ภัยคุกคามจาก Deepfake ที่เกิดขึ้นในการพิสูจน์และยืนยันตัวตนทางดิจิทัล

1. บทนำ

การพัฒนาระบบ Digital ID เป็นองค์ประกอบสำคัญของการขับเคลื่อนเศรษฐกิจดิจิทัล ซึ่งช่วยให้ประชาชนสามารถเข้าถึงบริการสาธารณะ การเงิน และสวัสดิการได้อย่างสะดวก น่าเชื่อถือ และมั่นคงปลอดภัย โดยเฉพาะเมื่อมีการใช้เทคโนโลยีรู้จำใบหน้า (Facial Recognition) เพื่อให้การพิสูจน์และยืนยันตัวตนมีความถูกต้องและน่าเชื่อถือมากขึ้น อย่างไรก็ตาม ความก้าวหน้าของเทคโนโลยีปัญญาประดิษฐ์ (AI) โดยเฉพาะ Deepfake ได้สร้างความท้าทายแก่การใช้เทคโนโลยีรู้จำใบหน้า เนื่องจาก Deepfake สามารถสร้างภาพ วิดีโอ หรือเสียงปลอมที่สมจริงจนยากต่อการตรวจจับ หากระบบขาดมาตรการป้องกันที่มีประสิทธิภาพ ผู้ใช้บริการอาจถูกสวมรอยเพื่อเข้าถึงข้อมูลหรือสิทธิประโยชน์โดยมิชอบ ซึ่งเป็นภัยคุกคามต่อความมั่นคงปลอดภับของระบบ Digital ID

Deepfake ใช้เทคนิคโครงข่ายประสาทเทียมปฏิปักษ์ (Generative Adversarial Networks: GANs) เพื่อสร้างสื่อสังเคราะห์ที่แนบเนียน โดยอาศัยข้อมูลภาพ วิดีโอ หรือเสียงของบุคคลเป้าหมาย ทำให้สามารถเลียนแบบใบหน้าและเสียงได้อย่างสมจริง ภัยคุกคามนี้ส่งผลโดยตรงต่อระบบ Digital ID ที่ใช้ข้อมูลชีวมิติ เช่น ใบหน้าและเสียง โดยเฉพาะเมื่อระบบขาดการตรวจสอบความมีชีวิตหรือเป็นบุคคลจริง (Liveness Detection) ทำให้ผู้ไม่หวังดีสามารถใช้ภาพหรือวิดีโอปลอมเพื่อหลอกลวงระบบยืนยันตัวตน และอาจนำไปสู่การขโมยข้อมูลอัตลักษณ์หรือเข้าถึงบริการที่ต้องการความปลอดภัยสูง เช่น ธุรกรรมทางการเงินหรือการยืนยันตัวตนกับหน่วยงานของรัฐ

ผลกระทบของ Deepfake ไม่ได้จำกัดอยู่เพียงการสวมรอยเป็นบุคคลอื่น แต่ยังส่งผลต่อความน่าเชื่อถือของผู้ให้บริการ เช่น การฉ้อโกงทางการเงิน การทำลายชื่อเสียงองค์กร หรือแม้แต่การสร้างข่าวปลอม

ในวงกว้าง ดังนั้น การรับมือกับภัยคุกคามนี้ต้องอาศัยมาตรการหลายมิติ ทั้งการพัฒนาเทคโนโลยีตรวจจับ Deepfake และระบบ Liveness Detection ที่มีประสิทธิภาพ รวมถึงการออกกฎหมายควบคุมการใช้เทคโนโลยี และการสร้างความตระหนักรู้ในสังคม เพื่อป้องกันไม่ให้ Deepfake กลายเป็นช่องโหว่สำคัญของระบบ Digital ID ในอนาคต

2. ภัยคุกคามที่มักพบจากการโจมตีโดย Deepfake

เทคโนโลยี Deepfake เป็นภัยคุกคามสำคัญต่อระบบ Digital ID ที่มีการใช้ระบบรู้จำใบหน้า เนื่องจาก Deepfake สามารถสร้างสื่อปลอมที่สมจริงจนยากต่อการตรวจจับ ทำให้ผู้ไม่หวังดีสวมรอยเป็นบุคคลอื่นเพื่อเข้าถึงข้อมูลหรือแอบอ้างในนการทำธุรกรรมได้ง่ายขึ้น โดยภัยคุกคามที่มักพบจากการโจมตีด้วย Deepfake มีดังนี้

- **การลงทะเบียนโดยปลอมแปลงข้อมูลเป็นผู้อื่น (Fraudulent Registration):** เป็นการโจมตีที่ผู้ไม่หวังดีสร้าง Digital ID ใหม่โดยสวมรอยเป็นบุคคลอื่น กระบวนการโจมตีนี้เริ่มจากการเข้าถึงข้อมูลส่วนบุคคลของเหยื่อ เช่น หมายเลขบัตรประชาชน พร้อมรวบรวมภาพหรือวิดีโอจากแหล่งสาธารณะ เช่น โซเชียลมีเดีย ข้อมูลเหล่านี้จะถูกนำไปใช้สร้างสื่อสังเคราะห์ด้วยเทคโนโลยี Deepfake เพื่อสร้างวิดีโอใบหน้าของเหยื่อที่สมจริงและเคลื่อนไหวได้ตามเงื่อนไขที่กำหนด จากนั้นวิดีโอนี้จะถูกใช้หลอกลวงกระบวนการทำความรู้จักลูกค้าผ่านช่องทางอิเล็กทรอนิกส์ (e-KYC) ที่ต้องตรวจสอบข้อมูลชีวมิติด้วยใบหน้า หากระบบไม่สามารถตรวจจับความผิดปกติได้ การลงทะเบียนจะสำเร็จ ทำให้ผู้ไม่หวังดีสามารถสร้าง Digital ID ที่ปลอมเป็นเหยื่อได้ ซึ่ง Digital ID นี้อาจถูกนำไปใช้ในการฉ้อโกงทางการเงิน ฟอกเงิน หรือกิจกรรมผิดกฎหมายอื่น ๆ ที่สร้างความเสียหายต่อเหยื่อที่เป็นเจ้าของข้อมูลตัวจริง
- **การใช้ Deepfake ปลอมแปลงใบหน้าเพื่อทำธุรกรรม (Transaction Spoofing):** เป็นการโจมตีที่มุ่งเข้าถึง Digital ID ของเหยื่อ เมื่อระบบของผู้ให้บริการร้องขอการยืนยันตัวตนด้วยใบหน้า ผู้ไม่หวังดีจะใช้วิดีโอที่สร้างจาก Deepfake ซึ่งจะแสดงใบหน้าของเหยื่อที่สามารถแสดงการขยับท่าทางต่าง ๆ ได้ มาแสดงต่อระบบรู้จำใบหน้า หากระบบขาดกลไกตรวจจับความมีชีวิตหรือเป็นบุคคลจริง (Liveness Detection) หรือเทคโนโลยีป้องกันการปลอมแปลง (Anti-spoofing) ที่มีประสิทธิภาพ ระบบจะยอมรับข้อมูลปลอมและอนุมัติให้ผู้ไม่หวังดีเข้าถึง Digital ID ของเหยื่อ และสามารถเข้าถึงทรัพย์สินหรือข้อมูลสำคัญของเหยื่อได้
- **การปลอมแปลงด้วยภาพนิ่ง/หน้ากาก (Static Image/Mask Spoofing):** เป็นการโจมตีโดยใช้ภาพถ่ายความละเอียดสูง วิดีโอบันทึกภาพใบหน้าและการขยับท่าทางต่าง ๆ ของเหยื่อ หรือหน้ากากสามมิติ เพื่อหลอกระบบจดจำใบหน้าที่ไม่มีเทคโนโลยีตรวจจับความมีชีวิตหรือเป็นบุคคลจริง (Liveness Detection) ที่เพียงพอ ทำให้ระบบไม่สามารถแยกแยะใบหน้าจริงกับภาพปลอมได้ จุดอ่อนนี้เกิดจากการที่ระบบไม่สามารถตรวจสอบสัญญาณชีวมิติที่บ่งบอกถึงการมีชีวิต เช่น การ

กะพริบตา การขยับกล้ามเนื้อใบหน้า หรือมิติความลึกที่แท้จริง ส่งผลให้ระบบอนุมัติการเข้าถึงผิดพลาด ทำให้ผู้ไม่หวังดีเข้าถึงข้อมูลหรืออุปกรณ์ที่ได้รับการป้องกันได้

3. แนวทางเบื้องต้นในการป้องกันภัยคุกคามจาก Deepfake

ในการป้องกันภัยคุกคามจากการโจมตีด้วย Deepfake ผู้ให้บริการอาจเลือกพิจารณานำแนวทางดังนี้ไปประยุกต์ใช้ในระบบของตนเองได้

- **การใช้ Liveness Detection แบบสุ่ม**: เป็นการใช้เทคโนโลยี เช่น AI ในการทำหน้าที่ตรวจสอบว่าบุคคลที่ทำธุรกรรมหรือยืนยันตัวตนเป็นมนุษย์จริงที่มีชีวิตและอยู่ต่อหน้ากล้องในขณะนั้น (physically present) กลไกนี้ช่วยป้องกันการโจมตีแบบ Presentation Attack ที่ผู้ไม่หวังดีใช้สิ่งปลอมแปลง เช่น ภาพถ่าย วิดีโอที่บันทึกไว้ หน้ากากสามมิติ หรือวิดีโอ Deepfake ที่สมจริง เพื่อหลอกระบบจดจำใบหน้า โดยการใช้ Liveness Detectionสามารถแบ่งเป็น 3 ประเภท [1] ได้แก่
    - **Active Liveness:** เป็นวิธีที่ต้องการให้ผู้ใช้บริการแสดงท่าทางตอบสนองตามคำสั่งของระบบ เพื่อยืนยันว่ามีตัวตนจริงและมีชีวิตอยู่ในขณะนั้น เช่น การหันศีรษะไปทางซ้ายหรือขวา การกะพริบตาตามจังหวะ หรือการยิ้ม วิธีนี้มีความแม่นยำสูงเพราะยากต่อการปลอมแปลงด้วยภาพนิ่งหรือวิดีโอที่บันทึกไว้ (ทั้งนี้ การสั่งให้ผู้ใช้บริการแสดงท่าทางตอบสนองต่าง ๆ ต้องมีความหลากหลาย และมีมีลำดับการแสดงท่าทางที่ไม่ซ้ำกันในแต่ละครั้งที่ทำการยืนยันตัวตน) แต่ก็อาจทำให้ผู้ใช้รู้สึกยุ่งยากและใช้เวลามากขึ้นในการยืนยันตัวตน
    - **Semi-Active Liveness:** เป็นวิธีแบบผสมที่ต้องการการโต้ตอบจากผู้ใช้บริการน้อยกว่าวิธีแรก เช่น การขยับศีรษะเล็กน้อยหรือทำท่าทางง่าย ๆ โดยไม่ต้องทำตามคำสั่งที่ซับซ้อนมากนัก วิธีนี้ช่วยลดความยุ่งยากของผู้ใช้ แต่ยังคงมีความปลอดภัยในระดับที่เหมาะสม อย่างไรก็ตาม อาจยังมีช่องโหว่หากผู้ไม่หวังดีใช้วิดีโอ Deepfake ที่สามารถแสดงท่าทางการเคลื่อนไหวพื้นฐานบางอย่างได้
    - **Passive Liveness:** เป็นวิธีที่ไม่ต้องให้ผู้ใช้บริการทำอะไรเพิ่มเติม แต่ระบบจะทำการวิเคราะห์ภาพหรือวิดีโอในขณะที่ผู้ใช้บริการกำลังยืนยันตัวตนหน้ากล้อง โดยระบบจะใช้เทคนิคต่าง ๆ ในการตรวจสอบสัญญาณชีวมิติ เช่น การสะท้อนแสงบนผิวหน้า ความลึกของภาพ (3D depth) และการเคลื่อนไหวตามธรรมชาติของกล้ามเนื้อใบหน้า วิธีนี้สะดวกที่สุดสำหรับผู้ใช้บริการเพราะไม่ต้องทำตามคำสั่งใด ๆ แต่ต้องอาศัยเทคโนโลยีขั้นสูงและฮาร์ดแวร์ที่มีคุณภาพ เช่น กล้องที่รองรับการจับภาพสามมิติ เพื่อป้องกันการโจมตีด้วยภาพนิ่งคุณภาพสูงหรือวิดีโอ Deepfake ที่สมจริง
- **การใช้ข้อมูลชีวมิติร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์** โดยอ้างอิงจาก มธอ. 11 เล่ม 3-2566 การพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3: ข้อกำหนดของการยืนยันตัวตน [2] การใช้งานชีวมิติ (biometrics) เช่น ภาพใบหน้า ลายนิ้วมือ และลายม่านตา ในการยืนยันตัวตน ถือเป็นปัจจัยของการยืนยันตัวตนประเภทสิ่งที่คุณเป็น (something you are) ทั้งนี้สิ่งที่ใช้ยืนยันตัวตนที่สามารถรองรับ

การใช้งานชีวมิติสำหรับการยืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) ประกอบด้วย อุปกรณ์ OTP แบบหลายปัจจัย ซอฟต์แวร์เข้ารหัสลับแบบหลายปัจจัย และอุปกรณ์เข้ารหัสลับแบบหลายปัจจัย โดยผู้ให้บริการต้องลงทะเบียนข้อมูลชีวมิติของผู้ใช้บริการร่วมกับสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์ประเภทสิ่งที่คุณมี (something you have) เนื่องจากหากตรวจพบว่าผู้ใช้บริการเป็นตัวปลอมหรือสงสัยว่ามีการใช้งานในทางที่ผิดปกติ ผู้ให้บริการจะสามารถเพิกถอนสิ่งที่ใช้ยืนยันตัวตนที่เป็นอุปกรณ์นั้น และปฏิเสธการให้บริการได้

4. สรุป

การพัฒนาระบบ Digital ID เป็นกลไกสำคัญของเศรษฐกิจดิจิทัล โดยเฉพาะการใช้เทคโนโลยีจดจำใบหน้าเพื่อยืนยันตัวตนที่รวดเร็วและปลอดภัย อย่างไรก็ตาม ความก้าวหน้าของเทคโนโลยี Deepfake ซึ่งใช้ AI และโครงข่ายประสาทเทียมปฏิปักษ์ (GANs) สามารถสร้างภาพ วิดีโอ หรือเสียงปลอมที่สมจริงจนยากต่อการตรวจจับ ทำให้เกิดความเสี่ยงต่อระบบ Digital ID โดยเฉพาะเมื่อขาดการตรวจสอบความมีชีวิต (Liveness Detection) ภัยคุกคามที่พบได้บ่อย ได้แก่ การลงทะเบียนโดยสวมรอยบุคคลอื่น (Fraudulent Registration) การใช้ Deepfake เพื่อทำธุรกรรม (Transaction Spoofing) และการปลอมแปลงด้วยภาพนิ่งหรือหน้ากาก (Static Image/Mask Spoofing) ซึ่งอาจนำไปสู่การโจรกรรมข้อมูล การฉ้อโกงทางการเงิน และการทำลายความน่าเชื่อถือขององค์กร

แนวทางป้องกันที่สำคัญคือการใช้เทคโนโลยี Liveness Detection ซึ่งมีทั้งแบบ Active, Semi-Active และ Passive เพื่อยืนยันว่าผู้ใช้บริการเป็นบุคคลจริงในขณะทำธุรกรรม นอกจากนี้ ควรใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication) โดยผสานข้อมูลชีวมิติกับปัจจัยอื่น เช่น อุปกรณ์ OTP เพื่อเพิ่มความปลอดภัย การรับมือกับภัยคุกคามจาก Deepfake ต้องดำเนินการแบบบูรณาการ ทั้งด้านเทคโนโลยี มาตรการทางกฎหมาย และการสร้างความตระหนักรู้ในสังคม เพื่อป้องกันไม่ให้ Deepfake กลายเป็นช่องโหว่สำคัญของระบบ Digital ID ในอนาคต

อ้างอิง

[1] Paravision, "An Introduction to Liveness Detection for Digital Identity", Paravision, Jun. 01, 2023. [Online]. Available: https://www.paravision.ai/news/introduction-to-liveness-detection-for-digital-identity/. [Accessed: Jun. 7, 2025].

[2] “มาตรฐานธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยการพิสูจน์และยืนยันตัวตนทางดิจิทัล – เล่ม 3 ข้อกำหนดของการยืนยันตัวตน เลขที่ มธอ. 11 เล่ม 3-2566”, สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2023. Available: https://www.etda.or.th/getattachment/Regulator/DigitalID/law/ETCAnnounce-_15Sep66_Standard-DID_TS.pdf.aspx?lang=th-TH. [Accessed: Jun. 7, 2025].