การเพิ่มความมั่นคงของข้อมูลและการสื่อสารด้วยเทคโนโลยีการกู้คืนกุญแจลับ
Enhancing Data and Communication Security with Key Recovery Technology

จำรูญ จันทร์กุญชร[1] และ กนกวรรณ กันยะมี[2*]

[1, 2]สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏอุตรดิตถ์

Jumroon Chankulchorn[1] and Kanokwan Kanyamee[2*]

[1, 2]Information Technology Program, Uttaradit Rajabhat University

kanokwan@uru.ac.th

Received 03 March 2025

Revised 29 April 2025

Accepted 14 May 2025

บทคัดย่อ

ในยุคดิจิทัลการสื่อสารผ่านระบบเครือข่าย กลายเป็นปัจจัยสำคัญที่ขับเคลื่อนกิจกรรมหลากหลายด้านของมนุษย์และสังคม โดยมีสิ่งที่ต้องตระหนักอย่างยิ่งคือ ความมั่นคงปลอดภัยของข้อมูล และความน่าเชื่อถือของการสื่อสาร ดังนั้นเพื่อปกป้องข้อมูลจากความเสียหายที่มีผลกระทบต่อความมั่นคงปลอดภัย เทคโนโลยีการกู้คืนกุญแจลับ (Key Recovery Technology) ได้เข้ามามีบทบาทสำคัญในการเสริมสร้างและยกระดับความน่าเชื่อถือ พร้อมทั้งเพิ่มความเชื่อมั่นในการสื่อสาร โดยเฉพาะในกรณีกุญแจลับ (Secret Key) ที่ใช้ในการเข้ารหัสข้อมูลสูญหาย หรือไม่สามารถใช้งานได้ ซึ่งมีผลให้เข้าถึงข้อมูลไม่ได้ อาจสร้างความเสียหายทั้งในระดับบุคคล องค์กร และโครงสร้างพื้นฐาน เช่น การสูญเสียหลักฐานทางธุรกิจ ข้อมูลส่วนบุคคล หรือการหยุดชะงักของระบบบริการสาธารณะ เป็นต้น ซึ่งเทคโนโลยีนี้ช่วยในการกู้คืนกุญแจลับ ทำให้สามารถเข้าถึงข้อมูลได้อย่างปลอดภัย โดยไม่กระทบต่อความเป็นส่วนตัวของผู้ใช้งาน นอกจากนี้ยังสนับสนุนการดำเนินงานตามนโยบายด้านกฎหมาย นั่นคือการเข้าถึงข้อมูลที่อยู่ในข่ายต้องสงสัยเพื่อการตรวจสอบอย่างเหมาะสม โปร่งใส รวมถึงการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ จึงถือเป็นเครื่องมือสำคัญที่ช่วยรักษาความมั่นคงปลอดภัยของข้อมูล ส่งเสริมสนับสนุนความต่อเนื่องของธุรกิจและเพิ่มความมั่นคงปลอดภัยในสังคมดิจิทัลอย่างยั่งยืน บนพื้นฐานของการรักษาความลับและความเป็นส่วนตัวของผู้ใช้งาน

คำสำคัญ: ความมั่นคงปลอดภัย, ข้อมูล, การกู้คืนกุญแจ, กุญแจลับ

Abstract

In the digital era, network-based communication has become a cornerstone of diverse human and societal activities. This evolution has brought to the forefront the critical importance of information security and communication reliability. To protect sensitive data from threats that

could compromise its integrity and availability, Key Recovery Technology (KRT) plays a pivotal role in enhancing trust and resilience in digital communication systems. It is particularly essential in cases where secret keys used for data encryption are lost or become unusable, which can result in a complete loss of access to encrypted information. Such incidents may result in significant damage at individual, organizational, and infrastructural levels, including the loss of business-critical evidence, breaches of personal data, or the disruption of essential public services. KRT enables the recovery of secret keys in a secure and privacy-preserving manner, ensuring that data remains accessible without violating user confidentiality. Moreover, this technology supports compliance with legal and regulatory frameworks by allowing authorized access to data under investigation, ensuring transparency and accountability while preventing unauthorized access. Therefore, KRT serves as a key enabler of robust information security, supporting business continuity and fostering sustainable trust in the digital ecosystem by upholding the principles of confidentiality, integrity, and user privacy.

Keywords: Security, Data, Key Recovery, Secret Key

1. บทนำ

ความมั่นคงปลอดภัยของข้อมูลและการสื่อสาร ถือเป็นรากฐานสำคัญที่ช่วยสนับสนุนการดำเนินชีวิตในยุคดิจิทัล ซึ่งเป็นยุคที่ข้อมูลกลายเป็นทรัพยากรที่มีมูลค่าสูง ใช้ในการขับเคลื่อนเศรษฐกิจ สังคม และเป็นเครื่องมือช่วยในการวิเคราะห์วางแผนการพัฒนาองค์กรและประเทศชาติ ในขณะเดียวกันข้อมูลก็มีความเสี่ยงที่จะถูกโจมตี เข้าถึง ตลอดจนถูกเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต เช่น การขโมย การปลอมแปลง หรือการละเมิดความเป็นส่วนตัว ส่งผลให้เกิดความเสียหายต่อตัวบุคคล องค์กร และโครงสร้างพื้นฐานของสังคม เช่น ระบบพลังงาน การคมนาคม และสาธารณสุข อาจส่งผลให้การดำเนินงานล้มเหลว หยุดชะงัก หรือถูกแทรกแซง ซึ่งส่งผลกระทบต่อความมั่นคงของประเทศในวงกว้าง ดังนั้นการรักษาความมั่นคงปลอดภัยของข้อมูลและการสื่อสาร จึงช่วยเสริมสร้างความไว้วางใจในระบบดิจิทัล ป้องกันการหยุดชะงักของระบบสารสนเทศที่สำคัญ อย่างไรก็ตามการให้ความสำคัญในเรื่องดังกล่าวจึงไม่ใช่เพียงปกป้องทรัพยากรที่มีค่า แต่ยังเป็นการรักษาเสถียรภาพและความยั่งยืนบนโลกดิจิทัล ที่ต้องพึ่งพาข้อมูลในการดำเนินกิจกรรมต่าง ๆ

เทคโนโลยีการเข้ารหัสข้อมูล (Cryptography Technology) [1] เป็นหนึ่งในกลไกที่สำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูล ด้วยการใช้กุญแจลับ (Secret Key) ในการเข้ารหัสข้อมูล (Data Encryption) ซึ่งเป็นการแปลงข้อความต้นฉบับ (Plaintext) ให้อยู่ในรูปแบบที่ซับซ้อนและไม่สามารถเข้าใจได้ (Ciphertext) เพื่อปกป้องข้อมูลจากบุคคลที่สามหรือผู้ที่ไม่ได้รับอนุญาต จะมีเฉพาะคู่สื่อสาร (Sender - Receiver) เท่านั้นที่มีสิทธิ์ในการเข้าถึงข้อมูลโดยใช้กุญแจในการถอดรหัส เทคโนโลยีนี้ถูกนำมาใช้ในหลายบริบท เช่น การปกป้องข้อมูลส่วนบุคคล การรักษาความลับของธุรกรรมทางการเงิน ตลอดจนการสื่อสารที่ปลอดภัยในองค์กร เป็นต้น ฉะนั้นจากการที่ข้อมูลจำนวนมากถูกเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต กุญแจลับจึงเป็นหัวใจสำคัญที่ช่วยรักษาความปลอดภัยของข้อมูล หากกุญแจลับสูญหายหรือใช้งานในการถอดรหัสไม่ได้ จะส่งผลให้ไม่สามารถเปิดอ่านข้อมูลสำคัญได้เช่นกัน ทำให้

ข้อมูลถูกล็อกอย่างถาวร เพื่อแก้ปัญหานี้จึงมีการคิดค้นกระบวนการที่ปลอดภัยในการกู้คืนกุญแจลับ เรียกว่า เทคโนโลยีการกู้คืนกุญแจลับ (Key Recovery Technology) [2] เป็นการผสานระบบการกู้คืนกุญแจเข้ากับการเข้ารหัสลับ เป็นเทคโนโลยีที่ทำให้สามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสได้ โดยไม่ละเมิดความปลอดภัยหรือความเป็นส่วนตัว ส่งผลให้สามารถรักษาความมั่นคงปลอดภัยของข้อมูลได้ในทุกมิติ อีกทั้งยังช่วยสนับสนุนความต่อเนื่องในการดำเนินงาน รองรับความพร้อมใช้งานของข้อมูล และลดผลกระทบที่อาจเกิดขึ้นจากการโจมตีหรือความผิดพลาดได้อย่างยั่งยืน โดยวัตถุประสงค์หลักของการพัฒนาเทคโนโลยีการกู้คืนกุญแจลับ มี 2 ประการด้วยกันคือ (1) เพื่อกู้คืนกุญแจลับที่สูญหายหรือไม่สามารถใช้งานได้ และ(2) เพื่อรองรับการเข้าถึงข้อมูลที่ต้องสงสัยเพื่อการตรวจสอบภายใต้นโยบายและกฎหมาย [3]

2. ความมั่นคงปลอดภัยของข้อมูลและการสื่อสาร

ความมั่นคงปลอดภัยของข้อมูลและการสื่อสารเป็นฐานสำคัญของความปลอดภัยในโลกยุคดิจิทัล โดยมุ่งเน้นการปกป้องข้อมูลให้มั่นคงปลอดภัยจากการเข้าถึง ทำลาย หรือถูกเปลี่ยนแปลงแก้ไขจากผู้ที่ไม่มีสิทธิ์ และทำให้มั่นใจว่าข้อมูลสามารถใช้งานได้อย่างมีประสิทธิภาพ ในขณะเดียวกันก็เป็นแนวทางในการปกป้องข้อมูลจากภัยคุกคามทางไซเบอร์ โดยอาศัยหลักการของวิทยาการเข้ารหัสลับข้อมูล ซึ่งจะทำให้การสื่อสารมีความมั่นคงปลอดภัย และลดความเสี่ยงจากการถูกแทรกแซงหรือโจมตีทางไซเบอร์

แนวคิดหลักของความมั่นคงปลอดภัยของข้อมูลและการสื่อสาร [4] มักเรียกย่อ ๆ ว่า CIA ซึ่งได้รับการนิยามและใช้อ้างอิงอย่างแพร่หลายในเอกสารมาตรฐานของ NIST เช่น NIST Special Publication 1800 Series [5] ซึ่งมีองค์ประกอบที่สำคัญ 3 ประการ

2.1 การรักษาความลับ (Confidentiality: C) คือ การป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงข้อมูล ด้วยการใช้วิธีการเข้ารหัส (Encryption) และควบคุมสิทธิ์การเข้าถึง (Access Control)

2.2 ความถูกต้องของข้อมูล (Integrity: I) คือ การป้องกันข้อมูลไม่ให้ถูกเปลี่ยนแปลงหรือแก้ไข โดยไม่ได้รับอนุญาต ด้วยการใช้เทคนิค เช่น การใช้ฟังก์ชันแฮช (Hashing) ลายมือชื่อดิจิทัล (Digital Signature) และ การตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูล (Checksums) เป็นต้น

2.3 ความพร้อมใช้งาน (Availability: A) คือ การทำให้ระบบหรือข้อมูล สามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ ซึ่งสามารถใช้วิธีสำรองข้อมูล (Backup) การปรับสมดุลโหลด (Load Balancing) และ การทำแผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan) เป็นต้น

อย่างไรก็ตาม แม้ว่าการเข้ารหัสลับจะเป็นกลไกสำคัญที่ช่วยปกป้องข้อมูลและการสื่อสารให้มั่นคงปลอดภัย จากการเข้าถึงโดยไม่ได้รับอนุญาต แต่ก็มีประเด็นที่ต้องให้ความตระหนักนั่นคือ หากกุญแจลับที่ใช้ในการเข้ารหัส สูญหายหรือถูกทำลาย จะส่งผลถึงข้อมูลที่เข้ารหัส คือทำให้ไม่สามารถถอดรหัสได้ เหตุการณ์ดังกล่าวส่งผลกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องในการสื่อสารข้อมูล ดังนั้นเพื่อแก้ไขปัญหาดังกล่าว จึงได้มีการพัฒนาเทคโนโลยีการกู้คืนกุญแจลับขึ้น เพื่อเป็นแนวทางในการช่วยให้ผู้ใช้หรือองค์กร สามารถกู้คืนกุญแจที่สูญหายได้ โดยไม่ส่งกระทบต่อความมั่นคงปลอดภัยและความเป็นส่วนตัว นอกจากนี้ยังช่วยในการรักษาข้อมูลที่เป็นความลับ มีการบริหารจัดการกุญแจที่สอดคล้องกับมาตรฐานความปลอดภัย ตลอดจนสนับสนุนรองรับการกู้คืนข้อมูลเพื่อวัตถุประสงค์ทางกฎหมายและการสืบสวนทางไซเบอร์

3. เทคโนโลยีการกู้คืนกุญแจลับ

3.1 ความเป็นมาและวิวัฒนาการของเทคโนโลยีการกู้คืนกุญแจลับ

เทคโนโลยีการกู้คืนกุญแจลับเกิดขึ้นจากความต้องการจัดเก็บกุญแจลับเพื่อสำรองไว้ในที่ปลอดภัย และสามารถใช้ในการกู้คืนกุญแจกรณีที่กุญแจหายหรือไม่สามารถใช้งานได้ รองรับการเข้าถึงข้อมูลต้องสงสัยที่สื่อสารบนระบบเครือข่ายอย่างถูกต้องตามกฎหมาย ซึ่งเป็นหนึ่งในกลไกสำคัญของการรักษาความปลอดภัยของระบบสารสนเทศ ความจำเป็นในการพัฒนาเทคโนโลยีนี้ เริ่มชัดเจนในยุคที่การเข้ารหัสลับเริ่มถูกใช้อย่างแพร่หลาย ในหน่วยงานรัฐบาลและองค์กรขนาดใหญ่

โดยในช่วงแรกการบริหารจัดการกุญแจลับอยู่ในรูปแบบที่ไม่ซับซ้อนมากนัก โดยใช้การเก็บรักษากุญแจไว้กับบุคคลใดบุคคลหนึ่งหรือหน่วยงานกลางของรัฐบาล [6] ซึ่งเป็นวิธีที่มีความเสี่ยงสูงในด้านความมั่นคงปลอดภัย เช่น กุญแจที่จัดเก็บสำรองไว้ถูกขโมยหรือมีการเข้าถึงโดยผู้ประสงค์ร้าย ความเสี่ยงด้านความลับของกุญแจถูกเปิดเผย ตลอดจนการผูกขาดกุญแจโดยบุคคลที่สาม และเสี่ยงต่อเกิดภัยคุกคามทางไซเบอร์ที่มีความรุนแรงเพิ่มขึ้น เป็นต้น จากเหตุการณ์ดังกล่าวทำให้การจัดการกุญแจรูปแบบเดิมไม่มีความปลอดภัย จึงเกิดการปรับปรุงและพัฒนาเทคโนโลยีการกู้คืนกุญแจอย่างต่อเนื่อง โดยสามารถแบ่งตามยุคสมัยได้ 7 ยุค ดังแสดงในตารางที่ 1

ตารางที่ 1 ยุคของเทคโนโลยีการกู้คืนกุญแจ

ยุคของเทคโนโลยี	รายละเอียด
ยุคที่ 1 การจัดการกุญแจแบบพื้นฐาน (ก่อนปี 1970)	ยุคเริ่มต้นของการเข้ารหัส ระบบการกู้คืนกุญแจยังไม่มีการพัฒนาอย่างเป็นรูปธรรมชัดเจน กุญแจลับถูกจัดเก็บในแบบที่ไม่ปลอดภัย เช่น บันทึกในหน่วยความจำ หรือเก็บไว้ในสภาพแวดล้อมที่ไม่มีการควบคุม หากสูญหายจะไม่สามารถกู้ข้อมูลกลับมาได้ และมีความเสี่ยงจากการถูกโจมตี
ยุคที่ 2 แนวคิดพื้นฐานของ Key Escrow (ช่วงทศวรรษ 1970-1980)	เริ่มมีการนำเสนอแนวคิด Key Escrow [6] ในเชิงวิชาการ กล่าวคือ การฝากกุญแจไว้กับบุคคลที่สามที่เชื่อถือได้ (Trusted Third Party: TTP) เพื่อใช้ในกรณีฉุกเฉิน แนวคิดยังอยู่ในช่วงต้นทางทฤษฎี ยังไม่มีการดำเนินเชิงนโยบายอย่างเป็นทางการ
ยุคที่ 3 การผลักดันนโยบาย Key Escrow โดยภาครัฐ (ช่วงปี 1990)	รัฐบาลสหรัฐฯ เสนอให้ใช้ระบบเข้ารหัส ที่สามารถให้รัฐเข้าถึงข้อมูลได้โดยชอบด้วยกฎหมายผ่าน TTP เพื่อความมั่นคงปลอดภัยภายใน เช่น โครงการ Clipper Chip และ มาตรฐาน Escrowed Encryption Standard (EES) [7] แต่ได้รับกระแสต่อต้านจากภาคประชาชน ว่าเป็นการละเมิดความเป็นส่วนตัว เช่น Howard S. Dakoff [8] ที่ได้ให้ความเห็นว่าการดำเนินการดังกล่าวต้องอยู่ภายใต้กรอบของกฎหมายที่มีความชัดเจน
ยุคที่ 4 การใช้เอเจนต์และศูนย์กลางในการกู้คืนกุญแจ (ช่วงปลายปี 1990)	เข้าสู่ยุคที่การกู้คืนกุญแจลับถูกบูรณาการเข้ากับการเข้ารหัสที่มีความซับซ้อนมากขึ้น มีการใช้ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center: KRC) ร่วมกับเอเจนต์กู้คืนกุญแจ (Key Recovery Agent: KRA) โดยอาศัยการแบ่งปันความลับ (Secret Sharing) [9] ซึ่งเป็นการทำงานแบบใช้หลายเอเจนต์ในการกู้คืนกุญแจ (Multiple Key Recovery Agent: M-KRA) [10] เพื่อลดความเสี่ยงจากการผูกขาดกุญแจแต่เพียงผู้เดียว
ยุคที่ 5 การห่อหุ้มกุญแจลับ	เกิดแนวคิดการสร้างฟิลด์ในการกู้คืนกุญแจ (Key Recovery Field: KRF) และการห่อหุ้มกุญแจลับ (Secret Key Encapsulation) [11] ที่ทำงาน

ยุคของเทคโนโลยี	รายละเอียด
(ช่วงปี 2000)	ภายใต้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) [12] เพื่อเสริมสร้างความมั่นคงปลอดภัยและง่ายในการจัดการมากขึ้น
ยุคที่ 6 การกู้คืนแบบกระจายโดยหลายเอเจนต์แบบกระจายศูนย์ หรือไม่พึ่งพาศูนย์กลาง (ช่วงปี 2010)	พัฒนาแนวคิดการกู้คืนกุญแจแบบหลายเอเจนต์ (Multiple Key Recovery Agent: M-KRA) แบบกระจายศูนย์ (Decentralized) [13] ลดความเสี่ยงจาก Single Point of Failure และเพิ่มความยืดหยุ่นในการกู้คืน
ยุคที่ 7 ยุคควอนตัมและอนาคต (ปี 2020 เป็นต้นไป)	เตรียมรับมือภัยคุกคามจากคอมพิวเตอร์ควอนตัม โดยใช้ Post-Quantum Cryptography (PQC) [14] เพื่อให้ระบบกู้คืนกุญแจสามารถรองรับภัยคุกคามในอนาคตได้อย่างยั่งยืน โดยใช้อัลกอริธึมที่มีความแข็งแกร่ง เช่น การเข้ารหัสลับแบบอสมมาตรด้วย Kyber และ สร้างลายมือชื่อดิจิทัลด้วย Dilithium กับ Falcon [15]

3.2 ความหมายและความสำคัญของเทคโนโลยีการกู้คืนกุญแจลับ

3.2.1 ความหมายของเทคโนโลยีการกู้คืนกุญแจลับ

เทคโนโลยีการกู้คืนกุญแจลับ (Key Recovery Technology) หมายถึง ระบบหรือกระบวนการที่ออกแบบเพื่อให้สามารถเข้าถึงหรือกู้คืนกุญแจลับ ในกรณีที่กุญแจลับสูญหายหรือเสียหาย ส่งผลให้ไม่สามารถใช้งานถอดรหัสได้ และรองรับการกู้คืนกุญแจลับเพื่อการเข้าถึงข้อมูลที่ต้องการตรวจสอบอย่างถูกต้องตามกฎหมาย โดยใช้กลไกในการบริหารจัดการกุญแจที่มีความมั่นคงปลอดภัยสูง ยืดหยุ่น สามารถเข้าถึงข้อมูลสำคัญได้ในกรณีฉุกเฉิน และยังคงรักษาความเป็นส่วนตัว ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

3.2.2 ความสำคัญของเทคโนโลยีการกู้คืนกุญแจลับ

เทคโนโลยีการกู้คืนกุญแจลับ เป็นองค์ประกอบที่สำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูลในยุคดิจิทัล เนื่องจากช่วยให้ผู้ใช้งาน องค์กร หน่วยงานต่าง ๆ สามารถรับมือกับความเสี่ยงจากการสูญหายของกุญแจและเพิ่มความยืดหยุ่นในการจัดการกับภัยคุกคามที่มีต่อข้อมูลบนไซเบอร์ อีกทั้งยังช่วยสร้างความมั่นใจให้กับผู้ใช้งานระบบเครือข่ายดิจิทัล และส่งเสริมความยั่งยืนของการใช้เทคโนโลยี ทั้งนี้สามารถสรุปถึงความสำคัญได้ 6 ประการหลัก ๆ ดังต่อไปนี้

3.2.2.1 ช่วยกู้คืนกุญแจลับ ลดความเสี่ยงการสูญหายของกุญแจ

การกู้คืนกุญแจลับเกิดขึ้นได้ 2 กรณี คือ (1) กุญแจลับสูญหายหรือไม่สามารถใช้งานได้ และ (2) รองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย กล่าวคือเทคโนโลยีการกู้คืนกุญแจลับช่วยให้เกิดกระบวนการกู้คืนกุญแจเมื่อเกิดเหตุการณ์ดังกล่าวได้อย่างมั่นคงปลอดภัย (Security) และคงความเป็นส่วนตัว (Privacy) ของผู้ใช้งาน ลดความเสี่ยงจากการสูญหายของกุญแจลับ

3.2.2.2 สนับสนุนความต่อเนื่องของธุรกิจ

ช่วยลดความเสี่ยงที่ทำให้ธุรกิจหยุดชะงัก ทำให้องค์กรสามารถกู้คืนข้อมูลที่เข้ารหัสได้ในภาวะฉุกเฉิน เช่น ข้อมูลถูกทำลายจากผู้ประสงค์ร้าย หรือเกิดความผิดพลาดในการจัดการกุญแจ เป็นต้น

3.2.2.3 สร้างความมั่นคงปลอดภัยของข้อมูลเมื่อเกิดการโจมตีทางไซเบอร์

เนื่องจากการมีกลไกการกู้คืนกุญแจที่แข็งแกร่ง ช่วยให้สามารถรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพมากขึ้น เช่น การโจมตีแบบแรนซัมแวร์ (Ransomware) ที่มีการเข้ารหัสข้อมูลไว้ หากมีระบบกู้คืนกุญแจที่ดี ก็สามารถกู้คืนข้อมูลหรือปลดล็อกข้อมูลได้ โดยไม่จำเป็นต้องชำระเงินค่าไถ่ หรือยอมจำนนต่อผู้โจมตี

3.2.2.4 ช่วยจัดการการกู้คืนระบบในช่วงเวลาวิกฤต

ในกรณีที่ระบบเกิดความล้มเหลว เทคโนโลยีนี้ช่วยให้สามารถฟื้นฟูหรือกู้คืนข้อมูล ที่มีการเข้ารหัสไว้ได้อย่างถูกต้องและมีประสิทธิภาพ

3.2.2.5 ส่งเสริมความยั่งยืนของการใช้เทคโนโลยีสารสนเทศ เพิ่มความไว้วางใจในระบบดิจิทัล

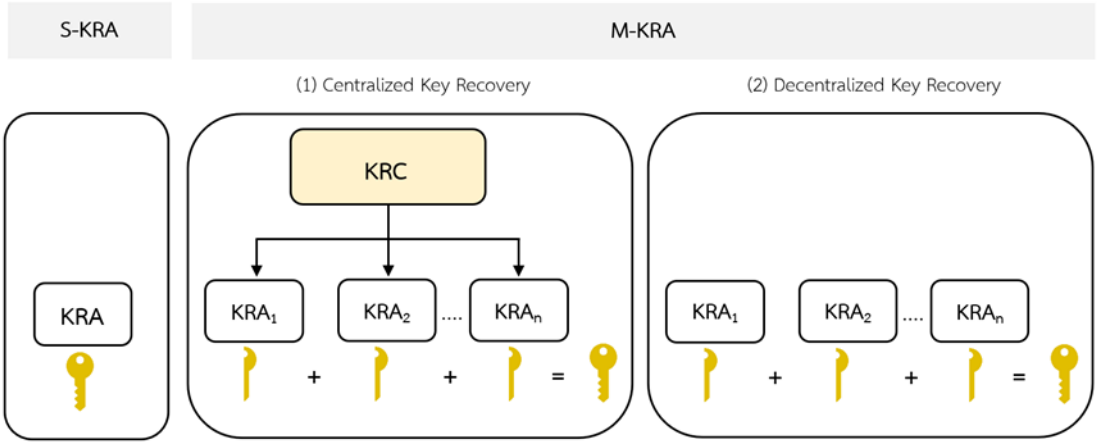
กล่าวคือเทคโนโลยีการกู้คืนกุญแจลับที่มีประสิทธิภาพ ช่วยสร้างความเชื่อมั่นให้กับผู้ใช้งานในบริบทต่าง ๆ ว่าข้อมูลที่ถูกจัดเก็บจะเป็นความลับ และมีหลักการบริหารจัดการที่มีความปลอดภัย แม้ในสถานการณ์ที่มีความเสี่ยงต่อภัยคุกคาม

3.2.2.6 สนับสนุนการปฏิบัติตามข้อกำหนดและกฎหมาย

การอุตสาหกรรมในหลายประเทศ มีกฎหมายหรือข้อกำหนดเกี่ยวกับการจัดการข้อมูล เช่น กฎหมายการคุ้มครองข้อมูลส่วนบุคคลของพลเมืองสหภาพยุโรป หรือ EU (General Data Protection Regulation : GDPR) ไม่ว่าจะเป็นการจัดการข้อมูลของประเทศสมาชิกภายในหรือภายนอก EU หรือกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act : PDPA) ซึ่งเมื่อมีกระบวนการกู้คืนกุญแจ จะช่วยให้สามารถปฏิบัติตามข้อกำหนดดังกล่าว ที่ให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคลได้ง่าย สะดวก ปลอดภัย และมีความโปร่งใสมากยิ่งขึ้น

3.3 รูปแบบการกู้คืนกุญแจลับ

จากการศึกษาเทคโนโลยีการกู้คืนกุญแจ สามารถแบ่งตามลักษณะการกู้คืนกุญแจได้ 2 รูปแบบ ดังแสดงในรูปที่ 1 และมีรายละเอียดดังต่อไปนี้



รูปที่ 1 รูปแบบการกู้คืนกุญแจลับ

3.3.1 รูปแบบที่ 1 การกู้คืนกุญแจแบบใช้เอเจนต์เดี่ยว (Single Key Recovery Agent: S-KRA)

กระบวนการทำงานของ S-KRA จะใช้เพียง 1 เอเจนต์ หรือใช้เอเจนต์เดี่ยว (Single Key Recovery Agent: S-KRA) ในการกู้คืนกุญแจ [16] เป็นการพัฒนาระบบที่เกิดขึ้นในช่วงเริ่มแรก มีกระบวนการทำงานที่ไม่ซับซ้อน ซึ่งต่อมาเกิดภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ และมีระดับความรุนแรงที่สามารถสร้างความเสียหายต่อระบบมากขึ้น [17] เช่น ความเสี่ยงจากความล้มเหลวในรูปแบบ Single Point of Failure (SPOF) การปฏิเสธการให้บริการ

(Denial of Service : DoS) หรือแม้กระทั่งการสมรู้ร่วมคิดของเอเจนต์ (Conspiracy) เป็นต้น ต่อมาการพัฒนาเทคโนโลยีในช่วงหลัง จึงได้ออกแบบส่วนการทำงานที่มีความมั่นคงปลอดภัยเพิ่มมากขึ้น ด้วยการให้เอเจนต์หลายเอเจนต์ (Multiple Key Recovery Agent : M-KRA) เก็บรักษาส่วนประกอบของกุญแจลับ และร่วมกันกู้คืน ทั้งนี้เพื่อลดความเสี่ยงต่อความเสียหายที่เกิดขึ้นกับ S-KRA

3.3.2 รูปแบบที่ 2 การกู้คืนกุญแจแบบใช้หลายเอเจนต์ (Multiple Key Recovery Agent : M-KRA)

M-KRA จะใช้เอเจนต์ตั้งแต่ 2 เอเจนต์ขึ้นไป ในการจัดเก็บส่วนประกอบของกุญแจลับ และร่วมกันกู้คืนกุญแจ โดยกระบวนการทำงานของ M-KRA มี 2 รูปแบบคือ

(1) M-KRA ที่อาศัย KRC หรือเรียกว่า การกู้คืนกุญแจแบบศูนย์กลาง (Centralized Key Recovery) [18] ในรูปแบบนี้ KRC มีหน้าที่ติดต่อประสานงานระหว่างเอเจนต์กู้คืนกุญแจ เพื่อทำหน้าที่ร่วมกันในการกู้คืนส่วนประกอบของกุญแจ

(2) M-KRA ที่ไม่อาศัย KRC หรือเรียกว่า การกู้คืนกุญแจแบบกระจายศูนย์ (Decentralized Key Recovery) [13] ในรูปแบบนี้ KRA จะทำงานร่วมกับผู้ร้องขอการกู้คืนกุญแจ โดยไม่มี KRC เป็นตัวกลางในการติดต่อประสานงาน

เมื่อเปรียบเทียบข้อดีและข้อเสียของการกู้คืนกุญแจแบบใช้หลายเอเจนต์ทั้งสองรูปแบบ ได้ผลลัพธ์ดังแสดงในตารางที่ 2

ตารางที่ 2 การเปรียบเทียบข้อดีและข้อเสียของการกู้คืนกุญแจแบบใช้หลายเอเจนต์

รูปแบบ	ข้อดี	ข้อเสีย
M-KRA ที่อาศัยศูนย์กลางในการกู้คืนกุญแจ	1. ระบบทำงานไม่ซับซ้อน 2. ยากต่อการปลอมแปลงของ KRA ในกลุ่มการกู้คืน	1. เมื่อ KRC เกิดข้อขัดข้องเสียหาย หรือได้รับความเสียหายจากภัยคุกคาม จะส่งผลให้ระบบล้มเหลวไม่สามารถให้บริการได้ (Single Point of Failure: SPOF) 2. จำเป็นต้องใช้งบประมาณในการบริหารจัดการ KRC ค่อนข้างสูง
M-KRA ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ	1. ระบบสามารถลดความเสี่ยงของการเกิดภัยคุกคามในรูปแบบ SPOF หรือ DoS 2. ไม่มีต้นทุนในส่วนการบริหารจัดการ KRC	1. การทำงานของระบบจะมีความซับซ้อนเพิ่มขึ้น 2. จำเป็นต้องมีฟังก์ชันการพิสูจน์ตัวจริงของ KRA ในกลุ่มการกู้คืนกุญแจที่รัดกุม

จากตารางที่ 2 สรุปได้ว่าการเลือกรูปแบบการกู้คืนกุญแจลับนั้น ขึ้นอยู่กับบริบทความจำเป็น และความต้องการความมั่นคงปลอดภัยขององค์กร หากเป็นองค์กรที่ต้องการความมั่นคงสูงเหมาะกับการใช้ M-KRA แบบกระจายศูนย์ (Decentralized) เพื่อลดความเสี่ยงจากการโจมตี ทั้งนี้ต้องมีกระบวนการพิสูจน์ตัวจริงที่รัดกุม ซึ่งอาจใช้แนวคิดของ Zero Trust Security (ZTS) [19] ที่ไม่ไว้วางใจผู้ใช้หรืออุปกรณ์ใด ๆ โดยอัตโนมัติ แม้ว่าจะอยู่ในเครือข่ายองค์กรเดียวกัน แต่จะมีการตรวจสอบตัวตนและสิทธิ์การร้องขอการกู้คืนกุญแจทุกครั้ง หรือใช้หลักการ Multi-Factor Authentication (MFA) [20] ซึ่งเป็นการยืนยันตัวตนแบบหลายขั้นตอน เพื่อให้แน่ใจว่าผู้ใช้มีสิทธิ์เท่านั้นที่สามารถกู้คืนกุญแจได้

3.4 องค์ประกอบของเทคโนโลยีการกู้คืนกุญแจลับ

เทคโนโลยีการกู้คืนกุญแจลับมีองค์ประกอบ 3 ส่วนที่สำคัญในการทำงานร่วมกัน เพื่อกู้คืนกุญแจลับและรองรับการเข้าถึงข้อมูล โดยมีโครงสร้างของแต่ละองค์ประกอบดังนี้

3.4.1 ส่วนความมั่นคงปลอดภัยของผู้ใช้งาน (User Security Component: USCn) มีบทบาทและหน้าที่ในการจัดการเรื่องความสามารถในการเข้ารหัสลับและถอดรหัสลับข้อมูล รวมทั้งสนับสนุนการกู้คืนกุญแจ ซึ่งจะมีการแนบฟิลด์ที่ใช้ในการกู้คืนกุญแจ (Data Recovery Field: DRF หรือ Key Recovery Field: KRF) ไปกับข้อมูลที่ผ่านการเข้ารหัสลับแล้ว (Ciphertext) USCn ทำหน้าที่เป็นส่วนที่เชื่อมต่อผู้ใช้งานกับระบบกู้คืนกุญแจ เพื่อให้มั่นใจว่าข้อมูลที่เข้ารหัสสามารถกู้คืนได้อย่างปลอดภัย

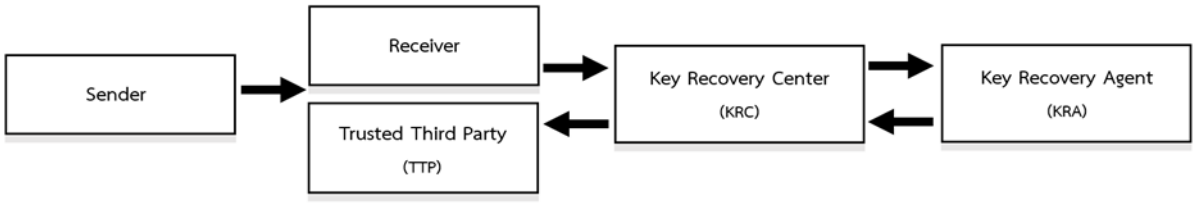
3.4.2 ส่วนหน่วยงานกู้คืนกุญแจ (Recovery Agent Component: RACn) ทำหน้าที่จัดการกุญแจลับรวมถึงการเก็บรักษาและการกู้คืนกุญแจในกรณีที่กุญแจสูญหายหรือไม่สามารถใช้งานได้ ประกอบด้วยศูนย์กลางการกู้คืนกุญแจ (KRC) และ/หรือ หน่วยงานกู้คืนกุญแจ (KRA) อาจมีการใช้ระบบการบริหารจัดการใบรับรองกุญแจสาธารณะ (Public Key Certificate) หรือใช้โครงสร้างพื้นฐานการบริหารจัดการกุญแจทั่วไป (General Key Management Infrastructure) ร่วมด้วยเพื่อสนับสนุนการดำเนินงาน

3.4.3 ส่วนการกู้คืนข้อมูล (Data Recovery Component: DRCn) ประกอบด้วยอัลกอริทึม โปรโตคอล และกระบวนการที่ช่วยให้ได้กุญแจลับจาก DRF หรือ KRF ที่แนบมากับข้อมูลเข้ารหัส เพื่อนำกุญแจที่ได้ไปถอดรหัสลับข้อมูล โดยกระบวนการนี้จะอนุญาตเฉพาะผู้ที่มีสิทธิ์ในการกู้คืนกุญแจเท่านั้น

3.5 ส่วนประกอบของกระบวนการการกู้คืนกุญแจลับ

เทคโนโลยีการกู้คืนกุญแจลับ เป็นการเข้ารหัสด้วยกุญแจลับที่อาศัยความสามารถของการสำรอง (Backup) ข้อมูลบางส่วนของกุญแจ เพื่อนำมาใช้ในการถอดรหัสลับ โดยอาศัยความไว้วางใจ (Trust) ยอมให้สิทธิ์ในการเข้าถึงข้อมูลดังกล่าวกับ TTP ซึ่งกระบวนการกู้คืนกุญแจลับต้องดำเนินการภายใต้นโยบายหรือกฎหมายที่แน่นอน บุคคลที่สามารถร้องขอการกู้คืนกุญแจและมีสิทธิ์เข้าถึงข้อมูลกุญแจ คือผู้ที่เป็นเจ้าของกุญแจ หรือหน่วยงาน/บุคลากรของรัฐบาลที่มีสิทธิ์ในการตรวจสอบข้อมูลที่ส่งผ่านระบบเครือข่ายโดยชอบด้วยกฎหมาย

กระบวนการกู้คืนกุญแจลับ ที่ทำงานภายใต้เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure : PKI) มีส่วนประกอบ 4 ส่วนหลัก ๆ ดังแสดงในรูปที่ 2 ซึ่งประกอบด้วย



รูปที่ 2 ส่วนประกอบของกระบวนการกู้คืนกุญแจลับ

ส่วนที่ 1 ผู้ส่ง (Sender) มีหน้าที่

(1) สร้างข้อมูลต้นฉบับ เพื่อส่งให้กับผู้รับ

(2) สร้างฟิลด์ที่เก็บ KRF เพื่อใช้ในการกู้คืนกุญแจในภายหลัง

(3) แนบฟิลด์ KRF เข้ากับข้อความต้นฉบับ ส่งไปยังผู้รับทุกครั้งของการสนทนาสื่อสาร

ส่วนที่ 2 ผู้รับ (Receiver)/TTP ในกรณีผู้รับกุญแจลับสูญหายหรือไม่สามารถใช้ถอดรหัสข้อความต้นฉบับได้ หรือ TTP ต้องการกุญแจในการถอดรหัสข้อมูลเพื่อการตรวจสอบ มีหน้าที่

(1) ร้องขอการกู้คืนส่วนประกอบของกุญแจ หรือ การกู้คืนกุญแจลับ ไปยัง KRC หรือ KRA ขึ้นอยู่กับรูปแบบการให้บริการ

(2) บางครั้งอาจทำหน้าที่คำนวณข้อมูลกุญแจลับ เมื่อได้รับข้อมูลส่วนประกอบของกุญแจครบถ้วนจาก KRC หรือ KRA

ส่วนที่ 3 ศูนย์กลางในการกู้คืนกุญแจ (KRC) มีหน้าที่

(1) บริการจัดการกุญแจ และ KRA กล่าวคือ เป็นศูนย์กลางในการกู้คืนกุญแจ และเชื่อมต่อประสานงานระหว่างผู้ร้องขอการกู้คืนกุญแจ กับ KRA

(2) ทำการรวบรวมส่วนประกอบของกุญแจลับ หรือกู้คืนกุญแจ ทั้งนี้เป็นไปตามฟังก์ชันการให้บริการ

ส่วนที่ 4 เอเจนต์ที่ให้บริการกู้คืนกุญแจ (KRA) มีหน้าที่

(1) กู้คืนส่วนประกอบของกุญแจลับ เมื่อได้รับการร้องขอการกู้คืนกุญแจจากผู้ร้องขอ

(2) จัดส่งส่วนประกอบของกุญแจที่ถูกต้องไปให้ผู้ร้องขอ เพื่อทำการกู้คืนกุญแจในขั้นตอนสุดท้าย

3.6 ขั้นตอนการกู้คืนกุญแจลับ

กระบวนการกู้คืนกุญแจลับเป็นขั้นตอนสำคัญในระบบความมั่นคงปลอดภัยของสารสนเทศ เพื่อให้สามารถเข้าถึงข้อมูลที่เข้ารหัสไว้ได้ แม้ในกรณีที่กุญแจสูญหาย หรือมีความจำเป็นต้องเข้าถึงข้อมูลตามข้อกำหนด อย่างไรก็ตามในขั้นตอนนี้ต้องมีมาตรการควบคุมที่เหมาะสม เพื่อจะไม่เป็นการละเมิดความเป็นส่วนตัวของผู้ใช้งาน โดยการกู้คืนกุญแจลับ มีลำดับขั้นตอนดังต่อไปนี้

3.6.1 การเตรียมข้อมูลและการสร้างฟิลด์ที่จัดเก็บ KRF (หน้าที่ของผู้ส่ง) ทั้งนี้ทำงานบนพื้นฐานของ PKI มีลำดับดังนี้

3.6.1.1 เตรียมข้อมูลต้นฉบับ (Plaintext) และสร้าง KRF เพื่อรองรับการกู้คืนกุญแจเมื่อจำเป็น

3.6.1.2 ส่งข้อมูลต้นฉบับไปพร้อมกับฟิลด์ KRF

3.6.2 การร้องขอการกู้คืนกุญแจ (หน้าที่ของผู้รับ หรือหน่วยงานที่มีสิทธิ์ในการเข้าถึงกุญแจ)

3.6.2.1 หากกุญแจสูญหายหรือไม่สามารถใช้บริการได้ จะมีการร้องขอการกู้คืนกุญแจ

3.6.2.2 ส่ง KRF ไปยัง KRC หรือ KRA ขึ้นอยู่กับรูปแบบของการให้บริการ

3.6.3 การรวบรวมส่วนประกอบของกุญแจ และการกู้คืนกุญแจ มีกระบวนการทำงาน 2 รูปแบบ คือ

รูปแบบที่ 1 กระบวนการกู้คืนกุญแจที่อาศัย KRC (หน้าที่ของ KRC และ KRA)

(1) เมื่อ KRC ได้รับคำร้องขอกู้คืนกุญแจ พร้อมกับ KRF จะมีการตรวจสอบสิทธิ์ในการเข้าถึงกุญแจในเบื้องต้น จากนั้นจะร้องขอส่วนประกอบกุญแจไปยัง KRA ที่เกี่ยวข้อง

(2) เมื่อ KRA ได้รับคำร้องขอส่วนประกอบของกุญแจ จะมีกระบวนการพิสูจน์ตัวจริง และจัดส่งส่วนประกอบของกุญแจไปให้กับ KRC

(3) จากนั้น KRC ทำการรวบรวมส่วนประกอบของกุญแจจาก KRA เมื่อรวบรวมได้ครบถ้วนสมบูรณ์แล้ว จะคำนวณกุญแจลับ ส่งให้กับผู้ร้องขอต่อไป

อย่างไรก็ตามการออกแบบกระบวนการกู้คืนกุญแจของรูปแบบนี้ สามารถมอบหมายให้ผู้ร้องขอการกู้คืน ทำหน้าที่ในการกู้คืนกุญแจลับด้วยตนเอง เพื่อเพิ่มความปลอดภัยและความเป็นส่วนตัวมากยิ่งขึ้น

รูปแบบที่ 2 กระบวนการกู้คืนกุญแจที่ไม่อาศัย KRC (หน้าที่ของ KRA และผู้ร้องขอการกู้คืนกุญแจ)

(1) เมื่อ KRA ได้รับคำร้องขอกู้คืนกุญแจ พร้อมกับ KRF จะมีการตรวจสอบสิทธิ์ในการเข้าถึงกุญแจ และส่งส่วนประกอบกุญแจไปยังผู้ร้องขอ

(2) ผู้ร้องขอรวบรวมส่วนประกอบของกุญแจจนครบ และทำการคำนวณกุญแจลับ เพื่อนำไปใช้ในการถอดรหัสข้อมูล

3.7 โครงสร้างฟิลด์ในการกู้คืนกุญแจ (KRF)

การจัดเก็บกุญแจลับเพื่อรองรับการกู้คืนกุญแจ มีการออกแบบโครงสร้างโดยคำนึงถึงความมั่นคงปลอดภัย ความยืดหยุ่น ความน่าเชื่อถือ ความเป็นส่วนตัว และความสามารถในการกู้คืนกุญแจ เพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ ซึ่งในเทคโนโลยีแบบ M-KRA จะแบ่งกุญแจออกเป็นส่วนย่อย ๆ ตามจำนวน KRA ที่ใช้สำหรับการกู้คืน โดยจัดเก็บไว้ในฟิลด์ KRF โดยโครงสร้าง KRF ที่มีความมั่นคงปลอดภัยสูง ควรประกอบไปด้วยข้อมูลที่จำเป็น ดังแสดงในรูปที่ 3 และมีรายละเอียดดังต่อไปนี้

รูปที่ 3 โครงสร้างฟิลด์ในการกู้คืนกุญแจ (KRF)

3.7.1 ส่วนประกอบของกุญแจลับ ที่มีการกระจายในลักษณะการแชร์ความลับ (Secret Sharing)

3.7.2 แอตทริบิวต์สำหรับการยืนยันตัวตนของ KRA ที่อยู่ในกลุ่มการกู้คืน หรือการกำหนดสิทธิ์การเข้าถึง KRF โดยใช้ รายการควบคุมการเข้าถึง (Access Control List) หรือการควบคุมสิทธิ์การเข้าถึงตามบทบาทหน้าที่ (Role-Based Access Control)

3.7.3 แอตทริบิวต์สำหรับการกู้คืนส่วนประกอบของกุญแจ ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล่ม หรือมีกลไกสำรอง (Failover Mechanism) ที่สามารถกำหนดจำนวน KRA ว่าต้องมีอย่างน้อย n จาก m เอเจนต์ ในการกู้คืนกุญแจ (Multi-Agent Consensus)

3.7.4 ข้อมูลที่จำเป็นอื่น ๆ สำหรับการตรวจสอบหรือการพิสูจน์ตัวจริงของผู้ที่เกี่ยวข้องในการสื่อสาร เพื่อเพิ่มความมั่นคงปลอดภัย และความน่าเชื่อถือของการสื่อสาร เช่น ข้อมูลใบรับรองกุญแจสาธารณะของเอเจนต์ และของผู้ที่มีสิทธิ์ในการร้องขอการกู้คืนกุญแจ เป็นต้น

อย่างไรก็ตามประเด็นการพิสูจน์ว่า KRF มีความสมบูรณ์ไม่ถูกเปลี่ยนแปลงแก้ไขเป็นเรื่องที่ต้องให้ความสำคัญ โดยสามารถใช้ระบบบันทึกแบบป้องกันการปลอมแปลง (Immutable Logging) [21] ซึ่งเป็นวิธีบันทึกข้อมูลที่ไม่สามารถลบ แก้ไข หรือดัดแปลงได้ เพื่อให้แน่ใจว่าเป็นข้อมูลเดิมแท้ (Integrity) และสามารถใช้เป็นหลักฐานในการตรวจสอบย้อนหลัง (Audit Trail) ที่เชื่อถือได้ ทั้งนี้ทุกการร้องขอและการกู้คืนกุญแจควรได้รับการบันทึกในระบบเพื่อการตรวจสอบ

4. การวิเคราะห์และสังเคราะห์แนวทางการพัฒนาเทคโนโลยีการกู้คืนกุญแจลับ

เทคโนโลยีการกู้คืนกุญแจลับมีการพัฒนาอย่างต่อเนื่อง เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีหลากหลายรูปแบบ และเพื่อสนับสนุนรองรับเทคโนโลยีใหม่ ๆ ในด้านความปลอดภัย ตลอดจนนำไปประยุกต์ใช้ในงานส่วนต่าง ๆ ตั้งแต่การรักษาความปลอดภัยของข้อมูลในองค์กร การปกป้องข้อมูลส่วนบุคคล และการบังคับใช้ในทางกฎหมาย เป็นต้น ดังกรณีตัวอย่างของการนำไปประยุกต์ใช้ดังนี้

กรณีที่ 1 งานการเงินและธนาคาร

ธนาคารพาณิชย์ระดับสากลมักใช้ระบบ Enterprise Key Management (EKM) ร่วมกับเทคโนโลยีการกู้คืนกุญแจ เพื่อให้สามารถเข้าถึงข้อมูลลูกค้า กรณีที่กุญแจลับที่ใช้เข้ารหัสสูญหาย ระบบจะกำหนดให้มีหน่วยงานกู้คืนที่เชื่อถือได้ (Trusted Recovery Agent: TRA) ทำงานภายใต้เงื่อนไขความปลอดภัยที่กำหนดไว้ เช่น การได้รับอนุมัติจากฝ่ายกฎหมาย และฝ่ายควบคุมความเสี่ยงก่อน จึงดำเนินการกู้คืนกุญแจลับและสามารถเข้าถึงข้อมูลได้

กรณีที่ 2 งานสาธารณสุข

โรงพยาบาลขนาดใหญ่ในหลายประเทศ เช่น สหรัฐอเมริกา และในยุโรป ได้นำแนวคิดการกู้คืนกุญแจลับมาใช้ร่วมกับ Health Information Systems (HIS) เพื่อปกป้องข้อมูลผู้ป่วย ในกรณีระบบฐานข้อมูลหรือรหัสผ่านถูกลืมหรือถูกโจมตี โดยใช้โครงสร้างแบบ M-KRA ที่ให้ฝ่ายงานสารสนเทศ ฝ่ายกฎหมาย และหัวหน้าหน่วยข้อมูล ต้องทำงานร่วมกัน จึงจะสามารถกู้คืนและเข้าถึงข้อมูลได้

อย่างไรก็ตามแนวทางการพัฒนาเทคโนโลยีนี้ในอนาคต ต้องมุ่งเน้นไปที่การแก้ปัญหาจุดอ่อนของเทคโนโลยี คือ ประเด็นความเสี่ยงของภัยคุกคามทางไซเบอร์ที่มีความรุนแรงและซับซ้อนมากขึ้น การพิสูจน์ตัวตนในกระบวนการกู้คืนกุญแจที่ต้องมีความรัดกุม สอดคล้องกับกฎหมายความปลอดภัย และเคารพสิทธิความเป็นส่วนตัวของผู้ใช้งาน

ทั้งนี้การนำเทคโนโลยีที่ทันสมัยมาพัฒนาส่วนการกู้คืนกุญแจ จะทำให้เกิดความยืดหยุ่น สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ พร้อมกับสร้างความเชื่อมั่นให้ผู้ใช้งานในยุคดิจิทัล โดยแนวทางในการพัฒนาเทคโนโลยีการกู้คืนกุญแจลับในอนาคต สามารถสรุปได้ดังต่อไปนี้

4.1 การนำปัญญาประดิษฐ์ (AI: Artificial Intelligence) และการเรียนรู้ของเครื่อง (ML: Machine Learning) มาใช้ในกระบวนการกู้คืนกุญแจลับ เพื่อให้การกู้คืนกุญแจมีความปลอดภัย เกิดความยืดหยุ่นตามการร้องขอกู้คืน โดยให้ AI ตรวจจับความผิดปกติและวิเคราะห์พฤติกรรมการร้องขอ ซึ่งจะอาศัยข้อมูลทางสถิติและรูปแบบพฤติกรรมที่เกิดขึ้นในอดีต (Anomaly Detection & Behavioral Analytics) โดยอาจใช้โมเดล Anomaly Detection หรือ Decision Tree ในการวิเคราะห์พฤติกรรมแบบเรียลไทม์ [22] ทั้งนี้เพื่อลดความเสี่ยงของภัยคุกคามทางไซเบอร์

4.2 การออกแบบโมเดลการกู้คืนกุญแจแบบผสมผสาน (Hybrid Model) เพื่อเพิ่มความมั่นคงปลอดภัยในกระบวนการกู้คืนกุญแจ เป็นการทำงานในรูปแบบ M-KRS ที่ใช้หลักการผสาน Zero Trust Security (ZTS) [19] โดยกำหนดให้มีการตรวจสอบตัวตนทุกครั้ง เข้ากับ Multi-Agent Authentication หรือการพิสูจน์ตัวตนแบบใช้หลายเอเจนต์ และ AI-Based Security [23] ที่ใช้ AI ในการตรวจจับพฤติกรรมผิดปกติ (Anomaly Detection) มุ่งเน้นที่การเรียนรู้รูปแบบพฤติกรรมปกติของระบบหรือผู้ใช้งาน และตรวจจับความเบี่ยงเบนที่อาจบ่งชี้ถึงภัยคุกคามหรือการโจมตี และ Blockchain Logging [24] ที่ใช้เทคโนโลยีบล็อกเชนในการบันทึกข้อมูล (Blockchain Logging) ช่วยให้สามารถสร้างระบบบันทึกที่ไม่สามารถแก้ไขย้อนหลังได้ ช่วยให้สามารถตรวจจับการปลอมแปลงข้อมูล และสร้างความน่าเชื่อถือในระบบรักษาความปลอดภัยของข้อมูลได้อย่างมีประสิทธิภาพสูงสุด และลดช่องโหว่จากภัยคุกคามได้

4.3 พัฒนาการกู้คืนกุญแจที่ไม่ละเมิดสิทธิ์ของผู้ใช้ และปกป้องข้อมูลจากการเข้าถึงโดยมิชอบ (Privacy-Preserving Key Recovery) โดยใช้การเข้ารหัสลับขั้นสูง เช่น Homomorphic Encryption (HE) [25] ซึ่งเป็นเทคนิคที่ช่วยให้สามารถคำนวณหรือประมวลผลข้อมูลที่ถูกเข้ารหัส โดยไม่จำเป็นต้องถอดรหัส กล่าวคือ ระบบสามารถตรวจสอบสิทธิ์ของผู้ร้องขอการกู้คืนกุญแจลับว่าเป็นผู้ที่มีสิทธิ์นั้นหรือไม่ ทั้งนี้จะขึ้นอยู่กับเงื่อนไขการตรวจสอบ เช่น

การตรวจสอบลายเซ็นดิจิทัล การพิสูจน์ตัวตนจากใบรับรองกุญแจ หรือเงื่อนไขการเข้าถึงโดยที่จำเป็นต้องเข้าถึงข้อมูลที่แท้จริง และใช้กระบวนการตรวจสอบหลายระดับ เพื่อให้มั่นใจว่าการกู้คืนกุญแจมีความมั่นคงปลอดภัย และมีความเป็นส่วนตัวสูงสุด

ถือได้ว่าการนำเทคโนโลยีการกู้คืนกุญแจลับมาใช้เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูลและการสื่อสาร เป็นแนวทางที่มีความจำเป็นและสำคัญ ในการพัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยในยุคดิจิทัลอย่างยั่งยืน

5. บทสรุป

เทคโนโลยีการกู้คืนกุญแจลับ (Key Recovery Technology) มีความสำคัญในการเสริมสร้างความมั่นคงด้านความปลอดภัยของข้อมูลในยุคดิจิทัล โดยช่วยป้องกันและแก้ไขปัญหา 2 ประเด็นคือ (1) การสูญหายของกุญแจลับหรือกุญแจลับใช้งานไม่ได้ (2) รองรับการเข้าถึงข้อมูลที่ต้องสงสัยโดยชอบด้วยกฎหมาย ทำให้สามารถเข้าถึงข้อมูลสำคัญที่ถูกเข้ารหัสไว้ได้อย่างปลอดภัย โดยไม่ละเมิดความลับและความเป็นส่วนตัวของผู้ใช้งาน อีกทั้งยังมีความสอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR) [26] และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act B.E. 2562: PDPA) [27] ซึ่งกำหนดให้ผู้ควบคุมข้อมูล ต้องจัดให้มีมาตรการที่เหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงต้องสามารถกู้คืนข้อมูลและกุญแจที่เกี่ยวข้องในกรณีฉุกเฉินอย่างปลอดภัยและตรวจสอบได้ เพื่อให้ตอบโจทย์ด้านกฎหมายและจริยธรรมได้อย่างสมบูรณ์ ลดความเสี่ยงจากการถูกดำเนินคดี และสร้างความโปร่งใสในการจัดการข้อมูล

เทคโนโลยีการกู้คืนกุญแจ สามารถแบ่งตามลักษณะการกู้คืนได้ 2 รูปแบบ คือ (1) การกู้คืนกุญแจแบบใช้เอเจนต์เดี่ยว และ(2) การกู้คืนกุญแจแบบใช้หลายเอเจนต์ ซึ่งในยุคปัจจุบันนิยมใช้รูปแบบที่ 2 เนื่องจากมีประสิทธิภาพด้านความมั่นคงปลอดภัยสูงกว่า ส่วนกระบวนการกู้คืนกุญแจลับนั้น แบ่งได้เป็น 4 ขั้นตอน คือ ขั้นตอนที่ 1 เป็นหน้าที่ของผู้ส่ง ในการเตรียมข้อมูลและการสร้างฟิลด์ KRF ขั้นตอนที่ 2 จะเกิดขึ้นในกรณีที่ต้องการร้องขอรับบริการกู้คืนกุญแจ โดยผู้รับหรือหน่วยงานที่มีสิทธิ์ในการเข้าถึงกุญแจ จะร้องขอไปยังส่วนที่ทำหน้าที่ให้บริการกู้คืน คือ KRC หรือ KRA ขั้นตอนที่ 3 และ 4 หน่วยงาน KRC หรือ KRA จะทำหน้าที่รวบรวมส่วนประกอบของกุญแจ และกู้คืนกุญแจ ตามฟังก์ชันงานที่ได้รับมอบหมายหรือกำหนดในระบบตามลำดับ

การกู้คืนกุญแจลับที่ออกแบบมาอย่างมั่นคงปลอดภัยและมีความยืดหยุ่น ช่วยให้องค์กรสามารถรับมือกับเหตุการณ์ฉุกเฉินหรือภัยคุกคามที่เกิดขึ้นได้ เช่น การโจมตีทางไซเบอร์ สามารถฟื้นฟูข้อมูลที่เสียหาย ลดความเสียหายทางธุรกิจ เพิ่มความน่าเชื่อถือให้กับระบบดิจิทัล และทำให้การดำเนินงานมีความต่อเนื่องแม้ในสภาพแวดล้อมที่มีความเสี่ยงจากภัยคุกคามสูง นอกจากนี้ยังช่วยปกป้องข้อมูลให้มีความมั่นคงปลอดภัย และลดผลกระทบต่อโครงสร้างพื้นฐานขององค์กรด้วยกระบวนการกู้คืนที่น่าเชื่อถือ ส่งผลให้เทคโนโลยีนี้เป็นกลไกสำคัญในการสร้าง ความมั่นคงปลอดภัยและความยั่งยืนในโลกดิจิทัล

แนวทางการพัฒนาในอนาคตควรมุ่งเน้นไปที่การใช้เทคโนโลยีปัญญาประดิษฐ์ และการเรียนรู้ของเครื่อง การออกแบบโมเดลการกู้คืนกุญแจแบบผสมผสาน เพื่อเพิ่มความมั่นคงปลอดภัยในกระบวนการกู้คืนกุญแจ และการใช้เทคนิคการเข้ารหัสลับขั้นสูงในการพัฒนาการกู้คืนกุญแจที่ไม่ละเมิดสิทธิ์ของผู้ใช้ และปกป้องข้อมูลจากการเข้าถึงโดยมิชอบ เพื่อให้กระบวนการกู้คืนกุญแจมีความปลอดภัยและมีประสิทธิภาพมากขึ้น การพัฒนามาตรฐานสากลด้านการกู้คืนกุญแจ (Key Recovery) จะช่วยให้เทคโนโลยีนี้ สามารถนำไปใช้ได้อย่างกว้างขวาง และมีความน่าเชื่อถือในระดับองค์กรและระดับโลก

6. เอกสารอ้างอิง

[1] W. Stallings, *Cryptography and Network Security Principles & Practice*, 8th ed. Pearson, 2023.

[2] กนกวรรณ กันยะมี และ จำรูญ จันทร์กุญชร, "การเพิ่มความมั่นคงในการบริหารจัดการกุญแจลับสำหรับการกู้คืนกุญแจแบบหลายเอเจนต์ที่อาศัยศูนย์กลางในการกู้คืนกุญแจ," *วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย ฉบับวิทยาศาสตร์และเทคโนโลยี*, ปีที่ 18, ฉบับที่ 2, หน้า 171-183, พฤษภาคม-สิงหาคม, 2567.

[3] National Institute of Standards and Technology, "*Requirements for Key Recovery Products*." [Online]. Available: https://csrc.nist.rip/tacdfipsfkmi/finalrpt.pdf (Accessed: June 10, 2024).

[4] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Boston, MA, USA: Pearson Education, 2017.

[5] National Institute of Standards and Technology (NIST), *NIST Cybersecurity Practice Guide: Data Integrity – Detecting and Responding to Ransomware and Other Destructive Events*, NIST Special Publication 1800-26, Gaithersburg, MD, USA, 2020.

[6] D. E. Denning, "The US Key Escrow Encryption Technology," *Computer Communications*, vol. 17, no. 7, pp. 453-457, July, 1994.

[7] M. Blaze, "Protocol Failure in the Escrowed Encryption Standard," in *2nd ACM Conference on Computer and Communications Security*, Fairfax Virginia USA, 1994, pp. 59-67.

[8] H. S. Dakoff, "The Clipper Chip Proposal: Deciphering the Unfounded Fears That Are Wrongfully Derailing Its Implementation," *John Marshall Law Review*, vol. 29, no. 2, pp. 475–530, 1996.

[9] A. Shamir, “How to share a secret,” *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, November, 1979.

[10] S. Lim, S. Kang, and J. Sohn, "Modeling of multiple agent based cryptographic key recovery protocol," in *19th Annual Computer Security Applications Conference*, Las Vegas, NV, USA, 2003, pp. 119-128.

[11] S. Han, S. Liu, and D. Gu, "Key encapsulation mechanism with tight enhanced security in the multi-user setting: Impossibility result and optimal tightness," in *27th International Conference on the Theory and Application of Cryptology and Information Security*, Singapore, 2021, pp. 483-513

[12] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA), "*เทคโนโลยีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI)*," [ออนไลน์]. Available: https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/articles/Public-Key-Infrastructure.aspx (เข้าถึงเมื่อ: 13 พ.ย. 2567).

[13] K. Kanyamee and C. Sathitwiriyawong, "High-availability decentralized multi-agent key recovery system," in *2009 Eighth IEEE/ACIS International Conference on Computer and Information Science*, Shanghai, China, 2009, pp. 290–294.

[14] National Institute of Standards and Technology (NIST), "*Post-Quantum Cryptography Standardization*," [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography. (Accessed: April. 20, 2025).

[15] D. J. Bernstein, J. Buchmann and E. Dahmen, *Post-Quantum Cryptography*, Berlin, Germany: Springer, 2009.

[16] Y.-C. Lee and C.-S. Laih, "On the key recovery of the key escrow system," in *13th Annual Computer Security Applications Conference*, California, USA, 1997, pp. 216-220.

[17] A. Kundu, N. Ghosh, I. Chokshi, and S. K. Ghosh, "Analysis of attack graph-based metrics for quantification of network security," in *2012 Annual IEEE India Conference (INDICON)*, India, 2012, pp. 530-535.

[18] K. Kanyamee and C. Sathitwiriyawong, "A secure multiple-agent cryptographic key recovery system," in *IEEE International Conference on Information Reuse & Integration (IRI)*, Las Vegas, NV, USA, 2009, pp. 91-96.

[19] R. N'goran, A. P. B. Brou, K. G. Pandry, J.-L. Tetchueng, Y. Kermarrec, and O. Asseu, "Zero Trust security strategy for collaboration systems," in *2023 International Symposium on Networks, Computers and Communications (ISNCC)*, Doha, Qatar, 2023, pp. 1-6.

[20] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, pp. 1-31, January, 2018.

[21] A. Aßmuth, R. Duncan, S. Liebl, and M. Söllner, "A secure and privacy-friendly logging scheme," in *Twelfth International Conference on Cloud Computing*, GRIDs, and Virtualization, Portugal, 2021, pp. 8-12.

[22] A. A. Wighneswara, A. Sjahrunnisa, Y. Romadhona, and K. I. Maula, "Network Behavior Anomaly Detection using Decision Tree," in *IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT)*, India, 2023, pp.1-6.

[23] M. J. Goswami, "AI-Based Anomaly Detection for Real-Time Cybersecurity," *International Journal of Research and Review Techniques (IJRRT)*, vol. 3, no. 1, pp. 45-53, Mar. 2024.

[24] T. H. Austin and F. Di Troia, "A Blockchain-Based Tamper-Resistant Logging Framework," in *Silicon Valley Cybersecurity Conference*, Virtual Event, 2022, pp. 90-104.

[25] J. Shen, Y. Zhao, S. Huang, and Y. Ren, "Secure and flexible privacy-preserving federated learning based on multi-key fully homomorphic encryption," *Electronics*, vol. 13, no. 22, November, 2024.

[26] European Parliament and Council of the European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Official Journal of the European Union, L 119, May 4, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Accessed: April, 13, 2025).

[27] สำนักเลขาธิการคณะรัฐมนตรี, *"พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562,"* [ออนไลน์]. Available: https://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF. (เข้าถึงเมื่อ:13 เมษายน 2567).