

การเพิ่มความมั่นคงในการบริหารจัดการกุญแจลับ สำหรับการกู้คืนกุญแจ แบบหลายเอเจนต์ที่อาศัยศูนย์กลางในการกู้คืนกุญแจ Enhancing Security in Secret Key Management for Multi-Agent Key Recovery Utilizing a Centralized Key Recovery Center

กนกวรรณ กันยะมี¹ และจรัมพร จันทร์ชู^{1*}

Kanokwan Kanyamee¹ and Jumroon Chankulchorn^{1*}

¹คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏอุดรดิตถ์

¹Faculty of Science and Technology, Uttaradit Rajabhat University

*Corresponding author: jumroon@uru.ac.th

Received: January 30, 2024

Revised: April 22, 2024

Accepted: April 30, 2024

บทคัดย่อ

ระบบการกู้คืนกุญแจลับ เป็นเทคโนโลยีที่มีความสำคัญในยุคการสื่อสารดิจิทัล ที่มีการนำวิทยาการเข้ารหัสลับมาใช้เพื่อเพิ่มความปลอดภัยของข้อมูล และรักษาความเป็นส่วนตัวของผู้ใช้งาน การวิจัยนี้เป็นการวิจัยเชิงพัฒนา มีวัตถุประสงค์เพื่อพัฒนารูปแบบการบริหารจัดการกุญแจลับ (Secret Key--Ks) รูปแบบใหม่ที่มีความมั่นคงปลอดภัย สำหรับการกู้คืนกุญแจแบบหลายเอเจนต์ (M-KRA) ที่อาศัยศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center--KRC) ทำงานร่วมกับเอเจนต์ (Key Recovery Agent--KRA) โดยเรียกรูปแบบนี้ว่า E-SHAM-KRS เป้าหมายการวิจัยคือ การนำเสนอกระบวนการจัดการกุญแจลับ Ks ให้เป็นความลับระหว่างผู้รับกับผู้ส่ง หรือ หน่วยงานที่มีสิทธิ์ในการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายเท่านั้น ทำให้การกู้คืนกุญแจ Ks มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ ตลอดจนผู้ใช้งานมีความเป็นส่วนตัว และรองรับการกู้คืนกุญแจได้ แม้ในกรณีที่ KRA ในกลุ่มการกู้คืนล้ม โดยทำงานบนโครงสร้างพื้นฐานกุญแจสาธารณะ จากการประเมินประสิทธิภาพของกระบวนการจัดการกุญแจลับ Ks ของ E-SHAM-KRS โดยได้ทำการเปรียบเทียบกับระบบเดิม พบว่า (1) มีความสามารถในการรักษาความลับของกุญแจ Ks ทำให้กุญแจมีความปลอดภัยสูง ไม่มีโอกาสเกิดการรั่วไหลของกุญแจ Ks ไปยังบุคคลที่สาม (2) พิลต์ในการกู้คืนกุญแจ มีขนาดเพิ่มขึ้นเล็กน้อย แต่มีความมั่นคงและมีความเป็นส่วนตัวสูงขึ้นอย่างมีนัยสำคัญ และ (3) ใช้เวลาในการสร้างพิลต์ในการกู้คืนกุญแจเพิ่มขึ้นเล็กน้อย เพื่อรองรับการจัดการกุญแจ Ks ให้มีความมั่นคงปลอดภัยเพิ่มขึ้น ทั้งนี้ E-SHAM-KRS ได้แก้ไขจุดอ่อนด้านการรั่วไหลของรหัสกุญแจลับได้ ส่งผลให้กระบวนการกู้คืนกุญแจมีความน่าเชื่อถือ และทำงานได้เต็มประสิทธิภาพในด้านความมั่นคงปลอดภัย

คำสำคัญ: ความมั่นคงปลอดภัย กุญแจลับ กู้คืนกุญแจ เอเจนต์ ศูนย์กลางการกู้คืนกุญแจ

Abstract

Key Recovery System is an important technology in the era of digital communication. Cryptography is used to increase data security and maintain user privacy. This research is a developmental research. The objective is to develop a new secure Secret Key--Ks management model for Multi-Agent Key Recovery--M-KRA that uses Key Recovery Center--KRC that works with Key recovery Agent--KRA. This method is called E-SHAM-KRS. The goal of this research is to present a model for the Ks management process to ensure confidentiality between the recipient and the sender or the agency that has legal access to the information. As a result, Ks recovery is secure, reliable, and provides users with privacy and supports key recovery even when KRA in the recovery group fails. It works on a public key infrastructure. The evaluation of the efficiency of the Ks management process of E-SHAM-KRS, which was compared with the previous system, shows that (1) E-SHAM-KRS can maintain the secret of Ks, resulting in the Ks having highly safe and there is no chance of the Ks being leaked to third parties. (2) Key Recover Filed--KRF has slightly increased in size but is significantly more secure and private. And (3) E-SHAM--KRS requires a slightly increased amount of time to generate KRF to support a more secure and stable Ks management function. Moreover, E-SHAM-KRS has successfully addressed vulnerabilities related to the leakage of Ks, resulting in a more reliable key recovery process.

Keywords: security, secret key, key recovery, agent, key recovery center



บทนำ

ยุคปัจจุบันการสื่อสารบนระบบเครือข่าย ถือเป็นส่วนหนึ่งที่มีความสำคัญในการดำเนินชีวิต สังเกตได้จากแนวโน้มอัตราการเติบโตของผู้ใช้งานเครือข่ายที่เพิ่มสูงขึ้นอย่างต่อเนื่อง เพื่อให้เกิดความแข็งแกร่งทางด้านความมั่นคงปลอดภัย (security) และความเป็นส่วนตัว (privacy) จึงมีการนำเทคโนโลยีวิทยาการเข้ารหัสลับ (cryptography technology) (Smart, 2016) มาใช้เพื่อรักษาความลับของข้อมูล โดยผู้ส่งจะทำการเข้ารหัสข้อมูล ด้วยกุญแจลับ (Secret Key หรือ Session Key--Ks) ซึ่งจะเป็นกระบวนการแปลงข้อความต้นฉบับ (plaintext) ให้เป็นข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้ (ciphertext) แล้วส่งข้อความดังกล่าวไปยังคู่สื่อสารคือผู้รับ ทางฝั่งผู้รับจะทำการถอดรหัสข้อมูล (data decryption) ที่ได้รับจากผู้ส่งข้างต้นด้วย Ks เช่นเดียวกัน ให้กลับเป็นข้อความต้นฉบับ โดยเรียกวิธีการดังกล่าวว่า การเข้ารหัสแบบสมมาตร (symmetric encryption) (Hughes, 2022) การใช้เทคโนโลยีดังกล่าวมีเพียงผู้รับและผู้ส่งเท่านั้น ที่จะสามารถอ่านข้อความตั้ง

ต้นได้เข้าใจ การเข้ารหัสลับแบบสมมาตรมีข้อดี คือ การดูแลจัดการกุญแจทำได้ง่าย สะดวก ไม่ซับซ้อน มีระยะเวลาตอบสนองที่รวดเร็ว

เมื่อเกิดกรณีที่ Ks ไม่สามารถใช้งานได้หรือสูญหาย ทำให้ผู้รับไม่สามารถถอดรหัสข้อความต้นฉบับได้ จึงจำเป็นต้องมีกลไกการกู้คืน Ks ที่เหมาะสม หรือในกรณีที่หน่วยงานของรัฐต้องการเข้าถึงข้อมูลที่ต้องสงสัยว่าเป็นภัยอันตรายต่อสังคมหรือบุคคลอื่น (โดยชอบด้วยกฎหมาย) จำเป็นต้องอาศัยกระบวนการกู้คืนกุญแจเช่นเดียวกัน โดยใช้ข้อมูลกุญแจและส่วนประกอบต่าง ๆ ที่เกี่ยวข้อง เช่น ข้อมูลการพิสูจน์ตัวจริง ข้อมูลของผู้ที่เกี่ยวข้องในการสื่อสาร จะถูกเก็บไว้ในฟิลด์ในการกู้คืนกุญแจ (Ket Recovery Field--KRF) (Kim et al., 2021)

ในกระบวนการกู้คืนกุญแจ Ks มีสองรูปแบบ ดังนี้ (1) การกู้คืนกุญแจแบบเอเจนต์เดี่ยว (Single Key Recovery Agent--S-KRA) (Lee et al., 1997) จะใช้เพียงหนึ่งเอเจนต์ในการกู้คืนกุญแจ มีโอกาสการรั่วไหลของ

กุญแจสูง (2) การกู้คืนกุญแจแบบหลายเอเจนต์ (Multiple Key Recovery Agent--M-KRA) (Lim et al., 2003) ใช้จำนวนเอเจนต์ ตั้งแต่ 2 เอเจนต์ขึ้นไป สำหรับการทำงานกู้คืนกุญแจ K_s ร่วมกัน ซึ่งเป็นวิธีที่ได้รับการยอมรับในปัจจุบัน ดังนั้นทำให้รูปแบบ M-KRA มีความมั่นคงปลอดภัยสูงกว่า S-KRA กล่าวคือ สามารถลดความเสี่ยงในหลาย ๆ กรณี อาทิเช่น การโจมตีเอเจนต์ที่ให้บริการ การปลอมแปลงเอเจนต์ การมีสิทธิ์ผูกขาดในกุญแจลับ ตลอดจนเมื่อเกิดการล่มของเอเจนต์ส่งผลให้ระบบไม่สามารถให้บริการได้ เป็นต้น (Lim et al., 2003; Kanyamee et al., 2010; Kanyamee et al., 2014)

การกู้คืนกุญแจ K_s จะอาศัยบุคคลที่สาม (third party) (Denning et al., 1997) ภายใต้โครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure--PKI) (Slaegell et al., 2006) ซึ่งมีวิธีการออกแบบการกู้คืน (โดยใช้บุคคลที่สาม) ได้ 2 วิธี คือ (1) อาศัยเอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent--KRA) วิธีนี้จะไม่มีส่วนกลางในการบริหารจัดการกุญแจ K_s เมื่อต้องการกู้คืนกุญแจ ผู้สื่อสาร (ผู้ส่ง-ผู้รับ) จะต้องติดต่อกับเอเจนต์โดยตรง และ (2) อาศัย KRC ทำงานร่วมกับเอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent--KRA) วิธีการนี้มี KRC ทำหน้าที่ในการจัดการกุญแจ K_s และต่อประสานกับ KRA เมื่อมีการร้องขอการกู้คืนกุญแจ KRC จะติดต่อให้ KRA ที่เกี่ยวข้องกู้คืนส่วนประกอบของกุญแจ และทำการรวบรวมเพื่อส่งให้กับผู้สื่อสารต่อไป วิธีการนี้จะช่วยลดภาระงานของผู้สื่อสารบนระบบเครือข่าย และให้ความเชื่อมั่นในด้านความมั่นคงปลอดภัยสูง

งานวิจัยที่ผ่านมาได้มีการนำเสนอการกู้คืนกุญแจหลายรูปแบบ ทั้งแบบ S-KRA (Lee et al., 1997) และ M-KRA (Lim et al., 2003; Kanyamee et al., 2010; Kanyamee et al., 2014) ที่ทำงานบนสภาพแวดล้อมและสถานการณ์แตกต่างกัน อาทิ การกู้คืนกุญแจบนแอปพลิเคชันสมาร์ตการ์ด (Huadpaknam et al., 2014) การสร้างข้อมูลสำหรับการกู้คืนกุญแจโดยใช้ทฤษฎีบทเศษเหลือของจีน (Kuacharoen et al., 2014) วิธีการห่อหุ้มฟิลด์สำหรับระบบการกู้คืนกุญแจ (Kim et al., 2021) วิธีการกู้คืนกุญแจส่วนตัวที่มีความปลอดภัย (Chang et al., 2023) เป็นต้น แต่ยังไม่มียานวิจัยที่นำเสนอวิธีการบริหารจัดการกุญแจลับสำหรับการกู้คืนกุญแจที่มีความมั่นคงปลอดภัยและน่าเชื่อถือ ดังนั้นในงานวิจัยนี้จะได้ทำการวิจัยเพื่อนำ

เสนอในประเด็นดังกล่าวข้างต้น โดยทำการวิจัยต่อยอดการกู้คืนกุญแจ SHAM-KRS (Kanyamee et al., 2010) ซึ่งเป็นการกู้คืนกุญแจแบบ M-KRA ที่กำหนดให้ KRC ทำหน้าที่ในการรวบรวม และกู้คืนกุญแจ K_s โดยวิธีการดังกล่าวส่งผลให้กุญแจ K_s ถูกส่งโดยบุคคลที่สาม (third party) อีกทั้งยังมีโอกาสเกิดการสมรู้ร่วมคิดกันระหว่างเอเจนต์ในกลุ่มการกู้คืนได้อีกด้วย เพื่อเป็นการปรับปรุงจุดอ่อนดังกล่าว ผู้วิจัยจะได้นำเสนอการพัฒนาแบบการบริหารจัดการกุญแจลับ K_s ในรูปแบบใหม่ เพื่อให้กุญแจ K_s มีความมั่นคงปลอดภัยสูงสุดอย่างเป็นรูปธรรม สามารถแก้ไขจุดอ่อนด้านการรั่วไหลของรหัสกุญแจลับได้โดยยังคงใช้รูปแบบการกู้คืนกุญแจแบบ M-KRA ที่อาศัย KRC ทำงานร่วมกับ KRA เรียกชื่อย่อว่า E-SHAM-KRS

E-SHAM-KRS พัฒนาต่อยอดด้านการจัดการกุญแจ K_s ให้เป็นความลับ ระหว่างผู้รับกับผู้ส่ง หรือ หน่วยงานที่มีสิทธิ์ในการเข้าถึงข้อมูลโดยชอบด้วยกฎหมายเท่านั้น ทำให้กระบวนการกู้คืนกุญแจ K_s มีความมั่นคงปลอดภัยและมีความน่าเชื่อถือสูง ตลอดจนผู้ใช้งานมีความเป็นส่วนตัว และยังสามารถกู้คืนกุญแจได้ แม้ในกรณีที่มี KRA ในกลุ่มการกู้คืนล่ม

วัตถุประสงค์การวิจัย

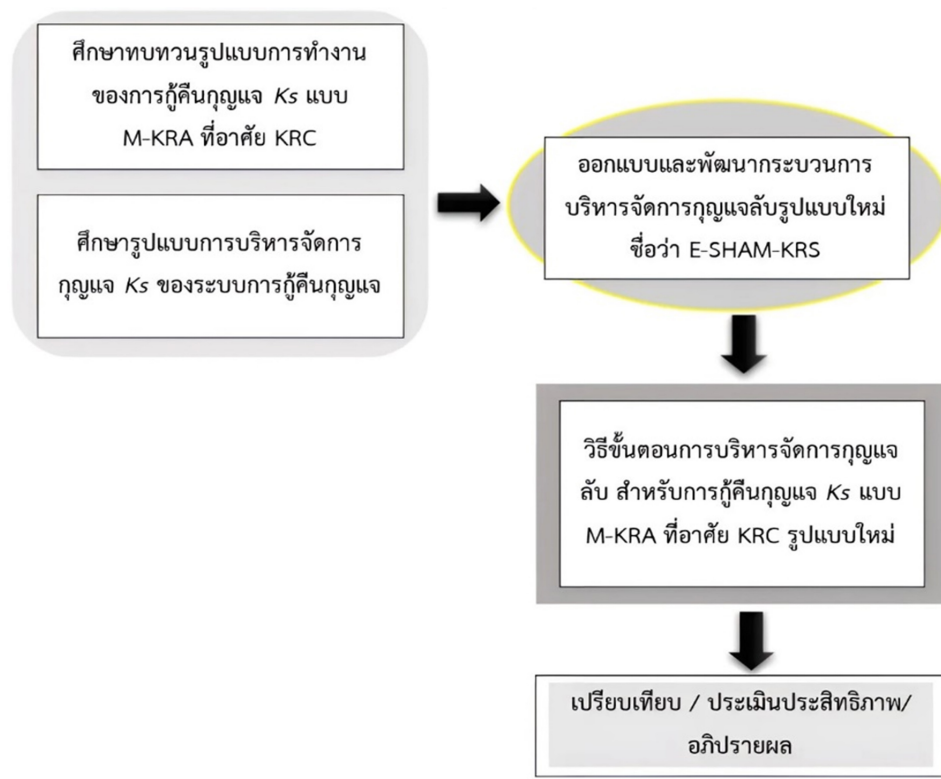
เพื่อวิจัยและพัฒนากระบวนการบริหารจัดการกุญแจ K_s รูปแบบใหม่ สำหรับการกู้คืนกุญแจแบบหลายเอเจนต์ที่ทำงานโดยอาศัยศูนย์กลางการกู้คืนกุญแจ เรียกชื่อว่า E-SHAM-KRS

สมมุติฐานการวิจัย

การพัฒนาแบบการบริหารจัดการกุญแจลับ K_s ในรูปแบบ E-SHAM-KRS จะสามารถแก้ไขจุดอ่อนด้านการรั่วไหลของกุญแจลับ K_s ไปยังบุคคลที่สามได้

กรอบแนวคิดการวิจัย

กรอบแนวคิดในการวิจัยเรื่อง การเพิ่มความมั่นคงในการบริหารจัดการกุญแจ K_s สำหรับการกู้คืนกุญแจแบบหลายเอเจนต์ ที่อาศัยศูนย์กลางในการกู้คืนกุญแจ สามารถแสดงได้ดังภาพ 1



ภาพ 1 กรอบแนวคิดการวิจัย

วิธีดำเนินการวิจัย

1. ทบทวนงานวิจัยที่เกี่ยวข้อง

1.1 ศึกษาทบทวนรูปแบบการบริหารจัดการกุญแจ และกระบวนการกู้คืนกุญแจแบบหลายเอเจนต์ ที่อาศัยศูนย์กลางการกู้คืนกุญแจ

1.2 ศึกษาประเด็นที่ต้องปรับปรุงพัฒนา เพื่อให้กระบวนการกู้คืนกุญแจลับมีความมั่นคงปลอดภัยมากขึ้น โดยเน้นการบริหารจัดการกุญแจลับ เพื่อให้กุญแจลับไม่ถูกเปิดเผยไปยังบุคคลที่สาม

2. ออกแบบและพัฒนา

2.1 ออกแบบและพัฒนากระบวนการบริหารจัดการกุญแจ Ks รูปแบบใหม่ สำหรับการกู้คืนกุญแจแบบ

หลายเอเจนต์ ที่ทำงานโดยอาศัยศูนย์กลางการกู้คืนกุญแจ (KRC) ร่วมกับเอเจนต์การกู้คืนกุญแจ (KRA) เรียกชื่อว่า E-SHAM-KRS

2.2 ออกแบบฟิลด์ในการกู้คืนกุญแจ Ks (Key Recovery Field--KRF) เพื่อให้กุญแจ Ks มีความมั่นคงปลอดภัยสูงขึ้น

3. ประเมินและสรุปผล

3.1 ประเมินกระบวนการทำงานในการบริหารจัดการกุญแจลับ ในด้านต่อไปนี้

3.1.1 เปรียบเทียบฟังก์ชันการทำงานการกู้คืนกุญแจ Ks

3.1.2 ขนาดของฟิลต์ในการกู้คืนกุญแจ

3.1.3 เวลาในการสร้างฟิลต์ในการกู้คืนกุญแจ
(ทดสอบและประเมินผลบนเครื่องคอมพิวเตอร์แล็ปท็อป
โปรเซสเซอร์ Intel (R) Core (TM) i5-13420H, 2.10 GHz)

3.2 สรุปผลการประเมิน

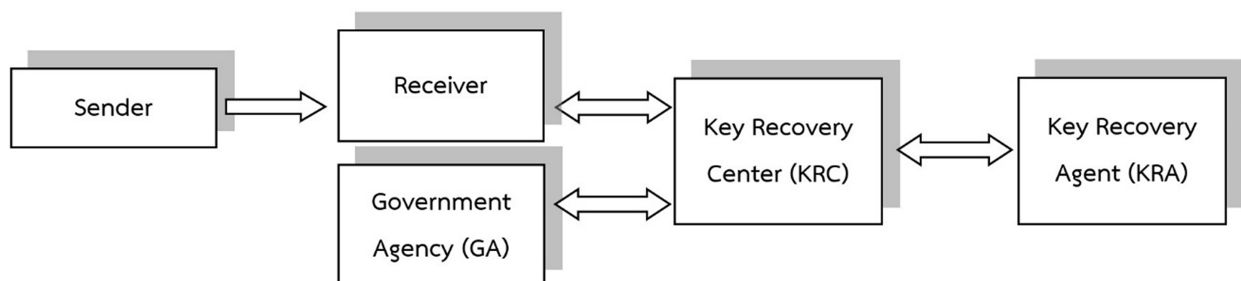
ผลการวิจัย

งานวิจัยนี้นำเสนอการบริหารจัดการกุญแจลับรูปแบบใหม่ สำหรับการกู้คืนกุญแจแบบหลายเอเจนต์ (M-KRA) ที่อาศัยศูนย์กลางในการกู้คืน (KRC) เรียกชื่อย่อว่า E-SHAM-KRS โดยมีจุดเด่นในเรื่องการรักษาความลับ (secret) และความมั่นคงปลอดภัย (security) ของกุญแจ K_s ส่งผลให้ผู้ใช้งานมีความเป็นส่วนตัวสูง (privacy) มีการทำงานโดยใช้ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center--KRC) ร่วมกับเอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent--KRA) โดยแต่ละส่วนทำหน้าที่กู้คืนส่วนประกอบของกุญแจอิสระจากกัน การออกแบบยังคงคำนึงถึงเรื่องความพร้อมใช้งาน คือ สามารถทำงานได้แม้ในกรณีที่ไม่มีบางเอเจนต์ในกลุ่มการกู้คืนล้ม (โดยเมื่อมีเอเจนต์ในกลุ่มการ

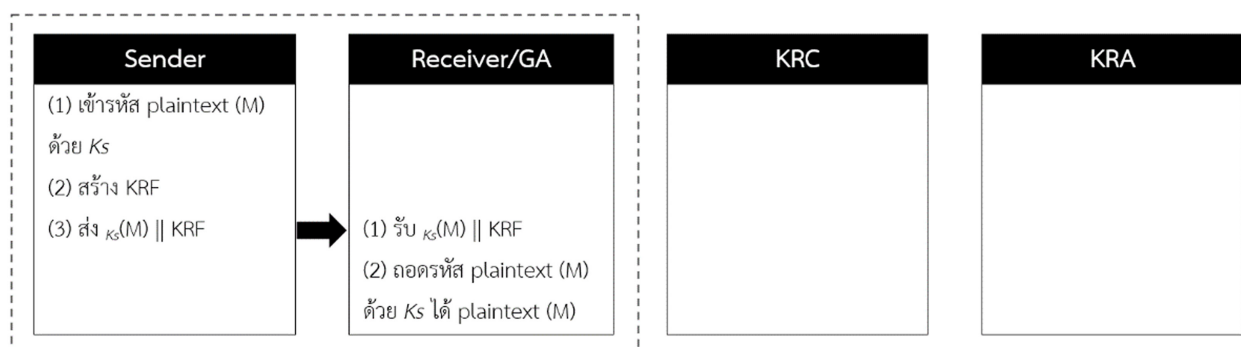
กู้คืนล้ม เอเจนต์อื่นที่อยู่ในกลุ่มการกู้คืนเดียวกันสามารถทำงานแทนกันได้) ทำให้ช่วยลดโอกาสการเกิดความล้มเหลวในการกู้คืนกุญแจ ทั้งนี้ผู้วิจัยได้ออกแบบกระบวนการบริหารจัดการกุญแจลับ ในส่วนของการสร้าง การจัดเก็บ และการใช้งานสำหรับการกู้คืนกุญแจ K_s เพื่อให้ทำงานได้อย่างดีและมีประสิทธิภาพ

1. องค์ประกอบของระบบการกู้คืนกุญแจ

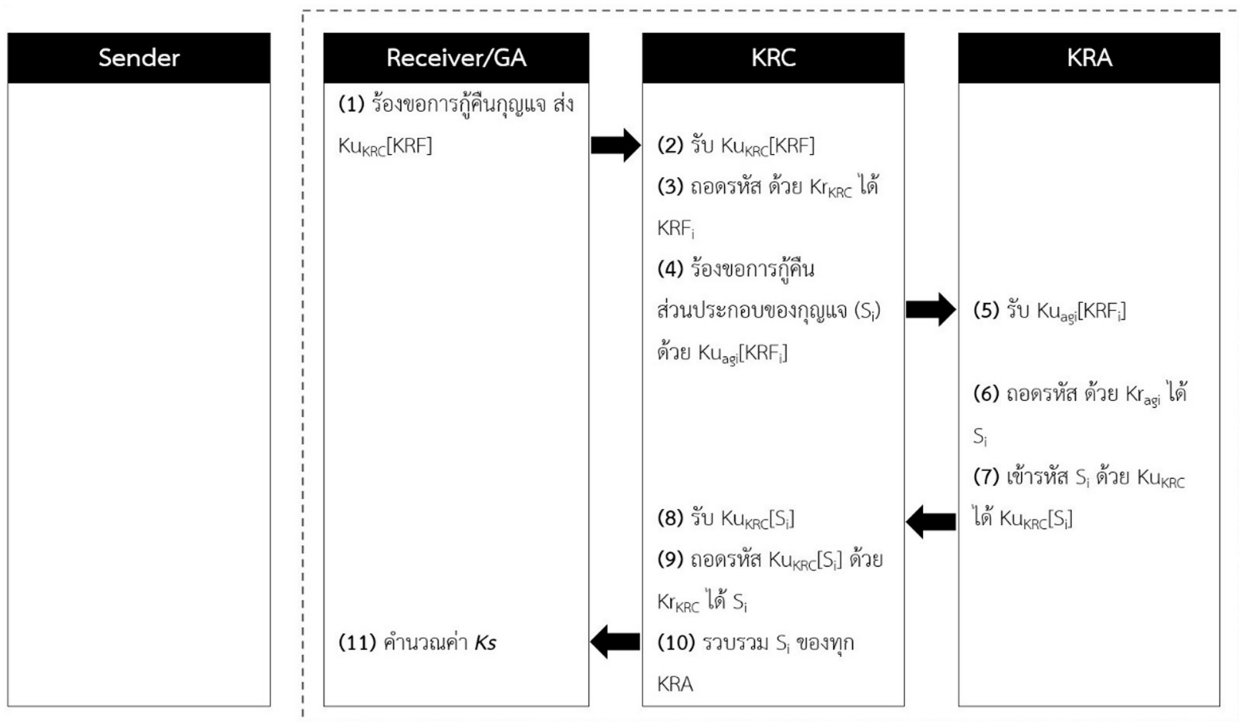
องค์ประกอบของการกู้คืนกุญแจแบบหลายเอเจนต์ที่อาศัยศูนย์กลางในการกู้คืน สามารถแสดงได้ดังภาพ 2 จากภาพ 2 ประกอบด้วยผู้ที่มีส่วนร่วม คือ (1) ผู้ส่ง (sender) (2) ผู้รับ (receiver) หรือ หน่วยงานรัฐ (Government Agency--GA) หรือ บุคคลที่สาม (third party) (3) ศูนย์กลางในการกู้คืนกุญแจ (KRC) และ (4) หน่วยงานหรือเอเจนต์ในการกู้คืนกุญแจ (KRA) ในการสื่อสารปกติจะเกิดขึ้นระหว่างผู้ส่งและผู้รับ ดังแสดงในภาพ 3 หากผู้รับไม่สามารถถอดรหัสได้ หรือหน่วยงานของรัฐต้องการถอดรหัสข้อมูล จึงต้องใช้บริการกู้คืนกุญแจ ซึ่งจะ เป็นหน้าที่ของ KRC และ KRA ดังแสดงในภาพ 4



ภาพ 2 องค์ประกอบของการกู้คืนกุญแจแบบหลายเอเจนต์ ที่อาศัยศูนย์กลางในการกู้คืน



ภาพ 3 ผู้มีส่วนร่วมในการสื่อสารในการกู้คืนกุญแจ



ภาพ 4 หน้าที่การทำงานในกระบวนการกู้คืนกุญแจ

จากภาพ 3 และภาพ 4 อธิบายกระบวนการกู้คืนกุญแจ ตามหน้าที่ของผู้เกี่ยวข้องได้ ดังนี้

(1) ผู้ส่ง (sender) ทำหน้าที่สร้างฟิลด์ที่ใช้ในการกู้คืนกุญแจ (KRF) และแนบฟิลด์ KRF เข้ากับข้อความต้นฉบับ ส่งไปยังผู้รับทุกครั้งที่มีการส่งข้อความต้นฉบับ

(2) ผู้รับ (receiver) หรือ หน่วยงานของรัฐ (government agency) หรือ บุคคลที่สาม (third party) ทำหน้าที่ ร้องขอการกู้คืนส่วนประกอบของกุญแจไปยัง KRC เมื่อกุญแจลับสูญหาย หรือไม่สามารถใช้ถอดรหัสข้อความต้นฉบับได้ และทำหน้าที่คำนวณข้อมูลกุญแจกลับเมื่อได้รับข้อมูลส่วนประกอบของกุญแจจาก KRC ครบถ้วน

(3) ศูนย์กลางในการกู้คืนกุญแจ (KRC) ทำหน้าที่ รวบรวมส่วนประกอบของกุญแจกลับจาก KRA เพื่อส่งให้กับผู้รับ หรือหน่วยงานของรัฐ หรือบุคคลที่สาม

(4) เอเจนต์ในการกู้คืนกุญแจ (KRA) ทำหน้าที่ กู้คืนส่วนประกอบของกุญแจกลับ เมื่อได้รับการร้องขอจาก KRC

2. กระบวนการบริหารจัดการกุญแจกลับ

การทำงานในช่วงเริ่มต้น ผู้ส่ง ร้องขอกุญแจกลับ (Ks) จากหน่วยงานให้บริการกุญแจ เช่น KDC (D'Arco, 2001) เป็นต้น เพื่อใช้ในการเข้ารหัสข้อมูลต้นฉบับ (M) ที่ต้องการส่งไปให้ผู้รับ และจะทำการแชร์กุญแจ Ks กันระหว่างผู้รับกับผู้ส่ง

กระบวนการบริหารจัดการกุญแจ Ks แบ่งออกเป็น 2 ขั้นตอน คือ (1) การสร้างส่วนประกอบของกุญแจและฟิลด์ KRF กระทำโดยผู้ส่ง และ (2) การกู้คืนส่วนประกอบของกุญแจ Ks กระทำโดย KRC และ KRA และการคำนวณกุญแจ Ks กระทำโดยผู้รับ โดยมีรายละเอียดดังต่อไปนี้

2.1) การสร้างส่วนประกอบของกุญแจ และฟิลด์ KRF แสดงในภาพ 5

❶ แบ่ง $K_s = n$ ชิ้น และคำนวณ S_R	$S_1, S_2, \dots S_n$ and S_R
❷ สุ่มค่า R	$R_1, R_2, \dots R_n$
❸ คำนวณ SGN	$SGN = R_1 \oplus R_2 \oplus \dots \oplus R_n$
❹ คำนวณ TT_i	$TT_i = S_i \oplus SGN$
❺ ประกอบ KRF	$Ku_{KRC}[KRF_i \text{'s} \parallel TT_1, TT_2, \dots TT_n \parallel Ku_R(S_R) \parallel Ku_G(S_R) \parallel h(SGN) \parallel \text{Other Information}]$

ภาพ 5 การสร้างส่วนประกอบของกุญแจ K_s และฟิลต์ KRF

ในขั้นตอนนี้ส่วนประกอบของกุญแจ K_s จะถูกห่อหุ้มอยู่ในฟิลต์ KRF และจะถูกแนบไปกับข้อมูลต้นฉบับ (M) ที่ผ่านการเข้ารหัสลับด้วยกุญแจลับ (K_s (M))) เรียบร้อยแล้วเพื่อส่งให้กับผู้รับ หากผู้รับต้องการร้องขอการกู้คืนกุญแจหรือหน่วยงานของรัฐต้องการตรวจสอบข้อมูล จะส่งคำร้องขอการกู้คืนกุญแจพร้อมกับฟิลต์ KRF ไปยัง KRC จากนั้น KRC จะส่งคำร้องขอส่วนประกอบของกุญแจไปยัง KRA เพื่อให้ทำการกู้คืน โดยมีขั้นตอนดังต่อไปนี้

2.1.1) แบ่งกุญแจลับ K_s ออกเป็น n ชิ้น เมื่อ n คือ จำนวน KRA ทั้งหมดที่ใช้ในการกู้คืนกุญแจ โดยได้ใช้แนวคิดพื้นฐานเรื่องการแชร์ความลับ (secret sharing) (Shamir, 1979)

กระบวนการแบ่งกุญแจลับ K_s สามารถทำได้ดังต่อไปนี้

2.1.1.1) สุ่มค่า S_i สำหรับ n เอเจนต์ เช่น $S_1, S_2, \dots, S_n$ สำหรับ $Agent_1, Agent_2, \dots, Agent_n$ ตามลำดับ

2.1.1.2) คำนวณค่า S_R สำหรับผู้รับ $Ku_R(S_R)$ และหน่วยงานรัฐ $Ku_G(S_R)$ ด้วยการ XOR ค่า S_i และกุญแจ K_s ดังสมการที่ (1)

$$S_R = S_1 \oplus S_2 \oplus \dots \oplus S_n \oplus K_s \quad (1)$$

2.1.2) สุ่มค่า R สำหรับทุก ๆ เอเจนต์ (R_i 's) เพื่อนำไปคำนวณหาค่าความลับของกลุ่มการกู้คืนกุญแจ (SGN) สำหรับการยืนยันตัวตนของ KRA

2.1.3) คำนวณหาค่าความลับ SGN ด้วยการ XOR ตัวแปร R_i ทั้งหมด ดังสมการที่ (2)

$$SGN = R_1 \oplus R_2 \oplus \dots \oplus R_n \quad (2)$$

2.1.4) คำนวณหาค่าตัวแปรพิเศษ (TT) สำหรับทุก ๆ เอเจนต์ (TT_i 's) เพื่อใช้ในการกู้คืน S_i ในกรณีที่บาง KRA ในกลุ่มการกู้คืนล้ม โดยสามารถคำนวณได้จากสมการที่ (3)

$$TT_i = S_i \oplus SGN \quad (3)$$

2.1.5) การประกอบฟิลต์ KRF

ฟิลต์ KRF ประกอบด้วยส่วนประกอบของกุญแจที่ถูกบรรจุอยู่ในฟิลต์ KRF ย่อย ๆ (KRF_i 's) ของเอเจนต์ในกลุ่มการกู้คืนกุญแจ (KRA_i) ซึ่งประกอบไปด้วย S_i, S_R, SGN, TT_i และ Other Information แต่ละส่วนประกอบมีความสำคัญ ดังนี้

S_i และ S_R คือ ส่วนประกอบของกุญแจ K_s

SGN เป็นค่าสำหรับการยืนยันตัวตนของ KRA ที่อยู่ในกลุ่มการกู้คืน

TT_i เป็นค่าสำหรับการกู้คืน S_i ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล้ม

Other Information เก็บค่าอื่น ๆ ที่จำเป็นสำหรับการพิสูจน์ตัวตนหรือการตรวจสอบเพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบ เช่น ใบรับรองกุญแจสาธารณะของเอเจนต์ และของผู้ที่มีสิทธิ์ในการร้องขอการกู้คืนกุญแจ เป็นต้น

โครงสร้างฟิลด์ KRF แสดงดังรูปแบบ (4) ประกอบด้วยฟิลด์ KRF_i จำนวน n ชั้น ดังรูปแบบที่ (5) นี้

$$KRF_i = \{Ku_{agi} [S_i \parallel SGN] \} \quad (4)$$

$$KRF = Ku_{KRC} [KRF_i 's \parallel TT_1.TT_2.TT_n \parallel Ku_R(S_R) \parallel Ku_G(S_R) \parallel h(SGN) \parallel Other Information] \quad (5)$$

ฟิลด์ KRF ประกอบด้วยข้อมูลดังต่อไปนี้ (1) S_i และ S_R คือ ส่วนประกอบของกุญแจ K_s (2) SGN คือ ตัวแปรสำหรับการระบุตัวตนของ KRA ในกลุ่มการกู้คืน (3) TT_i คือ ตัวแปรสำหรับการกู้คืนส่วนประกอบของกุญแจ K_s ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล้ม และ (4) Other Information คือ ข้อมูลที่จำเป็นสำหรับการระบุตัวตนของผู้ที่มีส่วนร่วมในระบบ

ฟิลด์ KRF จะถูกเข้ารหัสด้วยกุญแจสาธารณะของ KRC (Ku_{KRC}) และ KRF_i จะถูกเข้ารหัสด้วยกุญแจสาธารณะของ KRA (Ku_{agi}) ดังนั้น KRC และ KRA_i เท่านั้นที่สามารถถอดรหัส KRF และ KRF_i ได้ตามลำดับ

โดย KRC จะถอดรหัส KRF และส่ง KRF_i ไปยังเอเจนต์ในกลุ่มการกู้คืน เพื่อร้องขอส่วนประกอบของกุญแจ จากนั้นจะทำการรวบรวมส่วนประกอบของกุญแจเพื่อส่งให้กับผู้รับหรือหน่วยงานรัฐ ในการคำนวณหากุญแจลับ K_s ต่อไป

2.2) การกู้คืนส่วนประกอบของกุญแจ K_s และการคำนวณกุญแจ K_s

เมื่อผู้รับได้รับ K_s (M) และฟิลด์ KRF จะทำการถอดรหัสข้อมูลด้วยกุญแจ K_s ที่มีการแชร์กันในตอนต้นของการสื่อสาร

หากกุญแจ K_s ของผู้รับสูญหายหรือไม่สามารถใช้ในการถอดรหัสข้อมูลได้ ผู้รับจะทำการร้องขอการกู้คืนกุญแจ K_s ไปยัง KRC หรือหากหน่วยงานรัฐต้องการตรวจสอบข้อมูลที่ต้องสงสัย จะมีการร้องขอการกู้คืนกุญแจไปยัง KRC เช่นเดียวกัน ภาพรวมของการติดต่อสื่อสารระหว่างผู้ร้องขอการกู้คืนกุญแจ K_s กับ KRC สามารถแสดงได้ดังภาพ 6

ขั้นตอนการกู้คืนกุญแจ K_s สามารถแบ่งออกเป็นส่วนย่อย ๆ ได้ 2 ขั้นตอน ดังต่อไปนี้

2.2.1 การกู้คืนส่วนประกอบของกุญแจ K_s (S_i 's)

ในขั้นตอนนี้เป็นหน้าที่ของ KRC และ KRA กล่าวคือ เมื่อ KRC ได้รับการร้องขอการกู้คืนกุญแจจากผู้ร้องขอ ซึ่งก็คือผู้รับหรือหน่วยงานของรัฐ KRC จะส่ง KRF_i ไปยัง KRA_i เพื่อให้กู้คืนส่วนประกอบของกุญแจ K_s (S_i 's) โดยสามารถแบ่งกระบวนการนี้ ออกเป็น 2 ส่วน คือ

2.2.1.1 ส่วนการร้องขอการกู้คืนกุญแจ (Requester)

ในกรณีที่กุญแจ K_s สูญหายหรือเสียหาย ไม่สามารถถอดรหัสได้ มีกระบวนการ ดังนี้

(1) ผู้ร้องขอการกู้คืนกุญแจ ส่ง KRF ให้กับ KRC

(2) KRC ถอดรหัส KRF ด้วยกุญแจส่วนตัว (Kr_{KRC}) และส่งฟิลด์ KRF_i ให้กับ $Agent_i$ เมื่อ $i = 1$ ถึง n

2.2.1.2 ส่วนการกู้คืนส่วนประกอบของกุญแจ

โดย KRA มีกระบวนการ ดังนี้

(1) $Agent_i$ ถอดรหัสฟิลด์ KRF_i ด้วยกุญแจส่วนตัว (Kr_{agi}) จะได้ S_i และ SGN

(2) $Agent_i$ เข้ารหัส S_i และ SGN ด้วย Ku_{KRC}

(3) $Agent_i$ ส่ง $Ku_{KRC}[S_i \parallel SGN]$ ให้กับ KRC เพื่อให้ KRC รวบรวม

(4) KRC ถอดรหัส $Ku_{KRC}[S_i \parallel SGN]$ ด้วย Kr_{KRC} จะได้ S_i และ SGN

(5) KRC ตรวจสอบความถูกต้องของ Agent_i โดยการเปรียบเทียบ SGN ผ่านค่าแฮช h (SGN) หากถูกต้อง จะทำการรวบรวม S_i ของทุกเอเจนต์ในกลุ่มการกู้คืน และส่งต่อไปยังผู้ร้องขอการกู้คืน ๑ (ผู้รับหรือหน่วยงานรัฐ) ที่ทำการร้องขอส่วนประกอบของกุญแจ เพื่อนำไปคำนวณหากุญแจ K_s ต่อไป

2.2.2 การกู้คืนกุญแจ K_s

ส่วนนี้เป็นหน้าที่ของผู้ร้องขอการกู้คืน ๑ ในการคำนวณเพื่อกู้คืนกุญแจ K_s ซึ่งวิธีดังกล่าว เป็นการช่วยลดภาระของ KRC และ KRA และทำให้กุญแจ K_s มีความมั่นคง เป็นความลับ ผู้ใช้มีความเป็นส่วนตัวสูง กล่าวคือกุญแจ K_s จะรู้เฉพาะผู้รับและผู้ส่ง หรือคู่สนทนาเท่านั้น แต่ยังคงให้การสนับสนุนการตรวจสอบข้อมูลโดยขอด้วยกฎหมาย

การคำนวณการกู้คืนกุญแจ K_s มีขั้นตอนดังต่อไปนี้

- (1) ผู้ร้องขอถอดรหัส $[S_i || Ku_R(S_R)]$ หรือ $Ku_G(S_R) || SGN$ ด้วยกุญแจส่วนตัว จะได้ S_i, S_R และ SGN
- (2) ผู้ร้องขอตรวจสอบความถูกต้องของ Agent_i

โดยการเปรียบเทียบ SGN ผ่านค่าแฮช h (SGN) และรวบรวม S_i

(3) ถอดรหัส (S_R) ด้วยกุญแจส่วนตัว ได้ S_R

(4) คำนวณกุญแจ K_s ได้ดังสมการที่ (6) และนำกุญแจ K_s ไปใช้ในการถอดรหัสต่อไป

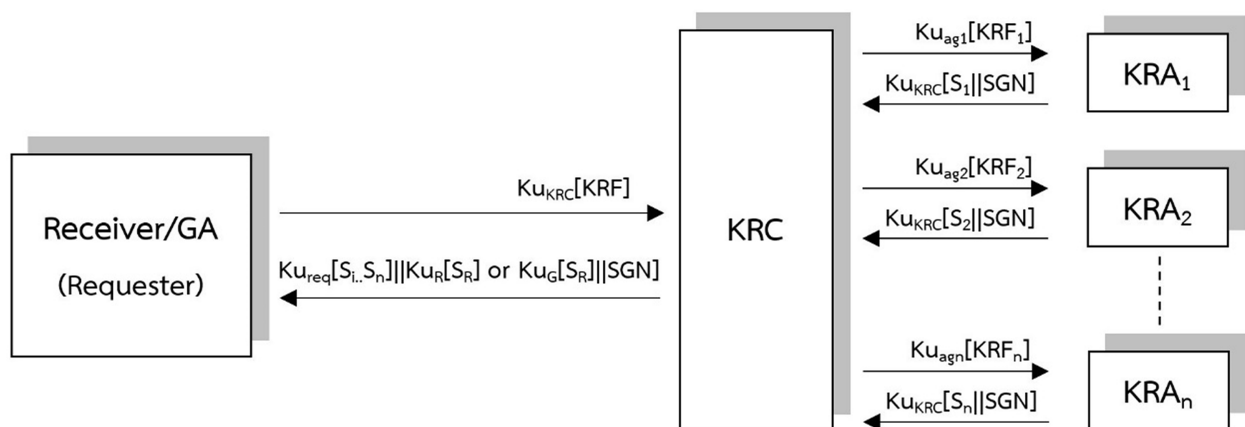
$$K_s = S_1 \oplus S_2 \oplus \dots \oplus S_n \oplus S_R \quad (6)$$

2.2.3 กรณีที่เอเจนต์ในกลุ่มการกู้คืนล้ม

ส่งผลให้ KRC รวบรวม S_i ได้ไม่ครบ ดังนั้น KRC จะทำการคำนวณค่า S_i จากตัวแปร TT_i ของ Agent_i (ที่ล้ม) โดยที่ S_i สามารถคำนวณได้จาก สมการที่ (7)

$$S_i = TT_i \oplus SGN \quad (7)$$

เมื่อ KRC รวบรวม S_i ครบทุกเอเจนต์ จะส่งไปให้ผู้รับหรือหน่วยงานรัฐ ที่ทำการร้องขอส่วนประกอบของกุญแจ เพื่อนำไปคำนวณหากุญแจ K_s ต่อไป



ภาพ 6 การกู้คืนส่วนประกอบของกุญแจลับ K_s

ผลการประเมินประสิทธิภาพ

การวิจัยได้ทดลองทำการประเมินประสิทธิภาพกระบวนการกู้คืนกุญแจ K_s ระหว่างวิธีการของรูปแบบเดิม คือ SHAM-KRS และรูปแบบใหม่ที่ได้พัฒนาขึ้น คือ E-SHAM-KRS ในประเด็นที่สำคัญ 3 ส่วน ประกอบด้วย (1) ฟังก์ชันการทำงานในการบริหารจัดการกุญแจและการกู้คืนกุญแจ K_s (2) ขนาดของฟิลต์ในการกู้คืนกุญแจ และ (3) เวลาในการสร้างฟิลต์ในการกู้คืนกุญแจ โดยจะได้แสดงรายละเอียด ดังต่อไปนี้

1. ฟังก์ชันความสามารถในการกู้คืนกุญแจ K_s

ในขั้นตอนนี้จะได้ทำการเปรียบเทียบฟังก์ชันการทำงานในการบริหารจัดการกุญแจ และการกู้คืนกุญแจ K_s ตามส่วนงานที่สำคัญ 6 ประเด็น ดังแสดงในตาราง 1

จากตาราง 1 ความสามารถในการบริหารจัดการกุญแจ และการกู้คืนกุญแจ K_s ในประเด็นที่ 1-5 ทั้ง 2 รูปแบบมีความสามารถเหมือนกัน ส่วนประเด็นที่ 6 คือ การประเมินโอกาสของการเกิดการรั่วไหลของกุญแจ K_s ไปยัง KRC และ KRA หรือการสมรู้ร่วมคิดกันระหว่างบุคคลที่สามนั้น พบว่า E-SHAM-KRS มีรูปแบบวิธีการบริหารจัดการกุญแจลับที่ดีกว่า คือ ในกระบวนการคำนวณกุญแจลับ K_s จะเป็นหน้าที่ของ ผู้รับ หรือบุคคลที่สามที่สามารถเข้าถึงข้อมูลได้โดยชอบด้วยกฎหมาย ทำให้สามารถจัดการปัญหาการรั่วไหลของรหัสกุญแจ K_s ได้ ในขณะที่ SHAM-KRS ยังมีจุดอ่อนในประเด็นนี้ เนื่องจากผู้ที่กู้คืนกุญแจลับ K_s จะกระทำโดย KRC

ดังนั้นจึงทำให้ E-SHAM-KRS มีความสามารถในการรักษาความลับของกุญแจ K_s กระบวนการกู้คืนกุญแจมีความน่าเชื่อถือ และทำงานได้เต็มประสิทธิภาพในด้านความมั่นคงปลอดภัย ข้อมูลจึงเป็นความลับ และผู้ใช้งานมีความเป็นส่วนตัว

2. ขนาดของฟิลต์ในการกู้คืนกุญแจ

การประเมินขนาดของฟิลต์ในการกู้คืนกุญแจ (KRF) ได้กำหนดให้ใช้เอเจนต์ จำนวน 2 4 6 8 และ 10 เอเจนต์ ผลการประเมิน เปรียบเทียบระหว่าง SHAM-KRS และ E-SHAM-KRS แสดงดังตาราง 2

จากตาราง 2 สามารถอธิบายได้ว่า เมื่อใช้จำนวน KRA ในการกู้คืนกุญแจเพิ่มขึ้น ส่งผลให้ขนาดของ KRF เพิ่มขึ้นตามลำดับ หากพิจารณาการเปรียบเทียบของทั้ง 2 รูปแบบจะสังเกตเห็นว่า KRF ของ E-SHAM-KRS มีขนาดมากกว่า SHAM-KRS เล็กน้อย อย่างไม่มีนัยสำคัญ ทั้งนี้เป็นผลเนื่องมาจากกระบวนการในการบริหารจัดการกุญแจของ E-SHAM-KRS ที่ให้ความสำคัญในการจัดการกุญแจ K_s ให้เป็นความลับสูงสุด โดยการเพิ่มค่าตัวแปร S_R เพื่อใช้ในการกู้คืนกุญแจ K_s จึงส่งผลให้ขนาดของ KRF เพิ่มขึ้นเล็กน้อย

3. เวลาในการสร้างฟิลต์ในการกู้คืนกุญแจ

การประเมินเวลาที่ใช้ในการสร้าง KRF ได้กำหนดให้ใช้เอเจนต์ จำนวน 2 4 6 8 และ 10 เอเจนต์ ผลการประเมิน เปรียบเทียบระหว่าง SHAM-KRS และ E-SHAM-KRS ดังแสดงในภาพ 7

จากภาพ 7 แสดงผลการวัดประเมินเวลาที่ใช้ในการสร้าง KRF (หน่วยเป็นวินาที) พบว่า E-SHAM-KRS ใช้เวลาในการสร้าง มากกว่า SHAM-KRS เล็กน้อย ซึ่งเป็นผลมาจากการเพิ่มตัวแปร S_R ในการกู้คืนกุญแจ เพื่อให้การบริหารจัดการกุญแจมีความมั่นคงปลอดภัยมากขึ้น

ตาราง 1

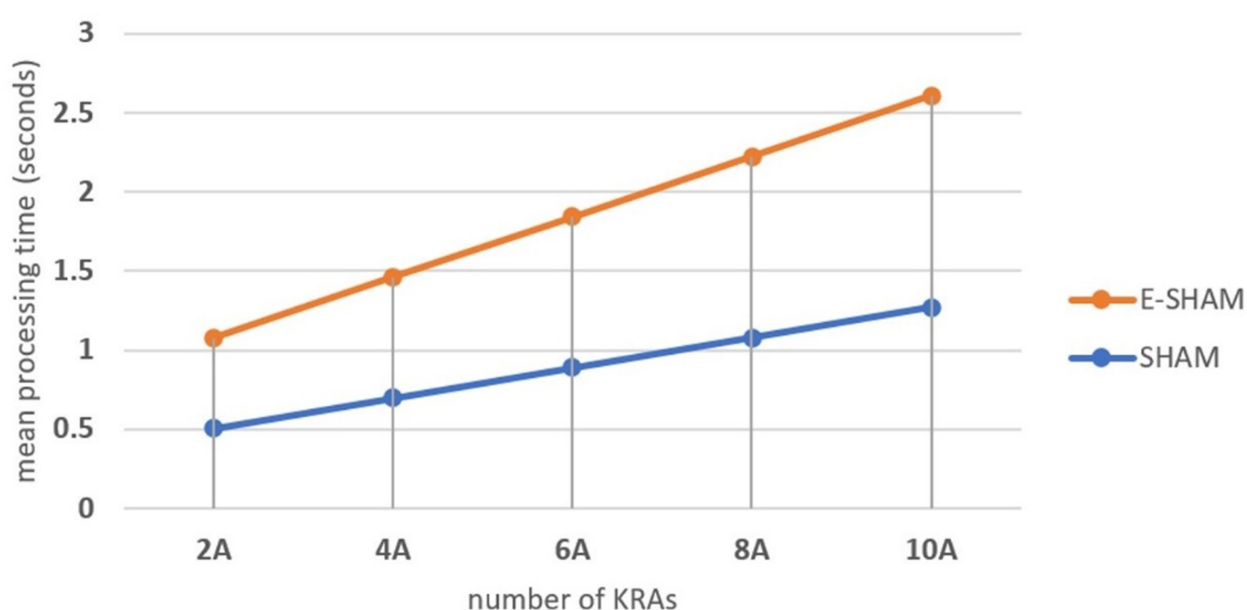
แสดงการเปรียบเทียบฟังก์ชันการทำงานในการบริหารจัดการกุญแจและการกู้คืนกุญแจ Ks

ความสามารถ	SHAM-KRS (รูปแบบเดิม)	E-SHAM-KRS (รูปแบบใหม่)
1) กุญแจเป็นความลับ Ks	✓	✓
2) กู้คืนกุญแจได้ เมื่อมีเอเจนต์ในกลุ่มการกู้คืนลุ่ม	✓	✓
3) มีฟังก์ชันการพิสูจน์ตัวตนของเอเจนต์	✓	✓
4) กู้คืนกุญแจโดยอาศัย KRC และ KRA ทำงานร่วมกัน	✓	✓
5) ทำงานบนพื้นฐาน PKI	✓	✓
6) ไม่มีโอกาสเกิดการรั่วไหลของกุญแจ Ks ไปยัง KRC และ KRA (บุคคลที่สาม)	-	✓

ตาราง 2

การเปรียบเทียบขนาดของไฟล์ในการกู้คืนกุญแจ (key recovery filed) (บิต)

จำนวน KRA	ขนาดของไฟล์ในการกู้คืนกุญแจ (บิต)	
	SHAM-KRS	E-SHAM-KRS
	(รูปแบบเดิม)	(รูปแบบใหม่)
2	2050	2306
4	2820	3076
6	3590	3846
8	4360	4616
10	5130	5386



ภาพ 7 การวัดประเมินเวลาที่ใช้ในการสร้าง KRF

การอภิปรายผล

จากการประเมินประสิทธิภาพของกระบวนการกู้คืนกุญแจ K_s ระหว่างวิธีการของรูปแบบเดิม คือ SHAM-KRS และรูปแบบใหม่ที่ได้พัฒนาขึ้น คือ E-SHAM-KRS ใน 3 ประเด็นที่สำคัญ พบว่า (1) การบริหารจัดการการกุญแจ E-SHAM-KRS สามารถแก้ไขจุดอ่อนด้านการรั่วไหลของรหัสกุญแจ K_s ได้ กล่าวคือ มีวิธีการบริหารจัดการการกุญแจ K_s ให้รู้เฉพาะผู้รับ-ผู้ส่ง และสนับสนุนการกู้คืนกุญแจในกรณีบุคคลที่สามต้องการเข้าถึงข้อมูลโดยชอบด้วยกฎหมาย ทำให้

กระบวนการกู้คืนกุญแจมีความน่าเชื่อถือ และทำงานได้เต็มประสิทธิภาพในด้านความมั่นคงปลอดภัย (2) ขนาดของ KRF ที่ห่อหุ้มความลับของกุญแจลับ K_s : E-SHAM-KRS มีขนาดใหญ่กว่า SHAM-KRS เพียงเล็กน้อยอย่างไม่มีนัยสำคัญ เนื่องจากมีการเพิ่มค่าตัวแปรด้านความปลอดภัย และ (3) เวลาที่ใช้ในกระบวนการสร้าง KRF: SHAM-KRS ใช้เวลามากกว่า SHAM-KRS เพียงเล็กน้อยอย่างไม่มีนัยสำคัญ เนื่องจากต้องใช้เวลาในกระบวนการสร้างตัวแปรสำหรับจัดการการกุญแจ K_s ให้เป็นความลับ



References

- Chang, W., & Tsay, R. (2023). A secure and reliable private key recovery method. *Proceedings of International Conference on Consumer Electronics* (pp. 535-536). Taiwan: Pingtung.
- D'Arco, P. (2001). On the distribution of a key distribution center. *Proceedings of Theoretical Computer Science* (pp. 357-369). Italy: Torino.
- Denning, D., & Branstad, D. (1997). A taxonomy for key recovery encryption systems. *Communications of the ACM*, 39(3), 34-40. <https://doi.org/10.1145/227234.227239>
- Huadpaknam, P., Pirak, C., & Mathar, R. (2014). A novel security key recovery framework for smart grid applications. *Proceedings of Asia-Pacific Conference on Communication* (pp. 387-390). Pattaya: IEEE (in Thai)
- Hughes, L.E. (2022). Basic cryptography: Symmetric Key Encryption. In L. E. Hughes (Ed.) *Pro Active Directory certificate sServices* (pp. 3-17). Berkeley, CA: Apress.
- Kanyamee, K., & Sathitwiriawong, C. (2010). A simple high-availability multiple-agent key recovery system. *Proceedings of International Conference for Internet Technology and Secured Transactions* (pp.734-739). London: IEEE
- Kanyamee, K., & Sathitwiriawong, C. (2010). High-availability decentralized multi-agent key recovery system. *Proceedings of International Conference on Computer and Information Science* (pp. 290-294). Shanghai: IEEE
- Kanyamee, K., & Sathitwiriawong, C. (2014). High-availability decentralized cryptographic multi-agent key recovery. *International Arab Journal of Information Technology (IAJIT)*, 11(1), 52-55. <https://www.iajit.org/portal/PDF/vol.11,no.1/4749.pdf>
- Kim, T., Kim, W., Seo, D., & Lee, I. Y. (2021). A secure encapsulation schemes based on Key Recovery System. In Y. Park, D. Jadav and T. Austin (Eds.), *Proceedings of Silicon Valley Cybersecurity Conference* (pp. 25-37). Cham: Springer International Publishing.

- Kim, T., Kim, W., Seo, D., & Lee, I. Y. (2021). Secure encapsulation schemes using key recovery system in IoMT environments. *Sensors Journal*, 21(10), 1-23. <https://doi.org/10.3390/s21103474>
- Kuacharoen, P. (2014). Generating data recovery keys using Chinese Remainder Theorem. *Journal of Computational and Theoretical Nanoscience*, 20(10), 2157-2161. <https://doi.org/10.1166/asl.2014.5650>
- Lee, Y. C., & Lai, C. S. (1997). On the key recovery of the key escrow system. *Proceedings of 13th Annual Computer Security Applications Conference* (pp. 216–20). San Diego: IEEE.
- Lim, S., Hani, H., Kim, M., & Kim, T. (2001). In design of key recovery system using multiple agent technology for electronic commerce. *Proceedings of the Industrial Electronics* (pp. 1351-1356). Korea South: IEEE.
- Lim, S., Kang, S., & Sohn, J. (2003). Modeling of multiple agent based cryptographic key recovery protocol. *Proceedings of 19th Annual Computer Security Applications Conference* (pp. 19–28). USA: IEEE
- Shamir, A. (1979). How to share a secret. *Info & Claims Communications of the ACM*, 22(11), 612-623. <http://dx.doi.org/10.1145/359168.359176>
- Slagell, A., Bonilla, R., & Yurcik, W. (2006). A survey of PKI components and scalability issues. *Proceedings of the 25th IEEE International Performance Computing and Communications Conference, IPCCC 2006, April 10-12, 2006* (p. 10). Arizona: IEEE
- Smart, N. (2016). *Cryptography made simple (Information Security and Cryptography)*. Berlin: Springer.

