PRIVACY · AI · TRUST

Privacy-Enhancing Technologies (PETs)

นวัตกรรมเพื่อใช้ข้อมูลอย่างปลอดภัยในยุค AI

นนทวัตต์ สาระมาน

กรรมการสภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย DCT
นายยกกิติมศักดิ์สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์ CIPAT
ผู้ร่วมก่อตั้งศูนย์ปฏิบัติการและวิจัยดิจิทัลเพื่ออนาคตที่ยั่งยืน

ผู้ร่วมก่อตั้ง SRAN Technology
ผู้ก่อตั้ง Qsense PQC Readiness Platform

SRAN®

QSENSE
PQC Readiness Platform

ปัจจุบันสำเนาบัตรประชาชนของเราไปอยู่ที่ใดบ้าง ?

คำถามชวนคิด

คุณรู้หรือไม่ว่า 'สำเนาบัตรประชาชน' ของคุณกระจายอยู่ทั่วโลกกี่ฉบับ?

ความเป็นจริง

ข้อมูลส่วนบุคคล (PII) และข้อมูลองค์กร ขยายตัวอย่างควบคุมไม่ได้ เรากังวลเรื่อง ความเป็นส่วนตัวแต่ขาดระบบตรวจสอบ

ความท้าทาย

องค์กรส่วนใหญ่มองคาบปลอดภัย ข้อมูลเป็นเพียงแค่การทำตามกฎระบียน (Checklist) แทนที่จะทำความเข้าหัน ข้อมูลจริงๆ

Nontawatt Saraman

ข้อมูลทุกชุดในองค์กรต้องถูกควบคุมผ่าน 3 ช่วงชีวิตหลัก

Lifecycle ของข้อมูล

1. เก็บ (Keep)
ข้อมูลถูกสร้างและจัดเก็บ
(Data at Rest)

2. ส่ง (Send)
ข้อมูลถูกถ่ายโอน
(Data in Transit)

3. อ่าน (Read)
มีการเข้าถึงข้อมูล
(Data in Use)

Breach = “ถูกแฮก / ถูกขโมย” โดยตั้งใจ
Loss = “หายไป / ใช้ไม่ได้”
Leak = “หลุดออกไปโดยไม่ได้ตั้งใจ”

DLP = Data Loss Prevention

แต่ในยุค AI DLP เอาไม่อยู่แล้ว เพราะ
ShadowAI
เราจึงต้องมาเรียนรู้ PETs

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

หัวใจของ PETs ในยุค AI

Use • Protect • Trust

ใช้ข้อมูล • ปกป้องข้อมูล • สร้างความเชื่อมั่น

Use
ใช้ข้อมูลให้เกิดคุณค่า

Protect
ปกป้องข้อมูลอย่างรับผิดชอบ

Trust
สร้างความเชื่อมั่นอย่างยั่งยืน

PETs = Privacy Enhancing Technologies

Nontawatt Saraman

OPENING · ทำไมเรื่องนี้ถึงสำคัญในเวลานี้

SRAN®

ข้อมูลคือเชื้อเพลิงของ AI · แต่ข้อมูลคือความเสี่ยงด้วย

องค์กรเผชิญแรงกดดัน 3 ด้านพร้อมกัน

1 ความต้องการของ AI

โมเดล AI ต้องการข้อมูลขนาดใหญ่ คุณภาพสูง และหลากหลายแหล่ง

2 ความเข้มงวดของกฎหมาย

PDPA, GDPR, HIPAA, EU AI Act บีบให้ต้องลดการ expose ข้อมูลส่วนบุคคลให้ต่ำสุด

3 ภัยคุกคามที่ขยายตัว

Data breach, model inversion, membership inference ทำให้ข้อมูลฝึก AI กลายเป็นเป้าโจมตี

PETs คือคำตอบที่ทำให้องค์กรใช้ข้อมูลได้ โดยไม่ต้องเลือกระหว่าง ‘ใช้’ กับ ‘ปลอดภัย’

PETs · Privacy-Enhancing Technologies

Nontawatt Saraman

วงจรชีวิตของการปกป้องข้อมูลด้วย PETs

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อมูลขาเข้า (Input Privacy)
ปกป้องข้อมูลก่อนเข้าสู่ระบบ

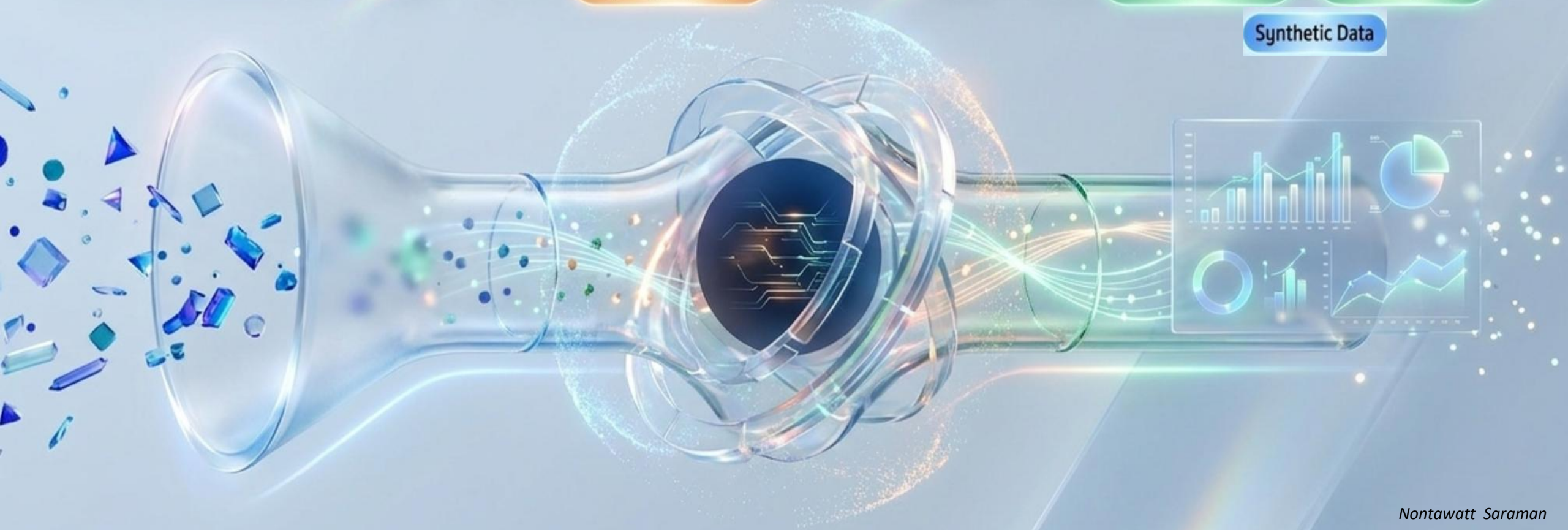
- Anonymization
- k-anonymity

ระหว่างประมวลผล (Computation Privacy)
คำนวณและวิเคราะห์โดยไม่เห็นข้อมูลดิบ

- Secure Computation (MPC, HE, TEE)
- Federated Learning (FL)

ผลลัพธ์ขาออก (Output Privacy)
ป้องกันไม่ให้ผลลัพธ์ย้อนกลับไปหาตัวบุคคลได้

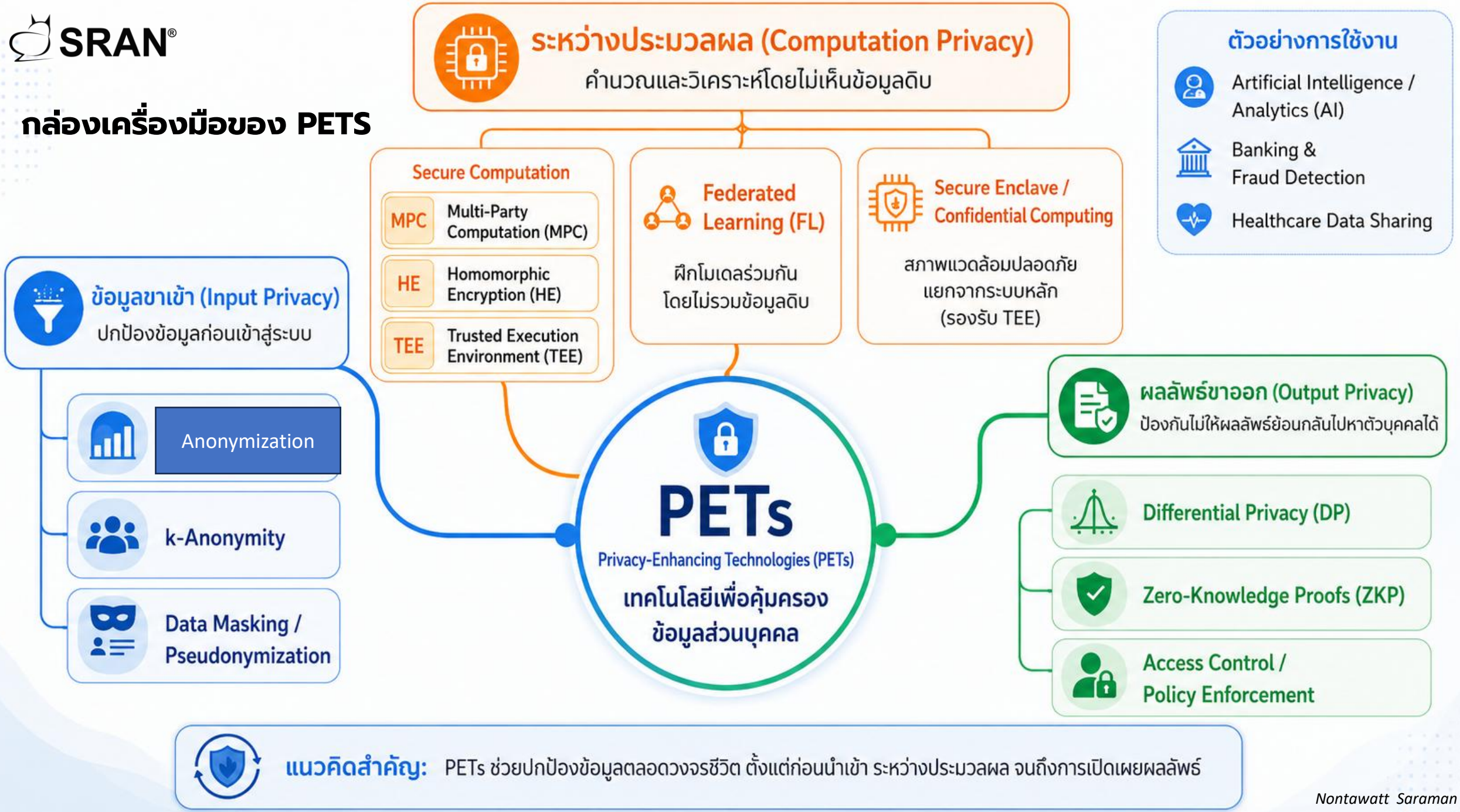
- Differential Privacy (DP)
- Zero-Knowledge Proofs (ZKP)
- Synthetic Data



Nontawatt Saraman

SRAN®

กล่องเครื่องมือของ PETS



แนวคิดสำคัญ: PETs ช่วยปกป้องข้อมูลตลอดวงจรชีวิต ตั้งแต่ก่อนนำเข้า ระหว่างประมวลผล จนถึงการเปิดเผยผลลัพธ์

Nontawatt Saraman

ข้อมูลขาเข้า (Input Privacy)
ปกป้องข้อมูลก่อนเข้าสู่ระบบ
Data Masking / Pseudonymization
k-anonymity

ระหว่างประมวลผล (Computation Privacy)
คำนวณและวิเคราะห์โดยไม่เห็นข้อมูลดิบ
Secure Computation (MPC, HE, TEE)
Federated Learning (FL)

ผลลัพธ์ขาออก (Output Privacy)
ป้องกันไม่ให้ผลลัพธ์ย้อนกลับไปหาตัวบุคคลได้
Differential Privacy (DP)
Zero-Knowledge Proofs (ZKP)

Anonymization vs Pseudonymization

การปกปิดข้อมูลส่วนบุคคล: ต่างกันอย่างไร

Anonymization (การทำให้ไม่สามารถระบุตัวตนได้)

ข้อมูลตั้งต้น

ชื่อ	เลขบัตรประชาชน	เบอร์โทร	อายุ	จังหวัด	ยอดใช้จ่าย (บาท/เดือน)
สมชาย ใจดี	1-2345-67890-12-3	081-234-5678	34	เชียงใหม่	12,450
สมหญิง รักดี	1-9876-54321-23-4	091-876-5432	29	ชลบุรี	7,890
อนันต์ มีสุข	3-1122-33445-56-7	062-345-6789	41	ขอนแก่น	15,600

ลบ / ปกปิด / ทำให้เป็นข้อมูลรวม

ผลลัพธ์

อายุ (ช่วงปี)	ภาค	ยอดใช้จ่าย (บาท/เดือน)
30-39	ภาคเหนือ	10,001 – 15,000
20-29	ภาคตะวันออก	5,001 – 10,000
40-49	ภาคตะวันออกเฉียงเหนือ	15,001 – 20,000

ไม่สามารถย้อนกลับไประบุตัวบุคคลได้

เหมาะกับ: การเปิดเผยข้อมูลสถิติ, งานวิจัย, รายงานสาธารณะ

Pseudonymization (การใช้นามแฝงแทนตัวตน)

ข้อมูลตั้งต้น

ชื่อ	เลขบัตรประชาชน	เบอร์โทร	อายุ	จังหวัด	ยอดใช้จ่าย (บาท/เดือน)
สมชาย ใจดี	1-2345-67890-12-3	081-234-5678	34	เชียงใหม่	12,450
สมหญิง รักดี	1-9876-54321-23-4	091-876-5432	29	ชลบุรี	7,890
อนันต์ มีสุข	3-1122-33445-56-7	062-345-6789	41	ขอนแก่น	15,600

แทนที่ตัวระบุด้วยรหัส

ผลลัพธ์

รหัสลูกค้า (Token)	อายุ	จังหวัด	ยอดใช้จ่าย (บาท/เดือน)
CUST-001	34	เชียงใหม่	12,450
CUST-002	29	ชลบุรี	7,890
CUST-003	41	ขอนแก่น	15,600

ตารางเชื่อมโยง / Key

รหัสลูกค้า (Token)	ชื่อ
CUST-001	สมชาย ใจดี
CUST-002	สมหญิง รักดี
CUST-003	อนันต์ มีสุข

ยังสามารถเชื่อมกลับได้
หากมี key แยกเก็บไว้อย่างปลอดภัย

เหมาะกับ: Analytics ภายในองค์กร, AI/ML, การทดสอบระบบ, การแชร์ข้อมูลแบบควบคุม

หัวข้อเปรียบเทียบ	Anonymization (การทำให้ไม่สามารถระบุตัวตนได้)	Pseudonymization (การใช้นามแฝงแทนตัวตน)
ย้อนกลับไประบุตัวตน	ไม่ได้	ได้ (ถ้ามี key)
ความเสี่ยงด้านข้อมูลส่วนบุคคล	ต่ำกว่า	ยังมีความเสี่ยง
คุณค่าการวิเคราะห์ข้อมูล	ลดลงบางส่วน	ยังวิเคราะห์ต่อได้ดี

Nontawatt Saraman

ข้อมูลขาเข้า (Input Privacy)
ปกป้องข้อมูลก่อนเข้าสู่ระบบ
Data Masking / Pseudonymization
k-anonymity

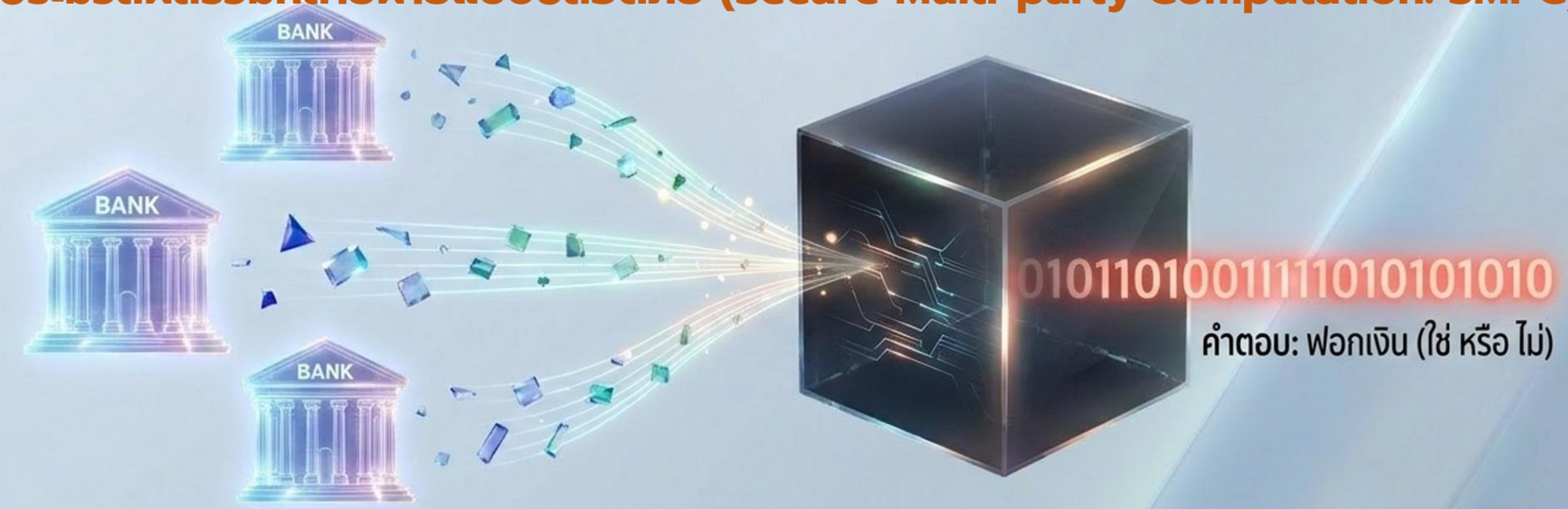
ระหว่างประมวลผล (Computation Privacy)
คำนวณและวิเคราะห์โดยไม่เห็นข้อมูลดิบ
Secure Computation (MPC, HE, TEE)
Federated Learning (FL)

ผลลัพธ์ขาออก (Output Privacy)
ป้องกันไม่ให้ผลลัพธ์ย้อนกลับไปหาตัวบุคคลได้
Differential Privacy (DP)
Zero-Knowledge Proofs (ZKP)
Synthetic Data

Secure Computation (MPC / TEE): ถอดสมการร่วมกันโดยปิดตา

แยกข้อมูลเป็นส่วนย่อย (Secret Shares) ให้คำนวณร่วมกัน โดยไม่มีใครเห็นข้อมูลองค์กรอื่น

การประมวลผลร่วมหลายฝ่ายแบบปลอดภัย (Secure Multi-party Computation: SMPC)



Use Case ในไทย: 3 ธนาคารตรวจสอบการฟอกเงินข้ามองค์กร
โดยไม่ต้องส่งข้อมูลลูกค้าให้แก่กัน (ปลดล็อกข้อจำกัดทางกฎหมาย)

Nontawatt Saraman

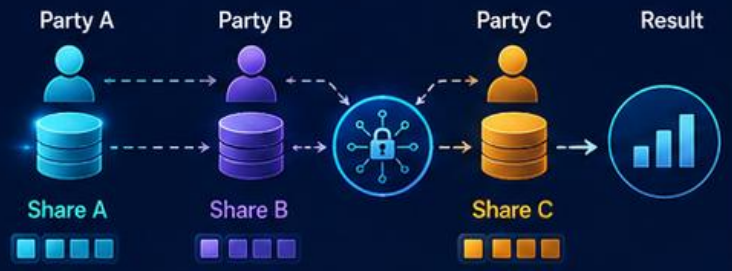
PRIVACY · AI · TRUST

SECURE COMPUTATION · ภาพรวม

Secure Computation · คำนวณบนข้อมูลที่ยังเข้ารหัสอยู่

กลุ่มเทคนิคที่ทำให้หลายฝ่ายร่วมประมวลผลข้อมูล โดยไม่มีใครเห็นข้อมูลดิบของอีกฝ่าย

01 Secure Multi-Party Computation (MPC)



วิธีทำงาน	แบ่งข้อมูลเป็น secret shares แจกให้หลายฝ่าย คำนวณร่วมกันโดยไม่มีฝ่ายใดเห็นค่าจริง
ข้อดี	ความปลอดภัยพิสูจน์ได้ · ไม่ต้องเชื่อใครเลย
ข้อจำกัด	ใช้ communication สูง · เหมาะกับการคำนวณไม่ใหญ่มาก

02 Homomorphic Encryption (HE)

วิธีทำงาน	แข้ารหัสข้อมูลแล้ว server คำนวณบน ciphertext ได้โดยตรง ผลลัพธ์ถอดรหัสได้ภายหลัง
ข้อดี	ไม่ต้อง interactive · ส่งข้อมูล cloud ได้อย่างปลอดภัย
ข้อจำกัด	ช้ามาก (1,000-1,000,000x) · เหมาะกับ workload เฉพาะ

03 Trusted Execution Environment (TEE)

วิธีทำงาน	เขตปลอดภัยใน CPU เช่น Intel SGX, AMD SEV, Arm CCA
ข้อดี	ประสิทธิภาพใกล้เคียง native · รองรับ workload ทั่วไป
ข้อจำกัด	ต้องเชื่อ vendor hardware · มี side-channel attack

PETs · Privacy-Enhancing Technologies

Nontawatt Saraman

ข้อมูลขาเข้า (Input Privacy)
ปกป้องข้อมูลก่อนเข้าสู่ระบบ
Data Masking / Pseudonymization
k-anonymity

ระหว่างประมวลผล (Computation Privacy)
คำนวณและวิเคราะห์โดยไม่เห็นข้อมูลดิบ
Secure Computation (MPC, HE, TEE)
Federated Learning (FL)

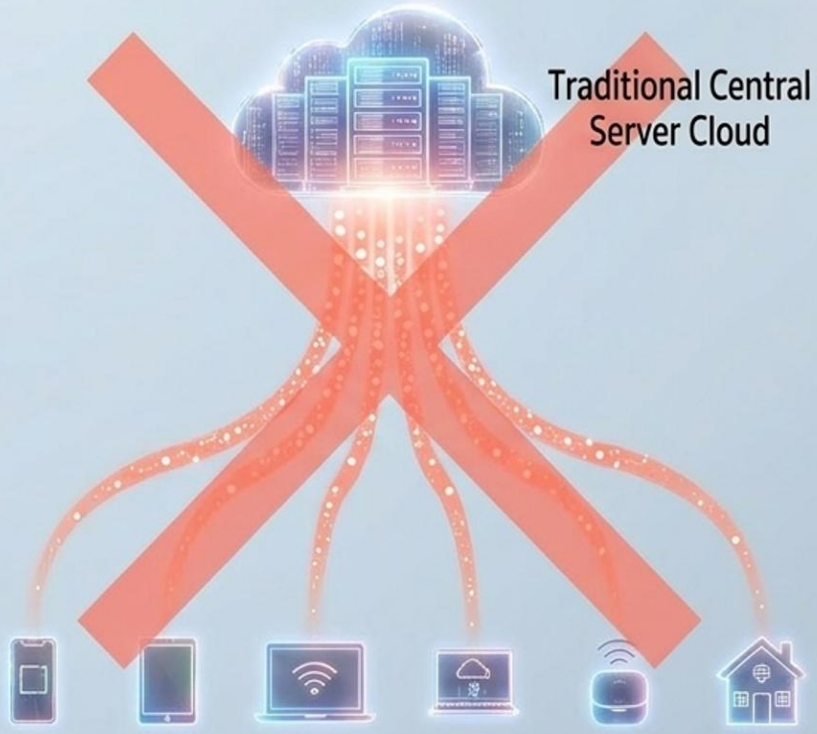
ผลลัพธ์ขาออก (Output Privacy)
ป้องกันไม่ให้ผลลัพธ์ย้อนกลับไปหาตัวบุคคลได้
Differential Privacy (DP)
Zero-Knowledge Proofs (ZKP)

สมาพันธ์ Learning

Federated Learning (FL): นำโมเดลไปหาข้อมูล ไม่ใช่ดึงข้อมูลมาหาโมเดล

ฝึก AI ที่หน้างาน (Local) และส่งกลับเฉพาะสิ่งที่เรียนรู้ (Updates) ข้อมูลดิบไม่เคยออกจากอุปกรณ์

Traditional Data Sharing (แบบดั้งเดิม)



Federated Learning (FL)

Proof: Google Gboard ทำนายคำบนมือถือกว่า 1,000 ล้านเครื่อง โดย Google ไม่เคยเห็นข้อความจริง

Nontawatt Saraman

ข้อมูลขาเข้า (Input Privacy)
ปกป้องข้อมูลก่อนเข้าสู่ระบบ
Data Masking / Pseudonymization
k-anonymity

ระหว่างประมวลผล (Computation Privacy)
คำนวณและวิเคราะห์โดยไม่เห็นข้อมูลดิบ
Secure Computation (MPC, HE, TEE)
Federated Learning (FL)

ผลลัพธ์ขาออก (Output Privacy)
ป้องกันไม่ให้ผลลัพธ์ย้อนกลับไปหาตัวบุคคลได้
Differential Privacy (DP)
Zero-Knowledge Proofs (ZKP)

ความเป็นส่วนตัวเชิงอนุพันธ์

Differential Privacy (DP): การเติม Noise ทางคณิตศาสตร์ที่ควบคุมได้

การปกป้องระดับบุคคลด้วยคณิตศาสตร์ที่พิสูจน์ได้ ไม่ใช่แค่การทำ Masking แบบดั้งเดิม

Low ε

ε (Epsilon) - Privacy Budget

High ε

ความเป็นส่วนตัวสูงสุด
แต่ผลลัพธ์คลาดเคลื่อน

แม่นยำสูง
แต่เสี่ยงต่อการระบุตัวตน

U.S. Census 2020:
ใช้งานกับข้อมูลประชากร 330 ล้านคน

Apple iOS:
เก็บสถิติข้ามอุปกรณ์นับล้านโดยไม่ละเมิดผู้ใช้

Google & LinkedIn:
เปิดเผยข้อมูลให้ปลอดภัย

ข้อมูลขาเข้า (Input Privacy)
ปกป้องข้อมูลก่อนเข้าสู่ระบบ

Data Masking / Pseudonymization

k-anonymity

ระหว่างประมวลผล (Computation Privacy)
คำนวณและวิเคราะห์โดยไม่เห็นข้อมูลดิบ

Secure Computation (MPC, HE, TEE)

Federated Learning (FL)

ผลลัพธ์ขาออก (Output Privacy)
ป้องกันไม่ให้ผลลัพธ์ย้อนกลับไปหาตัวบุคคลได้

Differential Privacy (DP)

Zero-Knowledge Proofs (ZKP)

Synthetic Data คืออะไร?

ข้อมูลที่สร้างขึ้นใหม่ให้คล้ายข้อมูลจริง แต่ไม่ใช่ข้อมูลจริงของคนจริง

เข้าใจแบบง่ายๆ

1 ข้อมูลจริง

ชื่อ	อายุ	รายได้	พฤติกรรม
นาย ก	35	45,000	โอน 10 ครั้ง
นาง ข	42	62,000	ซื้อสินค้า 6 ครั้ง
นาย ค	29	31,000	ใช้บัตร 14 ครั้ง

2 ลบชื่อ / ปิดบังบางส่วน

3 Synthetic Data

ID	อายุ	รายได้	พฤติกรรม
User_001	34	46,200	โอน 9 ครั้ง
User_002	44	60,800	ซื้อสินค้า 5 ครั้ง
User_003	30	32,500	ใช้บัตร 13 ครั้ง

คอมพิวเตอร์หรือ AI สร้างข้อมูลใหม่ ที่มีรูปแบบใกล้เคียงข้อมูลจริง

ข้อมูลจริง	Synthetic Data
นาย ก | อายุ 35 | รายได้ 45,000 | โอน 10 ครั้ง/เดือน	User_001 | อายุ 34 | รายได้ 46,200 | โอน 9 ครั้ง/เดือน
นาง ข | อายุ 42 | รายได้ 62,000 | ซื้อสินค้า 6 ครั้ง/เดือน	User_002 | อายุ 44 | รายได้ 60,800 | ซื้อสินค้า 5 ครั้ง/เดือน
นาย ค | อายุ 29 | รายได้ 31,000 | ใช้บัตร 14 ครั้ง/เดือน	User_003 | อายุ 30 | รายได้ 32,500 | ใช้บัตร 13 ครั้ง/เดือน

ข้อมูลฝั่งขวาไม่ใช่คนจริง แต่มีรูปแบบใกล้เคียงข้อมูลจริง

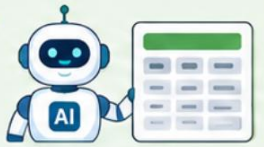
ใช้ทำอะไรได้บ้าง

- ฝึกโมเดล AI
- ทดสอบระบบโดยไม่ใช้ข้อมูลจริง
- แชร์ข้อมูลได้ปลอดภัยขึ้น
- ลดความเสี่ยงด้าน PDPA / Privacy

ภาพจำง่ายๆ

1  ข้อมูลจริง = คนจริง

2  Anonymized Data = คนจริงที่ถูกปิดบังข้อมูล

3  Synthetic Data = คนใหม่ที่ AI สร้างขึ้น

สรุป: Synthetic Data คือข้อมูลจำลองที่สร้างขึ้นใหม่ เพื่อใช้แทนข้อมูลจริงอย่างปลอดภัยมากขึ้น

Nontawatt Saraman

Zero-Knowledge Proof (ZKP) คืออะไร?

การพิสูจน์ว่าเรารู้คำตอบจริง โดยไม่ต้องเปิดเผยความลับ

1. เข้าใจง่ายๆ

ระบบมั่นใจได้ว่าผู้ใช้รู้ความลับจริง แต่ไม่เห็นความลับนั้น

2. ตัวอย่างในชีวิตจริง

ไม่ต้องบอกรหัสผ่านจริง

3. ZKP ทำงานอย่างไร

รู้จริง แต่ไม่ต้องบอกทั้งหมด

4. ใช้ทำอะไรได้บ้าง

- ยืนยันตัวตนแบบรักษาความเป็นส่วนตัว
- พิสูจน์ว่าอายุเกิน 18 ปี โดยไม่เปิดเผยวันเกิดเต็ม
- ใช้ใน Blockchain / Web3
- ลดการเปิดเผยข้อมูลสำคัญ

สรุป: Zero-Knowledge Proof คือการพิสูจน์ความจริงบางอย่าง โดยไม่ต้องเปิดเผยข้อมูลลับที่ใช้พิสูจน์

The Privacy Crisis in AI

AI ต้องการข้อมูลมากขึ้น แต่ Privacy บังคับให้องค์กรเปิดเผยข้อมูลน้อยลง

AI & Data Demand

AI ต้องการข้อมูลจำนวนมาก
เพื่อเรียนรู้และตัดสินใจ

Privacy Barriers

ข้อมูลอ่อนไหว แชร์ไม่ได้
รวมศูนย์ยาก และเสี่ยงหากรั่วไหล

PETs Solution

PETs ทำให้ใช้ข้อมูลได้
โดยไม่ต้องเปิดเผยทั้งหมด

1. ใช้ข้อมูลได้มากขึ้น
2. ลดการเปิดเผยข้อมูลดิบ
3. สร้าง Trusted AI

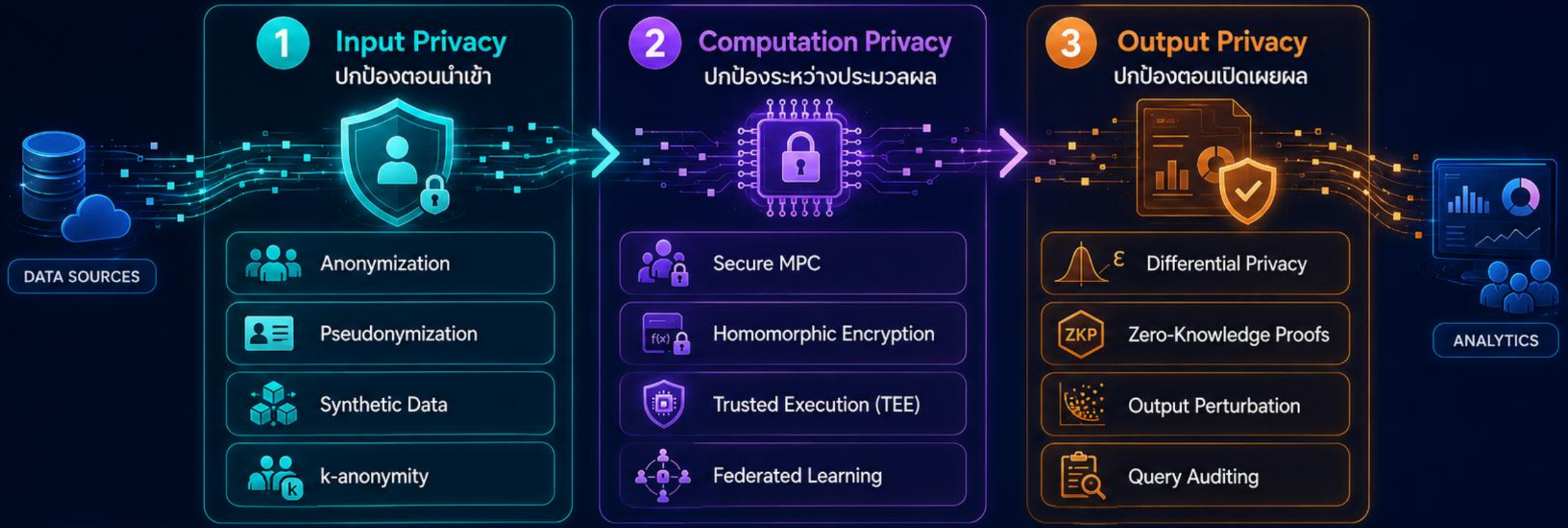
> “PETs เปลี่ยน Privacy จากข้อจำกัด ให้กลายเป็นตัวเปิดทางของ AI”

Nontawatt Saraman

TAXONOMY · การจัดประเภท PETs

PETs จัดกลุ่มได้ตามจุดที่เข้าไปปกป้องข้อมูล

ตามมาตรฐาน **UN Handbook** on Privacy-Enhancing Technologies (2023) และ NIST Privacy Engineering



ในวันนี้เราจะเจาะ 3 เทคโนโลยีที่สำคัญที่สุด: **Differential Privacy** · **Secure Computation** · **Federated Learning**

Nontawatt Saraman

From Data Sharing to Insight Sharing

จากการแชร์ข้อมูลดิบ ไปสู่การแชร์ผลลัพธ์อย่างปลอดภัย

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

แบบเดิม

แบบ PETs

	แบบเก่า	แบบ PETs
สิ่งที่แชร์: ข้อมูลดิบ / ผลลัพธ์เชิงลึก	ข้อมูลดิบ	ผลลัพธ์เชิงลึก / model update / ผลลัพธ์จากการคำนวณเข้ารหัส
สถาปัตยกรรม: รวมศูนย์ / กระจายศูนย์	รวมศูนย์	กระจายศูนย์
ความเสี่ยง: สูง / ต่ำลง	สูง	ต่ำลง
บทบาทของ Privacy: ข้อจำกัด / ตัวเปิดทาง	ข้อจำกัด	ตัวเปิดทาง

> “ PETs เปลี่ยนวิธีคิดจากการขอข้อมูล มาเป็นการคำนวณร่วมกัน โดยไม่ต้องเห็นข้อมูลทั้งหมด ”

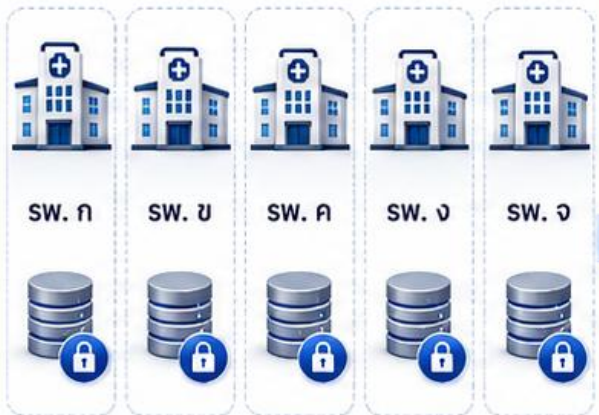
Nontawatt Saraman

เหตุการณ์ตัวอย่าง: โรงพยาบาลร่วมกันฝึก AI

สร้าง AI วินิจฉัยโรค โดยข้อมูลคนไข้ไม่ออกจากโรงพยาบาล

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

1 โจทย์

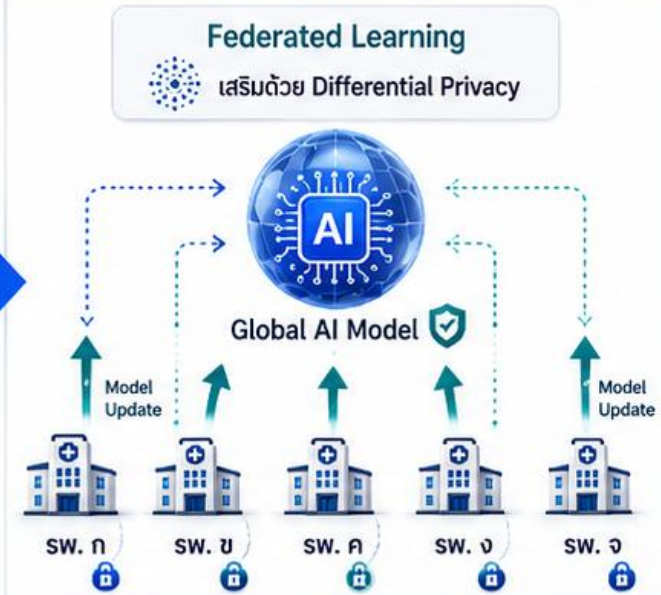


แต่ละโรงพยาบาลมีข้อมูลคนไข้
ไม่พอสำหรับ AI ที่แม่นยำ

2 ข้อจำกัด

การรวมข้อมูลคนไข้ไว้ที่เดียว
เสี่ยงต่อ PDPA ความเชื่อมั่น และการรั่วไหล

3 แนวทาง PETs



AI ไปเรียนรู้ที่แต่ละโรงพยาบาล
แล้วส่งกลับเฉพาะ model update

ผลลัพธ์ที่ได้

- ข้อมูลคนไข้ ไม่ออกจากโรงพยาบาล
- โมเดลแม่นยำขึ้น จากข้อมูลหลายแห่ง
- ลดความเสี่ยงด้าน กฎหมายและความเชื่อมั่น
- เร่งการพัฒนา Trusted Healthcare AI

> “ข้อมูลคนไข้ ไม่เดินทาง แต่ความรู้จากข้อมูลเดินทางได้” AI

Nontawatt Saraman

เหตุการณ์ตัวอย่าง: ธนาคารจับ Fraud ร่วมกัน

ร่วมกันตรวจจับธุรกรรมผิดปกติ โดยไม่ต้องเปิดข้อมูลลูกค้าให้กัน

ปัญหาเดิม
แต่ละธนาคารเห็นแค่บางส่วนของภาพรวม
จึงจับ fraud ได้ไม่เต็มประสิทธิภาพ

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

Bank A — ฐานข้อมูลลูกค้า A → พบธุรกรรมต้องสงสัย
Bank B — ฐานข้อมูลลูกค้า B → พบบัญชีเสี่ยง
Bank C — ฐานข้อมูลลูกค้า C → พบ pattern บัญชีม้า

ส่งข้อมูลแบบเข้ารหัส (Share / Secure Query)

MPC / Secure Computation

- เข้ารหัส (Encryption)
- คำนวณแบบกระจาย (Secure Computation)
- ไม่เปิดเผยข้อมูลดิบ (No Raw Data Exposure)

วิเคราะห์ร่วมกันอย่างปลอดภัย

ผลลัพธ์เชิงลึกที่ได้จากความร่วมมือ

- เครือข่ายบัญชีเสี่ยง
- ธุรกรรมผิดปกติข้ามธนาคาร
- 78 คะแนนความเสี่ยงร่วม
- แจ้งเตือนแบบ consortium

แต่ละธนาคารเก็บข้อมูลลูกค้าไว้กับตัวเอง (Data Stays in Bank)

คำนวณบนข้อมูลเข้ารหัส ได้ผลลัพธ์รวม โดยไม่เห็นข้อมูลลูกค้ารายใด

เห็นภาพรวมครบถ้วน จับ fraud ได้แม่นยำและรวดเร็วขึ้น

1. **ไม่ต้องแชร์ข้อมูลลูกค้าดิบ** — ข้อมูลลูกค้ายังปลอดภัย อยู่ที่แต่ละธนาคาร
2. **เห็น pattern ร่วมกันได้** — มองเห็นความเชื่อมโยงข้ามธนาคารที่ซับซ้อน
3. **ลด false negative** — ตรวจจับ fraud ได้มากขึ้น ลดจุดบอดของข้อมูล
4. **ยกระดับความร่วมมือด้าน AML/Fraud** — สร้างมาตรฐานและความเชื่อมั่นร่วมกันทั้งอุตสาหกรรม

> “ร่วมกันจับโจร โดยไม่ต้องเปิดสมุดบัญชีลูกค้าให้กันดู”

Nontawatt Saraman

PRIVACY · AI · TRUST

SRAN®

USE CASE 02 · Financial Services

Banking & Finance · Anti-Fraud และ Credit Scoring ข้ามธนาคาร

Challenge: Fraud ขยายข้ามธนาคารและข้ามประเทศ · ลูกค้ารายเดียวอาจมีบัญชีหลายแห่ง · Bank Secrecy + PDPA ห้ามแชร์ลูกค้า

01 Secure MPC

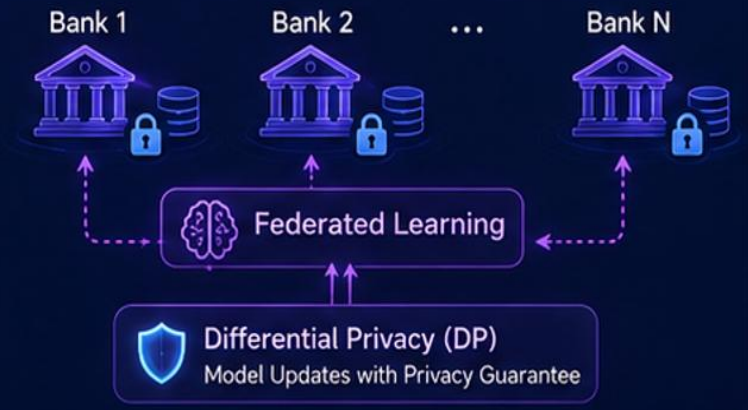
Inpher / Mastercard / SWIFT Sanction Screening

ใช้ MPC ตรวจว่าธุรกรรมเข้า sanction list หรือไม่ โดย bank ไม่ต้องส่ง raw payment ให้ใคร

02 FL + DP

Bank of England Fraud Detection Sandbox

ทดสอบให้ธนาคาร UK ฝึกโมเดลตรวจฉ้อโกงร่วมกัน ด้วย Federated Learning + DP



03 PETs Sandbox

Singapore Project Trinidad / Project Aurora

MAS ใช้ PETs ในการ joint analytics ระหว่างธนาคารและ regulator เพื่อตรวจ AML / TF

ในไทย: ธปท. มี Regulatory Sandbox · หลายธนาคารเริ่มทดลอง PETs สำหรับ AML และ KYC sharing

Nontawatt Saraman

เหตุการณ์ตัวอย่าง: เปิดข้อมูลสถิติ โดยไม่เปิดชีวิตประชาชน

ภาครัฐเผยแพร่ข้อมูลเชิงนโยบายได้ โดยลดความเสี่ยงการระบุตัวบุคคล

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

1 ข้อมูลต้นทาง

ข้อมูลรายบุคคล (ละเอียด)

อายุ	35 ปี
ภูมิภาค/จังหวัด	เชียงใหม่
สถานะสุขภาพ	เบาหวาน
รายได้	18,000 บาท
ระดับการศึกษา	ปริญญาตรี
ข้อมูลอื่น ๆ	...

ข้อมูลดิบมีความละเอียดสูง และอ่อนไหวมาก

2 ความเสี่ยง

ความเสี่ยงการระบุตัวบุคคลซ้ำ (Re-identification Risk)

แม้ลบชื่อแล้ว ก็ยังอาจระบุตัวบุคคลได้

3 Differential Privacy

ชั้นการคุ้มครองความเป็นส่วนตัว

เติม noise ให้กับข้อมูล

เติม noise เพื่อปกป้องรายบุคคล แต่คงคุณค่าของภาพรวม

4 ผลลัพธ์เชิงนโยบาย

ข้อมูลสถิติรวม (ไม่สามารถระบุตัวบุคคลได้) สำหรับวิเคราะห์และตัดสินใจเชิงนโยบาย

ใช้ได้กับ

- สถิติประชากร
- ข้อมูลสุขภาพภาพรวม
- open data เชิงนโยบาย
- public dashboard

1. **เปิด insight ไม่ใช่เปิด identity** — เผยแพร่เฉพาะสิ่งที่จำเป็นต่อการตัดสินใจ
2. **ลดความเสี่ยง re-identification** — ด้วยเทคนิคคุ้มครองความเป็นส่วนตัว
3. **สนับสนุน data-driven policy** — ใช้ข้อมูลสถิติที่เชื่อถือได้ เพื่อออกแบบนโยบายที่ดีขึ้น

> “Open Data ที่ดี ไม่ใช่เปิดทุกอย่าง แต่เปิดให้เกิดประโยชน์โดยไม่เปิดชีวิตของประชาชน”

Nontawatt Saraman

Cross-Border AI Collaboration

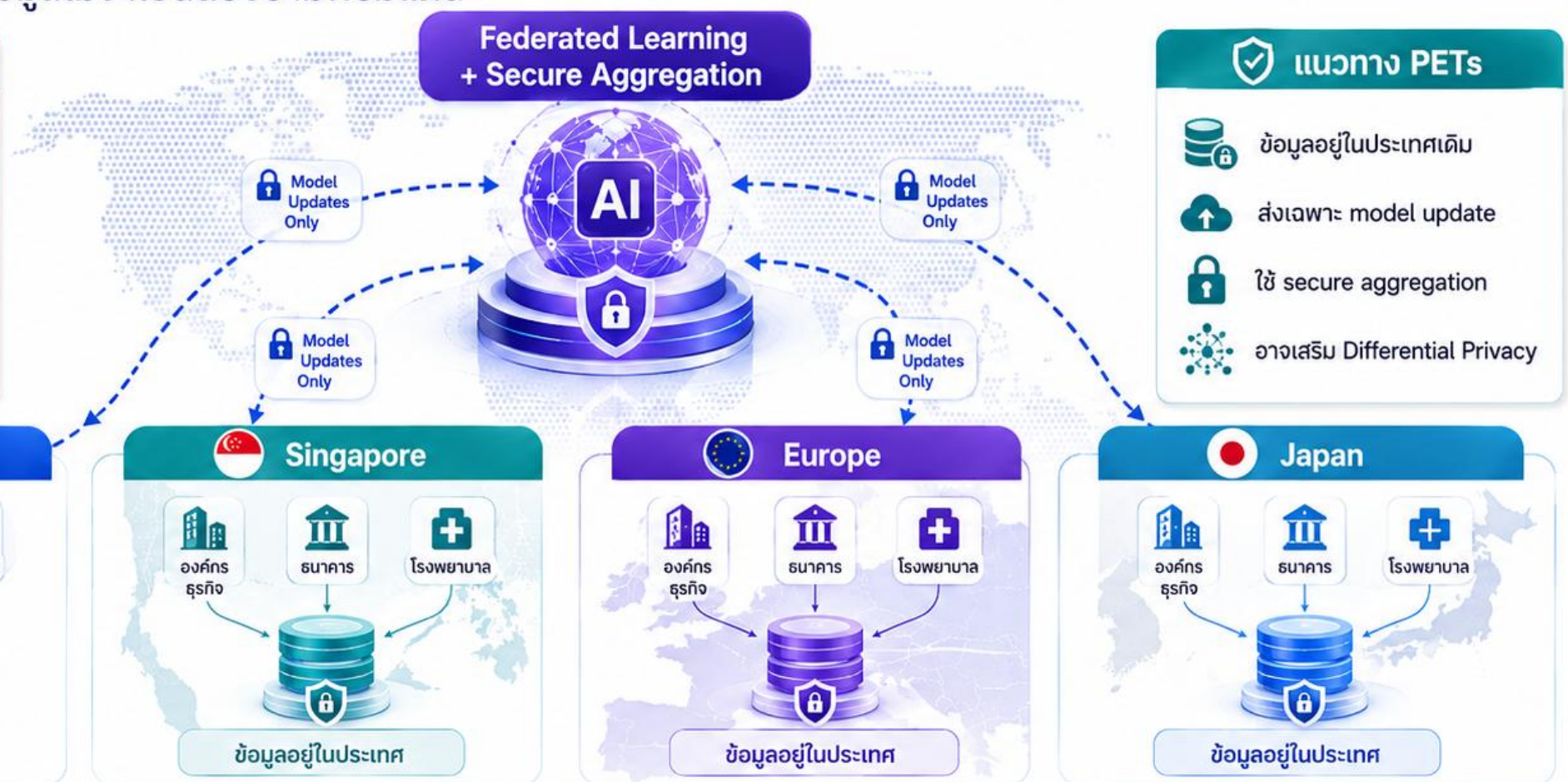
AI ข้ามพรมแดนได้ โดยข้อมูลไม่จำเป็นต้องข้ามพรมแดน

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

ข้อจำกัดเดิม

- Data residency
- Data sovereignty
- Privacy law แตกต่างกัน
- ย้ายข้อมูลข้ามประเทศยาก

Federated Learning + Secure Aggregation



แนวทาง PETs

- ข้อมูลอยู่ในประเทศเดิม
- ส่งเฉพาะ model update
- ใช้ secure aggregation
- อาจเสริม Differential Privacy

1 พัฒนา AI ร่วมกันได้
ร่วมเรียนรู้จากข้อมูลหลายประเทศ

2 ลดข้อจำกัดข้ามพรมแดน
ไม่ต้องย้ายข้อมูล ลดต้นทุนและความเสี่ยง

3 ตอบโจทย์ compliance
เคารพกฎหมายและกฎระเบียบท้องถิ่น

4 Move the model, not the data
โมเดลเดินทางได้ ข้อมูลปลอดภัยในประเทศ

> “โมเดล AI เดินทางได้ แต่ข้อมูลลูกค้าไม่จำเป็นต้องเดินทาง”

Nontawatt Saraman

CIPAT
สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์
Cyber Innovation Promotion Association of Technology

PETs Readiness • 5 เสาหลักที่ต้องประเมินก่อนลงทุน

01
Data & Use Case
- มี use case ชัดเจน?
- ข้อมูลอยู่ที่ไหน ใครเป็นเจ้าของ?
- ระดับ sensitivity ของข้อมูล?

02
Legal & Compliance
- PDPA / GDPR base, DPO เห็นด้วยกับ approach?
- Contract / DPA ระหว่างองค์กร

03
Technical Capability
- มีทีม ML / Crypto?
- Infrastructure: cloud / TEE?
- MLOps มาตรฐาน?

04
Governance
- Privacy budget management
- model risk management
- audit trail / logging

05
Stakeholders & Trust
- ผู้บริหารสนับสนุน?
- Partners / ลูกค้าเชื่อใจ?
- Communication กับ regulator

ใช้เป็น **self-assessment checklist** ภายใน 1 ชั่วโมงก่อนเริ่ม initiative

Nontawatt Saraman