จุดอ่อนและแนวทางป้องกันภัยคุกคามจากการใช้งานชีวมิติ (Biometrics)

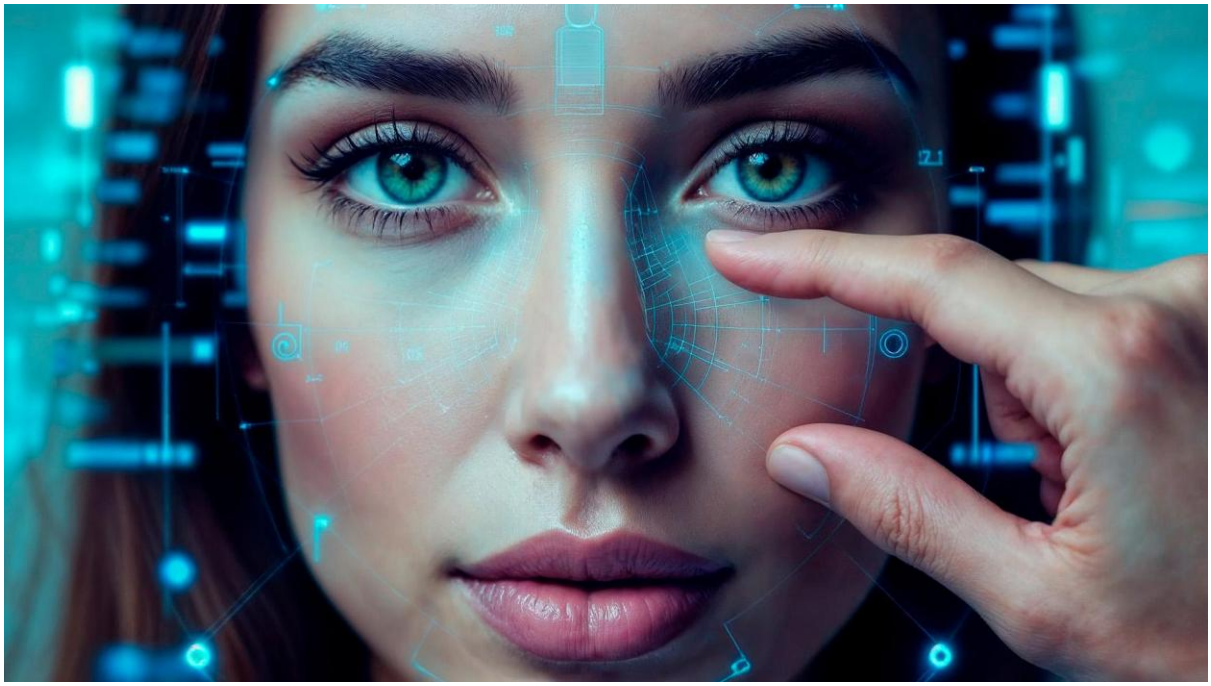
1. บทนำ

การใช้งานชีวมิติ (Biometric) เช่น ใบหน้า ลายนิ้วมือ และม่านตา ได้กลายเป็นแนวทางหลักของระบบพิสูจน์และยืนยันตัวตนทางดิจิทัลในยุคปัจจุบัน [1] ด้วยคุณสมบัติที่มีความปลอดภัย ใช้งานสะดวก และสามารถระบุตัวบุคคลได้อย่างแม่นยำ ทำให้ Biometric เป็นเทคนิคหรือวิธีการที่ใช้ในการตรวจสอบสิทธิ์ของบุคคลในการเข้าถึงบริการ หรืออาจกล่าวได้ว่าเป็นการป้องกันการเข้าถึงบริการโดยไม่ได้รับอนุญาต อย่างไรก็ตาม จากการวิเคราะห์มาตรฐานสากล ISO/IEC 24745:2022 Information security, cybersecurity and privacy protection — Biometric information protection [2] ซึ่งเป็นมาตรฐานด้านความมั่นคงปลอดภัยของการจัดเก็บข้อมูลชีวมิติ พบว่าระบบ Biometric มีจุดที่ต้องระวังในแต่ละส่วนของระบบย่อยชีวมิติ (Biometric subsystem) หากออกแบบโดยขาดความเข้าใจเชิงเทคนิค หรือไม่มีมาตรการควบคุมความเสี่ยงที่เหมาะสม อาจกลายเป็นช่องโหว่ให้ระบบถูกโจมตีได้

2. ข้อควรระวังในการใช้งานชีวมิติเพื่อการยืนยันตัวตน

การใช้งานชีวมิติ (Biometric) เพื่อยืนยันตัวตน (authentication) โดยการใช้ข้อมูลทางกายภาพ เช่น ลายนิ้วมือ ม่านตา และใบหน้า หรืออาจมีการใช้ข้อมูลเชิงพฤติกรรมร่วมด้วย เช่น จังหวะการพิมพ์หรือรูปแบบการเดิน เป็นวิธีการการยืนยันตัวตนบุคคลที่มีความน่าเชื่อถือค่อนข้างสูง ทั้งนี้ NIST 800-63B Digital Identity Guidelines Authentication and Lifecycle Management [1] ได้กำหนดให้การใช้งานชีวมิติเป็นวิธีการที่ต้องมีการจำกัด เนื่องจากเหตุผลทางเทคนิคและความมั่นคงปลอดภัยต่าง ๆ เช่น

- เมื่อข้อมูลชีวมิติเกิดการรั่วไหล จะไม่สามารถเปลี่ยนแปลงหรือออกใหม่เพื่อทดแทนได้เหมือนการใช้รหัสผ่านที่สามารถขอใหม่ได้เรื่อย ๆ
- การเก็บข้อมูลใบหน้าไว้ในอุปกรณ์ควรจัดเก็บในพื้นที่เฉพาะที่มีความปลอดภัยสูง เช่น Trusted Execution Environment (TEE) ทั้งนี้ NIST 800-63B ได้ระบุว่าข้อมูลชีวมิติไม่ถือเป็นข้อมูลลับ เนื่องจากสาเหตุ เช่น ภาพใบหน้าที่สามารถค้นหาได้บนอินเทอร์เน็ต, การถูกผู้อื่นถ่ายภาพใบหน้า และการเก็บลายนิ้วมือบนวัตถุที่ถูกสัมผัส เป็นต้น
- อัตราการจับคู่ผิด (False Match Rate – FMR) ของระบบ Biometric ไม่เพียงพอในการสร้างความมั่นใจว่าเป็นผู้ใช้ตัวจริง และไม่สามารถป้องกันการโจมตีแบบสวมรอย (Spoofing) ได้โดยสมบูรณ์
- แม้จะมีเทคโนโลยี PAD (Presentation Attack Detection) เช่น Liveness Detection แต่ยังต้องอาศัยความน่าเชื่อถือของตัวเซ็นเซอร์และอุปกรณ์ประมวลผลร่วมด้วย



3. จุดที่ต้องระวังในการพัฒนาระบบย่อยชีวมิติ (Biometric subsystem)

ระบบชีวมิติประกอบด้วยระบบย่อยที่ทำหน้าที่แตกต่างกัน ตั้งแต่การรับข้อมูลชีวมิติตั้งต้นของบุคคล ไปจนถึงการตัดสินผลการยืนยันตัวตน โดย ISO/IEC 24745:2022 ได้แบ่งระบบย่อยชีวมิติออกเป็น 5 ส่วน ได้แก่ Biometric Data Capture, Signal Processing, Data Storage, Comparison และ Decision โดยในแต่ละระบบย่อยนั้น มีจุดที่ต้องระวังซึ่งอาจถูกใช้เป็นช่องทางในการโจมตีได้ [2] [3] ดังนี้

- **Biometric Data Capture Subsystem:** ทำหน้าที่รวบรวมลักษณะทางชีวมิติของบุคคล เช่น ลายนิ้วมือ ใบหน้า หรือม่านตา ผ่านอุปกรณ์หรือเซ็นเซอร์ จากนั้นจะแปลงลักษณะทางชีวมิติเป็นข้อมูลชีวมิติ เช่น ภาพลายนิ้วมือ ภาพใบหน้า หรือภาพม่านตา เพื่อใช้ในระบบย่อยถัดไป

  ภัยคุกคามที่อาจเกิดขึ้นในขั้นตอนนี้ ได้แก่ การปลอมแปลงเซ็นเซอร์ (Sensor Spoofing) และการดักจับข้อมูลจากเซ็นเซอร์เพื่อใช้ซ้ำ (Capture/Replay Attack) แนวทางป้องกันที่สามารถนำมาใช้ได้ คือการใช้เทคนิคตรวจจับการโจมตีหลอกระบบชีวมิติ (Presentation Attack Detection) การใช้ระบบไบโอเมตริกหลายรูปแบบร่วมกัน (Multimodal Biometric) การใช้ทดสอบการตอบสนองของบุคคล (Challenge/Response) และการเข้ารหัสข้อมูลที่อุปกรณ์เก็บข้อมูล (Hardware Encryption)

- **Signal Processing Subsystem:** ทำหน้าที่ดึงคุณลักษณะสำคัญจากข้อมูลชีวมิติ และแปลงให้อยู่ในรูปแบบตัวเลขหรือรหัสที่สามารถนำไปใช้เปรียบเทียบได้ ข้อมูลนี้จะถูกจัดเก็บไว้ในฐานข้อมูลเพื่อใช้ในการยืนยันตัวตนหรือระบุตัวตนบุคคล

ภัยคุกคามที่มักเกิดขึ้นในระบบย่อยนี้คือการแก้ไขหรือดัดแปลงข้อมูลชีวมิติโดยไม่ได้รับอนุญาตระหว่างการประมวลผล โดยแนวทางป้องกันที่เป็นไปได้คือการใช้อัลกอริทึมที่เชื่อถือได้ (Trusted Algorithm) ในการปกป้องข้อมูลเพื่อลดความเสี่ยงจากการโจมตี

- **Data Storage Subsystem:** ทำหน้าที่เป็นฐานข้อมูลสำหรับจัดเก็บข้อมูลชีวมิติที่ได้ลงทะเบียนไว้ โดยเชื่อมโยงข้อมูลอ้างอิงทางชีวมิติ (Biometric Reference: BR) เข้ากับข้อมูลอ้างอิงตัวตน (Identity Reference: IR) เพื่อใช้ในกระบวนการตรวจสอบ ทั้งนี้เพื่อความปลอดภัยและความเป็นส่วนตัว ฐานข้อมูล BR และ IR มักถูกแยกออกจากกันทั้งในเชิงตรรกะหรือกายภาพ

  ภัยคุกคามหลักในระบบย่อยนี้คือการโจมตีฐานข้อมูล เช่น การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การแทนที่ แก้ไข หรือลบข้อมูล BR/IR รวมถึงการโจมตีแบบ Distributed Denial of Service (DDoS) โดยมีแนวทางป้องกันภัยคุกคามนี้ เช่น การควบคุมการเข้าถึงฐานข้อมูล การลงลายมือชื่อดิจิทัลและเข้ารหัสข้อมูล BR/IR รวมถึงการวางแผนสำรองและฟื้นฟูระบบอย่างเหมาะสม

- **Comparison Subsystem:** ทำหน้าที่เปรียบเทียบความเหมือนกันระหว่างข้อมูลชีวิมิติที่ต้องการตรวจสอบกับข้อมูลชีวมิติที่มีอยู่ในระบบ หากเป็นการยืนยันตัวตนแบบหนึ่งต่อหนึ่ง (One-to-One Verification) ระบบจะเปรียบเทียบข้อมูลชีวิมิติที่ต้องการตรวจสอบกับข้อมูลของบุคคลที่อ้างว่าเป็นเจ้าของข้อมูลชีวมิติดังกล่าวซึ่งถูกจัดเก็บในฐานข้อมูลเพื่อวัดคะแนนความเหมือนกันระหว่างข้อมูลชีวมิติทั้งสอง ในขณะที่การระบุตัวตนแบบหนึ่งต่อกลุ่ม (One-to-Many Identification) จะเปรียบเทียบข้อมูลชีวิมิติที่ต้องการตรวจสอบกับข้อมูลชีวมิติทั้งหมดของทุกคนในฐานข้อมูลเพื่อหารายการของกลุ่มคนที่มีคะแนนความเหมือนกันระหว่างข้อมูลชีวมิติสูงสุด

  แนวทางป้องกันที่สามารถพิจารณาเพื่อนำมาใช้ป้องกันระบบย่อยนี้ได้ คือการใช้เซิร์ฟเวอร์หรือไคลเอนต์ที่ปลอดภัย และใช้ Trusted OCC (Operational Control Component) เพื่อป้องกันการโจมตี

- **Decision Subsystem:** ทำหน้าที่ตัดสินผลลัพธ์การเปรียบเทียบความเหมือนของข้อมูลชีวมิติ โดยใช้คะแนนความเหมือนและนโยบายการตัดสินใจ เช่น เกณฑ์คะแนนขั้นต่ำ เพื่อตัดสินผลลัพธ์ หากเป็นการยืนยันตัวตน ระบบจะยอมรับหรือปฏิเสธบุคคลนั้น ส่วนในกรณีการระบุตัวตน ระบบจะแสดงรายชื่อผู้ที่มีความเป็นไปได้สูงสุดตามเกณฑ์ที่กำหนด

  ภัยคุกคามที่อาจเกิดขึ้นในขั้นตอนย่อยนี้ ได้แก่ การโจมตีแบบไต่ระดับคะแนน (Hill Climbing) การโจมตีแบบ DDoS และการดัดแปลงช่วงเกณฑ์คะแนนความเหมือนของข้อมูลชีวมิติ (Threshold) โดยมีแนวทางป้องกันที่สามารถนำมาใช้ได้ เช่น การใช้ช่องทางเชื่อมต่อที่ปลอดภัยระหว่างแต่ละระบบย่อย การปกปิดคะแนนการเปรียบเทียบความเหมือนของข้อมูลชีวมิติ การป้องกันการเข้าถึงการตั้งค่า Threshold และปกป้องค่าของ Threshold จากการแก้ไขโดยไม่ได้รับอนุญาต

4. แนวปฏิบัติเพิ่มเติมในการใช้งานชีวมิติเพื่อการพิสูจน์และยืนยันตัวตนทางดิจิทัล

เพื่อให้สามารถใช้งานชีวมิติอย่างมั่นคงปลอดภัย NIST 800-63B กำหนดแนวทางที่ควรปฏิบัติไว้ดังนี้:

- ข้อมูลชีวมิติต้องใช้ร่วมกับปัจจัยประเภทอื่นเสมอ เช่น physical authenticator
- ต้องใช้ช่องทางสื่อสารที่ปลอดภัย (authenticated protected channel) ระหว่างเซ็นเซอร์และตัวตรวจสอบ (verifier) ก่อนเริ่มการยืนยันตัวตน
- ระบบชีวมิติต้องมี FMR (False Match Rate) ไม่เกิน 1 ใน 1,000 ภายใต้การทดสอบ conformant attack ตามมาตรฐาน ISO/IEC 30107-1 [3]
- ควรมีการใช้เทคนิค PAD โดยระบบควรต้านทานการโจมตีอย่างน้อย 90% จากการโจมตีหลากหลายรูปแบบ และต้องผ่านการทดสอบตาม ISO/IEC 30107-1 [3]
- ระบบต้องจำกัดจำนวนความพยายามล้มเหลวในการพิสูจน์ตัวตน โดยต้องมีการหน่วงเวลาในการพยายามยืนยันตัวตนแต่ละครั้ง

5. สรุป

การใช้งานชีวมิติ (Biometric) เป็นเทคโนโลยีสำคัญในการยืนยันตัวตนที่ให้ความสะดวกและแม่นยำ แต่ก็มีความเสี่ยงด้านความมั่นคงปลอดภัยที่ต้องระวัง เนื่องจากข้อมูลชีวมิติไม่สามารถเปลี่ยนใหม่ได้หากรั่วไหล และอาจถูกโจมตีในหลายจุดของระบบย่อย เช่น การปลอมแปลงเซ็นเซอร์ การดัดแปลงข้อมูล และการโจมตีฐานข้อมูล โดยมาตรฐานสากล เช่น ISO/IEC 24745:2022 และ NIST 800-63B ได้เสนอแนวทางเพื่อลดความเสี่ยง เช่น การใช้เทคนิคตรวจจับการโจมตี (PAD) การเข้ารหัสข้อมูล การควบคุมการเข้าถึง และการใช้ช่องทางสื่อสารที่ปลอดภัย อย่างไรก็ตาม เทคโนโลยีเหล่านี้ยังไม่สามารถป้องกันการโจมตีได้สมบูรณ์ จึงต้องมีมาตรการและการออกแบบระบบชีวมิติที่รัดกุม เช่น การเลือกใช้อุปกรณ์และอัลกอริทึมที่ผ่านการรับรองมาตรฐาน และมีการทดสอบตามเกณฑ์สากล รวมถึงต้องมีการจัดการข้อมูลชีวมิติอย่างเหมาะสม เช่น การเข้ารหัส การแยกเก็บข้อมูล และการวางแผนกู้คืนระบบ เพื่อให้การใช้งานชีวมิติมีความมั่นคงปลอดภัยและน่าเชื่อถือ

อ้างอิง

[1] “NIST Special Publication 800-63B Digital Identity Guidelines Authentication and Lifecycle Management”, Available: https://pages.nist.gov/800-63-3/sp800-63b.html. [Accessed: Jun. 22, 2025]

[2] “ISO/IEC 24745:2022 Information security, cybersecurity and privacy protection — Biometric information protection”, *ISO*, 2022. Available: https://www.iso.org/standard/75302.html. [Accessed: Jun. 22, 2025]

[3] “ISO/IEC 30107-1:2023 Information technology — Biometric presentation attack detection — Part 1 : Framework”, *ISO*, 2023. Available: https://www.iso.org/standard/83828.html. [Accessed: Jun. 22, 2025]