AI X-Ray Analysis on Blockchain

ระบบวิเคราะห์ภาพเอกซเรย์ด้วยปัญญาประดิษฐ์บนบล็อกเชน

โดย

ชื่อ นายรวิพล มุ่งดี	รหัสนักศึกษา B6506469
ชื่อ นายณัฐภูมิ อุปมัย	รหัสนักศึกษา B6509712
ชื่อ นายสิทธินนท์ วงศ์สุทธิรัตน์	รหัสนักศึกษา B6606244
ชื่อ นางสาวนภสร วาริชอลังการ	รหัสนักศึกษา B6614768

รายงานนี้เป็นส่วนหนึ่งของรายวิชา ENG23 3055 เทคโนโลยีบล็อกเชนเบื้องต้น

หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์

สำนักวิชาวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีสุรนารี

ประจำภาคการศึกษาที่ 2 ปีการศึกษา 2568

1. **ทำไมถึงเลือกใช้ Blockchain ให้กับบริการหรือระบบนั้นๆ**

   การนำเทคโนโลยี Blockchain มาใช้แทน Database แบบ Centralized ทั่วไปในการจัดเก็บผลวิเคราะห์ภาพถ่ายทางการแพทย์ (X-rays) ร่วมกับ AI มีเหตุผลสำคัญดังนี้:

   1.1. ความทนทานต่อการแก้ไข (Immutability): ข้อมูลทางการแพทย์เป็นข้อมูลที่ละเอียดอ่อนและมีผลทางกฎหมาย การใช้ Blockchain ทำให้มั่นใจได้ว่าผลวินิจฉัยจาก AI และประวัติการรักษาที่ถูกบันทึกไปแล้ว จะไม่สามารถถูกแอบเปลี่ยนแปลงย้อนหลังได้ (Tamper-proof) หากมีการแก้ไข ค่า Hash จะเปลี่ยนและระบบจะตรวจจับได้ทันที

   1.2. ตรวจสอบย้อนกลับได้ (Auditability & Transparency): ระบบสามารถระบุได้ชัดเจนว่าข้อมูลชุดนี้ถูกสร้างขึ้นเมื่อไหร่ โดยโรงพยาบาลใด รวมถึงสามารถตรวจสอบสิทธิ์การเข้าถึง (Access Log) ได้อย่างโปร่งใส

   1.3. การแชร์ข้อมูลแบบรักษาความเป็นส่วนตัว (Privacy-Preserving Data Sharing): การใช้ Public/Private Key (Asymmetric Encryption) ช่วยให้สามารถแชร์ข้อมูลข้ามโรงพยาบาลได้ โดยที่เฉพาะแพทย์ผู้ได้รับอนุญาตเท่านั้นที่มีสิทธิ์ถอดรหัสข้อมูลมาดูได้ ตัดปัญหาเรื่องข้อมูลรั่วไหลในขณะส่งต่อ

2. **อธิบายการทำงานรวมของระบบ**

   ระบบ AI X-Ray Analysis on Blockchain แบ่งการทำงานออกเป็นส่วนย่อย (Modules) ที่ทำงานประสานกัน ดังนี้:

   2.1. การเตรียมข้อมูลและพิสูจน์ตัวตน (Data Acquisition & Auth)

   - **Medical Imaging:** แพทย์หรือเจ้าหน้าที่เทคนิคทำการถ่ายภาพ X-Ray (เช่น ไฟล์ DICOM หรือ PNG) ของคนไข้
   - **Key Management:** ระบบจะใช้คู่กุญแจ (Asymmetric Keys) ของแพทย์ผู้รับผิดชอบ โดย Public Key จะถูกใช้เป็นตัวระบุตัวตน (Identity) ในระบบ และใช้สำหรับเข้ารหัสข้อมูลส่วนบุคคล (PII - Personally Identifiable Information) เพื่อให้มั่นใจว่าจะมีเพียงแพทย์เจ้าของไข้ที่มี Private Key เท่านั้นที่เข้าถึงข้อมูลดิบได้

   2.2. กระบวนการวิเคราะห์ด้วย AI (AI Inference Pipeline)

   - **Image Pre-processing:** ภาพถ่ายจะถูกส่งผ่าน API ไปยัง AI Server (เช่น Flask หรือ FastAPI service ที่รันบน GPU) เพื่อปรับขนาดภาพ (Resize) และทำ Normalization
   - **CNN Processing:** ใช้โมเดลโครงข่ายประสาทเทียมแบบคอนโวลูชัน (Convolutional Neural Network - CNN) เช่น ResNet152 หรือ DenseNet ที่ผ่านการ Training มาเพื่อจำแนกโรคโดยเฉพาะ
   - **AI Output:** โมเดลจะส่งผลลัพธ์กลับมาในรูปแบบของ:
     - **Diagnosis:** ผลวินิจฉัย (เช่น Normal, Pneumonia, COVID-19)

- **Heatmap (Grad-CAM):** ภาพที่ระบุตำแหน่งที่โมเดลตรวจพบความผิดปกติ

2.3. การจัดเก็บข้อมูลแบบ Hybrid (On-chain & Off-chain)

- **Off-chain (IPFS):** ภาพถ่าย X-Ray และ Heatmap จะถูกอัปโหลดขึ้นไปยัง IPFS (InterPlanetary File System) หรือ Secure Cloud Storage จากนั้นจะได้รับ Content Hash (IPFS Hash) กลับมาเพื่อใช้เป็นตัวอ้างอิง
- **Encryption:** ข้อมูลส่วนตัวคนไข้ (ชื่อ, อายุ, อาการ) จะถูกเข้ารหัสด้วย Public Key ของแพทย์ กลายเป็น Ciphertext ที่อ่านไม่ออกหากไม่มีกุญแจ

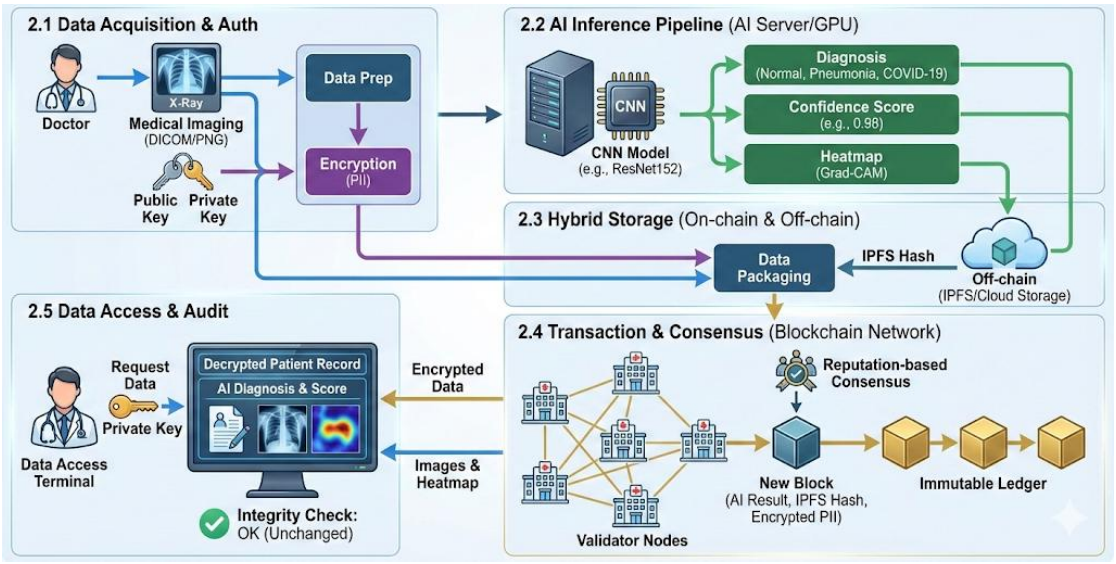
2.4. การสร้างธุรกรรมและระบบฉันทามติ (Transaction & Consensus)

- **Data Packaging:** ระบบจะรวบรวม (1) ผลจาก AI (2) IPFS Hash ของรูปภาพ และ (3) ข้อมูลคนไข้ที่เข้ารหัสแล้ว มาสร้างเป็นโครงสร้างข้อมูล Data object
- **Validation:** ข้อมูลจะถูกส่งไปยัง Blockchain Network โดยมี Nodes (โรงพยาบาลต่างๆ) ทำหน้าที่เป็น Validators
- **Reputation-based Consensus:** ระบบจะเลือก Validator ตามค่า Reputation Score (ความน่าเชื่อถือ) เพื่อตรวจสอบความถูกต้องของโครงสร้าง Block และ Hash ก่อนจะเขียนข้อมูลลงใน Ledger แบบถาวร

2.5. การเข้าถึงข้อมูลและการตรวจสอบ (Data Access & Audit)

- **Authorized Access:** เมื่อแพทย์ต้องการดูประวัติคนไข้ ระบบจะดึงข้อมูลที่เข้ารหัสมาจาก Blockchain และใช้ Private Key ของแพทย์ในการถอดรหัส (Decrypt) ข้อมูลส่วนตัวออกมาแสดงผลคู่กับภาพจาก IPFS
- **Integrity Check:** ตลอดเวลาที่ข้อมูลอยู่ในระบบ หากมีการพยายามแก้ไขข้อมูลใน Block ใดก็ตาม ค่า previous_hash ใน Block ถัดไปจะไม่ตรงกัน ทำให้ระบบสามารถปฏิเสธข้อมูลที่ถูกแก้ไขได้ทันที

System Architecture & Workflow:



3. **อธิบาย Consensus - ทำไมถึงเลือก Consensus ลักษณะนี้, ป้องกัน 51% Attack อย่างไร, Incentive ในระบบคืออะไร**

ระบบใช้กลไก **Weighted Random Selection ตามค่า Reputation** ซึ่งพัฒนาต่อยอดมาจากแนวคิด Proof of Stake (PoS)

3.1. ทำไมถึงเลือกแบบนี้?

- **Efficiency:** ประหยัดพลังงานมากกว่า Proof of Work (PoW) ของ Bitcoin เพราะไม่ต้องใช้การคำนวณทางคณิตศาสตร์ที่หนักหน่วง เหมาะสำหรับใช้งานในเครือข่ายโรงพยาบาล
- **Trust-Based:** ในระบบการแพทย์ "ความน่าเชื่อถือ" (Reputation) สำคัญที่สุด โรงพยาบาลที่มีประวัติการทำงานที่ดีจะมีโอกาสได้ตรวจสอบ Block มากกว่า

3.2. การป้องกัน 51% Attack

ในระบบนี้ 51% Attack จะเกิดขึ้นได้ก็ต่อเมื่อมี Node ใด Node หนึ่งมีค่า Reputation รวมกันมากกว่าครึ่งหนึ่งของทั้งระบบ ซึ่งทำได้ยากเพราะ

- **Identity-Based Weighted Voting:** สิทธิ์การโหวตไม่ได้ขึ้นอยู่กับกำลังเครื่อง (Computational Power) แต่ขึ้นอยู่กับ Reputation Score โดยค่า Reputation อ้างอิงมาจากอัตราเคสของโรงพยาบาลที่รักษาสำเร็จต่อเคสที่รับเข้ามัน มันความหมายคือยิ่งโรงพยาบาลให้รักษาคนไข้ได้สำเร็จ Reputation Score ก็จะมากขึ้นเท่านั้น ทำให้บ่งบอกว่าโรงพยาบาลนั้นเป็นโรงพยาบาลที่ดี ควรมา Reputation Score เยอะ
- **High Cost of Malicious Behavior:** หาก Node ใดพยายามโหวตรับข้อมูลเท็จหรือ Spam ระบบ จะถูกตรวจสอบเจอได้ง่าย (เพราะระบุตัวตนได้) และจะถูกลดคะแนน Reputation จนเหลือ 0 ซึ่งส่งผลให้ถูกตัดออกจากระบบ
- **Slashing:** บทลงโทษคือการถูก "แบน" จากเครือข่าย ทำให้โรงพยาบาลนั้นเสียชื่อเสียงและเสียสิทธิ์การใช้งานระบบ ซึ่งเป็นต้นทุนทางสังคมและธุรกิจที่สูงมากจนไม่คุ้มที่จะโกง

3.3. Incentive (แรงจูงใจในระบบ)

ระบบนี้ไม่มีการแจก "เหรียญดิจิทัล" (No Cryptocurrency Reward) แต่ใช้ "Data & Model Access" เป็นรางวัล:

- Central Pool Mechanism (กองทุนส่วนกลาง): ระบบจะมีกองทุนกลางที่เกิดจากค่าธรรมเนียมการใช้บริการ (Transaction Fees) เช่น เมื่อมีคนส่งภาพมาวิเคราะห์ AI จะมีการหักค่าธรรมเนียมเข้ากองทุน หรือมาจากการสนับสนุนของ Consortium
- Block Reward (รางวัลผู้สร้างบล็อก):
  - Node ที่ได้รับการคัดเลือกให้สร้าง Block ใหม่ (Proposer) และผ่านการตรวจสอบความถูกต้องจาก Node อื่นๆ จะได้รับรางวัลทันที

- Reward Rate: คิดเป็น 5% จากมูลค่าธุรกรรมรวมใน Block นั้น หรือ 5% จาก Allocation ของกองทุนส่วนกลางที่กำหนดไว้ในรอบนั้น

- Purpose: การมีตัวเงินเกี่ยวข้องจะสร้างแรงจูงใจให้โรงพยาบาลต่างๆ ลงทุนดูแล Server ให้มีประสิทธิภาพ (High Availability) และไม่กล้าทุจริต เพราะหากถูกแบน (Slashing) จะสูญเสียโอกาสในการสร้างรายได้ 5% นี้ไป

4. ผลการทำงานของตัวอย่างจาก Code (Simulated 5 Blocks)

จากการทำงานของ MedicalBlockchain ใน blockchain.py หากมีการทำรายการ 5 ครั้ง โครงสร้างของ Chain จะเชื่อมต่อกันดังนี้:

Block Index	Validator (Selected by Reputation)	Data Content (Partial)	Status	Previous Hash
0	Genesis Block	[]	Secure	0
1	Bangkok Hospital	Patient A (Diagnosis: Normal)	Secure	Hash of Block 0
2	Research Center AI	Patient B (Diagnosis: Pneumonia)	Secure	Hash of Block 1
3	Bangkok Hospital	Patient C (Diagnosis: Covid-19)	Secure	Hash of Block 2
4	General Clinic Node	Patient D (Diagnosis: Tuberculosis)	Secure	Hash of Block 3