วารสารวิชาการวิทยาศาสตร์
มหาวิทยาลัยราชภัฏจันทรเกษม

การเปรียบเทียบประสิทธิภาพของระบบกู้คืนกุญแจลับแบบหลายเอเจนต์ที่ไม่อาศัยศูนย์กลาง ระหว่าง IHADM-KRS และ SSDM-KRS

A Comparative Study on the Performance of Decentralized Multi-Agent Key Recovery Systems between IHADM-KRS and SSDM-KRS

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

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

[1] หลักสูตรเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏอุตรดิตถ์

[1] Information Technology Program, Faculty of Science and Technology, Uttaradit Rajabhat University

บทคัดย่อ

การจัดการความเสี่ยงของกุญแจลับจากการถูกโจมตีหรือสูญหาย เป็นประเด็นสำคัญต่อการ รักษาความมั่นคงปลอดภัยของข้อมูล โดยระบบกู้คืนกุญแจ (Key Recovery System : KRS) ถือเป็นเทคโนโลยีหนึ่งที่ถูกพัฒนาขึ้นเพื่อลดความเสี่ยงดังกล่าว งานวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์และเปรียบเทียบประสิทธิภาพ ของระบบกู้คืนกุญแจลับแบบหลายเอเจนต์ (Multiple Key Recovery System) 2 รูปแบบ คือ SSDM-KRS และ IHADM-KRS โดยเน้นการประเมินประสิทธิภาพใน 3 กระบวนการหลัก ได้แก่ (1) การสร้างฟิลด์ในการกู้คืนกุญแจ (Key Recovery Filed : KRF) (2) การกู้คืนกุญแจในกรณีปกติ และ(3) การกู้คืนกุญแจในกรณีที่มีเอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent : KRA) ล่มหรือไม่สามารถให้บริการได้ การวิจัยได้จำลองการทำงานของ KRA ตั้งแต่ 5 ถึง 50 เอเจนต์ โดยกำหนดเกณฑ์การกู้คืนขั้นต่ำที่ 2 เอเจนต์ ผลการประเมินประสิทธิภาพในการสร้าง KRF พบว่า SSDM-KRS มีข้อได้เปรียบด้านความเร็วมากกว่า IHADM-KRS เนื่องจากโครงสร้างไม่ซับซ้อน ในขณะที่ IHADM-KRS มีความยืดหยุ่นในการบริหารจัดการ KRA และมีความมั่นคงปลอดภัยสูงกว่า SSDM-KRS ส่วนการกู้คืนกุญแจลับในสถานการณ์ปกติที่ไม่มี KRA ล่มนั้น ทั้งสองระบบใช้เวลาในการกู้คืนใกล้เคียงกัน อย่างไรก็ตามเมื่อทดลองกู้คืนกุญแจในกรณีที่มี KRA ล่ม พบว่า IHADM-KRS มีศักยภาพในการกู้คืนที่เสถียร มีความมั่นคงปลอดภัยสูง แต่ใช้เวลามากกว่า SSDM-KRS โดยเฉพาะเมื่อจำนวน KRA เพิ่มขึ้น ผลการวิจัยแสดงให้เห็นว่า การเลือกใช้ระบบกู้คืนกุญแจที่เหมาะสมควรพิจารณาให้สอดคล้องกับความต้องการด้านประสิทธิภาพ และนโยบายความมั่นคงปลอดภัย ทั้งนี้ระบบทั้งสองรูปแบบได้รับการออกแบบให้สามารถต้านทานการสมรู้ร่วมคิดของ KRA และมีความแข็งแกร่งทนทานต่อความล้มเหลว ซึ่งช่วยเสริมสร้างความมั่นคงปลอดภัยของระบบโดยรวม

สำคัญ: กู้คืนกุญแจลับ หลายเอเจนต์ ความมั่นคง เปรียบเทียบ ประสิทธิภาพ

** Corresponding author: kanokwan@uru.ac.th*

***Received**: 20 มิถุนายน 2568* ***Revised:** 2 พฤศจิกายน 2568* ***Accepted**: 28 พฤศจิกายน 2568*

Abstract

Managing the risks of secret keys from attacks or loss is a critical aspect of maintaining information security. The Key Recovery System (KRS) is a technology developed to mitigate such risks. This study aims to analyze and compare the performance of two types of Multiple Key Recovery Systems (M-KRS): SSDM-KRS and IHADM-KRS, focusing on three key processes: (1) creation of the Key Recovery Field (KRF), (2) key recovery in normal conditions, and (3) key recovery in scenarios where some Key Recovery Agents (KRAs) fail or are unavailable. The experiment simulated KRA operations ranging from 5 to 50 agents, with a minimum recovery threshold set at two agents. The performance evaluation of KRF creation revealed that SSDM-KRS outperformed IHADM-KRS in terms of processing speed due to its simpler structure, while IHADM-KRS demonstrated greater flexibility in KRA management and offered higher security. In normal recovery scenarios without KRA failures, both systems achieved comparable recovery times. However, in scenarios with KRA failures, IHADM-KRS maintained stable recovery performance and high security but required more time than SSDM-KRS, particularly as the number of KRAs increased. The findings indicate that selecting an appropriate key recovery system should align with performance requirements and security policies. Both systems were designed to resist KRA collusion and are robust against failures, thereby enhancing the overall security of the system.

Keywords: Secret Key Recovery, Multi-Agent, Security, Comparative, Performance

1. บทนำ

ในยุคดิจิทัลที่ข้อมูลมีบทบาทสำคัญต่อการดำเนินงานในทุกภาคส่วน ไม่ว่าจะเป็นภาครัฐ ภาคเอกชน หรือการทำธุรกิจ และการติดต่อสื่อสารส่วนบุคคล ทำให้ความมั่นคงปลอดภัยของข้อมูลเป็นประเด็นที่ได้รับความสนใจอย่างต่อเนื่อง โดยเฉพาะการเข้ารหัสลับข้อมูล (Data Encryption) (Stallings, 2023) ซึ่งเป็นวิธีป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต อย่างไรก็ตามความมั่นคงปลอดภัยของข้อมูลจะดำเนินไปอย่างมีประสิทธิภาพและมีความสมบูรณ์ได้ก็ต่อเมื่อ สามารถจัดการกับสถานการณ์ฉุกเฉินหรือเหตุการณ์ที่ไม่คาดคิด เช่น เกิดการสูญหายของกุญแจลับ (Secret Key : Ks) (Hughes, 2022) หรือการที่กุญแจลับไม่สามารถใช้สำหรับการถอดรหัสข้อมูลได้ ตลอดจนความเสี่ยงต่อการรั่วไหลของข้อมูลและการละเมิดความเป็นส่วนตัว หากไม่มีมาตรการควบคุมความปลอดภัยที่เพียงพอ (Abelson et al., 1997)

เทคโนโลยีระบบกู้คืนกุญแจลับ (Key Recovery System: KRS) (Al-Salqan, 1997) เป็นแนวทางหนึ่งที่ถูกพัฒนาขึ้นเพื่อรองรับเหตุการณ์เหล่านี้ ในบริบทของการใช้หลายเอเจนต์ร่วมมือกันกู้คืน (Multiple Key Recovery Agent: M-KRA) โดยไม่อาศัยศูนย์กลาง (Decentralized Multi-Agent Systems) เช่น การกู้คืนกุญแจลับที่มีการจำลองพฤติกรรมโปรโตคอลโดยใช้ ECTPN (Lim et al., 2003) และระบบกู้คืนกุญแจในสภาพแวดล้อมของอุปกรณ์ทางการแพทย์ (IoMT) (Kim et al., 2021) เป็นต้น วิธีการดังกล่าวใช้หลักการแชร์ความลับ (Shamir, 1979) เพื่อช่วยลดความเสี่ยงจากการผูกขาดกุญแจลับ และเพิ่มระดับความปลอดภัยของการกู้คืนกุญแจ ด้วยการประสานการทำงานร่วมกันของกลุ่ม KRA (National Institute of Standards and Technology, 1998)

อย่างไรก็ตามยังพบจุดอ่อนหรือมีข้อจำกัดด้านความเสี่ยงจากการสมรู้ร่วมคิดระหว่าง KRA เพื่อเป็นการแก้ปัญหาประเด็นดังกล่าว จึงได้มีการพัฒนาระบบกู้คืนกุญแจลับที่มีฟังก์ชันสนับสนุนด้านความมั่นคงปลอดภัยครบถ้วน สามารถทำงานอย่างมีประสิทธิภาพรองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย ช่วยลดความเสี่ยงจากการโจมตีแบบจุดเดียว (Single Point of Failure : SPOF) และลดการโจมตีที่เกิดจากการสมรู้ร่วมคิดบางส่วนของ KRA คือ ระบบ IHADM-KRS จากงานวิจัยเรื่อง Improved High Availability Decentralized Multi-agent KRS (กนกวรรณ กันยะมี, 2566) และระบบ SSDM-KRS จากงานวิจัยเรื่อง Simple Secret-key Splitting and Sharing in Decentralized Multi-agent KRS (กนกวรรณ กันยะมี, 2566) โดย IHADM-KRS มีจุดเด่นในด้านความยืดหยุ่นของการกำหนดเงื่อนไขจำนวน KRA ที่ใช้ในการกู้คืนกุญแจ ซึ่งทำให้ระบบมีความมั่นคงปลอดภัยสูง ในขณะที่ SSDM-KRS เน้นความเรียบง่าย โครงสร้างไม่ซับซ้อน

มีความเร็วในการประมวลผล ทั้งสองระบบสามารถจัดการกระบวนการกู้คืนกุญแจลับได้อย่างถูกต้องและมีประสิทธิภาพ เหมาะสมกับลักษณะการนำไปประยุกต์ใช้งานในบริบทที่แตกต่างกัน อย่างไรก็ดียังขาดการศึกษาวิเคราะห์เปรียบเทียบในเชิงลึก โดยเฉพาะในแง่มุมของประสิทธิภาพเชิงเวลาในกระบวนการสร้างฟิลด์กู้คืนกุญแจ (Key Recovery Field : KRF) การกู้คืนกุญแจลับในสถานการณ์ปกติ และการกู้คืนกุญแจลับในกรณีที่ KRA บางส่วนล่ม ส่งผลให้ข้อจำกัดนี้ยังไม่มีข้อมูลสรุปที่ชัดเจนอย่างเป็นรูปธรรม ภายใต้เงื่อนไขด้านความมั่นคงปลอดภัย และความเร็วในการประมวลผลที่แตกต่างกัน

ดังนั้นผู้วิจัยจึงได้ทำการทดลองเปรียบเทียบประสิทธิภาพของระบบ IHADM-KRS และ SSDM-KRS โดยมุ่งเน้นไปที่ 3 ประเด็นหลัก ได้แก่ (1) ประสิทธิภาพเวลาในการประมวลผลขั้นตอนการสร้าง KRF (2) ประสิทธิภาพเวลาของการกู้คืนกุญแจลับในสถานการณ์ปกติ และ (3) ประสิทธิภาพเวลาของการกู้คืนกุญแจลับเมื่อเกิดเหตุการณ์มี KRA ในกลุ่มการกู้คืนล่ม เพื่อนำไปสู่ข้อสรุปในการเลือกใช้รูปแบบการกู้คืนกุญแจที่เหมาะสมสอดคล้องกับบริบทด้านความมั่นคงปลอดภัย โดยสามารถพิจารณาปัจจัยด้านความเร็วในการประมวลผล การบริหารจัดการ KRA และระดับความมั่นคงปลอดภัย

2. วัตถุประสงค์การวิจัย

เพื่อวิเคราะห์เปรียบเทียบการประเมินประสิทธิภาพด้านเวลาในการประมวลผล ของการกู้คืนกุญแจลับ 2 รูปแบบ คือ (1) IHADM-KRS และ (2) SSDM-KRS ใน 3 ประเด็นที่สำคัญ ดังต่อไปนี้

2.1 ประสิทธิภาพด้านเวลาในการประมวลผล การสร้าง KRF

2.2 ประสิทธิภาพด้านเวลาในการประมวลผล ที่ใช้ในการกู้คืนกุญแจในกรณีปกติ

2.3 ประสิทธิภาพด้านเวลาในการประมวลผล ที่ใช้ในการกู้คืนกุญแจในกรณีที่มี KRA ในกลุ่มการกู้คืนล่ม

3. วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงทดลอง (Experimental Research) มีวัตถุประสงค์เพื่อเปรียบเทียบประสิทธิภาพของการกู้คืนกุญแจลับ 2 รูปแบบ คือ (1) IHADM-KRS และ (2) SSDM-KRS โดยมีขั้นตอนดำเนินการวิจัยดังนี้

3.1 ศึกษาทบทวนทฤษฎีของการกู้คืนกุญแจลับหลายเอเจนต์ (M-KRA) แบบไม่อาศัยศูนย์กลางหรือแบบกระจาย และงานวิจัยที่เกี่ยวข้อง

3.1.1 การกู้คืนกุญแจลับ M-KRA แบบไม่อาศัยศูนย์กลาง

การกู้คืนกุญแจลับ (Secret Key Recovery) เป็นกระบวนการที่ช่วยให้ผู้ใช้หรือระบบสามารถเข้าถึงข้อมูลที่ถูกเข้ารหัสได้ แม้ในกรณีที่กุญแจลับสูญหายหรือไม่สามารถเข้าถึงได้ตามปกติ โดยเฉพาะในระบบที่มีการเข้ารหัสแบบสมมาตร ระบบกู้คืนกุญแจลับแบบ M-KRA เป็นแนวทางที่ใช้ตัวแทน KRA จำนวน 2 เอเจนต์ขึ้นไป เข้ามามีบทบาทร่วมกันในการกู้คืนกุญแจลับ โดยอาศัยหลักการกระจายความรับผิดชอบและลดความเสี่ยงจากการพึ่งพาศูนย์กลางเพียงรายเดียว ในระบบแบบไม่อาศัยศูนย์กลางนั้น KRA แต่ละรายจะทำหน้าที่ร่วมกันในการกู้คืนกุญแจลับตามกลไกที่กำหนด โดยไม่มีหน่วยงานควบคุมส่วนกลาง ระบบลักษณะนี้จึงสามารถออกแบบให้มีความยืดหยุ่นในการควบคุมสิทธิ์การเข้าถึงของ KRA และรองรับการกำหนดจำนวน KRA ขั้นต่ำเพื่อให้สามารถทำการกู้คืนกุญแจลับได้ (Kanyamee et al., 2014)

จุดเด่นของระบบกู้คืนกุญแจลับแบบ M-KRA ที่ไม่อาศัยศูนย์กลาง ได้แก่

(1) มีความมั่นคงปลอดภัย ด้วยการแบ่งข้อมูลส่วนประกอบของกุญแจออกเป็นส่วน ๆ เพื่อกระจายให้ KRA ในกลุ่มการกู้คืน

(2) ลดความเสี่ยงจากการสมรู้ร่วมคิดกันระหว่าง KRA

(3) สามารถปรับขนาดและความซับซ้อนของระบบได้ ตามระดับความปลอดภัยที่ต้องการ

(4) การออกแบบระบบรองรับการล่มของ KRA บางส่วน เหมาะสำหรับการนำไปใช้ในสภาพแวดล้อมที่ต้องการความมั่นคงปลอดภัยสูง และสามารถประยุกต์ใช้ในงานที่เกี่ยวข้องกับการเข้ารหัสข้อมูล การควบคุมการเข้าถึง และระบบการจัดการกุญแจในระดับองค์กร

3.1.2 วิเคราะห์เหตุผลในการเลือกเปรียบเทียบ IHADM-KRS และSSDM-KRS ในงานวิจัย

(1) พัฒนาภายใต้แนวคิดของการทำงานในรูปแบบที่ไม่อาศัยศูนย์กลาง หรือแบบกระจายศูนย์ (Decentralized Multi-Agent KRS) ซึ่งสนับสนุนการจัดการกุญแจลับในยุคที่ต้องการความมั่นคงปลอดภัยสูง และลดความเสี่ยงจากการพึ่งพาศูนย์กลางเพียงจุดเดียว (Single Point of Failure)

(2) มีพื้นฐานจากการใช้แนวคิดเดียวกัน แต่มีกระบวนการกู้คืนกุญแจที่ต่างกันอย่างมีนัยสำคัญ

(3) มีสถาปัตยกรรมพื้นฐานที่ใกล้เคียงกัน ช่วยให้สามารถเปรียบเทียบได้อย่างเที่ยงตรง ไม่มีความแตกต่างด้านโครงสร้างหรือตัวแปรที่อาจเป็นจุดอ่อนต่อการประเมินและวิเคราะห์ผล

(4) สามารถควบคุมตัวแปรในการทดลองได้อย่างมีประสิทธิภาพ ส่งผลให้การวิเคราะห์เปรียบเทียบด้านประสิทธิภาพและความมั่นคงปลอดภัยเป็นไปอย่างตรงประเด็นและเชื่อถือได้

3.1.3 งานวิจัย Improved High Availability Decentralized Multi-agent KRS (IHADM-KRS)

ระบบ IHADM-KRS (กนกวรรณ กันยะมี, 2566) เป็นแนวทางการออกแบบระบบกู้คืนกุญแจลับที่เน้นความยืดหยุ่นในการควบคุมระดับความมั่นคงปลอดภัย ระบบมีโครงสร้างแบบลำดับชั้น สามารถกำหนดจำนวน KRA ขั้นต่ำในการร่วมกันกู้คืนกุญแจลับได้ตามความเหมาะสม จุดเด่นของ IHADM-KRS คือการกระจายข้อมูลที่เกี่ยวข้องกับกุญแจลับ (เช่น แอตทริบิวต์ TTi ตามสมการ (1)) ไปยัง KRA แต่ละรายแบบเฉพาะเจาะจง โดยแต่ละ KRA จะมีข้อมูลส่วนประกอบของกุญแจบางส่วนเท่านั้น ทำให้สามารถควบคุมสิทธิ์ในการเข้าถึงข้อมูลกุญแจได้อย่างเหมาะสมปลอดภัย ช่วยลดความเสี่ยงจากการสมรู้ร่วมคิดของ KRA และสามารถกู้คืนกุญแจลับได้แม้ในกรณีที่มี KRA ล่ม โดยมีรูปแบบของ KRF ดังนี้

$$KRF = \{ Ku_{agi}[KRF_i\text{'s}] \,||\, Ku_R(S_R) \,||\, Ku_G(S_R) \}$$

$$KRF_i = Ku_{agi}[S_i \,||\, SGN \,||\, TT_i\text{'s} \,||\, \text{Other information}]$$

และ IHADM-KRS มีรูปแบบการกระจายแอตทริบิวต์ TTi สำหรับบริหารจัดการกู้คืนกุญแจในกรณีที่มี KRA ในกลุ่มการกู้คืนล่ม ดังนี้

$$\mathbf{TT}_i = \{\mathbf{KRA}_{i,1_i} \bmod n, \mathbf{KRA}_{i,2_i} \bmod n, \ldots, \mathbf{KRA}_{i,t_i} \bmod n\} \quad (1)$$

โดยที่

i = ลำดับของ KRA_i (เริ่มจาก 1)

$t = n - mr$

ใช้ modulo n เพื่อให้วนกลับไปที่ KRA_1 เมื่อถึง KRA_n

จากการศึกษาวิเคราะห์พบว่า IHADM-KRS มีความแข็งแกร่งในด้านความมั่นคงปลอดภัยและมีความสามารถในการควบคุมเชิงนโยบาย แต่มีต้นทุนด้านเวลาและโครงสร้างที่ซับซ้อนกว่า SSDM-KRS ที่มีจุดเด่นด้านความเรียบง่าย รวดเร็ว

3.1.4 งานวิจัย Simple Secret-key Splitting and Sharing in Decentralized Multi-agent KRS (SSDM-KRS)

ระบบ SSDM-KRS (กนกวรรณ กันยะมี, 2566) เป็นระบบกู้คืนกุญแจลับที่ออกแบบโดยมุ่งเน้นความเรียบง่าย รวดเร็ว แต่ยังสามารถกู้คืนกุญแจได้ในกรณีที่มี KRA ล่ม ระบบนี้จัดเก็บส่วนประกอบของกุญแจทั้งหมดสำหรับการกู้คืนไว้ที่ KRF โดยไม่ใช้วิธีการกระจายส่วนประกอบของกุญแจลับไปยัง KRA ทำให้สามารถเข้าถึงและกู้คืนกุญแจลับได้อย่างรวดเร็ว จุดเด่นของ SSDM-KRS คือ มีการออกแบบให้โครงสร้างของ KRF ไม่ซับซ้อน จัดเก็บส่วนประกอบของกุญแจที่เอื้อให้การกู้คืนทำได้อย่างรวดเร็ว แต่ยังคงมีความมั่นคงปลอดภัย เนื่องจากมีฟังก์ชันการพิสูจน์ตัวจริงของ KRA ในกลุ่มการกู้คืนที่แข็งแกร่ง การกู้คืนกุญแจลับสามารถดำเนินการได้โดยใช้ KRA ขั้นต่ำจำนวน 2 รายในการตรวจสอบสิทธิ์และยืนยันการร้องขอการกู้คืนกุญแจ โดยมีรูปแบบของ KRF ดังนี้

$$KRF = \{ Kuagi[KRFi's] \| TTi's \| KuR(SR) \| KuG(SR) \| h(SGN) \}$$
$$KRFi = Kuagi[Si \| SGN \| Other information]$$

อย่างไรก็ตาม SSDM-KRS มีข้อจำกัดคือ ไม่สามารถกำหนดจำนวน KRA ขั้นต่ำในการกู้คืนกุญแจตามเงื่อนไขได้ ทั้งนี้ระบบกำหนดให้มี KRA อย่างน้อย 2 ราย (ที่ไม่ล่ม) ก็สามารถให้บริการกู้คืนกุญแจได้ SSDM-KRS มีประสิทธิภาพสูงในด้านเวลาและการประมวลผล โดยเฉพาะอย่างยิ่งเมื่อจำนวน KRA เพิ่มขึ้น ระบบยังสามารถรักษาความเร็วในการกู้คืนได้อย่างมีเสถียรภาพ

3.2 ออกแบบการทดลอง กำหนดค่าตัวแปร และจำลองการทำงานของ IHADM-KRS และ SSDM-KRS โดยใช้จำนวนตัวแทน KRA ในการกู้คืนกุญแจ (KRA) ตั้งแต่ 5 ถึง 50 เอเจนต์ และกำหนดให้มี KRA ขั้นต่ำในการกู้คืนกุญแจ เท่ากับ 2 เอเจนต์

3.3 ทดลองเปรียบเทียบประสิทธิภาพในการทำงานของการกู้คืนกุญแจ และเก็บผลการทดลองใน 3 ประเด็น คือ การสร้าง KRF การกู้คืนกุญแจในสถานการณ์ปกติ และการกู้คืนกุญแจเมื่อมี KRA ล่ม

3.4 รวบรวมผลการทดลองเพื่อนำมาวิเคราะห์เปรียบเทียบประสิทธิภาพใน 3 ประเด็นข้างต้น

3.5 อภิปราย และสรุปผลการวิจัย

4. ผลการวิจัย

4.1 การเปรียบเทียบรูปแบบการกู้คืนกุญแจแบบ IHADM-KRS และ SSDM-KRS

การเลือกใช้รูปแบบการกู้คืนกุญแจลับที่เหมาะสม ส่งผลต่อประสิทธิภาพและความมั่นคงปลอดภัยของระบบสารสนเทศ การเปรียบเทียบรูปแบบระหว่าง IHADM-KRS และ SSDM-KRS ดังแสดงในตารางที่ 1 ช่วยให้เห็นข้อดี ข้อจำกัด ตลอดถึงโครงสร้างการจัดเก็บส่วนประกอบของกุญแจ และการห่อหุ้ม KRF ของแต่ละระบบ ซึ่งเป็นแนวทางในการเลือกใช้หรือเพื่อสนับสนุนการออกแบบระบบกู้คืนกุญแจที่สอดคล้องกับระดับความมั่นคงปลอดภัยที่ต้องการในการบริหารจัดการสารสนเทศ

ตารางที่ 1 การเปรียบเทียบรูปแบบการกู้คืนกุญแจแบบ IHADM-KRS และ SSDM-KRS

หัวข้อเปรียบเทียบ	IHADM-KRS	SSDM-KRS
ชื่อเต็ม	Improved High Availability Decentralized Multi-agent KRS	Simple Secret-key Splitting and Sharing in Decentralized Multi-agent KRS
(1) รูปแบบการกู้คืนกุญแจลับ	กู้คืนกุญแจแบบ M-KRA ที่ไม่อาศัยศูนย์กลาง (แบบปรับปรุงขั้นสูง)	กู้คืนกุญแจแบบ M-KRA ที่ไม่อาศัยศูนย์กลาง (แบบง่าย)
(2) แนวคิดหลัก	ปรับปรุงฟิลด์กู้คืนกุญแจด้วย Power Set และ Secret Sharing	แบ่งและแชร์กุญแจลับแบบง่าย

หัวข้อเปรียบเทียบ	IHADM-KRS	SSDM-KRS
(3) ความสามารถในการต้านทานการสมรู้ร่วมคิด	ป้องกันได้	ป้องกันได้
(4) การยืนยันตัวตน KRA	ใช้ SGN โดยตรง	ใช้ hash ของ SGN (*h(SGN)*)
(5) วิธีเก็บส่วนประกอบของกุญแจใน KRF	ใช้ Power Set ในการกระจายส่วนประกอบของกุญแจ	ใช้การเก็บแอตทริบิวต์ TT_i
(6) โครงสร้าง KRF	ซับซ้อนและยืดหยุ่นสูง	เรียบง่าย
(7) ขนาดของ KRF	เล็กกว่า SSDM-KRS เล็กน้อย อย่างไม่มีนัยสำคัญ	ใหญ่กว่า IHADM-KRS เล็กน้อย อย่างไม่มีนัยสำคัญ
(8) ความพร้อมใช้งาน	มีความพร้อมใช้งานแม้ในกรณีที่มี KRA ล่ม และสามารถกำหนดจำนวน KRA ในการกู้คืนกุญแจได้	มีความพร้อมใช้งานแม้ในกรณีที่มี KRA ล่ม
(9) การรองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย	รองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยเข้าถึงได้จาก KRF	รองรับการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายโดยเข้าถึงได้จาก KRF
(10) ความเหมาะสมในการใช้งาน	ระบบที่ต้องการความยืดหยุ่นสูง กู้คืนกุญแจลับได้ในสถานการณ์ที่ซับซ้อน	ระบบที่ต้องการความเร็ว ไม่ซับซ้อน

จากตารางที่ 1 สามารถสรุปได้ว่า IHADM-KRS ถูกออกแบบให้มีความยืดหยุ่นสูง สามารถบริหารจัดการจำนวน KRA ที่ใช้ในการกู้คืนกุญแจได้ตามความเหมาะสมของระดับความมั่นคงปลอดภัยที่ต้องการ มีฟังก์ชันกำหนดจำนวน KRA ขั้นต่ำที่ใช้ในการกู้คืนกุญแจ เหมาะกับระบบที่ต้องการความมั่นคงปลอดภัยสูง และสามารถป้องกันการสมรู้ร่วมคิดของ KRA ในกลุ่มการกู้คืน ส่วน SSDM-KRS ออกแบบให้ทำงานง่าย ไม่ซับซ้อน มีประสิทธิภาพ เหมาะกับนำไปใช้ในสภาพแวดล้อมที่ต้องการการประมวลผลที่รวดเร็ว มีการป้องกันการสมรู้ร่วมคิด และมีกระบวนการพิสูจน์ตัวจริงของ KRA

4.2 การเปรียบเทียบประสิทธิภาพในการประมวลผลเวลาที่ใช้ในการสร้าง KRF ของรูปแบบการกู้คืนกุญแจ SSDM-KRS และ IHADM-KRS (หน่วย มิลลิวินาที: ms)

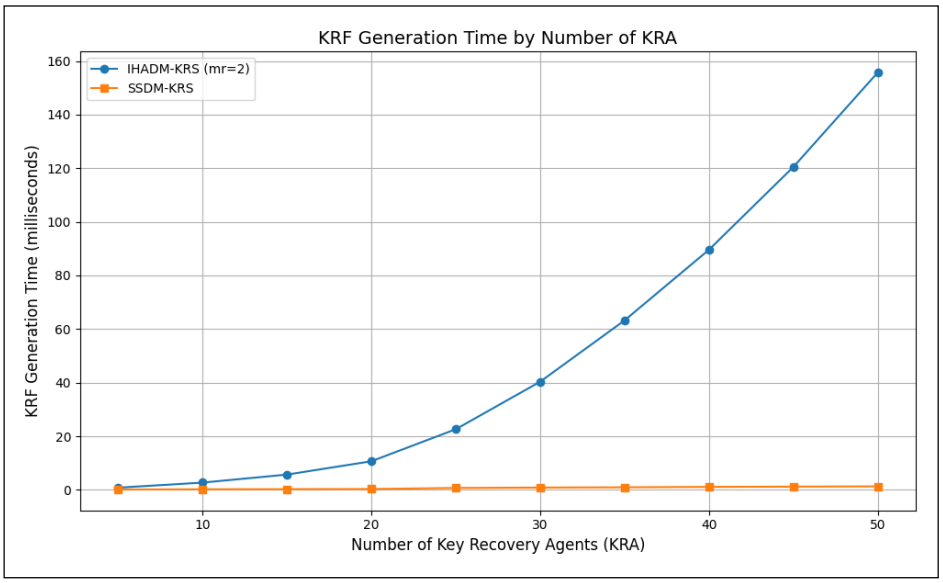
การสร้างฟิลด์ในการกู้คืนกุญแจ (Key Recovery Field: KRF) เป็นขั้นตอนที่มีผลกระทบโดยตรงต่อประสิทธิภาพของระบบทั้งด้านเวลาและทรัพยากร การทดลองนี้จึงมีจุดประสงค์ในการวัดและเปรียบเทียบเวลาที่ใช้ในการสร้าง KRF ระหว่างระบบ SSDM-KRS และ IHADM-KRS โดยจำลองจำนวนตัวแทน KRA ในการกู้คืนกุญแจ (KRA) ตั้งแต่ 5 ถึง 50 เอเจนต์ ทั้งนี้ได้กำหนดให้มี KRA ขั้นต่ำในการกู้คืนกุญแจ เท่ากับ 2 เอเจนต์ เพื่อประเมินแนวโน้มของเวลาในการสร้าง KRF ภายใต้โครงสร้างการจัดเก็บส่วนประกอบของกุญแจที่แตกต่างกันของทั้งสองระบบ ผลลัพธ์ดังแสดงในตารางที่ 2 และภาพที่ 1

ตารางที่ 2 การเปรียบเทียบประสิทธิภาพในการประมวลผลเวลาที่ใช้ในการสร้าง KRF

จำนวน KRA	IHADM-KRS, mr=2 (ms)	SSDM-KRS (ms)
5	0.808	0.121
10	2.702	0.216
15	5.692	0.266
20	10.658	0.317

จำนวน KRA	IHADM-KRS, mr=2 (ms)	SSDM-KRS (ms)
25	22.599	0.708
30	38.743	0.437
35	32.546	0.62
40	46.548	0.644
45	54.873	0.633
50	67.585	0.762

จากผลการทดลองในตารางที่ 2 พบว่า ระบบ SSDM-KRS ใช้เวลาในการสร้าง KRF น้อยกว่า IHADM-KRS อย่างมีนัยสำคัญ โดยเฉพาะเมื่อจำนวน KRA เพิ่มขึ้น เนื่องจาก SSDM-KRS มีโครงสร้างการจัดเก็บข้อมูลแบบรวมไว้ที่ KRF ซึ่งไม่ต้องประมวลผลการกระจายส่วนประกอบของกุญแจแบบเฉพาะเจาะจง ในขณะที่ IHADM-KRS ต้องดำเนินการกระจายส่วนประกอบของกุญแจไปใน KRF ของทุก KRA ตามเงื่อนไขที่กำหนด ทำให้ใช้เวลาเพิ่มขึ้นตามลำดับ ส่งผลให้แนวโน้มของเวลาที่ใช้สำหรับการสร้าง KRF ของ IHADM-KRS มีลักษณะเพิ่มสูงขึ้นมากตามจำนวน KRA ที่เพิ่มขึ้น ในขณะที่ SSDM-KRS มีเวลาที่เพิ่มเล็กน้อยเกือบเป็นเส้นตรงและคงที่กว่า ดังแสดงในภาพที่ 1



ภาพที่ 1 เปรียบเทียบเวลาที่ใช้ในการสร้าง KRF

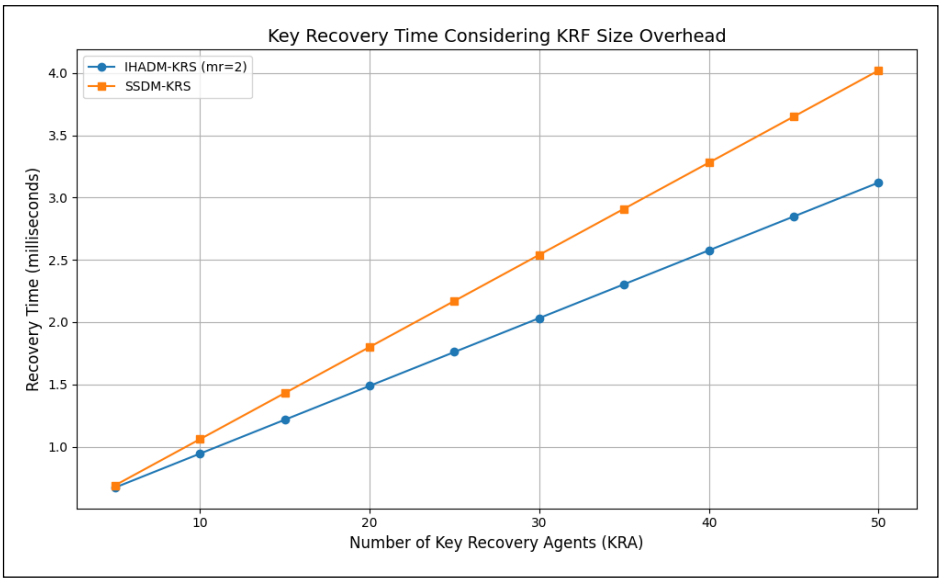
4.3 การเปรียบเทียบประสิทธิภาพในการประมวลผลเวลาที่ใช้ในการกู้คืนกุญแจลับแบบปกติ ของรูปแบบการกู้คืนกุญแจ SSDM-KRS และ IHADM-KRS (หน่วย มิลลิวินาที: ms)

การกู้คืนกุญแจลับในสถานการณ์ปกติ หมายถึงการกู้คืนในภาวะที่ไม่มี KRA ในกลุ่มการกู้คืนล่ม เป็นกระบวนการที่สะท้อนถึงประสิทธิภาพของการกู้คืนกุญแจภายใต้เงื่อนไขความพร้อมใช้งาน (Availability) ซึ่งช่วยให้สามารถประเมินความเร็วในการเข้าถึงข้อมูลส่วนประกอบของกุญแจ ที่ถูกห่อหุ้มไว้ใน KRF และเวลาในการคำนวณกุญแจลับ โดยได้ทดลองจำลอง KRA ตั้งแต่ 5 ถึง 50 เอเจตน์ กำหนดให้มี KRA ขั้นต่ำในการกู้คืนกุญแจ (mr) เท่ากับ 2 เอเจนต์ ผลลัพธ์แสดงดังตารางที่ 3 และ ภาพที่ 2

ตารางที่ 3 การเปรียบเทียบประสิทธิภาพในการประมวลผลเวลาที่ใช้ในการกู้คืนกุญแจลับแบบปกติ

จำนวน KRA	IHADM-KRS, mr=2 (ms)	SSDM-KRS (ms)
5	0.672	0.692
10	0.971	1.023
15	1.277	1.354
20	1.551	1.682
25	1.872	2.014
30	2.171	2.347
35	2.470	2.677
40	2.773	3.112
45	3.072	3.331
50	3.371	3.661

จากผลการทดลองในตารางที่ 3 พบว่า ระบบ SSDM-KRS และ IHADM-KRS มีเวลาในการกู้คืนกุญแจลับในสถานการณ์ปกติที่ใกล้เคียงกัน เนื่องจากทั้ง 2 ระบบสามารถใช้ข้อมูลส่วนประกอบของกุญแจ ที่ห่อหุ้มไว้ใน KRF ได้โดยตรง อย่างไรก็ตามเมื่อจำนวน KRA เพิ่มขึ้น ระบบ SSDM-KRS มีแนวโน้มใช้เวลามากกว่าเล็กน้อย ดังแสดงในภาพที่ 2 ซึ่งเป็นผลจากขนาดของ KRF ที่เพิ่มขึ้นตามจำนวน KRA ซึ่งส่งผลต่อเวลาในการโหลดหรือเข้าถึงข้อมูล ในขณะที่ IHADM-KRS ยังคงรักษาประสิทธิภาพได้ดีด้วยขนาด KRF ที่คงที่ ทำให้ระบบเหมาะสมกับการใช้งานที่ต้องการความเร็วและความเสถียรในการกู้คืนในภาวะปกติ



ภาพที่ 2 เปรียบเทียบเวลาที่ใช้ในการกู้คืนกุญแจลับแบบปกติ

4.4 การเปรียบเทียบประสิทธิภาพในการประมวลผลเวลาที่ใช้ในการกู้คืนกุญแจลับที่มี KRA ในกลุ่มการกู้คืนล่มของรูปแบบการกู้คืนกุญแจ SSDM-KRS และ IHADM-KRS (หน่วย มิลลิวินาที: ms)

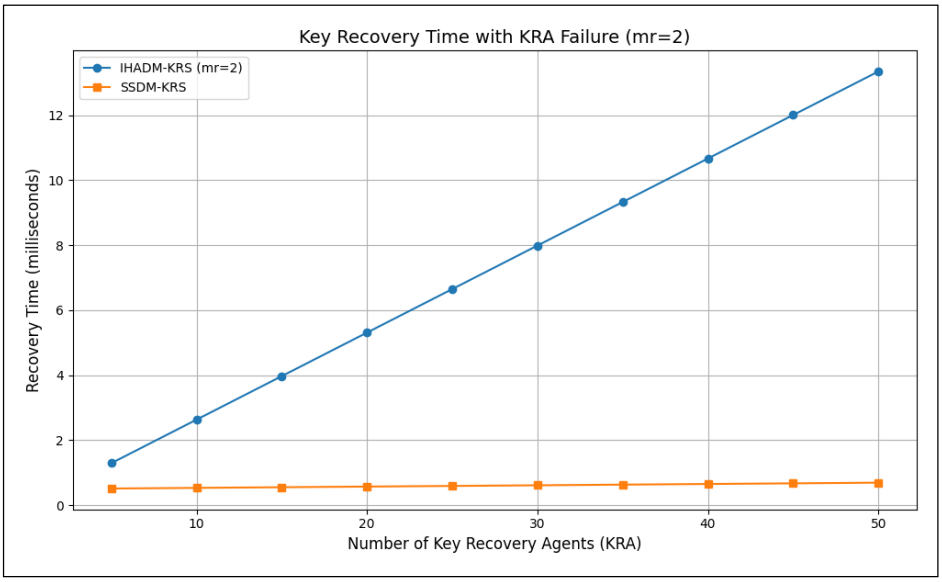
ระบบ SSDM-KRS และ IHADM-KRS มีความสามารถในการกู้คืนกุญแจลับได้ แม้ในกรณีที่มี KRA ล่ม โดยอาศัยวิธีการสำรองส่วนประกอบของกุญแจไว้ใน KRF การทดลองนี้จึงประเมินเวลาในการกู้คืนกุญแจลับ และความสามารถในการรักษาเสถียรภาพของเวลา

ในการกู้คืน โดยกำหนดเงื่อนไขจำลอง KRA ตั้งแต่ 5 ถึง 50 เอเจตน์ และใช้ KRA ขั้นต่ำ เท่ากับ 2 เอเจนต์ ผลลัพธ์แสดงดังตารางที่ 4 และภาพที่ 3

ตารางที่ 4 การเปรียบเทียบประสิทธิภาพในการประมวลผลเวลาที่ใช้ในการกู้คืนกุญแจลับในกรณีที่มี KRA ในกลุ่มการกู้คืนล่ม

จำนวน KRA	IHADM-KRS, mr=2 (ms)	SSDM-KRS (ms)
5	1.293	0.511
10	3.122	0.542
15	4.954	0.575
20	6.781	0.611
25	8.617	0.635
30	10.445	0.661
35	12.272	0.693
40	14.132	0.720
45	15.931	0.751
50	17.764	0.783

ผลการทดลองในตารางที่ 4 แสดงให้เห็นว่า เมื่อมี KRA ในกลุ่มการกู้คืนล่ม จะต้องใช้ข้อมูลส่วนประกอบของกุญแจที่สำรองไว้ใน KRF ทำให้ระบบ IHADM-KRS มีแนวโน้มใช้เวลามากกว่าระบบ SSDM-KRS โดยเฉพาะเมื่อจำนวน KRA เพิ่มสูงขึ้น เนื่องจาก IHADM-KRS ใช้วิธีการกระจายค่าส่วนประกอบของกุญแจแบบเฉพาะเจาะจง ทำให้ต้องประมวลผลชุดข้อมูลจำนวนมากขึ้น ในขณะที่ SSDM-KRS รวบรวมจัดเก็บส่วนประกอบของกุญแจของทุก KRA ไว้ใน KRF ส่งผลให้การเข้าถึงข้อมูลทำได้อย่างรวดเร็วและมีค่าเวลาคงที่ ดังแสดงในภาพที่ 3 อย่างไรก็ตาม IHADM-KRS มีความยืดหยุ่นในการการบริหารจัดการ KRA ได้ดี และสามารถมีศักยภาพในการรักษาความมั่นคงปลอดภัยที่สูงกว่า SSDM-KRS



ภาพที่ 3 เปรียบเทียบเวลาที่ใช้ในการกู้คืนกุญแจลับแบบเมื่อมี KRA ล่ม (mr=2)

4.5 การเปรียบเทียบเชิงคุณภาพของประสิทธิภาพระบบ IHADM-KRS และ SSDM-KRS

เพื่อแสดงภาพรวมของความแตกต่างระหว่าง IHADM-KRS และ SSDM-KRS อย่างชัดเจน จึงได้สรุปผลการเปรียบเทียบเชิงคุณภาพในประเด็นด้านประสิทธิภาพการประมวลผลการกู้คืนกุญแจ ทั้ง 2 รูปแบบ ใน 3 กระบวนการหลัก ดังแสดงในตารางที่ 5

ตารางที่ 5 การเปรียบเทียบเชิงคุณภาพของประสิทธิภาพระบบ IHADM-KRS และ SSDM-KRS ในกระบวนการกู้คืนกุญแจ

รายการประเมิน	IHADM-KRS	SSDM-KRS
1. การสร้าง KRF	ใช้เวลามากกว่า ตามจำนวน KRA เนื่องจากใช้กระบวนการกระจายส่วนประกอบของกุญแจตามเงื่อนไขความมั่นคงปลอดภัย	ใช้เวลาน้อยกว่าอย่างมีนัยสำคัญ เนื่องจากโครงสร้างไม่ซับซ้อน ไม่มีกระบวนการคำนวณสำหรับการกระจายส่วนประกอบของกุญแจ
2. การกู้คืนกุญแจ (กรณีปกติ)	คงประสิทธิภาพดี แม้จำนวน KRA เพิ่มขึ้น เนื่องจากขนาดของ KRF คงที่	เวลาเพิ่มขึ้นเล็กน้อยตามการเพิ่มจำนวนของ KRA เพราะขนาด KRF ใหญ่ขึ้น
3. การกู้คืนกุญแจ (กรณีมี KRA ล่ม)	ใช้เวลามากขึ้นอย่างมีนัยสำคัญตามจำนวน KRA แต่มีความเสถียรและความปลอดภัยสูง	ใช้เวลาน้อยกว่าคงที่ เพราะเก็บส่วนประกอบไว้รวมใน KRF

จากตารางที่ 5 จะเห็นได้ว่า SSDM-KRS มีข้อได้เปรียบในด้านความเร็ว โดยเฉพาะในกระบวนการ สร้าง KRF และการกู้คืนในกรณีที่ KRA ล่ม ซึ่งระบบใช้โครงสร้างที่ไม่ซับซ้อนและจัดเก็บข้อมูลส่วนประกอบของกุญแจไว้ใน KRF ทำให้ไม่ต้องใช้เวลาในการประมวลผลการกระจายส่วนประกอบของกุญแจ ส่งผลให้ประสิทธิภาพด้านเวลาคงที่ และตอบสนองได้รวดเร็ว แม้เมื่อจำนวน KRA เพิ่มขึ้น

อย่างไรก็ตาม IHADM-KRS แม้จะใช้เวลาในการประมวลผลมากกว่าในบางกระบวนการ แต่มีจุดเด่นในด้านความยืดหยุ่นและความมั่นคงปลอดภัย โดยเฉพาะในกรณีที่มี KRA ล่ม ระบบสามารถกู้คืนกุญแจได้อย่างเสถียร ผ่านกลไกการกระจายข้อมูลที่ออกแบบตามเงื่อนไขของความมั่นคงปลอดภัย อีกทั้งยังรักษาประสิทธิภาพในการกู้คืนกรณีปกติได้ดี แม้มีการเพิ่มจำนวน KRA

ในด้านความเหมาะสมของบริบทการใช้งาน พบว่า ระบบ IHADM-KRS เหมาะสำหรับสภาพแวดล้อมที่มีความต้องการความมั่นคงปลอดภัยในระดับสูงมาก เช่น หน่วยงานภาครัฐ ภาคการเงิน หรือระบบโครงสร้างพื้นฐานที่มีความสำคัญ เนื่องจากระบบนี้สามารถกำหนดจำนวน KRA ขั้นต่ำ (Threshold) ได้อย่างยืดหยุ่น ทำให้สามารถควบคุมความเสี่ยงจากการสมรู้ร่วมคิดของ KRA และเพิ่มความทนทานต่อเหตุการณ์ที่ KRA บางส่วนล่มได้เป็นอย่างดี ในขณะที่ระบบ SSDM-KRS เหมาะสำหรับบริบทที่ให้ความสำคัญกับความเร็วในการประมวลผล มีโครงสร้างไม่ซับซ้อน โดยเฉพาะองค์กรที่มีข้อจำกัดด้านทรัพยากร เช่น ระบบงานธุรกิจทั่วไป ระบบสำรองข้อมูล หรือระบบ IoT ที่ต้องการความรวดเร็วและการติดตั้งใช้งานที่ไม่ซับซ้อน อย่างไรก็ตามแม้ว่าระดับความมั่นคงปลอดภัยจะน้อยกว่า IHADM-KRS แต่สามารถเสริมด้วยมาตรการรักษาความปลอดภัยอื่นเพื่อให้เพียงพอต่อความต้องการขององค์กรได้ ดังนั้นการเลือกประยุกต์ใช้งาน 2 รูปแบบ ควรพิจารณาตามลักษณะการใช้งานจริงเพื่อให้เกิดประโยชน์และมีประสิทธิภาพสูงสุด

5. อภิปรายผลการวิจัยและข้อเสนอแนะ

5.1 อภิปรายผลการวิจัย

การพัฒนาระบบกู้คืนกุญแจลับเริ่มจากแนวคิดที่นำเสนอเทคโนโลยีการกู้คืนกุญแจ เพื่อรองรับกรณีสูญหายของกุญแจเข้ารหัสหรือการเข้าถึงข้อมูลตามข้อกำหนดทางกฎหมาย (Al-Salqan, 1997) ในระยะแรกนิยมใช้หน่วยงานกลางที่เชื่อถือได้ (Trusted Third Party: TTP) ซึ่งมีโครงสร้างที่ไม่ซับซ้อน แต่มีข้อจำกัดด้านความมั่นคงปลอดภัยจากความเสี่ยง Single Point of Failure (SPOF) และการผูกขาดการควบคุมกุญแจในจุดเดียว เพื่อแก้ปัญหานี้สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ ซึ่งเป็นหน่วยงานของรัฐบาลสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) (NIST, 1998) จึงเสนอแนวคิดการใช้การกู้คืนกุญแจแบบ M-KRA ในสถาปัตยกรรมแบบกระจายศูนย์ (Decentralized Multi-Agent Systems) ลดการพึ่งพา

ศูนย์กลางและเพิ่มความทนทานของระบบ ต่อมาได้มีงานวิจัยที่จำลองพฤติกรรมโปรโตคอลกู้คืนกุญแจด้วย Extended Cryptographic Timed Petri Net (ECTPN) (Lim et al., 2003) เพื่ออธิบายการทำงานร่วมกันของ M-KRA ซึ่งสะท้อนศักยภาพของโครงสร้างแบบกระจายศูนย์ในการลดความซับซ้อนของขั้นตอนโปรเซส ขณะที่ต่อมามีงานวิจัยที่ได้ประยุกต์ใช้ระบบในสภาพแวดล้อมของอุปกรณ์ทางการแพทย์ (IoMT) (Kim et al., 2021) มีการฝังข้อมูลฟิลด์สำหรับกู้คืนกุญแจไว้ภายในข้อความที่ถูกเข้ารหัส และใช้กระบวนการเข้ารหัสซ้ำผ่านพร็อกซีเพื่อเพิ่มความปลอดภัยของข้อมูล แม้มีความมั่นคงปลอดภัยสูง แต่ยังมีข้อจำกัดด้านความยืดหยุ่นและความทนทานต่อการล่มของ KRA บางส่วน

จากข้อจำกัดของงานก่อนหน้า จึงมีการพัฒนาระบบ IHADM-KRS และ SSDM-KRS ขึ้น ซึ่งเป็นระบบกู้คืนกุญแจลับแบบ M-KRA ที่ไม่อาศัยศูนย์กลาง โดย IHADM-KRS มุ่งเน้นความยืดหยุ่นในการกำหนดจำนวน KRA ขั้นต่ำ เพื่อเพิ่มความมั่นคงปลอดภัยและรองรับการล่มของ KRA ได้ดีกว่า ขณะที่ SSDM-KRS เน้นความความเร็วในการประมวลผล มีโครงสร้างไม่ซับซ้อนเพื่อลดภาระการจัดการ ซึ่งงานวิจัยนี้มุ่งนำเสนอการทดลองเชิงลึกโดยทำการเปรียบเทียบประสิทธิภาพของ 2 ระบบ ในสามประเด็นหลัก ได้แก่ (1) เวลาที่ใช้ในการสร้าง KRF (2) เวลาที่ใช้ในการกู้คืนกุญแจในสถานการณ์ปกติ และ (3) เวลาที่ใช้ในการกู้คืนกุญแจเมื่อ KRA บางส่วนล่ม ซึ่งยังไม่มีการนำเสนอในงานวิจัยก่อนหน้า ผลการวิจัยช่วยให้เข้าใจข้อได้เปรียบและข้อจำกัดของแต่ละระบบได้ชัดเจนในบริบทการนำไปประยุกต์ใช้งาน

โดยผลการทดลองชี้ว่า IHADM-KRS เหมาะสมกับระบบที่ให้ความสำคัญกับความมั่นคงปลอดภัย และความสามารถในการกำหนดจำนวนขั้นต่ำของ KRA ที่ใช้ในการกู้คืนกุญแจลับ ให้เหมาะสมกับระดับนโยบายความมั่นคงปลอดภัย โดยแม้จะใช้เวลาประมวลผลมากกว่า แต่สามารถรักษาความถูกต้องและความสมบูรณ์ของการกู้คืนได้ดี แม้ในสถานการณ์ KRA ล่ม ซึ่งสอดคล้องกับแนวคิดของ NIST และสนับสนุนข้อเสนอในงานก่อนหน้าเกี่ยวกับการกระจายความรับผิดชอบเพื่อลดความเสี่ยงจากจุดล้มเหลวเพียงจุดเดียว ส่วน SSDM-KRS มีจุดเด่นอย่างชัดเจนด้านความเร็วในการสร้าง KRF และการกู้คืนกุญแจในสถานการณ์ปกติ อันเป็นผลจากโครงสร้างที่ไม่ซับซ้อนและกระบวนการทำงานที่รวดเร็ว ข้อสังเกตนี้สอดคล้องกับแนวคิดของการวิจัยกู้คืนกุญแจ (Lim et al., 2003) ที่ระบุว่าการลดความซับซ้อนของโครงสร้างสามารถช่วยเพิ่มความเร็วของระบบได้อย่างมีนัยสำคัญ

5.2 ข้อเสนอแนะการวิจัย

5.2.1 แนวทางการพัฒนาและต่อยอด

สามารถพัฒนาอัลกอริทึมในรูปแบบไฮบริดหรือผสมผสาน (Hybrid Adaptive Decentralized Key Recovery System) ซึ่งเป็นการสังเคราะห์ข้อดีของทั้งสองระบบเข้าด้วยกัน โดยผสานการทำงานระหว่าง IHADM-KRS และ SSDM-KRS เพื่อให้เกิดความสมดุลด้านความเร็วในการประมวลผลและความมั่นคงปลอดภัย เพิ่มสมรรถนะและประสิทธิภาพของการกู้คืนกุญแจลับให้สูงขึ้น โดยใช้หลักการปรับระดับความมั่นคงปลอดภัยแบบอัตโนมัติ ซึ่งพิจารณาจากค่าดัชนีความปลอดภัยแบบพลวัตเรียกว่า Adaptive Security Threshold (AST) (Canetti et al., 1999) โดยคำนวณจากตัวแปรตามสถานะของระบบ 3 ด้าน คือ (1) ความพร้อมของเอเจนต์ (Availability) (2) ความหน่วงของเวลาเฉลี่ยในระบบ (Latency) และ (3) ความเชื่อมั่นของการยืนยันตัวตน (Authentication Confidence)

อัลกอริทึมแบบไฮบริดนี้ เอื้อต่อการประยุกต์ใช้ในสภาพแวดล้อมที่ต้องการสมดุลระหว่างความเร็วและความมั่นคงปลอดภัย จากโหมดการทำงาน 2 โหมด คือ

(1) โหมดความเร็วสูง (Fast Recovery Mode) ใช้หลักการของ SSDM-KRS เพื่อให้การกู้คืนทำได้รวดเร็ว ระยะเวลาการรอคอยต่ำ

(2) โหมดความมั่นคงปลอดภัยสูง (Secure Recovery Mode) ใช้หลักการของ IHADM-KRS เพื่อเพิ่มความมั่นคงปลอดภัยในกรณีที่มีแนวโน้มการเกิดความเสี่ยง

ผลลัพธ์ที่คาดหวังคือ จะช่วยให้ระบบกู้คืนกุญแจลับมีสมรรถนะที่ดีกว่าระบบเดิมทั้งสองรูปแบบ โดยสามารถลดเวลาเฉลี่ยในการสร้าง KRF ได้ และเพิ่มความเสถียรของการกู้คืนในสภาวะที่เกิดความเสี่ยงได้อย่างมีนัยสำคัญ เป็นแนวทางใหม่ที่นำไปพัฒนาและใช้งานได้จริงบนระบบความมั่นคงปลอดภัยในยุคดิจิทัล

5.2.2 การทดสอบในสภาพแวดล้อมการโจมตีจริง

งานวิจัยในอนาคตอาจออกแบบการทดสอบโดยจำลองการโจมตีรูปแบบต่าง ๆ เช่น การโจมตีแบบสมรู้ร่วมคิด (Collusion Attack) หรือการโจมตีเพื่อทำให้เอเจนต์ล่ม (Denial of Service) เพื่อประเมินความทนทานของระบบในสภาพแวดล้อมที่ใกล้เคียงการใช้งานจริงมากที่สุด

6. เอกสารอ้างอิง

กนกวรรณ กันยะมี. (2566). การกระจายและการแชร์กุญแจลับอย่างง่ายบนระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่ไม่อาศัยศูนย์กลาง. *วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏมหาสารคาม, 6*(1), 104-115.

กนกวรรณ กันยะมี. (2566). การปรับปรุงฟิลด์การกู้คืนกุญแจ เพื่อแก้ปัญหาการสมรู้ร่วมคิดกันระหว่างเอเจนต์ บนระบบการกู้คืนกุญแจแบบไม่อาศัยศูนย์กลาง. *รายงานสืบเนื่องจากการประชุมวิชาการระดับชาติวิทยาศาสตร์และเทคโนโลยีระหว่างสถาบัน ครั้งที่ 9*. (น. 651-658). มหาวิทยาลัยหอการค้าไทย.

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., & Schneier, B. (1997). The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal, 2*(3), 241-257.

Al-Salqan, Y. Y. (1997). Cryptographic key recovery. *Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of Distributed Computing Systems* (pp. 34-37). IEEE Computer Society. https://doi.org/10.1109/FTDCS.1997.644700

Arbogast, J. K., Sumner, I. B., & Lam, M. O. (2018). Parallelizing Shamir's secret sharing algorithm. *Journal of Computing Sciences in Colleges, 33*(3), 12-18.

Canetti, R., Gennaro, R., Jarecki, S., Krawczyk, H., & Rabin, T. (1999). Adaptive security for threshold cryptosystems. In M. Wiener (Ed.), *Advances in cryptology—CRYPTO '99* (Vol. 1666, pp. 98–116). Springer. https://doi.org/10.1007/3-540-48405-1_7

Hughes, L. E. (2022). Basic cryptography: Symmetric key encryption. In Pro Active Directory Certificate Services (pp. 3-17). Apress. https://doi.org/10.1007/978-1-4842-7486-6_1

Kanyamee, K., & Sathitwiriyawong, C. (2014). High-availability decentralized cryptographic multi-agent key recovery. *The International Arab Journal of Information Technology, 11*(1), 52-60.

Kim, T., Kim, W., Seo, D., & Lee, I. (2021). Secure encapsulation schemes using key recovery system in IoMT environments. *Sensors, 21*(10), Article 3474. https://doi.org/10.3390/s21103474

Lim, S., Kang, S., & Sohn, J. (2003). Modeling of multiple agent based cryptographic key recovery protocol. *Proceedings of the 19th Annual Computer Security Applications Conference*, 119–128. IEEE Computer Society. https://doi.org/10.1109/CSAC.2003.1254317

National Institute of Standards and Technology. (1998). *Requirements for key recovery products: Final report*. Federal Information Processing Standard for Federal Key Management Infrastructure.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612-613. https://doi.org/10.1145/359168.359176

Stallings, W. (2023). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.