ระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่มีความมั่นคงและยืดหยุ่นสูง

จันทร์บูรณ์ สถิตวิริยวงศ์[1] และ กนกวรรณ กันยะมี[2]

[1]คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง กรุงเทพมหานคร

[2]คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏอุตรดิตถ์ จ.อุตรดิตถ์

Emails: chanboon@it.kmitl.ac.th, kikuit@hotmail.com

บทคัดย่อ

การเข้ารหัสข้อมูลโดยใช้กุญแจลับเป็นการเพิ่มความมั่นคงปลอดภัยให้กับข้อมูลที่ส่งผ่านระบบเครือข่าย เมื่อผู้รับข้อมูลไม่สามารถถอดรหัสข้อมูลหรือภาครัฐต้องการใช้สิทธิ์ในการเข้าถึงข้อมูล จะต้องขอใช้บริการกู้คืนกุญแจ ดังนั้นงานวิจัยนี้จึงได้เสนอระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่มีความมั่นคงและยืดหยุ่นสูง ที่มีชื่อว่า เอสเอฟเอ็ม-เคอาร์เอส (SFM-KRS: Secure and Flexible Multiple-Agent Key Recovery System) โดยเน้นกระบวนการทำงานที่มีความมั่นคงและความยืดหยุ่นสูงในการบริหารจัดการจำนวนเอเจนต์ที่ใช้ในการกู้คืนกุญแจ ให้สอดคล้องกับโยบายและสภาพแวดล้อมของการใช้งาน และได้ออกแบบฟิลด์ที่ใช้ในการกู้คืนกุญแจที่มีความเหมาะสมสำหรับการกู้คืนกุญแจอย่างถูกต้องและรวดเร็ว แม้เกิดเหตุการณ์ที่มีเอเจนต์ในกลุ่มการกู้คืนล่ม ทั้งนี้ระบบยังให้การสนับสนุนการตรวจสอบข้อมูลโดยชอบด้วยกฎหมายอีกด้วย

คำสำคัญ—การกู้คืนกุญแจ; เอเจนต์ในการกู้คืนกุญแจ; ฟิลด์ในการกู้คืนกุญแจ; กุญแจเข้ารหัสลับ; การร่วมกันรักษาความลับ

1. บทนำ

ในปัจจุบันการติดต่อสื่อสารข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ตเกิดขึ้นอย่างกว้างขวางทั่วโลก สังเกตได้จากอัตราการเติบโตของผู้ใช้งานเครือข่ายที่เพิ่มขึ้นอย่างต่อเนื่อง เพื่อให้การติดต่อสื่อสารเกิดความมั่นคงและมีความเป็นส่วนตัว จึงมีการใช้เทคโนโลยีวิทยาการเข้ารหัสลับ (Cryptography Technology) โดยการใช้กุญแจ (Key) สำหรับการเข้ารหัสลับและถอดรหัสลับข้อมูล อย่างไรก็ตาม อาจมีการนำเทคโนโลยีนี้ไปใช้ในทางที่มิชอบ คือใช้การเข้ารหัสลับเพื่อการปิดบังซ่อนเร้นการกระทำที่เป็นอันตรายต่อผู้อื่นและสังคม ดังนั้น จึงเป็นจุดเริ่มต้นของการออกกฎหมายคุ้มครองผู้ใช้งานจากภัยคุกคามต่าง ๆ ด้วยการให้อำนาจสิทธิ์แก่ภาครัฐในการตรวจสอบข้อมูลที่ต้องสงสัยที่มีการส่งผ่านระบบเครือข่าย

เริ่มจากรัฐบาลสหรัฐอเมริกาได้ประกาศใช้ระบบการเข้ารหัสลับแบบใหม่ เรียกว่า ระบบฝากกุญแจ (Key Escrow System (KES)) [1] และประกาศให้ใช้มาตรฐานการเข้ารหัสลับแบบสมมาตร (Symmetric Encryption) วิธีนี้เอื้อให้แก่ภาครัฐในการเข้าถึงข้อมูลที่ต้องการตรวจสอบด้วยการจัดเก็บกุญแจไว้กับซอฟต์แวร์ที่มีภาครัฐเป็นผู้รับผิดชอบ ซึ่งจะช่วยให้รัฐบาลสามารถตรวจสอบข้อมูลที่ต้องสงสัยและสกัดกั้นการกระทำอันเป็นการบ่อนทำลายความมั่นคงทางสังคมได้ แต่จะส่งผลให้ความเป็นส่วนตัวของผู้ใช้งานลดน้อยลง

ต่อมาทีไอเอส (Trusted Information System: TIS) ได้นำเสนอระบบการกู้คืนกุญแจ (Key Recovery System) [2] ขึ้นเพื่อแก้ปัญหาเรื่องความเป็นส่วนตัว และแก้ปัญหากุญแจเข้ารหัสลับแบบใช้ครั้งเดียว (Session Key) ของผู้รับหาย (ต่อจากนี้จะเรียกย่อ ๆ ว่า กุญแจลับ) โดยระบบนี้ไม่ใช้วิธีการฝากกุญแจ แต่จะใช้วิธีการเก็บกุญแจลับไว้ในฟิลด์สำหรับการกู้คืนกุญแจ (Key Recovery Field: KRF) โดยจะเก็บ KRF ไว้ที่ผู้รับ เมื่อผู้รับต้องการกู้คืนกุญแจ หรือเมื่อรัฐบาลต้องการตรวจสอบข้อมูลจึงจะส่ง KRF ให้กับหน่วยงานที่ทำหน้าที่กู้คืนกุญแจ วิธีการนี้จะทำให้ผู้ใช้งานระบบมีความเป็นส่วนตัวมากขึ้น กุญแจมีความมั่นคง และลดปัญหาของการใช้ฐานข้อมูลขนาดใหญ่

จากนั้นก็ได้มีการปรับปรุงพัฒนาวิธีการกู้คืนกุญแจอย่างต่อเนื่อง งานวิจัยในช่วงแรก จะเป็นการนำเสนอแนวทางการกู้คืนกุญแจแบบเอเจนต์เดี่ยว (Single Key Recovery Agent: S-KRA) [3, 4] โดยมีเอเจนต์ที่ให้บริการกู้คืนกุญแจ (Key Recovery Agent: KRA) ทำหน้าที่ในการกู้คืนกุญแจ และสนับสนุนการตรวจสอบข้อมูลโดยชอบด้วยกฎหมาย แต่ระบบการกู้คืนกุญแจแบบเอเจนต์เดี่ยวยังมีจุดอ่อนอยู่หลายประการ เช่น ความลับของกุญแจลับ ปัญหาภัยคุกคามที่มีต่อระบบและกุญแจลับ และปัญหาการผูกขาดในการรักษาความลับของกุญแจลับ เป็นต้น

งานวิจัยในช่วงหลังได้เพิ่มความมั่นคงของระบบการกู้คืนกุญแจเพื่อแก้ปัญหาภัยคุกคาม ลดโอกาสการสมรู้ร่วมคิด (Collusion) และลดปัญหาการผูกขาดกุญแจ โดยการนำเสนอแนวทางการกู้คืนกุญแจแบบใช้หลายเอเจนต์ (Multiple Key Recovery Agent: M-KRS) [5, 6] เช่น งานวิจัย Multiple Agent Model [6] ที่ได้ทำการออกแบบให้แต่ละ KRA ที่อยู่ในกลุ่มการกู้คืนกุญแจ ทำหน้าที่ในการกู้คืนส่วนประกอบของกุญแจ โดยให้ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center: KRC) ทำหน้าที่เป็นศูนย์กลางในการประสานงานระหว่าง KRA ต่าง ๆ กับผู้ร้องขอการกู้คืนกุญแจ (Requester) และได้ออกแบบให้ระบบมีการสนับสนุนการตรวจสอบข้อมูลโดยชอบด้วยกฎหมายด้วยเช่นกัน

อย่างไรก็ตามยังพบจุดอ่อนของระบบ M-KRS ไม่ว่าจะเป็นประเด็นทางด้าน (1) ความมั่นคงของกุญแจลับ (2) ระบบไม่มีความพร้อมใช้งาน หรือไม่สามารถให้บริการกู้คืนกุญแจได้ เมื่อมีเอเจนต์ที่อยู่ในกลุ่ม

การกู้คืนล่มหรือขัดข้องในการให้บริการ และ (3) ระบบยังขาดความสามารถในการตรวจสอบเอเจนต์แปลกปลอม

จากปัญหาดังกล่าว จึงเกิดงานวิจัย เอสเอชเอเอ็ม-เคอาร์เอส (SHAM-KRS: Simple High-Availability Multiple-agent Key Recovery System) ขึ้น [7] ซึ่งเป็นงานวิจัยที่สามารถแก้ปัญหาดังกล่าวข้างต้นได้ทั้งหมด โดย SHAM-KRS เป็นระบบการกู้คืนกุญแจที่มีกระบวนการกู้คืนกุญแจลับที่ง่ายและไม่ซับซ้อน ให้ความสำคัญในเรื่องความลับของกุญแจ และมีการออกแบบ KRF ที่ใช้แนวคิดการใช้หลายเอเจนต์ร่วมกันรักษาความลับ (Secret Splitting) ของกุญแจ อย่างไรก็ตาม ด้วยกระบวนการทำงานและโครงสร้าง KRF ของ SHAM-KRS ที่มีความเรียบง่าย ไม่ซับซ้อน ระบบจึงยังขาดฟังก์ชั่นในการบริหารจัดการจำนวนเอเจนต์ขั้นต่ำในการกู้คืนกุญแจลับ

ดังนั้นเพื่อให้ระบบมีความมั่นคงสูงขึ้น และมีความยืดหยุ่นในการบริหารจัดการจำนวนเอเจนต์ขั้นต่ำในการกู้คืนกุญแจลับให้สอดคล้องกับนโยบายและสภาพแวดล้อมของการใช้งานได้ ผู้วิจัยจึงได้นำเสนอระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่มีความมั่นคงและยืดหยุ่นสูงคือ เอสเอฟเอ็ม-เคอาร์เอส (SFM-KRS : Secure and Flexible Multiple-Agent Key Recovery System) โดยที่ SFM-KRS มีคุณสมบัติและความสามารถของระบบดังนี้ (1) ผู้ดูแลระบบหรือผู้ใช้งานสามารถกำหนดเอเจนต์ขั้นต่ำในการกู้คืนกุญแจลับได้ (2) มีความพร้อมใช้งานและมีความน่าเชื่อถือสูง เนื่องจากสามารถรองรับกรณีที่มีปัญหาเอเจนต์ที่อยู่ในกลุ่มการกู้คืนล่ม (Single point of failure) ดังนั้นเมื่อเกิดปัญหาดังกล่าวขึ้น ระบบก็ยังสามารถให้บริการกู้คืนกุญแจได้ (3) มีฟังก์ชั่นการตรวจสอบหรือการพิสูจน์ตัวจริงของเอเจนต์ในกลุ่มการกู้คืน และ (4) SFM-KRS มี KRF ที่เป็นมาตรฐาน สามารถรองรับการตรวจสอบข้อมูลโดยชอบด้วยกฎหมาย (Law enforcement) จากรัฐบาลหรือหน่วยงานที่รับผิดชอบได้ โดยกำหนดให้ระบบทำงานบนโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure) หรือพีเคไอ (PKI) [8]

2. คำจำกัดความ

การกู้คืนกุญแจ (Key Recovery) คือ การกู้คืนกุญแจลับ ในกรณีที่กุญแจลับทางฝั่งผู้รับสูญหายหรือเสียหาย หรืออีกนัยหนึ่งคือ การกู้คืนกุญแจลับเพื่อการเข้าถึงข้อมูลที่ต้องสงสัยของคู่สื่อสาร โดยชอบด้วยกฎหมาย

ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center: KRC) คือ หน่วยงานที่ทำหน้าที่ในการให้บริการกู้คืนส่วนประกอบของกุญแจ หรือกู้คืนกุญแจ และทำหน้าที่เป็นศูนย์กลางในการติดต่อสื่อสารสำหรับทำภารกิจในการกู้คืนกุญแจ เมื่อได้รับการร้องขอการกู้คืนจากผู้ใช้บริการ

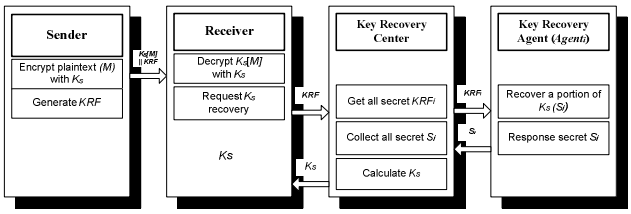
เอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent: KRA) คือ หน่วยงานที่ทำหน้าที่ในการให้บริการกู้คืนส่วนประกอบของกุญแจลับ เมื่อได้รับการร้องขอการกู้คืนกุญแจจากผู้ใช้บริการ

ฟิลด์ในการกู้คืนกุญแจ (Key Recovery Field: KRF) คือ ฟิลด์ที่บรรจุข้อมูลที่เกี่ยวข้องกับกุญแจลับ ใช้สำหรับการกู้คืนกุญแจลับ โดยผู้ร้องขอจะส่งฟิลด์นี้ให้กับหน่วยงานที่ทำหน้าที่ในการกู้คืนกุญแจหรือกู้คืนส่วนประกอบของกุญแจ

3. ระบบการกู้คืนกุญแจ SFM-KRS

SFM-KRS เป็นระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่มีความมั่นคงและยืดหยุ่นสูง โดยมีองค์ประกอบที่เกี่ยวข้องในระบบดังนี้ (1) ผู้ส่ง (Sender) (2) ผู้รับ (Receiver) (3) ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center: KRC) และ(4) เอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent: KRA) ในการเริ่มต้นกระบวนการทำงานทุกองค์ประกอบของระบบ จะต้องมีกุญแจคู่ของตัวเอง คือ กุญแจส่วนตัว (Kr) และกุญแจสาธารณะ (Ku) ที่มีใบรับรองจากหน่วยงานออกใบรับรอง (Certificate Authority: CA) เพื่อใช้ในการสื่อสารระหว่างกันอย่างมั่นคงปลอดภัย โดยมีการเชื่อถือกัน (Trusted) บนโครงสร้างพื้นฐานของกุญแจสาธารณะ (Public Key Infrastructure: PKI)

ภาพรวมการทำงานของระบบ SFM-KRS ได้แสดงในรูปที่ 1 และมีขั้นตอนการทำงานดังต่อไปนี้



รูปที่ 1. ภาพรวมการทำงานของระบบ SFM-KRS

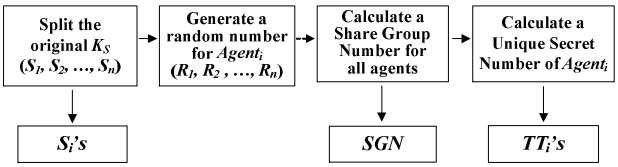
3.1 กระบวนการด้านผู้ส่ง

ในขั้นตอนเริ่มต้นของผู้ส่งนั้น จะมีการร้องขอกุญแจลับ (K_S) จากหน่วยงานให้บริการกุญแจ เช่น KDC [9] หรือ เคอร์เบอรอส [10] เป็นต้น เพื่อใช้ในการเข้ารหัสข้อมูลที่ต้องการส่งไปให้ผู้รับ ในขั้นตอนนี้จะมีการแชร์กุญแจลับกันระหว่างผู้รับกับผู้ส่ง

การรับส่งข้อมูลที่รองรับการกู้คืนกุญแจลับ ผู้ส่งจะต้องสร้าง KRF เพื่อใช้สำหรับการกู้คืนกุญแจลับ ซึ่งฟิลด์นี้จะถูกแนบไปกับข้อมูลต้นฉบับที่ถูกเข้ารหัสด้วยกุญแจลับ ($K_S[M]||KRF$) เพื่อส่งให้ผู้รับ กระบวนการสร้าง KRF สามารถแสดงได้ดังต่อไปนี้

3.1.1 ขั้นตอนการเตรียมการสร้าง KRF

กระบวนการเตรียมการสร้าง KRF เพื่อนำไปใช้ในการกู้คืนกุญแจลับสามารถอธิบายได้ดังรูปที่ 2



รูปที่ 2. การเตรียมค่าส่วนประกอบย่อยของ KRF

ภายใน KRF ประกอบด้วย (1) KRF ย่อย ๆ (KRF_i) และ (2) *Other Information* โดย KRF_i จะมีจำนวน n ชิ้น (เมื่อ n คือ จำนวนเอเจนต์ทั้งหมดที่ใช้ในการกู้คืนกุญแจ)

ภายใน KRF_i จะประกอบด้วย (1) ส่วนประกอบของกุญแจ (S_i) (2) Share Group Number (*SGN*) และ (3) Unique Secret Number (TT_i)

แต่ละส่วนประกอบมีความสำคัญดังนี้คือ S_i คือส่วนประกอบของกุญแจลับ *SGN* เป็นค่าสำหรับการระบุตัวตนของแต่ละ KRA ที่อยู่ในกลุ่มการกู้คืน *(Agent)* TT_i เป็นค่าสำหรับการกู้คืน S_i ในกรณีที่เอเจนต์ล่ม *SGN* เป็นค่าสำหรับการตรวจสอบตัวตนของ KRA ที่อยู่ในกลุ่มการกู้คืน และ *Other Information* เก็บค่าอื่น ๆ ที่จำเป็นสำหรับการระบุตัวตนหรือค่าสำหรับการตรวจสอบเพื่อเพิ่มความมั่นคง

ขั้นตอนการเตรียมการสร้าง *KRF* สามารถแสดงได้ดังต่อไปนี้

1) แบ่งกุญแจลับออกเป็น n ชิ้น (เมื่อ n คือ จำนวนเอเจนต์ทั้งหมดที่ใช้ในการกู้คืนกุญแจ) โดยใช้แนวคิดพื้นฐานในการร่วมกันรักษาความลับ (Secret Splitting) [11] และกำหนดให้กุญแจลับสามารถกู้คืนได้จากการทำ Exclusive-OR (XOR) ส่วนประกอบของกุญแจทุกชิ้น ซึ่งกระบวนการแบ่งกุญแจลับสามารถทำได้ดังต่อไปนี้

- สุ่มตัวเลข จำนวน n-1 ตัว สำหรับ n-1 เอเจนต์ (*Agent*) เช่น S_1, S_2, ..., S_{n-1} สำหรับ $Agent_1$, $Agent_2$, ..., $Agent_{n-1}$ ตามลำดับ
- คำนวณ S_n สำหรับ $Agent_n$ ด้วย $S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1} \oplus K_S$

2) สุ่มตัวเลข (R) สำหรับทุกๆ เอเจนต์ (R_i)

3) คำนวณหาค่าความลับ สำหรับกลุ่มการกู้คืนกุญแจ (*SGN*) ด้วยการทำ XOR ค่า R_i

$$SGN = R_1 \oplus R_2 \oplus \ldots \oplus R_n$$

4) คำนวณหาค่าพิเศษ (*TT*) สำหรับทุก ๆ เอเจนต์ (TT_i) เพื่อใช้ในการกู้คืนส่วนประกอบของกุญแจ ในกรณีที่มีเอเจนต์ในกลุ่มการกู้คืนล่ม

$$TT_i = S_i \oplus SGN$$

3.1.2 ขั้นตอนการประกอบ KRF

ในขั้นตอนนี้ได้ออกแบบ KRF ให้มีความยืดหยุ่นในการกำหนดจำนวนเอเจนต์ขั้นต่ำสำหรับการกู้คืนกุญแจลับ และสามารถกู้คืนกุญแจลับได้อย่างสมบูรณ์ในกรณีที่มีเอเจนต์ในกลุ่มการกู้คืนล่ม ซึ่งได้นำหลักการพื้นฐานทางคณิตศาสตร์เรื่องพาวเวอร์เซต (Power Set) มาช่วยในกระบวนการสำรองค่า *TT* ไปไว้ใน KRF

การสำรองค่า TT_i ไปไว้ใน KRF_i สามารถดำเนินการได้ดังนี้

1) เลือกจำนวน KRA ที่จะใช้ในการกู้คืนกุญแจ (n)

2) ระบุจำนวน KRA ขั้นต่ำสำหรับการกู้คืนกุญแจ (mr) โดยที่ $mr \leq 2$

3) คำนวณหาจำนวนของ KRA ไว้สำหรับการกระจายค่า TT_i (t) ว่าจะกระจายค่า TT_i ไปให้กับ KRA กี่ตัว

$$t = n - mr \text{ เมื่อ } t \leq mr$$

4) กระจายค่า TT_i ของ KRA_i (A_i) ไปยังเอเจนต์ที่อยู่ใกล้เคียงจำนวน t เอเจนต์ เมื่อ i=1 ถึง n ตามฟังชั่นต่อไปนี้

$$A_i \rightarrow \begin{cases} A_{i+1}, A_{i+2}, \ldots, A_{i+t} & \text{where } i<mr \text{ and } i=mr \\ A_{i+1}, A_{i+2}, \ldots, A_n, A_1, A_2, \ldots, A_j & \text{where } i>mr \text{ and } j=i-mr \\ A_1, A_2, \ldots, A_t & \text{where } i=n \end{cases}$$

KRF ประกอบด้วย KRF_i's และ *Other Information* ที่นำมาเข้ารหัสลับด้วยกุญแจสาธารณะของ KRC (Ku_{KRC}) ดังนี้

$$KRF = Ku_{KRC}[KRF_i\text{'s} \,||\, Other\ Information]$$

และ KRF_i ประกอบด้วย S_i *SGN* และ TT_i's ที่นำมาเข้ารหัสลับด้วยกุญแจสาธารณะของแต่ละเอเจนต์ (Ku_{agi}) ดังนี้

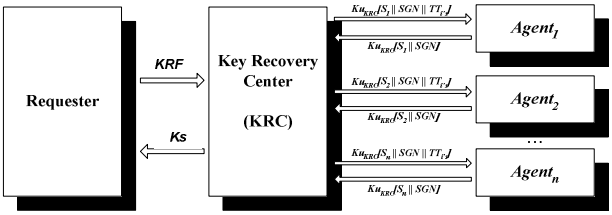
$$KRF_i = Ku_{agi}[S_i \,||\, SGN \,||\, TT_i\text{'s}]$$

3.2 กระบวนการด้านผู้รับ

ผู้รับจะได้รับ $K_S[MJ]$ และ *KRF* จากนั้นผู้รับจะทำการถอดรหัสข้อมูลด้วยกุญแจลับ หากไม่สามารถถอดรหัสข้อมูลได้ จะต้องทำการร้องขอการกู้คืนกุญแจลับ ด้วยการส่ง *KRF* ไปยัง KRC เพื่อร้องขอการกู้คืนกุญแจลับ

3.3 กระบวนการด้าน KRC และ KRA

ขั้นตอนนี้เป็นการกู้คืนกุญแจลับโดยจะเป็นการทำงานร่วมกันระหว่าง KRC กับ KRA โดยที่ KRC เป็นศูนย์กลางในการรวบรวมส่วนประกอบของกุญแจลับที่ได้รับมาจาก KRA และทำหน้าที่กู้คืนกุญแจลับ ส่วน KRA ทำหน้าที่ในการกู้คืนส่วนประกอบของกุญแจ โดยมีกระบวนการทำงานดังแสดงในรูปที่ 3



รูปที่ 3. ภาพรวมของกระบวนการกู้คืนกุญแจลับ

3.3.1 การกู้คืนกุญแจลับ

กระบวนการนี้จะเกิดขึ้นก็ต่อเมื่อ KRC ได้รับ *KRF* จากผู้ร้องขอการกู้คืนกุญแจลับ (ผู้รับหรือหน่วยงานที่รับผิดชอบในการตรวจสอบข้อมูล) เท่านั้น โดยสามารถแสดงกระบวนการได้ดังรูปที่ 4 ถึง 6 ตามลำดับ และมีขั้นตอนการทำงานดังต่อไปนี้

1) KRC ถอดรหัส *KRF* ด้วยกุญแจส่วนตัวของตนเอง (Kr_{KRC}) จะได้ส่วนประกอบของ *KRF* (KRF_i) คือ $Ku_{agi}[KRF_i]$ จำนวน n ชิ้น

2) KRC ส่ง KRF_i ให้ $Agent_i$

3) $Agent_i$ ถอดรหัสด้วยกุญแจส่วนตัวของตนเอง (Kr_{agi}) จะได้ S_i, *SGN* และ TT_i

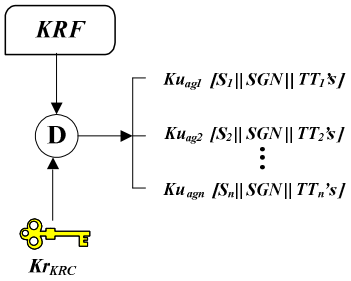
4) $Agent_i$ เข้ารหัส S_i และ *SGN* ด้วย Ku_{KRC} จะได้ $Ku_{KRC}[S_i \,||\, SGN]$

5) $Agent_i$ ส่ง $Ku_{KRC}[S_i \,||\, SGN]$ ให้ KRC

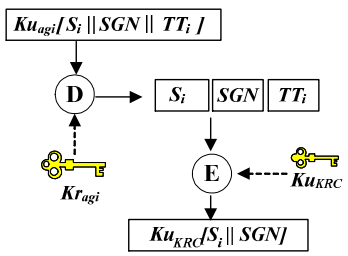
6) KRC ถอดรหัสด้วย Kr_{KRC} จะได้ S_i และ *SGN*

7) KRC ตรวจสอบ *SGN* ว่าเป็นเอเจนต์ในกลุ่มการกู้คืนจริง

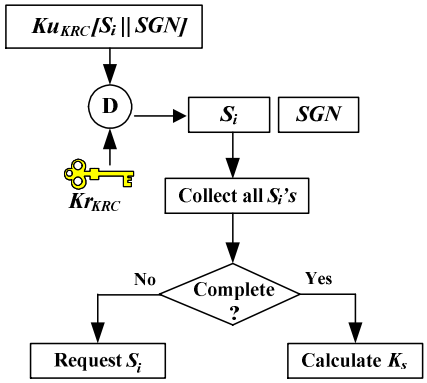
8) KRC คำนวณหา K_S ด้วย $S_1 \oplus S_2 \oplus .... \oplus S_n$ และ เข้ารหัส K_S ด้วย กุญแจสาธารณะของผู้ร้องขอ (Ku_{req}) ส่งให้กับผู้ร้องขอต่อไป



รูปที่ 4. การถอดรหัส *KRF* โดย KRC



รูปที่ 5. การกู้คืนส่วนประกอบของกุญแจลับโดย KRA



รูปที่ 6. การกู้คืนกุญแจลับโดย KRC

3.3.2 การกู้คืนส่วนประกอบของกุญแจลับ ในกรณีที่มีเอเจนต์ในกลุ่มการกู้คืนล่ม

ในกรณีที่มีเอเจนต์ในกลุ่มการกู้คืนล่ม ส่งผลให้ KRC รวบรวม S_i ได้ไม่ครบ ดังนั้นจะเป็นหน้าที่ของ KRC ที่จะต้องทำการร้องขอการกู้คืนส่วนประกอบกุญแจที่หายไปหรือที่ยังไม่ได้รับ โดยทำการร้องขอกับเอเจนต์ที่สามารถให้บริการได้ในกลุ่มการกู้คืนเดียวกัน ซึ่งจะต้องเป็นเอเจนต์ที่อยู่ในตำแหน่งใกล้เคียง (ถัดไป) กับเอเจนต์ที่ล่ม โดยมีขั้นตอนการร้องขอดังต่อไปนี้

1) KRC ตรวจสอบ S_i ว่ายังไม่ได้รับมาจากเอเจนต์ ($Agent_i$) ใด

2) KRC เข้ารหัสคำร้องขอการกู้คืน ($req\text{-}S_i$) และ *SGN* ด้วยกุญแจสาธารณะของเอเจนต์ถัดไป ($Agent_{nxt}$) ที่จะให้ทำการกู้คืนส่วนประกอบของกุญแจ (Ku_{nxt} of $Agent_{nxt}$) จะได้ $Ku_{nxt}[req\text{-}S_i \,||\, SGN \,||\, Other\ Information]$

3) $Agent_{nxt}$ ถอดรหัส $Ku_{nxt}[req\text{-}S_i \,||\, SGN]$ ด้วยกุญแจส่วนตัวของตัวเอง (Kr_{nxt})

4) $Agent_{nxt}$ ตรวจสอบ *SGN* และคำนวณ S_i ด้วย $S_i = TT_i \oplus SGN$

5) $Agent_{nxt}$ เข้ารหัส S_i และ *SGN* ด้วย Ku_{KRC} จะได้ $Ku_{KRC}[S_i \,||\, SGN]$

6) $Agent_{nxt}$ ส่ง $Ku_{KRC}[S_i \,||\, SGN]$ ให้ KRC เพื่อทำการรวบรวม S_i และกู้คืน K_S

4. การเปรียบเทียบความสามารถของระบบการกู้คืนกุญแจ

งานวิจัยได้ทำการเปรียบเทียบความสามารถของระบบการกู้คืนกุญแจแบบหลายเอเจนต์ทั้งหมด 3 ระบบดังนี้ (1) ระบบที่มีผู้วิจัยไว้ตั้งเดิมคือ Multiple-Agent Model [6] (2) ระบบที่ผู้วิจัยได้ทำไว้ก่อนหน้าคือ SHAM-KRS [7] และ (3) ระบบที่ผู้วิจัยได้นำเสนอคือ SFM-KRS โดยมีรายละเอียดดังแสดงในตารางที่ 1

ตารางที่ 1. การเปรียบเทียบความสามารถของระบบ

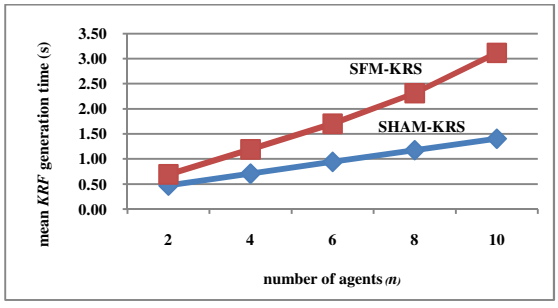
ความสามารถของระบบ	Multiple Agent Model	SHAM-KRS	SFM-KRS (ระบบที่นำเสนอ)
ใช้หลักการ Secret Splitting	-	✓	✓
กู้คืนกุญแจลับได้ แม้ในกรณีเกิดเหตุการณ์มีเอเจนต์ล่ม	-	✓	✓
ความยืดหยุ่นในการบริหารจัดการจำนวนเอเจนต์ขั้นต่ำ	-	-	✓
สามารถตรวจสอบเอเจนต์แปลกปลอม	-	✓	✓
รูปแบบมาตรฐานของ KRF	✓	✓	✓

จากตารางที่ 1 จะสังเกตเห็นได้ว่า SFM-KRS เป็นระบบที่มีความสามารถมากที่สุด โดยมีคุณสมบัติเด่นคือ ความสามารถในการบริหารจัดการจำนวนเอเจนต์ กล่าวคือ ผู้บริหารหรือผู้ดูแลระบบสามารถกำหนดจำนวนเอเจนต์ขั้นต่ำที่ใช้สำหรับการกู้คืนกุญแจ เพื่อให้เข้ากับสภาพแวดล้อมการใช้งานได้ ส่งผลให้ระบบมีความยืดหยุ่นและมั่นคงเพิ่มขึ้น

5. การประเมินสมรรถนะของ SFM-KRS

การประเมินสมรรถนะได้พิจารณาเปรียบเทียบค่าเฉลี่ยเวลา (หน่วยเป็นวินาที) ในการสร้าง KRF และเวลาในการกู้คืนกุญแจระหว่าง SFM-KRS กับ SHAM-KRS [7] รวมทั้งได้ทำการทดลองเพื่อหาเวลาที่ใช้ในการกู้คืนส่วนประกอบของกุญแจลับในกรณีที่มีเอเจนต์ล่ม โดยทดลองบนเครื่องคอมพิวเตอร์ที่มีหน่วยประมวลผลกลาง Genuine Intel® CPU, 794 MHz หน่วยความจำขนาด 1 GB

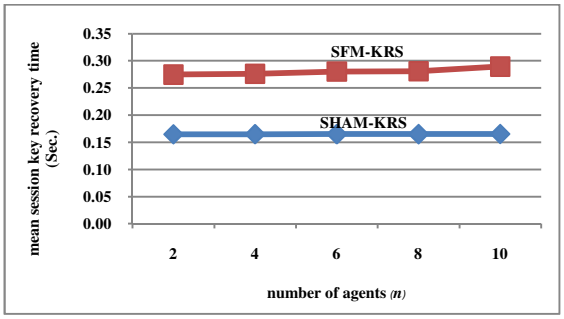
5.1 เวลาเฉลี่ยของการสร้าง KRF



รูปที่ 7. เวลาเฉลี่ยของการสร้าง KRF

จากรูปที่ 7 จะเห็นว่า SFM-KRS ใช้เวลาเฉลี่ยในการสร้าง KRF สูงกว่า SHAM-KRS เพียงเล็กน้อยอย่างไม่มีนัยสำคัญ เหตุที่มีค่าเฉลี่ยเวลามากกว่านั้น เนื่องจาก SFM-KRS จะต้องใช้เวลาสำหรับกระบวนการสำรองค่า *TT* เพื่อใช้ในการกู้คืนกุญแจในกรณีที่มีเอเจนต์ล่ม และใช้สำหรับการบริหารจัดการเอเจนต์ขั้นต่ำในการกู้คืนกุญแจ ส่งผลให้ระบบมีความพร้อมใช้งานและมีความยืดหยุ่นมากขึ้น และจะใช้เวลาเพิ่มขึ้นเล็กน้อยตามลำดับ เมื่อใช้จำนวนเอเจนต์เพิ่มขึ้น

5.2 เวลาที่ใช้ในการกู้คืนกุญแจลับ

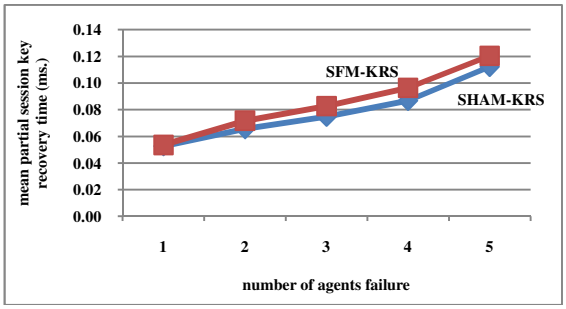


รูปที่ 8. เวลาเฉลี่ยของการกู้คืนกุญแจลับ

จากรูปที่ 8 แสดงให้เห็นว่า SFM-KRS ใช้เวลาเฉลี่ยในการกู้คืนกุญแจลับมากกว่า SHAM-KRS เล็กน้อย เนื่องจาก SFM-KRS มีโครงสร้างของ KRF ที่เพิ่มการสำรองค่า *TT* ที่ใช้สำหรับการบริหารจัดการเอเจนต์ เพิ่มความมั่นคงให้กับระบบ จึงส่งผลให้ SFM-KRS มีความยืดหยุ่นมากกว่า SHAM-KRS แต่ใช้เวลาในการกู้คืนกุญแจลับเพิ่มขึ้นเพียงเล็กน้อยอย่างไม่มีนัยสำคัญ และกราฟค่อนข้างคงที่ เมื่อใช้จำนวนเอเจนต์เพิ่มขึ้น เนื่องจากกระบวนการในการกู้คืนกุญแจลับได้ถูกออกแบบมาอย่างเหมาะสมและไม่ซับซ้อน

5.3 เวลาที่ใช้ในการกู้คืนส่วนประกอบของกุญแจในกรณีที่มีเอเจนต์ล่ม

การทดลองนี้ได้ทำการทดลองโดยใช้เอเจนต์ในการกู้คืนกุญแจลับ จำนวน 7 เอเจนต์ และสมมติให้มีเอเจนต์ล่มตั้งแต่ 1 ถึง 5 เอเจนต์ (หน่วยเป็นมิลลิวินาที (millisecond: ms))



รูปที่ 9. เวลาเฉลี่ยของการกู้คืนส่วนประกอบของกุญแจลับ

จากรูปที่ 9 แสดงให้เห็นว่า SFM-KRS และ SHAM-KRS ใช้เวลาเฉลี่ยในการกู้คืนส่วนประกอบของกุญแจลับเพียงเล็กน้อยในเวลาที่ใกล้เคียงกัน และเมื่อมีจำนวนเอเจนต์ที่ล่มเพิ่มขึ้น จะส่งผลให้ต้องใช้เวลาในการกู้คืนส่วนประกอบของกุญแจลับเพิ่มขึ้นตามลำดับ

6. บทสรุป

งานวิจัยนี้ได้นำเสนอระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่มีความมั่นคงและยืดหยุ่นสูง คือ SFM-KRS ซึ่งเป็นระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่มีกระบวนการทำงานอย่างมีประสิทธิภาพ ใช้เวลาเฉลี่ยในการทำงานน้อย โดยได้ออกแบบให้อยู่บนพื้นฐานของเรื่องการรักษาความลับ (Confidentiality) การรักษาความสมบูรณ์ (Integrity) และมีความพร้อมใช้งานสูง (Availability) ระบบสามารถรองรับปัญหาการล่มของเอเจนต์อย่างได้ผล และสามารถบริหารจัดการจำนวนเอเจนต์ขั้นต่ำที่ใช้สำหรับการกู้คืนกุญแจลับได้ จึงส่งผลให้ระบบมีความมั่นคงและยืดหยุ่นสูง รวมทั้งมีฟิลด์สำหรับการกู้คืนกุญแจที่เป็นมาตรฐาน และสามารถรองรับการตรวจสอบข้อมูลโดยชอบด้วยกฎหมายอีกด้วย

เอกสารอ้างอิง

[1] D.E. Denning, “The US Key Escrow Encryption Technology”, *Computer Communications,* Vol. 17, No. 7, pp. 453-457, July 1994.

[2] S.T. Walker, S.B. Lipner, C.M. Ellison and D.M. Balenson, “Commercial Key Recovery”, *Communications of the ACM*, Vo1. 39, No. 3, pp. 41-47, March 1996.

[3] Yung-Cheng Lee and Chi-Sung Laih, **“**On the Key Recovery of the Key Escrow System**”,** *Proceedings of the 13th Annual Computer Security Applications Conference*, pp. 216-220, December 1997.

[4] D.E. Denning and D.K. Branstad, **“**A Taxonomy for Key Recovery Encryption Systems**”,** *Internet Besieged: Countering Cyberspace Scofflaws,* pp. 357-371, 1997.

[5] S. Lim, S. Kang, and J. Sohn, “Modeling of Multiple Agent Based Cryptographic Key Recovery Protocol”, *Proceedings of the 19th Annual Computer Security Applications Conference*, pp. 119-128. Las Vegas, December 2003.

[6] Shin-Young Lim, Ho-Sang Hani, Myoung-Jun Kim and Tai-Yun Kim, “Design of Key Recovery System Using Multiple Agent Technology for Electronic Commerce”, *Proceedings of 2001 IEEE Industrial Electronics,* Vol. 2, pp. 1351-1356, 2001.

[7] K. Kanyamee and C. Sathitwiriyawong, “A Simple High-Availability Multiple-Agent Key Recovery System”, *Proceedings of the 4th International Conference for Internet Technology and Secured Transactions*, pp. 734-739, 2010.

[8] R. Perlman, “An Overview of PKI Trust Models”, *IEEE Network*, Vol. 13, Issue 6, pp. 38-43, November 1999.

[9] Paolo D'Arco, “On the Distribution of a Key Distribution Center”**,** *Proceedings of the 7th Italian Conference on Theoretical Computer Science*, Vol. 2202, pp. 357-369**,** 2001.

[10] Neuman, B.C. and Ts'o, T. “Kerberos: an Authentication Service for Computer Networks”, *Communications Magazine of the IEEE*, Vol. 32, pp. 32-38, September 1994.

[11] Bruce Schneier, *Applied Cryptography*, New York, NY, John Wiley & Sons, 1996.