(outputPin, OUTPUT);       // ตั้งค่า LED เป็นเอาต์พุต (พอร์ตดิจิตอล 3)
  pinMode(buzzerPin, OUTPUT);       // ตั้งค่า Buzzer เป็นเอาต์พุต (พอร์ตดิจิตอล 8)

  if (!huskylens.writeAlgorithm(ALGORITHM_FACE_RECOGNITION)) {
    Serial.println("ตั้งค่าอัลกอริทึมไม่สำเร็จ");
    while (1);
  }

  // ล็อกประตูล็อกทั้งสองขั้นตอนเริ่มต้น
  doorLock1.write(0); // ล็อกประตูล็อก 1
  doorLock2.write(0); // ล็อกประตูล็อก 2
}

void loop() {
  faceAuthorized = false; // รีเซ็ตสถานะการตรวจจับใบหน้าที่ได้รับอนุญาต

  if (huskylens.request()) {
    HUSKYLENSResult result = huskylens.read();
    if (result.command == COMMAND_RETURN_BLOCK) {
      for (int i = 0; i < numAuthorizedIDs; i++) {
        if (result.ID == authorizedIDs[i]) { // ตรวจสอบว่า ID ของใบหน้าที่ตรงกับ ID ที่
        ได้รับอนุญาตหรือไม่
          Serial.println("ตรวจพบใบหน้าที่ได้รับอนุญาต!");
        }
      }
    }
  }
}

```

```

        faceAuthorized = true; // ตั้งค่าสถานะว่าพบใบหน้าที่ได้รับอนุญาต
        break; // ออกจาก loop เมื่อตรวจพบใบหน้าที่ได้รับอนุญาต
    }
}

if (!faceAuthorized) { // หากไม่มีการตรวจพบใบหน้าที่ได้รับอนุญาต
    Serial.println("ตรวจพบใบหน้าที่ไม่ได้รับอนุญาต!");
    triggerAlarm2(); // แจ้งเตือนด้วย Buzzer หากเป็นใบหน้าที่ไม่ได้รับอนุญาต
}

}

if (faceAuthorized) {
    unlockDoor1(); // ปลดล็อกประตูชั้นแรกเมื่อใบหน้าได้รับอนุญาต
} else {
    triggerAlarm1(); // ถ้าไม่ใช่ใบหน้าที่ได้รับอนุญาต ให้แจ้งเตือน
}

// ตรวจสอบสวิตช์สำหรับการปลดล็อกประตูชั้นที่สอง
if (digitalRead(switchPin) == LOW) { // เมื่อกดสวิตช์ (สัญญาณ LOW)
    unlockDoor2(); // ปลดล็อกประตูชั้นที่ 2
} else {
    triggerAlarm1(); // ถ้าไม่ใช่ใบหน้าที่ได้รับอนุญาต ให้แจ้งเตือน
}

delay(1000); // รอ 1 วินาที
}

void unlockDoor1() {
    doorLock1.write(90); // ปลดล็อกประตูชั้นที่ 1
    digitalWrite(outputPin, HIGH); // เปิด LED
    delay(5000); // รอ 5 วินาทีเพื่อให้ผ่าน
    doorLock1.write(0); // ล็อกประตูชั้นที่ 1
    digitalWrite(outputPin, LOW); // ปิด LED
}

```

```

void unlockDoor2() {
  doorLock2.write(90); // ปลดล็อกประตูชั้นที่ 2
  digitalWrite(outputPin, HIGH); // เปิด LED
  delay(5000); // รอ 5 วินาทีเพื่อให้ผ่าน
  doorLock2.write(0); // ล็อกประตูชั้นที่ 2
  digitalWrite(outputPin, LOW); // ปิด LED
}

void triggerAlarm1() {
  digitalWrite(outputPin, HIGH); // เปิดสัญญาณ LED แจ้งเตือน
  delay(2000); // แจ้งเตือนเป็นเวลา 2 วินาที
  digitalWrite(outputPin, LOW); // ปิดสัญญาณ LED
}

void triggerAlarm2() {
  digitalWrite(buzzerPin, HIGH); // เปิดสัญญาณเสียง Buzzer
  delay(2000); // แจ้งเตือนเป็นเวลา 2 วินาที
  digitalWrite(buzzerPin, LOW); // ปิดสัญญาณเสียง Buzzer
}

```

ชื่อไฟล์

1.3 ตรวจสอบความถูกต้องของโปรแกรมโดยกด Toolbar verify

1.4 อัปโหลดโปรแกรมลงบอร์ด โดยกด Toolbar upload

1.5 ทดสอบพร้อมบันทึกผลการทำงานของของโปรแกรม

.....

.....

.....

1.6 อธิบายพร้อมแสดงผลการทำงานของวงจร(หยุดรอตรวจสอบ)

ขั้นตอนที่ 4 การทดสอบการทำงานของระบบ

1. ทดสอบระบบด้วยการเปิดสวิตช์เพื่อให้ระบบเริ่มการตรวจจับใบหน้า

2. ตรวจสอบการทำงานของเซอร์โวมอเตอร์และ LED ว่าทำงานตามโปรแกรมที่กำหนดไว้หรือไม่
3. เมื่อระบบตรวจพบใบหน้าที่ได้รับอนุญาต ประตูล็อก (เซอร์โวมอเตอร์หมุน)
4. หากพบใบหน้าที่ไม่ได้รับอนุญาต Buzzer ควรดังเพื่อแจ้งเตือน

ขั้นตอนที่ 5 การแก้ไขปัญหและพัฒนาระบบ

1. หากระบบทำงานผิดพลาด เช่น ไม่สามารถจดจำใบหน้าได้ ให้ตรวจสอบการเชื่อมต่อของ HuskyLens หรือการตั้งค่าไลบรารี
2. ปรับปรุงโค้ดให้เหมาะสม เช่น เพิ่มเวลาในการปลดล็อกประตู หรือปรับระดับความไวในการตรวจจับใบหน้า
3. ปรับแต่งโปรแกรม AI เพื่อเพิ่มประสิทธิภาพในการตรวจจับโดย
 - ปรับปรุงเพื่อลด False Positive และ False Negative
 - เพิ่มความแม่นยำของระบบ $\geq 10\%$
4. วิเคราะห์ข้อผิดพลาดและแก้ไขโปรแกรม

.....

.....

.....

ขั้นตอนที่ 6 ทดสอบระบบในสถานการณ์จำลอง

1. ทดสอบระบบในสภาพแสงปกติ
2. ทดสอบระบบในสภาพแสงน้อย
3. ทดสอบระบบในการตรวจจับหลายเป้าหมายพร้อมกัน
4. ปรับแต่งโปรแกรมให้ระบบตอบสนองในสถานการณ์หลากหลาย
 - ปรับโปรแกรมให้ตอบสนองในสถานการณ์แสงน้อย
 - ปรับโปรแกรมให้รองรับการตรวจจับหลายเป้าหมายพร้อมกัน

คำถามเพื่อการทบทวน:

1. โมดูล HuskyLens ทำหน้าที่อะไรในระบบนี้
2. ระบบนี้สามารถนำไปใช้งานจริงในสถานการณ์ใดได้บ้าง
3. หากต้องการเพิ่มความปลอดภัยในระบบนี้ คุณจะแก้ไขหรือเพิ่มอุปกรณ์ใดบ้าง

สรุปผล

.....

.....

.....

.....



แบบบันทึกผลการประเมิน

คำชี้แจงสำหรับผู้เข้าสอบ: แบบบันทึกผลการปฏิบัติงานสำหรับระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก

ส่วนที่ 1 ข้อมูลผู้เข้าสอบ

ชื่อผู้เข้า

สอบ:

เลขประจำตัว

วันที่สอบ:

คะแนนรวม (เต็ม 80 คะแนน):	
ผลการประเมิน:	☐ ผ่าน (≥ 56 คะแนน) ☐ ไม่ผ่าน (< 56 คะแนน)
ข้อเสนอแนะจากผู้ตรวจ:	

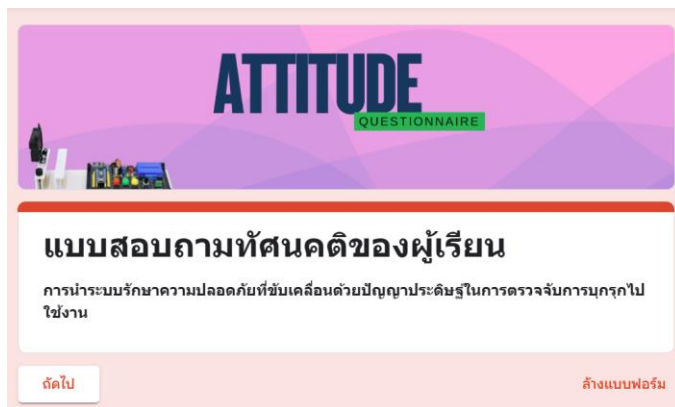
ลงชื่อ.....ผู้ตรวจ
()

ส่วนที่ 3 สรุปคะแนนและผลการประเมิน

ส่วนที่ 2 บันทึกผลการประเมิน

ตารางประเมินแบบรูบริคสำหรับการประเมินแบบปฏิบัติ (ระดับคุณภาพ 5 ระดับ)

งาน/หัวข้อ	ระดับ 5 (ยอดเยี่ยม)	ระดับ 4 (ดีมาก)	ระดับ 3 (ดี)	ระดับ 2 (พอใช้)	ระดับ 1 (ควรปรับปรุง)	คะแนน เต็ม	คะแนน ที่ได้
งานที่ 1 การ ตั้งค่า HuskyLens	เชื่อมต่อ HuskyLens กับ Arduino และตั้งค่า Face Recognition Algorithm ได้สำเร็จโดย ไม่มีข้อผิดพลาด การ เดินสายสะอาดและมั่นคง	เชื่อมต่อและตั้งค่าได้ สมบูรณ์ แต่มี ข้อผิดพลาดเล็กน้อย	เชื่อมต่อและตั้งค่าได้ บางส่วน มี ข้อผิดพลาดในสาย หรือการตั้งค่า	เชื่อมต่อและตั้ง ค่าได้เพียง เล็กน้อย ระบบ ทำงานไม่ สมบูรณ์	ไม่สามารถ เชื่อมต่อหรือตั้ง ค่าได้ มีปัญหา สำคัญใน กระบวนการ	10	
งานที่ 2 การ ตั้งค่า AI สำหรับ ควบคุม อุปกรณ์	ตั้งค่า AI ให้ควบคุม Servo Motor และ Buzzer/LED ตอบสนอง ได้แม่นยำทุกครั้ง	ตั้งค่า AI สำเร็จเกือบ สมบูรณ์ มี ข้อผิดพลาดเล็กน้อย ในบางครั้ง	ตั้งค่า AI ได้บางส่วน การตอบสนองล่าช้า หรือไม่เสถียร	ตั้งค่าได้เพียง บางส่วน ระบบ ทำงานไม่ สมบูรณ์	ไม่สามารถตั้งค่า AI สำหรับ ควบคุมอุปกรณ์ ได้	10	
งานที่ 3 การ ทดสอบความ ถูกต้องและ ประสิทธิภาพ	ความแม่นยำ $\geq 90\%$ ใน True Positive และ $\leq 5\%$ ใน False Positive	ความแม่นยำ 80– 89% ใน True Positive และ $\leq 10\%$ ใน False Positive	ความแม่นยำ 70– 79% ใน True Positive และ $\leq 15\%$ ใน False Positive	ความแม่นยำ 60–69% หรือ False Positive $\leq 20\%$	ความแม่นยำ $< 60\%$ หรือ False Positive $> 20\%$	15	
งานที่ 4 การ ปรับปรุง ประสิทธิภาพ โปรแกรม AI	ลด False Positives/Negatives $\geq 15\%$ และเพิ่มความ แม่นยำ $\geq 15\%$	ลด False Positives/Negatives $\geq 10\%$ และเพิ่มความ แม่นยำ $\geq 10\%$	มีการปรับปรุง บางส่วนใน False Positives/Negatives หรือความแม่นยำ	ปรับปรุงได้ น้อย ระบบยังมี ข้อผิดพลาด ชัดเจน	ไม่มีการ ปรับปรุงระบบ	10	
งานที่ 5 การ ทดสอบใน สถานการณ์ จำลอง	ระบบทำงานได้สมบูรณ์ ในทุกเงื่อนไข (แสงปกติ แสงน้อย หลายเป้าหมาย พร้อมกัน)	ระบบทำงานได้ดีใน เกือบทุกเงื่อนไข มี ปัญหาเล็กน้อย	ระบบทำงานได้ใน 1- 2 เงื่อนไข แต่มีปัญหา ในบางสถานการณ์	ระบบล้มเหลว ในเงื่อนไขที่ทำให้ หาย แต่ สามารถทำงาน พื้นฐานได้	ระบบล้มเหลว ในหลาย สถานการณ์ การตอบสนอง ไม่สม่ำเสมอ	15	
งานที่ 6 การ วิเคราะห์ ข้อผิดพลาด และแก้ไข	วิเคราะห์และแก้ไข ข้อผิดพลาดได้อย่าง ละเอียดสมบูรณ์ ระบบ ปรับปรุงดีขึ้นชัดเจน	วิเคราะห์และแก้ไข ข้อผิดพลาดส่วนใหญ่ ได้	วิเคราะห์และแก้ไข ข้อผิดพลาดได้ บางส่วน	วิเคราะห์ ข้อผิดพลาดได้ เล็กน้อย ระบบ ยังคงมีปัญหา	ไม่สามารถ วิเคราะห์หรือ แก้ไข ข้อผิดพลาดได้	10	
งานที่ 7 การ ปรับปรุง ให้ตอบสนอง ใน สถานการณ์ หลากหลาย	ปรับปรุงโปรแกรมให้รองรับ สถานการณ์แสงน้อยและ หลายเป้าหมายได้ สมบูรณ์	ปรับปรุงโปรแกรมรองรับ สถานการณ์ส่วนใหญ่ ได้	ปรับปรุงโปรแกรมได้ บางส่วน ระบบ ทำงานได้ดีขึ้นในบาง สถานการณ์	ปรับปรุงโปรแกรม ได้น้อยมาก ระบบยังไม่ ตอบสนองดีพอ	ไม่สามารถปรับ โปรแกรมให้ รองรับ สถานการณ์ใหม่ ได้	10	
รวม						80	



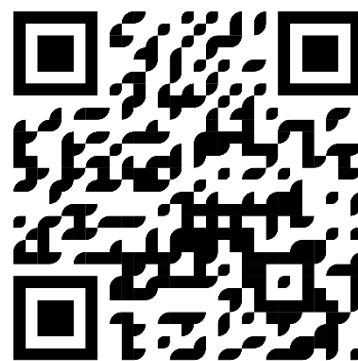
ATTITUDE
QUESTIONNAIRE

แบบสอบถามทัศนคติของผู้เรียน

การนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน

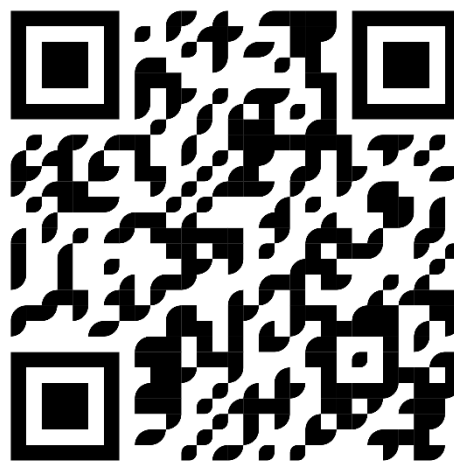
ถัดไป

ล้างแบบฟอร์ม



ภาพที่ ข-2 แบบสอบถามทัศนคติของผู้เรียนการนำระบบรักษาความปลอดภัยที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุกไปใช้งาน





ภาพ ข-3 คู่มือการใช้งาน

ภาคผนวก ค

- หนังสือเชิญเข้าร่วมการประชุม
- เกียรติบัตรเข้าร่วมนำเสนอบทความทางวิชาการ
- เอกสารเผยแพร่บทความทางวิชาการ





17th International Congress on Advanced Applied Informatics

December 16 - 18, 2024, Hotel Ciputra Jakarta, Indonesia

Invitation Letter

December 13th, 2024

Dear Jirawan Khoprakhon,

We would like to invite you to present your paper and to exchange advanced issues in the applied informatics research at the IIAI AAI 2024-Winter (December 16 - 18, 2024 at Jakarta). And we invite you to stay at the city in the period of congress for your participation to the convention to be held in Jakarta. This visit will provide opportunity for you to contribute your experience to the IIAI AAI 2024-Winter as a speaker, as an audience, or as staffs in the Conference and workshop. Further, in addition to the Conference and workshop, we provide you the opportunity of discussion with multiple researchers who specialize the Information technology, Computer science and other related areas.

Sincerely,

Tokuro Matsuo, Ph.D
Finance Chair
Advanced Institute of Industrial Technology

ภาพที่ ค-1 หนังสือเชิญเข้าร่วมการประชุม



ภาพที่ ค-2 เกียรติบัตรเข้าร่วมนำเสนอบทความทางวิชาการ



ภาพที่ ค-3 เกียรติบัตรรางวัลของบทความทางวิชาการ

Design and Implementation of a Practical AI Security System Learning Kit for Intrusion Detection

Jirawan Khoprakhon
Faculty of Technical Education
King Mongkut's University of Technology
North Bangkok
Bangkok, Thailand
jirawan.khoprakhon@gmail.com

Suppachai Howimanporn
Faculty of Technical Education
King Mongkut's University of Technology
North Bangkok
Bangkok, Thailand
suppachai.h@fte.kmutnb.ac.th

Sasithorn Chookaew
Faculty of Technical Education
King Mongkut's University of Technology
North Bangkok
Bangkok, Thailand
sasithorn.c@fte.kmutnb.ac.th

Abstract— Artificial intelligence (AI) is an essential component of today's security systems, especially in intrusion detection systems that use AI to analyze images and signals from closed-circuit television (CCTV) cameras and sensors, which will increase detection accuracy and reduce human errors. Therefore, vocational education must be developed in line with the advancement of AI technology to better prepare students for careers in related industries. However, the current challenge is that vocational education needs to fully integrate AI technology, primarily due to the lack of appropriate learning materials and understanding of the application of AI in security systems. This study aims to create a practical AI security system learning kit for intrusion detection to teach students practical skills in AI-driven security systems in real-world scenarios. A total of 20 vocational students were recruited for the experiment study. The results showed that the students had high-practical skills and positive attitudes after using the learning kit.

Keywords— *AI in Security Systems, Practical Learning Kit, Intrusion detection systems.*

I. INTRODUCTION

Today, technology and artificial intelligence (AI) play vital roles in daily life, particularly securing assets and information. Utilizing AI in intrusion detection systems has greatly enhanced both accuracy and efficiency. As a result, vocational education must update its curriculum and teaching methods to keep pace with these technological advancements, ensuring that students acquire modern skills and knowledge [1].

AI-powered security systems are gaining popularity in both business and residential sectors. AI intrusion detection systems can accurately analyze CCTV footage and other signals, significantly reducing human error and increasing security where these systems are installed [2]. Therefore, integrating AI technology into security systems has become a critical skill for vocational students. Developing practical learning kits that focus on AI-driven intrusion detection will provide students

with the understanding and hands-on experience needed to apply their knowledge in real-world scenarios, helping them better meet the demands of the job market [3].

Thailand's vocational certificate curriculum clearly emphasizes modern technology's importance in teaching and learning. This includes developing practical learning kits that address market and industry demands. Many curricula aim to equip students with applicable knowledge and skills for their future careers [4]. One current challenge is that vocational education still needs to integrate AI technology fully into its teaching due to a need for appropriate learning materials and an understanding of AI's role in security systems. As a result, students need to develop the necessary skills to work in industries that require these technologies [5].

The learning of AI-driven intrusion detection technology can help enhance vocational students' skills and knowledge, enabling them to apply what they have learned in real-world settings effectively. Furthermore, it prepares them for careers related to security and AI technology [6]. The research and development of these learning kits must consider content design that is easy to understand and engaging, incorporating modern technology and equipment to give students real-world experience. The kits must be suitable for classroom teaching and practical application in the workplace [7-8].

Thus, this study focuses on developing practical learning kits for AI-based intrusion detection systems that will enhance the capabilities of vocational students in electronics, aligning their skills with labor market demands. It increases their career opportunities and contributes to national development in technology and innovation. Investing in human resources is critical to ensuring sustainable progress for the country.

II. RELATE WORK

A. AI and Security Systems

In the digital age, where artificial intelligence (AI) and security systems play a crucial role in many industries, the demand for AI skills such as data processing, image analysis, and machine learning to improve the accuracy and efficiency of systems such as facial recognition and intrusion detection is increasing rapidly [9]. In addition, security skills in designing, installing, and maintaining AI-connected systems are in high demand, especially CCTV installation and access control system design [10]. Programming skills and algorithm development are also crucial in creating systems that can learn from data and improve performance [11].

B. Vocational Students' AI Skills

Developing AI skills for vocational students is crucial, as AI plays a key role in driving technology and innovation across industries. Teaching the Python programming language can help vocational students develop practical AI-related programming skills by providing a foundational understanding of machine learning (ML) and understanding AI algorithms, which are essential foundations for developing AI skills for future careers [12]. Some studies presented project-based learning as a highly effective method, providing students with real-world problem-solving experience using HuskyLens as an AI tool that helps them practice understanding how to use AI to detect and control systems [13]. In addition, AI can significantly improve manufacturing efficiency by reducing manufacturing errors and enabling more effective, informed decision-making [14]. According to AI being combined with Internet of Things (IoT) technologies, students can develop more complex skills related to controlling and connecting devices in automation systems, which will be helpful in industries that rely on intelligent systems to operate effectively in today's era [15].

C. Intrusion detection systems

Intrusion Detection Systems (IDS) in physical security often use facial recognition technology, an effective way to identify people and prevent unauthorized access to areas. This technology can be used in various contexts, such as buildings, offices, factories, and smart homes. CCTV is used in conjunction with facial recognition to prevent intrusion into buildings. The system detects people's faces entering the area and compares them to a database of authorized persons [16].

The system will send an alarm if the intruder is not found in the database, stating that industrial plants use facial recognition technology to control access to specific critical areas [17]. It suggests that smart homes use a facial recognition system connected to a door lock system and send an alert via a smartphone to increase the accuracy and efficiency of intrusion detection in high-security areas [18]. Therefore, the combination of facial recognition and suspicious behavior detection can increase the accuracy and efficiency of intrusion detection in high-security areas [19].

D. Practical learning modules

The AI practical learning modules for intrusion detection systems should cover theory and practice. Starting with teaching the basics of AI and machine learning, learners will practice using AI camera modules such as HuskyLens for face detection and recognition. They will also practice programming the cameras and sensors used for intrusion detection. Testing the system in real-world situations will allow learners to gain a deeper understanding of the system's operation and improve it to increase its accuracy. Finally, there should be an evaluation to ensure that learners can develop a detection system that meets the needs of real-world applications [20].

III. DEVOPMENT OF LEARNING KIT

A. Conceptual framework

In this study, we have proposed the conceptual framework to plan the research design and develop an AI-driven security-focused practical learning module for intrusion detection to build students' skills, as shown in Fig 1.

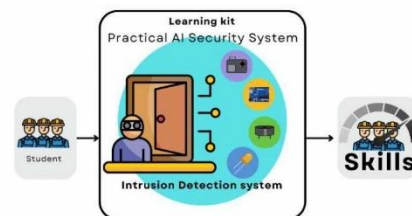


Fig. 1. The conceptual framework

B. Designing a practical learning kit in an AI security system

We attempted to design a low-cost AI security learning kit for intruder detection, so we used Arduino Nano, alarm, servomotor, and ESP-01 based on several critical theoretical concepts. In addition, we have selected HuskyLens as an AI module that uses convolutional neural network (CNN) technology for image processing, enabling face and object recognition even on resource-constrained and low-cost devices [21].

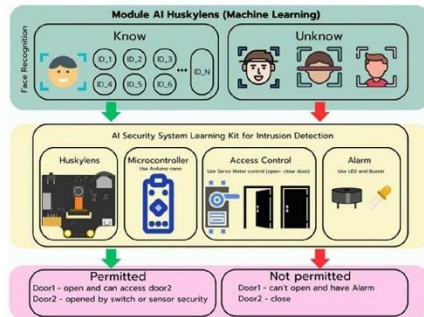


Fig. 2. The structure of practical AI security system operation

Fig 2 shows the structure of practical AI security system operation. Integrating AI into security systems enables the system to detect and respond to threats quickly and efficiently without requiring considerable resources [25]. Energy-efficient system designs, such as those of ESP-01 and Arduino Nano, are cost-effective regarding both usage and operating costs [26]. Integrating AI into security systems enables the system to detect and respond to threats quickly and efficiently without requiring considerable resources. Energy-efficient system designs, such as those of ESP-01 and Arduino Nano, are cost-effective regarding both usage and operating costs.

Fig 3 shows the design of a printed circuit board (PCB), also called a printed wiring board (PWB). It is a medium used to connect or "wire" components to one another in a circuit of learning kits.

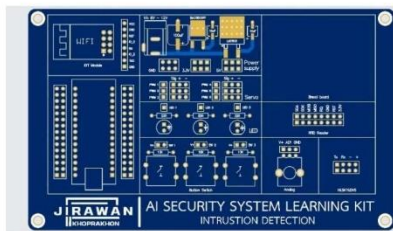
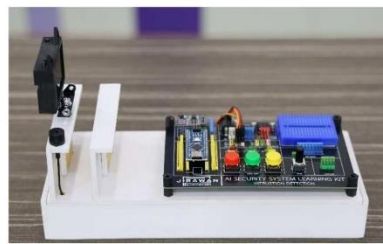


Fig. 3. Design of printed wiring board

After that, we have developed a practical learning kit in an AI security system based on planning (see in Fig 4 (a) & (b)).



(a)



(b)

Fig. 4. A Practical AI Security System Learning Kit

In addition, we use Arduino program to control the learning kit to detect the object based on condition, as shown in Fig 5.

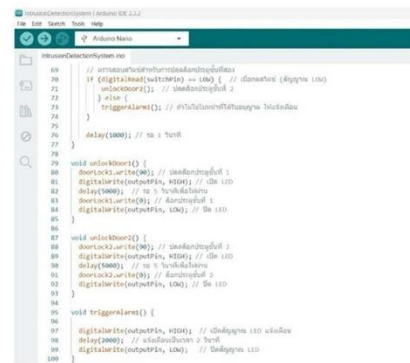


Fig. 5. Example of writing the Arduino program

IV. METHOD

A. Participants

Twenty vocational students in major of electronics engineering in 3rd years vocational certificate program at Nakhonnayok Technical College in central of Thailand. They enrolled the electronic devices in security systems course. We have the leaning activity is part of subject. They take the a performance test to evaluate the student's performance skill after using AI-powered security systems for intrusion detection.



Fig. 6. The students participated in learning activities

B. Data collection

In this research experiment, 20 vocational students attended the learning activity. They had an estimated 4 hours to participate in learning activities and demonstrations. Before they used the AI-driven security system learning kit for intrusion detection, they received instructions from instructors on how to use and learn. After completing the learning activity, they took the practical skills test for about 60 minutes, as shown in Fig 7.



Fig. 7. Implementation in classroom

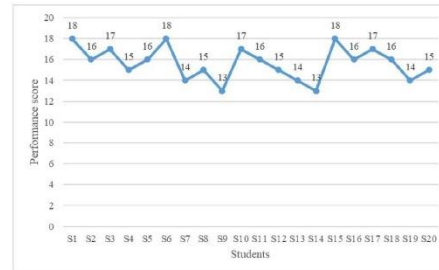


Fig. 8. The result of students' performance skill

Fig 8 shows the results of 20 vocational students' practical skills after using the learning kit in a learning activity. The total score is 20 in this activity, and they scored a performance skill score between 13 and 18. Namely, they have high-practical skills ($M=15.65$, $S.D.=1.35$).

In addition, we have a semi-structured interview to assess the student attitudes after using the learning kit in learning activities as follows:

How do you feel about using the training kit?

Student A: "I like it because it is easy to connect. It does not need to be connected to the ground, and there are few wires."

Do you think about the code written?

Student B: "It is similar to when I studied microcontrollers, but it adds more conditions."

Do you think about using an AI camera to capture and integrate faces with the system?

Student C: "It can identify more people because the camera module captures faces, stores them as IDs, and can be used with the system code."

Can you write a program to capture faces ourselves and use it with this system?

Student D: "I think I can do it; however, based on the theory, it will be more complicated and difficult than this one and might take a long time."

V. CONCLUSION

The study is the development of a practical AI security system learning kit for intrusion detection. The results show that they had the performance skills, indicating that the developed learning kit increased the performance skills of the learners. In addition to learning the intrusion detection system, this learning kit can be applied to teach other systems, such as access control systems, object recognition systems, motion detection systems, vehicle inspection systems, automated warehouse management systems, and many others. One area for improvement is the use of the learning kit, as it is a cheap learning kit with a clear separation of learning sections. The devices used in the kit, such as the controller, may not be as

efficient as expensive controllers. It is only used to learn skills in AI technology applications.

VI. FUTURE WORK

Future research may improve the practical learning kit by integrating advanced AI technologies, such as machine learning algorithms, for predictive security measures. In addition, one limitation found in using this learning kit is that some of the devices in the learning kit, such as controllers, may need more performance compared to expensive controllers used in real work. Cheap learning kits are mainly designed to allow learners to practice skills in applying AI technology, but they may need to be able to replace commercial equipment fully. Therefore, further development should focus on improving the performance of the devices used in the learning kit to respond to more complex applications.

In addition, consideration should be given to upgrading the devices used in the learning kit, such as controllers with higher processing capabilities, to support the operation of more complex AI systems. In addition, developing learning content that covers AI in depth, such as teaching learners how to train and adjust machine learning models, and allowing learners to try to apply the knowledge they have gained to develop other projects related to AI and automation. The expansion of this learning kit has the potential to help build learners' skills in many dimensions, whether in terms of security, automation, or technology used for control and inspection. Finally, further research on the impact of using this practical AI security system learning kit in the long term will be very beneficial so that we can improve both the devices and the teaching content to align with the rapid development of AI technology in the future.

ACKNOWLEDGMENT

The authors thank the Department of Electronics, Nakhonayok Technical College, Thailand, for supporting this research.

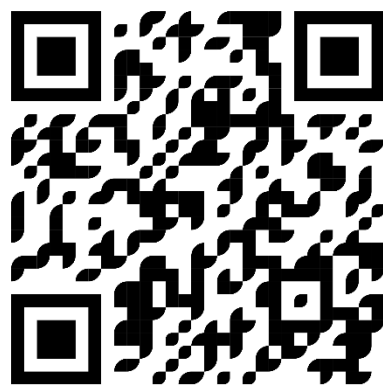
REFERENCES

- [1] S. Kwon and J. Park, "The role of AI in modern vocational education: A study on curriculum enhancement," *Education and Technology Research*, vol. 18, no. 4, pp. 301–320, 2022.
- [2] Q. Zhou, S. Li, and Y. Wang, "AI-powered security systems: A comprehensive study of AI-driven intrusion detection," *Journal of Security and Intelligence Technology*, vol. 9, no. 3, pp. 145–164, 2021.
- [3] H. Lee, "Integrating AI technology into vocational training for security systems," *Journal of Applied Learning in Electronics*, vol. 12, no. 1, pp. 72–89, 2020.
- [4] Ministry of Education, Vocational Certificate curriculum for electronics 2024, Ministry of Education Publications, 2024.
- [5] D. Smith and M. Taylor, "Challenges in integrating AI technology into vocational education," *Educational Technology and AI Journal*, vol. 5, no. 2, pp. 187–199, 2023.
- [6] P. Johnson and T. Wong, "AI-driven intrusion detection systems: Preparing vocational students for the future," *International Journal of Security Technology*, vol. 10, no. 3, pp. 211–230, 2023.
- [7] X. Chen and Y. Liu, "Developing practical learning kits for vocational education: A focus on AI technology in security systems," *Journal of Vocational Education and Training*, vol. 74, no. 2, pp. 145–162, 2022.
- [8] T. Nguyen and P. Tran, "Investing in human resources: The key to sustainable national development," *Journal of Economic and Educational Development*, vol. 29, no. 5, pp. 334–356, 2021.
- [9] H. Lee and J. Kim, "AI and security systems: Skills demand in the digital age," *Journal of Digital Security*, vol. 15, no. 2, pp. 66–78, 2020.
- [10] H. Saini, B. Bhushan, and N. Verma, "Design and maintenance of AI-driven security systems: A study of vocational education needs," *Journal of Digital Security*, vol. 18, no. 2, pp. 77–89, 2022.
- [11] H. Lee, "Workforce demands for AI skills in security systems: Preparing vocational students for the future," *International Journal of Technical Education*, vol. 14, no. 1, pp. 45–58, 2020.
- [12] X. Chen and Z. Xie, "Teaching AI skills to vocational students: A hands-on approach with Python," *Journal of Vocational Education Studies*, vol. 12, no. 3, pp. 45–58, 2023.
- [13] Y. Wu and L. Zhang, "Enhancing vocational students' AI skills through project-based learning," *International Journal of Education and Technology*, vol. 14, no. 1, pp. 89–104, 2022.
- [14] J. Smith and H. Liu, "AI application in vocational education: Case studies from the manufacturing industry," *Journal of Applied Vocational Research*, vol. 10, no. 2, pp. 77–93, 2021.
- [15] A. Gupta and R. Patel, "The future of AI in vocational training: Integrating IoT and real-world problem solving," *Journal of Emerging Technologies in Education*, vol. 9, no. 4, pp. 133–150, 2020.
- [16] J. Park, et al., "Facial recognition for intrusion detection in buildings using CCTV," *Journal of Security and Surveillance Systems*, vol. 9, no. 3, pp. 123–135, 2017.
- [17] X. Liu and Y. Zhang, "Industrial security systems using facial recognition and imaging sensors," *International Journal of Industrial Security*, vol. 17, no. 2, pp. 67–81, 2019.
- [18] R. Kumar and V. Suresh, "Smart home intrusion detection using facial recognition and cloud-based processing," *Journal of Smart Home Technologies*, vol. 5, no. 4, pp. 45–58, 2020.
- [19] A. Singh, et al., "Behavioral and facial recognition systems for enhanced intrusion detection in security-sensitive areas," *Security and Technology Review*, vol. 12, no. 1, pp. 29–48, 2021.
- [20] Y. Zhang, et al., "Integrating theory and practice in AI education: A case for security systems," *Journal of Applied AI Education*, vol. 19, no. 2, pp. 88–99, 2022.
- [21] A. G. Howard, M. Sandler, G. Chu, et al., "Searching for MobileNetV3," *arXiv*, vol. 1905, pp. 02244, 2019.
- [22] A. Kumar, R. Bhanot, and A. Gupta, "Development of a low-cost embedded control system using Arduino Nano for smart applications," *Journal of Engineering Research and Reports*, vol. 24, no. 3, pp. 1–9, 2023.
- [23] J. Zhang, Q. Sun, and Z. Wang, "Design and application of low-cost servo system based on Arduino platform," *Journal of Robotics and Automation*, vol. 18, no. 2, pp. 101–108, 2021.
- [24] A. S. Bonaldo, T. S. Brito, and E. M. de Jesus, "Design and evaluation of an IoT-based low-cost home automation system using ESP8266," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 3, pp. 1417–1430, 2022.
- [25] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1153–1176, 2019.
- [26] V. Raghunathan, C. Schurgers, Sung Park and M. B. Srivastava, "Energy-aware wireless microsensor networks," in *IEEE Signal Processing Magazine*, vol. 19, no. 2, pp. 40–50, 2002.

ภาคผนวก ง

- ผลการวิเคราะห์ข้อมูลการวิจัยด้วยโปรแกรม IBM SPSS





ภาพที่ ง-1 ผลการวิเคราะห์ข้อมูลการวิจัยด้วยโปรแกรม IBM SPSS



ประวัติผู้เขียน

ชื่อ	นางสาวจิราวรรณ โคประโคน
ชื่อการค้นคว้าอิสระ	การพัฒนาชุดการเรียนรู้เชิงปฏิบัติระบบรักษาความปลอดภัยด้วยปัญญาประดิษฐ์ในการตรวจจับการบุกรุก
สาขาวิชา	วิศวกรรมเครื่องกลศึกษา แขนงวิชาวิศวกรรมแมคคาทรอนิกส์และหุ่นยนต์
ประวัติ	การศึกษา - ปริญญาตรีครุศาสตร์อุตสาหกรรมบัณฑิต (ค.อ.บ.) สาขาวิชา วิศวกรรมอิเล็กทรอนิกส์และโทรคมนาคม มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เมื่อปีพุทธศักราช 2559 การทำงาน - พ.ศ. 2559 - 2562 ตำแหน่ง Engineer บริษัท ฟอर्थคอร์ปอเรชั่น จำกัด (มหาชน) - พ.ศ. 2562 - 2565 ตำแหน่งครู โรงเรียนบ้านสมบัติเจริญ สำนักงานเขตพื้นที่การศึกษาประถมศึกษานครราชสีมาเขต 3 - พ.ศ. 2565 - ปัจจุบัน ตำแหน่งครู แผนกอิเล็กทรอนิกส์ วิทยาลัยเทคนิคนครนายก สำนักงานคณะกรรมการการอาชีวศึกษา