

การยกระดับการตรวจจับทุจริตทางการเงิน ด้วยปัญญาประดิษฐ์

Powering Financial Fraud Detection with Artificial Intelligence

ไพลิน ตระมณีรัตน์*

รองศาสตราจารย์ประจำภาควิชาการบัญชี
คณะพาณิชยศาสตร์และการบัญชี
มหาวิทยาลัยธรรมศาสตร์
Email: pailin@tbs.tu.ac.th
*ผู้ประพันธ์บรรณกิจ

นงนภัส เขียวขำ

นักศึกษาปริญญาตรี คณะพาณิชยศาสตร์และ
การบัญชี มหาวิทยาลัยธรรมศาสตร์
Email: nongnapat_kea64@tbs.tu.ac.th

ธัญชนก เรืองเดช

นักศึกษาปริญญาตรี คณะพาณิชยศาสตร์และ
การบัญชี มหาวิทยาลัยธรรมศาสตร์
Email: thanchanok_rua64@tbs.tu.ac.th

Pailin Trongmateerut*, Ph.D.

Associate Professor of Accounting
Faculty of Commerce and Accountancy
Thammasat University
Email: pailin@tbs.tu.ac.th
*Corresponding author

Nongnapat Keawkham

Undergraduate Student
Faculty of Commerce and Accountancy
Thammasat University
Email: nongnapat_kea64@tbs.tu.ac.th

Thanchanok Ruangdech

Undergraduate Student
Faculty of Commerce and Accountancy
Thammasat University
Email: thanchanok_rua64@tbs.tu.ac.th

การยกระดับการตรวจจับทุจริตทางการเงินด้วยปัญญาประดิษฐ์

ไพลิน ตรงเมธีรัตน์*

รองศาสตราจารย์ประจำภาควิชาการบัญชี

คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

Email: pailin@tbs.tu.ac.th

*ผู้ประพันธ์บรรณกิจ

นงนภัส เขียวขำ

นักศึกษาปริญญาตรี คณะพาณิชยศาสตร์และ

การบัญชี มหาวิทยาลัยธรรมศาสตร์

Email: nongnapat_kea64@tbs.tu.ac.th

ธัญชนก เรืองเดช

นักศึกษาปริญญาตรี คณะพาณิชยศาสตร์และ

การบัญชี มหาวิทยาลัยธรรมศาสตร์

Email: thanchanok_rua64@tbs.tu.ac.th

วันที่ได้รับบทความต้นฉบับ: 24 มกราคม 2568

วันที่แก้ไขปรับปรุงบทความ: 10 มีนาคม 2568

วันที่ตอบรับตีพิมพ์บทความ: 31 มีนาคม 2568

บทคัดย่อ

ปัญญาประดิษฐ์และเทคโนโลยีอย่าง Machine Learning, Behavioral Analytics และ Natural Language Processing ช่วยยกระดับการตรวจจับการทุจริตทางการเงินซึ่งเป็นงานสำคัญหนึ่งของการบัญชีนิติวิทยา การตรวจจับการทุจริตที่มีประสิทธิภาพในการตรวจข้อมูลทางการเงินที่มีจำนวนเพิ่มขึ้นมหาศาลจะช่วยลดความเสียหายและป้องปรามการกระทำการทุจริตในอนาคต บทความนี้อภิปรายถึงความท้าทายและความเสี่ยงที่เกิดขึ้น รวมทั้งผลที่ไม่พึงประสงค์ในการพัฒนาและใช้งานปัญญาประดิษฐ์ที่ควรได้รับการบริหารจัดการ ได้แก่ คุณภาพและความสมบูรณ์ของข้อมูล ความสามารถในการชี้แจงได้ ความเป็นส่วนตัวและการปฏิบัติตามกฎหมาย การต่อต้านการเปลี่ยนแปลง ค่าใช้จ่ายและทรัพยากร และการพึ่งพาเทคโนโลยีมากเกินไป ผู้ประกอบวิชาชีพสามารถพิจารณาประยุกต์ใช้กฎหมายที่เกี่ยวข้องและกรอบการบริหารความเสี่ยงปัญญาประดิษฐ์กับการใช้ปัญญาประดิษฐ์ซึ่งเป็นเครื่องมือในการตรวจจับการทุจริตได้

คำสำคัญ: การบัญชีนิติวิทยา ปัญญาประดิษฐ์ การตรวจจับการทุจริต

Powering Financial Fraud Detection with Artificial Intelligence

Pailin Trongmateerut*, Ph.D.

Associate Professor of Accounting

Faculty of Commerce and Accountancy

Thammasat University

Email: pailin@tbs.tu.ac.th

*Corresponding author

Nongnapat Keawkham

Undergraduate Student

Faculty of Commerce and Accountancy

Thammasat University

Email: nongnapat_kea64@tbs.tu.ac.th

Thanchanok Ruangdech

Undergraduate Student

Faculty of Commerce and Accountancy

Thammasat University

Email: thanchanok_rua64@tbs.tu.ac.th

Received: January 24, 2025

Revised: March 10, 2025

Accepted: March 31, 2025

ABSTRACT

Artificial intelligence and techniques such as Machine Learning, Behavioral Analytics, and Natural Language Processing, can power the financial fraud detection, which is a critical task in forensic accounting. Effective fraud detection amid a massive increase in financial data can help reduce damage and deter future fraudulent activities. This article discusses the challenges and risks involved, as well as the unintended consequences of developing and implementing artificial intelligence that need to be managed, including data quality and integrity, interpretability, privacy and compliance, resistance to change, costs and resources, and technology over-reliance. Accounting professionals should consider applying laws and risk management frameworks for artificial intelligence as a tool for fraud detection.

Key word: Artificial Intelligence, Forensic accounting, Fraud detection

■ บทนำ

อุบัติการณ์การทุจริตทางการเงินสร้างความเสียหายอย่างร้ายแรงต่อเศรษฐกิจและองค์กรทั่วโลกหลากหลายรูปแบบ ทั้งยังเพิ่มขึ้นอย่างต่อเนื่อง กรณีตัวอย่างมากมายที่แสดงให้เห็นถึงการฉ้อโกงที่ซับซ้อนและยากต่อการตรวจจับ อันเนื่องมาจากความตั้งใจที่จะฉ้อโกง ปิดบังหลักฐานในการกระทำทุจริตที่ซับซ้อนของเหล่าผู้นำในองค์กร บางกิจการสร้างรายการทางการเงินเท็จเพื่อแสดงผลการดำเนินงานและการเติบโตที่ดีเกินจริง ทำให้นักลงทุนหลงเชื่อและนำเงินมาลงทุนในกิจการทั้งในรูปแบบตราสารทุนและตราสารหนี้ เช่น เผยแพร่ข้อความอันเป็นเท็จหรือข้อความอันอาจก่อให้เกิดความสำคัญผิดในสาระสำคัญเกี่ยวกับฐานะทางการเงินและผลการดำเนินงานของ STARK (The Securities and Exchange Commission [SEC], 2024) กรณีกระทำผิดหน้าที่โดยทุจริต เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายของ TSF (SEC, 2024) แต่ละกรณีนั้นสร้างความเสียหายเป็นมูลค่าสูงแก่สาธารณชนเป็นจำนวนมาก

การบัญชีนิติวิทยา (forensic accounting) เป็นวิชาชีพที่ตรวจสอบข้อมูลทางการเงินในการพิสูจน์ หรือรวบรวมหลักฐานประกอบข้อเท็จจริงเกี่ยวกับอาชญากรรมทางการเงินหรือเรื่องเฉพาะที่ได้รับมอบหมาย (Supphatada, 2020) วิชาชีพนี้ต้องอาศัยความรู้ด้านการบัญชีการเงิน การตรวจสอบ และความสามารถด้านการสืบสวนสอบสวนประกอบกัน เพื่อตรวจสอบการเงินของหน่วยธุรกิจหรือบุคคลธรรมดา สอบหาข้อเท็จจริงและหลักฐานที่องค์กรได้บิดเบือนข้อมูลในการทำงานการเงิน เพื่อพิสูจน์หรือรวบรวมหลักฐานประกอบข้อเท็จจริงที่เป็นประโยชน์ต่อกระบวนการยุติธรรม (Supphatada, 2020)

นักบัญชีนิติวิทยาจึงต้องมีความรู้และทักษะสำคัญ ได้แก่ การทุจริต การสืบสวน กฎหมาย กฎเกณฑ์ด้านพยานหลักฐาน ธุรกิจ การสื่อสาร และเทคโนโลยีสารสนเทศ (Srijunpetch, 2010; Supphatada, 2020) ความรู้และทักษะด้านเทคโนโลยีสารสนเทศมีความจำเป็นอย่างยิ่งในยุคดิจิทัลที่ทุกองค์กรดำเนินงานบนโครงสร้างพื้นฐานระบบสารสนเทศ การทำงานแบบไร้รอยต่อที่อาศัยเครือข่ายอินเทอร์เน็ต การทำธุรกรรมทางการเงินแบบเรียลไทม์ผ่านช่องทางอิเล็กทรอนิกส์และอุปกรณ์พกพาอย่างสมาร์ทโฟน ความก้าวหน้าทางเทคโนโลยีสารสนเทศเหล่านี้ ทำให้การดำเนินงานสะดวกสบาย ใช้ระยะเวลาเพียงเสี้ยววินาทีในการทำธุรกรรมการเงิน ต้นทุนการทำธุรกรรมลดลง แต่ก็ทำให้มีความเสี่ยงการฉ้อโกงรูปแบบใหม่ ๆ ที่แยบยลมากขึ้น การทำงานของนักบัญชีนิติวิทยาจึงต้องก้าวล่วงหน้าก่อนความเสี่ยงเหล่านั้นและสามารถใช้ประโยชน์จากเทคโนโลยีสารสนเทศที่พัฒนาอย่างก้าวกระโดดได้อย่างวิทียาการวิเคราะห์ข้อมูล (data analytics) และปัญญาประดิษฐ์ (Artificial Intelligence: AI)

การตรวจจับทุจริต (fraud detection) เป็นส่วนหนึ่งของการบัญชีนิติวิทยา (Supphatada, 2020) ที่ได้ มีการนำ AI มาประยุกต์ใช้ในการตรวจสอบเชิงรุก เนื่องจาก AI สามารถช่วยระบุและตรวจสอบพฤติกรรมที่ผิดปกติจากข้อมูลทางการเงินได้อย่างมีประสิทธิภาพ โดยใช้เทคนิคต่าง ๆ เช่น Machine Learning เพื่อวิเคราะห์พฤติกรรมของธุรกรรมและระบุความผิดปกติที่อาจเกี่ยวข้องกับการฉ้อโกง นอกจากนี้ AI ยังสามารถเรียนรู้และปรับปรุงการตรวจจับจากข้อมูลที่มีการเปลี่ยนแปลงได้อย่างต่อเนื่อง ซึ่งทำให้การตรวจจับการทุจริตมีความแม่นยำและทันสมัยมากขึ้น AI ไม่เพียงแต่ช่วยเพิ่มความแม่นยำในการตรวจจับการทุจริต แต่ยังช่วยในการประหยัดเวลาและทรัพยากรในการตรวจสอบ โดยสามารถประมวลผลข้อมูลจำนวนมากได้อย่างรวดเร็วและลดภาระงานที่ซ้ำซ้อนในการวิเคราะห์ข้อมูล การลดต้นทุนในการตรวจสอบและการเสริมสร้างความเชื่อมั่นในระบบการเงิน

บทความนี้อธิบายการประยุกต์ใช้เทคโนโลยี AI กับงานการบัญชีนิติวิทยาโดยเฉพาะอย่างยิ่งการตรวจจับการทุจริต ตัวอย่างการประยุกต์ใช้ ความท้าทายและความเสี่ยงจากการใช้ AI และผู้ประกอบวิชาชีพกับการใช้งาน AI

■ การบัญชีนิติวิทยา

การบัญชีนิติวิทยามักกล่าวถึงว่าเป็นการสืบสวนสอบสวนการทุจริต รวมถึงการตรวจสอบรายการทางการเงิน การพิสูจน์หรือพิสูจน์หักล้างข้อสงสัยการทุจริตทางการเงิน กระบวนการสัมภาษณ์ทุกฝ่ายที่เกี่ยวข้องกับการทุจริต การเป็นพยานผู้เชี่ยวชาญในศาล (Singleton et al., 2006; Supphatada, 2020) นักบัญชีนิติวิทยามักเข้าไปปฏิบัติงานเพื่อตอบสนองต่อข้อร้องเรียนเกี่ยวกับเหตุอาชญากรรมทางการเงิน ข้อกล่าวหาหรือ ข้อสอบถามในการสอบสวนระดับกิจการ นักบัญชีนิติวิทยาต้องเข้าถึงแหล่งทรัพยากรหลากหลายแหล่งเพื่อค้นหา รวบรวมหลักฐาน พยานทางการเงิน ติความ และนำเสนอพยานหลักฐานเหล่านั้นเพื่อสนับสนุนให้กระบวนการสืบสวนข้อเท็จจริงแก้ไขข้อร้องเรียนให้เสร็จสิ้น (resolve the complaint) ได้อย่างรวดเร็วและมีประสิทธิภาพ (Singleton et al., 2006)

การปฏิบัติงานการบัญชีนิติวิทยาแบ่งเป็น 4 ขั้นตอน ได้แก่ การรับรู้ปัญหา การรวบรวมหลักฐาน การประเมินหลักฐาน และการสรุปผลเพื่อรายงาน (Srijunpetch, 2010) บทบาทสำคัญของการบัญชีนิติวิทยา คือ การวิเคราะห์รายการทางการเงินอย่างละเอียด เพื่อระบุความผิดปกติที่อาจบ่งชี้ถึงการกระทำผิด เช่น การตรวจจับทุจริต เนื่องด้วยจากการที่ต้องมีหลักฐาน และข้อมูลที่ผ่านการตรวจสอบและวิเคราะห์ที่ชี้แจงแน่ชัดเพื่อยืนยันว่า มีกระทำการทุจริตจริง ๆ ไม่เป็นเพียงแค่คำกล่าวหา จึงจะสามารถดำเนินคดีหรือตรวจสอบผู้กระทำความผิดในชั้นศาลได้ นักบัญชีนิติวิทยาจึงจำเป็นต้องมีทักษะความรู้มากกว่านักบัญชีทั่วไปทั้งในด้านกฎหมาย ด้านอาชญาวิทยา และยังต้องมีทักษะและความคิดสร้างสรรค์ในการสงสัยเยี่ยงผู้ประกอบวิชาชีพมากกว่าผู้สอบบัญชีทั่วไป นอกจากนี้ นักบัญชีนิติวิทยายังมีหน้าที่จัดเตรียมหลักฐานสำหรับกระบวนการทางกฎหมาย รวมถึงการให้ข้อมูลในฐานะพยานผู้เชี่ยวชาญในชั้นศาล งานนี้มีความสำคัญต่อการตรวจจับการบิดเบือนข้อมูลและช่วยสร้างความน่าเชื่อถือให้กับองค์กร

นักบัญชีนิติวิทยายังมีบทบาทในระบบการบริหารความเสี่ยงจากการทุจริตที่มีองค์ประกอบ ได้แก่ การป้องกัน การทุจริต การตรวจจับทุจริต การสืบสวนทุจริต และการติดตามผล (Supphatada, 2020) การป้องกันการทุจริตเป็นการบริหารความเสี่ยงที่มีประสิทธิผลสูงสุด แม้กิจการได้ติดตั้งการควบคุมเชิงป้องกันที่มีประสิทธิผลก็ตาม กิจการต้องบริหารความเสี่ยงด้วยกลไกการตรวจจับการทุจริตที่มีประสิทธิภาพประสิทธิผล เพื่อตรวจจับระบุการกระทำทุจริตได้ทันเวลา และจัดการระงับปัญหาการทุจริต

■ การตรวจจับการทุจริตด้วยปัญญาประดิษฐ์

การตรวจจับการทุจริต คือ กระบวนการที่เป็นระบบในการระบุความผิดปกติ การกระทำหรือกิจกรรมที่น่าสงสัย ซึ่งบ่งชี้ว่ามีการกระทำผิดอาชญากรรม การฉ้อโกง ข้อมูล หรือทรัพยากรต่าง ๆ กำลังเกิดการตรวจจับการทุจริตมีเป้าหมายเพื่อปกป้องทรัพย์สินและทรัพยากร วิธีการตรวจจับการทุจริตได้นั้นอาจเป็นการพบโดยบังเอิญ การได้รับแจ้งเบาะแส (Supphatada, 2007) และการวิเคราะห์เปรียบเทียบ (Supphatada, 2020)

เทคนิคการวิเคราะห์ที่ใช้เพื่อการตรวจจบบรรายการผิดปกติในรายการทางการเงิน ได้แก่ การวิเคราะห์อัตราส่วนทางการเงิน การตรวจสอบติดตามรายการ การสัมภาษณ์ (International Association of Independent Accounting Firms, 2024) ซึ่งมักใช้การสุ่มตัวอย่างจากรายการทั้งหมดโดยกำหนดค่าความ น่าจะเป็นในระดับที่เชื่อถือได้ เทคนิคเหล่านี้ให้ผลที่ดีในบางกรณี แต่ก็มีข้อจำกัดอย่างชัดเจนเมื่อองค์กรต้องเผชิญกับข้อมูลที่มีปริมาณมากและความซับซ้อนของธุรกรรม AI ได้กลายเป็นเครื่องมือสำคัญที่ช่วยให้นักบัญชีนิติวิทยาสามารถตรวจจับความผิดปกติได้อย่างมีประสิทธิภาพและถูกต้องแม่นยำมากขึ้น ทั้งช่วยลดเวลา ลดค่าใช้จ่าย ในการตรวจสอบความผิดปกติในงบการเงิน ทำให้ผู้ตรวจสอบสามารถที่จะพุ่งความสนใจหรือตั้งเป้าหมายที่จะตรวจสอบและวิเคราะห์ข้อมูลที่ผิดปกติได้อย่างตรงจุด

คุณลักษณะเด่นของ AI ในการตรวจจับทุจริต คือ การวิเคราะห์ข้อมูลเชิงลึก และการตรวจจับความผิดปกติ ซึ่งเป็นกระบวนการที่ AI ใช้ในการค้นหาธุรกรรมที่ไม่สอดคล้องกับรูปแบบปกติในระบบ เช่น การโอนเงินในช่วงเวลาที่ผิดปกติ หรือธุรกรรมที่มีลักษณะเชื่อมโยงกับบัญชีที่น่าสงสัย เทคโนโลยีนี้ช่วยให้องค์กรสามารถระบุและตอบสนองต่อภัยการฉ้อโกงได้ในเวลาอันรวดเร็ว นอกจากนี้ AI ที่มีความสามารถในการวิเคราะห์ข้อมูลธุรกรรมแบบทันทีซึ่งสอดคล้องกับการประมวลผลแบบเรียลไทม์ในอุตสาหกรรมการเงินการธนาคาร ทำให้องค์กรสามารถตรวจจับและแจ้งเตือนความผิดปกติได้แบบเรียลไทม์ เทคโนโลยีนี้ได้รับการนำไปใช้ในสถาบันการเงินขนาดใหญ่ เช่น ธนาคาร บริษัทบัตรเครดิต ซึ่งต้องบริหารจัดการธุรกรรมจำนวนมากในแต่ละวัน

นอกจากนี้ ผู้ผลิตและให้บริการซอฟต์แวร์ทางการเงินบัญชีแบบบูรณาการได้พัฒนาเครื่องมือการตรวจจับ การทุจริต เพื่อผนวกรวมในโซลูชัน เช่น QuickBooks SAP ก็ได้ผสมเทคโนโลยี AI เพื่อเพิ่มความสามารถในการตรวจสอบข้อมูลทางการเงิน เทคโนโลยีเหล่านี้ช่วยให้กับบัญชีสามารถมุ่งเน้นไปที่การวิเคราะห์เชิงกลยุทธ์มากขึ้นแทนที่การทำงานที่ต้องใช้เวลานาน เช่น การตรวจสอบที่ละรายการ การวิเคราะห์เอกสารและข้อความด้วย Natural Language Processing (NLP) ก็มีบทบาทสำคัญในปัจจุบัน NLP ช่วยให้นักบัญชีสามารถตรวจสอบเอกสารจำนวนมาก เช่น สัญญา อีเมล เพื่อระบุข้อความหรือข้อมูลที่อาจเกี่ยวข้องกับการฉ้อโกง เช่น การเปลี่ยนแปลงเงื่อนไขสัญญาที่ไม่ได้รับอนุญาต หรือการสื่อสารที่อาจระบุความเสี่ยง

AI เป็นเทคโนโลยีที่ทำให้คอมพิวเตอร์และเครื่องจักรสามารถเลียนแบบการเรียนรู้ของมนุษย์ การทำความเข้าใจ การแก้ปัญหา การตัดสินใจ ความคิดสร้างสรรค์ และการทำงานอย่างอิสระ โปรแกรมประยุกต์และอุปกรณ์ ที่มี AI สามารถมองเห็นและระบุวัตถุได้ สามารถเข้าใจและตอบสนองต่อภาษามนุษย์ สามารถเรียนรู้สารสนเทศและประสบการณ์ใหม่ ๆ สามารถให้คำแนะนำแก่ผู้ใช้ สามารถทำการได้อย่างเป็นอิสระทดแทนความฉลาดหรือการแทรกแซงของมนุษย์ (IBM, 2024) หลักการที่เกี่ยวพันกันกับ AI ได้รับการพัฒนามากว่า 70 ปี คือ Machine Learning เป็นระบบ AI ที่เรียนรู้จากข้อมูลในอดีต พัฒนาขึ้นเป็น Deep Learning ที่เลียนแบบการทำงานของสมองมนุษย์ ปัจจุบันพัฒนาเป็น Generative AI เป็นโมเดล Deep Learning ที่สามารถสร้างเนื้อหาได้เอง

การพัฒนาเทคโนโลยี Machine Learning มีผลต่อการตรวจจับการทุจริตทางการเงินอย่างมีนัยสำคัญ Deep Learning และ Reinforcement Learning ได้รับการออกแบบมาให้สามารถประมวลผลข้อมูลที่ซับซ้อนได้อย่างแม่นยำ Deep Learning ซึ่งใช้เครือข่ายประสาทเทียมที่ซับซ้อน (Neural Networks) ได้กลายเป็นเครื่องมือสำคัญที่ช่วยระบุรูปแบบการฉ้อโกงที่ยากต่อการตรวจจับในระบบการเงิน เช่น การวิเคราะห์ความเชื่อมโยงของธุรกรรมที่มีลักษณะต้องสงสัย หรือการตรวจจับธุรกรรมที่มีพฤติกรรมผิดปกติ AI สามารถสร้างแบบจำลองที่เรียนรู้จากข้อมูลในอดีตและปรับปรุงความแม่นยำได้ตลอดเวลา

ตัวอย่างการตรวจสอบการฉ้อโกงของบัตรเครดิต มีการตรวจสอบโดยการใช้ Neural Networks โดยที่สามารถเรียนรู้และวิเคราะห์ลักษณะพฤติกรรมที่ไม่ปกติจากข้อมูล เช่น จำนวนเงิน เวลา สถานที่ และพฤติกรรมการใช้บัตรเครดิต ระบบที่ใช้ Neural Networks สามารถตรวจจับการฉ้อโกงได้แบบเรียลไทม์ ซึ่งทำให้ผู้ให้บริการสามารถตอบสนองและยับยั้งการฉ้อโกงได้ทันที (Chaudhary et al., 2012) ขณะเดียวกัน Reinforcement Learning ได้รับการนำมาใช้ในการพัฒนาระบบที่สามารถตัดสินใจและตอบสนองต่อสถานการณ์ฉ้อโกงในแบบเรียลไทม์ ระบบเหล่านี้ช่วยให้ AI สามารถพัฒนาแนวทางใหม่ ๆ ในการจัดการกับความเสี่ยงที่เปลี่ยนแปลงอยู่เสมอ การตรวจจับการฉ้อโกงได้รับการขับเคลื่อนด้วยการผนวกรวมระหว่าง AI และเทคโนโลยีใหม่ เช่น Internet of Things (IoT) ในการติดตามและตรวจสอบธุรกรรมในเครือข่ายที่กว้างขึ้น หรือการพัฒนา AI ที่สามารถวิเคราะห์ข้อมูลแบบหลายมิติได้ในเวลาอันสั้น เทคโนโลยีเหล่านี้จะช่วยเสริมสร้างความปลอดภัยในระบบการเงินและลดความเสียหายจากการฉ้อโกงได้อย่างมีประสิทธิภาพ

การใช้เทคโนโลยี AI ช่วยยกระดับการตรวจจับการทุจริตทางการเงินในการระบุและตรวจสอบพฤติกรรมหรือกิจกรรมที่น่าสงสัยว่าอาจเป็นการฉ้อโกงจากข้อมูลหรือรายการทั้งหมด ตัวอย่างเทคนิค AI ที่มีการใช้ในการตรวจจับการทุจริตทางการเงินอย่างแพร่หลาย ดังนี้

1. Machine Learning

โมเดล Machine Learning สามารถระบุข้อมูลรายการค้าที่ผิดปกติ หรือพฤติกรรมผู้ใช้งาน (Hong, 2024) ตัวอย่างการใช้งานในอุตสาหกรรมบริการการเงิน เช่น การถอนเงินจำนวนมากจากบัญชีในเวลาอันสั้น การใช้จ่ายบัตรเครดิตหลายรายการอย่างต่อเนื่องจากสถานที่ที่ไม่ปกติ (Chaudhary et al., 2012) การโอนเงินระหว่างบัญชีในประเทศที่มีความเสี่ยงสูง รูปแบบของ Machine Learning มี 2 กลุ่ม คือ

1.1 Supervised learning เป็นการฝึกหัดโมเดลด้วยการใช้ข้อมูลที่มีคำตอบหรือระบุชัดเจนว่ารายการในชุดข้อมูลรายใดเป็นการทุจริต รายการใดเป็นรายการปกติ นั่นคือ ต้องมีผลสะท้อนกลับและการสนับสนุนจากมนุษย์เพื่อบอกว่าพฤติกรรมใดเป็นการทุจริต โมเดลที่ใช้งาน เช่น logistic regression random forest หรือ decision trees เทคนิคนี้อาจใช้เพื่อตรวจจับการทุจริตบัตรเครดิต การทุจริตประกันสุขภาพ (InfoSys, n.d.)

1.2 Unsupervised learning เป็นการจัดกลุ่มของข้อมูลตามความคล้ายคลึง ความผิดปกติที่ไม่เข้ากับกลุ่มข้อมูลที่จัดไว้จะได้รับการทำสัญลักษณ์หรือเครื่องหมายว่า อาจเป็นรายการทุจริต โมเดลที่ใช้ Unsupervised learning เช่น isolation forest ตัวอย่างการใช้งาน เช่น การอ่านและวิเคราะห์รายงานสถานะบัญชีเงินฝากธนาคาร สกัดคำเพื่อวิเคราะห์ตัวอักษร ประเภทหรือกลุ่มชื่อบริษัท ความเชื่อมโยง มูลค่าเงิน (InfoSys, n.d.)

2. Behavioral Analytics

Behavioral Analytics เป็นวิธีการศึกษารูปแบบพฤติกรรมซึ่งวิเคราะห์รูปแบบต่างๆ ของผู้ใช้ กระบวนการเริ่มด้วยการเก็บข้อมูลจากการติดตามกิจกรรมของผู้ใช้งานเพื่อสร้างฐานความรู้พฤติกรรมที่เป็นปกติของผู้ใช้ เพื่อระบุการทุจริตที่อาจเกิดขึ้นหรือกิจกรรมที่ผิดกฎหมาย Behavior Analytics ใช้งานร่วมกับ Machine Learning เพื่อติดตาม วิเคราะห์ข้อมูลรายการ ปรับให้เข้าใจหรือเรียนรู้รูปแบบการใช้งานที่เกิดขึ้นใหม่และเปลี่ยนแปลงเพื่อตรวจจับการทุจริตที่ปรับเปลี่ยนไป (Curry, 2025) การใช้งาน Machine Learning เพิ่มความแม่นยำในการวิเคราะห์พฤติกรรมผู้ใช้ ทำให้สามารถระบุชี้กิจกรรมของผู้ใช้หรือรายการที่อาจเป็นการทุจริตได้ (InfoSys, 2025) ตัวอย่างการใช้งาน ตรวจจับรายการค้า e-commerce ที่ผิดปกติแบบอัตโนมัติและเรียลไทม์ รายการซื้อสินค้าที่มากผิดปกติ การตรวจจับรายการบัตรเครดิตที่ถูกขโมยโดยวิเคราะห์ว่าผู้ใช้เคยทำธุรกรรมในร้านค้าเฉพาะในท้องถิ่น แต่การทำธุรกรรมเกิดขึ้นในต่างประเทศ

3. Natural Language Processing (NLP)

NLP เป็นส่วนหนึ่งของ AI ที่เน้นการวิเคราะห์ภาษามนุษย์ทั้งภาษาเขียนและภาษาพูด ทำให้สามารถจัดโครงสร้าง แปลความ ใช้งาน และรวมข้อมูลเกี่ยวกับภาษาเข้าร่วมในการประมวลผล (Martinez, 2023) การทำงานของ NLP แบ่งเป็น 3 กลุ่ม คือ การวิเคราะห์คำ การวิเคราะห์ข้อความ และการสร้างข้อความ

NLP สามารถสังเคราะห์วิเคราะห์ข้อมูลที่ลูกค้าให้ตอนสมัครหรือเปิดบัญชี ใช้วิเคราะห์ลำดับของพฤติกรรมหรือการกระทำของผู้ใช้งานเพื่อระบุธุรกรรมที่เป็นการฉ้อโกง โดยเปลี่ยนปัญหาจากการวิเคราะห์ ณ จุดหนึ่งของข้อมูล (point-in-time analysis) มาเป็นการวิเคราะห์ลำดับของเหตุการณ์ (sequence analysis) ที่เกิดขึ้นก่อนการทำธุรกรรม เช่น การเข้าสู่ระบบ การดยอดคงเหลือ หรือการโอนเงิน รวมทั้งสามารถวิเคราะห์แบบพยากรณ์ได้ ประเมินระดับความเสี่ยงจากการทุจริตของรายการ ตัวอย่างโมเดล NLP ที่มักนำมาใช้ได้แก่

3.1 Recurrent Neural Networks (RNNs) ใช้ในการวิเคราะห์ข้อมูลลำดับเหตุการณ์ โดยสามารถ จับความสัมพันธ์ ในข้อมูลที่ต่อเนื่อง เช่น ความถี่ของเหตุการณ์ในช่วงเวลาที่กำหนด และการเปลี่ยนแปลงพฤติกรรมที่ผิดปกติในระหว่าง การใช้งาน (Boulieris et al., 2024)

3.2 Long, Short-Term Memory (LSTM) เป็นโมเดลที่พัฒนามาจาก RNNs เพื่อแก้ปัญหากลืมข้อมูล ในลำดับที่ยาว โดยสามารถจับข้อมูลสำคัญที่เกิดขึ้นในอดีต และนำมาใช้ในการประมวลผลเหตุการณ์ปัจจุบัน เช่น การวิเคราะห์ว่าการโอนเงินครั้งล่าสุดมีความเกี่ยวข้องกับเหตุการณ์ก่อนหน้านี้ในลำดับหรือไม่ (Boulieris et al., 2024)

3.3 Transformers เป็นโมเดล NLP ที่ได้รับความนิยมในงานด้านการประมวลผลภาษาธรรมชาติ และได้นำมาใช้ ในบริบทของการตรวจจับการฉ้อโกง โดยสามารถวิเคราะห์ความสัมพันธ์ของเหตุการณ์ทั้งหมดในลำดับโดยไม่ถูกจำกัด ด้วยความยาวของข้อมูล ตัวอย่างเช่น การวิเคราะห์ว่าเหตุการณ์ที่เกิดขึ้นในช่วงเช้าส่งผลต่อธุรกรรมที่เกิดขึ้นในช่วงค่ำ ของวันเดียวกันหรือไม่ (Boulieris et al., 2024)

การตรวจจับการฉ้อโกงด้วย AI สามารถทำงานแบบเรียลไทม์และมีประสิทธิภาพสูง เนื่องจากสามารถประมวลผล ข้อมูลขนาดใหญ่และซับซ้อนได้อย่างรวดเร็วและแม่นยำ ทำให้สามารถตรวจจับพฤติกรรมที่น่าสงสัยและแจ้งเตือนล่วงหน้า ได้อย่างมีประสิทธิภาพ ตัวอย่างการใช้งานเช่น การตรวจสอบธุรกรรมในระบบธนาคารหรือบัตรเครดิตแบบเรียลไทม์ หรือการวิเคราะห์ข้อความจากเอกสารเพื่อระบุความผิดปกติ และสั่งระงับการทำรายการได้ทันที AI ยังสามารถเรียนรู้ จากข้อมูลใหม่และปรับปรุงความแม่นยำของการตรวจจับได้อย่างต่อเนื่อง ทำให้การตรวจจับการฉ้อโกงมีประสิทธิภาพ และตอบสนองต่อความเปลี่ยนแปลงในระบบการเงินได้ดีขึ้น อย่างไรก็ตาม การประยุกต์ใช้เทคโนโลยีคอมพิวเตอร์ ย่อมต้องมีการบริหารความเสี่ยง ส่วนต่อไปกล่าวถึงความท้าทายและความเสี่ยงจากการใช้งานเทคโนโลยี AI

■ ความท้าทายและความเสี่ยงในการใช้ AI

การนำ AI มาใช้ในงานบัญชีนิติวิทยามีศักยภาพสูง แต่ AI นั้นต้องได้รับการฝึกฝนทักษะในการคิด การวิเคราะห์ เพราะยังไม่สามารถใช้วิจารณ์ญาณและจริยธรรมเช่นเดียวกับมนุษย์ ประสิทธิภาพของ AI ขึ้นอยู่กับ การพัฒนา ออกแบบ โมเดลอัลกอริทึม รวมทั้ง ต้องได้รับการฝึกฝนโดยอาศัยสัญญาอนุญาต ประสิทธิภาพและการวิเคราะห์ของมนุษย์ (Kasztelnik & Jermakowicz, 2024) ความเสี่ยงจากข้อมูล โมเดล และการปฏิบัติงานอาจนำไปสู่ความล้มเหลวของระบบ ความเปราะบางของความมั่นคงไซเบอร์ที่อาจถูกเจาะระบบได้ง่าย (IBM, 2024) การใช้และบำรุงรักษาระบบการตรวจจับทุจริตทางการเงินที่ใช้งาน AI ย่อมพบกับความเสี่ยงอย่าง Type I and Type II Errors ในการสรุปผล บทความนี้ขอแยกตัวอย่าง ความท้าทายและความเสี่ยงในการใช้ AI ดังนี้

1. คุณภาพและความสมบูรณ์ของข้อมูล

ประสิทธิภาพของ AI ขึ้นอยู่กับอัลกอริทึมและข้อมูลที่ใช้ในการฝึกฝนและวิเคราะห์ หากข้อมูลมีคุณภาพต่ำ เช่น ข้อมูลที่ไม่ครบถ้วน ถูกบิดเบือน หรือมีความลำเอียง เทคโนโลยี AI อาจให้ผลลัพธ์ที่ไม่ถูกต้อง ข้อมูลที่ด้อยคุณภาพอาจเกิดจาก

1.1. ข้อมูลสูญหาย ขาดช่วงหรือไม่ครบถ้วน การบันทึกรายการธุรกรรมที่ไม่สมบูรณ์ทำให้ AI ไม่สามารถระบุรูปแบบการทุจริตได้

1.2. ข้อมูลบิดเบือน (Biased Data) หากข้อมูลในอดีตเน้นการทุจริตเพียงบางประเภท AI อาจละเลย การตรวจจับรูปแบบใหม่ที่ไม่ได้ระบุไว้ก่อนหน้านี้ กิจกรรมการพัฒนาคอนสตรัคข้อมูลที่เป็นระบบจัดเก็บข้อมูลอย่างถูกต้อง และทำความสะอาดข้อมูล (Data Cleaning) เพื่อให้ข้อมูลพร้อมสำหรับ การประมวลผลของ AI

1.3. ข้อมูลถูกโจมตีทำให้เสียหาย ข้อมูลที่อยู่ในระหว่างการประมวลผล การส่งผ่านและการจัดเก็บถูกโจมตี และถูกทำลาย แก้ไข ดัดแปลงโดยไม่ได้รับอนุญาต ทำให้ข้อมูลขาดความน่าเชื่อถือหรือไม่ถูกต้อง

กิจกรรมการบริหารความเสี่ยงด้านข้อมูลด้วยการปกป้องความบูรณาภาพของข้อมูลและจัดให้มีการกำกับดูแลข้อมูล การควบคุมความมั่นคงและสภาพพร้อมใช้งานให้ครอบคลุมทั่ววงจรอายุของ AI ตั้งแต่การพัฒนา การฝึกฝน การเริ่มใช้งาน และหลังการใช้งาน

2. ความสามารถในการชี้แจงได้ (Interpretability of AI Models)

AI ประเภท Deep Learning มีโครงสร้างและอัลกอริทึมที่ซับซ้อนและทำให้เกิดปัญหา “Black Box” กล่าวคือ ผู้ใช้งานไม่สามารถเข้าใจวิธีที่ AI ตัดสินใจได้ นับเป็นข้อเสียใหญ่ในงานการบัญชีนิติวิทยาที่ต้องใช้หลักฐานทางกฎหมาย ที่ชัดเจน (Chou, 2023) ตัวอย่างผลกระทบ เช่น ในกรณีที่ AI ระบุการทุจริตได้แต่ไม่สามารถอธิบายได้ว่าข้อมูลหรือรูปแบบใด เป็นหลักฐาน อาจไม่สามารถนำข้อมูลนั้นมาใช้ในการฟ้องร้องทางกฎหมาย

ความท้าทายนี้อาจจัดการด้วยการใช้ปัญญาประดิษฐ์ที่อธิบายได้ (Explainable AI: XAI) ในระบบการตรวจจับทุจริตทางการเงิน XAI เป็น AI ที่สามารถเข้ามาชี้แจงและไขข้อสงสัยได้ว่า กระบวนการคิดวิเคราะห์อย่างไร ทำไมจึงตัดสินใจ แนะนำและให้คำตอบแบบนี้แก่มนุษย์ที่เป็นผู้ใช้งาน เป็น AI ที่สามารถอธิบายการตัดสินใจได้ที่เข้าใจได้ง่าย คำอธิบายของ XAI ต้องมีความถูกต้องแม่นยำและสามารถสะท้อนให้เห็นได้ว่า ทำไมระบบจึงวิเคราะห์คำสั่งแล้วได้ผลลัพธ์นั้น ๆ XAI ต้องได้รับการกำหนดขอบเขตองค์ความรู้ (Knowledge limits) นั่นคือ XAI จะทำงานได้ภายใต้สถานการณ์และข้อจำกัด ที่ผู้พัฒนาได้ออกแบบมาเท่านั้น หาก XAI ยังขาดข้อมูลที่น่าเชื่อถือหรือมีความไม่แน่นอนสูง ก็จะไม่ประมวลผล และแสดงผลลัพธ์ (Xu et al., 2019) การใช้ XAI ผสมผสานกับความเชี่ยวชาญของมนุษย์ เพื่อวิเคราะห์ผลลัพธ์ร่วมกัน จึงเป็นทางออกสำหรับความท้าทายนี้

3. ความเป็นส่วนตัวและการปฏิบัติตามกฎหมาย

งานการบัญชีนิติวิทยาัมักเกี่ยวข้องกับข้อมูลที่เป็นความลับหรือข้อมูลส่วนบุคคล เช่น รายงานทางการเงินหรือข้อมูลของลูกค้า การใช้ AI ในการตรวจสอบทุจริตอาจละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น General Data Protection Regulation (GDPR) ของสหภาพยุโรป และ Personal Data Protection Act (PDPA) ของประเทศไทยหากองค์กรไม่ได้รับความยินยอมจากเจ้าของข้อมูล การประมวลผลด้วย AI อาจนำไปสู่คดีความทางกฎหมายหรือค่าปรับสูง องค์กรควรมีการจัดตั้งระบบการจัดการข้อมูลที่สอดคล้องกับข้อกำหนดทางกฎหมายและใช้การเข้ารหัสข้อมูลและระบบปกป้องความมั่นคงของข้อมูล รวมทั้งการสร้างโปรแกรมเพื่อบริหารจัดการความเสี่ยงด้านจริยธรรมในการการพัฒนา AI การใช้ข้อมูลและการใช้งาน AI

4. การต่อต้านการเปลี่ยนแปลง

การนำ AI มาใช้ในงานอาจทำให้บุคลากรรู้สึกกังวล เช่น กลัวหรือกังวลว่า AI จะมาแทนที่งานของตน และขาดความเข้าใจเกี่ยวกับเทคโนโลยีและความสามารถของ AI อาจเกิดการต่อต้านหรือการใช้งานที่ไม่เต็มประสิทธิภาพจากบุคลากร องค์กรต้องจัดโปรแกรมฝึกอบรมให้บุคลากรเข้าใจความสำคัญของ AI ชี้ให้เห็นว่า AI เป็นเครื่องมือสนับสนุนไม่ใช่สิ่งที่มาแทนที่บุคลากร

5. ค่าใช้จ่ายและทรัพยากร

การพัฒนาและนำ AI มาใช้ต้องการการลงทุนที่สูงในหลายด้าน เช่น การพัฒนาระบบและโครงสร้างพื้นฐาน การว่าจ้างผู้เชี่ยวชาญด้าน AI และ ค่าใช้จ่ายในการบำรุงรักษาระบบ องค์กรขนาดเล็กหรือองค์กรที่มีงบประมาณจำกัดอาจไม่สามารถนำ AI มาใช้งานได้จากปัจจัยนี้ องค์กรควรเริ่มต้นจากการใช้โซลูชัน AI แบบสำเร็จรูปที่มีต้นทุนไม่แพง และพิจารณาร่วมมือกับบริษัทผู้ให้บริการ AI นอกจากนี้ค่าใช้จ่ายและทรัพยากรที่มีความสัมพันธ์ทางตรงกับการใช้ AI ก็คือการควรต้องพิจารณาต้นทุนหรือความเสียหายจากความเสี่ยงที่ยังมองไม่เห็นรวมทั้งต้นทุนการจัดการความมั่นคงและการกำกับดูแล (Lanz, 2024)

6. การพึ่งพาเทคโนโลยีมากเกินไป

การใช้เทคโนโลยีในการปฏิบัติงานอาจทำให้บุคลากรพึ่งพาเทคโนโลยีและผลลัพธ์เหล่านั้นมากเกินไปและเพิกเฉยละเลยองค์ประกอบการใช้วิจารณญาณของมนุษย์ในการตรวจจับการทุจริต ความเสี่ยงจากการพึ่งพาเทคโนโลยีมากเกินไปทำให้ผู้ประกอบการวิชาชีพไม่ใช้วิจารณญาณ ความสงสัย ความระมัดระวัง และประสบการณ์ ในการแปลความหมายผลลัพธ์การสรุปผลรายงานและการใช้ผลลัพธ์จาก AI (Kasztelnik & Jermakowicz, 2024)

■ ผู้ประกอบวิชาชีพกับการใช้ AI

การใช้งาน AI ให้เกิดประโยชน์ระดับที่เหมาะสมต้องมีการบริหารความเสี่ยงเพื่อลดระดับความเสี่ยงและผลที่ไม่พึงประสงค์ การพัฒนาและใช้งานระบบการตรวจจัดการทุจริตทางการเงินด้วย AI ที่อธิบายได้ (XAI) และมีความรับผิดชอบ (Responsible AI: RAI) จึงต้องมีการกำกับดูแลเพื่อให้มั่นใจว่าระบบและเครื่องมือ AI นั้นปลอดภัย สอดคล้องกับจริยธรรม และกฎระเบียบ การใช้งาน AI นั้นอยู่ภายใต้การกำกับดูแลที่ครบตั้งแต่ต้นจนจบ มีหลักการที่สามารถตอบประเด็นอคติ และความยุติธรรม (bias and fairness) การตีความและอธิบายได้ (interpretability and explainability) และความเข้มแข็ง และความมั่นคง (robustness and security) (PwC, 2019)

ประกอบวิชาชีพควรอ้างอิงกรอบการบริหารความเสี่ยง AI (Artificial Intelligence Risk Management Framework: AI RMF 1.0) ที่ National Institute of Standards and Technology (NIST) พัฒนาและเผยแพร่ให้กับสาธารณชนบนเว็บไซต์ของ NIST (<https://www.nist.gov/itl/ai-risk-management-framework>) โดยไม่คิดค่าใช้จ่าย (National Institute of Standards and Technology [NIST], 2023) เพื่อช่วยให้บุคคล องค์กรและสังคม ได้บริหารจัดการ AI ได้ดีขึ้น AI RMF 1.0 เป็นแนวทางการบริหารความเสี่ยงเพื่อปรับปรุงความสามารถในการพิจารณาผนวก รวม ความน่าเชื่อถือในกระบวนการออกแบบ การพัฒนา การใช้ และการประเมินผลของผลิตภัณฑ์ บริการและระบบงาน ที่ใช้ AI นอกจากนี้ NIST ได้เผยแพร่ทรัพยากรต่าง ๆ ที่เกี่ยวกับการบริหารความเสี่ยง AI เช่น Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST, 2024) เพื่อช่วยให้องค์กรระบุ ความเสี่ยงจำเพาะจาก Generative AI และเสนอการปฏิบัติเพื่อการบริหารความเสี่ยงให้สอดคล้องกับเป้าหมาย และลำดับความสำคัญขององค์กร

การใช้งาน AI ในการทำงานการตรวจสอบยังต้องพิจารณากฎหมายที่เกี่ยวข้องกับการกำกับดูแล AI เช่น Artificial Intelligence Act of the European Union (EU AI Act) ในปี ค.ศ. 2024 ใช้แนวทางการกำกับดูแลอิงตามความเสี่ยง นับเป็นกรอบกฎระเบียบครอบคลุม AI ฉบับแรกในโลก EU AI Act ห้ามการใช้งาน AI บางกลุ่มและกำหนดให้ต้องมีการกำกับดูแลที่เข้มงวด การบริหารความเสี่ยงและข้อกำหนดด้านความโปร่งใส EU AI Act กำหนดวันที่มีผลบังคับสำหรับ AI แต่ละชั้นต่างวันกัน เช่น วันที่ 2 กุมภาพันธ์ ค.ศ. 2025 ห้ามการใช้งาน AI ที่มีระดับความเสี่ยงที่รับไม่ได้ตามกลุ่มงาน ที่กฎหมายกำหนด (Kosinski & Scapicchio, 2024)

สำหรับประเทศในภูมิภาคเอเชียแปซิฟิก ได้มีการเผยแพร่หลักการและแนวทางสำหรับการกำกับดูแล AI เช่น รัฐบาลสิงคโปร์ ได้เผยแพร่กรอบและแนวทางในการจัดการจริยธรรม AI ในปี ค.ศ. 2019 กรอบกำกับดูแล AI ในปี ค.ศ. 2024 (Mucci & Stryker, 2024) ในประเทศไทย ศูนย์ธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance Center: AIGC) ภายใต้สำนักพัฒนาธุรกรรม ทางอิเล็กทรอนิกส์ (สพธอ. หรือ Electronic Transactions Development Agency: ETDA) ได้พัฒนาและนำเสนอ แนวทางการประยุกต์ใช้ AI ให้เหมาะสมกับบริบทของไทยและสอดคล้องกับนโยบายระดับสากล ทั้งนี้ AIGC ได้เผยแพร่ แหล่งทรัพยากรต่าง ๆ บนเว็บไซต์เกี่ยวกับการกำกับดูแล AI (<https://www.etda.or.th/th/Our-Service/AIGC/index.aspx>)

■ บทสรุป

การนำ AI มาใช้ในงานบัญชีเชิงนิติวิทยากำลังเปลี่ยนแปลงบทบาทของผู้ประกอบวิชาชีพการตรวจสอบรวมถึงนักบัญชีนิติวิทยา กระบวนการตรวจสอบและการวิเคราะห์ข้อมูลทางการเงินขององค์กรที่มีอยู่จำนวนมาก มีความซับซ้อนและต้องการความแม่นยำสูง การใช้ AI ช่วยส่งผลดีให้กระบวนการเหล่านี้สามารถตรวจสอบได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้นโดยปราศจากความอคติแบบมนุษย์ เทคนิค AI ที่กล่าวในบทความนี้ได้แก่ Machine Learning Behavioral Analytics และ Natural Language Processing เครื่องมือ AI สามารถอ่าน วิเคราะห์ข้อมูลและเอกสารทางการเงิน ทำให้สามารถระบุช่องโหว่หรือความเสี่ยงที่ซ่อนอยู่ได้อย่างมีประสิทธิภาพ

ประสิทธิภาพและประสิทธิผลจากการใช้งาน AI เพื่อการตรวจจับการทุจริตทางการเงินนั้นก่อให้เกิดประโยชน์ในการป้องปรามการทุจริตทางการเงินได้ การพัฒนาและสร้างระบบตรวจจับการทุจริตด้วย AI ต้องอาศัยมนุษย์ในการพัฒนาอัลกอริทึม การฝึกฝนด้วยชุดข้อมูลที่มาจากรู้ความชำนาญของมนุษย์จนทำให้ AI สามารถเรียนรู้ได้ด้วยตนเองถึงการตรวจสอบข้อมูลที่ผิดปกติ การใช้งาน AI อาจมีการวิเคราะห์หรือตรวจสอบที่ผิดพลาดจากการใช้ข้อมูลที่ไม่เหมาะสมหรือการตัดสินใจโดยอัตโนมัติโดยอาจไม่ได้สะท้อนถึงข้อเท็จจริงทั้งหมด นักบัญชีนิติวิทยายังคงต้องใช้ทักษะการสงสัยเยี่ยงผู้ประกอบวิชาชีพบัญชี (Professional skepticism) ในการตรวจประเมินผลลัพธ์จาก AI ผู้ประกอบวิชาชีพพึงทำความเข้าใจและตระหนักถึงความท้าทายและความเสี่ยงจากการใช้ AI ทั้งด้านข้อมูล โมเดลและจริยธรรม ทั้งต้องขยายขอบเขตถึงการกำกับดูแลและบริหารความเสี่ยงการ ใช้งาน AI ในการปฏิบัติงานเพื่อได้รับประโยชน์จากเทคโนโลยีที่ได้ลงทุนไป การตรวจสอบการทุจริตด้วย AI สามารถเพิ่มศักยภาพในการทำงานและคุณภาพการตรวจสอบได้ดีขึ้น แต่ผู้ประกอบวิชาชีพก็ต้องพิจารณาประเด็นการบริหารความเสี่ยงในการใช้เครื่องมือเพื่อลดความเสี่ยงและผลกระทบอันไม่พึงประสงค์



■ References

- Boulrieris, P., Pavlopoulos, J., Xenos, A., & Vassalos, V. (2024). Fraud detection with natural language processing. *Machine Learning*, 113(3), 5087–5108. <https://doi.org/10.1007/s10994-023-06354-5>
- Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques: Credit card. *International Journal of Computer Applications*, 45(1), 39–41. <https://doi.org/10.5120/6748-8991>
- Chou, B. (2023, July 3). The digital sentry: How AI will revolutionize financial fraud investigation. *Forbes*. <https://www.forbes.com/councils/forbestechcouncil/2023/07/03/the-digital-sentry-how-ai-will-revolutionize-financial-fraud-investigation/>
- Curry, J. (2025, January–February). Behavioral analytics could’ve detected and prevented Evergrande fraud. *Fraud Magazine*, 40(1). <https://www.fraud-magazine.com/article.aspx?id=4295024317>
- Hong, Z. (2024, April 20). Fraud detection with machine learning: Identifying suspicious patterns in financial transactions. *Medium*. <https://medium.com/@zhonghong9998/fraud-detection-with-machine-learning-identifying-suspicious-patterns-in-financial-transactions-8558f3f1e22a>
- IBM. (2024, August 9). What is artificial intelligence (AI)? *IBM*. <https://www.ibm.com/think/topics/artificial-intelligence>
- InfoSys. (2025, January 4). Behavioural analytics for fraud detection. *InfoSys BPM*. <https://www.infosysbpm.com/blogs/bpm-analytics/behavioural-analytics-fraud-detection.html>
- InfoSys. (n.d.). Fraud detection technologies: Make AI and machine learning work for you. *BPM Analytics*. <https://www.infosysbpm.com/blogs/bpm-analytics/financial-fraud-detection.html>
- International Association of Independent Accounting Firms. (2024, July 2). The role of forensic accounting in fraud detection. *International Association of Independent Accounting Firms*. <https://www.inaa.org/the-role-of-forensic-accounting-in-fraud-detection>
- Kasztelnik, K., & Jermakowicz, E. K. (2024, July). Financial statement fraud detection in the digital age: Artificial intelligence versus traditional methodologies. *The CPA Journal*. <https://www.cpajournal.com/2024/07/23/financial-statement-fraud-detection-in-the-digital-age-2/>
- Kosinski, M., & Scapicchio, M. (2024, September 20). What is the Artificial Intelligence Act of the European Union (EU AI Act)? *IBM*. <https://www.ibm.com/think/topics/eu-ai-act>
- Lanz, J. (2024, December). Worst AI risk-management practices. *The CPA Journal*. <https://www.cpajournal.com/2024/12/31/worst-ai-risk-management-practices/>

- Martinez, A. (2023, May 10). Getting value from NLP for fraud detection. *Forbes*. <https://www.forbes.com/councils/forbesbusinesscouncil/2023/05/10/getting-value-from-nlp-for-fraud-detection/>
- Mucci, T., & Stryker, C. (2024, October 10). What is AI governance? *IBM*. <https://www.ibm.com/think/topics/ai-governance>
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0). *National Institute of Standards and Technology*. <https://doi.org/10.6028/NIST.AI.100-1>
- National Institute of Standards and Technology. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile. <https://doi.org/10.6028/NIST.AI.600-1>
- PwC. (2019). A practical guide to responsible artificial intelligence (AI). *PwC*. <https://www.pwc.com/gx/en/issues/data-and-analytics/artificial-intelligence/what-is-responsible-ai/responsible-ai-practical-guide.pdf>
- Singleton, T., Singleton, A., Bologna, J., & Lindquist, R. (2006). *Fraud auditing and forensic accounting*. John Wiley & Sons.
- Srijunpetch, S. (2010). Get to know forensic accounting. *Journal of Accounting Profession*, 6(17), 22–28.
- Supphatada, S. (2007). Let's blow the whistle. *Journal of Accounting Profession*, 3(7), 13–15. <https://www.jap.tbs.tu.ac.th/files/Article/Jap07/Column/JAP07SomchaiC.pdf>
- Supphatada, S. (2020). *Forensic accounting: Integrative knowledge for the digital era*. Supphatada, Somchai.
- The Securities and Exchange Commission, Thailand. (2024, September 18). SEC news. *The Securities and Exchange Commission, Thailand*. https://www.sec.or.th/TH/Pages/News_Detail.aspx?NewsNo=197&NewsYear=2567&Lang=TH
- Xu, F., Uszkoreit, H., Du, Y., & Fan, W. (2019). Explainable AI: A brief survey on history, research areas, approaches, and challenges. In J. Tang, M.-Y. Kan, D. Zhao, S. Li, & H. Zan (Eds.), *Natural language processing and Chinese computing* (Vol. 11839, pp. 563–574). Springer. https://doi.org/10.1007/978-3-030-32236-6_51