ชื่อโครงการ
Adaptive Soft Identity Framework for Cybersecurity Risk Detection in Digital Financial Systems

1. ที่มาและปัญหา (Background and Problem Statement)

ในปัจจุบัน สังคมดิจิทัลมีการพึ่งพาระบบออนไลน์และธุรกรรมดิจิทัลเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะในภาคการเงินและบริการออนไลน์ เช่น Mobile Banking, E-Commerce และ Digital Services ต่างๆ ถึงแม้ระบบเหล่านี้จะช่วยเพิ่มความสะดวกสบายให้กับผู้ใช้งาน แต่ขณะเดียวกันก็เปิดโอกาสให้เกิดอาชญากรรมทางไซเบอร์ในรูปแบบที่ซับซ้อนและแนบเนียนมากขึ้น เช่น การหลอกลวงทางออนไลน์ (Scam), การทำ Social Engineering และการใช้ “บัญชีม้า” เป็นเครื่องมือในการกระทำผิด

ระบบยืนยันตัวตนที่ถูกใช้งานอยู่ในปัจจุบันส่วนใหญ่ยังคงอาศัย Hard Identity เป็นหลัก เช่น เลขบัตรประชาชน, ข้อมูลชีวมาตร(ม่านตา ใบหน้า ลายนิ้วมือ), รหัสผ่าน (Password), OTP หรือเอกสารแสดงตัวตนต่างๆ ซึ่งแม้จะมีความสำคัญในการยืนยันตัวบุคคลในเชิงกฎหมายและเชิงระบบ แต่ในทางปฏิบัติกลับพบว่ากลไกเหล่านี้ ไม่เพียงพอ ต่อการรับมือกับภัยคุกคามรูปแบบใหม่

ปัญหาสำคัญของ Hard Identity คือ เมื่ออาชญากรสามารถเข้าถึงหรือครอบครองข้อมูลยืนยันตัวตนเหล่านี้ได้ ไม่ว่าจะผ่านการหลอกลวง การขโมยข้อมูล หรือการใช้ช่องโหว่ทางสังคม (Social Engineering) ระบบจะไม่สามารถแยกแยะได้ว่า ผู้ที่กำลังใช้งานระบบอยู่นั้น เป็นเจ้าของบัญชีตัวจริง หรือเป็นผู้ไม่หวังดีที่ถือครองข้อมูลถูกต้องครบถ้วน เนื่องจากในมุมมองของระบบ Hard Identity เหล่านั้นยังคงถูกต้องสมบูรณ์

ตัวอย่างเช่น กรณีบัญชีม้า เจ้าของบัญชีอาจเป็นผู้เปิดบัญชีด้วยตนเอง มีเอกสารยืนยันตัวตนครบถ้วน และผ่านกระบวนการยืนยันตัวตนตามกฎหมายทุกประการ แต่ภายหลังบัญชีนั้นกลับถูกนำไปใช้ในลักษณะที่ผิดปกติหรือเกี่ยวข้องกับอาชญากรรมทางการเงิน ระบบที่พึ่งพา Hard Identity เพียงอย่างเดียวจะไม่สามารถตรวจจับความเสี่ยงในลักษณะนี้ได้อย่างมีประสิทธิภาพ เพราะไม่สามารถสะท้อน “วิธีการใช้งานจริง” ของบัญชีในเชิงพฤติกรรมได้

นอกจากนี้ รูปแบบการหลอกลวงในปัจจุบันไม่ได้อาศัยเพียงช่องโหว่ทางเทคนิค แต่ใช้การโน้มน้าวทางจิตวิทยาและพฤติกรรมมนุษย์เป็นหลัก ผู้ใช้งานจำนวนมากถูกหลอกให้เป็นผู้ดำเนินการธุรกรรมด้วยตนเอง ทั้งการโอนเงิน การยืนยันตัวตน หรือการให้ข้อมูลสำคัญ โดยที่ระบบมองว่าธุรกรรมนั้นถูกต้องตามขั้นตอนทุกประการ ส่งผลให้การป้องกันในระดับ Hard Identity ไม่สามารถตอบโจทย์ภัยคุกคามรูปแบบนี้ได้

จากปัญหาดังกล่าว จะเห็นได้ว่าระบบความปลอดภัยดิจิทัลในปัจจุบันยังขาดความสามารถในการเข้าใจพฤติกรรมของผู้ใช้งาน และไม่สามารถแยกแยะความแตกต่างระหว่างการใช้งานที่เป็นปกติกับการใช้งานที่มีความเสี่ยงได้อย่างลึกซึ้ง แม้ว่าข้อมูลยืนยันตัวตนในเชิง Hard Identity จะถูกต้องครบถ้วนก็ตาม นี่จึงเป็นช่องว่างสำคัญที่เปิดโอกาสให้เกิดอาชญากรรมทางไซเบอร์ในรูปแบบใหม่ และเป็นที่มาของความจำเป็นในการมองหากลไกการยืนยันและประเมินความเสี่ยงที่ก้าวไปไกลกว่า Hard Identity แบบเดิม

2. แนวคิดของโครงการ (Concept Overview)

โครงการนี้นำเสนอแนวคิดของ Soft Identity หรือ อัตลักษณ์เชิงพฤติกรรม ซึ่งเป็นตัวตนของผู้ใช้งานที่เกิดจากการสะสมของพฤติกรรมในหลายมิติอย่างต่อเนื่อง เช่น รูปแบบการพิมพ์ (Typing Patterns), การสัมผัสหน้าจอ (Touch Dynamics), การใช้งานอุปกรณ์เดิม, ช่วงเวลาการใช้งาน, สถานที่, ความถี่และระยะเวลาการใช้งาน รวมถึงลำดับและรูปแบบของการกระทำต่างๆ

แนวคิดหลักคือ พฤติกรรมของมนุษย์มีลักษณะเฉพาะตัวและมีความสม่ำเสมอในระยะยาว แม้พฤติกรรมเพียงมิติเดียวจะไม่เพียงพอในการระบุตัวบุคคลได้อย่างชัดเจน แต่เมื่อพฤติกรรมหลายมิติถูกนำมาประกอบกัน จะเกิดเป็นรูปแบบเฉพาะที่สะท้อนตัวตนของผู้ใช้งานแต่ละราย ซึ่งเรียกว่า Soft Identity

Soft Identity แตกต่างจาก Hard Identity ตรงที่ไม่ใช่ข้อมูลที่ผู้ใช้งาน “มี และจับต้องได้ชัดเจน” แต่เป็นข้อมูลที่เกิดจาก “การกระทำ” และมีลักษณะยืดหยุ่น เปลี่ยนแปลงได้ตามบริบท แต่ในขณะเดียวกันก็มีความยากต่อการปลอมแปลงหรือเลียนแบบอย่างสมบูรณ์

3. หลักการทำงานของระบบ (Methodology)

ระบบจะใช้เทคนิค Machine Learning / AI ในการเรียนรู้พฤติกรรมของผู้ใช้งานในหลายมิติ เพื่อสร้าง Baseline Soft Identity ซึ่งหมายถึง รูปแบบพฤติกรรมปกติของผู้ใช้งานแต่ละราย ที่เกิดจากการสะสมข้อมูลการใช้งานในช่วงเวลาหนึ่ง โดย Baseline Soft Identity ไม่ได้เป็นค่าคงที่ แต่เป็นแบบจำลองเชิงพฤติกรรมที่สามารถปรับตัวได้อย่างมีเงื่อนไข โดยการอัปเดตจะเกิดขึ้นภายใต้กลไกการควบคุมความเสี่ยง เพื่อป้องกันการเปลี่ยนแปลงของ Baseline จากพฤติกรรมที่มีความผิดปกติหรือมีความเสี่ยงสูง

Baseline Soft Identity ประกอบด้วยลักษณะพฤติกรรมในหลายด้าน เช่น รูปแบบการโต้ตอบกับอุปกรณ์และแอปพลิเคชัน ช่วงเวลาและความถี่ในการใช้งาน ลำดับของการกระทำ ลักษณะการทำธุรกรรม และบริบทการใช้งานต่าง ๆ ซึ่งเมื่อนำพฤติกรรมหลายมิติมาประกอบกัน จะสะท้อนตัวตนเชิงพฤติกรรมของผู้ใช้งานแต่ละรายได้

เมื่อมีการใช้งานระบบหรือเกิดธุรกรรมใหม่ AI จะทำการเปรียบเทียบพฤติกรรมที่เกิดขึ้นกับ Baseline Soft Identity ที่ได้เรียนรู้ไว้ เพื่อประเมินระดับความเบี่ยงเบน (Deviation) ของพฤติกรรม หากตรวจพบว่าพฤติกรรมมีความแตกต่างจากรูปแบบปกติในระดับที่ผิดปกติหรือไม่สอดคล้องกับบริบทเดิม ระบบจะทำการประเมินความเสี่ยงและแปลงผลลัพธ์เป็นระดับความเสี่ยง (Risk Score)

Risk Score ดังกล่าวจะถูกใช้เป็นข้อมูลประกอบการตัดสินใจทั้งในฝั่งผู้ใช้งานและฝั่งสถาบันการเงิน เช่น การแจ้งเตือนเชิงป้องกัน การเพิ่มระดับการยืนยันตัวตน หรือการเฝ้าระวังเพิ่มเติม โดย AI จะทำหน้าที่เป็น ระบบสนับสนุนการตัดสินใจ (Decision Support System) ไม่ใช่การตัดสินใจแทนมนุษย์โดยสมบูรณ์ เพื่อรักษาสมดุลระหว่างความปลอดภัย ความโปร่งใส และประสบการณ์ผู้ใช้งาน

4. ตัวอย่างการประยุกต์ใช้งาน (Use Cases)

4.1 การป้องกันการหลอกลวง (Scam & Social Engineering)

ระบบ Soft Identity ไม่ได้มุ่งเน้นเพียงการตรวจจับการเข้าถึงที่ผิดปกติ แต่ให้ความสำคัญกับ การเปลี่ยนแปลงของพฤติกรรมเชิงการตัดสินใจ (Decision Behavior) ของผู้ใช้งาน ซึ่งมักเป็นจุดอ่อนสำคัญในกรณีการหลอกลวงแบบ Social Engineering

AI จะเรียนรู้รูปแบบพฤติกรรมปกติของผู้ใช้งาน เช่น ความเร็วและลำดับการทำธุรกรรม ความถี่ในการโอนเงิน รูปแบบการโต้ตอบกับแอปพลิเคชัน (Touch Dynamics, Typing Patterns) ช่วงเวลาและบริบทของการใช้งาน รวมถึงรูปแบบการตัดสินใจในสถานการณ์ต่างๆ เมื่อเกิดพฤติกรรมที่เบี่ยงเบนจากรูปแบบเดิมอย่างมีนัยสำคัญ เช่น การตัดสินใจโอนเงินในเวลาที่ไม่ปกติ การดำเนินการที่เร่งรีบผิดจากพฤติกรรมเดิม หรือการทำธุรกรรมที่มีลักษณะต่างจากนิสัยปกติของผู้ใช้งาน ระบบจะประเมินความเสี่ยงและทำการแจ้งเตือนเชิงป้องกันแบบ Real-time

การแจ้งเตือนดังกล่าวไม่ได้มีวัตถุประสงค์เพื่อยับยั้งการใช้งาน แต่ถูกออกแบบให้ทำหน้าที่เป็น Cognitive Friction เพื่อกระตุ้นให้ผู้ใช้งานหยุดทบทวนการตัดสินใจของตนเองในช่วงเวลาที่มีความเสี่ยง โดยจะแสดงข้อความเตือนในลักษณะ Chat Head หรือ In-app Notification เช่น การแจ้งว่ารูปแบบการตัดสินใจในขณะนั้นแตกต่างจากพฤติกรรมปกติ และอาจมีความเสี่ยงจากการถูกหลอกลวง

นอกจากนี้ ระบบยังมี AI Chatbot ทำหน้าที่เป็นเครื่องมือสนับสนุนผู้ใช้งาน โดยผู้ใช้งานสามารถส่งข้อมูลเพิ่มเติมให้ระบบช่วยตรวจสอบได้ เช่น หมายเลขโทรศัพท์ ลิงก์ ข้อความสนทนา หรือบริบทของเหตุการณ์ที่กำลังเผชิญอยู่ AI จะช่วยวิเคราะห์ข้อมูลเหล่านี้ร่วมกับบริบทเชิงพฤติกรรม เพื่อให้ข้อมูล ความรู้ และคำแนะนำที่ถูกต้องแก่ผู้ใช้งาน ลดความตื่นตระหนก และเพิ่มความมั่นใจในการตัดสินใจอย่างมีเหตุผล ซึ่งถือเป็นการผสานบทบาทของ AI ในเชิงป้องกันและการให้ความรู้ไปพร้อมกัน

1
4.2 การตรวจจับบัญชีม้า

4.2.1 กรณีบัญชีที่มี Soft Identity เดิม

สำหรับบัญชีที่ระบบมีข้อมูล Soft Identity ของเจ้าของบัญชีเดิมอยู่แล้ว AI จะใช้ข้อมูลพฤติกรรมในอดีตเพื่อสร้าง Baseline ของการใช้งาน เช่น อุปกรณ์ที่ใช้เป็นประจำ ช่วงเวลาการทำธุรกรรม ความถี่และจำนวนครั้งในการโอนเงินต่อวัน ลักษณะการโต้ตอบกับระบบ ตำแหน่งที่ตั้ง หรือรูปแบบเครือข่ายที่เกี่ยวข้องกับบัญชีนั้น

เมื่อบัญชีถูกนำไปใช้งานในลักษณะที่แตกต่างจาก Baseline อย่างมีนัยสำคัญ เช่น การเปลี่ยนอุปกรณ์อย่างกะทันหัน การโอนเงินถี่ผิดปกติ การใช้งานในช่วงเวลาที่ไม่สอดคล้องกับพฤติกรรมเดิม หรือการเชื่อมโยงกับอุปกรณ์และ IP Address ที่มีความเสี่ยง ระบบจะประเมินความผิดปกติในเชิงพฤติกรรม ถ้าพบความผิดปกติระบบจะติด Tag ให้บัญชีนั้นๆว่ามีความเสี่ยงที่จะเป็นบัญชีม้า พร้อมทั้งแปลงเป็นระดับความเสี่ยง (Risk Score) ที่ระบุความเสี่ยงเป็นช่วง 0% - 100%

ผลการประเมินดังกล่าวจะถูกใช้เพื่อเพิ่มระดับการยืนยันตัวตนในขั้นตอนการทำธุรกรรม เช่น การร้องขอการยืนยันเพิ่มเติม และจะแจ้งเตือนไปยังสถาบันการเงินเพื่อให้สามารถติดตาม เฝ้าระวัง และตัดสินใจดำเนินการที่เหมาะสมได้มากขึ้น โดยไม่จำเป็นต้องบล็อกบัญชีทันทีโดยอัตโนมัติ

4.2.2 กรณีบัญชีใหม่ที่ไม่มี Soft Identity

ในกรณีบัญชีใหม่ที่ยังไม่มีข้อมูล Soft Identity เพียงพอ ระบบจะใช้แนวทางการเรียนรู้เชิงพฤติกรรมจากบัญชีม้าและเครือข่ายอาชญากรรมในอดีต โดย AI จะวิเคราะห์รูปแบบการใช้งานที่มีลักษณะร่วมกัน เช่น รูปแบบการโอนเงินที่ซ้ำกันหลายบัญชี การใช้อุปกรณ์หรือ IP Address ร่วมกับบัญชีที่มีความเสี่ยง การเคลื่อนไหวของเงินในลักษณะเดียวกัน และความสัมพันธ์เชิงพฤติกรรมระหว่างหลายบัญชีในระดับเครือข่าย (Behavioral Network)

แทนที่จะพิจารณาบัญชีใหม่แบบแยกส่วน ระบบจะมองพฤติกรรมในเชิงกลุ่มและความเชื่อมโยงระหว่างบัญชีเพื่อประเมินแนวโน้มความเสี่ยงว่าอาจเป็นส่วนหนึ่งของเครือข่ายบัญชีม้าในอนาคตหรือไม่ หากตรวจพบรูปแบบที่มีความคล้ายคลึงกับเครือข่ายที่มีความเสี่ยง ระบบจะทำการแจ้งเตือนไปยังสถาบันการเงินเพื่อให้สามารถติดตามและเฝ้าระวังบัญชีนั้นอย่างต่อเนื่องระยะเริ่มต้น

5. ประเด็นด้านกฎหมาย จริยธรรม และประสบการณ์ผู้ใช้งาน

โครงการนี้ตระหนักถึงความละเอียดอ่อนของข้อมูลพฤติกรรม ซึ่งเกี่ยวข้องโดยตรงกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) และประสบการณ์ผู้ใช้งาน ระบบจึงต้องถูกออกแบบภายใต้แนวคิด User-Centered Design (UCD) โดยให้ความสำคัญกับความโปร่งใส ความใช้งานง่าย ความเข้าใจของผู้ใช้งาน ความปลอดภัยต่อผู้ใช้ และการใช้ AI ในลักษณะสนับสนุน ไม่ใช่ควบคุมหรือรุกล้ำสิทธิ์ของผู้ใช้งาน

6. บทสรุป (Conclusion)

แนวคิด Soft Identity เป็นแนวทางใหม่ในการเสริมความมั่นคงปลอดภัยของระบบดิจิทัล โดยทำหน้าที่เติมเต็มช่องว่างของระบบที่พึ่งพา Hard Identity เพียงอย่างเดียว ผ่านการทำความเข้าใจพฤติกรรมจริงของผู้ใช้งานในหลายมิติอย่างต่อเนื่อง ซึ่งช่วยให้ระบบสามารถตรวจจับความผิดปกติที่ไม่สามารถมองเห็นได้จากข้อมูลยืนยันตัวตนแบบดั้งเดิม แนวคิดนี้สามารถนำไปประยุกต์ใช้ในการป้องกันการหลอกลวง การตรวจจับบัญชีม้า และการลดความเสี่ยงของธุรกรรมดิจิทัลได้อย่างมีประสิทธิภาพ

อย่างไรก็ตาม การนำ Soft Identity ไปใช้งานจริงจำเป็นต้องพิจารณาอย่างรอบด้าน ทั้งในมิติทางเทคนิค กฎหมาย และประสบการณ์ผู้ใช้งาน ระบบต้องถูกออกแบบให้สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) มีความโปร่งใส และเคารพสิทธิของผู้ใช้งาน โดยใช้ AI ในลักษณะของระบบสนับสนุนการตัดสินใจ ไม่ใช่การตัดสินแทนมนุษย์โดยสมบูรณ์

ในด้านเทคนิค การพัฒนา Soft Identity จำเป็นต้องอาศัยการเรียนรู้และปรับปรุงโมเดล Machine Learning / AI อย่างต่อเนื่อง ทั้งในแง่ของเทคนิคการฝึกโมเดล การเลือกคุณลักษณะเชิงพฤติกรรม (Behavioral Features) และการจัดการกับบริบทที่เปลี่ยนแปลงตลอดเวลา นอกจากนี้ รูปแบบอาชญากรรมและพฤติกรรมของผู้ไม่หวังดียังมีการพัฒนาอย่างไม่หยุดนิ่ง ทำให้ระบบต้องสามารถเรียนรู้รูปแบบ (Patterns) และแนวทางการแก้ปัญหา (Solutions) ใหม่ๆอยู่เสมอ เพื่อรักษาความแม่นยำในการตรวจจับ

ในอนาคตแนวคิด Soft Identity ยังสามารถต่อยอดด้วยการบูรณาการองค์ความรู้จากศาสตร์อื่นๆ เช่น พฤติกรรมศาสตร์ จิตวิทยาการตัดสินใจ เครือข่ายสังคม และการวิเคราะห์เชิงระบบ เพื่อเพิ่มมิติของข้อมูลและตัวแปรที่ใช้ในการประเมินความเสี่ยง ซึ่งจะช่วยให้ Algorithm ของ Soft Identity มีความแม่นยำและความยืดหยุ่นสูงขึ้น พร้อมรองรับภัยคุกคามทางไซเบอร์ที่ซับซ้อนมากขึ้นในอนาคต