รายงานผลการวิจัยฉบับสมบูรณ์

การแชร์ความลับอย่างง่ายและมีประสิทธิภาพสำหรับระบบการกู้คืนกุญแจแบบหลายเอเจนต์

กนกวรรณ กันยะมี

งานวิจัยนี้ได้รับทุนอุดหนุนการวิจัยจากงบประมาณแผ่นดิน
มหาวิทยาลัยราชภัฏอุตรดิตถ์ ปีงบประมาณ 2561
พ.ศ. 2561

หัวข้อวิจัย การแชร์ความลับอย่างง่ายและมีประสิทธิภาพสำหรับระบบการกู้คืนกุญแจแบบหลายเอเจนต์
ผู้ดำเนินวิจัย กนกวรรณ กันยะมี
หน่วยงาน คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏอุตรดิตถ์
ปีการศึกษา 2561

บทคัดย่อ

ในยุคปัจจุบันประเด็นทางด้านความปลอดภัยของข้อมูลสารสนเทศ และความเป็นส่วนตัวของบุคคลผู้ที่เกี่ยวข้องกับสารสนเทศบนเครือข่ายถือว่าเป็นเรื่องที่มีความสำคัญ วิทยาการเข้ารหัสลับเป็นเทคโนโลยีที่จะช่วยเพิ่มความมั่นคงปลอดภัยให้กับข้อมูล และเพิ่มความเป็นส่วนตัวแก่ผู้ที่ใช้งานระบบเครือข่าย ซึ่งเทคโนโลยีนี้จะใช้กุญแจลับในการเข้ารหัสและถอดรหัสข้อมูล หากเกิดกรณีที่ผู้รับไม่สามารถใช้กุญแจในการถอดรหัสข้อมูลได้ หรือกุญแจที่ใช้ในการถอดรหัสสูญหาย จะต้องอาศัยกระบวนการเพื่อให้ได้มาซึ่งกุญแจลับ หรือเรียกว่า วิธีการกู้คืนกุญแจลับจากฟิลด์ในการกู้คืนกุญแจเพื่อนำมาใช้ในการถอดรหัสข้อมูล

งานวิจัยนี้มีวัตถุประสงค์เพื่อ พัฒนารูปแบบขั้นตอนวิธีการสำหรับการแชร์ความลับของกุญแจลับในฟิลด์กู้คืนกุญแจ เพื่อรองรับการกู้คืนกุญแจ โดยการออกแบบจะคำนึงถึงเรื่องความปลอดภัยของข้อมูล และความเป็นส่วนตัวของผู้ใช้ระบบเครือข่ายและสารสนเทศ รองรับการเข้าถึงข้อมูลอย่างถูกต้อง ทำให้ระบบมีความพร้อมใช้งานและมีความน่าเชื่อถือสูง ระบบสามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกันได้

คำสำคัญ – กู้คืนกุญแจ; การแชร์ความลับ; เอเจนต์; หลายเอเจนต์

กิตติกรรมประกาศ

การวิจัยหัวข้อ “การแชร์ความลับอย่างง่ายและมีประสิทธิภาพสำหรับระบบการกู้คืนกุญแจแบบหลายเอเจนต์” นี้ ได้รับทุนอุดหนุนการวิจัยจากงบประมาณแผ่นดิน มหาวิทยาลัยราชภัฏอุตรดิตถ์ คณะผู้วิจัยใคร่ขอกราบขอบพระคุณผู้บริหาร คณาจารย์ เจ้าหน้าที่ทุกท่านของมหาวิทยาลัย ฯ เป็นอย่างสูง ที่ให้การสนับสนุนการวิจัย และให้ข้อเสนอแนะอันเป็นประโยชน์ในการดำเนินการวิจัย

ขอกราบขอบคุณสาขาเทคโนโลยีสารสนเทศ และสาขาวิทยาการคอมพิวเตอร์ ที่เอื้อเฟื้อสถานที่ และเวลาในการทำวิจัย

ขอบกราบขอบพระคุณครอบครัวที่เป็นกำลังใจที่ดีและอบอุ่น ส่งผลให้การทำวิจัยในครั้งนี้สำเร็จลุล่วงไปได้ด้วยดี

กนกวรรณ กันยะมี

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

เทคโนโลยีการเข้ารหัสลับจะช่วยเพิ่มความมั่นคงปลอดภัยให้กับข้อมูลสารสนเทศ และเพิ่มความเป็นส่วนตัวแก่ผู้ที่ใช้งานระบบเครือข่าย การเข้ารหัสลับแบบสมมาตรจะใช้กุญแจลับในการเข้ารหัสและถอดรหัสข้อมูล ในกรณีที่ผู้รับไม่สามารถใช้กุญแจในการถอดรหัสข้อมูลได้ หรือกุญแจที่ใช้ในการถอดรหัสสูญหาย หรือภาครัฐต้องการใช้สิทธิ์ในการเข้าถึงข้อมูลที่ต้องสงสัย จะต้องขอใช้บริการกู้คืนกุญแจจากหน่วยงานที่ทำหน้าที่ให้บริการกู้คืนกุญแจ ซึ่งเรียกว่า เอเจนต์กู้คืนกุญแจ (Key Recovery Agent : KRA)

การกู้คืนกุญแจ มีการทำงานสองรูปแบบ คือ การกู้คืนกุญแจแบบใช้เอเจนต์เดี่ยว (Single Key Recovery System: S-KRS) และการกู้คืนกุญแจแบบใช้หลายเอเจนต์ (Multiple Key Recovery System: M-KRS) โดยกระบวนการทำงานของ S-KRS จะใช้เอเจนต์เดียว (Single Key Recovery Agent: S-KRA) ในการกู้คืนกุญแจ ส่วน M-KRS จะใช้หลายเอเจนต์ (Multiple Key Recovery Agent: M-KRA) ร่วมกันกู้คืนกุญแจ

การพัฒนาระบบในช่วงเริ่มแรกจะเป็นรูปแบบ S-KRS ซึ่งมีกระบวนการทำงานที่ไม่ซับซ้อน จึงทำให้เกิดภัยคุกคามต่อระบบได้ง่าย ระบบมีความมั่นคงปลอดภัยน้อยเมื่อเทียบกับภัยคุกคามที่มีหลากหลายรูปแบบ และมีความรุนแรงมากขึ้น เช่น การปฏิเสธการให้บริการ (Denial of Service) เป็นต้น ต่อมาการพัฒนาระบบในช่วงหลัง จึงได้ออกแบบระบบโดยใช้รูปแบบ M-KRS ทั้งนี้เพื่อลดความเสี่ยงต่อความเสียหายที่เกิดขึ้นกับ S-KRS

อย่างไรก็ตามการกู้คืนกุญแจในรูปแบบ M-KRS ที่คำนึงถึงความเป็นส่วนของผู้ใช้งาน และรองรับการเข้าถึงข้อมูลอย่างถูกต้อง จะต้องอาศัยกระบวนการแชร์กุญแจไปยังเอเจนต์ที่เกี่ยวข้อง ซึ่งจากการศึกษางานวิจัยที่ผ่านมายังไม่มีการนำเสนอองค์ความรู้เกี่ยวกับวิธีขั้นตอนของกระบวนการในการแชร์กุญแจลับ ที่คำนึงถึงเรื่องดังกล่าว

ผู้วิจัยจึงจะได้ศึกษาและนำเสนออัลกอริทึมของการแชร์กุญแจลับ สำหรับ M-KRS เพื่อให้กุญแจมีความมั่นคง เป็นความลับ ผู้ใช้งานมีความเป็นส่วนตัว และรองรับการเข้าถึงข้อมูลอย่างถูกต้อง ทำให้ระบบมีความพร้อมใช้งานและมีความน่าเชื่อถือสูง ระบบสามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกัน ทั้งนี้ระบบทำงานบนโครงสร้างพื้นฐานกุญแจสาธารณะหรือพีเคไอ (Public Key Infrastructure: PKI)

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษากระบวนการสร้างฟิลด์ในการกู้คืนกุญแจ และการทำงานของระบบการกู้คืนกุญแจแบบหลายเอเจนต์

1.2.2 เพื่อพัฒนารูปแบบขั้นตอนวิธีการสำหรับการแชร์ความลับอย่างง่าย ในระบบการกู้คืนกุญแจแบบหลายเอเจนต์

1.3 ขอบเขตการวิจัย

นำเสนอรูปแบบขั้นตอนวิธีการแชร์ความลับในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ ประกอบด้วย วิธีการจัดเก็บส่วนประกอบของกุญแจ โดยการแบ่งและจัดสรรส่วนประกอบของกุญแจเป็นส่วนๆ การกระจายเพื่อแชร์ส่วนประกอบของกุญแจไปอยู่ในฟิลด์ในการกู้คืนกุญแจ หรือการแชร์ความลับแบบหลายเอเจนต์ โดยพัฒนาเพื่อให้ระบบมีความสามารถในด้านต่อไปนี้

กุญแจมีความมั่นคง เป็นความลับ ผู้ใช้งานมีความเป็นส่วนตัว และรองรับการเข้าถึงข้อมูลอย่างถูกต้อง ทำให้ระบบมีความพร้อมใช้งานและมีความน่าเชื่อถือสูง ระบบสามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกัน

(1) การรักษาความลับ (Secrecy) ของข้อมูลและกุญแจลับ คือการกู้คืนกุญแจเพื่อการถอดรหัสลับข้อมูล ต้องใช้ความร่วมมือของเอเจนต์มากกว่าหนึ่งเอเจนต์ ลดความเสี่ยงเรื่องการผูกขาดความลับของกุญแจลับ กุญแจมีความมั่นคง

(2) มีความปลอดภัย (Security) ของข้อมูลและกุญแจลับ คือกระบวนการกู้คืนกุญแจลับจะต้องมีกระบวนการพิสูจน์ตัวตน

(3) มีความยืดหยุ่นและความพร้อมใช้งาน (Flexibility and Availability) ของการกู้คืนกุญแจ คือสามารถกู้คืนกุญแจได้ในกรณีที่มีบางเอเจนต์ไม่สามารถให้บริการได้

(4) มีความเป็นส่วนตัว (Privacy) ของผู้ใช้งาน คือใช้กระบวนการจัดเก็บส่วนประกอบของกุญแจแทนการจัดเก็บกุญแจโดยตรง และมีกระบวนการพิสูจน์ตัวจริงของผู้ใช้งาน

(5) รองรับการเข้าถึงข้อมูลอย่างถูกต้อง การจัดเก็บส่วนประกอบของกุญแจสำหรับการกู้คืนกุญแจลับ จะอาศัยแนวคิดพื้นฐานเรื่องการแชร์ความลับ (Secret Sharing) มาใช้ในการแบ่งกุญแจออกเป็นส่วนๆ และจัดสรรส่วนประกอบของกุญแจ ใช้ทฤษฎีพื้นฐานเรื่องเพาเวอร์เซต (Power Set) มาใช้ในกระบวนการสำรองส่วนประกอบของกุญแจสำหรับการกู้คืนกุญแจในกรณีที่มีบางเอเจนต์ไม่สามารถให้บริการได้

1.4 ประโยชน์ที่คาดว่าจะได้รับ

ได้รูปแบบขั้นตอนวิธีการสำหรับการแชร์ความลับอย่างง่าย ในระบบการกู้คืนกุญแจแบบหลายเอเจนต์

1.5 คำนิยามศัพท์เฉพาะ

1.5.1 การกู้คืนกุญแจ (Key Recovery) คือ การกู้คืนกุญแจเซสชั่น ในกรณีที่กุญแจเซสชั่นทางฝั่งผู้รับสูญหาย หรือ เสียหาย หรืออีกนัยหนึ่งคือ การกู้คืนกุญแจเซสชั่นเพื่อการเข้าถึงข้อมูลของคู่สื่อสารโดยชอบด้วยกฎหมาย

1.5.2 เอเจตน์ในการกู้คืนกุญแจ (Key Recovery Agent : KRA) หน่วยงานที่ทำหน้าที่ในการให้บริการกู้คืนส่วนประกอบของกุญแจเซสชั่น เมื่อได้รับการร้องขอการกู้คืนกุญแจจากผู้ใช้บริการ

1.5.3 ฟิลด์ในการกู้คืนกุญแจ (Key Recovery Filed : KRF) ฟิลด์ที่บรรจุข้อมูลที่เกี่ยวข้องกับกุญแจเซสชั่น ใช้สำหรับการกู้คืนกุญแจเซสชั่น

1.5.4 กุญแจลับ (Secret Key : Ks) คือ กุญแจที่ใช้ในการเข้ารหัสข้อมูล เพื่อให้ข้อมูลมีความปลอดภัย

1.5.5 การแชร์ความลับ (Secret Sharing) คือ การแบ่งส่วนประกอบของความลับออกเป็นส่วน ๆ แล้วกระจายหรือแชร์ส่วนประกอบของความลับนั้น

บทที่ 2
ทฤษฎีพื้นฐานและงานวิจัยที่เกี่ยวข้อง

ในบทนี้เป็นการอธิบายเกี่ยวกับทฤษฎีพื้นฐาน และงานวิจัยที่เกี่ยวข้องกับการวิจัยเรื่อง การแชร์ความลับอย่างง่ายและมีประสิทธิภาพ โดยแบ่งออกเป็นหัวข้อต่างๆ ดังนี้

1) ระบบการเข้ารหัสลับการกู้คืนกุญแจ
2) องค์ประกอบของระบบการเข้ารหัสลับการกู้คืนกุญแจ
3) หน่วยงานกู้คืนกุญแจ (KRA)
4) รูปแบบความไว้วางใจ (Trust Model) ของผู้ให้บริการออกใบรับรอง (Certificate Authority : CA)
5) รูปแบบของ Trusted Third Party (TTP) ที่เกี่ยวข้องกับระบบการกู้คืนกุญแจ
6) วิธีการ/กระบวนการพื้นฐานสำหรับการกู้คืนกุญแจ
7) การแชร์ความลับ (Secret Sharing)
8) เพาเวอร์เซต (Power Set)
9) การห่อหุ้มกุญแจ (Key Encapsulation)
10) งานวิจัยที่เกี่ยวข้อง

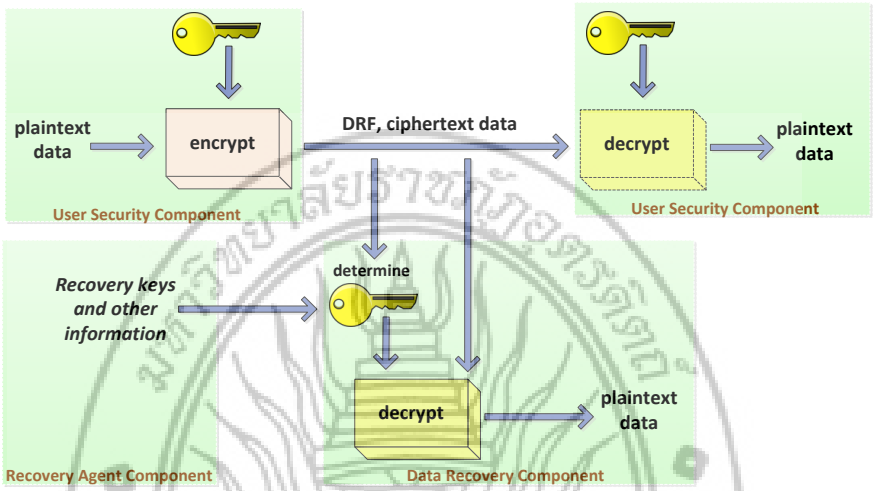
2.1 ระบบการเข้ารหัสลับการกู้คืนกุญแจ

ระบบการเข้ารหัสลับการกู้คืนกุญแจ (A Key Recovery Encryption System) [1, 2] คือ ระบบที่ให้บริการกู้คืนกุญแจลับ ในกรณีที่กุญแจลับทางฝั่งผู้รับสูญหายหรือเสียหาย หรือเป็นการกู้คืนกุญแจลับเพื่อการเข้าถึงข้อมูลที่ต้องสงสัยโดยชอบด้วยกฎหมาย

ระบบการเข้ารหัสลับการกู้คืนกุญแจ เป็นระบบการเข้ารหัสลับที่อาศัยความสามารถของการสำรอง (Backup) ข้อมูลบางส่วนของกุญแจ เพื่อนำมาใช้ในการถอดรหัสลับ โดยอาศัยความไว้วางใจ (Trust) ยอมให้สิทธิ์ในการเข้าถึงข้อมูลดังกล่าวกับบุคคลที่สาม (Trusted Third Party: TTP) เช่น หน่วยงานของรัฐบาลหรือองค์กรที่จัดตั้งขึ้นโดยถูกต้องตามกฎหมาย เป็นต้น ซึ่งการกู้คืนกุญแจจะต้องอยู่ภายใต้นโยบายหรือกฎหมายที่แน่นอน บุคคลที่สามารถร้องขอการกู้คืนกุญแจและมีสิทธิ์ในกุญแจนั้น คือผู้ที่เป็นเจ้าของกุญแจที่ต้องการกู้คืนหรือหน่วยงาน/บุคคลากรของรัฐบาลที่มีสิทธิ์ในการตรวจสอบข้อมูลที่ส่งผ่านระบบเครือข่ายซึ่งต้องการเข้าถึงข้อมูลกุญแจ และนำกุญแจไปถอดรหัสลับข้อมูลเพื่อตรวจสอบอีกครั้งหนึ่ง

2.2 องค์ประกอบของระบบการเข้ารหัสลับการกู้คืนกุญแจ

องค์ประกอบของระบบการเข้ารหัสลับการกู้คืนกุญแจ แบ่งออกเป็น 3 ส่วนหลัก ๆ ซึ่งจะมีการทำงานที่สัมพันธ์กัน ดังแสดงตามรูปที่ 2.1



รูปที่ 2.1 องค์ประกอบของระบบการเข้ารหัสลับการกู้คืนกุญแจ

(1) ส่วนความมั่นคงของผู้ใช้งาน (User Security Component: USCn) ทำหน้าที่ในการจัดการเรื่องความสามารถในการเข้ารหัสลับและถอดรหัสลับข้อมูล รวมทั้งสนับสนุนการกู้คืนกุญแจรูปแบบการกู้คืนกุญแจซึ่งจะมีการแนบฟิลด์ที่ใช้ในการกู้คืนกุญแจ (Data Recovery Field: DRF หรือ Key Recovery Field: KRF) ไปกับข้อมูลที่ผ่านการเข้ารหัสลับแล้ว (Ciphertext)

(2) ส่วนหน่วยงานกู้คืนกุญแจ (Recovery Agent Component: RACn) อาจประกอบด้วยศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center : KRC) และ/หรือ หน่วยงานกู้คืนกุญแจ (KRA) ซึ่งทำหน้าที่ในการบริหารจัดเก็บกุญแจ กู้คืนกุญแจ ใช้กุญแจในการกู้คืนข้อมูล รวมทั้งจัดเก็บข้อมูลอื่น ๆ ที่ช่วยให้การถอดรหัสลับทำได้โดยสะดวก ในกรณีเกิดปัญหากุญแจที่ใช้ในการถอดรหัสลับไม่สามารถใช้งานได้หรือสูญหาย และในส่วนของหน่วยงานนี้อาจมีการใช้ระบบการบริหารจัดการใบรับรองกุญแจสาธารณะ (Public Key Certificate) หรือใช้โครงสร้างพื้นฐานการบริหารจัดการกุญแจทั่วไป (General Key Management Infrastructure) ร่วมด้วย

(3) ส่วนการกู้คืนข้อมูล (Data Recovery Component: DRCn) ประกอบไปด้วยอัลกอริทึมโพรโทคอล และกระบวนการขั้นตอนที่ทำให้ได้มาซึ่งกุญแจลับ โดยเอาจาก DRF หรือ KRF ที่แนบไปกับข้อมูลที่ผ่านการเข้ารหัสลับแล้ว เพื่อนำกุญแจที่ได้ไปถอดรหัสลับข้อมูลอีกครั้งหนึ่ง ในส่วนการกู้คืนข้อมูลหรือการกู้คืนกุญแจนี้ จะอนุญาตเฉพาะผู้ที่มีสิทธิ์ในการกู้คืนกุญแจเท่านั้น

2.3 หน่วยงานกู้คืนกุญแจ (Ker Recovery Agent : KRA)

KRA จัดเป็น TTP ที่มีหน้าที่ในการบริหารจัดเก็บกุญแจ ทดแทนกุญแจ กู้คืนกุญแจ และใช้กุญแจในการถอดรหัสลับเพื่อกู้คืนข้อมูล รวมทั้งจัดเก็บข้อมูลอื่น ๆ ที่ช่วยให้การถอดรหัสลับทำได้โดยสะดวก ในกรณีเกิดปัญหากุญแจที่ใช้ในการถอดรหัสลับไม่สามารถใช้งานได้หรือสูญหาย หรือในกรณีที่หน่วยงานของรัฐต้องการตรวจสอบข้อมูลต้องสงสัย ซึ่งถือว่าเป็นหน่วยงานที่มีบทบาทและมีหน้าที่ที่สำคัญ

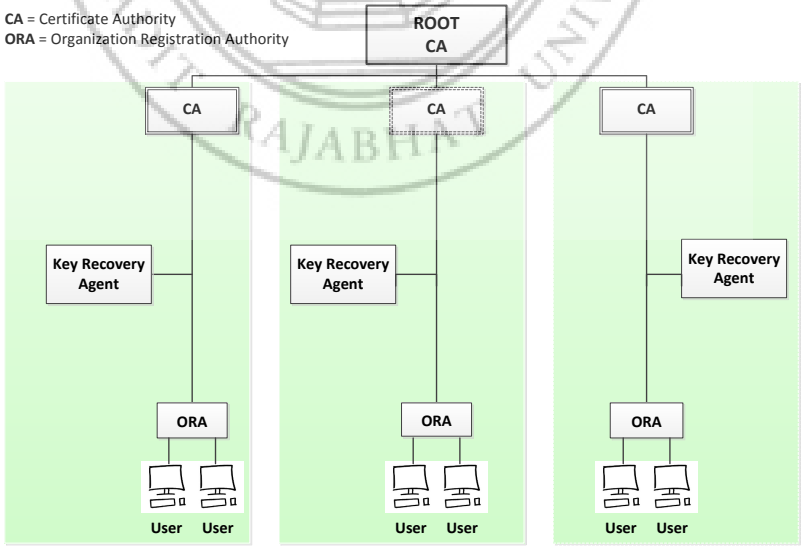
KRA จำเป็นที่จะต้องได้รับการรับรองและยืนยันความน่าเชื่อถือของหน่วยงานจาก TTP เพื่อเป็นการสร้างความไว้ใจ/เชื่อมั่นในเรื่องความมั่นคงและความเป็นส่วนตัวให้กับผู้ที่ใช้บริการ

2.3.1 ตัวอย่างของ KRA

KRA ที่มีการขอใบรับรองหน่วยงานจากหน่วยงานที่ให้บริการออกใบรับรองคือ องค์กรออกใบรับรอง (CA) และองค์กรผู้ได้รับอนุญาตในการออกใบรับรอง KRA มีดังนี้

(1) หน่วยงานกู้คืนกุญแจที่ได้รับการรับรองจาก CA

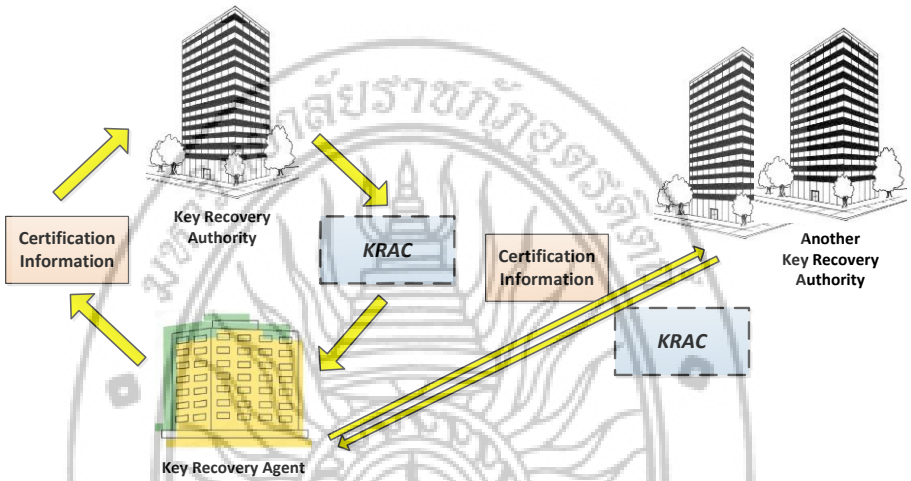
KRA จะทำการส่งข้อมูลส่วนตัวและข้อมูลกุญแจสาธารณะให้กับ CA เพื่อให้ CA ทำการรับรองข้อมูลส่วนตัวของหน่วยงาน และรับรองข้อมูลกุญแจด้วยการออกใบรับรองและประกาศการรับรองนั้นบนเครือข่าย โดย CA จะทำงานประสานกับหน่วยงานรับลงทะเบียน (Organization Registration Authorities: ORA) ซึ่งจะมีหน้าที่ตรวจสอบ/พิสูจน์ผู้ใช้งาน ตรวจสอบการร้องขอ และติดต่อกับ CA จากนั้น ORA จะร้องขอการกู้คืนกุญแจจาก KRA เพื่อให้ได้มาซึ่งกุญแจที่สามารถนำไปถอดรหัสลับข้อมูลต้นฉบับได้ ดังแสดงความสัมพันธ์ของการทำงานตามรูปที่ 2.2



รูปที่ 2.2 การให้การรับรองหน่วยงานที่ให้บริการกู้คืนกุญแจโดย CA

(2) KRA ที่ได้รับการรับรองจาก Key Recovery Authority หรือ KRAu

KRA สามารถขอใบรับรองหน่วยงานได้จาก KRAu ดังแสดงตามรูปที่ 2.3 โดยส่งข้อมูลคำร้องและข้อมูลการขอใบรับรองไปยังหน่วยงานดังกล่าว จากนั้นก็จะได้รับใบรับรองหน่วยงานกู้คืนกุญแจ (Key Recovery Agent Certificate: KRAC) ที่มีการลงลายมือชื่อจาก KRAu เรียบร้อยแล้ว ทั้งนี้ KRA สามารถส่งคำร้องและข้อมูลการขอใบรับรองไปให้หลาย ๆ KRAu รับรองได้ด้วย



รูปที่ 2.3 กระบวนการขอใบรับรองจาก KRAu

2.3.2 การให้บริการของ KRA

สามารถแบ่งตามรูปแบบการจัดการกุญแจได้ 4 รูปแบบ ดังแสดงตามรูปที่ 2.4

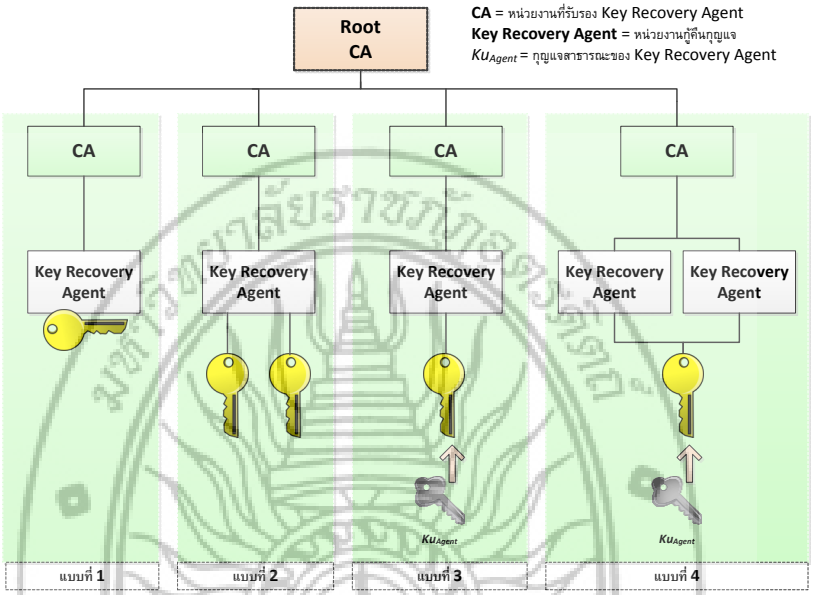
รูปแบบที่ 1 กุญแจต้นฉบับถูกจัดเก็บที่ KRA หรือหน่วยงานที่ทำหน้าที่ในการกู้คืนกุญแจ โดยหน่วยงานที่รับผิดชอบกุญแจจะสามารถเข้าถึงข้อมูลกุญแจได้โดยตรง

รูปแบบที่ 2 กุญแจถูกแยกส่วน และมีการจัดเก็บแยกกันตามตำแหน่งของการจัดเก็บ เมื่อต้องการกู้คืนกุญแจ KRA จะทำหน้าที่ในการนำส่วนที่แยกกันอยู่มารวมกันเป็นข้อมูลกุญแจ

รูปแบบที่ 3 KRA ไม่จัดเก็บกุญแจของผู้ใช้งาน แต่จะให้ผู้ใช้งานนำกุญแจสาธารณะของหน่วยงานไปเข้ารหัสลับข้อมูลกุญแจ ซึ่งจัดเก็บเป็นฟิลด์ที่ใช้ในการกู้คืนกุญแจ และเมื่อต้องการกู้คืนกุญแจ KRA ก็จะใช้กุญแจส่วนตัวในการถอดรหัสลับและทำการกู้คืนกุญแจให้ได้

รูปแบบที่ 4 ให้ KRA ทำงานร่วมกันมากกว่าหนึ่งหน่วยงาน แต่เป็นการนำกุญแจสาธารณะของหน่วยงานมาเข้ารหัสลับชิ้นส่วนกุญแจ ซึ่งจัดเก็บไว้ใน KRF เมื่อต้องการกู้คืนกุญแจต้องใช้กุญแจส่วนตัวของ KRA ถอดรหัสลับข้อมูลกุญแจเช่นเดียวกัน

การให้ KRA ทำงานร่วมกันมากกว่าหนึ่งหน่วยงาน เป็นการเพิ่มความมั่นคงในการกู้คืนกุญแจ ผู้ใช้งานมีความเป็นส่วนตัวมากขึ้น แต่อาจเป็นการเพิ่มความซับซ้อนและเพิ่มระยะเวลาในการกู้คืนกุญแจ



รูปที่ 2.4 รูปแบบการจัดการกุญแจของหน่วยงานกู้คืนกุญแจ

2.4 รูปแบบความไว้วางใจ (Trust Model) ของผู้ให้บริการออกใบรับรอง (Certificate Authority : CA)

ผู้ให้บริการออกใบรับรองเป็นบุคคลที่สาม (Trusted Third Party : TTP) ที่มีรูปแบบความไว้วางใจ [3] ที่มีลำดับชั้นของการออกใบรับรองที่เข้มงวด (Strict Certification Hierarchy) กล่าวคือ ใบรับรองของบุคคลใด ๆ จะถูกสร้างโดยผู้ให้บริการออกใบรับรองเท่านั้น โดยผู้ให้บริการออกใบรับรองสามารถมีได้หลายลำดับชั้น ชั้นบนสุดเรียกว่า ผู้ให้บริการออกใบรับรองหลัก (Root CA) โดยที่ใบรับรองของผู้ให้บริการออกใบรับรองหลักเป็นแบบการรับรองตนเอง (Self-Signed) และเป็นผู้ออกใบรับรองสำหรับผู้ให้บริการออกใบรับรองในชั้นถัดลงมา (Intermediate CA) ที่อยู่ติดกันเป็นลำดับไปเรื่อย ๆ จนไปสิ้นสุดที่ผู้ให้บริการออกใบรับรองสำหรับผู้ใช้งาน

การมีผู้ให้บริการออกใบรับรองแบบหลายลำดับชั้นมีประโยชน์ในแง่ของการแบ่งกลุ่มผู้ใช้งานออกเป็นหลาย ๆ กลุ่ม เนื่องจากมีจำนวนผู้ใช้งานมาก ดังนั้นจึงมีการแบ่งกลุ่มผู้ใช้ตามหน่วยงานของผู้ใช้ตามความสามารถในการใช้งานใบรับรอง หรือตามระดับความรับผิดชอบของผู้ให้บริการออกใบรับรอง เป็นต้น

2.5 รูปแบบของ Trusted Third Party (TTP) ที่เกี่ยวข้องกับระบบการกู้คืนกุญแจ

ระบบการกู้คืนกุญแจมีการทำงานร่วมกับ TTP ที่ได้รับความไว้วางใจ โดยแบ่งตามหน้าที่ได้เป็น 3 กรณี คือ

2.5.1 TTP ที่ทำหน้าที่ในการกู้คืนกุญแจ

มีฟังก์ชั่นการทำงานหลากหลายรูปแบบขึ้นอยู่กับการให้บริการของแต่ละ TTP วิธีการที่นิยมในงานวิจัยส่วนใหญ่จะใช้วิธีการสร้างกุญแจคู่ของตัวเอง แล้วทำการส่งกุญแจสาธารณะให้กับผู้ใช้งาน (ผู้ส่งข้อมูล) เพื่อนำไปเข้ารหัสลับลับข้อมูลกุญแจที่ต้องการกู้คืน เมื่อผู้รับไม่สามารถใช้กุญแจถอดรหัสลับได้ TTP จะใช้กุญแจส่วนตัวในการกู้คืนกุญแจนั้น ตัวอย่างของ PPT ที่ทำหน้าที่ดังกล่าวได้แก่ บริการของศูนย์กลางให้การรับรอง Trusted Center (TC) ผู้ให้บริการออกใบรับรอง (Certificate Authority : CA) ศูนย์กลางการกู้คืนข้อมูล (Data Recovery Center : DRC) ศูนย์กลางการกู้คืนกุญแจ (Key Recovery Center : KRC) และหน่วยงานที่ให้บริการกู้คืนกุญแจ (Key Recovery Agent : KRA)

2.5.2 TTP ที่ทำหน้าที่เป็นผู้ให้บริการออกใบรับรองผู้ใช้งาน

มีหน้าที่ออกใบรับรองข้อมูลของผู้ใช้และใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ซึ่งข้อมูลของผู้ใช้ประกอบไปด้วย ข้อมูลส่วนบุคคลและข้อมูลกุญแจสาธารณะของผู้ใช้งาน เช่น ข้อมูลผู้ให้บริการออกใบรับรอง (CA)
ผู้ให้บริการออกใบรับรองที่น่าเชื่อถือ จำเป็นต้องมีระบบรักษาความปลอดภัยของข้อมูลระดับสูง เนื่องจากข้อมูลดังกล่าวมีผลต่อการยืนยันตัวบุคคลในการสื่อสารบนเครือข่าย และการประกอบธุรกรรมทางอิเล็กทรอนิกส์

2.5.3 TTP ที่ทำหน้าที่ ในการออกใบรับรองหน่วยงานกู้คืนกุญแจ

ซึ่งสามารถจะกระทำโดย CA [4] หน่วยงานผู้ให้บริการที่มีสิทธิ์ในการออกใบรับรองหน่วยงานกู้คืนกุญแจ (Key Recovery Authority : KRAu) หรือ หน่วยงานออกใบรับรองการจัดเก็บกุญแจ (Certificate Escrow Authority : CEA) โดยเฉพาะก็ได้

2.5.4 TTP ที่ทำหน้าที่ในการให้บริการกุญแจ (Key Distribution)

เพื่อให้ผู้ใช้นำกุญแจไปใช้ในการเข้ารหัสลับลับข้อมูลที่มีการสื่อสารกัน ในแต่ละช่วงเวลา (Session) เช่น บริการของ Kerberos [5] หรือ ศูนย์กลางกระจายกุญแจ (Key Distribution Center : KDC) [6] เป็นต้น โดยทำการสุ่มค่าตัวเลขเพื่อสร้างกุญแจ และใช้วิธีการที่ปลอดภัยในการส่งกุญแจผ่านระบบเครือข่าย

2.6 วิธีการ/กระบวนการพื้นฐานสำหรับการกู้คืนกุญแจ

ฟิลด์ที่ใช้ในการกู้คืนกุญแจ หรือที่เรียกว่า เคอาร์เอฟ (KRF) [7] จะถูกสร้างโดยผู้ส่ง และถูกแนบไปกับข้อความที่ผ่านการเข้ารหัสลับแล้ว โดย KRF ประกอบด้วย ส่วนประกอบของกุญแจที่ใช้ในการถอดรหัสลับข้อมูล และเพื่อความมั่นคงของกุญแจ กุญแจจะถูกเข้ารหัสลับ ผู้ที่สามารถถอดรหัสลับกุญแจได้คือ KRA ที่ผู้ส่งเลือกใช้บริการเท่านั้น

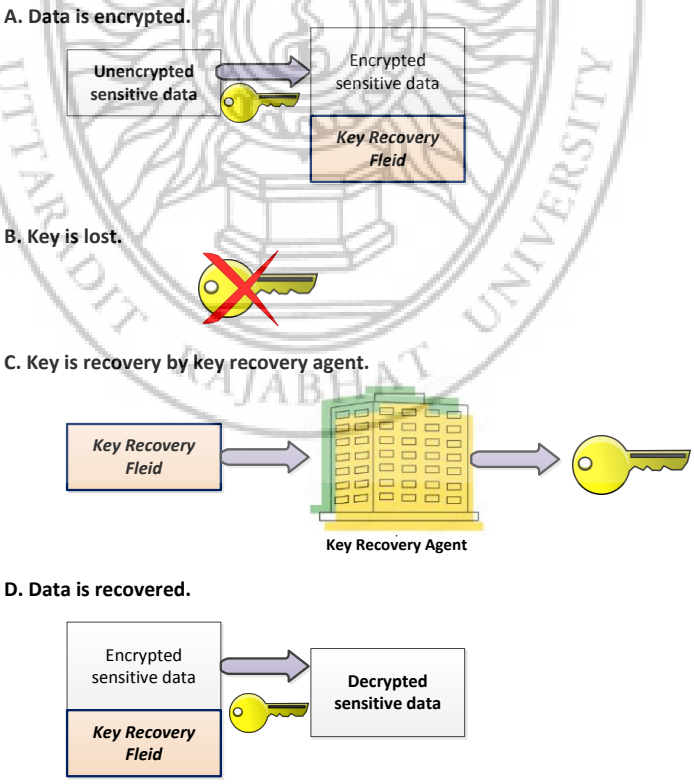
พื้นฐานของกระบวนการกู้คืนกุญแจประกอบไปด้วยขั้นตอนง่าย ๆ โดยได้แสดงตามรูปที่ 2.5 ดังนี้

ขั้นตอนที่ 1 (A) ข้อความต้นฉบับถูกเข้ารหัสลับ และผู้ส่งสร้าง KRF โดยข้อมูลทั้งสองส่วนถูกแนบส่งไปด้วยกัน

ขั้นตอนที่ 2 (B) เมื่อทางฝั่งผู้รับไม่มีกุญแจในการถอดรหัสลับข้อมูล อาจเนื่องมาจากกุญแจหายหรือกุญแจไม่สามารถใช้งานได้

ขั้นตอนที่ 3 (C) ผู้รับร้องขอบริการการกู้คืนกุญแจ โดยส่ง KRF ให้ KRA

ขั้นตอนที่ 4 (D) KRA ทำการกู้คืนกุญแจโดยอาศัยข้อมูลจาก KRF และผู้ส่งสามารถนำกุญแจที่ได้ไปใช้ในการถอดรหัสลับต่อไป



รูปที่ 2.5 กระบวนการพื้นฐานในการกู้คืนกุญแจ

2.7 การแชร์ความลับ (Secret Sharing)

การแชร์ความลับ หรือการแบ่งปันค่าของความลับ [8] หมายถึงวิธีการกระจายความลับไปในสมาชิกของกลุ่มที่เกี่ยวข้องกัน เปรียบเสมือนการจัดสรรชิ้นส่วนของความลับให้กับผู้ที่เกี่ยวข้องในกลุ่มนั่นเอง การที่จะได้มาซึ่งความลับนั้นจะต้องนำชิ้นส่วนทุกชิ้นส่วนที่กระจายไปยังสมาชิกในกลุ่มมาประกอบกันให้ครบทุกชิ้นส่วน โดยจะมีการกำหนดให้สมาชิกในกลุ่ม เท่ากับ n

วิธีการแชร์ความลับขั้นพื้นฐานหรือการแชร์ความลับอย่างง่าย คือ การจัดสรรความลับ (SC) ออกเป็น n ชิ้น เพื่อแจกให้กับสมาชิกในกลุ่ม n คน ซึ่งจะอาศัยการสุ่มค่าตัวเลข (Random Number) และคำนวณทางคณิตศาสตร์ คือ Excursive OR (XOR) เข้ามาช่วยในการแบ่งความลับและการรวมความลับ โดยมีขั้นตอนอย่างง่ายดังนี้

การจัดสรรแบ่งความลับ

1) การจัดสรรความลับหรือการแบ่งความลับ ทำได้ด้วยการสุ่มค่าตัวเลข (S_R) มาจำนวน n-1 ตัว คือ S_{R1} , S_{R2} , ..., $S_{R\,n-1}$ ดังนั้นจากขั้นตอนนี้จะสามารถจัดสรรความลับให้สมาชิกในกลุ่ม n-1 คน

2) นำตัวเลขที่ได้จากการสุ่มข้างต้นทุกตัวมา XOR กัน และ XOR กับ S_C เพื่อเป็นค่าความลับสำหรับสมาชิกคนที่ n ซึ่งสามารถแสดงได้ดังนี้ $S_{Rn} = S_{R1} \oplus S_{R2} \oplus ... \oplus S_{R\,n-1} \oplus S_C$

การรวมความลับ

1) การรวมความลับหรือการได้มาซึ่งความลับจะเกิดจาก การนำส่วนประกอบของความลับทั้งหมดตั้งแต่ S_{R1} ถึง S_{Rn} มาทำการ XOR กัน สามารถแสดงได้ดังนี้ $S_C = S_{R1} \oplus S_{R2} \oplus ... \oplus S_{Rn}$

2.8 เพาเวอร์เซต (Power Set)

ในคณิตศาสตร์ หากกำหนดให้ S แทนเซต ดังนั้นสามารถเขียนเพาเวอร์เซต [9] ของเซต S ได้ดังนี้ P(S) ซึ่งก็คือ สมาชิกทั้งหมดเป็นซับเซตของเซต S ใช้สัญลักษณ์ $P(S) = \{x \mid x \subset S\}$

ถ้า S เป็นเซตจำกัด

ถ้า n(S) = k แล้ว

(1) $n[P(S)] = 2^k$

(2) $n[P(P(S))] = 2^{2^k}$

ทฤษฎีเกี่ยวกับเพาเวอร์เซต : ถ้า A และ B เป็นเซตจำกัดใด ๆ

(1) สมาชิกทุกตัวของเพาเวอร์เซต ต้องเป็นเซต

(2) $\phi \in P(A)$ และ $\phi \subset P(A)$ เสมอ

(3) $A \in P(A)$ เสมอ แต่ A ไม่จำเป็นต้องเป็นสับเซตของP(A)

(4) เมื่อ $A \in P(A)$ ดังนั้น $P(A) \in P(P(A))$

(5) เพาเวอร์เซต จะไม่มีทางเป็นเซตว่างได้เลยนั่นคือ $P(A) \neq \phi$

(6) $P(\phi) = \{\phi\}$

(7) $\{A\} \subset P(A)$ เสมอ ดังนั้น $\{P(A)\} \subset P(P(A))$

(8) $P(A \cap B)=P(A) \cap P(B)$

(9) ถ้า $A \subset B$ แล้ว $P(A) \subset P(B)$

ตัวอย่าง ถ้า S = {*x*, *y*, *z*}, แล้ว สมาชิกของซับเซต S คือ { } หรือ ϕ, {*x*}, {*y*}, {*z*}, {*x*, *y*}, {*x*, *z*}, {*y*, *z*} และ {*x*, *y*, *z*}

ดังนั้น P(S) = {{}, {*x*}, {*y*}, {*z*}, {*x*, *y*}, {*x*, *z*}, {*y*, *z*},{*x*, *y*, *z*}}

2.9 การห่อหุ้มกุญแจ (Key Encapsulation)

เมื่อนำกุญแจลับ (Secret Key: Ks) หรือส่วนประกอบของกุญแจลับมาผ่านกระบวนการเข้ารหัสลับ พร้อมด้วยข้อมูลสำหรับการกู้คืนกุญแจ จากนั้นถูกห่อหุ้ม (Capsule)ไว้ เรียกว่า Key Encapsulation ซึ่งมีลักษณะเป็นบล็อกหรือฟิลด์ที่ใช้สำหรับการกู้คืนกุญแจ (Key Recovery Block: KRB หรือ Key Recovery Field: KRF) ผู้ที่สามารถถอดรหัสลับบล็อกหรือฟิลด์นี้ได้ คือ หน่วยงานที่มีหน้าที่รับผิดชอบในการกู้คืนกุญแจ (KRC หรือ KRA) เมื่อผู้ใช้งานต้องการกู้คืนกุญแจ ฟิลด์ KRB หรือ KRF จะถูกส่งไปยังหน่วยงานกู้คืนกุญแจ เพื่อทำการกู้คืนกุญแจลับดังกล่าว แล้วส่งให้กับผู้ร้องขอการกู้คืนต่อไป

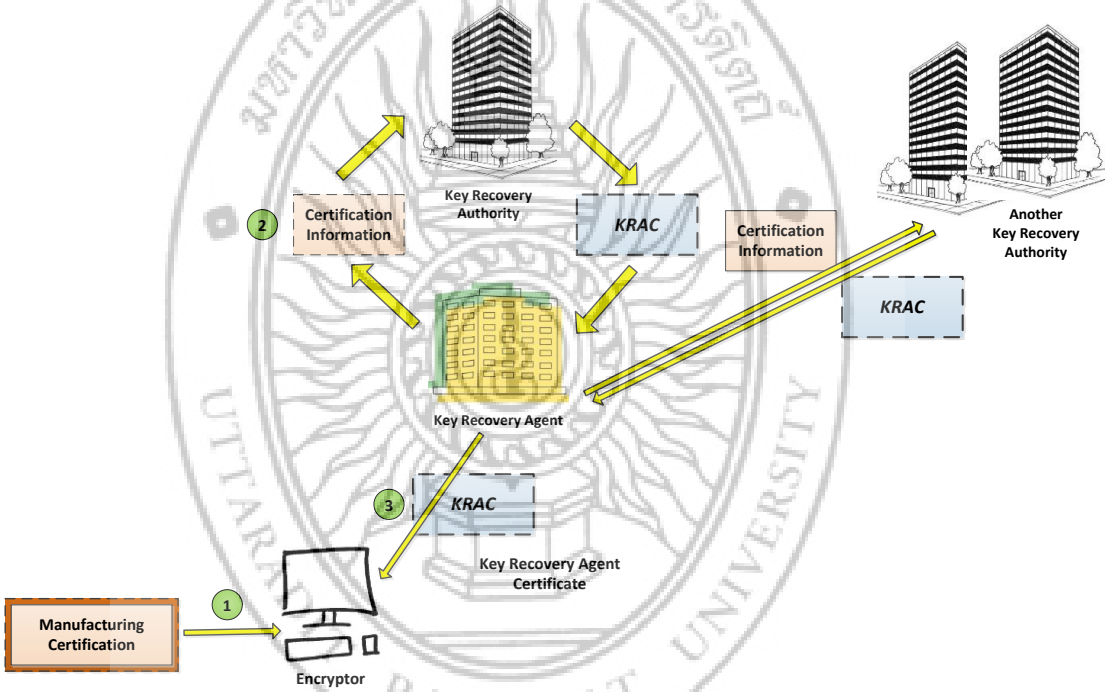
การใช้วิธีการห่อหุ้มกุญแจลับนี้ ช่วยลดความเสี่ยงในเรื่องของการคุกคามความเป็นส่วนตัวของเจ้าของกุญแจได้

2.10 งานวิจัยที่เกี่ยวข้อง

2.10.1 Cylink's Key Recovery

งานวิจัยนี้ได้นำเสนอลักษณะการทำงานของระบบกู้คืนกุญแจ [7] โดยมีฟิลด์ที่ใช้ในการกู้คืนกุญแจที่เรียกว่า เคอาร์เอฟ (Key Recovery Field : KRF) ซึ่งผู้ใช้งานจะต้องมีการเลือกใช้บริการจากเอเจนต์ในการกู้คืนกุญแจ (Key Recovery Agent : KRA) โดยกุญแจจะถูกจัดเก็บและปกป้องไว้ใน KRF ซึ่งเป็นส่วนที่นำมาใช้ในการกู้คืนกุญแจ ผู้ที่ทำหน้าที่ในการกู้คืน คือ KRA เท่านั้น

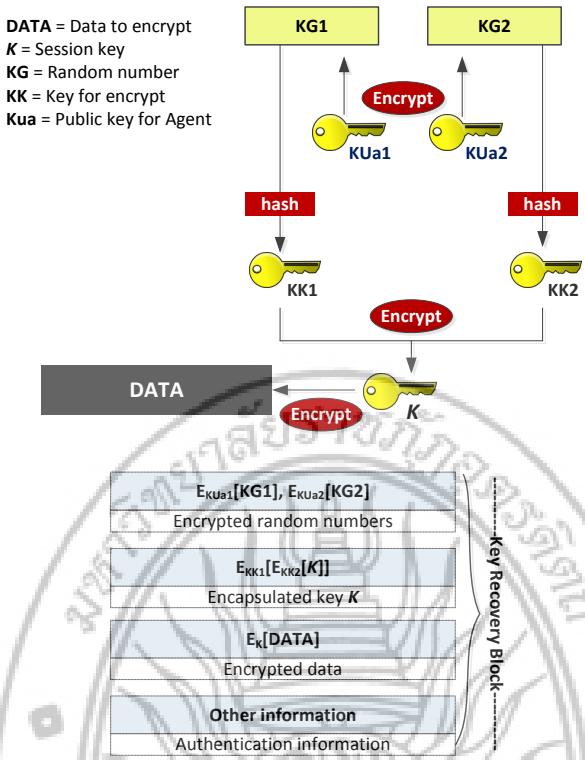
Cylink's Key Recovery สนับสนุนการกู้คืนกุญแจสำหรับข้อมูลที่ถูกเข้ารหัสลับบนพื้นฐานของความสัมพันธ์แบบไว้วางใจ (Trusted Relationship) ระหว่างส่วนของผู้ใช้งาน ส่วนของ KRA และหน่วยงานผู้ให้บริการที่มีสิทธิ์ในการออกใบรับรองหน่วยงานกู้คืนกุญแจ (Key Recovery Authority: KRAu) ดังแสดงตามรูปที่ 2.6 และงานวิจัยนี้ได้เน้นถึงความต้องการพื้นฐานสำหรับระบบการกู้คืนกุญแจที่น่าสนใจ คือ ระบบต้องสามารถกู้คืนกุญแจที่ผู้ใช้งานทำหาย หรือเกิดกรณีที่กุญแจไม่สามารถใช้งานได้ ผู้ใช้งานจะต้องเลือกใช้บริการจาก KRA ระบบจะกู้คืนเฉพาะกุญแจเท่านั้น จะไม่มีการเปิดเผยข้อมูล และระบบจะต้องสอดคล้องกับกฎระเบียบและข้อบังคับของรัฐบาลที่ว่าด้วยเรื่องการนำเข้าและส่งออกผลิตภัณฑ์ที่เกี่ยวข้องกับเทคโนโลยีการเข้ารหัสลับ



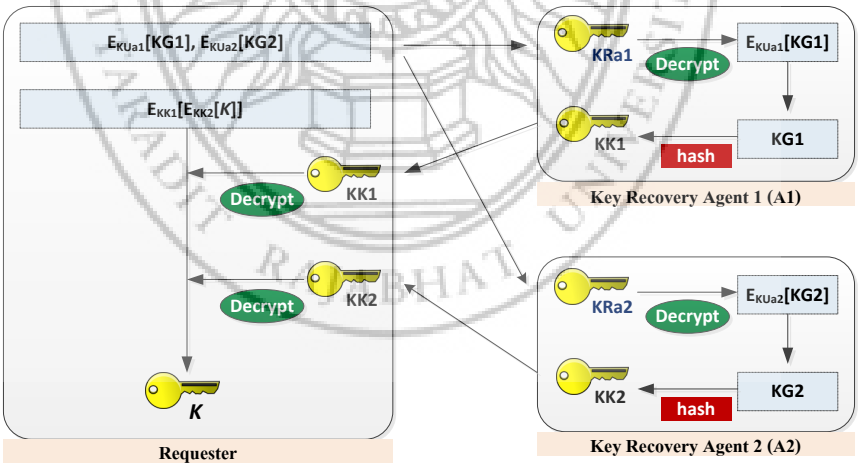
รูปที่ 2.6 การสร้างความสัมพันธ์แบบไว้วางใจระหว่างผู้ใช้งาน หน่วยงานกู้คืนกุญแจ และหน่วยงานผู้ให้บริการที่มีสิทธิ์ในการออกใบรับรองหน่วยงานกู้คืนกุญแจ

2.10.2 Internet Archiving Server with Key Recovery Function

งานวิจัยนี้ได้นำเสนอวิธีการกู้คืนกุญแจแบบ M-KRS โดยไม่อาศัย KRC [10] ใช้ฟิลด์ในการกู้คืนกุญแจที่เรียกว่า เคอาร์บี (Key Recovery Block: KRB) โดยมีวิธีการสร้าง KRB ดังแสดงในรูปที่ 2.7 และให้ KRA ทำหน้าที่ในการกู้คืนกุญแจ ดังแสดงในรูปที่ 2.8 กู้คืนกุญแจได้อย่างถูกต้องในกรณีที่ KRA ทำงานครบทุกเอเจนต์ หากมีเอเจนต์ใดเอเจนต์หนึ่งขัดข้อง คือ ไม่สามารถให้บริการกู้คืนกุญแจได้ จะส่งผลให้ระบบไม่สามารถกู้คืนกุญแจได้เช่นกัน



รูปที่ 2.7 การสร้างฟิลด์สำหรับการกู้คืนกุญแจ

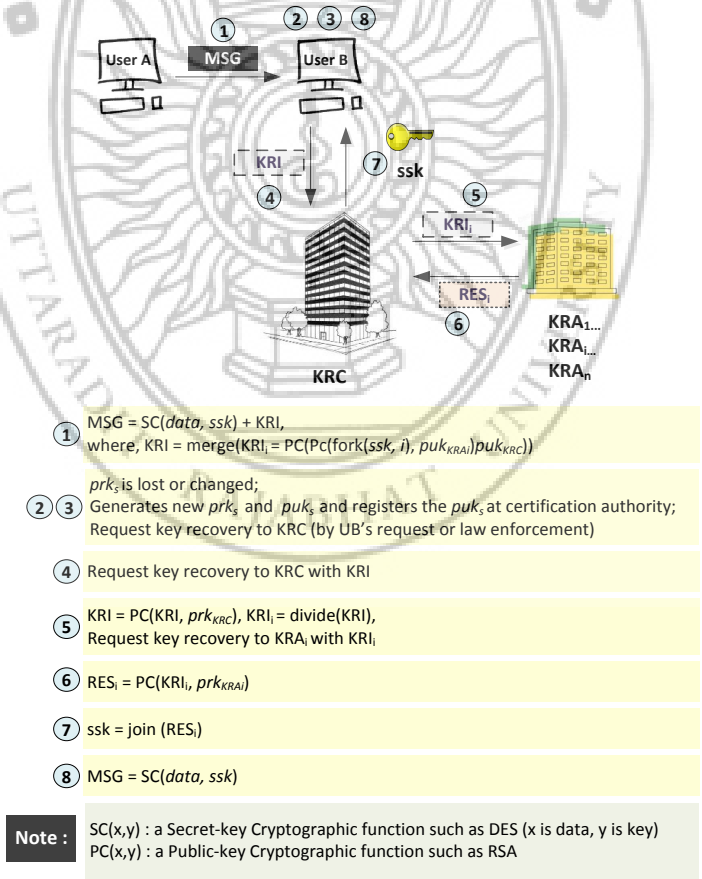


รูปที่ 2.8 การกู้คืนกุญแจ

2.10.3 Modeling of Multiple Agent Based Cryptographic Key Recovery Protocol

งานวิจัยนี้เน้นอธิบายโครงสร้างของสถาปัตยกรรมการทำงานของ KRS แบบ M-KRS [11, 12] ที่ผู้ใช้บริการกู้คืนกุญแจสามารถระบุจำนวนการขอใช้บริการ KRA ได้มากกว่าหนึ่งเอเจนต์ การกู้คืนกุญแจลับสามารถกู้คืนได้จากฟิลด์ข้อมูลกู้คืนกุญแจ ที่เรียกว่า เคอาร์ไอ (Key Recovery Information: KRI) โดยได้นำเสนอความต้องการพื้นฐานและสมมติฐานของระบบกู้คืนกุญแจที่น่าสนใจไว้ดังนี้ คือ การกู้คืนกุญแจจะกระทำสำเร็จได้ต้องอยู่ภายใต้การควบคุมของผู้ที่มีสิทธิ์หรือมีความมั่นคงภายใต้นโยบายหรือกฎหมาย การกู้คืนถูกจำกัดได้เฉพาะการกู้คืนกุญแจลับเท่านั้น (ไม่รวมถึงการกู้คืนข้อมูล) การกู้คืนกุญแจจะกระทำการอยู่บนโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) ดังนั้น ใบรับรองของแต่ละหน่วยงานกู้คืนกุญแจจะถูกกระจายหรือประกาศโดยผู้ให้บริการออกใบรับรอง (Certificate Authority: CA)

การกู้คืนกุญแจแบบใช้ KRA ได้มากกว่า 1 เอเจนต์หรือที่เรียกว่า M-KRS นั้น ได้แบ่งกระบวนการทำงานหลัก ๆ ออกเป็น 3 ขั้นตอน ดังแสดงตามรูปที่ 2.9 คือ



รูปที่ 2.9 กระบวนการทำงานของ Multiple Agent Based Cryptographic Key Recovery Protocol

ขั้นตอนที่ 1 เริ่มต้นระบบ (Initialization) กุญแจสาธารณะของทุก ๆ KRA ถูกกระจายและประกาศ บนโครงสร้างพื้นฐานกุญแจสาธารณะ หลังจากที่ CA ออกใบรับรองให้กับ KRA แล้ว ในใบรับรองจะให้การรับรองกุญแจสาธารณะและข้อมูลของ KRA เพื่อการระบุตัวตน และไว้สำหรับการพิสูจน์ตัวจริง

ขั้นตอนที่ 2 การสื่อสารและการสร้างข้อมูลกู้คืนกุญแจ (Communication and Key Recovery Information Generation) ผู้ส่งทำการสุ่มเลือก KRA ว่าจะใช้กี่เอเจนต์ในการกู้คืนกุญแจ และทำการสร้าง KRI โดยใช้กุญแจสาธารณะของ KRC กับกุญแจสาธารณะของ KRA ในการเข้ารหัสลับ และทำการเลือก KRA ที่จะใช้บริการ ขั้นตอนนี้จะใช้กุญแจลับในการเข้ารหัสลับข้อมูลต้นฉบับ จากนั้นจะแนบข้อมูลต้นฉบับไปกับ KRI ส่งให้ผู้รับ

ขั้นตอนที่ 3 เมื่อผู้รับไม่สามารถทำการถอดรหัสลับได้ เนื่องจากกุญแจที่ใช้ในการถอดรหัสลับไม่สามารถใช้งานได้หรือสูญหาย หรือหน่วยงานที่มีอำนาจต้องการตรวจสอบ (กู้คืน) ข้อมูล จะต้องทำการสร้างกุญแจคู่ใหม่ และลงทะเบียนกุญแจสาธารณะไว้กับ CA เพื่อขอใบรับรองกุญแจสาธารณะ เมื่อได้รับใบรับรองแล้วจึงร้องขอการกู้คืนกุญแจต่อไป ด้วยการส่งใบรับรองของผู้ร้องขอความต้องการและข้อมูลในการกู้คืนกุญแจไปยัง KRC จากนั้นจะเป็นกระบวนการถอดรหัสลับข้อมูลตามลำดับ จนกระทั่งได้กุญแจลับเพื่อนำไปถอดรหัสลับข้อมูล

อย่างไรก็ตามงานวิจัยนี้ได้เสนอระบบ M-KRS แบบอาศัย KRC โดยใช้เทคนิคการแชร์ความลับ (Secret Sharing) ในการแบ่งและจัดสรรส่วนประกอบของกุญแจลับไปไว้ใน KRI ของทุก KRA ที่อยู่ในกลุ่มการกู้คืนกุญแจ ซึ่งวิธีการดังกล่าวเป็นวิธีการที่ไม่ซับซ้อน ทำให้เกิดความรวดเร็วต่อกระบวนการกู้คืนกุญแจ ทั้งนี้สามารถอธิบายวิธีการแบ่งและจัดสรรกุญแจ และการรวมกุญแจ ได้ดังต่อไปนี้

การแบ่งและจัดสรรกุญแจ โดยผู้ส่ง

1) สุ่มตัวเลข (rk) จำนวน n-1 ตัว สำหรับ n เอเจนต์ (*Agent*) เช่น $rk_1, rk_2, ..., rk_{n-1}$, สำหรับ $Agent_1, Agent_2, ..., Agent_n$

2) รวมส่วนประกอบของกุญแจ ด้วยการใช้ XOR เพื่อนำค่าดังกล่าวไปเก็บไว้ใน KRF ดังนี้

ค่าใน KRF สำหรับ $Agent_1$ (ik_1) : ssk $\oplus$ rk_1

ค่าใน KRF สำหรับ $Agent_2$ (ik_2) : $rk_1 \oplus rk_2$

ค่าใน KRF สำหรับ $Agent_i$ (ik_i) : $rk_{i-1} \oplus rk_i$

ค่าใน KRF สำหรับ $Agent_n$ (ik_n) : rk_{n-1}

การรวมกุญแจ โดย KRC

1) นำค่าใน KRF มาทำการคำนวณกุญแจลับ ดังนี้

join (ik_1, ... ik_i, ... ik_n) = $ik_1 \oplus ik_2 \oplus ...., \oplus ik_i ... \oplus ... \oplus ik_n$

ดังนั้นกุญแจลับ (ssk) = (ssk $\oplus$ rk_1) $\oplus$ (rk_1 $\oplus$ rk_2) $\oplus$..., (rk_{i-1} $\oplus$ rk_i),...(rk_{n-2} $\oplus$ rk_{n-1}) $\oplus$ rk_{n-1}

โดยที่ ik_i ถูกเข้ารหัสลับที่ผู้ส่ง ด้วยกุญแจสาธารณะของ KRA และถอดรหัสลับที่ KRA ที่ i (KRA_i) ด้วยกุญแจส่วนตัวของ KRA_i

บทที่ 3
วิธีดำเนินการวิจัย

3.1 ประเภทโครงการวิจัย

งานวิจัยนี้เป็นงานวิจัยพื้นฐาน (Pure Research)

3.2 ตัวแปรที่ทำการศึกษา

3.2.1 ตัวแปรต้น

ขั้นตอนวิธีการแชร์ความลับ

3.2.2 ตัวแปรตาม

การสร้างฟิลด์ในการกู้คืนกุญแจ (KRF)

3.3 ขั้นตอนวิธีดำเนินการวิจัย

ขั้นตอนและวิธีการที่ใช้ในการวิจัยแบ่งออกเป็น 2 ระยะ คือ

ระยะที่ 1 (ศึกษากระบวนการ)

(1.1) ศึกษากระบวนการทำงานของระบบการกู้คืนกุญแจแบบหลายเอเจนต์

(1.2) ศึกษาวิธีการพื้นฐานในการแชร์ความลับ (Secret Sharing)

ระยะที่ 2 (เสนอรูปแบบ ทดสอบ และสรุปผล)

(2.1) เสนอรูปแบบขั้นตอนวิธีการแชร์ความลับในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ โดยใช้แนวคิดเรื่องการแชร์ความลับ (Secret Sharing) มาใช้ในการแบ่งกุญแจออกเป็นส่วนๆ และจัดสรรส่วนประกอบของกุญแจ และนำทฤษฎีพื้นฐานเรื่องเพาเวอร์เซต (Power Set) มาใช้ในกระบวนการสำรองส่วนประกอบของกุญแจ สำหรับการกู้คืนกุญแจในกรณีที่มีบางเอเจนต์ไม่สามารถให้บริการได้

(2.2) ทดสอบขั้นตอนวิธีการแชร์ความลับ โดยพิจารณาถึงความถูกต้องในการกู้คืนกุญแจ ความเป็นส่วนตัวของผู้ใช้งาน ความสามารถในการเข้าถึงข้อมูลได้อย่างถูกต้อง ระบบมีความพร้อมใช้งานและมีความน่าเชื่อถือ สามารถพิสูจน์ตัวจริงของเอเจนต์ได้ และทำงานบนโครงสร้างพื้นฐาน PKI

(2.3) ประเมินผล สรุปผล และจัดทำเอกสาร

บทที่ 4
ผลการวิจัย

การวิจัยนี้มีวัตถุประสงค์เพื่อเสนอรูปแบบขั้นตอนวิธีการแชร์ความลับ ในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ โดยใช้แนวคิดเรื่องการแชร์ความลับ (Secret Sharing) มาใช้ในการแบ่งกุญแจออกเป็นส่วนๆ และจัดสรรส่วนประกอบของกุญแจ

ทั้งนี้จะได้ทดสอบนำไปใช้ในการกู้คืนกุญแจแบบหลายเอเจนต์ในรูปแบบ การกู้คืนกุญแจแบบหลายเอเจนต์ ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ โดยมีผลการวิจัยดังต่อไปนี้

4.1 ขั้นตอนวิธีการแชร์ความลับ ในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ

ขั้นตอนวิธีการแชร์ความลับในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ จะอาศัยการแบ่งและจัดสรรส่วนประกอบของกุญแจ Ks ทำให้การจัดเก็บค่าแอตทริบิวต์ในฟิลด์ KRF เป็นไปอย่างเหมาะสม โดยจะประกอบด้วยกระบวนการแชร์ความลับของกุญแจ Ks และการถอดรหัสความลับ โดยสามารถแสดงได้ในตารางที่ 4.1 และ 4.2 ตามลำดับ

ตารางที่ 4.1 ขั้นตอนการแชร์ความลับของกุญแจ Ks

ขั้นตอนการแชร์ความลับของ *Ks*	วิธีการ
(1) สุ่มตัวเลขจำนวน *n*-1 ตัว สำหรับ *n*-1 เอเจนต์	$S_1, S_2, ..., S_{n-1}$
(2) คำนวณ S_n สำหรับ $Agent_n$	$S_n = S_1 \oplus S_2 \oplus ... \oplus S_{n-1} \oplus Ks$
(3) สุ่มตัวเลข *R* สำหรับทุก ๆ เอเจนต์ $(R_i's)$	$R_1, R_2, ..., R_n$
(4) คำนวณหาค่าความลับ *SGN*	$SGN = R_1 \oplus R_2 \oplus ... \oplus R_n$
(5) คำนวณค่า *TT* สำหรับทุก ๆ เอเจนต์ $(TT_i's)$	$TT_i = S_i \oplus SGN$; เมื่อ $i = 1$ ถึง n

ตารางที่ 4.2 การถอดรหัสความลับของกุญแจ Ks

ขั้นตอนการถอดรหัสความลับของ Ks		วิธีการ
แอตทริบิวต์สำหรับใช้ในการกู้คืนกุญแจ Ks { S_i , TT_i , SGN }	S_i	คือ ส่วนประกอบของกุญแจ Ks { **Ks** = $S_1 \oplus S_2 \oplus ... \oplus S_n$ }
	TT_i	ใช้กู้คืน S_i เมื่อมีบางเอเจนต์ล่ม { $TT_i = S_i \oplus SGN$ }
	SGN	ใช้พิสูจน์ตัวจริงของเอเจนต์ในกลุ่มการกู้คืน

จากตารางที่ 4.1 และ 4.2 จะได้นำไปใช้ในขั้นตอนการสร้างฟิลด์ KRF ของระบบการกู้คืนกุญแจแบบหลายเอเจนต์ ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ

4.2 การใช้วิธีการแชร์ความลับในกระบวนการสร้าง KRF สำหรับการกู้คืนกุญแจแบบหลายเอเจนต์ ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ

4.2.1 การสร้างฟิลด์ในการกู้คืนกุญแจ (KRF)

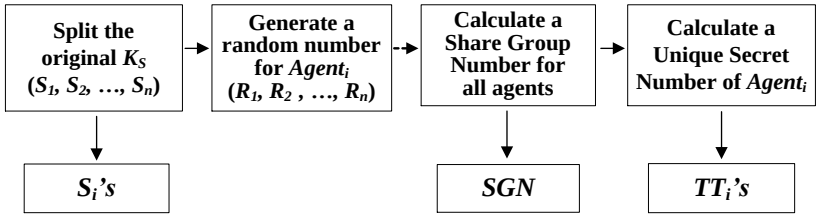
KRF จะถูกสร้างขึ้นเพื่อใช้ในการกู้คืนกุญแจ Ks ในกรณีที่กุญแจหาย หรือกุญแจไม่สามารถใช้งานได้ ซึ่งจะถูกแนบไปกับข้อมูลต้นฉบับ (M) ที่ผ่านการเข้ารหัสลับด้วยกุญแจลับ (Ks[M]) เรียบร้อยแล้ว

KRF ประกอบด้วยข้อมูลต่อไปนี้ (1) ส่วนประกอบของกุญแจ Ks (2) แอตทริบิวต์สำหรับการระบุตัวตนของ KRA ในกลุ่มการกู้คืน (3) แอตทริบิวต์สำหรับการกู้คืนส่วนประกอบของกุญแจ Ks ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล่ม และ (4) ข้อมูลที่จำเป็นสำหรับการระบุตัวตนของผู้ที่มีส่วนร่วมในระบบ

การสร้างฟิลด์ KRF แบ่งออกเป็นส่วนย่อย ๆ ได้สองขั้นตอน คือ (1) การสร้างส่วนประกอบของฟิลด์ KRF โดยใช้วิธีการแชร์ความลับ และ (2) การประกอบฟิลด์ KRF

1) การสร้างส่วนประกอบของฟิลด์ KRF โดยใช้วิธีการแชร์ความลับ

ฟิลด์ KRF ถูกสร้างขึ้นเพื่อใช้ในการกู้คืนส่วนประกอบของกุญแจลับ (S_i) และกุญแจลับ Ks ขั้นตอนการสร้างส่วนประกอบของฟิลด์ KRF สามารถอธิบายได้ดังรูปที่ 4.1 ซึ่งมีกระบวนการดังต่อไปนี้



รูปที่ 4.1 กระบวนการสร้างส่วนประกอบของฟิลด์ KRF

1.1) แบ่ง Ks ออกเป็น *n* ชิ้น เมื่อ *n* คือ จำนวน KRA ทั้งหมดที่ใช้ในการกู้คืนกุญแจ โดยได้ใช้แนวคิดเรื่องการแชร์ความลับ

กระบวนการแบ่งกุญแจลับสามารถทำได้ดังต่อไปนี้

1.1.1) สุ่มตัวเลข จำนวน *n*-1 ตัว สำหรับ *n*-1 เอเจนต์ (*Agent*) เช่น $S_1, S_2,\ldots, S_{n-1}$ สำหรับ $Agent_1, Agent_2, \ldots, Agent_{n-1}$ ตามลำดับ

1.1.2) คำนวณ S_n สำหรับ $Agent_n$ ด้วยการ XOR ค่า S_i และกุญแจ Ks

$$S_n = S_1 \oplus S_2 \oplus \ldots \oplus S_{n-1} \oplus Ks$$

1.2) สุ่มตัวเลข *R* สำหรับทุก ๆ เอเจนต์ (R_i'*s*) เพื่อนำไปคำนวณหาค่าความลับของกลุ่มการกู้คืนกุญแจ (*SGN*) สำหรับการยืนยันตัวตนของ KRA

1.3) คำนวณหาค่าความลับ *SGN* ด้วยการ XOR ค่าของแอตทริบิวต์ R_i ทั้งหมด

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

1.4) คำนวณหาค่าของแอตทริบิวต์พิเศษ (*TT*) สำหรับทุก ๆ เอเจนต์ (TT_i'*s*) เพื่อใช้ในการกู้คืน S_i ในกรณีที่มีบาง KRA ในกลุ่มการกู้คืนล่ม โดยสามารถคำนวณได้จาก

$$TT_i = S_i \oplus SGN$$

2) การประกอบฟิลด์ KRF

ฟิลด์ KRF ของ HADM-KRS ประกอบด้วยฟิลด์ KRF ย่อย ๆ (KRF_i'*s*) ของเอเจนต์ในกลุ่มการกู้คืนกุญแจ (KRA_i)

ฟิลด์ KRF_i ประกอบด้วย S_i, *SGN*, TT_i และ *other information* แต่ละส่วนประกอบมีความสำคัญดังนี้

S_i คือส่วนประกอบของกุญแจ Ks

SGN เป็นค่าสำหรับการยืนยันตัวตนของ KRA ที่อยู่ในกลุ่มการกู้คืน

TT_i เป็นค่าสำหรับการกู้คืน S_i ในกรณี KRA ที่อยู่ในกลุ่มการกู้คืนล่ม

Other information เก็บค่าอื่น ๆ ที่จำเป็นสำหรับการพิสูจน์ตัวจริงหรือการตรวจสอบเพื่อเพิ่มความมั่นคงปลอดภัยให้กับระบบ เช่น ใบรับรองกุญแจสาธารณะของเอเจนต์ และของผู้ที่มีสิทธิ์ในการร้องขอการกู้คืนกุญแจ เป็นต้น

4.2.2 โครงสร้างฟิลด์ KRF

4.2.2.1 ฟิลด์ *KRF* ประกอบด้วยฟิลด์ KRF_i จำนวน n ชิ้น ดังนี้

$KRF = \{Ku_{agi}[\ KRF_i\text{'s }]\}$

4.2.2.2 ฟิลด์ KRF_i ประกอบด้วย S_i, SGN, TT_i และ *other information* ดังนี้

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

ฟิลด์ KRF_i จะถูกเข้ารหัสด้วยกุญแจสาธารณะของ KRA (Ku_{agi}) ดังนั้น KRA_i เท่านั้นที่สามารถถอดรหัส KRF_i ได้ โดย KRA_i จะถอดรหัสฟิลด์ KRF_i เพื่อส่ง S_i และ SGN ไปยังผู้ร้องขอการกู้คืนส่วนประกอบของกุญแจ เพื่อจะได้ทำการคำนวณกุญแจลับ Ks ต่อไป

วิธีการแชร์ความลับมีการออกแบบให้ระบบมีความพร้อมใช้งานสูง กล่าวคือระบบสามารถทำงานได้แม้ในกรณีที่มีบาง KRA ล่ม โดยใช้ค่าของแอตทริบิวต์ TT_i ซึ่งจัดเก็บในฟิลด์ KRF_i สำหรับคำนวณ S_i ของ KRA_i ที่ล่ม

การจัดสรรค่าของแอตทริบิวต์ TT_i ไว้ในฟิลด์ KRF_i จะใช้ทฤษฎีเพาเวอร์เซต (Power Set) โดยมีขั้นตอนการแบ่งและจัดสรรดังนี้

1) ระบุจำนวน KRA ที่จะใช้ในการกู้คืนกุญแจ (n)

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

3) คำนวณหาจำนวนของ KRA สำหรับการกระจายค่า TT_i (t) ว่าจะกระจายค่า TT_i ไปให้กับ KRA กี่เอเจนต์ ได้จากสูตร

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

4) กระจายค่า TT_i ของ KRA_i (A_i) ไปยังเอเจนต์ที่อยู่ถัดไปในลักษณะของการหมุนตามเข็มนาฬิกา จำนวน t เอเจนต์ เมื่อ $i=1$ ถึง n ตามฟังก์ชันต่อไปนี้

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

ทั้งนี้ KRA จะใช้ค่า TT_i สำหรับการกู้คืน S_i ได้ไม่เกิน t-1

4.2.3 การกู้คืนส่วนประกอบของกุญแจ Ks และกุญแจ Ks

หากกุญแจ Ks สูญหายหรือไม่สามารถใช้ในการถอดรหัสข้อมูลได้ จะต้องมีกระบวนการกู้คืนกุญแจ Ks โดยในขั้นตอนการกู้คืนกุญแจ *Ks* สามารถแบ่งออกเป็นส่วนย่อย ๆ ได้สองขั้นตอน คือ (1) การกู้คืนส่วนประกอบของกุญแจ Ks (S_i*'s*) และ (2) การกู้คืนกุญแจ Ks

1) การกู้คืนส่วนประกอบของกุญแจ Ks (S_i*'s*)

ในขั้นตอนนี้จะเป็นการกู้คืน S_i ซึ่งกระบวนการกู้คืน S_i แบ่งออกเป็นสองส่วน คือ (1) ส่วนของผู้ร้องขอการกู้คืนกุญแจ(Requester) และ(2) ส่วนของ KRA โดยมีรายละเอียดดังต่อไปนี้

1.1) ส่วนของผู้ร้องขอการกู้คืนกุญแจ Ks

1.1.1) ผู้ร้องขอการกู้คืนกุญแจถอดรหัสฟิลด์ KRF จะได้ฟิลด์ KRF_i*'s*

1.1.2) ผู้ร้องขอการกู้คืนกุญแจส่งฟิลด์ KRF_i ให้กับ $Agent_i$ เมื่อ $i = 1$ ถึง n

1.2) ส่วนของ KRA

ขั้นตอนในการกู้คืน S_i สามารถแสดงได้ดังรูปที่ 3.5 โดยมีขั้นตอนดังต่อไปนี้

1.2.1) $Agent_i$ ถอดรหัสฟิลด์ KRF_i ด้วยกุญแจส่วนตัว (Kr_{agi}) จะได้ S_i, *SGN*, TT_i*'s*, และ *other information*

1.2.2) $Agent_i$ ตรวจสอบ *other information* เช่น ใบรับรองกุญแจสาธารณะ (Public Key Certificate) ของผู้ร้องขอ เป็นต้น

1.2.3) $Agent_i$ เข้ารหัส S_i และ *SGN* ด้วยกุญแจสาธารณะของผู้ร้องขอ (Ku_{req})

1.2.4) $Agent_i$ ส่ง $Ku_{req}[S_i \,||\, SGN]$ ให้กับผู้ร้องขอ เพื่อให้ผู้ร้องขอนำไปคำนวณหากุญแจ Ks ต่อไป

2) การกู้คืนกุญแจ Ks

ส่วนนี้เป็นหน้าที่ของผู้รับที่จะทำการคำนวณเพื่อกู้คืนกุญแจ Ks ซึ่งวิธีการดังกล่าวเป็นการช่วยลดภาระของ KRA และทำให้กุญแจ Ks มีความมั่นคง เป็นความลับ กล่าวคือกุญแจ Ks จะรู้เฉพาะผู้รับและผู้ส่ง หรือคู่สนทนาเท่านั้น การคำนวณการกู้คืนกุญแจ Ks มีขั้นตอนดังต่อไปนี้

2.1) ผู้ร้องขอถอดรหัส $Ku_{req}[S_i \,||\, SGN]$ ด้วย Kr_{req} จะได้ S_i และ *SGN*

2.2) ผู้ร้องขอตรวจสอบ S_i ของ $Agent_i$ โดยการเปรียบเทียบ *SGN*

2.3) ผู้ร้องขอคำนวณกุญแจ Ks ด้วย $S_1 \oplus S_2 \oplus \ldots \oplus S_n$ และนำกุญแจ Ks ไปใช้ในการถอดรหัสต่อไป

4.2.4 กรณีที่มีบาง KRA ล่ม

ในกรณีนี้ส่งผลให้ผู้ร้องขอการกู้คืนกุญแจ (ผู้รับ) รวบรวม $Ku_{req}[S_i]$ ได้ไม่ครบ ดังนั้นผู้ร้องขอจะต้องทำการร้องขอการกู้คืน S_i ที่หายไปหรือที่ยังไม่ได้รับกับ KRA ที่สามารถให้บริการได้ที่อยู่ในตำแหน่งถัดไป โดยกำหนดให้ KRA กู้คืน S_i ได้ไม่เกิน t-1 โดยมีกระบวนการดังต่อไปนี้

1) ผู้ร้องขอตรวจสอบ S_i ว่ายังไม่ได้รับมาจาก $Agent_i$ ใด

2) ผู้ร้องขอเข้ารหัสและส่งคำร้องขอการกู้คืนส่วนประกอบของกุญแจที่ยังไม่ได้รับ ($req\text{-}S_i$) และ SGN ด้วยกุญแจสาธารณะของเอเจตน์ถัดไป ($Agent_{nxt}$) ที่จะให้ทำการกู้คืนส่วนประกอบของกุญแจ (Ku_{nxt} of $Agent_{nxt}$) จะได้ $Ku_{nxt}[req\text{-}S_i \parallel SGN \parallel other\ information]$

3) $Agent_{nxt}$ ถอดรหัส $Ku_{nxt}[req\text{-}S_i \parallel SGN \parallel other\ information]$ ด้วยกุญแจส่วนตัว (Kr_{nxt})

4) $Agent_{nxt}$ ตรวจสอบ SGN พร้อมทั้งใบรับรองกุญแจสาธารณะของผู้ส่ง และคำนวณ S_i ดังนี้

$$S_i = TT_i \oplus SGN$$

5) $Agent_{nxt}$ เข้ารหัส S_i และ SGN ด้วย Ku_{req} จะได้ $Ku_{req}[S_i, SGN]$

6) $Agent_{nxt}$ ส่ง $Ku_{req}[S_i, SGN]$ ไปยังผู้ร้องขอ

จากการนำเสนอขั้นตอนวิธีการแชร์ความลับ สามารถนำมาใช้ในกระบวนการกู้คืนกุญแจ ทำให้กุญแจมีความมั่นคง ผู้ใช้งานมีความเป็นส่วนตัว และรองรับการเข้าถึงข้อมูลอย่างถูกต้อง ทำให้ระบบมีความพร้อมใช้งาน และมีความน่าเชื่อถือสูง ระบบสามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกันได้ อีกทั้งยังทำให้การกู้คืนกุญแจมีความยืดหยุ่น และมีความพร้อมใช้งานสูง (Flexibility and Availability) คือสามารถกู้คืนกุญแจได้ในกรณีที่มีบางเอเจนต์ล่มหรือไม่สามารถให้บริการได้ โดยอาศัยกระบวนการสำรองส่วนประกอบของกุญแจสำหรับการกู้คืนกุญแจ

บทที่ 5
สรุปผล และข้อเสนอแนะ

การวิจัยนี้ได้ศึกษาและนำเสนออัลกอริทึมของการแชร์กุญแจลับ สำหรับ M-KRS เพื่อให้กุญแจมีความมั่นคง เป็นความลับ ผู้ใช้งานมีความเป็นส่วนตัว และรองรับการเข้าถึงข้อมูลอย่างถูกต้อง ทำให้ระบบมีความพร้อมใช้งานและมีความน่าเชื่อถือสูง ระบบสามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกัน บนโครงสร้างพื้นฐานกุญแจสาธารณะหรือพีเคไอ (Public Key Infrastructure: PKI)

5.1 สรุปผล

จากการนำเสนอรูปแบบขั้นตอนวิธีการแชร์ความลับ สามารถนำไปใช้ในกระบวนการกู้คืนกุญแจในระบบการกู้คืนกุญแจแบบหลายเอเจนต์ที่ไม่อาศัยศูนย์กลางในการกู้คืนกุญแจ โดยประกอบด้วย วิธีการจัดเก็บส่วนประกอบของกุญแจ การแบ่งและจัดสรรส่วนประกอบของกุญแจเป็นส่วนๆ การกระจายเพื่อแชร์ส่วนประกอบของกุญแจไปอยู่ในฟิลด์ในการกู้คืนกุญแจ หรือการแชร์ความลับแบบหลายเอเจนต์

เมื่อนำขั้นตอนวิธีการแชร์ความลับ มาใช้ในการออกแบบกระบวนการกู้คืนกุญแจ Ks ทำให้กุญแจมีความมั่นคงปลอดภัย ผู้ใช้งานมีความเป็นส่วนตัว และรองรับการเข้าถึงข้อมูลอย่างถูกต้อง นอกจากนี้ยังส่งเสริมให้ระบบมีความพร้อมใช้งาน และมีความน่าเชื่อถือสูง เนื่องจากสามารถพิสูจน์ตัวจริงของเอเจนต์ที่อยู่ในกลุ่มการกู้คืนกุญแจเดียวกันได้ อีกทั้งยังทำให้การกู้คืนกุญแจมีความยืดหยุ่นและมีความพร้อมใช้งาน (Flexibility and Availability) สูง กล่าวคือสามารถกู้คืนกุญแจได้ในกรณีที่มีบางเอเจนต์ล่มหรือไม่สามารถให้บริการได้ โดยอาศัยกระบวนการสำรองส่วนประกอบของกุญแจสำหรับการกู้คืนกุญแจ

5.2 ข้อเสนอแนะ

สามารถนำขั้นตอนวิธีการแชร์ความลับไปใช้ในกระบวนการกู้คืนกุญแจแบบหลายเอเจนต์ที่อาศัยศูนย์กลางในการกู้คืนกุญแจได้

บรรณานุกรม

[1] Dorothy E. Denning and Dennis K. Branstad. 1996. “A Taxonomy for Key Escrow Encryption Systems.” Communications of the ACM, pp. 34-40.

[2] Dorothy E. Denning and Dennis K. Branstad. 1997. “A Taxonomy for Key Recovery Encryption Systems.” Internet besieged: countering cyberspace scofflaws, pp. 357-371.

[3] Guo Z., Okuyama. T and Finley M.R. “A New Trust Model for PKI Interoperability.” in Proceedings of the International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services, October 2005.

[4] Computer Security Resource Center, National Institute of Standards and Technology. Key Recovery Examples. [Online]. Available: http://csrc.nist.gov/krdp/exa.html, accessed 13 April 2013.

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

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

[7] Cylink. CyKeyTM: Cylink’s Key Recovery Solution. [Online].Available: http://tnlandforms.us/ornlwww/cykey.pdf, accessed 1 July 2018.

[8] Lv C., Jia X., Tiany L, Jing J., and Suny M. “Efficient Ideal Threshold Secret Sharing Schemes Based on EXCLUSIVE-OR Operations.” in Proceedings of the Fourth International Conference on Network and System Security, pp. 136-143, 2010.

[9] Jech T. 2006. Set Theory. New York: Springer-Verlag.

[10] Numao M. and Nakayama Y. “Internet Archiving Server with Key Recovery Function.” in Proceedings of the Symposium on Cryptography and Information Security, 1998.

[11] Shinyoung Lim, Sangseung Kang and Joochan Sohn. “Modeling of Multiple Agent Based Cryptographic Key Recovery Protocol.” in Proceedings of the Annual Computer Security Applications Conference, pp. 119-128, December 2003.

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

ประวัตินักวิจัย

ชื่อ-สกุล นางสาวกนกวรรณ กันยะมี
Miss Kanokwan Kanyamee
วันเกิด 16 เมษายน พ.ศ. 2521
ที่อยู่ 54 หมู่ 9 ต.ผาสิงห์ อ.เมือง จ.น่าน
อีเมล์ kanokwan@uru.ac.th

ประวัติการศึกษา

2555 ปร.ด. (เทคโนโลยีสารสนเทศ) สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
2546 วท.ม. (เทคโนโลยีสารสนเทศ) มหาวิทยาลัยนเรศวร
2542 วท.บ. (วิทยาการคอมพิวเตอร์) สถาบันราชภัฏอุตรดิตถ์

การทำงานปัจจุบัน

อาจารย์สังกัด คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏอุตรดิตถ์
โทรศัพท์ (055) 411-096 ต่อ 1326