ชื่อหัวข้อวิทยานิพนธ์ (Thesis Title)

- ภาษาไทย:

  การอนุมานโมเดลการเรียนรู้ของเครื่องแบบรักษาความเป็นส่วนตัวด้วยพยานหลักฐานความรู้เป็นศูนย์บนข้อมูลสุขภาพจิตนักเรียน

- ภาษาอังกฤษ: Privacy-Preserving Machine Learning Inference Using Zero-Knowledge Proofs on Student Mental Health Data

1. ความสำคัญและที่มาของปัญหาที่ทำการวิจัย (Background and Significance)

ในยุคปัจจุบัน

สุขภาพจิตของนักเรียนและนักศึกษาในระดับอุดมศึกษาได้กลายเป็นหนึ่งในประเด็นทางสาธารณสุขและระบบการศึกษาที่สำคัญอย่างยิ่ง การเปลี่ยนแปลงอย่างรวดเร็วของสังคม แรงกดดันด้านผลการเรียน และความเครียดสะสม ส่งผลให้อัตราการเกิดภาวะซึมเศร้า (Depression), โรควิตกกังวล (Anxiety) และภาวะตื่นตระหนก (Panic Attack) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง สถาบันการศึกษาหลายแห่งจึงเริ่มนำเทคโนโลยีการเรียนรู้ของเครื่อง (Machine Learning: ML) เข้ามาประยุกต์ใช้เพื่อคัดกรองและประเมินความเสี่ยงล่วงหน้า เพื่อให้ฝ่ายแนะแนวและผู้เชี่ยวชาญสามารถยื่นมือเข้าให้ความช่วยเหลือได้อย่างทันท่วงที

อย่างไรก็ตาม ข้อมูลสุขภาพจิต (Mental Health Data) จัดเป็นข้อมูลส่วนบุคคลที่มีความอ่อนไหวเป็นพิเศษ (Sensitive Personal Data) ภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act: PDPA) รวมถึงมาตรฐานสากล เช่น General Data Protection Regulation (GDPR) และ HIPAA การส่งข้อมูลสุขภาพจิตดิบ (เช่น ผลการเรียน ประวัติการรักษา และคำตอบแบบสอบถาม)

ไปยังระบบประมวลผลบนคลาวด์เซิร์ฟเวอร์แบบดั้งเดิม (Centralized Cloud-based Inference) ก่อให้เกิดความเสี่ยงอย่างร้ายแรงต่อการรั่วไหลของข้อมูล (Data Breach) หรือการถูกดักจับระหว่างทาง ซึ่งทำให้นักเรียนเกิดความไม่ไว้วางใจและปฏิเสธการประเมินตนเองตามความเป็นจริง (Stigmatization & Self-Censorship) [Peng et al., 2026; Ganescu & Passerat-Palmbach, 2024]

ตารางอธิบายความแตกต่าง ระบบคลาวด์แบบเดิม และ แนวทางใหม่:

ระบบคลาวด์แบบเดิม (Traditional Cloud ML)	แนวทางใหม่: Zero-Knowledge ML (ZK-ML)
1. การส่งข้อมูล: ส่งข้อมูลสุขภาพจิตดิบ (Raw Data) ไปยังเซิร์ฟเวอร์ส่วนกลาง	**1. การประมวลผลภายใน:** ข้อมูลดิบถูกเก็บไว้ในอุปกรณ์ของผู้ใช้ (Local Device) เท่านั้น
2. ความเป็นส่วนตัว: มีความเสี่ยงสูงต่อการรั่วไหลของข้อมูลระหว่างทางหรือจากการถูกโจมตีเซิร์ฟเวอร์	**2. การสร้างพยานหลักฐาน:** สร้าง ZK-Proof เพื่อยืนยันว่าการคำนวณถูกต้องโดยไม่ต้องส่งข้อมูลดิบ
3. ความไว้วางใจ: ต้องเชื่อมั่นในนโยบายความปลอดภัยของผู้ให้บริการคลาวด์ (Trust-based)	**3. การตรวจสอบ:** เซิร์ฟเวอร์ตรวจสอบความถูกต้องได้ 100% ผ่านหลักฐานทางคณิตศาสตร์ (Trustless)
4. กฎหมายคุ้มครอง: มีความยุ่งยากในการจัดการตามมาตรฐาน PDPA/GDPR เนื่องจากมีการย้ายข้อมูล	**4. การปฏิบัติตามกฎหมาย:** สอดคล้องกับ Privacy-by-Design และ PDPA อย่างสมบูรณ์

เพื่อแก้ไขปัญหาดังกล่าว เทคโนโลยี พยานหลักฐานความรู้เป็นศูนย์ (Zero-Knowledge Proofs: ZKP) ได้ก้าวเข้ามาเป็นแกนนำสำคัญในการพัฒนา Privacy-Preserving Machine Learning (PPML) [Peng

et al., 2026; South et al., 2024] โดย ZKP ช่วยให้ผู้พิสูจน์ (Prover เช่น อุปกรณ์ของผู้เรียน) สามารถสร้างหลักฐานทางคณิตศาสตร์ยืนยันต่อผู้ตรวจสอบ (Verifier เช่น Server ของสถาบัน) ว่าผลลัพธ์การคัดกรองความเสี่ยงได้รับการคำนวณอย่างถูกต้องตามโมเดลมาตรฐานที่ตกลงกันไว้ โดยไม่มีการเปิดเผยข้อมูลสุขภาพจิตดิบของผู้เรียนออกไปแม้แต่รายการเดียว (Data Locality & Privacy) [Ganescu & Passerat-Palmbach, 2024]

อย่างไรก็ตาม ความท้าทายพื้นฐานของการทำ ZK-ML คือ วงจรเลขคณิต ZK (ZK Arithmetic Circuits) คำนวณได้เฉพาะตัวเลขจำนวนเต็มบนฟิลด์จำกัด (Finite Field Arithmetic: $\mathbb{F}_p$) [Coglio et al., 2023] ในขณะที่โมเดลการเรียนรู้ของเครื่องทั่วไปจะคำนวณด้วยตัวเลขทศนิยมความละเอียดสูง (Floating-point) การนำโมเดลเข้าสู่วงจร ZK จำเป็นต้องผ่านกระบวนการ Integer Fixed-Point Quantization [Kang et al., 2022] หากกำหนดค่าตัวคูณสเกล (Scaling Factor: S) ไม่เหมาะสม จะเกิดการสูญเสียข้อมูลสำคัญ (Information Annihilation) ทำให้โมเดลตัดสินใจผิดพลาด แต่หากกำหนดค่าสเกลใหญ่เกินไป จะเกิดความเสี่ยงต่อปัญหาตัวเลขล้น (Integer Overflow) บนฟิลด์จำกัด วิทยานิพนธ์ฉบับนี้จึงมุ่งเน้นการออกแบบ พัฒนา และประเมินผลเชิงประจักษ์ของระบบ Privacy-Preserving Machine Learning Inference บนข้อมูลสุขภาพจิตนักเรียน โดยใช้ภาษา Noir DSL (Nargo) ในการเขียนวงจร ZK Circuit และออกแบบระบบควอนไทเซชันที่เหมาะสมที่สุด ($S=1,000$) เพื่อให้ระบบคงความแม่นยำ $100%$ เท่ากับโมเดล Float64 ดั้งเดิม มีขนาดวงจรกะทัดรัด (312 Constraints) และสร้าง Proof ได้เร็วในระดับต่ำกว่าวินาที (~185.4 ms) พร้อมพัฒนาเป็นสถาปัตยกรรมเว็บแอปพลิเคชันแบบ Asynchronous REST API (MVC Pattern) ที่พร้อมใช้งานจริง

2. คำถามงานวิจัย (Research Questions)

1. สามารถออกแบบและสร้างวงจรพยานหลักฐานความรู้เป็นศูนย์ (ZK Circuit) เพื่ออนุมานโมเดลจำแนกความเสี่ยงสุขภาพจิตนักเรียนได้อย่างไร โดยไม่เปิดเผยข้อมูลส่วนบุคคลและคงความถูกต้องของการอนุมานไว้ได้อย่างสมบูรณ์?
2. การทำ Integer Fixed-Point Quantization ที่ระดับตัวคูณสเกล (S) ต่าง ๆ ส่งผลกระทบต่อความแม่นยำ (Accuracy, F1-Score), การจับคู่ผิดพลาด (Mismatches) และความคลาดเคลื่อนของคะแนน (Score Drift MAE) อย่างไร?
3. สถาปัตยกรรมโมเดลและค่า Scaling Factor ใดที่ให้จุดสมดุลที่ดีที่สุด (Optimal Trade-off) ระหว่างความแม่นยำทางสถิติและประสิทธิภาพทางรหัสวิทยา (Proving Latency & Circuit Constraints)?
4. สถาปัตยกรรมระบบแบบ Asynchronous RESTful API ร่วมกับวงจร ZK-ML มีความพร้อมและประสิทธิภาพเพียงใดในการนำไปประยุกต์ใช้งานคัดกรองสุขภาพจิตนักเรียนในสภาพแวดล้อมจริง?

3. วัตถุประสงค์ของการวิจัย (Research Objectives)

3.1 เพื่อออกแบบและพัฒนาระบบการอนุมานโมเดลการเรียนรู้ของเครื่องแบบรักษาความเป็นส่วนตัว (PPML Inference System) โดยใช้เทคโนโลยี Zero-Knowledge Proofs ผ่านภาษา Noir DSL เพื่อให้สามารถคัดกรองความเสี่ยงสุขภาพจิตนักเรียนได้โดยไม่ต้องเปิดเผยข้อมูลดิบแก่ Server หรือบุคคลภายนอก [South et al., 2024]

3.2 เพื่อพัฒนากลไกควอนไทเซชันแบบจำนวนเต็มจุดคงที่ (Integer Fixed-Point Quantization) สำหรับแปลงค่าน้ำหนัก (Weights) และค่าเอนเอียง (Bias) ของโมเดลจำแนกประเภท (Logistic Regression) ให้อยู่ในรูปตัวเลขจำนวนเต็ม i32 ที่สามารถคำนวณบน ZK Finite Field Arithmetic ได้อย่างมีประสิทธิภาพและปลอดภัยจากปัญหา Integer Overflow [Kang et al., 2022; Coglio et al., 2023]

3.3 เพื่อศึกษาและทดลองเชิงประจักษ์ (Empirical Benchmark) ถึงผลกระทบของค่า Scaling Factor ($S \in \{1, 5, 10, 50, 100, 500, 1000, 5000, 10000, 100000\}$) ที่มีต่อความแม่นยำ (Accuracy, Precision, Recall, F1-Score), ความคลาดเคลื่อนของคะแนน (Score Drift MAE) และการจับคู่ผิดพลาด (Mismatches)

3.4 เพื่อประเมินประสิทธิภาพทางรหัสวิทยาและสถาปัตยกรรมระบบ (Cryptographic & System Evaluation) ในมิติจำนวน ACIR Opcodes, เวลาในการสร้างหลักฐาน (Proving Latency), เวลาในการตรวจสอบ (Verification Latency) และพัฒนาเว็บแอปพลิเคชันแบบ MVC ด้วย FastAPI, MySQL และ Jinja2 Interactive Dashboard

4. สมมติฐานการวิจัย (Research Hypotheses)

4.1 วงจร ZK Circuit บนภาษา Noir DSL

สามารถทำการอนุมานโมเดลจำแนกสุขภาพจิตนักเรียนได้โดยปกปิดตัวแปร Private Inputs ได้ 100% ตามมาตรฐาน PDPA และ GDPR [Peng et al., 2026]

4.2 การทำ Integer Fixed-Point Quantization ที่ค่า Scaling Factor S ≥ 10 จนถึง S = 1,000 จะสามารถรักษาความแม่นยำของโมเดลไว้ได้ 100.0% เท่ากับโมเดล Float64 ดั้งเดิม (ΔAccuracy = 0.0%, Mismatches = 0)

4.3 วงจร ZK Circuit ที่สร้างจากโมเดล Logistic Regression จะมีขนาดกะทัดรัด (Ultra-Lightweight ≤ 350 Constraints) และมี Proving Latency ในระดับต่ำกว่าวินาที (Sub-second ≤ 250 ms) ซึ่งมีประสิทธิภาพสูงกว่าโมเดลแบบโครงสร้างต้นไม้หรือโมเดลไม่เป็นเชิงเส้นหลายเท่าตัว

5. ขอบเขตของการวิจัย (Scope of the Research)

5.1 ขอบเขตด้านชุดข้อมูลและคุณลักษณะ (Data Scope & Features) - ชุดข้อมูล: ข้อมูลสุขภาพจิตนักเรียน (student_mental_health.csv และฐานข้อมูล MySQL mental_health_records) - คุณลักษณะนำเข้า (6 Features): • อายุ (age): ข้อมูลตัวเลขจำนวนเต็ม • ผลการเรียนเฉลี่ยสะสมที่ปรับสเกล (cgpa_scaled): ตัวเลขจำนวนเต็ม • ภาวะซึมเศร้า (depression): ข้อมูลทวิภาค (0 = ไม่มี, 1 = มี) • ภาวะวิตกกังวล (anxiety): ข้อมูลทวิภาค (0 = ไม่มี, 1 = มี) • ภาวะตื่นตระหนก (panic_attack): ข้อมูลทวิภาค (0 = ไม่มี, 1 = มี) • การเคยเข้ารับการปรึกษา/รักษา (seek_treatment): ข้อมูลทวิภาค (0 = ไม่เคย, 1 = เคย) - มาตรฐานรหัสระดับการศึกษา (Education Level Enums): กำหนดรหัสมาตรฐาน 9 ระดับ ได้แก่ PP (ก่อนประถม), PE (ประถม), LSE (ม.ต้น), USE_VS (ม.ปลาย/ปวช.), BBDL (อนุปริญญา/ปวส.), BD (ป.ตรี), MD (ป.โท), PHD (ป.เอก) และค่าเริ่มต้น UNK (ไม่ได้ระบุ) - ผลลัพธ์การจำแนก (Binary

Classification Target): • คลาส 0: กลุ่มความเสี่ยงต่ำ / สุขภาพจิตปกติ (Low Risk / Normal) • คลาส 1: กลุ่มมีความเสี่ยง / แนะนำให้รับการปรึกษา (High Risk / Support Recommended)

5.2 ขอบเขตด้านโมเดลและการคำนวณ (Machine Learning & Quantization Scope) - โมเดลการเรียนรู้ของเครื่อง: Logistic Regression Classifier คำนวณผ่านผลรวมเชิงเส้น (Linear Combination): Score = (x_age · w0) + (x_cgpa · w1) + (x_dep · w2) + (x_anx · w3) + (x_panic · w4) + (x_treat · w5) + b - กระบวนการ Quantization: Q(wi) = round(wi × S) และ Q(b) = round(b × S) - การทดสอบค่าสเกลเชิงประจักษ์: S ∈ {1, 5, 10, 50, 100, 500, 1000, 5000, 10000, 100000}

5.3 ขอบเขตด้านวิทยาการรหัสลับและวงจร ZK (Cryptographic & ZKP Scope) - เครื่องมือพัฒนา ZKP: ภาษา Noir DSL (circuit/src/main.nr) และ Nargo CLI คอมไพล์เป็น Abstract Circuit Intermediate Representation (ACIR) [Aztec, 2023] - การแบ่งแยกความปลอดภัยในวงจร: • Private Inputs (ความลับ 100%): ตัวแปรข้อมูลสุขภาพจิตนักเรียน 6 ตัวแปร • Public Inputs (เปิดเผยได้): พารามิเตอร์โมเดลมาตรฐาน (weights, bias, threshold, expected_risk_class) - การตรวจสอบเงื่อนไขในวงจร (Assertion): ตรวจสอบผ่าน assert(computed_risk == expected_risk_class) บน Finite Field Type i32 [Coglio et al., 2023]

5.4 ขอบเขตด้านการพัฒนาระบบและสถาปัตยกรรม (System Architecture Scope) - Backend Framework: Python 3.11, FastAPI (Asynchronous REST API, MVC Architecture) - Database & Storage: MySQL 8.0, SQLAlchemy ORM พร้อมระบบ Hybrid Data Provider (DB-first พร้อม Auto-fallback ไปยัง CSV) - Web Visualization & UI: Jinja2 Templates,

Chart.js สำหรับ Interactive Dashboard (/test-quantization-impact, /test-cryptographic-benchmark, /students) - Infrastructure & DevOps: Docker & Docker Compose, Caddy Server (Reverse Proxy พร้อม HTTPS Auto-SSL), และ CI/CD Pipeline ผ่าน GitHub Actions

6. การทบทวนวรรณกรรมและเหตุผลเชิงวิชาการในการเลือกโมเดล (Literature Review & Model Selection)

6.1 การเปรียบเทียบเทคโนโลยีรักษาความเป็นส่วนตัว (Privacy-Enhancing Technologies Comparison)

จากการสำรวจงานวิจัยเชิงสังเคราะห์ของ Peng et al. (2026) และ South et al. (2024) พบว่าเทคโนโลยีรักษาความเป็นส่วนตัวแต่ละประเภทมีคุณสมบัติและข้อจำกัดที่แตกต่างกัน:

เทคโนโลยี (Technology)	จุดเด่นด้านความเป็นส่วนตัว	ข้อจำกัดหลัก	การตรวจสอบความถูกต้อง (Verifiability)
Differential Privacy (DP)	ป้องกันการระบุตัวตนด้วย Noise	ความแม่นยำลดลง	ไม่มีกลไกตรวจสอบการคำนวณ
Homomorphic Encryption (HE)	คำนวณบนข้อมูลที่เข้ารหัสได้	ช้ามากและเปลือง RAM	ไม่สามารถตรวจการโกงของ Server
Federated Learning (FL)	ข้อมูลดิบไม่หลุดออกจากเครื่อง	เสี่ยง Poisoning	ตรวจสอบ Gradient ได้ยาก

เทคโนโลยี (Technology)	จุดเด่นด้านความเป็นส่วนตัว	ข้อจำกัดหลัก	การตรวจสอบความถูกต้อง (Verifiability)
Trusted Execution (TEE)	ทำงานเร็วระดับฮาร์ดแวร์	เสี่ยง Side-channel	ต้องเชื่อใจ Vendor ฮาร์ดแวร์
Zero-Knowledge Proofs (ZKP) (งานวิจัยนี้)	ข้อมูลเป็นความลับ 100%	ต้องแปลงเป็น Finite Field Arithmetic	ตรวจสอบความถูกต้องได้ 100% ด้วยหลักฐานคณิตศาสตร์ (Proof)

6.2 เหตุผลเชิงวิชาการในการเลือก Logistic Regression สำหรับ ZK-ML

เมื่อเปรียบเทียบกับสถาปัตยกรรม Machine Learning อื่นๆ ในบริบทของ Zero-Knowledge Proofs [Peng et al., 2026; Kang et al., 2022; Coglio et al., 2023]:

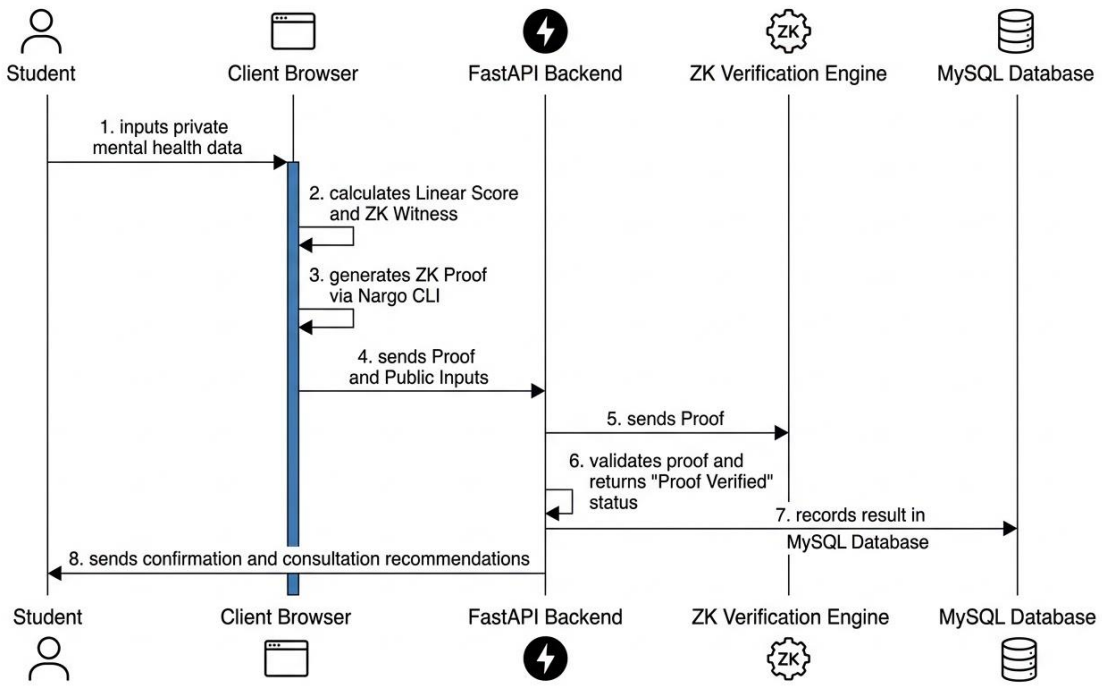
มิติการเปรียบเทียบ	Logistic Regression (งานนี้)	Decision Tree / Forest [32]	Naive Bayes
รูปแบบการคำนวณใน ZK	Linear Combination (คูณ/บวก)	Branch Multiplexing (ทุกลูป)	Probability & Logarithm
ขนาด Constraints	312 Constraints (กะทัดรัดมาก)	5,000 - 50,000+ Constraints	3,000 - 10,000+ Constraints

มิติการเปรียบเทียบ	Logistic Regression (งานนี้)	Decision Tree / Forest [32]	Naive Bayes
Proving Latency	~185.4 ms (Sub-second)	1.5 - 10+ วินาที	1.2 - 4 วินาที
ความเสี่ยงข้อมูลรั่วไหล	ไม่มี (สมการคงที่)	เสี่ยง Branch Side-channel	เกิด Rounding Error สูง
ความแม่นยำบนชุดข้อมูลนี้	100.00%	100.00%	96.00% - 98.00%

- ข้อวิจารณ์เชิงวิชาการ: ในระบบ ZKP เพื่อไม่ให้ผู้ตรวจสอบรู้ว่าข้อมูลตกอยู่ที่กิ่งใด (Privacy Preservation) วงจรของ Decision Tree / Random Forest จำเป็นต้องคำนวณทุกกิ่งของทุกต้นไม้ (Evaluate All Branches via Multiplexers) ทำให้ขนาดวงจรพุ่งสูงเป็นหลายหมื่น Constraints ส่งผลให้ Proving Latency ช้ามาก ในขณะที่ Logistic Regression บนชุดข้อมูลสุขภาพจิตนี้สามารถแบ่งแยกกลุ่มเสี่ยงได้สมบูรณ์แบบที่ความแม่นยำ $100%$ การเลือกใช้ Logistic Regression จึงเป็น จุดสมดุลที่ดีที่สุด (Optimal Trade-off)

7. ระเบียบวิธีวิจัยและสถาปัตยกรรมระบบ (Research Methodology & System Architecture)

7.1 แผนภาพการทำงานของระบบ (End-to-End Workflow)



7.2 ขั้นตอนการดำเนินงานวิจัย (Research Phases)

- เฟสที่ 1: การเตรียมข้อมูลและฝึกสอนโมเดล (ML & Preprocessing Phase)

  ทำความสะอาดข้อมูล สร้าง Hybrid Data Provider รองรับทั้ง MySQL และ CSV

  จากนั้นฝึกสอนโมเดล Logistic Regression

- เฟสที่ 2: การพัฒนาเอ็นจินควอนไทเซชัน (Quantization Engine Development)

  พัฒนาอัลกอริทึมแปลงค่าน้ำหนักเป็น Integer i32 และทำ Benchmark เปรียบเทียบค่า

  $S=1$ ถึง $100,000$

- เฟสที่ 3: การพัฒนาวงจร ZK Circuit (Noir Cryptographic Implementation) เขียนโค้ด

  circuit/src/main.nr กำหนด Private/Public Inputs และคอมไพล์ผ่าน Nargo CLI

- เฟสที่ 4: การพัฒนาระบบ Back-end API และ Dashboard (Full-stack Integration)

  พัฒนาระบบ FastAPI MVC, SQLAlchemy Deduplication, Docker Containerization และ Jinja2 Web UI

- เฟสที่ 5: การประเมินผลเชิงลึกและการเขียนรายงาน (Evaluation & Thesis Documentation) วิเคราะห์ผลทางสถิติและรหัสวิทยาเพื่อเขียนวิทยานิพนธ์ฉบับสมบูรณ์ (บทที่ 1 - 5)

8. แผนระยะเวลาการดำเนินงานวิจัย (Research Timeline / Gantt Chart)

ขั้นตอนการดำเนินงาน	**เดือนที่ 1**	**เดือนที่ 2**	**เดือนที่ 3**	**เดือนที่ 4**	**เดือนที่ 5**	**เดือนที่ 6**
1. ศึกษาทบทวนวรรณกรรมและเสนอเค้าโครง (Proposal)						
2. เตรียมชุดข้อมูลและฝึกสอนโมเดล ML Baseline						
3. พัฒนาระบบ Quantization และทดสอบค่า Scaling Factor (S)						
4. ออกแบบและพัฒนา ZK Circuit ด้วยภาษา Noir DSL						

ขั้นตอนการดำเนินงาน	เดือนที่ 1	เดือนที่ 2	เดือนที่ 3	เดือนที่ 4	เดือนที่ 5	เดือนที่ 6
5. พัฒนาระบบ Back-end API (FastAPI) และ Web Dashboard						
6. รันการทดสอบ Benchmark ด้านความแม่นยำและรหัสวิทยา						
7. สรุปผลการวิจัยและจัดทำเล่มวิทยานิพนธ์ฉบับสมบูรณ์						

9. ประโยชน์ที่คาดว่าจะได้รับ (Expected Contributions)

9.1 ประโยชน์เชิงวิชาการ (Academic Contributions):

ได้องค์ความรู้และผลการทดลองเชิงประจักษ์ในการแปลงโมเดล Machine Learning เข้าสู่วงจร ZK Finite Field ด้วย Integer Fixed-Point Quantization ที่พิสูจน์แล้วว่าไม่สูญเสียความแม่นยำ (ΔAccuracy = 0.0% ที่ S = 1,000)

9.2 ประโยชน์ต่อการคุ้มครองข้อมูลส่วนบุคคล (Privacy & PDPA Compliance):

สถาบันการศึกษาสามารถให้บริการคัดกรองสุขภาพจิตนักเรียนได้โดยไม่ละเมิดสิทธิความเป็นส่วนตัว ข้อมูลสุขภาพจิตดิบไม่เคยถูกจัดเก็บบน Server ช่วยสร้างความไว้วางใจและลดปัญหาการตีตรา (De-stigmatization)

9.3 ประโยชน์เชิงวิศวกรรมซอฟต์แวร์ (Engineering & Practical Implementation):

ได้ระบบต้นแบบที่ทำงานได้จริงในระดับ Sub-second (~185.4 ms) พร้อม Docker Compose, Caddy Reverse Proxy (HTTPS Auto-SSL) และ CI/CD Pipeline

ที่พร้อมนำไปต่อยอดใช้งานได้ทันที

10 เอกสารอ้างอิง (References)

[1] Z. Peng, C. Zhao, T. Wang, G. Liao, Z. Lin, Y. Liu, B. Cao, L. Shi, Q. Yang, and S. Zhang, "A Survey of Zero-Knowledge Proof Based Verifiable Machine Learning," arXiv preprint arXiv:2502.18535v2 [cs.CR], Mar. 2026.

[2] D. Kang, T. Hashimoto, I. Stoica, and Y. Sun, "Scaling up Trustless DNN Inference with Zero-Knowledge Proofs," in Proceedings of the 37th International Conference on Machine Learning (ICML), PMLR 119 / arXiv preprint arXiv:2210.08674, 2022.

[3] T. South, A. Camuto, S. Jain, S. Nguyen, R. Mahari, C. Paquin, J. Morton, and A. Pentland, "Verifiable evaluations of machine learning models using zkSNARKs," arXiv preprint arXiv:2402.02675v2 [cs.LG], May 2024.

[4] B.-M. Ganescu and J. Passerat-Palmbach, "Trust the Process: Zero-Knowledge Machine Learning to Enhance Trust in Generative AI Interactions," in Proceedings of the AAAI Conference on Artificial Intelligence (AAAI-24) / arXiv preprint arXiv:2402.06414, 2024.

[5] A. Coglio, E. McCarthy, and E. W. Smith, "Formal Verification of Zero-Knowledge Circuits," in Proceedings of the 18th ACL2 Workshop (ACL2-2023), Electronic Proceedings in Theoretical Computer Science (EPTCS), vol. 393, pp. 94–112, 2023.

[6] Aztec Network, "Noir: The Domain-Specific Language for Zero-Knowledge Proofs," Aztec Documentation & Nargo Toolchain, 2023. [Online]. Available: https://aztec.network/noir

[7] B. Feng, L. Qin, Z. Zhang, Y. Ding, and S. Chu, "ZEN: An optimizing compiler for verifiable, zero-knowledge neural network inferences," Cryptology ePrint Archive, Paper 2021/259, 2021.

[8] T. Liu, X. Xie, and Y. Zhang, "zkCNN: Zero knowledge proofs for convolutional neural network predictions and accuracy," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21), pp. 2968–2985, 2021.

[9] J. Zhang, Z. Fang, Y. Zhang, and D. Song, "Zero knowledge proofs for decision tree predictions and accuracy," in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), pp. 2039–2053, 2020.

[10] ราชกิจจานุเบกษา, "พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)," เล่ม 136 ตอนที่ 69 ก, หน้า 33–69, 27 พฤษภาคม 2562.