การสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆ ตามข้อตกลงคีย์กลุ่ม Diffie-Hellman

ปริญญา นาโท

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
คณะสถิติประยุกต์
สถาบันบัณฑิตพัฒนบริหารศาสตร์
2557

การสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆ ตามข้อตกลงคีย์กลุ่ม Diffie-Hellman

ปริญญา นาโท

คณะสถิติประยุกต์

ผู้ช่วยศาสตราจารย์.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(ดร.ปราโมทย์ กั่วเจริญ)

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)

รองศาสตราจารย์.....ประธานกรรมการ

(ดร.สุรพงค์ เอื้อวัฒนามงคล)

ผู้ช่วยศาสตราจารย์.....กรรมการ

(ดร.ปราโมทย์ กั่วเจริญ)

รองศาสตราจารย์.....กรรมการ

(ดร. โอม ศรนิล)

รองศาสตราจารย์.....กรรมการ

(ดร.ดำรัส วงศ์สว่าง)

อาจารย์.....คณบดี

(ดร.ศิวิกา ดุษฎีโหนด)

พฤษภาคม 2558

บทคัดย่อ

ชื่อวิทยานิพนธ์	การสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆตามข้อตกลงคีย์กลุ่ม Diffie-Hellman
ชื่อผู้เขียน	นายปริญญา นาโท
ชื่อปริญญา	วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
ปีการศึกษา	2557

วิทยานิพนธ์นี้ มีวัตถุประสงค์เพื่อนำเสนอวิธีการสร้างความปลอดภัยของไฟล์ข้อมูลในการประมวลผลแบบกลุ่มเมฆ โดยไฟล์ข้อมูลจะถูกเข้ารหัสก่อนการอัพโหลด และมีคีย์สำหรับเข้ารหัสและถอดรหัสของแต่ละไฟล์ สมาชิกสามารถเข้าร่วมกลุ่มหรือออกจากกลุ่มสมาชิกได้ตลอดเวลา ในการรักษาความปลอดภัยของกลุ่มสมาชิกจะใช้วิธีการแลกเปลี่ยนคีย์กลุ่มตามข้อตกลง Diffie-Hellman นอกจากนี้ได้นำแนวคิดการนำโครงสร้างต้นไม้มาประยุกต์เพื่อช่วยเพิ่มประสิทธิภาพในการคำนวณหาคีย์กลุ่ม สมาชิกภายในกลุ่มจะสามารถเปิดข้อมูลที่เข้ารหัสไว้ได้โดยใช้คีย์กลุ่มซึ่งสมาชิกสามารถคำนวณหาคีย์กลุ่มได้ตามโครงสร้างต้นไม้

ABSTRACT

Title of Thesis	Cloud Storage Security Based on Diffie-Hellman Group Key Agreement
Author	Mr.Parinya Natho
Degree	Master of Science (Computer Science)
Year	2014

In this thesis, we present a cryptographic file system designed for cloud based data storage. Files are encrypted before they are uploaded to the cloud storage providers. We allow file sharing within a group of users by using an underlying group key agreement protocol. The idea is to divide the group into subgroups; each maintains its subgroup keys using Group Diffie-Hellman (GDH) protocol and links with other subgroups in a tree structure using Tree-Based Group Diffie-Hellman (TGDH) protocol. A key feature is that it handles changes in group membership and modifications of files in an extremely efficient manner.

กิตติกรรมประกาศ

ในการจัดทำวิทยานิพนธ์ฉบับนี้สามารถสำเร็จลุล่วงไปได้ผู้เขียนขอกราบขอบพระคุณอาจารย์ที่ปรึกษาวิทยานิพนธ์ คือ ผู้ช่วยศาสตราจารย์ ดร.ปราโมทย์ กั่วเจริญ ที่ได้ให้คำแนะนำปรึกษาแนวทางในการดำเนินการทำวิจัย รวบรวม และตรวจสอบข้อบกพร่องในระหว่างการจัดทำทุกขั้นตอน

ขอขอบคุณคณาจารย์ทุกท่านของคณะสถิติประยุกต์ ที่ได้ถ่ายทอดประสาทวิชาความรู้ให้แก่ผู้ศึกษา และขอขอบคุณเจ้าหน้าที่ทุกท่านที่ได้ให้ความช่วยเหลือประสานงานอำนวยความสะดวกเป็นอย่างดีด้วยอัธยาศัยที่เป็นกันเอง

ท้ายที่สุดนี้ หากวิทยานิพนธ์ฉบับนี้จะมีประโยชน์อันใด ผู้เขียนขอมอบความดีทั้งหมดนี้ให้แก่นายบุญเพ็ง และนางไกรษร นาโท ผู้ซึ่งเป็นบิดาและมารดาของผู้เขียน เป็นผู้ให้ความรักและความปรารถนาดีและขอขอบคุณพี่น้องและเพื่อน ๆ ที่คอยให้กำลังใจตลอดมา

ปริญญา นาโท

พฤษภาคม 2558

สารบัญ

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

บทที่ 1

บทนำ

1.1 การประมวลผลแบบกลุ่มเมฆ

ความก้าวหน้าของเทคโนโลยีอินเทอร์เน็ตในปัจจุบันได้ทำให้โลกมีขนาดเล็กลงมาก เนื่องจากการสื่อสารที่มีความรวดเร็วขึ้น โดยเมื่อไม่นานมานี้หนึ่งในเทคโนโลยีที่ได้รับความสนใจมากที่สุดคือเทคโนโลยีการประมวลผลแบบกลุ่มเมฆ หรือที่รู้จักกันดีในชื่อ คลาวด์คอมพิวติ้ง (Cloud Computing)

คลาวด์คอมพิวติ้ง คือรูปแบบการประมวลผลที่ให้บริการทรัพยากรผ่านระบบเครือข่าย เพื่อให้สามารถเข้าถึงข้อมูลได้ทุกที่ทุกเวลาแก่ผู้ใช้บริการ คลาวด์คอมพิวติ้งบริหารจัดการทรัพยากรแบบคลัสเตอร์ (Cluster) และการประมวลผลแบบกริด (Grid) ผ่านเครื่องเสมือน (Virtualization) ที่ทำงานบนเครื่องให้บริการที่มีความยืดหยุ่นและความพร้อมใช้งานสูง (High Availability) ซึ่งในการคิดค่าบริการจะคิดตามการใช้งานตามจริง (Pay Per Use) ซึ่งอยู่ภายใต้การทำข้อตกลงทำสัญญาระหว่างกัน (Service Level Agreements หรือ SLAs) โดยที่ผู้ใช้บริการสามารถปรับเพิ่มหรือลดขนาดจำนวนของทรัพยากรให้มีความเหมาะสมกับความต้องการของผู้ใช้บริการ คลาวด์คอมพิวติ้งทำให้ผู้ที่ใช้บริการไม่มีความจำเป็นที่จะต้องทราบถึงกระบวนการทำงานที่อยู่เบื้องหลัง ซึ่งในปัจจุบันการทำธุรกรรมต่าง ๆ ของธุรกิจ ล้วนแล้วแต่ต้องการใช้งานระบบที่มีประสิทธิภาพและมีความยืดหยุ่นสูง ซึ่งไม่จำเป็นที่ผู้ใช้งานจำเป็นจะต้องติดตั้งโปรแกรมไว้ภายในเครื่องของตัวเอง

เทคโนโลยีดังกล่าวมีความเกี่ยวข้องกับการทำงานในลักษณะการทำงานเป็นแบบกลุ่มที่มีการเคลื่อนไหว (กลุ่มที่มีการเคลื่อนไหวของสมาชิกในการเข้าและออกจากกลุ่มที่เกิดขึ้นได้แบบตลอดเวลา) เพราะเนื่องจากระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันส่วนใหญ่จะเป็นระบบเครือข่ายแบบเปิด

ในการใช้งานระบบคลาวด์คอมพิวติ้ง นั้นจะมีผู้ที่คอยให้บริการเรียกว่า Cloud Providers ซึ่งทำหน้าที่เป็นผู้ให้บริการทรัพยากรต่าง ๆ บนคลาวด์คอมพิวติ้งซึ่งจะมีรูปแบบการให้บริการที่หลากหลาย เช่น การบริการโครงสร้างขั้นพื้นฐาน (IaaS หรือ Infrastructure as a Service) บริการแพลตฟอร์ม (PaaS หรือ Platform as a Service) และบริการซอฟแวร์ (SaaS หรือ Software as a Service) เพื่อให้ผู้ใช้บริการได้เลือกใช้บริการตามความเหมาะสมและตามความต้องการ โดยที่คลาวด์คอมพิวติ้งมีหลายประเภท เช่น คลาวด์สาธารณะ (Public Cloud) คลาวด์ส่วนตัว (Private Cloud) และคลาวด์แบบรวม (Hybrid Cloud)

ปัญหาที่สำคัญในการใช้บริการผู้ให้บริการ Cloud Providers คือปัญหาเกี่ยวกับความมั่นใจในการส่งข้อมูลผ่านเครือข่ายได้อย่างปลอดภัย ตั้งแต่กระบวนการขั้นตอนของการส่งข้อมูล การประมวลผลข้อมูล ความมั่นใจในการเก็บรักษาผลลัพธ์หรือแม้กระทั่งความปลอดภัยของข้อมูลที่เก็บไว้ใน Cloud Providers แม้ว่าจะได้รับการประกันจาก Cloud Providers ยิ่งถ้าข้อมูลที่ถูกเข้ารหัสไว้และกุญแจที่ใช้ในการถอดรหัสข้อมูลถูกจัดเก็บไว้กับผู้ให้บริการนั่นหมายความว่าผู้ให้บริการหรือผู้ไม่ประสงค์ดีสามารถที่จะล่วงรู้กุญแจที่ใช้ในการถอดรหัสข้อมูลได้เช่นเดียวกัน ทำให้ข้อมูลหรือกุญแจที่จัดเก็บกับผู้ให้บริการไม่มีความปลอดภัย

ดังนั้นการติดต่อสื่อสารระหว่างสมาชิกภายในกลุ่มควรจะมีระบบการรักษาความปลอดภัยและยังคงไว้ซึ่งประสิทธิภาพโดยรวมของระบบไว้ โดยจะต้องคำนึงถึงความปลอดภัย และความมีประสิทธิภาพในการจัดการข้อตกลงร่วมกันของรหัสคีย์ลับ มีการตรวจสอบและรับรองตัวบุคคลที่รัดกุม พร้อมกันนั้นควรมีการจัดเตรียมเพื่อรองรับสภาวะการเปลี่ยนแปลงของสมาชิกที่สามารถเข้าและออกจากกลุ่มได้ตามต้องการ ในขณะเดียวกันข้อมูลที่ทำการแบ่งบันให้กับสมาชิกภายในกลุ่มจะต้องมีความถูกต้องและปลอดภัย

การเข้ารหัสลับแบบกลุ่ม เป็นการส่งข้อมูลจากผู้ส่งไปยังกลุ่มสมาชิกผ่านการเข้ารหัสลับเพื่อให้สามารถถอดรหัสและรับทราบข้อมูลที่ส่งด้วยคีย์ส่วนตัวของแต่ละสมาชิกซึ่งในการเข้ารหัสลับแบบกลุ่มนี้จะทำให้บุคคลที่ไม่ใช่สมาชิกภายในกลุ่มไม่สามารถถอดรหัสเพื่อทราบข้อมูลได้

การวิจัยของการเข้ารหัสลับแบบกลุ่มมีการดำเนินการอย่างแพร่หลาย เพราะสามารถนำมาประยุกต์ใช้ในงานด้านต่าง ๆ ยกตัวอย่างเช่น การประชุมทางไกล การเรียนรู้ผ่านทางสื่ออิเล็กทรอนิกส์หรือแม้กระทั่งการสื่อสารกันผ่านเครือข่ายอินเตอร์เน็ตทั้งระหว่างบุคคลภายในและบุคคลภายนอกกลุ่มสมาชิก

ปัญหาที่สำคัญในการส่งข้อมูลแบบกลุ่มคือ มีปริมาณจำนวนของข้อมูลที่ต้องการส่งระหว่างสมาชิกไปเป็นจำนวนมากทำให้ต้องเสียเวลาในการคำนวณการเข้ารหัสและถอดรหัสส่งผลให้เกิดภาระหนักเป็นอย่างมากสำหรับคีย์เซิร์ฟเวอร์

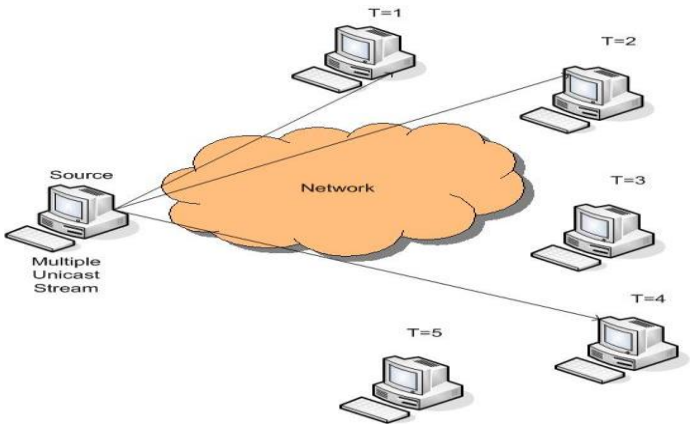
ในบทนี้จะแนะนำแนวคิดของการสื่อสารกลุ่มและแนวคิดของการรักษาความปลอดภัยสำหรับการสื่อสารกลุ่มเมื่อมีสมาชิกเข้าร่วมกลุ่มและออกจากกลุ่มได้ตลอดเวลา

1.2 การสื่อสารกลุ่ม

ในปัจจุบันการสื่อสารของระบบคอมพิวเตอร์สามารถทำได้โดยวิธีการสื่อสารได้กลุ่ม กล่าวคือ ผู้ส่งหนึ่งคนส่งไปยังหนึ่งผู้รับหรือหลายผู้รับภายในกลุ่ม หรือหลายผู้ส่งต้องการส่งข้อมูลไปยังหลายผู้รับภายในกลุ่ม โดยที่ผู้ที่ไม่ใช่สมาชิกของกลุ่มไม่สามารถเข้าถึงข้อมูลเหล่านั้นได้ ซึ่งรูปแบบของการสื่อสารกลุ่มแบ่งออกได้เป็น 3 ประเภทดังนี้

1.2.1 Unicast Communication

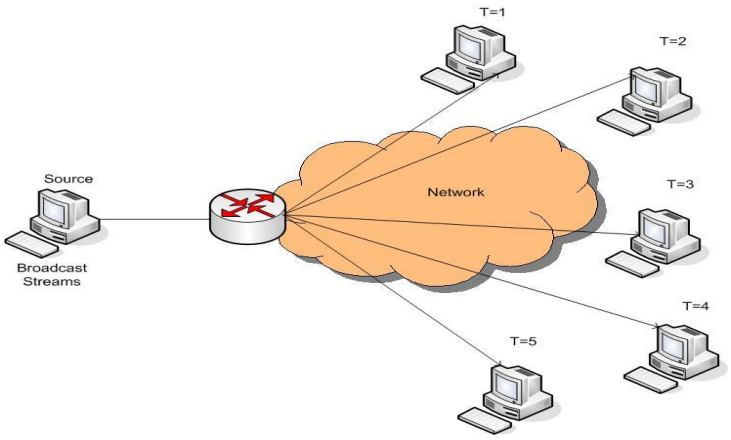
ในการสื่อสารแบบ Unicast จะเป็นการสื่อสารระหว่างผู้ส่งรายเดียวกับผู้รับรายเดียวบนเครือข่ายของตนเองและข้อความหนึ่งสามารถส่งระหว่างผู้รับและผู้ส่งได้ในช่วงเวลาหนึ่ง แสดงได้ดังภาพที่ 1.1



ภาพที่ 1.1 Unicast Communication

1.2.2 Broadcast Communication

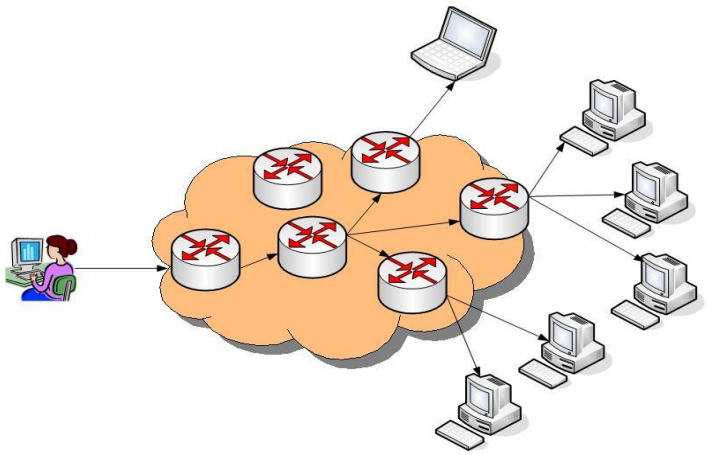
การสื่อสารแบบ Broadcast เป็นการส่งข้อมูลจากโหนดต้นทางหนึ่งไปยังโหนดปลายทางทุกโหนดที่ติดต่อสื่อสารกันในลักษณะของการแพร่กระจายข้อมูลแบบหนึ่งต่อทั้งหมด ซึ่งการแพร่ข้อมูลแบบส่งไปยังโหนดทุกโหนดนั้น จะต้องมีการประมวลผลข้อมูลที่โหนดปลายทางเหล่านั้น โหนดที่ไม่ต้องการรับข้อมูลนั้นจะทิ้งข้อมูลที่ได้รับมา วิธีการสื่อสารแบบนี้ทำให้โหนดทุกโหนดต้องประมวลผล และทำให้ปริมาณข้อมูลที่ส่งอยู่ในเครือข่ายจำนวนมากโดยเปล่าประโยชน์ การสื่อสารแบบ Broadcast นี้ปัจจุบันมีการใช้งานอยู่เฉพาะใน LAN เท่านั้น เนื่องจากเป็นการยากในการหาเส้นทางเพื่อ Broadcast ข้อมูลในระบบเครือข่าย WAN ดังภาพที่ 1.2



ภาพที่ 1.2 Broadcast Communication

1.2.3 Multicast Communication

ในการสื่อสารแบบ Multicast เป็นการส่งข้อมูลจากโหนดต้นทางหนึ่งไปยังกลุ่มของโหนดปลายทางเฉพาะกลุ่มที่มีการกำหนดแบบหนึ่งต่อกลุ่มเฉพาะ หรือ One-to-N การส่งข้อมูลจะส่งไปยังโหนดในกลุ่มเฉพาะที่ต้องการรับข้อมูลเท่านั้น โดยข้อมูลจะถูกส่งจากต้นทางเพียงแพ็กเก็ตเดียว และจะถูกส่งต่อโดยตัวค้นหาเส้นทางจนถึงเครื่องในกลุ่มเฉพาะที่กำหนดโดยจะทำการคัดลอกแพ็กเก็ตข้อมูลแล้วส่งให้แก่โหนดปลายทางทุกโหนดที่ต้องการ ดังภาพที่ 1.3



ภาพที่ 1.3 Multicast Communication

1.3 การรักษาความปลอดภัยการสื่อสารกลุ่ม

เมื่อสมาชิกคนหนึ่งต้องการที่จะสื่อสารกับสมาชิกคนอื่น ๆ ในกลุ่ม การส่งข้อความจะต้องถูกปกปิดไม่ให้ผู้ที่ไม่ใช่สมาชิกรับทราบข้อมูล ดังนั้นการเข้ารหัสเป็นสิ่งที่จำเป็นสำหรับวัตถุประสงค์นี้ ในการเข้ารหัสและถอดรหัสข้อความผ่านการสื่อสารนั้นสมาชิกทุกคนต้องถือคีย์ลับตัวเดียวกันซึ่งคีย์ลับนี้ เรียกว่า คีย์กลุ่ม

อย่างไรก็ตามการจัดการและการรักษาความปลอดภัยของคีย์กลุ่มมีความซับซ้อนเช่นการทำให้คีย์กลุ่มที่รู้ได้เฉพาะภายในสมาชิกของกลุ่ม กลไกการทำข้อตกลงสำหรับสมาชิกใหม่ วิธีการกระจายคีย์สำหรับกลุ่ม การเปลี่ยนแปลงคีย์กลุ่มเมื่อมีสมาชิกใหม่เข้าร่วมกลุ่มหรือมีสมาชิกออกจากกลุ่ม เพื่อป้องกันไม่ให้ข้อมูลรั่วไหลออกจากกลุ่มเป็นต้น โดยทั่วไปแล้วระบบที่มีความปลอดภัยสำหรับการสื่อสารกลุ่มมีลักษณะดังต่อไปนี้

สมาชิกทั้งหมดในปัจจุบันใช้คีย์กลุ่มเดียวกันในการสื่อสารกับแต่ละสมาชิกอื่นโดยผ่านการเข้ารหัสคีย์ลับ

มีคีย์เซิร์ฟเวอร์หนึ่งเป็นผู้รับผิดชอบในการสร้างและการกระจายกลุ่มผู้ใช้ใหม่และเป็นคีย์สำหรับแต่ละกลุ่มข้อมูลสำหรับการเปลี่ยนค่าคีย์กลุ่มเก่า

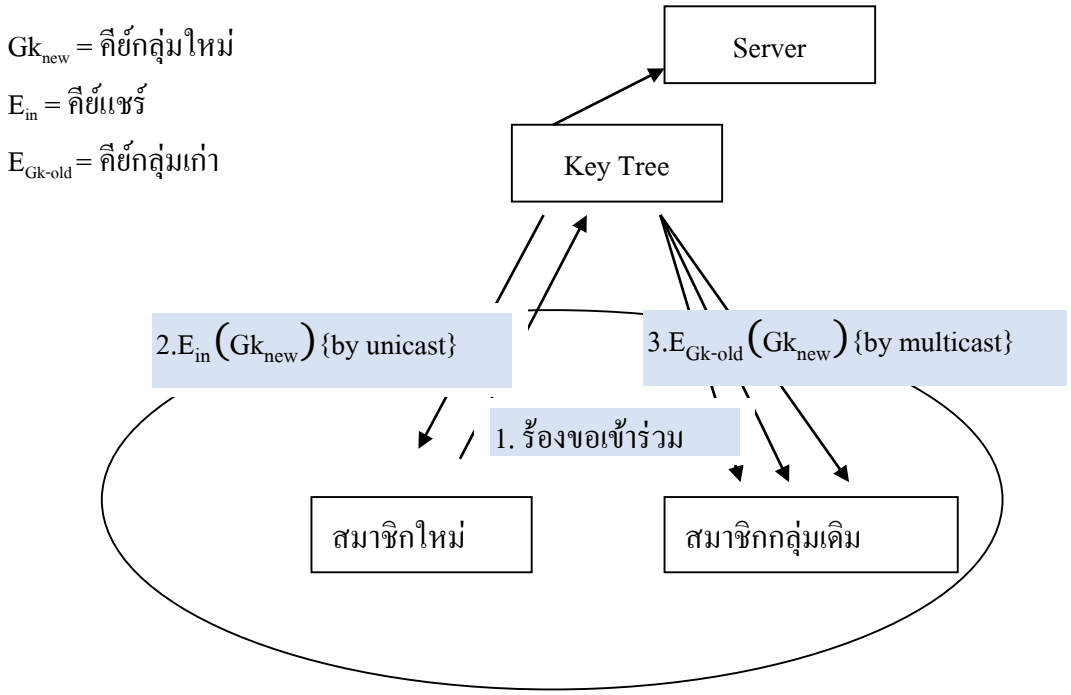
สมาชิกแต่ละคนมีคีย์ส่วนตัวที่ใช้ร่วมกันกับคีย์เซิร์ฟเวอร์

สมาชิกสามารถเข้าร่วมหรือออกจากกลุ่มได้ตลอดเวลา

1.3.1 การเข้าร่วมกลุ่ม

ในกรณีเมื่อมีสมาชิกใหม่ต้องการเข้าร่วมกลุ่ม คีย์กลุ่มจำเป็นจะต้องมีการเปลี่ยนแปลงคีย์กลุ่มเพื่อไม่ให้สมาชิกใหม่เข้าถึงการสนทนาที่ผ่านมาในอดีตของกลุ่ม ซึ่งถูกเข้ารหัสด้วยคีย์กลุ่มเดิม เรียกกระบวนการนี้ว่า การควบคุมการเข้าถึงย้อนกลับ

สำหรับการกระจายคีย์ใหม่ให้ไปยังสมาชิกที่มีอยู่ คีย์ที่ใช้ร่วมกันระหว่างสมาชิกใหม่ถูกตั้งค่าจากคีย์ทรี ซึ่งก็คือคีย์แชร์โดยคีย์ทรีที่เก็บในเซิร์ฟเวอร์จะใช้คีย์แชร์ที่ใช้ร่วมกันสำหรับการเข้ารหัสคีย์กลุ่มใหม่ก่อนที่จะส่งไปให้สมาชิกใหม่ผ่านการสื่อสารแบบ Unicast และสมาชิกที่มีอยู่ภายในกลุ่มจะได้รับคีย์กลุ่มใหม่ที่ถูกเข้ารหัสด้วยคีย์กลุ่มเก่าผ่านการสื่อสารแบบ Multicast ดังภาพที่ 1.4

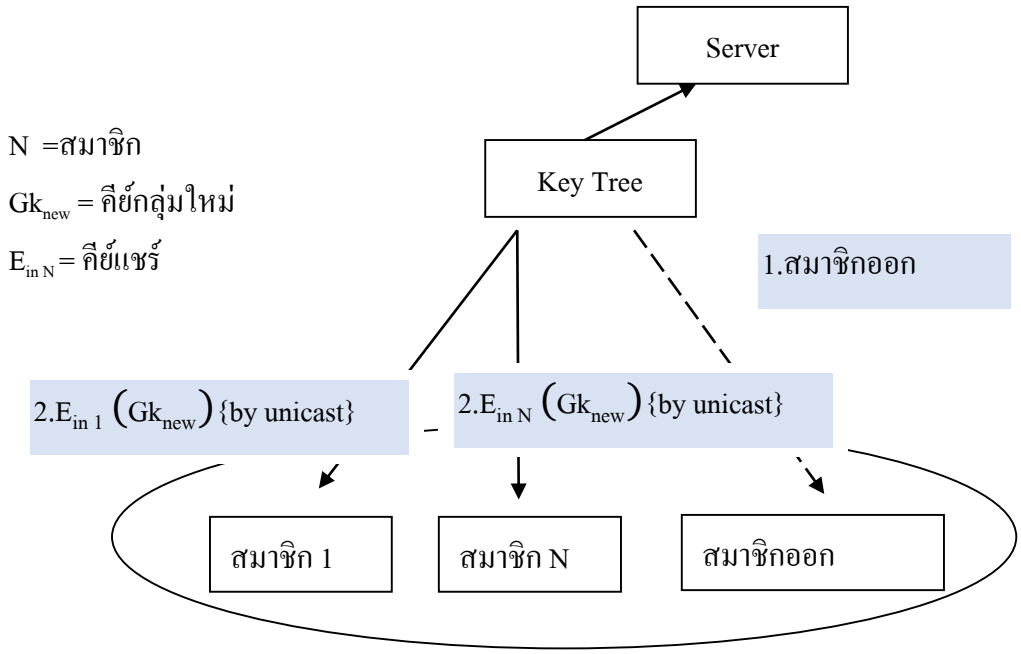


ภาพที่ 1.4 การจัดการคีย์กลุ่มเมื่อสมาชิกเข้าร่วมกลุ่ม

1.3.2 การออกจากกลุ่ม

เมื่อสมาชิกออกจากกลุ่ม คีย์กลุ่มจะต้องเปลี่ยนแปลงใหม่เพื่อป้องกันไม่ให้สมาชิกที่ออกจากกลุ่มไปแล้วสามารถเข้าถึงข้อมูลหรือการสนทนาของกลุ่มได้ในอนาคต เรียกว่า การควบคุมการเข้าถึงไปข้างหน้า

ในการกระจายคีย์ใหม่ไปยังสมาชิกที่เหลือของกลุ่ม คีย์ทรีจะเข้ารหัสคีย์ใหม่ถ้าคีย์แชร์ของแต่ละสมาชิกและส่งไปยังสมาชิกแต่ละคนผ่านการสื่อสารแบบ Unicast คีย์ทรีจะไม่ใช้คีย์กลุ่มเก่าในการเข้ารหัสใหม่ตั้งแต่รู้ว่ามีสมาชิกออกจากกลุ่ม ดังภาพที่ 1.5



ภาพที่ 1.5 การจัดการคีย์กลุ่มเมื่อสมาชิกออกจากกลุ่ม

1.4 ปัญหาและแรงจูงใจ

ปัญหาหลักในการจัดเก็บข้อมูลไว้ที่ผู้ให้บริการ Cloud Providers คือความมั่นคงปลอดภัยของข้อมูลที่จัดเก็บไว้ ซึ่งผู้ใช้บริการจะมีความมั่นใจได้อย่างไรว่าเมื่อข้อมูลที่ถูกส่งไปเก็บแล้วผู้ให้บริการจะไม่แอบเก็บข้อมูลเพื่อนำไปใช้ประโยชน์ส่วนตนหรือเปิดเผยข้อมูลแก่บุคคลอื่น ถึงแม้ว่าจะได้รับการประกันจากผู้ให้บริการแล้วก็ตาม แม้ว่าข้อมูลเหล่านั้นจะถูกเข้ารหัสไว้และกุญแจที่ใช้ในการถอดรหัสถูกจัดเก็บไว้กับผู้ให้บริการถ้าผู้ไม่ประสงค์ดีสามารถล่วงรู้กุญแจนั้นได้ก็สามารถใช้ในการถอดรหัสข้อมูลได้เช่นกัน

จากงานวิจัยที่ผ่านมาได้นำเสนอเกี่ยวกับแนวทางการจัดการคีย์กลุ่มและการจัดเก็บข้อมูลในการประมวลผลแบบกลุ่มเมฆ จะสังเกตเห็นได้ว่าวิธีการบริหารจัดการคีย์กลุ่มที่ดีควรมีคุณสมบัติสามประการคือ ประการที่หนึ่งคือ คีย์กลุ่มควรจะถูกสร้างในลักษณะที่สมาชิกทุกคนสามารถเข้าร่วมในกิจกรรมที่สำคัญนี้และไม่มีสมาชิกใดเพียงคนเดียวควบคุมการสร้างคีย์กลุ่มส่งผลให้ไม่มีจุดศูนย์กลางของความล้มเหลวและมีความยืดหยุ่นสูงเมื่อจำนวนของสมาชิกมีเพิ่มขึ้น ประการที่สองการติดต่อสื่อสารระหว่างสมาชิกในระบบต้องอยู่ภายใต้การรักษาความปลอดภัยด้วคคีย์กลุ่ม ประการสุดท้ายคือ คีย์ที่สมาชิกแต่ละคนควรจะเก็บรักษาไว้ควรมีจำนวนน้อยที่สุดเท่าที่จะเป็นไปได้เพื่อลดความเสี่ยงที่คีย์อาจถูกเปิดเผย

งานวิจัยที่นำเสนอนี้จึงมีจุดประสงค์ที่จะทำให้กระบวนการสร้างคีย์กลุ่มมีลักษณะสมาชิกทุกคนมีส่วนร่วมในกระบวนการหนึ่งของคีย์กลุ่ม นอกจากนี้ ขบวนการสร้างคีย์กลุ่มจะใช้อัลกอริทึม Diffie-Hellman เนื่องจากเป็นวิธีที่ช่วยให้การแลกเปลี่ยนคีย์ที่มีความปลอดภัยทั้งสองฝ่าย อีกทั้งข้อมูลที่สื่อสารกันระหว่างสมาชิกภายในกลุ่มจะถูกเข้ารหัสด้วยวิธีการเข้ารหัสแบบขั้นสูง (AES) ในโหมด CBC เพื่อทำให้มีความปลอดภัยในการสื่อสารเพิ่มขึ้นโดยข้อมูลที่ถูกเข้ารหัสจะมีคีย์ของตนเองใช้ในการถอดรหัสข้อมูล ซึ่งคีย์เหล่านี้จะถูกเก็บในไฟล์ที่ผู้ที่จะสามารถเปิดดูคีย์ในไฟล์นี้จะต้องอยู่ภายในกลุ่มสื่อสารเท่านั้น

นอกจากนี้เพื่อลดเวลาในการประมวลผลจึงมีการใช้โครงสร้างต้นไม้มาช่วยในขบวนการคำนวณเพื่อสร้างคีย์ ซึ่งวิธีการนี้จะช่วยให้การทำงานมีความยืดหยุ่นสูงต่อการเปลี่ยนแปลงของสมาชิกในกลุ่ม

1.5 วัตถุประสงค์ของงานวิจัย

1) เพื่อนำเสนอแนวทางการคำนวณคีย์กลุ่มตามข้อตกลง Diffie-Hellman โดยใช้โครงสร้างแบบต้นไม้

2) เพื่อนำเสนอวิธีการเข้ารหัสระบบไฟล์ข้อมูลในการประมวลผลแบบกลุ่มเมฆโดยใช้การเข้ารหัสแบบสมมาตรด้วยวิธีการเข้ารหัสลับแบบขั้นสูงในการสื่อสารกลุ่ม

1.6 ทฤษฎีที่ใช้ในการวิจัย

ในการวิจัยครั้งนี้มีทฤษฎีที่นำมาประยุกต์ใช้ดังต่อไปนี้

1) ทฤษฎีเกี่ยวกับ การรักษาความปลอดภัยในเครือข่าย

2) ทฤษฎีเกี่ยวกับ วิทยาการเข้ารหัสลับ

3) ทฤษฎีเกี่ยวกับ การเข้ารหัสแบบสมมาตรด้วยวิธีการเข้ารหัสลับแบบขั้นสูง Advanced Encryption Standard (AES)

4) ทฤษฎีเกี่ยวกับ โปรโตคอลข้อตกลงคีย์กลุ่มตามข้อตกลง Diffie-Hellman โดยใช้โครงสร้างแบบต้นไม้ Tree-based Group Key Agreement Protocol (TGDH)

1.7 วิธีดำเนินการวิจัย

1) ศึกษางานวิจัยที่เกี่ยวข้องเพื่อเปรียบเทียบข้อดีและข้อเสียพร้อมนำข้อดีของงานวิจัยเหล่านั้นมาประยุกต์ใช้ในงานวิจัย

2) ศึกษาการจัดการคีย์กลุ่มตามข้อตกลง Diffie-Hellman โดยใช้โครงสร้างต้นไม้เพื่อใช้ในการกระจายคีย์ให้กับสมาชิกในกลุ่ม

3) ศึกษาทฤษฎีการเข้ารหัสลับและการถอดรหัสข้อมูลด้วยการเข้ารหัสแบบสมมาตรด้วยวิธีการเข้ารหัสลับแบบขั้นสูง

4) ออกแบบการจัดการคีย์กลุ่มตามข้อตกลง Diffie-Hellman โดยใช้โครงสร้างแบบต้นไม้และการเข้ารหัสและถอดรหัสข้อมูลแบบสมมาตรที่ต้องการส่งด้วยวิธีการเข้ารหัสลับแบบขั้นสูง

5) สรุปผลการวิจัยและข้อเสนอแนะ

1.8 ประโยชน์ที่คาดว่าจะได้รับ

1) สามารถสร้างความปลอดภัยของข้อมูลในการประมวลผลแบบกลุ่มเมฆด้วยวิธีการเข้ารหัสลับแบบสมมาตรที่ใช้การเข้ารหัสแบบขั้นสูงได้และวิธีการจัดการคีย์กลุ่มตามข้อตกลง Diffie-Hellman สำหรับการสื่อสารและส่งข้อมูลแบบกลุ่มโดยใช้โครงสร้างแบบต้นไม้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงาน

2) สามารถนำเอาวิธีการที่ได้นำเสนอในงานวิจัยนี้ไปประยุกต์ใช้เพื่อพัฒนาโปรแกรมสำหรับอุปกรณ์เคลื่อนที่

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 การรักษาความปลอดภัยของเครือข่าย

การรักษาความปลอดภัยของเครือข่ายมีสิ่งที่เกี่ยวข้องและต้องคำนึงถึงสามด้านด้วยกันคือ การบริการรักษาความปลอดภัย การโจมตีที่อาจเกิดขึ้นได้และกลไกการรักษาความปลอดภัย

ด้านการบริการรักษาความปลอดภัยหมายถึงการทำงานที่จำเป็นต้องจัดให้มีเพื่อให้เกิดสภาพแวดล้อมเครือข่ายที่มีความปลอดภัย ในขณะที่การโจมตีที่อาจเกิดขึ้นครอบคลุมวิธีการที่จะนำมาใช้เพื่อทำลายการบริการรักษาความปลอดภัยเหล่านี้ สุดท้ายคือกลไกการรักษาความปลอดภัยคือส่วนประกอบพื้นฐานที่ใช้ในการให้บริการด้านการรักษาความปลอดภัย

2.1.1 การบริการรักษาความปลอดภัย

การให้บริการด้านการรักษาความปลอดภัยอาจต้องใช้บางส่วนหรือทั้งหมดของการให้บริการต่อไปนี้

2.1.1.1 ความลับของข้อมูลเพื่อให้แน่ใจว่าข้อมูลที่ถูกส่งออกไปสามารถเข้าถึงได้โดยผู้รับเท่านั้น

2.1.1.2 การพิสูจน์ตัวตนของข้อมูลเพื่อให้บุคคลที่จะสื่อสารมั่นใจในตัวตนของคนอื่น ๆ ได้

2.1.1.3 ความบูรณภาพเพื่อให้แน่ใจว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลงในระหว่างการส่งข้อมูล

2.1.1.4 การตรวจสอบที่ทำให้บุคคลผู้ส่งหรือรับข้อมูลไม่สามารถปฏิเสธความรับผิดชอบได้

2.1.1.5 ความพร้อมใช้งานในการตรวจสอบเพื่อให้แน่ใจว่ามีการบริการเครือข่ายให้บุคคลใช้เมื่อจำเป็น

2.1.2 การโจมตีการรักษาความปลอดภัย

การโจมตีการรักษาความปลอดภัยสามารถจำแนกได้เป็นสองประเภทดังต่อไปนี้

2.1.2.1 การโจมตีแบบ passive

ผู้โจมตีลักลอบเข้าใช้หรือดักฟังการรับส่งข้อมูลในเครือข่ายเท่านั้น เป็นรูปแบบที่ง่ายที่สุดของการโจมตีและสามารถดำเนินการได้โดยไม่ยากในเครือข่ายที่มีการใช้งานเป็นจำนวนมาก ยกตัวอย่างเช่น เครือข่าย Broadcast Ethernet และเครือข่ายไร้สาย

2.1.2.2 การโจมตีแบบใช้งานอยู่

ผู้โจมตีไม่เพียงสามารถที่จะดักฟังเพื่อการส่งเท่านั้นแต่ยังสามารถเปลี่ยนแปลงหรือขัดขวางการส่งนั้นได้

2.1.2.3 การดักฟัง

การโจมตีแบบนี้จะใช้การเรียนรู้จากข้อมูลที่ส่งออกโดยเป็นการโจมตีแบบpassive ซึ่งจะดำเนินการได้อย่างง่ายในสภาพแวดล้อมการเชื่อมต่อเครือข่ายขนาดใหญ่ การโจมตีนี้สามารถป้องกันได้โดยการเข้ารหัสข้อมูลก่อนที่ส่งออกไป

2.1.2.4 การวิเคราะห์การจราจร

เป้าหมายหลักของการโจมตีนี้ไม่ต้องการดักฟังหรือทราบข้อมูลที่ถูกส่ง แต่ต้องการทราบลักษณะของการส่งข้อมูลเช่น จำนวนของข้อมูลที่ส่ง รหัสประจำตัวของโหนดสื่อสาร เป็นต้น ข้อมูลเหล่านี้อาจทำให้ผู้โจมตีได้ข้อสรุปที่สำคัญ เช่น บทบาทหน้าที่ของโหนด การติดต่อสื่อสาร หรือตำแหน่ง การโจมตีประเภทนี้เป็นเรื่องยากมากที่จะป้องกัน

2.1.2.5 การเลียนแบบ

ผู้โจมตีจะใช้ตัวตนของโหนดอื่นในการเข้าถึงทรัพยากรหรือข้อมูลที่ไม่ได้รับอนุญาต การโจมตีนี้มักจะถูกกระทำก่อนการดักฟัง โดยการปลอมตัวเป็นโหนดที่ถูกต้อง เพื่อให้เข้าถึงคีย์เข้ารหัสที่ใช้ในการป้องกันข้อมูลที่ส่งออก เมื่อทราบคีย์แล้วผู้โจมตีสามารถดักฟังข้อมูลได้อย่างอิสระ

2.1.2.6 การเปลี่ยนแปลงการโจมตี

การโจมตีนี้จะปรับเปลี่ยนข้อมูลในระหว่างการส่งข้อมูล ตัวอย่างเช่น เมื่อการทำธุรกรรมทางการเงินผู้โจมตีอาจมีการปรับเปลี่ยนค่าข้อมูลที่ถูกส่งไปในการทำธุรกรรมทางการเงิน

2.1.2.7 การแทรก

การโจมตีแบบนี้เป็นการแทรกข้อมูลใหม่ในข้อมูลที่ถูกส่งออกไป การโจมตีแบบนี้เป็นต้องอาศัยกับการโจมตีด้วยการเลียนแบบ

2.1.2.8 การทำซ้ำ

ผู้โจมตีจะเก็บข้อมูลของโหนดที่ถูกส่งออกแล้วทำการเก็บไว้สักระยะหนึ่งแล้วค่อยส่งต่อ

2.1.2.9 การปฏิเสธการให้บริการ

การโจมตีแบบนี้มีวัตถุประสงค์ที่จะขัดขวางการเข้าใช้ทรัพยากรบางอย่าง ทรัพยากรนี้อาจจะไม่สามารถบริการให้กับบางโหนดหรือเครือข่ายทั้งหมด

2.1.3 กลไกการรักษาความปลอดภัย

การบริการด้านการรักษาความปลอดภัยจะต้องอาศัยเทคนิคการเข้ารหัสลับข้อมูล ส่วนต่อไปนี้จะทำให้เห็นภาพรวมของกลไกการรักษาความปลอดภัย

2.1.3.1 การรักษาความลับ

เป็นวิธีที่จะป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงเนื้อหาของข้อความ การใช้อัลกอริธึมการเข้ารหัสข้อมูลที่มีเพียงผู้ใช้ที่มีรหัสที่ถูกต้องและรู้อัลกอริธึมที่สามารถถอดรหัสได้ การเข้ารหัสสามารถแบ่งออกได้เป็นสองประเภทคือ การเข้ารหัสแบบสมมาตร และการเข้ารหัสแบบอสมมาตร

2.1.3.2 ความสมบูรณ์ของข้อมูล

เป็นวิธีที่จะป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตเปลี่ยนแปลงข้อมูล

2.1.3.3 การไม่ปฏิเสธ

เป็นวิธีที่จะป้องกันการปฏิเสธการเป็นผู้ส่งข้อความและผู้รับจะมั่นใจถึงตัวตนของผู้ส่งข้อความ ตัวอย่างเช่นการใช้ลายมือชื่อดิจิตอลกับข้อความอิเล็กทรอนิกส์

2.1.3.4 ความพร้อมใช้งาน

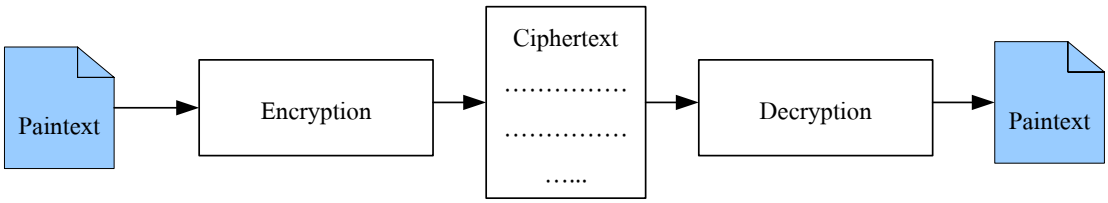
การบริการควรจะพร้อมใช้งานได้ทุกเวลาและจะต้องมีความแข็งแกร่งพอที่จะทนต่อความล้มเหลวของเครือข่ายและต้องทนต่อการโจมตีแบบปฏิเสธการให้บริการ (DOS)

2.1.3.5 การพิสูจน์ตัวตน

การพิสูจน์ตัวตนแบ่งออกเป็นสองประเภทคือ การตรวจสอบตัวตนและตรวจสอบที่มาของข้อมูล ในกรณีแรกฝ่ายหนึ่งฝ่ายใดที่ร่วมในการสื่อสารใด ๆ จะต้องสามารถระบุตัวตนให้กับผู้เข้าร่วมคนอื่น

2.2 วิทยาการเข้ารหัสลับ (Cryptography)

วิทยาการเข้ารหัสลับ (Cryptography) คือ วิทยาศาสตร์แขนงหนึ่งที่ใช้หลักทางคณิตศาสตร์ช่วยในการเข้ารหัสลับและการถอดรหัสลับ ก่อนที่จะทำการส่งหรือจัดเก็บข้อมูล ซึ่งจะทำให้ข้อมูลมีความมั่นคงปลอดภัยมากขึ้น ทั้งนี้เนื่องจากข้อมูลนั้นจะสามารถเปิดอ่านได้โดยบุคคลที่ได้รับอนุญาตเท่านั้น หลักการของการเข้ารหัสลับ (Encryption) คือการแปลงข้อมูลให้อยู่ในรูปของข้อมูลที่ไม่สามารถอ่านได้โดยตรง ข้อมูลที่เข้ารหัสลับไว้จะถูกถอดกลับด้วยการถอดรหัสลับ (Decryption) ดังภาพที่ 2.1

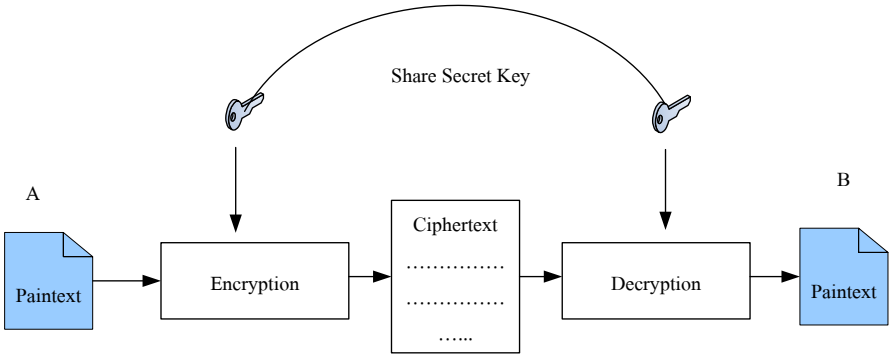


ภาพที่ 2.1 การเข้ารหัสลับและการถอดรหัสลับ

จากภาพที่ 2.1 ข้อมูลที่สามารถอ่านได้เรียกว่า Plaintext ข้อมูลที่เข้ารหัสลับแล้วเรียกว่า Ciphertext และเมื่อทำการถอดรหัสลับแล้วจะได้เป็น Plaintext เหมือนเดิม

2.3 การเข้ารหัสลับสมมาตร (Symmetric Cryptography)

การเข้ารหัสลับแบบสมมาตรคือการเข้ารหัสลับและถอดรหัสลับโดยใช้กุญแจรหัสลับชุดเดียว คือผู้ส่งและผู้รับจะต้องมีกุญแจรหัสลับที่เหมือนกันเพื่อใช้ในการเข้ารหัสลับและถอดรหัสลับ (Share Secret Key) โดยกุญแจลับดังกล่าวจะถูกเก็บเป็นความลับระหว่างผู้รับและผู้ส่งเท่านั้นเพื่อป้องกันไม่ให้ผู้อื่นที่ไม่ได้รับอนุญาตถอดรหัสข้อมูลได้ กระบวนการทำงานเข้ารหัสแบบสมมารถแสดงให้เห็นในภาพที่ 2.2



ภาพที่ 2.2 การเข้ารหัสลับแบบสมมาตร

การเข้ารหัสลับแบบสมมาตรจะต้องคำนึงถึงกระบวนการกระจายคีย์ระหว่างผู้ส่งและผู้รับก่อนทำการส่งข้อความระหว่างกัน การกระจายคีย์จะต้องมีดังต่อไปนี้ ความมั่นคงปลอดภัยเพื่อให้ผู้รับและผู้ส่งทราบคีย์เท่านั้นตามตัวอย่างอัลกอริทึมการเข้ารหัสลับแบบสมมาตรมีดังต่อไปนี้

2.3.1 Data Encryption Standard (DES)

วิธีการเข้ารหัสลับแบบนี้ได้รับการรับรองโดยรัฐบาลสหรัฐอเมริกาในปีค.ศ. 1977 ให้เป็นมาตรฐานการเข้ารหัสลับข้อมูลสำหรับหน่วยงานของรัฐทั้งหมด ในปี 1981 การเข้ารหัสลับแบบนี้ยังถูกกำหนดให้เป็นมาตรฐานการเข้ารหัสลับข้อมูลในระดับนานาชาติตามมาตรฐาน ANSI (American National Standards) อีกด้วย DES เป็นการเข้ารหัสลับแบบบล็อกโดยข้อมูลตั้งต้น (Plaintext) แต่ละบล็อกมีขนาด 64 บิตซึ่งใช้คีย์สาหรับการเข้ารหัสลับที่มีขนาดความยาว 56 บิตซึ่งกุญแจจะถูกสร้างจากความยาวของคีย์ที่มีขนาดเพียง 56 บิตถือได้ว่าสั้นเกินไปสำหรับในปัจจุบัน ผู้บุกรุกอาจใช้วิธีการลองผิดลองถูกเพื่อค้นหาคีย์ที่ถูกต้องสำหรับการถอดรหัสลับได้

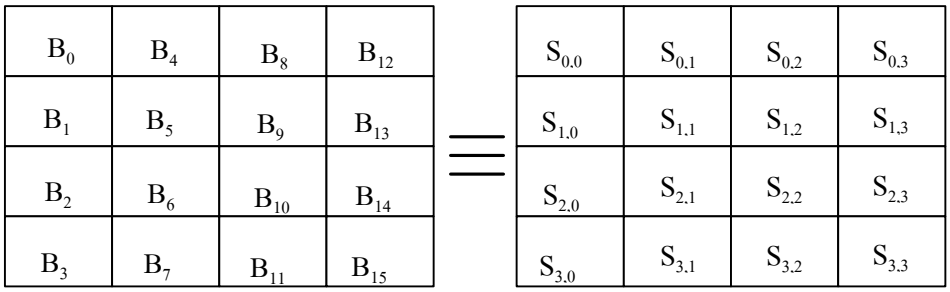
2.3.2 Triple-DES (3DES)

เป็นวิธีการเข้ารหัสลับที่เพิ่มความมั่นคงปลอดภัยของ DES ให้มีความแข็งแกร่งมากขึ้นโดยการเข้ารหัสลับ DES เป็นจำนวนสามครั้งแต่ละครั้งจะใช้กุญแจในการเข้ารหัสลับที่แตกต่างกันจึงเปรียบเสมือนการใช้กุญแจเข้ารหัสลับที่มีความยาวเท่ากับ 56 x 3 = 168 บิตซึ่งยาวกว่า DES ถึงสามเท่า อย่างไรก็ตามประสิทธิภาพการทำงานโดยรวมของระบบจะลดลงเนื่องจากต้องทำการถอดรหัสลับ DES สามครั้ง

2.3.3 Advanced Encryption Standard (AES) หรือ Rijndael

วิธีการเข้ารหัสลับนี้ได้รับการพัฒนาโดย Joan Daemen และ Vincent Rijmen ในปี 2000 วิทยาการเข้ารหัสลับได้รับการคัดเลือกโดย National Institute of Standard and Technology (NIST) ของสหรัฐอเมริกาให้เป็นมาตรฐานในการเข้ารหัสลับชั้นสูงของประเทศ วิธีการเข้ารหัสลับนี้มีความเร็วสูงโดยขนาดของข้อมูลตั้งต้น (Plaintext) 128 บิต สามารถเลือกใช้คีย์ที่มีความยาวขนาด 128, 192 และ 256 บิตซึ่งมีความมั่นคงปลอดภัยและทำงานได้เร็วกว่า 3DES

อัลกอริทึม AES จะเข้ารหัสลับข้อมูลเป็นกลุ่ม ๆ ละ 128 บิต คีย์ที่ใช้ในการเข้าและถอดรหัสมีขนาด 128, 192 หรือ 256 บิต ขึ้นอยู่กับผู้ใช้งาน เทคนิคพื้นฐานที่ AES ใช้ในการเข้ารหัสลับคือ การดำเนินการผสมกันระหว่างกลุ่มข้อมูลในเชิงพีชคณิตเช่นเดียวกันกับอัลกอริทึม IDEA อย่างไรก็ตาม กลุ่มบิตย่อยที่ใช้ในการประมวลผลของ AES จะถูกจัดให้อยู่ในรูปของแถวลำดับ (Array) 2 มิติขนาด 4 x 4 ไบต์ (Byte) เรียกทับศัพท์ว่า สเตท (State) โดยแต่ละแถวของสเตทจะประกอบด้วยกลุ่มบิตข้อมูลในรูปของคำ (Word ,w) ขนาด 32 บิตจำนวน *Nb* คำ (*Nb* คำนวณจากความยาวของกลุ่มบิตนำเข้าหารด้วย 32 ในที่นี้ *Nb* จะมีค่าเท่ากับ 4 เนื่องจาก 128 บิต / 32 บิต = 4) ดังนั้นเมื่อกลุ่มบิตนำเข้าขนาด 128 บิตเข้ามา AES จะแบ่งกลุ่มบิตนำเข้าเหล่านั้นออกเป็นกลุ่มไบต์ (B_n) จำนวน 16 กลุ่ม โดยจัดให้อยู่ในรูปของแถวลำดับ 2 มิติเรียงจากบนลงล่าง และจากซ้ายไปขวาตามลำดับ กลุ่มบิตนำเข้าที่จัดเรียงให้อยู่ในรูปแบบของสเตทแสดงดังภาพที่ 2.3 โดยให้สังเกตว่า กลุ่มไบต์ในหนึ่งคอลัมน์ก็คือ กลุ่มบิตข้อมูลขนาดหนึ่งคำ



ภาพที่ 2.3 การจัดเรียงกลุ่มบิตนำเข้าให้อยู่ในรูปของสเตท

ขนาดของคีย์ที่ใช้ในการประมวลผลอาจแสดงในรูปของบิตหรือคำก็ได้ โดยคีย์ขนาด *n* บิต จะมีขนาด *Nk = n/32* คำ ขนาดของคีย์จะเป็นตัวกำหนดจำนวนรอบของการประมวลผล *Nr* ในการเข้ารหัสลับ AES โดยใช้คีย์ขนาด 128 บิตสามารถเขียนให้อยู่ในรูปแบบย่อที่แสดงถึงโหมดการทำงานได้คือ AES-128 สำหรับโหมดอื่น ๆ ที่เหลือแสดงให้เห็นในตารางที่ 2.1

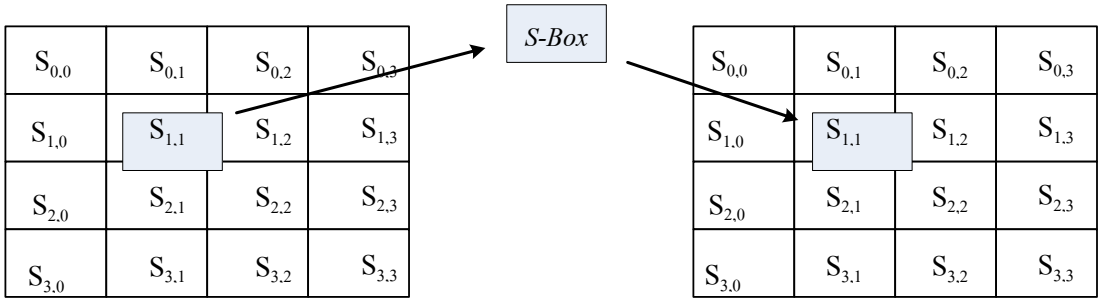
ตารางที่ 2.1 โหมดการทำงานในอัลกอริทึม AES

Mode	Key Length (*Nk* words)	Block Size (*Nb* words)	Number of Rounds (*Nr*)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

ในแต่ละรอบของการประมวลผล จะประกอบไปด้วยกระบวนการย่อย 4 กระบวนการคือ SubBytes, ShiftRows, MixColumns และ AddRoundKey ดังนี้

1) กระบวนการย่อย SubBytes

กระบวนการนี้จะทำการแทนที่ไบต์ข้อมูลที่อยู่ในสเตทโดยอ้างอิงจาก S-box ที่กำหนดดังภาพที่ 2.4 และภาพที่ 2.5 ประกอบแสดงการทำงาน



ภาพที่ 2.4 กระบวนการย่อย SubBytes

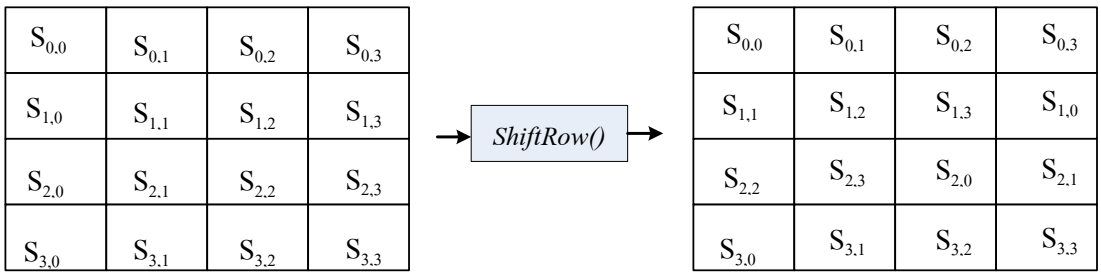
การแทนที่โดยใช้ *S-box* ในอัลกอริทึม AES นั้น กลุ่มบิตนำเข้าขนาด 8 บิต ($b_1b_2b_3b_4b_5b_6b_7b_8$) จะเป็นตัวกำหนดค่ากลุ่มบิตส่งออกขนาด 8 บิตที่เก็บบันทึกไว้ใน *S-box* โดยบิตที่ 1 ถึง 4 ($b_1b_2b_3b_4$) จะใช้เป็นตัวกำหนดตำแหน่งเชิงตัวเลขฐานสิบหก 0-F ในแต่ละแถวของ *S-box* ในขณะที่บิตที่ 5 ถึง 8 ($b_5b_6b_7b_8$) จะใช้กำหนดตำแหน่งเชิงตัวเลขฐานสิบหก 0-F ในแต่ละคอลัมน์ของ *S-box* ยกตัวอย่างเช่น ถ้ากลุ่มบิตนำเข้า $S_{1,1}$ มีค่าเท่ากับ 62_{16} ตำแหน่งของกลุ่มบิตส่งออกที่ได้จะอยู่ที่แถวที่ 6_{16} คอลัมน์ที่ 2_{16} ซึ่งก็คือ AA_{16} ในทำนองเดียวกัน ถ้า $S_{1,0}$ มีค่าเท่ากับ 53_{16} ผลลัพธ์ที่ได้จากกระบวนการย่อย SubBytes ก็คือ ED_{16} นั่นเอง

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	46	EE	B8	14	DE	5E	0B	DB
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	AC	62	91	95	E4	79
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

ภาพที่ 2.5 การแทนที่ *S-box* ในอัลกอริทึม AES

2) กระบวนการย่อย ShiftRows

กระบวนการนี้จะทำการเลื่อนไบต์ลักษณะเป็นวงกลมไปทางซ้าย *n* ไบต์ โดยแถวที่ 1,2, 3 และ 4 จะมีค่า *n* เท่ากับ 0, 1, 2 และ 3 ตามลำดับดังภาพที่ 2.6



ภาพที่ 2.6 กระบวนการย่อย ShiftRows

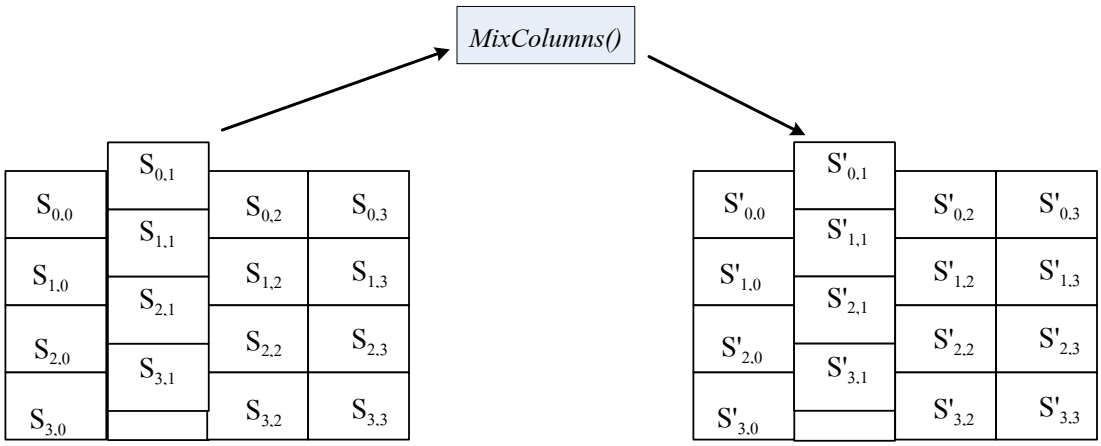
3) กระบวนการย่อย MixColumns

กระบวนการนี้จะทำการคูณมอดูโล x^4+1 ระหว่างคอลัมน์ภายในสเตทกับพหุนามคงที่ $a(x)=03_{16}x^3+01_{16}x^2+01_{16}x+02_{16}$ ในการดำเนินการนี้ กลุ่มไบต์ทั้ง 4 ในแต่ละคอลัมน์ของสเตทซึ่งจะถูกมองเปรียบเสมือนกับพหุนามของตัวหนึ่งที่มีขนาด 4 เทอม $b(x)=B_{i+0}x^3+B_{i+1}x^2+B_{i+2}x+B_{i+3}$ ซึ่งการคูณกันของพหุนามทั้งสองในมอดูโล x^4+1 ทั้ง 4 คอลัมน์นี้สามารถเขียนให้อยู่ในรูปของสมการการคูณเมทริกซ์ได้ดังนี้

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad \text{for } 0 \leq c \leq Nb$$

และผลลัพธ์ที่ได้จากการคูณกันในมอดูโล x^4+1 สามารถเขียนในรูปของสมการได้ดังนี้

$$S'_{0,c}=(02_{16} \cdot S_{0,c}) \oplus (03_{16} \cdot S_{1,c}) \oplus S_{2,c} \oplus S_{3,c}$$
$$S'_{1,c}=S_{0,c} \oplus (02_{16} \cdot S_{1,c}) \oplus (03_{16} \cdot S_{2,c}) \oplus S_{3,c}$$
$$S'_{2,c}=S_{0,c} \oplus S_{1,c} \oplus (02_{16} \cdot S_{2,c}) \oplus (03_{16} \cdot S_{3,c})$$
$$S'_{3,c}=(03_{16} \cdot S_{0,c}) \oplus S_{1,c} \oplus S_{2,c} \oplus (02_{16} \cdot S_{3,c})$$



ภาพที่ 2.7 กระบวนการย่อย MixColumns

4) กระบวนการย่อย AddRoundKey

กระบวนการย่อยนี้จะทำการ Xor ระหว่างสเตทของกลุ่มข้อมูลกับสเตทของกลุ่มคีย์ย่อยดังสมการนี้

$$\left[S'_{0,c},S'_{1,c},S'_{2,c},S'_{3,c}\right]=\left[S_{0,c},S_{1,c},S_{2,c},S_{3,c}\right]\oplus w\left[r^{*}N^{*}b+c\right]$$

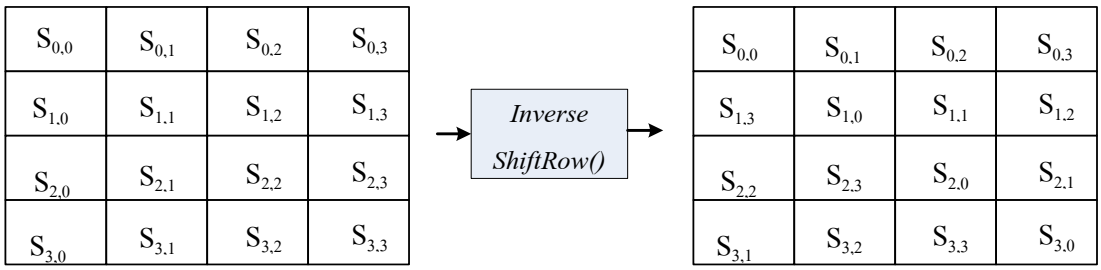
$$\text{for } 0 \leq c \leq N^{*}b \text{ and } 0 \leq r \leq N^{*}r$$

ในการเข้ารหัสลับ AES จะทำการจัดเรียงกลุ่มข้อมูลขนาด 128 บิตให้ในรูปของสเตท จากนั้นจะผ่านกระบวนการย่อย AddRoundKey 1 ครั้งก่อน ผลลัพธ์ที่ได้จะเริ่มเข้าสู่กระบวนการประมวลผลเป็นจำนวน 10, 12 หรือ 14 รอบขึ้นอยู่กับขนาดของคีย์ที่ใช้ในการเข้ารหัสลับ ซึ่งแต่ละรอบของการประมวลผลจะเป็นการดำเนินการกระบวนการย่อยทั้ง 4 ที่กล่าวมาข้างต้นตามลำดับ อย่างไรก็ตามในรอบสุดท้ายของการประมวลผล ทั้ง 3 โหมดการทำงาน จะไม่มีกระบวนการย่อย MixColumns รวมอยู่ด้วย เมื่อผ่านกระบวนการประมวลผลครบตามรอบที่กำหนดแล้ว ผลลัพธ์สุดท้ายที่ได้ก็คือ ข้อความรหัส

สำหรับขั้นตอนในการถอดรหัสลับของ AES นั้น จะดำเนินการในลักษณะย้อนกลับกับขั้นตอนการเข้ารหัสลับ กระบวนการย่อยต่าง ๆ ที่ใช้ในการเข้ารหัสลับจะเปลี่ยนเป็นกระบวนการย่อยแบบผกผันแทนซึ่งในแต่ละรอบของการประมวลผลจะประกอบไปด้วย 4 กระบวนการย่อยเช่นเดียวกันคือ

1) กระบวนการย่อย InvShiftRows

กระบวนการนี้จะทำการเลื่อนไบต์เป็นวงกลมไปทางขวา n ไบต์ โดยในแถวที่ 2, 3 และ 4 จะมีค่า n เท่ากับ 0, 1, 2 และ 3 ตามลำดับดังภาพที่ 2.8



ภาพที่ 2.8 กระบวนการย่อย InvShiftRows

2) กระบวนการย่อย InvSubBytes

กระบวนการนี้จะทำการแทนที่ไบต์ข้อมูลที่อยู่ในสเตทโดยอ้างอิงจาก S-box ผกผัน (Inverse S-box) ที่กำหนด ดังแสดงในภาพที่ 2.9

		Y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
X	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

ภาพที่ 2.9 การแทนที่ S-box ผกผัน

3) กระบวนการย่อย *InvMixColumns*

กระบวนการนี้จะทำการคูณมอดูโล x^4+1 ระหว่างคอลัมน์ภายในสเตทกับพหุนามคงที่ $a^{-1}(x)=0B_{16}x^2+0D_{16}x^2+09_{16}x+0E_{16}$ ซึ่งการคูณกันของพหุนามทั้งสองในมอดูโล x^4+1 ทั้ง 4 คอลัมน์นี้สามารถเขียนในรูปของสมการการคูณเมทริกซ์ได้ดังนี้

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \quad \text{for } 0 \leq c \leq Nb$$

และผลลัพธ์ที่ได้จากการคูณกันในมอดูโล x^4+1 สามารถเขียนในรูปของสมการได้ดังนี้

$$S'_{0,c}=(0E_{16} \cdot S_{0,c}) \oplus (0B_{16} \cdot S_{1,c}) \oplus (0D_{16} \cdot S_{2,c}) \oplus (09_{16} \cdot S_{3,c})$$
$$S'_{1,c}=(09_{16} \cdot S_{0,c}) \oplus (0E_{16} \cdot S_{1,c}) \oplus (0B_{16} \cdot S_{2,c}) \oplus (0D_{16} \cdot S_{3,c})$$
$$S'_{2,c}=(0D_{16} \cdot S_{0,c}) \oplus (09_{16} \cdot S_{1,c}) \oplus (0E_{16} \cdot S_{2,c}) \oplus (0B_{16} \cdot S_{3,c})$$
$$S'_{3,c}=(0B_{16} \cdot S_{0,c}) \oplus (0D_{16} \cdot S_{1,c}) \oplus (09_{16} \cdot S_{2,c}) \oplus (0E_{16} \cdot S_{3,c})$$

4) กระบวนการย่อยAddRoundKey

เนื่องจากกระบวนการนี้เป็นการ Xor ฉะนั้นกระบวนการย้อนกลับจึงสามารถทำได้โดยการ Xor กับผลลัพธ์ที่ได้ในตอนแรกอีกครั้งหนึ่ง

2.4 ข้อตกลงคีย์ Diffie-Hellman

ข้อตกลงคีย์ Diffie-Hellman พัฒนาโดย Diffie และ Hellman มีการนำเสนอครั้งแรกในปีคริสต์ศักราช 1976 ความปลอดภัยของอัลกอริทึมนี้ขึ้นอยู่กับความยากในการคำนวณลอการิทึมแบบไม่ต่อเนื่องภายในฟิลด์จำกัด เมื่อเทียบกับความง่ายในการคำนวณตัวเลขชี้กำลังภายในฟิลด์จำกัดเดียวกัน และอัลกอริทึมนี้ช่วยให้สามารถสร้างคีย์ลับสำหรับการเข้ารหัสลับระหว่างสองฝ่ายโดยใช้การแลกเปลี่ยนข้อมูลผ่านช่องทางการสื่อสารที่ไม่ปลอดภัย การดำเนินการของอัลกอริทึมระหว่างผู้ใช้งานสองคนกำหนดไว้ดังนี้

สมมติว่าในเครือข่ายสื่อสารใด ๆ นายดำกับนายแดงต้องการจะสร้างคีย์ตัวหนึ่งขึ้นมาเพื่อใช้ในการแลกเปลี่ยนความลับระหว่างกัน

1) นายดำกับนายแดงเห็นชอบร่วมกันที่จะใช้ตัวเลขจำนวนเฉพาะค่ามาก ๆ p หนึ่งค่า และตัวเลขจำนวนใด ๆ g ที่เป็นค่าปฐมฐานของมอดูโล p(Primitive)$mod\ p$ อีกหนึ่งค่า ตัวเลขทั้งสองนี้ไม่จำเป็นต้องเก็บรักษาเป็นความลับ เนื่องจากจะนำมาใช้ในการคำนวณหาคีย์ที่ใช้ร่วมกันผ่านช่องทางสื่อสารที่ไม่ปลอดภัย

2) นายดำเลือกตัวเลขสุ่ม x ซึ่งมีค่ามาก ๆ มาหนึ่งค่า ตัวเลขนี้จำเป็นต้องเก็บเป็นความลับ จากนั้นทำการคำนวณค่า

$$A = g^x \ mod\ p$$

นายดำส่งผลลัพธ์จากการคำนวณที่ได้ให้กับนายแดง

3) นายแดงเลือกตัวเลขสุ่ม y ซึ่งมีค่ามาก ๆ มาหนึ่งค่า ซึ่งตัวเลขนี้จำเป็นต้องเก็บเป็นความลับเหมือนกัน จากนั้นทำการคำนวณค่า

$$B = g^y \ mod\ p$$

นายแดงส่งผลลัพธ์จากการคำนวณที่ได้ให้กับนายดำ

4) นายดำคำนวณหาค่าตัวเลขที่จะใช้เป็นคีย์จากผลลัพธ์ที่นายแดงส่งมา

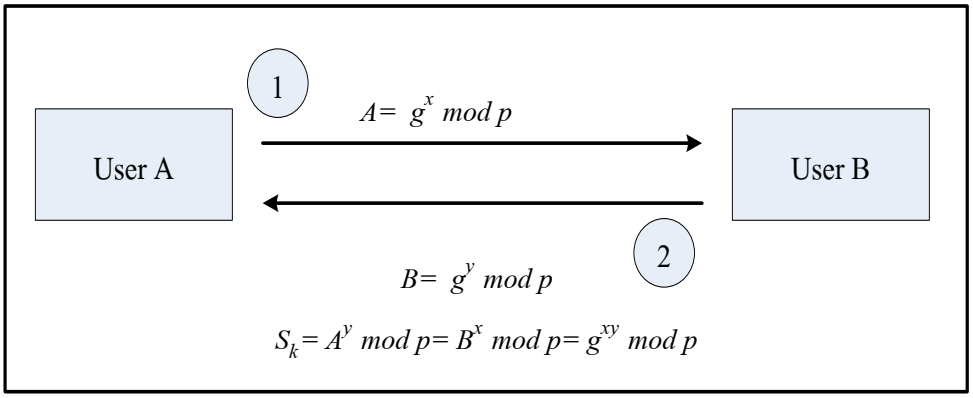
$$S_k = B^x \ mod\ p$$

ซึ่งมีค่าเท่ากับ $g^{xy} \ mod\ p$

5) นายแดงคำนวณหาค่าตัวเลขที่จะใช้เป็นคีย์จากผลลัพธ์ที่นายดำส่งมา

$$S_k = A^y \ mod\ p$$

ซึ่งมีค่าเท่ากับ $g^{xy} mod\ p$ ดังภาพที่ 2.10 แสดงขั้นตอนการสร้างคีย์ร่วมกันระหว่างผู้ใช้งานสองคน



ภาพที่ 2.10 ขั้นตอนการสร้างคีย์ร่วมกันระหว่างผู้ใช้สองคน

ในอัลกอริทึมข้อตกลงคีย์ของ Diffie-Hellman ตัวเลข p และ g จะพิจารณาว่าเป็นคีย์สาธารณะขณะที่ตัวเลข x และ y จะพิจารณาว่าเป็นคีย์ส่วนตัวของนายดำและนายแดงตามลำดับ เหตุผลที่เลือกตัวเลข p เป็นจำนวนเฉพาะเนื่องมาจาก การคำนวณลอการิทึมแบบไม่ต่อเนื่องภายในฟิลด์จำกัดของเลขจำนวนเฉพาะจะมีความซับซ้อนสูงกว่าในกรณีของตัวเลขทั่ว ๆ ไปมาก ความยากในการคำนวณนี้จะเพิ่มสูงขึ้น ถ้าตัวเลข p ที่ใช้เป็นจำนวนเฉพาะที่มีค่ามาก ๆ เช่น เป็นตัวเลขขนาด 512 บิตหรือ 1024 บิต

ในการนำไปใช้งาน ขณะที่อยู่ในขั้นตอนการสร้างคีย์ ถ้ามีใครบางคนดักฟังตัวเลข 3 ตัวคือ p , g และ A ที่นายดำส่งให้นายแดง และตัวเลข B ที่นายแดงส่งให้นายดำ คน ๆ นั้นจะไม่สามารถหาค่าคีย์ S_k ได้ เว้นแต่เพียงว่า เขาจะสามารถคำนวณหาค่าลอการิทึมแบบไม่ต่อเนื่องภายในฟิลด์จำกัดได้ ดังนั้นค่า S_k ที่สร้างขึ้นร่วมกันโดยการคำนวณอย่างอิสระต่อกันของนายดำกับนายแดง จะนำมาใช้เป็นคีย์เข้ารหัสลับและถอดรหัสลับข้อความต้นฉบับที่ส่งไปมาระหว่างบุคคลทั้งสอง

2.5 โปรโตคอลข้อตกลงคีย์กลุ่ม

ในงานวิจัยนี้จะนำเสนอโปรโตคอลที่ทำงานในกรณีของกลุ่มแบบไดนามิกและโปรโตคอลจะประกอบด้วยข้อตกลงของการทำงานดังต่อไปนี้

ข้อตกลงคีย์ครั้งแรก (Initial Key Agreement:IKA) หมายถึงขั้นตอนการตั้งค่ากำหนดเมื่อจำนวนของผู้ใช้ใหม่ตัดสินใจที่จะรับคีย์กลุ่มใหม่

ข้อตกลงคีย์เสริม (Auxiliary Key Agreement: AKA) หมายถึงขั้นตอนการปรับเปลี่ยนกลุ่ม (หลังจากที่กลุ่มจะเกิดขึ้น) เป็นสิ่งจำเป็นอย่างยิ่งที่การทำงานแต่ละครั้งเหล่านี้นำไปสู่การเปลี่ยนแปลงคีย์ในกลุ่ม (เพื่อรักษาความเป็นอิสระ) การดำเนินการนี้ได้แก่

การเข้าร่วม หนึ่งในสมาชิกใหม่มีความประสงค์ที่จะเข้าร่วมกลุ่มที่จัดตั้งขึ้นแล้ว

การออกจากกลุ่ม สมาชิกที่ออกจากกลุ่ม (โดยสมัครใจหรือไม่ก็ตาม)

การพาร์ติชันกลุ่ม กลุ่มถูกแบ่งออกเป็นสองกลุ่ม (หรือมากกว่า) เป็นกลุ่มเล็ก ๆ ซึ่งอาจมองได้ว่าเป็นการ “ลบ” สมาชิกที่มีจำนวนมากกว่าหนึ่งคน

การรวมสองกลุ่ม (หรือมากกว่า) ทำให้เป็นกลุ่มเดียว ซึ่งอาจมองได้ว่าเป็นการ “เข้าร่วม” ของสมาชิกที่มีจำนวนมากกว่าหนึ่ง

2.5.1 Tree-based Group Key Agreement (TGDH) Protocol

TGDH คือการปรับตัวของต้นไม้ (Kim et al. 2000; 2004) ในบริบทของการกระจายเต็มการคำนวณคีย์กลุ่มได้มาจากการมีส่วนร่วมของสมาชิกทุกคนของกลุ่มโดยใช้ต้นไม้ไบนารี

ในต้นไม้คีย์ TGDH โหนดอยู่ที่ระดับ 0 node(0,0) จะเป็น root มีความสูง h เท่ากับระดับความลึกของต้นไม้ สมาชิกมีความสัมพันธ์กับโหนดใบ โหนดที่ไม่ใช่โหนดใบจะเรียกว่าโหนดภายในที่มีลูกสองโหนด ลูกด้านซ้ายของโหนด (l,v) เป็นโหนด $(l+1, 2v)$ และลูกด้านขวาจะเป็นโหนด $(l+1, 2v+1)$ โหนดทุกโหนดจะคำนวณคีย์ส่วนตัว $K(l,v)$ และคีย์สาธารณะ $BK(l,v)$ ซึ่งสามารถคำนวณได้จาก $BK(l,v)= g^{K(l,v)} \bmod p$ โดยเมื่อต้องการติดต่อสื่อสารกับสมาชิกคนอื่นจะต้องคำนวณหาคีย์ลับ $SK(l,v)$ ซึ่งสามารถคำนวณตามลำดับได้ดังนี้

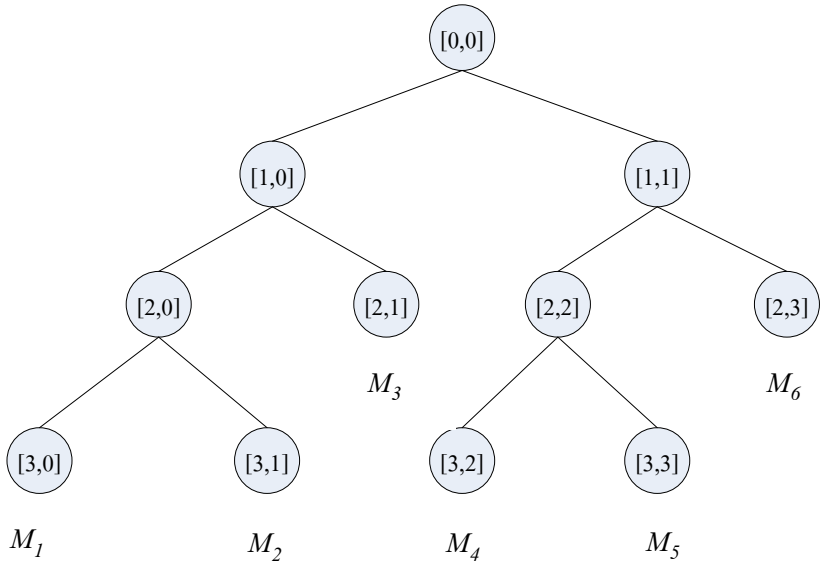
$$SK(l,v) = BK_{(l+1,2v)}^{K(l+1,2v+1)} \bmod p$$

$$= BK_{(l+1,2v+1)}^{K(l+1,2v} \bmod p$$

$$= g^{K_{(l+1,2v)}K_{(l+1,2v+1)}} \bmod p$$

ภาพที่ 2.11 แสดงตัวอย่างของต้นไม้คีย์ของกลุ่มซึ่งประกอบด้วยสมาชิกทั้งหกคน คีย์กลุ่มสำหรับสมาชิกกลุ่มนี้คือ

$SK(0,0)= g^{g^{K3 \cdot g^{K1 \cdot K2}} \cdot g^{K6 \cdot g^{K4 \cdot K5}}} \bmod p$ โดยที่ $K1,\cdots,K6$ เป็นคีย์ลับของสมาชิก $M1,\cdots, M6$ ตามลำดับ



ภาพที่ 2.11 โปรโตคอล TGDH ตามโครงสร้างต้นไม้

การวิเคราะห์ประสิทธิภาพของโปรโตคอล TGDH ขึ้นอยู่กับปัจจัยหลายอย่าง เช่น ความสูง ความสมดุลของต้นไม้ ตำแหน่งของจุดแทรกและตำแหน่งของสมาชิกที่ออกจากกลุ่มเป็นต้น ปัจจัยบางอย่างสามารถคาดการณ์ได้สำหรับกรณีที่เลวร้ายที่สุดแต่ก็มีบางปัจจัยที่อาจไม่สามารถประเมินได้

สมมติฐานว่าต้นไม้ TGDH พร้อมด้วยสมาชิก n โหนดมีโหนดภายใน $n-1$ โหนดสมาชิกแต่ละคนจะต้องรู้ว่าคีย์ที่ซ่อนในโหนดภายในทั้งหมดยกเว้นโหนดราก

2.5.1.1 การเข้าร่วมของสมาชิกใหม่

สมมติมีสมาชิกใหม่ M_{n+1} ต้องการเข้าร่วมกลุ่มซึ่งมีสมาชิกทั้งหมด n คน $\{M_1,\ldots,M_n\}$ สมาชิกใหม่กระจายการร้องขอเข้าร่วมกลุ่มด้วยตนเองหลังจากที่ได้รับการร้องขอเข้าร่วมกลุ่ม สมาชิกแต่ละคนในกลุ่มปัจจุบันจะกำหนดจุดแทรก หากต้นไม้ที่มีความสมดุล (Balance Tree) สมาชิกใหม่ที่เข้าร่วมจะเป็นโหนดราก หรือมิฉะนั้น โหนดใบสุดท้ายด้านขวาสุดจะเป็นโหนดแทรก เหตุผลของการเลือกจุดแทรกดังกล่าวคือการให้ต้นไม้คีย์มีลักษณะความสมดุล

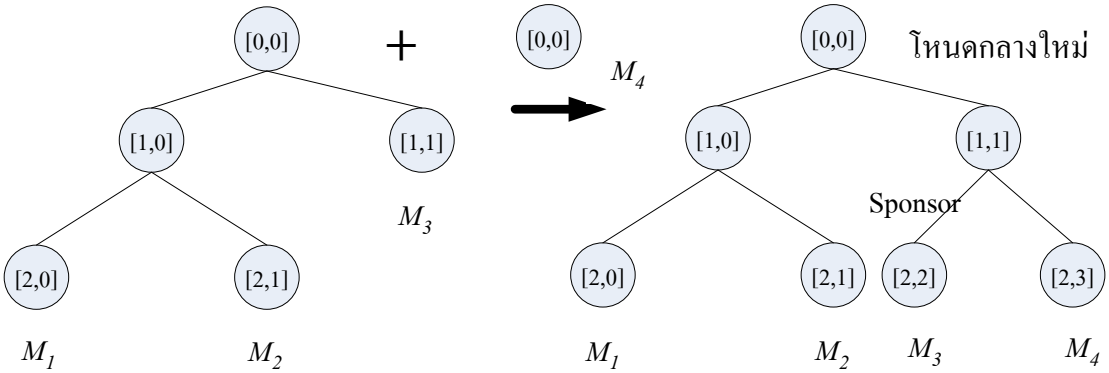
เมื่อมีการเพิ่มโหนดใบของสมาชิกใหม่ ต้นไม้จะต้องมีการปรับปรุงโดย Sponsor ซึ่งเป็นโหนดใบที่ตื้นสุดด้านขวาในต้นไม้ย่อยที่โหนดแทรก โหนดใหม่จะถูกสร้างขึ้นระหว่างกลางโดยโหนดแทรกจะกลายเป็นลูกอยู่ทางด้านซ้ายของโหนดใหม่และสมาชิกใหม่จะกลายเป็นลูกด้านขวา การเข้าของสมาชิกใหม่ในโปรโตคอล TGDH ประกอบด้วยขั้นตอนต่อไปนี้

1) สมาชิกใหม่กระจายร้องขอการเข้าร่วมด้วยตัวสมาชิกเอง

2) สมาชิกทุกคนปรับปรุงคีย์ต้นไม้ลบคีย์ทั้งหมดและคีย์ซ่อนจากโหนด Sponsorไปยังโหนดราก Sponsor M_S ปรับปรุงและคำนวณคีย์ใหม่ในโหนดเส้นทางของคีย์และกระจายการปรับปรุงต้นไม้และคีย์ลับทั้งหมด

3) สมาชิกทุกคนในกลุ่มคำนวณคีย์ใหม่ในคีย์ต้นไม้

ภาพที่ 2.12 แสดงตัวอย่างของกลุ่มที่ประกอบด้วยสมาชิกสามคนเมื่อมีสมาชิกใหม่ M_4 ต้องการเข้าร่วมกลุ่ม สมาชิก M_3 ถูกเลือกให้เป็น Sponsor สมาชิกแต่ละคนปรับปรุงต้นไม้เก่าโดยการใส่ M_4 พร้อมลบคีย์และคีย์ลับในเส้นทางคีย์ M_3 นอกจากนี้ Sponsor M_3 จะต้องปรับปรุงคีย์ที่ใช้ร่วมกันระหว่างสมาชิกและคำนวณ $K_{(1,1)}$,$BK_{(1,1)}$, และ $K_{(0,0)}$และกระจายการปรับปรุงต้นไม้ด้วยคีย์ลับทั้งหมด (ตัวอย่าง $BK_{(2,0)}$,$BK_{(2,1)}$,$BK_{(2,2)}$,$BK_{(2,3)}$,$BK_{(1,0)}$ และ $BK_{(1,1)}$) พร้อมกับข้อความกระจาย M_1 และ M_2 คำนวณค่าคีย์ใหม่ $K_{(1,0)}$และ M_4 คำนวณ $K_{(1,1)}$และ $K_{(0,0)}$



ภาพที่ 2.12 ตัวอย่างการเข้าร่วมของสมาชิกใหม่ M_4 ในโปรโตคอล TGDH

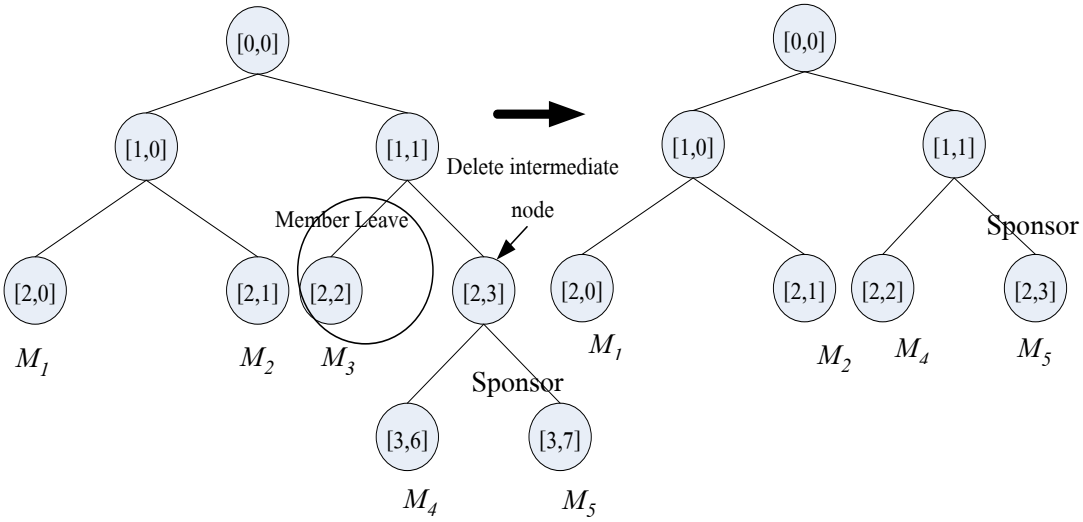
2.5.1.2 การออกจากกลุ่มของสมาชิก

สมมติว่ามีสมาชิกกลุ่มจำนวน nสมาชิกและมีสมาชิก M_l ออกจากกลุ่ม โหนดใบที่อยู่ขวาสุดของ M_l จะถูกเลือกเป็น Sponsor ในการปรับปรุงคีย์ให้กับสมาชิกที่เหลืออยู่ในต้นไม้ โดยทำการการลบโหนด M_l และโหนดพี่น้อง (Intermediate node) ของสมาชิก M_l ออกจากโครงสร้างต้นไม้ หลังจากนั้นโหนด Sponsor จะดำเนินการปรับปรุงโหนดแม่ของโหนด Sponsor นอกจากนี้ต้องปรับปรุงและคำนวณคีย์ใหม่ให้กับสมาชิกทุกคนในเส้นทางของคีย์เพื่อให้สมาชิกทุกคนสามารถคำนวณคีย์ใหม่ในคีย์ต้นไม้ได้ การออกจากกลุ่มของสมาชิกในโปรโตคอล TGDH ประกอบด้วยขั้นตอนดังต่อไปนี้

1) โหนด Sponsor ลบโหนดสมาชิกและโหนดพี่น้องของสมาชิกที่ออกจากกลุ่ม Sponsor ปรับปรุงและคำนวณคีย์ใหม่ในเส้นทางของคีย์และกระจายการปรับปรุงคีย์ต้นไม้และคีย์ลับทั้งหมด

2) สมาชิกทุกคนในกลุ่มคำนวณคีย์ใหม่ในคีย์ต้นไม้

ภาพที่ 2.13 แสดงตัวอย่างของกลุ่มที่มีสมาชิกห้าคนเมื่อสมาชิก M_3 ออกจากกลุ่มและสมาชิก M_5 เป็น Sponsor ในการปรับปรุงและคำนวณคีย์ใหม่สำหรับสมาชิกที่เหลืออยู่คือ M_1,M_2,M_4,และ M_5 โดยที่สมาชิก M_5 ทำการลบโหนด *(2,2)* และ *(2,3)* แล้วทำการปรับปรุงและคำนวณคีย์ $K_{(1,1)}$,$BK_{(1,1)}$,$K_{(0,0)}$ จากนั้นกระจายการปรับปรุงและคำนวณคีย์ทั้งหมด เพื่อให้สมาชิก M_1และสมาชิก M_2 สามารถคำนวณคีย์ใหม่ $K_{(0,0)}$ และสมาชิก M_4 สามารถคำนวณคีย์ $K_{(1,1)}$ และ $K_{(0,0)}$



ภาพที่ 2.13 ตัวอย่างการออกจากกลุ่มของ M_3 ในโปรโตคอล TGDH

2.5.1.3 การรวมกลุ่มของสมาชิก

การรวมสมาชิกกลุ่มสองกลุ่มหรือมากกว่าหลายกลุ่มสามารถดำเนินการได้ดังนี้ สมมติสมาชิก m ต้องการเข้าร่วมกลุ่ม G_1 โดยสมาชิก m เป็นสมาชิกแต่ละรูปแบบของ TGDH ของกลุ่ม G_2 เมื่อกลุ่ม G_2 รวมตัวกับ G_1 โปรโตคอลพิจารณาก่อนการผสานของทั้งสองกลุ่ม สามารถขยายเพื่อผสานมากกว่าสองกลุ่มกล่าวคือ $k>2$ โดยความสูงการดำเนินการผสานทีละ 2 กลุ่มการดำเนินการทั้งสองกลุ่มผสาน $k-1$ ครั้ง

เริ่มแรกต้นไม้สองต้นจะเรียงลำดับจากมากไปหาน้อย ซึ่งหมายถึง T_1 และ T_2 ถ้าต้นไม้สองต้นมีความสูงเดียวกัน การเข้าร่วมจะทำได้โดยเลือก T_2 ไปยังโหนดรากของ T_1 หรือมิเช่นนั้นแล้วจะหาโหนดที่ตื้นทางด้านขวาที่จะเข้าร่วมเพื่อเพิ่มความสูงของต้นไม้ หากไม่มีโหนดดังกล่าวอยู่จุดแทรกจะเป็นตำแหน่งโหนดราก

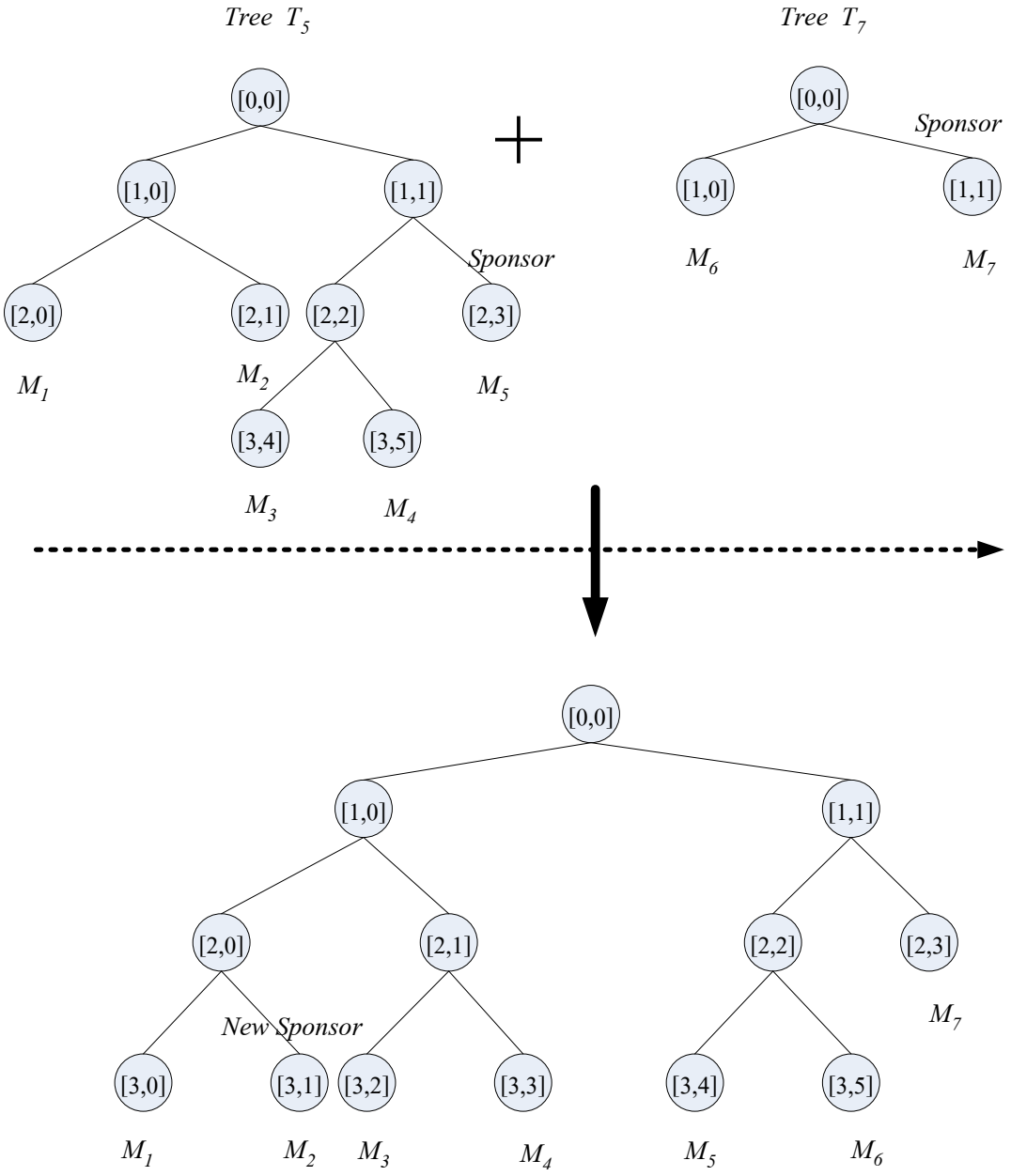
สมมติมีต้นไม้คีย์อยู่ m ต้น สามารถนำมาจัดเรียงระดับคามความสูงจากมากไปหาน้อยได้คือ $T_1,\cdots,T_m$ การรวมกันของต้นไม้แต่ละต้น T_i จะมีโหนดใบขวาสุดที่เข้าร่วมเป็น Sponsor M_{S_i} การรวมกลุ่มสมาชิกในโปรโตคอล TDGH ประกอบด้วยขั้นตอนดังต่อไปนี้

1) Sponsor M_{S_i} ในต้นไม้ T_i ปรับปรุงการเข้าร่วมคำนวณคีย์ทั้งหมดและคีย์ลับในเส้นทางคีย์ของ T_i (รวมถึง $BK_{(0,0)}$) กระจายการปรับปรุงต้นไม้ T_i รวมถึงคีย์ลับทั้งหมด *For i = 1, 2, … , m* นอกจากนี้สมาชิกแต่ละคนปรับปรุงคีย์ต้นไม้และให้การสนับสนุนการตัดสินใจใหม่ $M_{S_i},\cdots,M_{S_m}$ ลบคีย์ทั้งหมดและคีย์ลับในเส้นทางคีย์ของ Sponsor

2) ทำซ้ำขั้นตอนนี้ไปจนกว่า Sponsor จะคำนวณคีย์กลุ่มที่เกี่ยวข้องกันแต่ละ Sponsor M_{S_i} โดยที่ $1 \leq i \leq m$ ปรับปรุงและคำนวณคีย์ใหม่ในเส้นทางคีย์ที่อยู่ในระยะไกลที่สุดเท่าที่เป็นไปได้และกระจายการปรับปรุงการคำนวณคีย์ใหม่ในคีย์ต้นไม้

3) สมาชิกทุกคนในกลุ่มคำนวณคีย์ใหม่ในคีย์ต้นไม้

ตัวอย่างการรวมกลุ่มของสมาชิกทั้งสองกลุ่มดังแสดงในภาพที่ 2.14 สมาชิก M_5 และสมาชิก M_7 ซึ่งเป็น Sponsor ปรับปรุงและคำนวณคีย์ใหม่ตามโครงสร้างทั้งหมดตามลำดับ โดยที่เมื่อสมาชิก M_5 คำนวณคีย์ใหม่ $K_{(1,1)},BK_{(1,1)},K_{(0,0)}$ และ $BK_{(0,0)}$ ในโครงสร้างต้นไม้ T_5 แล้วและสมาชิก M_7 คำนวณคีย์ $K_{(0,0)}$ และ $BK_{(0,0)}$ ในโครงสร้างต้นไม้ T_7 แล้วเช่นกัน Sponsor ทั้งสมาชิก M_5 และสมาชิก M_7 กระจายการปรับปรุงและคำนวณคีย์ลับทั้งหมดให้กับสมาชิกแต่ละรายผสมผสานเข้ากับต้นไม้ทั้งสองได้อย่างเป็นอิสระ และเลือก M_2 เป็น Sponsor ใหม่ แล้วสมาชิกทุกคนลบคีย์ทั้งหมดและคีย์ลับในเส้นทางคีย์ M_2 นอกจากนี้ M_2 ปรับปรุงและคำนวณคีย์ใหม่ $K_{(2,1)},BK_{(2,1)},K_{(1,0)},BK_{(1,0)}$ และ $K_{(0,0)}$ จากนั้นสมาชิก M_2 กระจายการปรับปรุงและคำนวณคีย์ลับทั้งหมดให้กับสมาชิกเพื่อให้ สมาชิก M_1 สามารถคำนวณคีย์ $K_{(2,0)},K_{(1,0)}$ และ $K_{(0,0)}$ ได้และสมาชิก M_6 และสมาชิก M_7 สามารถคำนวณ $K_{(1,0)}$ และ $K_{(0,0)}$ ส่วนสมาชิกที่เหลือทั้งหมดคือสมาชิก M_3,M_4 และสมาชิก M_5 จะคำนวณเฉพาะคีย์กลุ่มใหม่ $K_{(0,0)}$ เนื่องจากมีเพียงแค่หนึ่ง Sponsor เท่านั้น



ภาพที่ 2.14 ตัวอย่างการรวมต้นไม้คีย์ของสองกลุ่มสมาชิกในโปรโตคอล TGDH

2.5.1.4 การพาร์ติชันของสมาชิก

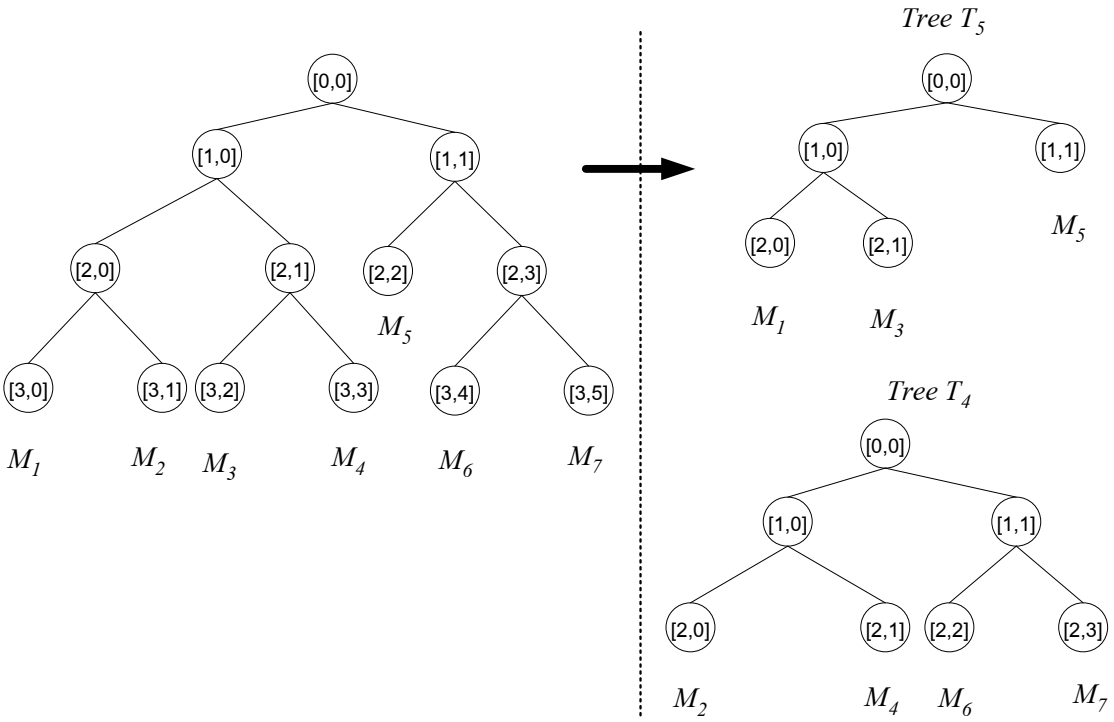
สมมติกลุ่มของสมาชิกมี n สมาชิก และ k เป็นสมาชิกที่ต้องการออกจากกลุ่ม ในรอบแรก การปรับปรุงสมาชิกที่เหลืออยู่ของต้นไม้โดยการลบพาร์ติชันสมาชิกทั้งหมดรวมทั้งโหนดแม่ของตน กล่าวอีกนัยหนึ่งว่าถ้าทุกโหนดใบของต้นไม้ย่อยที่ออกจากกลุ่ม หากโหนดรากของต้นไม้ย่อยนี้ถูกทำเครื่องหมายให้เป็นการออกและโหนดใบของมันจะถูกลบออกจากรายการโหนด สำหรับโหนดออกแต่ละครั้งที่ระบุว่ามี Sponsor จะใช้วิธีเดียวกันกับการออกของสมาชิกในกลุ่ม การพาร์ติชันของสมาชิกในโปรโตคอล TGDH ประกอบด้วยขั้นตอนดังต่อไปนี้

1) สมาชิกทุกคนที่คีย์ต้นไม้ปรับปรุงแต่ละต้นไม้โดยการลบโหนดสมาชิกออกจากโหนดทั้งหมดและโหนดพ่อแม่ของตน ลบคีย์ทั้งหมดและคีย์ลับจาก Sponsor ไปยังโหนดราก Sponsor ด้านขวาสุดปรับปรุงและคำนวณคีย์ใหม่

2) ทำซ้ำขั้นตอนนี้ไปจนกว่า Sponsor ใด ๆ คำนวณคีย์กลุ่ม Sponsor แต่ละราย M_{S_i} คำนวณคีย์ทั้งหมดและคีย์ลับในเส้นทางคีย์ที่อยู่ในระยะไกลที่สุดเท่าที่เป็นไปได้รวมทั้งการกระจายการปรับปรุงและคำนวณคีย์ลับทั้งหมด

3) สมาชิกทุกคนในกลุ่มคำนวณคีย์ใหม่ในคีย์ต้นไม้

ภาพที่ 2.15 แสดงตัวอย่างการแบ่งพาร์ติชันของสมาชิกในโปรโตคอล TGDH สมาชิกทั้งหมดเจ็ดคนคือสมาชิก $M_1, . . ,M_7$ และสมาชิก M_2, M_4, M_6 และสมาชิก M_7 ต้องการแยกตัวออกจากกลุ่ม ดังนั้นสมาชิก M_5 จะอยู่ในโครงสร้างของต้นไม้ T_5 เหมือนกันกับสมาชิก M_1 และสมาชิก M_3 หลังจากพาร์ติชัน อย่างไรก็ตามมุมมองของสมาชิก M_4 สมาชิกที่ออกจะเป็นสมาชิก M_1, M_3 และสมาชิก M_5 ดังนั้นสมาชิก M_4 จะอยู่ในโครงสร้างของต้นไม้ T_4 เช่นเดียวกันกับสมาชิก M_2,M_6 และสมาชิก M_7 หลังจากพาร์ติชัน



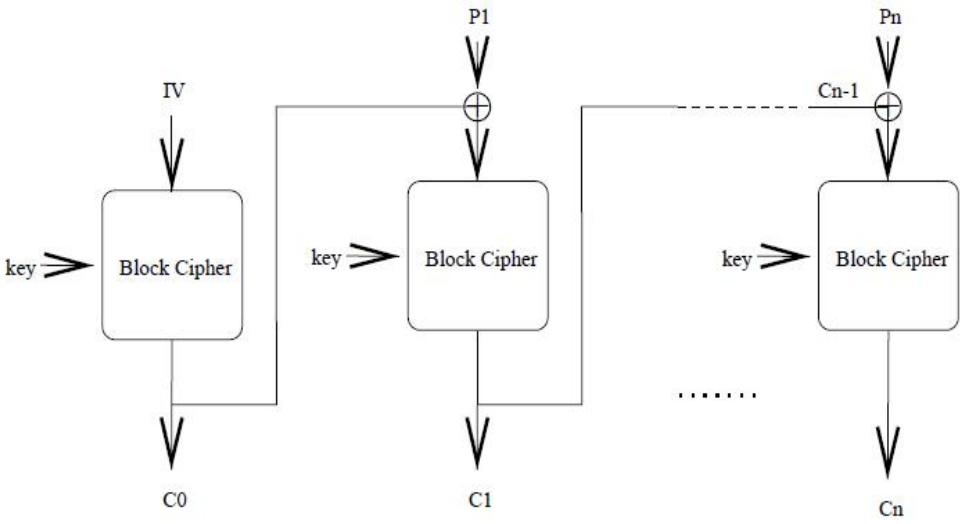
ภาพที่ 2.15 ตัวอย่างการพาร์ติชันของกลุ่มสมาชิกในโปรโตคอล TGDH

2.5.1.5 Key Refresh

ในการสื่อสารภายในกลุ่มเมื่อถึงในเวลาระยะหนึ่งแล้ว หากสมาชิกภายในกลุ่มไม่มีการเปลี่ยนแปลงใด ๆ เกิดขึ้นกับคีย์ต้นไม้ คีย์เซิร์ฟเวอร์จะดำเนินการปรับปรุงและคำนวณคีย์กลุ่มใหม่เพื่อรักษาความปลอดภัยในการสื่อสารให้คงอยู่

2.5.2 การรักษาความปลอดภัยของระบบไฟล์ที่ใช้ร่วมในกลุ่ม

K. E. Fu (1999) ได้นำเสนองานวิจัยเรื่อง Group sharing and random access in cryptographic storage file Systems ซึ่งได้นำเสนอการเข้ารหัสไฟล์ก่อนที่จะอัพโหลดไปยังเครือข่ายและสนับสนุนการใช้ไฟล์ร่วมกันของกลุ่ม งานวิจัยนี้เสนอแนวความคิดที่ใช้กล่องล็อคนี้เปรียบเสมือนระบบหลักเมื่อต้องการส่งข้อความจะทำการเข้ารหัสข้อมูลโดยทั่วไปแล้วจะมีขนาด 8 ไบต์ ดังนั้นจะต้องแบ่งขนาดของบล็อคไฟล์ข้อมูลขนาด 8KB เป็นบล็อคขนาดเล็กจำนวน 1024 บล็อกไฟล์แทนค่าด้วย $P_1 ... P_{1024}$ และใช้การเข้ารหัสแบบสมมาตรในโหมด Cipher Block Chaining (CBC) ตามภาพที่ 2.16 โดยใช้เว็กเตอร์เริ่มต้น (IV) เข้ารหัสรอบแรกเพื่อให้แน่ใจว่าบล็อคข้อมูลที่คล้ายกันในไฟล์ไม่ได้เข้ารหัสบล็อคข้อความที่เหมือนกัน



ภาพที่ 2.16 ตัวอย่างไฟล์ข้อมูลที่ถูกเข้ารหัสโดยโหมด CBC ต่อบล็อก

ดังนั้นในการรักษาความปลอดภัยของไฟล์ข้อมูลและแฟ้มข้อมูลจะทำการแบ่งข้อมูลเป็นบล็อคแล้วทำการเข้ารหัสข้อมูลโดยใช้โหมด CBC ก่อนที่จะทำการจัดเก็บ อย่างไรก็ตามการรักษาข้อมูลอาจเป็นเรื่องที่ยากเนื่องจากข้อมูลถูกจัดเก็บในเครื่องเซิร์ฟเวอร์ส่วนกลาง

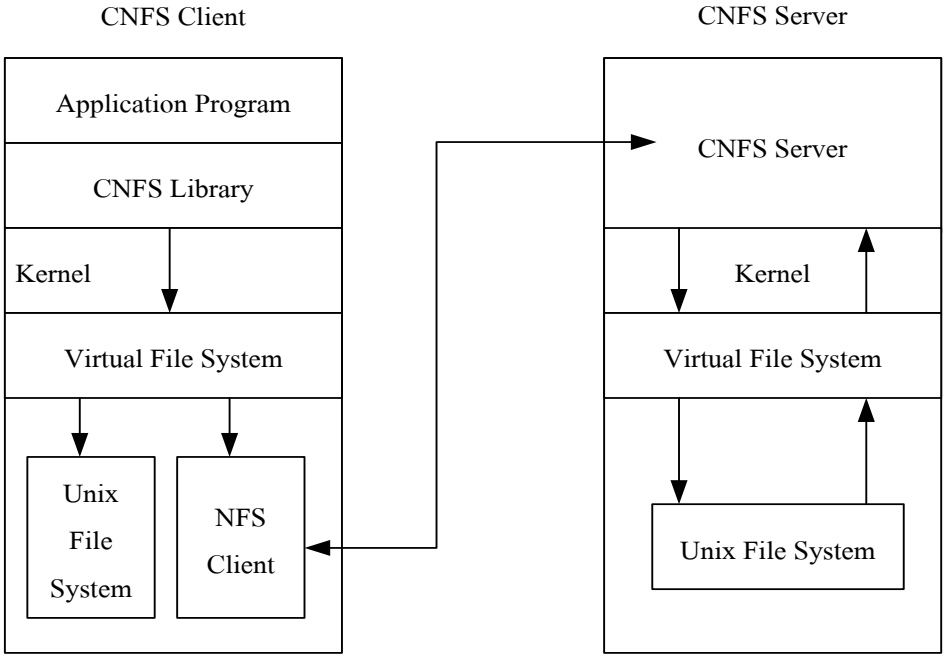
A. Harrington และ C. Jensen (2003) ได้นำเสนองานวิจัยเรื่อง Cryptographic access control in a distributed file system ซึ่งจัดเก็บข้อมูลด้วยสถาปัตยกรรมของระบบดังแสดงในภาพที่ 2.17 ระบบมีลักษณะการทำงานแบบไคลเอนต์ / เซิร์ฟเวอร์ โดยแบ่งการทำงานเป็นดังนี้

1) โครงสร้างการทำงานของฝั่งไคลเอ็นต์

ข้อมูลทั้งหมดจะถูกจัดเก็บไว้บนเซิร์ฟเวอร์โดยจะถูกเข้ารหัสจากฝั่งไคลเอ็นต์ก่อนที่จะมีการส่งผ่านเครือข่ายและไฟล์ข้อมูลที่อ่านจากเซิร์ฟเวอร์ฝั่งไคลเอ็นต์จะเป็นผู้รับผิดชอบในการตรวจสอบความถูกต้องและความสมบูรณ์ของข้อมูล

2) โครงสร้างการทำงานของฝั่งเซิร์ฟเวอร์

เซิร์ฟเวอร์ของระบบจะถูกออกแบบโดยเรียบง่ายที่สุดเท่าที่จะเป็นไปได้ โดยระบบการตรวจสอบความถูกต้องจะอยู่ทางฝั่งไคลเอ็นต์ ซึ่งเซิร์ฟเวอร์จะคอยให้บริการดิสก์สำหรับไคลเอ็นต์ที่ร้องขอ โดยโค๊ดหลักของ CNFS เซิร์ฟเวอร์จะถูกนำมากจาก NFS ลีนุกซ์เซิร์ฟเวอร์แต่การออกแบบมีความแตกต่างอย่างมีนัยสำคัญ โดยรูปแบบความล้มเหลวของ NFS ถือว่าเป็นการบริการที่ไร้รูปแบบและการดำเนินการไฟล์ทั้งหมดได้รับการออกแบบให้มีเหมือนกัน การทำงานของไฟล์เหล่านี้จะดำเนินการในหน่วยข้อมูลที่ตรงกับขนาดบล็อก NFS และเซิร์ฟเวอร์ NFS ไม่มีรูปแบบของไฟล์ที่เป็นหน่วยตรรกะในตัวของมันเอง



ภาพที่ 2.17 สถาปัตยกรรมการจัดเก็บไฟล์ข้อมูลตามรูปแบบ Client-Server

อย่างไรก็ตามในการจัดการคีย์จะไม่ได้กระทำในลักษณะของการกระจายซึ่งอาจทำให้ไม่มีความยืดหยุ่น

E.Geron และ A. Wool (2009) ได้นำเสนองานวิจัยเรื่อง Cryptographic remote untrusted storage without public keys โดยได้นำเสนอระบบการรักษาความปลอดภัยของระบบแฟ้มใหม่โดยใช้การเข้ารหัสคีย์แบบสมมาตรเพื่อให้ใช้ไฟล์ร่วมกันที่ปลอดภัยผ่านเซิร์ฟเวอร์ที่ไม่น่าเชื่อถือ โดยมีวัตถุประสงค์เพื่อป้องกันจากบุคคลที่สามโดยจะทำการสร้างคีย์ลับหลักขึ้นมาสองตัวคือ K และ K' การใช้คีย์และฟังก์ชันรหัสเทียมแบบสุ่ม $h(\cdot)$ ผู้ให้บริการคำนวณคีย์ที่เปลี่ยนแปลงของผู้ใช้แต่ละคนแทนค่าด้วย K_i และการตรวจสอบคีย์เฉพาะ K_i' โดยเขียนเป็นสมการได้ดังนี้

$$K_i = h(K\ ,\ i),\ K'_i = h(K'\ ,\ i)$$

ในทางปฏิบัติจะใช้อัลกอริทึม HMAC เนื่องจากเป็นฟังก์ชันรหัสเทียมแบบสุ่ม นอกจากนี้ฐานข้อมูลสาธารณะที่มีการเผยแพร่จากตัวแทนที่เชื่อถือได้ ซึ่งประกอบด้วยสองเมตทริกซ์แทนด้วย P และ A รวมทั้งคู่คีย์และคีย์ของการตรวจสอบความถูกต้องตามลำดับเขียนได้ดังสมการ

$$P_{i,j}=h(K_{i,j}) \oplus h(K_{j,i}),\ A_{i,j}=h(K_i^{'},h(K_{j,i}))$$

ผู้ใช้แต่ละคน i ที่ต้องการเข้ารหัสข้อมูลกับผู้ใช้ j คำนวณคีย์ลับที่ใช้ร่วมกัน $K_{i,j}$ กำหนดได้โดย

$$K_{i,j}=P_{i,j} \oplus h(K_{i,j})(=h(K_{i,j}))$$

ผู้ใช้ i สามารถตรวจสอบความถูกต้องของคีย์ได้

$$h(K_i^{'},K_{i,j})=A_{i,j}$$

ผู้ใช้ j สามารถถอดรหัสได้โดยการคำนวณ $K_{i,j}=h(K_{j,i})$ โดยไม่ต้องอ่านค่าเมตทริกซ์แต่ในกรณีนี้เมื่อเจ้าของไฟล์ผู้ใช้ i แบ่งปันไฟล์ให้กับผู้ใช้ j แล้วผู้ใช้ i สามารถสร้างกล่องล็อคสำหรับผู้ใช้ j ได้ในเมตาข้อมูลของไฟล์ โดยการใช้การเข้ารหัสคีย์ $K_{i,j}^{Enc}$ และตรวจสอบความถูกต้องโดยใช้ MAC สำหรับ $K_{i,j}^{MAC}$ จะได้

$$K_{i,j}^{Enc}=h(K_{i,j},\ "Enc"),\ K_{i,j}^{MAC}=h(K_{i,j},\ "MAC")$$

ในลักษณะเดียวกันผู้ใช้ j ใช้คีย์เหล่านี้ล้วนมาจาก $K_{i,j}$ ในกล่องล็อคจะมีเฉพาะเมตาข้อมูลของไฟล์ที่จำเป็นที่ผู้ใช้ j ต้องการเข้าถึงไฟล์ต่อไป

แม้ว่างานวิจัยนี้จะนำเสนอการรักษาความปลอดภัยของแฟ้มข้อมูลเพื่อให้ใช้งานร่วมกันผ่านเครือข่ายที่ไม่ปลอดภัยโดยการเข้ารหัสคีย์ลับแบบสมมาตรมาประยุกต์ใช้ประกอบกับการสร้างกล่องล็อคสำหรับข้อมูลระหว่างผู้ใช้แต่ละคน แต่ก็ยังมีข้อจำกัดในการนำไปใช้งานเนื่องจากในการสื่อสารปัจจุบันโดยส่วนเป็นการสื่อสารแบบกลุ่มในงานวิจัยของ E.Geron และ A. Wool นี้ยังไม่สามารถตอบสนองความต้องการทำงานร่วมกันแบบกลุ่มซึ่งอาจจะมีจำนวนสมาชิกที่มีความต้องการเข้าร่วมกลุ่มและออกจากกลุ่มสมาชิกได้ตลอดเวลาของการสื่อสาร

บทที่ 3

วิธีการวิจัย

ในบทนี้จะนำเสนอถึงแนวคิดและวิธีการจัดการคีย์กลุ่มตามข้อตกลงคีย์กลุ่ม Diffie-Hellman เพื่อเป็นแนวทางในการแลกเปลี่ยนคีย์สำหรับการสื่อสารแบบกลุ่มซึ่งมีจุดประสงค์ในการสื่อสารส่งข้อมูลระหว่างกันอย่างมีประสิทธิภาพ ในการออกแบบโปรโตคอลได้ให้ความสำคัญในการพิจารณาความปลอดภัยที่รวมถึงการรักษาความลับคีย์กลุ่ม การรักษาความลับของการส่งต่อ การรักษาความลับย้อนกลับ และความเป็นอิสระของคีย์โดยสมาชิกทุกคนจะมีส่วนร่วมในการคำนวณคีย์กลุ่ม โดยโปรโตคอลข้อตกลงการกระจายคีย์กลุ่มคือ Tree-based Group Diffie-Hellman (TGDH) โดยไม่จำเป็นต้องมี Group Controller เป็นผู้ดำเนินการจัดการคีย์กลุ่ม สำหรับกระบวนการเข้ารหัสระบบไฟล์ที่ใช้ร่วมกันระหว่างสมาชิกในกลุ่มจะกระทำได้โดยใช้การเข้ารหัสแบบสมมาตร ซึ่งจะใช้การเข้ารหัสลับแบบขั้นสูง Advanced Encryption Standard (AES) โดยใช้โหมด CBC

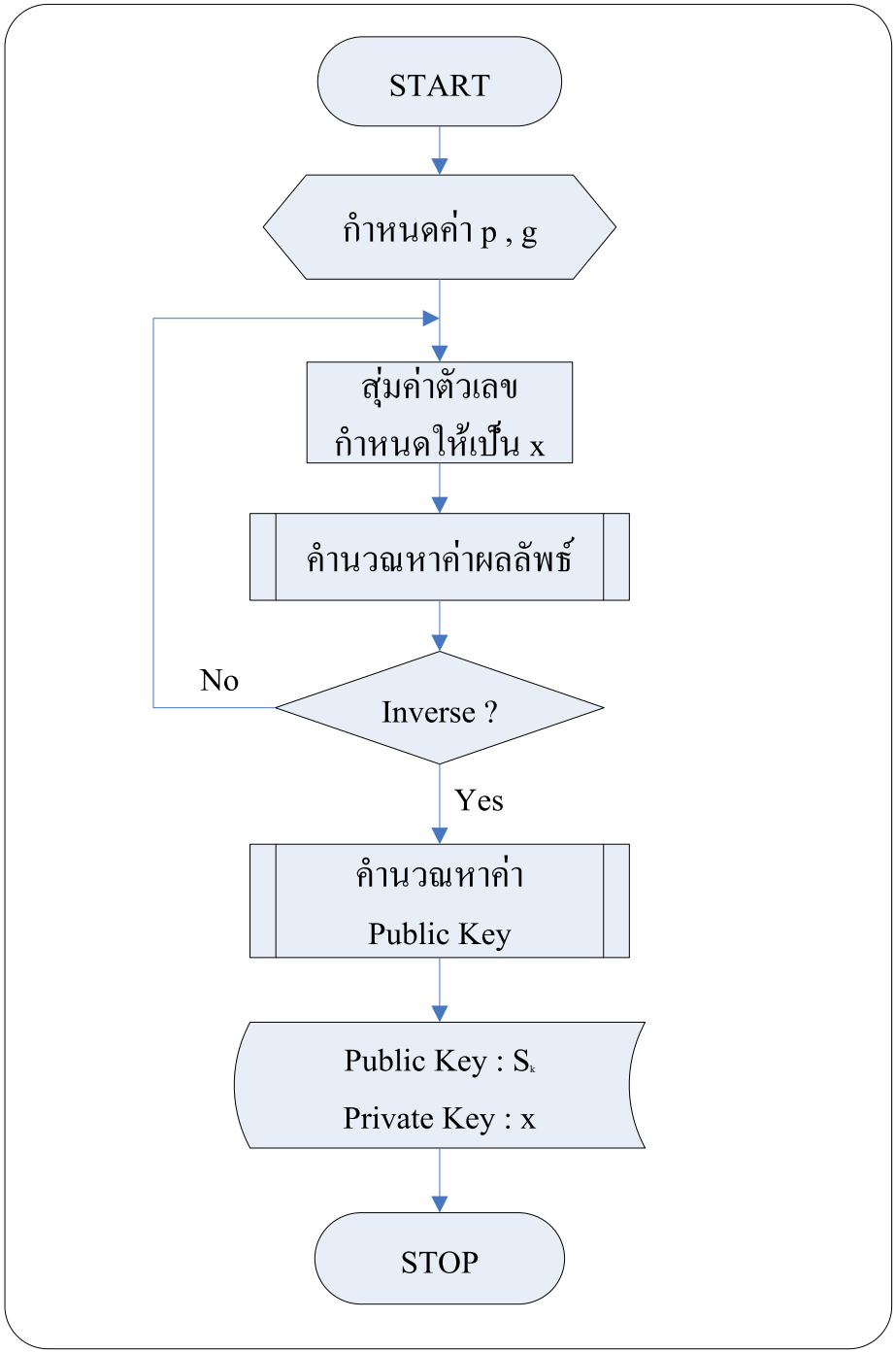
3.1 การเข้ารหัสคีย์กลุ่มตามข้อตกลง Diffie-Hellman

ในการสื่อสารข้อมูลระหว่างสมาชิกอย่างมีประสิทธิภาพและมุ่งเน้นในเรื่องความปลอดภัยของข้อมูล งานวิจัยนี้จึงนำเสนอวิธีการเข้ารหัสคีย์ที่กำหนดขึ้นก่อนการส่งข้อมูล เพื่อไม่ให้ผู้ที่ไม่ใช่สมาชิกของกลุ่มสามารถอ่านข้อมูลที่ถูกส่งเพื่อสื่อสารกันระหว่างสมาชิกได้ จึงใช้วิธีการเข้ารหัสลับของการกระจายคีย์กลุ่มตามข้อตกลงคีย์ของ Diffie-Hellman โดยในงานวิจัยนี้ได้นำโครงสร้างต้นไม้มาประยุกต์ใช้เพื่อให้การคำนวณคีย์เป็นไปได้อย่างรวดเร็ว โดยที่ไม่จำเป็นที่จะต้องมี Group Controller เป็นผู้ดำเนินการ กล่าวคือสมาชิกที่อยู่ภายในกลุ่มทุกคน สามารถที่ทำงานร่วมกันเพื่อคำนวณหาคีย์กลุ่มตามข้อตกลงของ Diffie-Hellman ตามโครงสร้างต้นไม้ โครงสร้างต้นไม้ที่ใช้ในงานวิจัยนี้จะมีลักษณะเป็น Binary Tree ที่โหนดใบคือสมาชิกแต่ละคนในกลุ่มและต้นไม้มีลักษณะเป็น Skew Tree ที่แต่ละระดับจะมีโหนดเพียง 2 โหนดเท่านั้น ขั้นตอนแรกคือกระบวนการเตรียมคีย์โดยแต่ละสมาชิก ที่จะกำหนดคีย์ส่วนตัวและคำนวณหาคีย์สาธารณะคู่หนึ่งของตนเอง หลังจากนั้นจึงส่งคีย์สาธารณะของตนให้กับคีย์เซิร์ฟเวอร์ กรณีที่สมาชิกต้องการร่วมกลุ่มสื่อสาร จะต้อง

ดำเนินการแสดงตัวตนด้วยคีย์สาธารณะที่ส่งมานั้น เมื่อคีย์เซิร์ฟเวอร์พิสูจน์ตัวตนของสมาชิกนั้นเรียบร้อยแล้ว จะดำเนินการกำหนดสิทธิเป็นสมาชิกของกลุ่มสื่อสารได้ กรณีที่สมาชิกต้องการแชร์ไฟล์ข้อมูลภายในกลุ่มก่อนการอัพโหลดไฟล์ข้อมูลจะถูกเข้ารหัสก่อนด้วยการเข้ารหัสแบบขั้นสูง Advanced Encryption Standard (AES) โดยใช้โหมด CBC

3.1.1 การเตรียมคีย์ของแต่ละสมาชิก

สมาชิกใด ๆ ที่อยู่ในกลุ่มสื่อสารจะต้องสร้างคีย์คู่หนึ่ง สำหรับเข้าและถอดรหัสลับเพื่อการติดต่อกับสมาชิกโดยเฉพาะ การกำหนดคีย์คู่นี้จะทำด้วยวิธี Diffie-Hellman ภาพที่ 3.1 แสดงขั้นตอนของการจัดเตรียมคีย์สำหรับสมาชิกแต่ละคนในกลุ่มสื่อสารโดยเมื่อสมาชิกในกลุ่มตกลงที่จะสื่อสารกันจะต้องกำหนดตัวเลขจำนวนเฉพาะให้มีค่ามาก ๆ (p) หนึ่งค่า และตัวเลขจำนวนใด ๆ (g) ที่เป็นค่าปฐมฐานของมอดูโล p (Primitive mod p) ให้กับกลุ่มสื่อสาร แต่ละสมาชิกจะสุ่มตัวเลขซึ่งมีค่ามาก ๆ มาค่าหนึ่งคือ x โดยตัวเลขที่สุ่มมานี้จำเป็นต้องเก็บรักษาเป็นความลับจากนั้นมาคำนวณหาค่า $g^x \ mod \ p$ จะได้ว่าแต่ละสมาชิกจะต้องเก็บรักษาคีย์หนึ่งสำหรับใช้ในการเข้าและถอดรหัสลับ คือ x ซึ่งเป็นคีย์ส่วนตัว (Private Key) ซึ่งต้องเก็บไว้เป็นความลับเพื่อใช้ในการถอดรหัสข้อความลับที่ส่งถึงตนและคำนวณคีย์สาธารณะ (Public Key) มีค่าเป็น $S_k = g^x \ mod \ p$ โดยค่าคีย์สาธารณะนี้จะเปิดเผยเพื่อให้ผู้ที่ต้องการส่งข้อความลับนำไปเข้ารหัสข้อความ โดยแต่ละสมาชิกจะส่งคีย์สาธารณะของตนเองให้คีย์เซิร์ฟเวอร์เพื่อให้สมาชิกอื่นทราบคีย์สาธารณะนี้ได้



ภาพที่ 3.1 การเตรียมคีย์ของแต่ละผู้ใช้ตามข้อตกลง Diffie-Hellman

3.2 การประยุกต์ใช้กับโครงสร้างต้นไม้

3.2.1 เริ่มต้นการทำงาน (การสร้างกลุ่มสมาชิกใหม่)

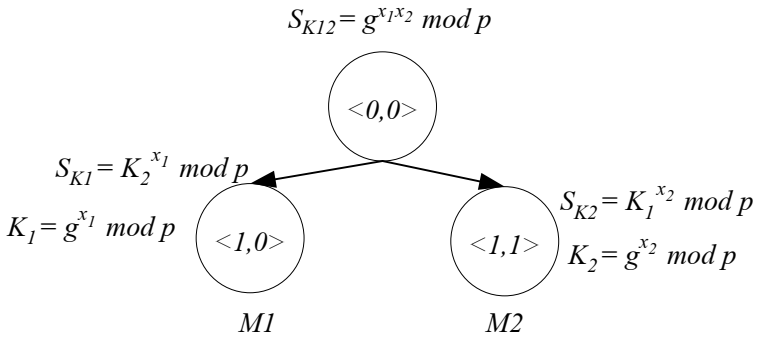
เมื่อสมาชิกทุกคนได้เตรียมคีย์สาธารณะและคีย์ส่วนตัวของตนและจัดเก็บไว้ในคีย์ทรีแล้ว กลุ่มสมาชิกจะสามารถสร้างขึ้นได้ ดังภาพที่ 3.2 แสดงกระบวนการสร้างกลุ่มสมาชิกใหม่ที่มีสมาชิกเริ่มต้นคือ M_1 และ M_2 ที่มีคีย์ส่วนตัวคือ x_1 และ x_2 ตามลำดับ ซึ่งความสัมพันธ์ระหว่างค่าที่คำนวณจาก $S_{K1} = K_2^{x_1} \bmod p$ กับ $S_{K2} = K_1^{x_2} \bmod p$ เมื่อคำนวณแล้วจะได้ค่าที่ตรงกัน และมีความสัมพันธ์กับสมการ $S_{K12} = g^{x_1 x_2} \bmod p$ ซึ่งเมื่อคำนวณแล้วจะมีค่าที่เท่ากันเช่นกันซึ่งสามารถสรุปได้คือ $S_{K1} = S_{K2} = S_{K12}$ โดยแสดงขั้นตอนการทำงานได้ดังนี้

ขั้นที่ 1 สมาชิกร่วมกันสุ่มค่าตัวเลขกำหนดให้เป็น p , g

ขั้นที่ 2 สมาชิกแต่ละคนสุ่มค่าตัวเลขขึ้นมาหนึ่งค่ากำหนดให้เป็น x ซึ่งค่านี้ต้องเก็บไว้เป็นความลับ

ขั้นที่ 3 สมาชิกคำนวณหาผลลัพธ์คีย์สาธารณะตามสมการ $g^x \bmod p$ โดยผลลัพธ์ที่ได้จะเก็บค่าไว้ส่งให้กับสมาชิกที่ต้องการสื่อสาร เพื่อใช้ในการเข้ารหัสข้อความ

ขั้นที่ 4 สมาชิกทุกคนร่วมกันคำนวณหาค่าของคีย์กลุ่มตามโครงสร้างต้นไม้ (จากโหนดใบสู่โหนดราก)



ภาพที่ 3.2 ตัวอย่างการคำนวณคีย์ของแต่ละโหนดสมาชิกเพื่อร่วมกันคำนวณคีย์กลุ่ม

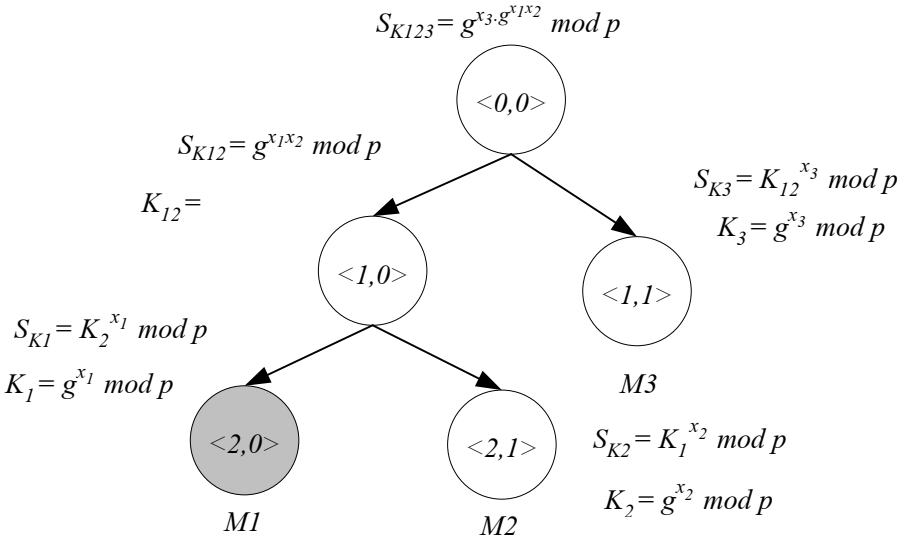
3.2.2 สมาชิกเข้าร่วมกลุ่ม (Member Join)

เมื่อมีสมาชิกใหม่ต้องการเข้าร่วมในกลุ่มสื่อสารปัจจุบันที่มี n สมาชิกอยู่ สมาชิกใหม่จะถูกแทนด้วย M_{n+1} เนื่องจากโครงสร้างต้นไม้ที่ใช้จะมีโหนดที่อยู่ในระดับเดียวกันเพียง 2 โหนด ทำให้สามารถเพิ่มโหนดใหม่ได้อย่างรวดเร็วโดยส่วนขยายโหนดใหม่นี้จะอยู่ด้านบนสุดของโครงสร้างต้นไม้ จากนั้นสมาชิกใหม่ M_{n+1} จะสามารถคำนวณคีย์ร่วมกับสมาชิกที่อยู่ในระดับเดียวกัน ภาพที่ 3.3 แสดงตัวอย่างโครงสร้างต้นไม้ก่อนที่สมาชิก M_4 เข้าร่วมกลุ่ม ภาพที่ 3.4 แสดงตัวอย่างโครงสร้างต้นไม้หลังจากที่สมาชิก M_4 เข้าร่วมกลุ่มแล้ว รายละเอียดขั้นตอนกระบวนการสมาชิกเข้าร่วมกลุ่มดังนี้

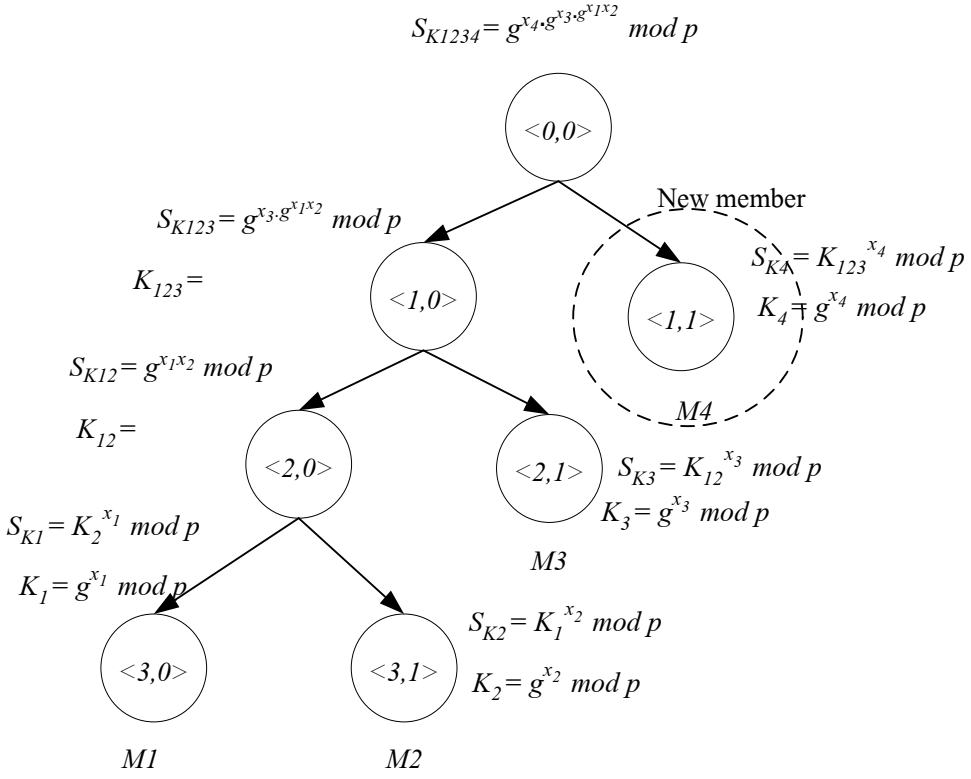
ขั้นที่ 1 สมาชิกใหม่ M_{n+1} สร้างโหนดใหม่ <0,0> ดังภาพที่ 3.4

ขั้นที่ 2 ปรับปรุงโหนดทุกโหนดโดยเพิ่มระดับขึ้นอีกหนึ่งระดับ

ขึ้นที่ 3 สมาชิกใหม่ทำการคำนวณคีย์ใหม่ตามโครงสร้างต้นไม้



ภาพที่ 3.3 ตัวอย่างกระบวนก่อนการจัดการคีย์กลุ่มกรณีสมาชิกเข้าร่วมกลุ่ม



ภาพที่ 3.4 ตัวอย่างกระบวนหลังการจัดการคีย์กลุ่มกรณีสมาชิก M_4 เข้าร่วมกลุ่มแล้ว

3.2.3 สมาชิกออกจากกลุ่ม (Member Leave)

ในกรณีที่มีสมาชิก M_i ต้องการออกจากกลุ่มสื่อสาร สมาชิกที่ได้รับการคำนวณคีย์กลุ่มใหม่จะต้องดำเนินการคำนวณคีย์กลุ่มใหม่และปรับปรุงโครงสร้างต้นไม้ดังตัวอย่างภาพที่ 3.5 แสดงตัวอย่างโครงสร้างต้นไม้ก่อนที่สมาชิก M_3 จะออกจากกลุ่มสื่อสาร โดยจะเกิดเหตุการณ์ประกอบด้วยกันอยู่ 2 กรณีดังภาพที่ 3.6 กรณีที่โหนดของสมาชิก M_5 ได้รับการคำนวณคีย์ซึ่งอยู่เหนือโหนดสมาชิกที่ออกจากกลุ่ม M_3 วิธีดำเนินการคือสมาชิก M_5 จะทำการปรับปรุงโครงสร้างต้นไม้โดยแทนตำแหน่งของตัวเองไปยังตำแหน่งสมาชิก M_3 ออกจากกลุ่มแล้วทำการคำนวณหาคีย์กลุ่มใหม่ตัวอย่างภาพที่ 3.7 แสดงตัวอย่างกรณีที่สมาชิกที่อยู่ด้านล่างของโหนดสมาชิกที่ออกเป็นผู้ดำเนินการคำนวณคีย์ใหม่วิธีการนี้สมาชิกสามารถปรับปรุงการคำนวณคีย์ใหม่ตามโครงสร้างต้นไม้ได้ทันที แสดงวิธีลำดับขั้นตอนการทำงานได้ดังนี้

ขั้นที่ 1 สมาชิกทุกคนตรวจสอบตำแหน่งของตนเองกับตำแหน่งของโหนดสมาชิกที่ออกจากกลุ่ม

กรณีมีโหนดอยู่เหนือโหนดสมาชิกที่ต้องการออกจากกลุ่มสื่อสาร

โหนดนั้นจะแทนตำแหน่งของตนเองไปยังตำแหน่งที่สมาชิกที่ออกจากกลุ่มและกลายเป็นตำแหน่งที่จะเริ่มการคำนวณคีย์กลุ่มใหม่

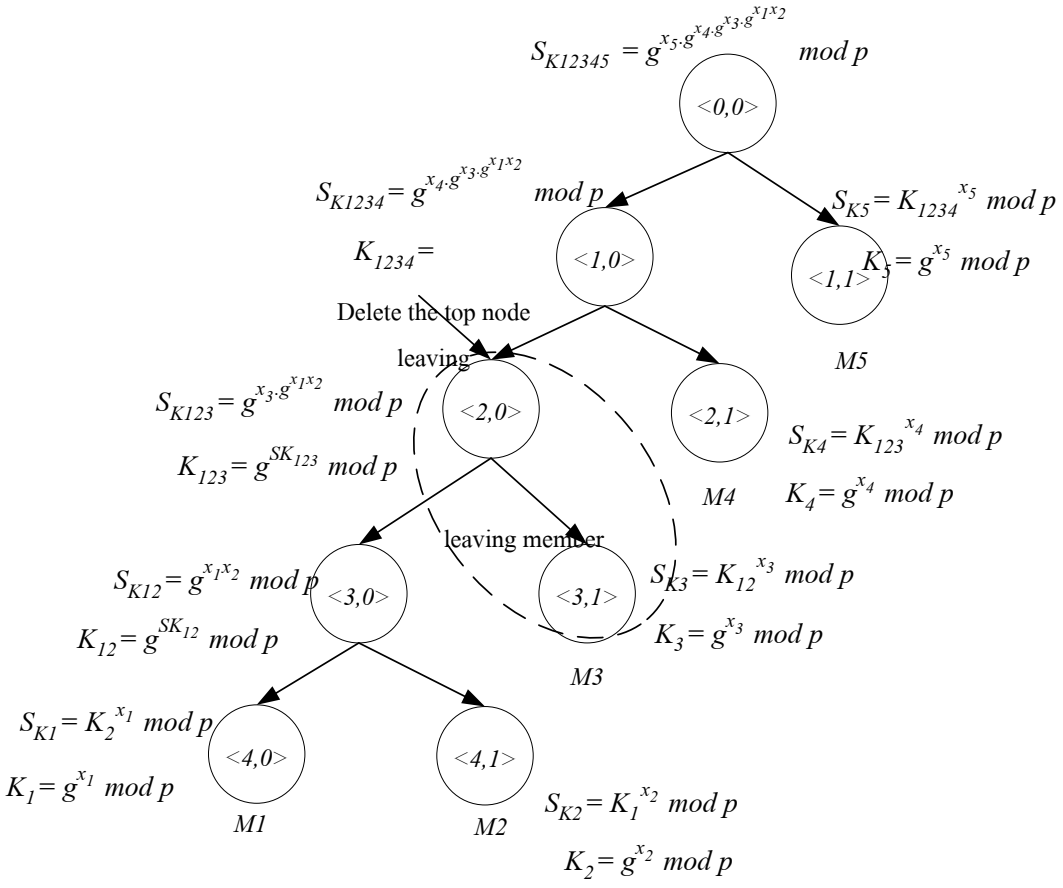
กรณีที่สมาชิกที่ต้องการออกจากกลุ่มสื่อสารเป็นโหนดราก

โหนดอยู่ด้านล่างโหนดที่ออกจากกลุ่มจะเป็นตำแหน่งที่จะเริ่มการคำนวณคีย์กลุ่มใหม่

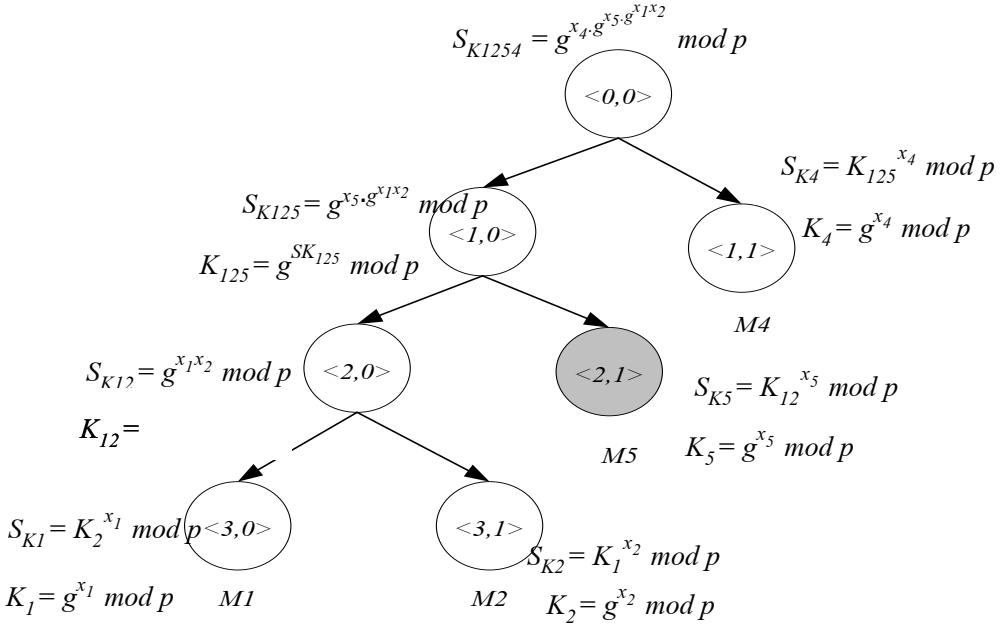
ขั้นที่ 2 สมาชิกลบโหนดที่อยู่เหนือสมาชิกที่ออกจากกลุ่ม

ขั้นที่ 3 สมาชิกปรับปรุงโครงสร้างต้นไม้ใหม่

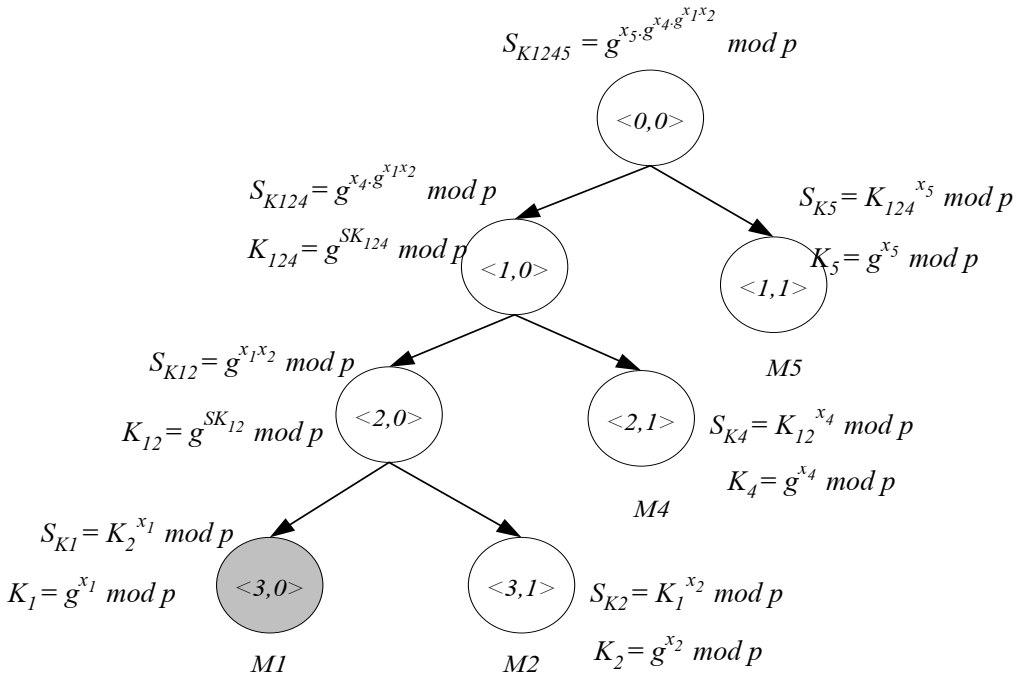
ขั้นที่ 4 สมาชิกทุกคนตั้งแต่ตำแหน่งของโหนดที่เริ่มการคำนวณคีย์กลุ่มใหม่ร่วมทำการคำนวณคีย์ใหม่ตามโครงสร้างต้นไม้



ภาพที่ 3.5 ตัวอย่างก่อนสมาชิก M_3 ออกจากกลุ่ม



ภาพที่ 3.6 ตัวอย่างหลังสมาชิก M_3 ออกจากกลุ่มกรณีสมาชิก M_5 เป็นผู้ดำเนินการ



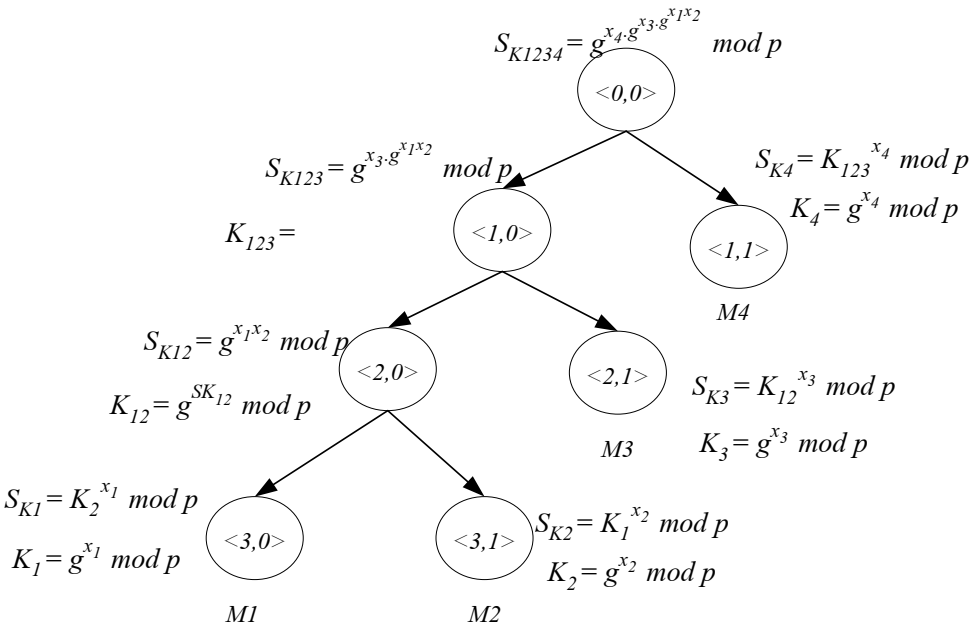
ภาพที่ 3.7 ตัวอย่างหลังสมาชิก M_3 ออกจากกลุ่มกรณีสมาชิก M_1 เป็นผู้ดำเนินการ

3.2.4 การรวมกลุ่ม (Group Merge)

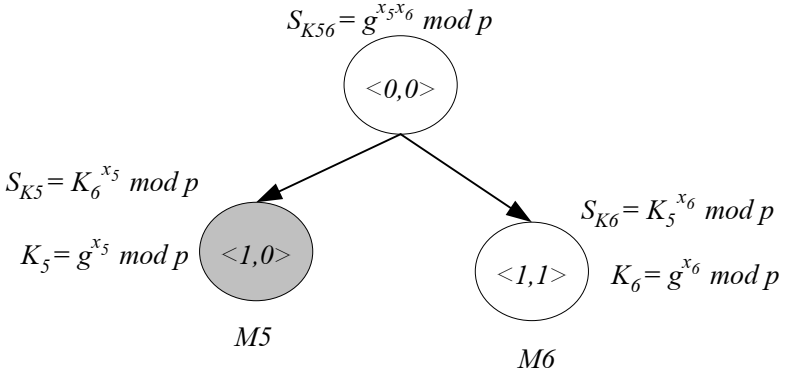
ในกรณีที่สมาชิกในกลุ่มสื่อสารบางคนต้องการเข้าร่วมสื่อสารกับสมาชิกอีกกลุ่มสื่อสาร สมาชิกที่ต้องการให้กลุ่มของตนเข้าร่วมกลุ่มจะดำเนินการปรับปรุงโครงสร้างสร้างต้นไม้คล้ายกับกรณีวิธีการเพิ่มโหนดสมาชิกใหม่ ภาพที่ 3.9 แสดงตัวอย่างโครงสร้างต้นไม้ของกลุ่มสมาชิก M_5 ที่ต้องการเข้าร่วมกลุ่มสื่อสารกับกลุ่มที่โครงสร้างต้นไม้ตามภาพที่ 3.8 สมาชิก M_5 จะทำการปรับปรุงโครงสร้างต้นไม้ของกลุ่มที่เข้าร่วมด้วย โดยการเพิ่มโหนดของสมาชิกในกลุ่มตนเองให้อยู่เหนือโหนดสมาชิกเดิมของกลุ่มที่จะเข้าร่วมด้วย ดังภาพที่ 3.10 การดำเนินการรวมกลุ่มประกอบด้วยขั้นตอนดังนี้

ขั้นที่ 1 สมาชิกที่ต้องการรวมกลุ่มปรับปรุงโครงสร้างต้นไม้โดยปรับปรุงต้นไม้ของกลุ่มจะเข้าร่วมด้วย โดยเพิ่มโหนดของสมาชิกในกลุ่มตนเองให้อยู่เหนือโหนดสมาชิกทั้งหมดในกลุ่มที่จะเข้าร่วมด้วย

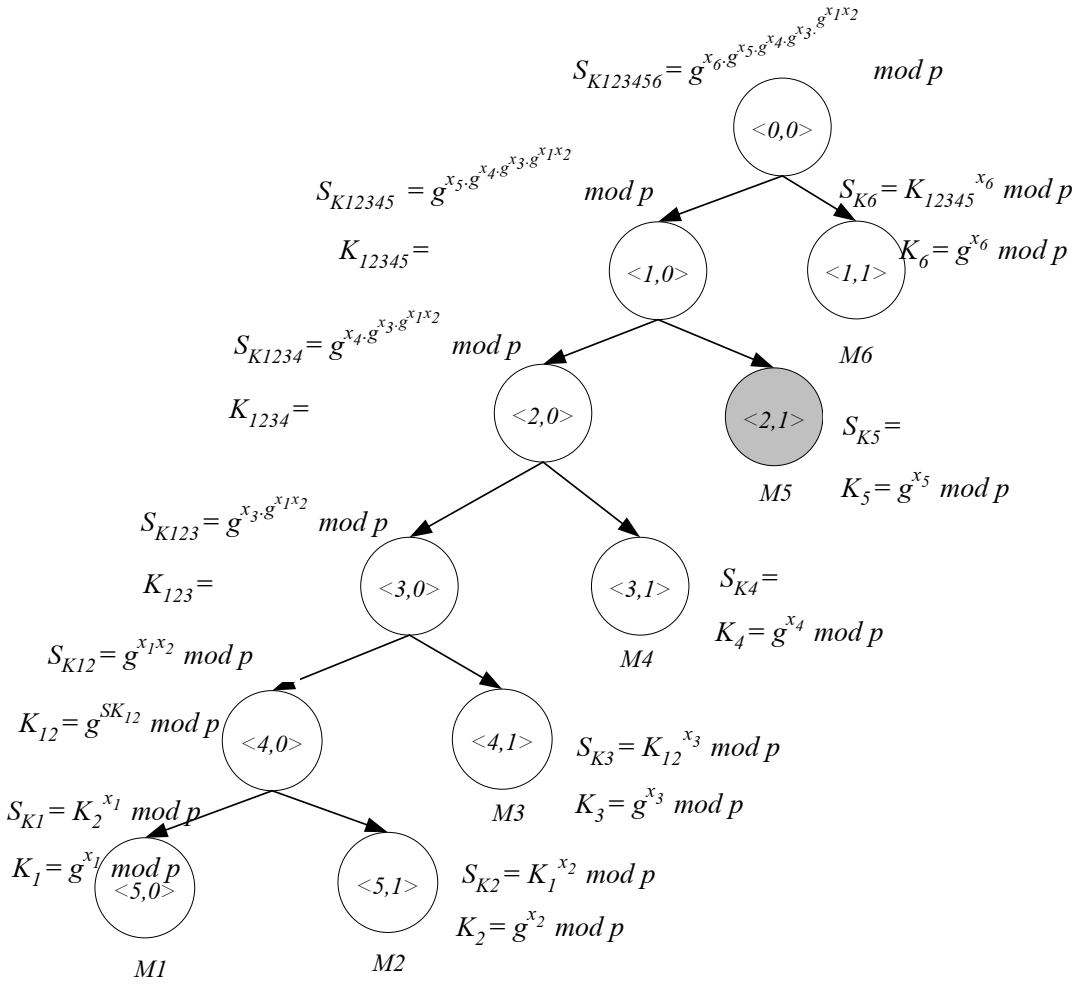
ขั้นที่ 2 สมาชิกทุกคนในกลุ่มที่ต้องการรวมกลุ่มร่วมกันคำนวณหาคีย์กลุ่มใหม่ตามโครงสร้างต้นไม้



ภาพที่ 3.8 ตัวอย่างโครงสร้างต้นไม้ปัจจุบันก่อนรวมกลุ่ม



ภาพที่ 3.9 ตัวอย่างโครงสร้างต้นไม้ที่ต้องการรวมกลุ่ม



ภาพที่ 3.10 ตัวอย่างโครงสร้างต้นไม้หลังการรวมกลุ่ม

3.2.5 การแยกกลุ่ม (Group Partition)

ในกรณีที่มีสมาชิกในกลุ่มต้องการแยกกลุ่มการสื่อสารสมาชิกคนขึ้นจะทำหน้าที่ปรับปรุงโครงสร้างต้นไม้โดยทำการลบสมาชิกที่ต้องการแยกออกและทำการสร้างโครงสร้างของต้นไม้ของกลุ่มสมาชิกใหม่นี้แยกตัวออกไป ภาพที่ 3.11 แสดงตัวอย่างสมาชิก M_3 และสมาชิก M_5 ต้องการแยกออกจากกลุ่มสื่อสารใหม่ กรณีนี้สมาชิก M_3 ถูกเลือกให้เป็นผู้ดำเนินการปรับปรุงโครงสร้างต้นไม้เนื่องจากเป็นโหนดที่อยู่ล่างสุดที่แยกตัวออกไปเป็นอีกกลุ่ม ดังภาพที่ 3.12 แสดงตัวอย่างการแยกกลุ่มกรณีที่ M_3 เป็นผู้ดำเนินการ จากภาพที่ 3.12 M3 จะเป็นตำแหน่งของโหนดที่เริ่มการคำนวณคีย์รวมของกลุ่มใหม่ที่ตนเป็นสมาชิกในขณะนี้ M4 จะเป็นตำแหน่งของโหนดที่เริ่มการคำนวณคีย์รวมของอีกกลุ่ม ในขณะที่ภาพที่ 3.13 กรณีที่สมาชิก M_6 เป็นผู้ดำเนินการในการแยกกลุ่มก็จะปรับปรุงตำแหน่งของสมาชิกเองให้อยู่ในตำแหน่งโหนดด้านซ้ายของสมาชิกในกลุ่ม

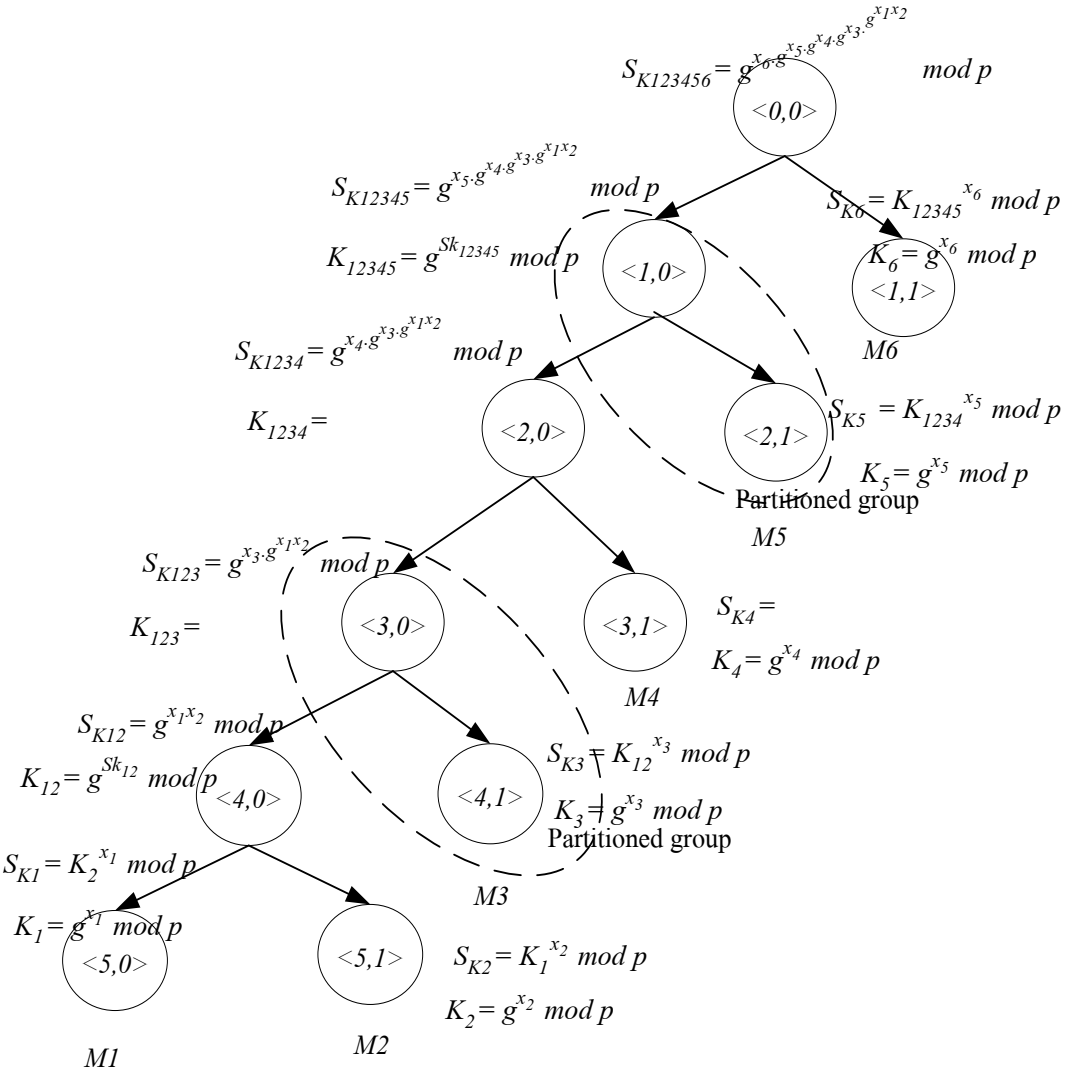
กลุ่มสื่อสารเดิมสมาชิกที่เป็นผู้ดำเนินการกรณีที่อยู่เหนือโหนดสมาชิกที่แยกออกจากกลุ่มสื่อสารจะดำเนินการปรับปรุงโครงสร้างต้นไม้โดยการปรับปรุงตำแหน่งของตนเองให้มาแทนตำแหน่งของสมาชิกที่ออกจากกลุ่มดังภาพที่ 3.14 แสดงตัวอย่างกรณีสมาชิก M_6 เป็นผู้ดำเนินการปรับปรุงโครงสร้างต้นไม้โดยการแทนตำแหน่งของสมาชิก M_3 ซึ่งได้ออกจากกลุ่มจากนั้นสมาชิกจะทำการปรับปรุงโครงสร้างต้นไม้เพื่อให้สมาชิกสามารถคำนวณคีย์กลุ่มตามโครงสร้างต้นไม้ในขณะที่สมาชิกที่ได้รับการดำเนินอยู่ต่ำกว่าโหนดที่ต้องการแยกกลุ่มจะสามารถปรับปรุงโครงสร้างต้นไม้และคำนวณคีย์ตามโครงสร้างต้นไม้ได้ดังภาพที่ 3.15 แสดงตัวอย่างกรณีที่สมาชิก M_1 เป็นผู้ดำเนินการในการปรับปรุงโครงสร้างต้นไม้ ลำดับขั้นตอนการแยกกลุ่มมีดังนี้

ขั้นที่ 1 สมาชิกที่ต้องการแยกกลุ่มสื่อสารแยกกลุ่มสื่อสารออกจากกลุ่มปัจจุบัน

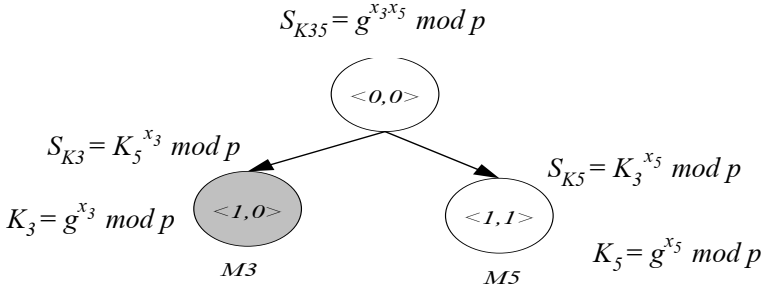
ขั้นที่ 2 สมาชิกที่เป็นผู้ดำเนินการปรับปรุงโครงสร้างต้นไม้กลุ่มใหม่ โดยปรับปรุงตำแหน่งของสมาชิกผู้ดำเนินการให้อยู่ทางด้านซ้ายของโครงสร้างต้นไม้

ขั้นที่ 3 สมาชิกในกลุ่มปัจจุบันปรับปรุงโครงสร้างต้นไม้ กรณีที่สมาชิกที่เป็นผู้ดำเนินการอยู่เหนือโหนดสมาชิกที่แยกกลุ่มให้ปรับปรุงตำแหน่งของสมาชิกไปยังตำแหน่งของสมาชิกที่แยกออกจากกลุ่มสื่อสาร

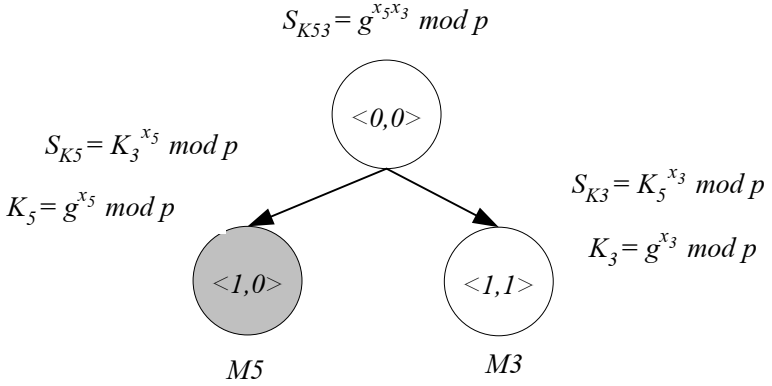
ขั้นที่ 4 สมาชิกทุกคนคำนวณคีย์กลุ่มใหม่ตามโครงสร้างต้นไม้



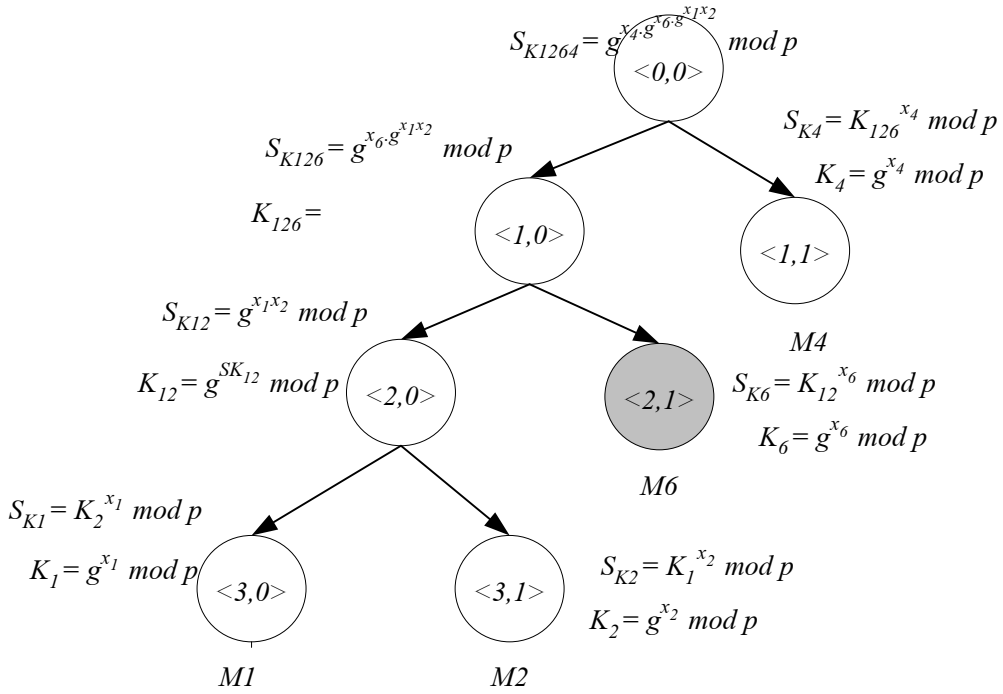
ภาพที่ 3.11 ตัวอย่างโครงสร้างต้นไม้ก่อนการแบ่งกลุ่ม



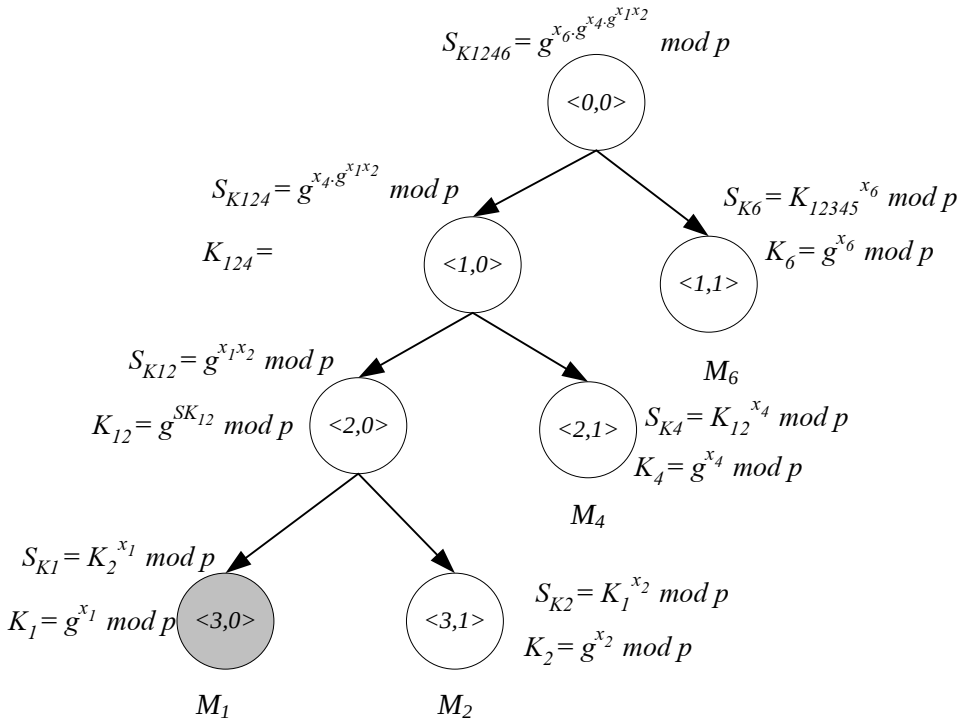
ภาพที่ 3.12 ตัวอย่างหลังการแบ่งกลุ่มกรณี M_3 เป็นผู้ดำเนินการ



ภาพที่ 3.13 ตัวอย่างหลังการแบ่งกลุ่มกรณี M_5 เป็นผู้ดำเนินการ



ภาพที่ 3.14 ตัวอย่างหลังการแบ่งกลุ่มกรณี M_6 เป็นผู้ดำเนินการ



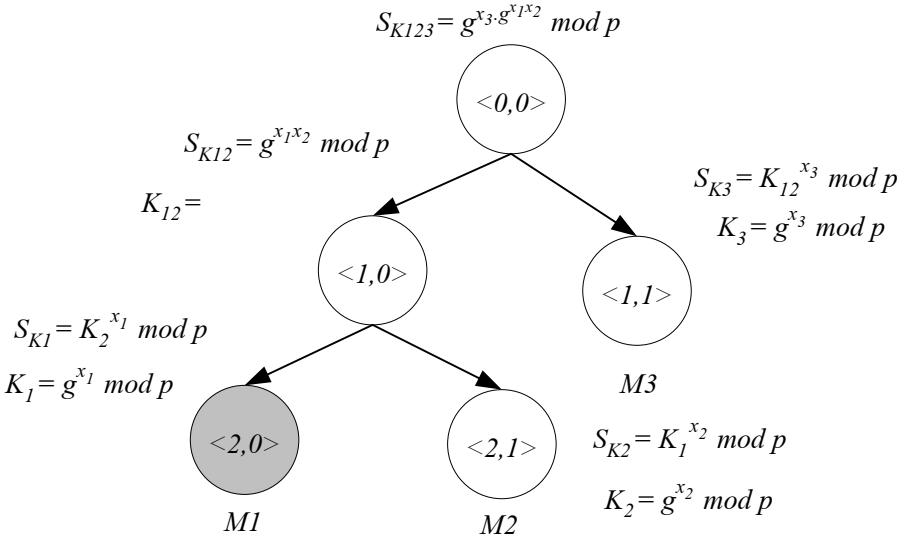
ภาพที่ 3.15 ตัวอย่างหลังการแบ่งกลุ่มกรณี M_1 เป็นผู้ดำเนินการ

3.2.6 Key Refresh

ในการพัฒนาระบบกรณีที่เมื่อการดำเนินของสมาชิกในกลุ่มมีการเปลี่ยนแปลงเหตุการณ์อะไรบางอย่างเกิดขึ้น ดังภาพที่ 3.16 กรณีที่มีสมาชิก M_1 เปลี่ยนแปลงคีย์ส่วนตัว (Private Key) สมาชิกภายในกลุ่มทุกคนจะต้องคำนวณหาคีย์กลุ่มใหม่เพื่อความปลอดภัยในการสื่อสารกลุ่ม โดยสมาชิกที่ดำเนินการเปลี่ยนแปลงคีย์ส่วนตัวจะต้องเป็นผู้ดำเนินการขั้นตอนการในการคำนวณคีย์ใหม่ตามโครงสร้างต้นไม้สำหรับสมาชิกภายในกลุ่ม โดยขั้นตอนการทำงานสามารถแสดงได้ดังต่อไปนี้

ขั้นที่ 1 เมื่อสมาชิกในกลุ่มเปลี่ยนแปลงคีย์ส่วนตัว (Private Key) จะทำการคำนวณหาคีย์ใหม่แล้วกระจายคีย์ให้กับสมาชิกภายในกลุ่มเพื่อคำนวณหาคีย์กลุ่มใหม่ตามโครงสร้างต้นไม้

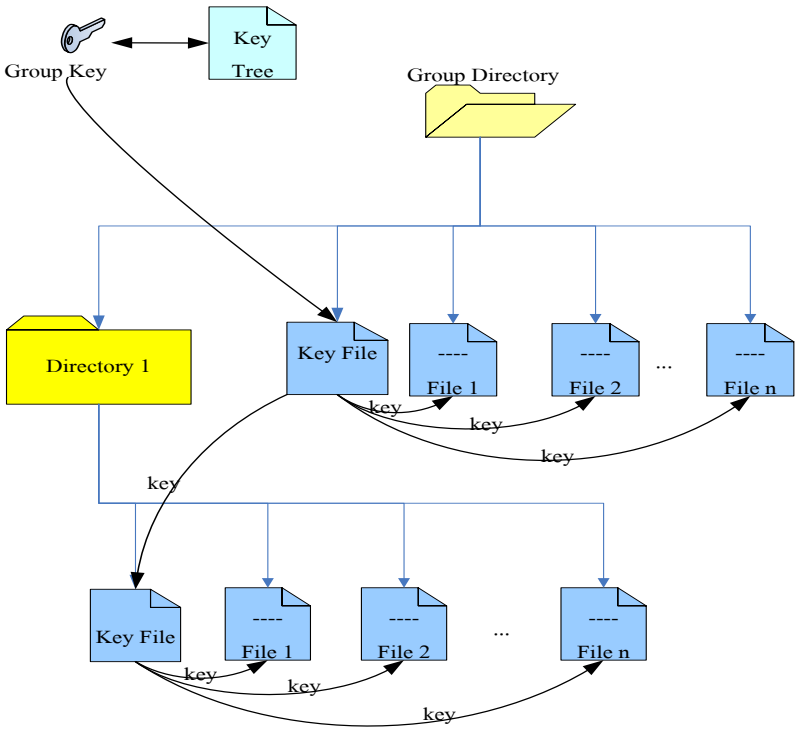
ขั้นที่ 2 สมาชิกทุกคนร่วมกันคำนวณหาคีย์กลุ่มใหม่ตามโครงสร้างต้นไม้



ภาพที่ 3.16 ตัวอย่างเมื่อสมาชิก M_1 เปลี่ยนแปลงคีย์

3.3 โครงสร้างไฟล์ข้อมูลภายในกลุ่ม

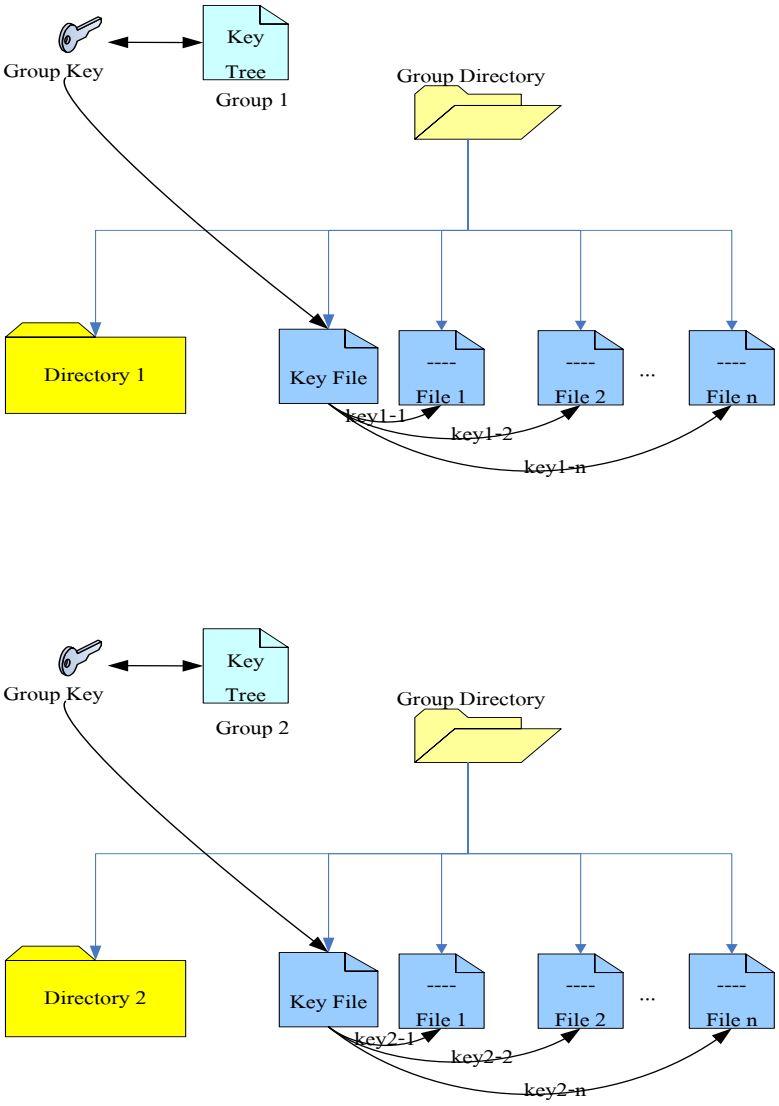
ในการสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆนั้นข้อมูลที่จัดเก็บจะถูกเข้ารหัสไว้โดยกระบวนการเข้ารหัสข้อมูลแบบขั้นสูง AES ในโหมด CBC โดยแต่ละไฟล์จะมีคีย์สำหรับเข้ารหัสและถอดรหัสข้อมูลของตนเอง ซึ่งคีย์ของทุกไฟล์ในไดเร็กทอรี่จะถูกเก็บอยู่คีย์ไฟล์ คีย์ไฟล์นี้จะถูกเข้ารหัสด้วยคีย์กลุ่มอีกครั้งหนึ่งเพื่อความปลอดภัยในการสื่อสารข้อมูลกลุ่ม สมาชิกภายในกลุ่มสามารถใช้คีย์กลุ่มเปิดดูคีย์ไฟล์ที่อยู่ภายในไดเร็กทอรี่หลักได้ ซึ่งในไดเร็กทอรี่หลักอาจจะมีไฟล์ซึ่งสามารถทำการเปิดโดยใช้คีย์ที่เก็บอยู่ในคีย์ไฟล์ดังที่ได้อธิบายข้างต้น สำหรับไฟล์ที่จัดเก็บอยู่ในไดเร็กทอรี่ย่อยอีกลำดับหนึ่ง ในไดเร็กทอรี่ย่อยก็จะประกอบด้วยคีย์ไฟล์ที่ใช้จัดเก็บคีย์สำหรับเข้ารหัสและถอดรหัสของไฟล์ที่อยู่ในไดเร็กทอรี่ย่อยนั้น ส่วนคีย์ไฟล์ที่อยู่ในไดเร็กทอรี่ย่อยนี้จะถูกเข้ารหัสด้วยคีย์ไดเร็กทอรี่ซึ่งเก็บอยู่ในคีย์ไฟล์ที่อยู่บนไดเร็กทอรี่ด้านบน ภาพที่ 3.17 แสดงตัวอย่างลำดับขั้นตอนการเข้ารหัสไฟล์ข้อมูลสำหรับการสื่อสารกลุ่ม



ภาพที่ 3.17 ตัวอย่างลำดับขั้นการเข้ารหัสข้อมูลสำหรับกลุ่ม

3.3.1 การจัดการไฟล์ข้อมูลเมื่อมีการแยกกลุ่ม

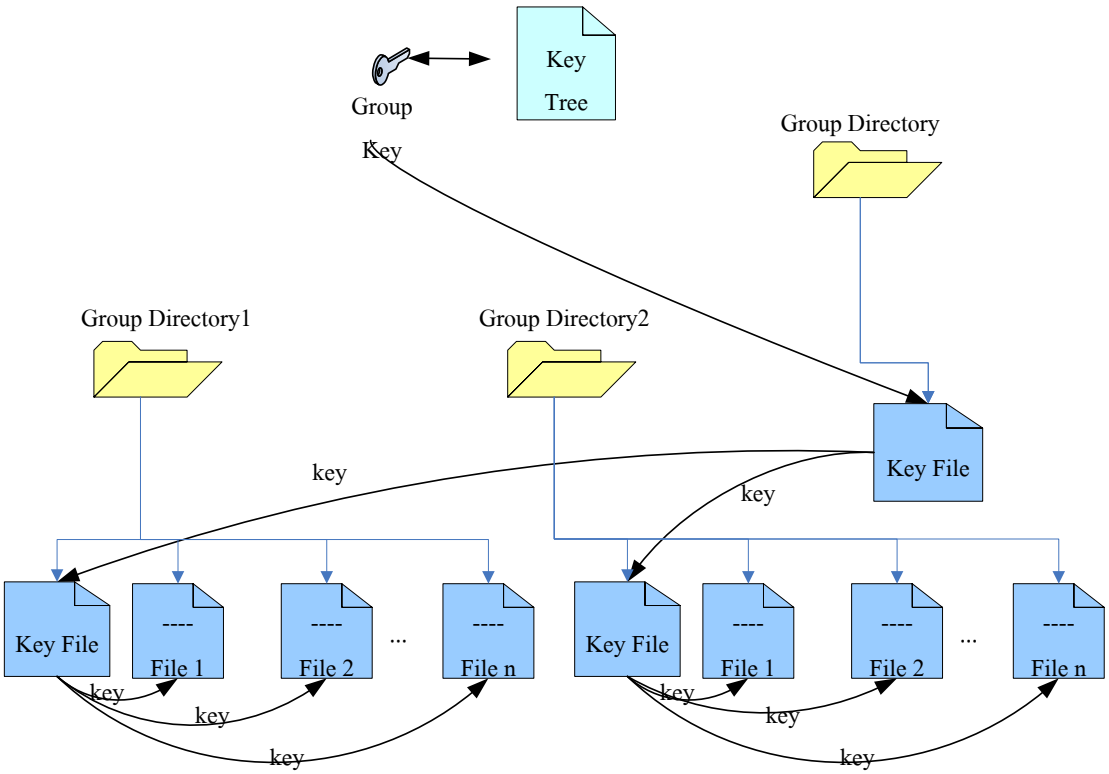
กรณีที่สมาชิกภายในกลุ่มต้องการแยกกลุ่มสื่อสารออกเป็นกลุ่มย่อยสมาชิกสามารถแยกไฟล์ข้อมูลออกจากกลุ่มเดิมโดยการแยก Group Directory ออกเป็น 2 Directories ซึ่งคีย์ไฟล์ของแต่ละ Directory จะถูกเข้ารหัสด้วยคีย์กลุ่มของตนเอง ตัวอย่างการจัดการไฟล์ข้อมูลเมื่อมีการแยกกลุ่มแสดงให้เห็นในภาพที่ 3.18



ภาพที่ 3.18 ตัวอย่างโครงสร้างไฟล์กรณีที่สมาชิกแยกกลุ่ม

3.3.2 การจัดการไฟล์ข้อมูลเมื่อมีการรวมกลุ่ม

กรณีที่สมาชิกต้องการรวมกลุ่มสื่อสาร ไฟล์ข้อมูลเดิมของแต่ละกลุ่มที่มีการรวมกลุ่มจะต้องสามารถเข้าถึงได้โดยสมาชิกทั้งหมดในกลุ่มที่ได้รวมกันแล้วจะต้องสร้าง Group Directory ขึ้นมาใหม่สำหรับกลุ่มใหม่ที่เกิดจากการรวมกลุ่มสมาชิกเข้าด้วยกัน Group Directory ใหม่นี้จะประกอบไปด้วยคีย์ไฟล์ซึ่งไฟล์นี้จะเก็บคีย์ต่าง ๆ ที่ใช้เข้ารหัสคีย์ไฟล์เดิมของกลุ่มสมาชิกที่รวมเข้าด้วยกัน คีย์ไฟล์ของกลุ่มใหม่นี้จะถูกเข้ารหัสด้วยคีย์กลุ่มนี้สร้างขึ้นหลังรวมกลุ่มซึ่งรวมเข้าด้วยกัน ตัวอย่างการปรับโครงสร้างไฟล์เมื่อมีการรวมกลุ่มสมาชิก สามารถแสดงได้ดังภาพที่ 3.19



ภาพที่ 3.19 ตัวอย่างโครงสร้างไฟล์กรณีรวมกลุ่มสมาชิก

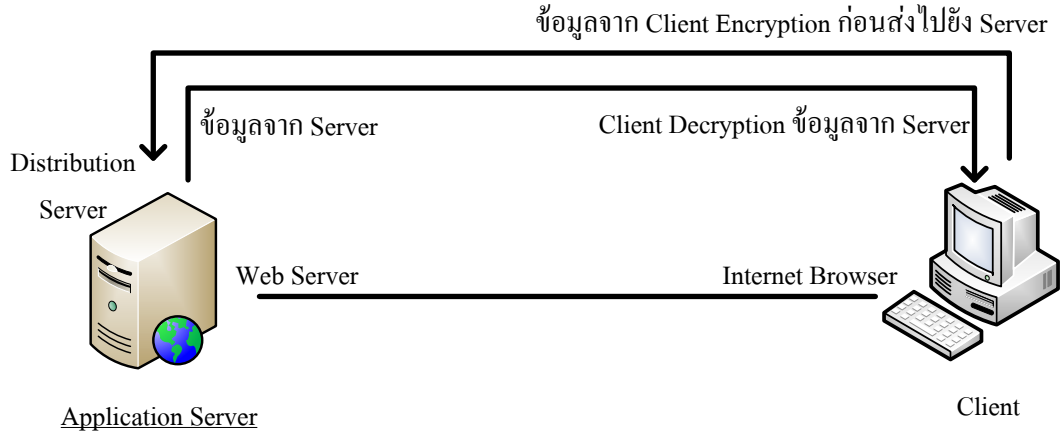
บทที่ 4

การพัฒนาระบบต้นแบบ

ในการพัฒนาระบบต้นแบบเมื่อสมาชิกทุกคนที่ติดต่อสื่อสารกันสามารถใช้ไฟล์ข้อมูลร่วมกันนั้นจะมุ่งเน้นในเรื่องความปลอดภัยของข้อมูล เพื่อป้องกันไม่ให้ผู้ที่ไม่ใช่สมาชิกของกลุ่มสามารถดูไฟล์ข้อมูลที่ใช้ร่วมกันระหว่างสมาชิกในกลุ่มสื่อสารได้โดยใช้วิธีการเข้ารหัสลับตามข้อตกลงคีย์ของ Diffie-Hellman และใช้โครงสร้างแบบต้นไม้มาช่วยในการคำนวณหาคีย์กลุ่ม กระบวนในระบบประกอบด้วย กระบวนการเริ่มต้น กระบวนการสมาชิกเข้าร่วม กระบวนการสมาชิกออกจากกลุ่ม กระบวนการรวมกลุ่ม กระบวนการแยกกลุ่ม และกระบวนการคีย์รีเฟรช

4.1 กระบวนการทำงาน

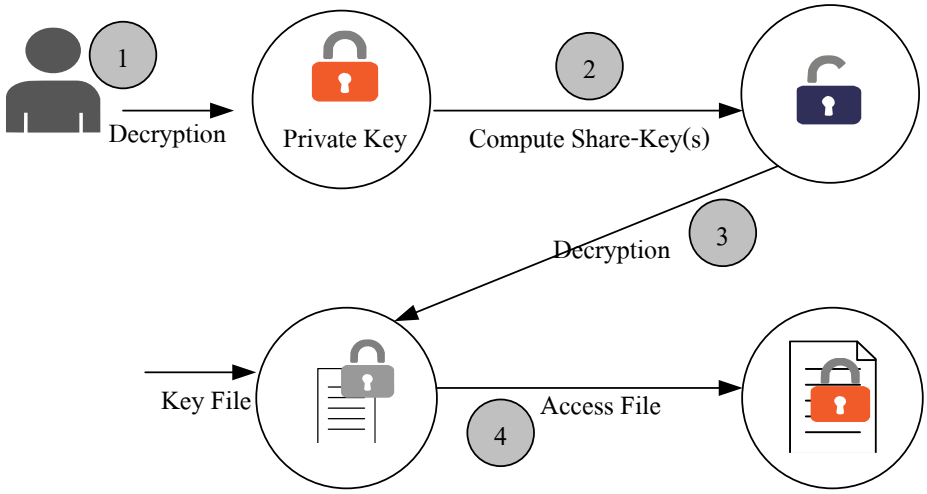
เนื่องจากระบบ Cloud Computing เป็นระบบที่มีโครงสร้างขนาดใหญ่มากและมีการลงทุนค่อนข้างสูง การทดลองพัฒนาระบบในงานวิจัยนี้จึงไม่สามารถกระทำบนระบบ Cloud Computing จริงได้ จึงจำเป็นที่จะต้องจำลองระบบบนเครื่องคอมพิวเตอร์แม่ข่าย Server ที่มีขนาดเล็กลงเพื่อใช้ในการทดสอบการทำงาน การสร้างระบบต้นแบบจะใช้ภาษาพีเอชพี (PHP Programming Language) ในการพัฒนา โดยประกอบกับภาษาจาวาสคริปต์ (JavaScript Language) จัดเก็บข้อมูลด้วยฐานข้อมูลมายเอสคิวแอล (MySQL Database) การพัฒนาระบบจะใช้รูปแบบโปรแกรมเว็บบราวเซอร์โดยมีกระบวนการทำงานดังนี้



ภาพที่ 4.1 แสดงลักษณะการทำงานของระบบ

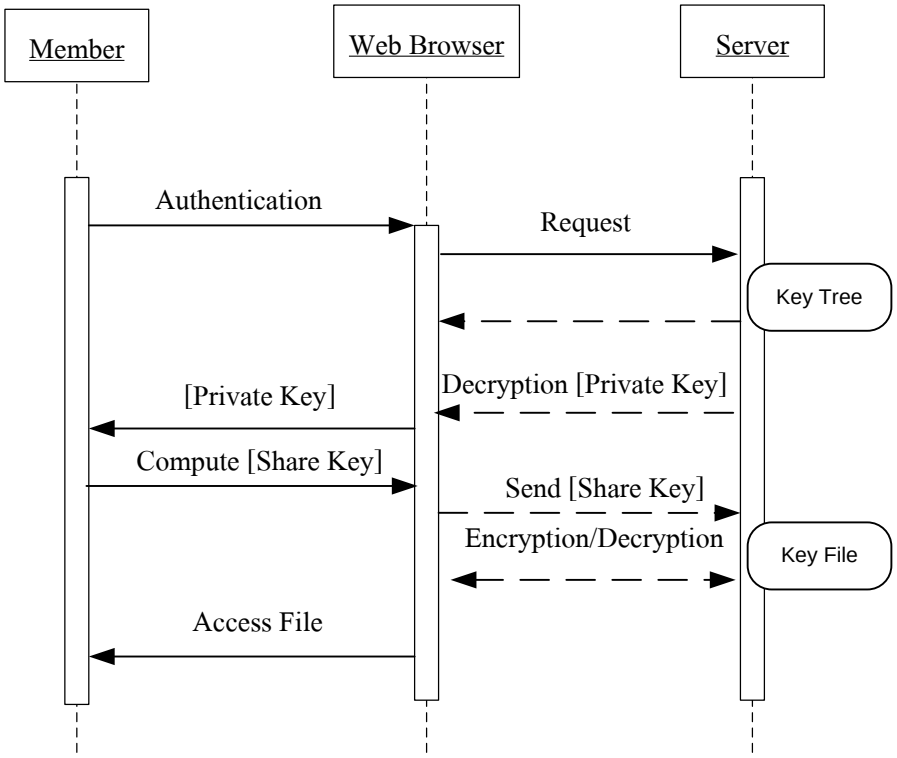
4.1.1 เริ่มต้นการทำงาน

ในกระบวนการเริ่มต้นการทำงาน สมาชิกที่อยู่ในกลุ่มสื่อสารสมาชิกจะได้รับคีย์คู่หนึ่ง เพื่อใช้เข้ารหัสและถอดรหัสลับสำหรับการสร้างคีย์กลุ่ม โดยสมาชิกเริ่มต้นจะทำการกำหนดตัวเลขเฉพาะให้มีค่ามากขึ้นมาหนึ่งค่า (p) และตัวเลขจำนวนที่เป็นค่าปฐมฐานของมอดูโล p แทนด้วย g (Primitive mod p) ให้สำหรับกลุ่มสื่อสาร สมาชิกแต่ละคนจะต้องสุ่มค่าตัวเลขขึ้นมาหนึ่งค่าคือ x (Private Key) โดยค่านี้สมาชิกจะเก็บไว้เป็นความลับเพื่อใช้ในเข้ารหัสและถอดรหัส ซึ่งในการเข้ารหัสสามารถคำนวณหาค่าตามสมการ $g^x \ mod \ p$ ซึ่งสมาชิกในกลุ่มก็จะคำนวณหาค่าคีย์ลับส่วนตัวเช่นกัน หลังจากนั้นจะทำการคำนวณหาค่าคีย์สาธารณะ (Public Key) ตามสมการ $S_k = g^x \ mod \ p$ เพื่อส่งค่าที่คำนวณได้ไปยังสมาชิกที่ต้องการสื่อสารเพื่อใช้ในการเข้ารหัสข้อความต่อไป ซึ่งกระบวนการที่สมาชิกคำนวณคีย์จะเกิดขึ้นเมื่อสมาชิกเริ่มต้นเข้าสู่ระบบโดยกระบวนการคำนวณคีย์ส่วนตัวและคีย์ต่าง ๆ จะเกิดขึ้นที่ส่วนของสมาชิก Client Side เมื่อคำนวณคีย์ต่าง ๆ ได้แล้วจะทำการเข้ารหัสคีย์ส่วนตัวไว้ และทำการแชร์คีย์ที่ได้จากการคำนวณให้กับสมาชิกที่ต้องการสื่อสารต่อไปแสดงกระบวนการทำงานได้ ภาพที่ 4.2 แสดงขั้นตอนกระบวนการเริ่มต้นการทำงานของสมาชิกแต่ละคน

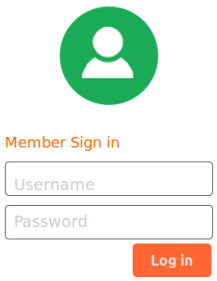


ภาพที่ 4.2 กระบวนการเริ่มต้นทำงาน

การทำงานในช่วงเริ่มต้นของสมาชิกเมื่อสมาชิกยืนยันตัวตนแล้วสมาชิกจะนำรหัสผ่านของตนเองเพื่อถอดรหัสคำนวณหาคีย์ส่วนตัวของตนเอง เมื่อสมาชิกได้รับคีย์ส่วนตัวแล้วจะทำการคำนวณหาคีย์สาธารณะเพื่อใช้สำหรับแลกเปลี่ยนการสื่อสารกรณีต้องการสื่อสารกับสมาชิกคนอื่น โดยสมาชิกจะใช้คีย์สาธารณะเพื่อถอดรหัสข้อมูลจาก Key File ดังภาพที่ 4.3 และภาพที่ 4.4 แสดงขั้นตอนเริ่มต้นการทำงานของสมาชิกทุกคน



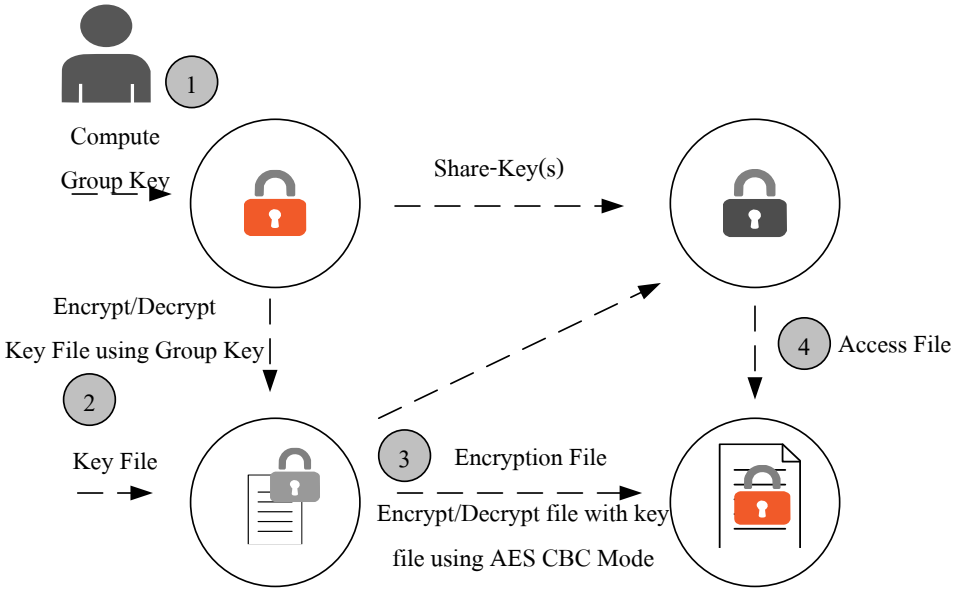
ภาพที่ 4.3 Sequence Diagram ของสมาชิกทุกคน



ภาพที่ 4.4 โปรแกรมเริ่มต้นของสมาชิก

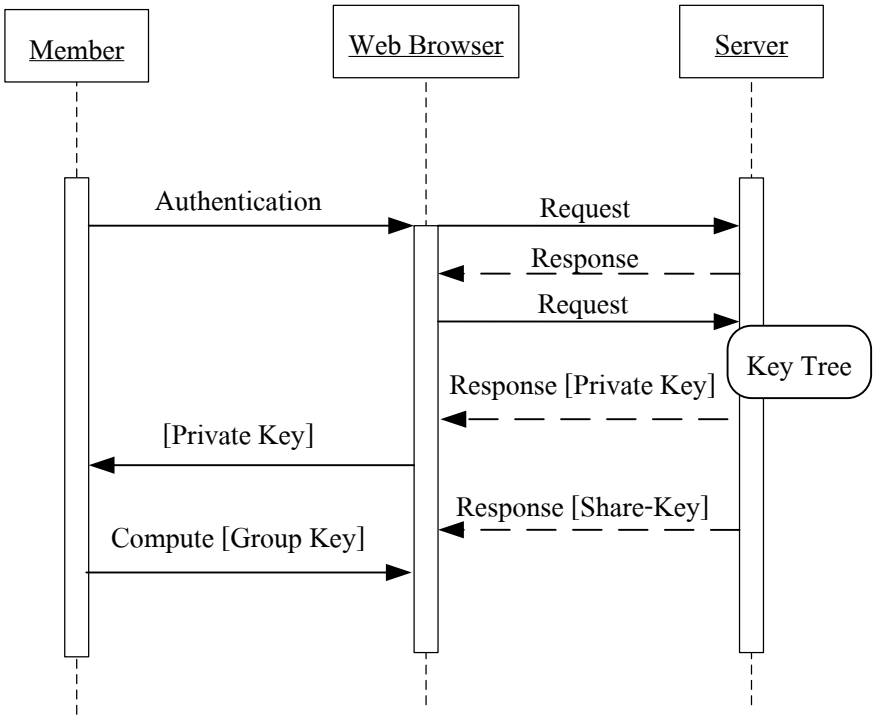
4.2 การสร้างความปลอดภัยไฟล์ข้อมูลภายในกลุ่ม

ในการสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆนั้นข้อมูลที่จัดเก็บจะถูกเข้ารหัสไว้โดยกระบวนการเข้ารหัสข้อมูลแบบขั้นสูง AES ในโหมด CBC โดยข้อมูลที่เข้ารหัสไว้ในแต่ละไฟล์จะมีคีย์ไฟล์สำหรับทำหน้าที่ในการเข้ารหัสและถอดรหัสข้อมูลอยู่ ซึ่งคีย์ไฟล์ โดยในเอกสารนี้จะจัดเก็บข้อมูลเกี่ยวกับคีย์ไฟล์ คีย์ของไดเร็กทอรี่ คีย์โครงสร้างต้นไม้ ซึ่งไฟล์ข้อมูลนี้จะถูกเข้ารหัสด้วยคีย์กลุ่มอีกครั้งหนึ่งเพื่อความปลอดภัยในการสื่อสารข้อมูลกลุ่ม โดยเมื่อสมาชิกภายในกลุ่มสามารถคำนวณคีย์กลุ่มได้จะสามารถเปิดดูข้อมูลที่อยู่ภายในไดเร็กทอรี่หลักได้ ซึ่งในไดเร็กทอรี่หลักอาจจะมีไฟล์ซึ่งสามารถทำการเปิดโดยใช้คีย์ไฟล์ที่เข้ารหัสไว้ดังที่ได้อธิบายข้างต้น ส่วนกรณีที่ไฟล์จัดเก็บอยู่ในไดเร็กทอรี่ย่อยอีกลำดับหนึ่ง ในไดเร็กทอรี่ย่อยก็จะประกอบด้วยคีย์ไฟล์ที่ใช้จัดเก็บคีย์สำหรับไฟล์ในการเข้ารหัสและถอดรหัสของไฟล์ที่อยู่ในไดเร็กทอรี่ย่อย ส่วนไดเร็กทอรี่ย่อยนี้จะถูกเข้ารหัสด้วยคีย์ไดเร็กทอรี่ซึ่งสามารถคำนวณได้จากคีย์ไฟล์ที่อยู่บนไดเร็กทอรี่ด้านบน ภาพที่ 4.5 แสดง Diagram กระบวนการทำงานของการเข้ารหัสไฟล์ข้อมูลที่ใช้ร่วมกันในสมาชิกของกลุ่ม

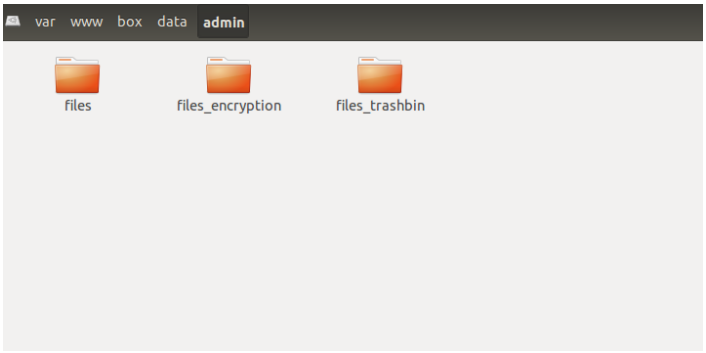


ภาพที่ 4.5 Diagram ขบวนการเข้ารหัสไฟล์ข้อมูลภายในกลุ่ม

เริ่มต้นสมาชิกจะยืนยันตัวตนเข้าสู่ระบบโดยการกำหนดชื่อผู้ใช้และรหัสผ่าน ระบบจะดำเนินการตรวจสอบความถูกต้อง จากนั้นสมาชิกจะดำเนินการคำนวณหาคีย์ส่วนตัว หลังจากนั้นจึงทำการคำนวณหาคีย์กลุ่มตามโครงสร้างของต้นไม้ คีย์กลุ่มนี้จะใช้ในการเข้ารหัสและถอดรหัสคีย์ไฟล์ที่อยู่ใน Group Directory ซึ่งในคีย์ไฟล์จะเก็บคีย์ต่าง ๆ ที่ใช้ในการเข้ารหัสและถอดรหัสไฟล์ต่าง ๆ ที่เก็บภายใต้ Group และ Sub Directory นี้ต่อไป การเข้ารหัสและถอดรหัสข้อมูลในไฟล์จะใช้วิธีแบบขั้นสูง AES ในโหมด CBC ภาพที่ 4.6 แสดง Sequence Diagram เริ่มต้นการทำงานเมื่อสมาชิกอยู่ในกลุ่มสื่อสาร และภาพที่ 4.7 แสดงตัวอย่างโครงสร้างไฟล์ข้อมูลของสมาชิกในกลุ่ม



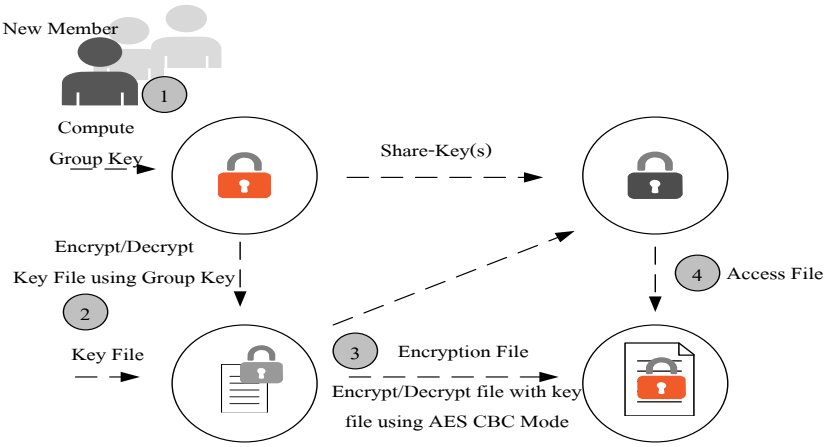
ภาพที่ 4.6 Sequence Diagram การทำงานของสมาชิกในกลุ่ม



ภาพที่ 4.7 แสดงตัวอย่างโครงสร้างไฟล์ของสมาชิกในกลุ่ม

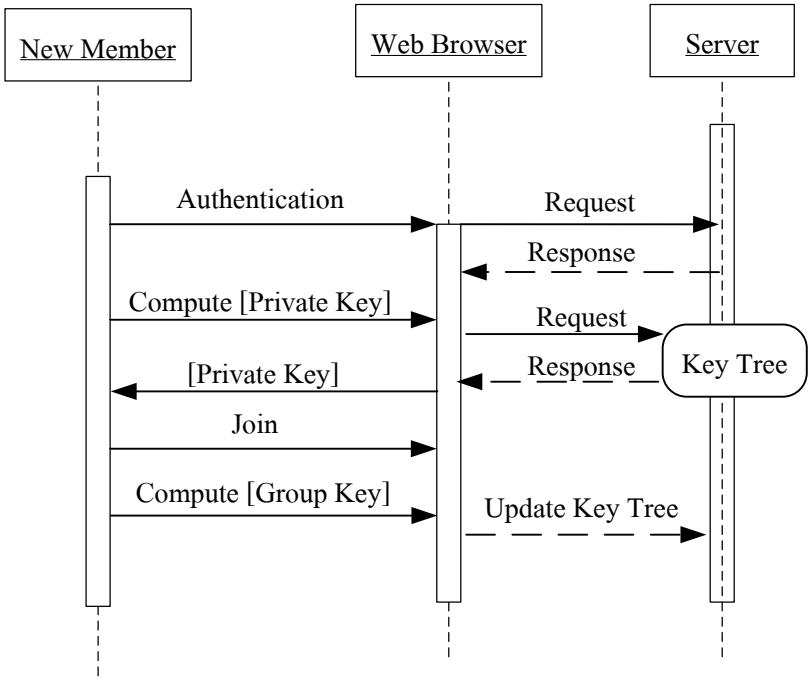
4.2.1 การจัดการโครงสร้างไฟล์เมื่อสมาชิกเข้าร่วมกลุ่ม

เมื่อมีสมาชิกใหม่ต้องการเข้าร่วมในกลุ่มสื่อสารปัจจุบันสมาชิกใหม่ที่จะเข้าร่วมกันจะเป็นผู้ดำเนินการในการคำนวณหาคีย์กลุ่มใหม่เพื่อกระจายให้กับสมาชิกในกลุ่มสื่อสารต่อไป โดยที่สมาชิกที่อยู่ภายในกลุ่มไม่จำเป็นที่จะต้องดำเนินการหรือออนไลน์พร้อมกันทั้งหมดสำหรับการคำนวณเพื่อหาคีย์กลุ่ม เนื่องจากสมาชิกใหม่จะถูกเพิ่มเข้าเป็นโหนดใบที่ระดับบนสุด การคำนวณหาคีย์กลุ่มใหม่จะใช้วิธีคำนวณคีย์ตามกระบวนการเริ่มต้นการทำงาน หลังจากเมื่อคำนวณคีย์กลุ่มแล้วจะกระจายคีย์นั้นให้สมาชิกตามโครงสร้างต้นไม้ต่อไป โดยสมาชิกใหม่ที่ได้เข้าร่วมกลุ่มในปัจจุบันแล้วจะไม่สามารถที่จะทราบหรือดูข้อมูลของกลุ่มสมาชิกที่ได้ดำเนินการไว้ก่อนหน้าได้ ทั้งนี้เนื่องจากคีย์กลุ่มได้ถูกเปลี่ยนใหม่แล้ว ในภาพที่ 4. 8 แสดงขบวนการทำงานเมื่อสมาชิกใหม่เข้าร่วมกลุ่ม

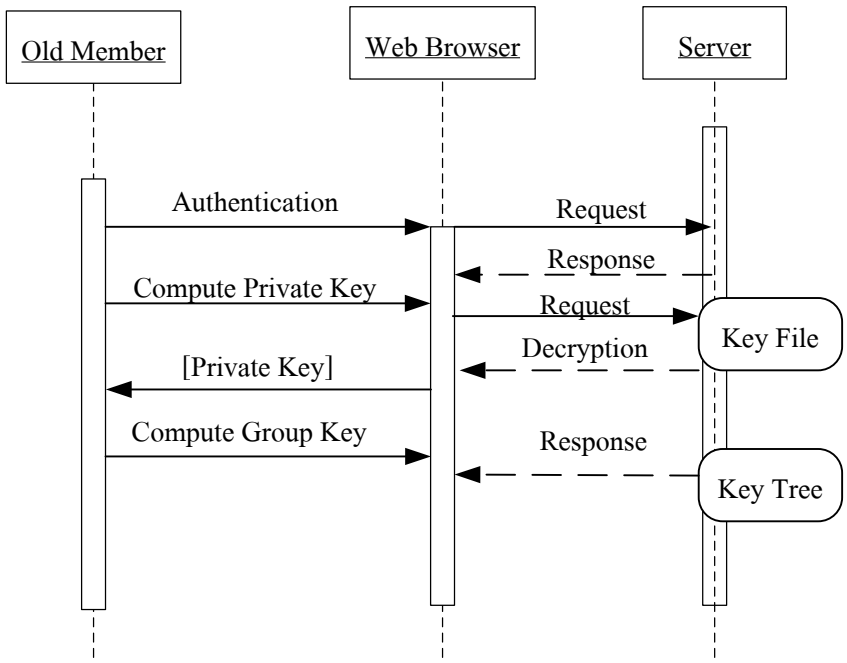


ภาพที่ 4.8 ขบวนการทำงานเมื่อสมาชิกใหม่เข้าร่วมกลุ่ม

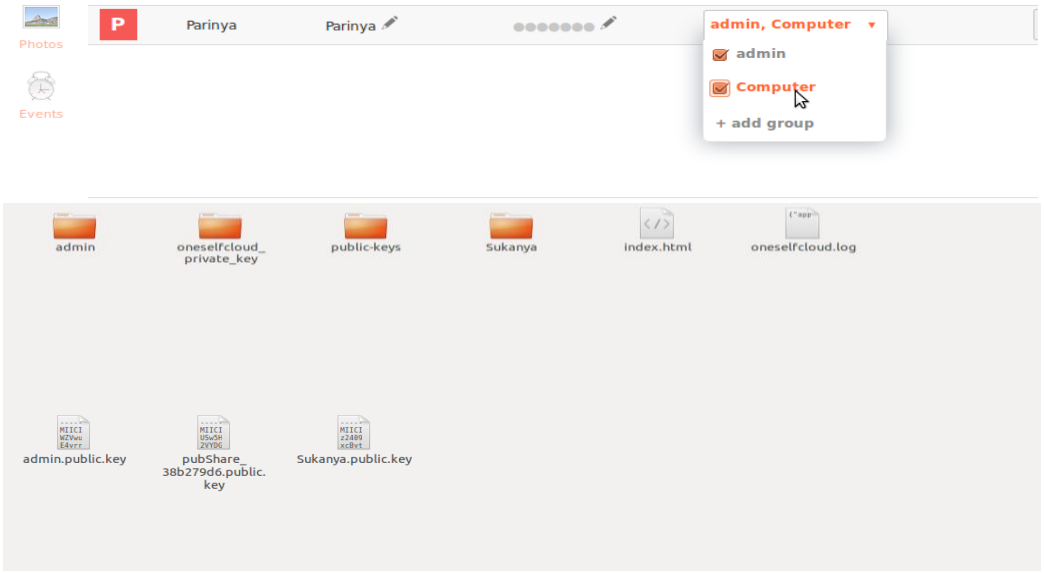
เมื่อมีสมาชิกใหม่ต้องการเข้าร่วมกลุ่มสมาชิกใหม่หรือสมาชิกที่ออนไลน์จะเป็นผู้คำนวณคีย์กลุ่มใหม่แล้วกระจายให้กับสมาชิกทุกคนที่อยู่ภายในกลุ่มเพื่อให้สมาชิกที่อยู่ในกลุ่มเมื่อออนไลน์แล้วสามารถที่จะคำนวณหาคีย์กลุ่มเพื่อใช้สำหรับเปิดคีย์ไฟล์ที่ถูกเข้ารหัสด้วยคีย์กลุ่ม โดยเมื่อสมาชิกใหม่เมื่อเข้าร่วมกลุ่มแล้วจะยังไม่สามารถใช้ข้อมูลร่วมกันกับสมาชิกที่อยู่ในกลุ่มเดิมได้จนกว่าจะมีสมาชิกกลุ่มเดิมออนไลน์และแบ่งปันข้อมูลให้กับสมาชิกใหม่ให้ใช้งานร่วมกันได้ และสมาชิกที่อยู่ภายในกลุ่มจะมีคีย์ไฟล์ที่ใช้ร่วมกันภายในกลุ่มใหม่ขึ้นมา โดยคีย์ไฟล์นี้จะถูกเข้ารหัสด้วยคีย์กลุ่มใหม่ แสดงขั้นตอนการทำงาน ภาพที่ 4.9 แสดง Sequence Diagram เมื่อสมาชิกใหม่เข้าร่วมกลุ่ม ส่วนภาพที่ 4.10 แสดง Sequence Diagram ของสมาชิกเก่า และภาพที่ 4.11 แสดงตัวอย่างโครงสร้างไฟล์เมื่อสมาชิกใหม่เข้าร่วมกลุ่ม



ภาพที่ 4.9 Sequence Diagram ของสมาชิกใหม่เมื่อต้องการเข้าร่วมกลุ่ม

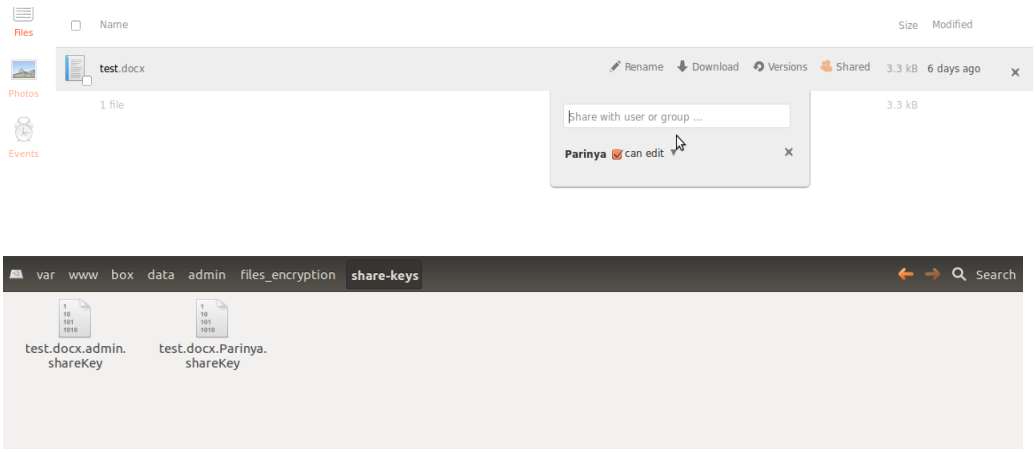


ภาพที่ 4.10 Sequence Diagram ของสมาชิกเก่าเมื่อสมาชิกใหม่เข้าร่วมกลุ่ม



ภาพที่ 4.11 แสดงโครงสร้างไฟล์เมื่อสมาชิกใหม่เข้าร่วมกลุ่ม

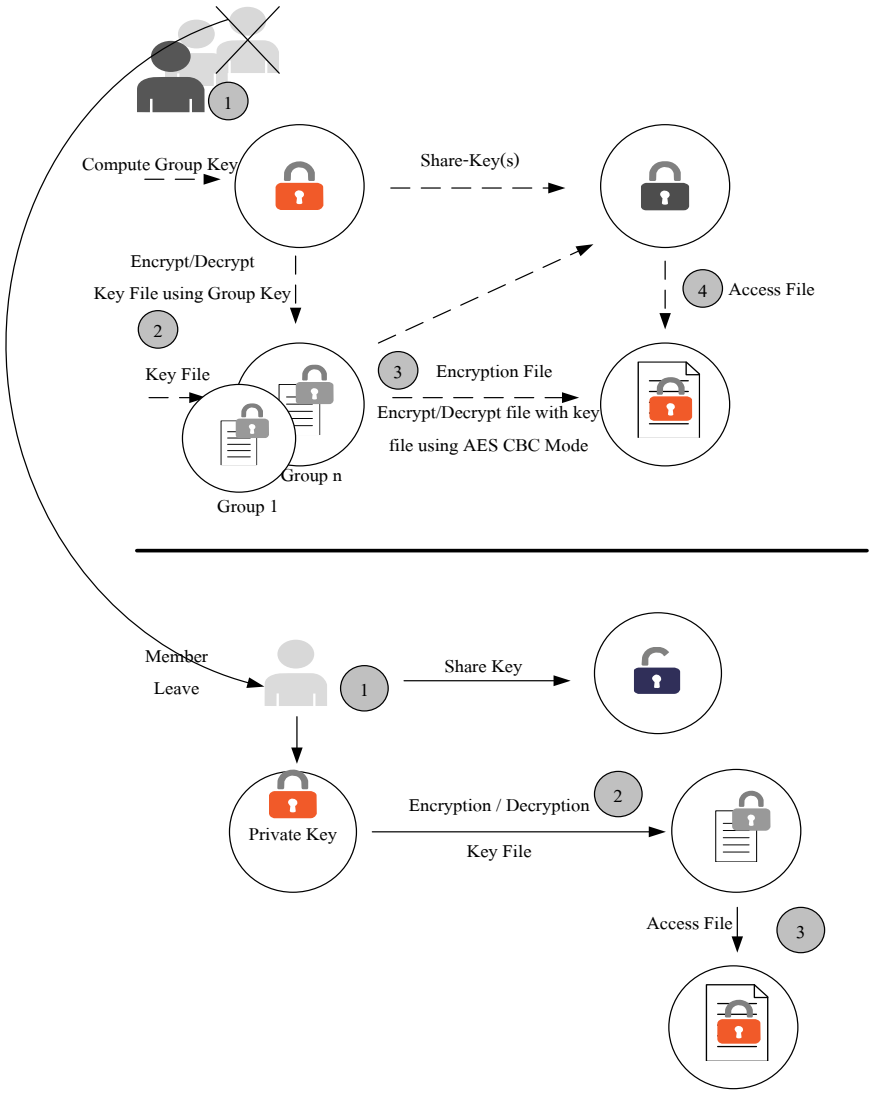
ในกรณีที่สมาชิกต้องการแบ่งปันไฟล์ให้กับสมาชิกในกลุ่มสามารถทำได้โดยการแชร์ไฟล์ข้อมูลโดยสมาชิกสามารถกำหนดการแชร์ให้กับสมาชิกหรือให้กับกลุ่มทั้งหมด ดังภาพที่ 4.12 แสดงขั้นตอนสมาชิกแบ่งปันไฟล์ในกลุ่ม



ภาพที่ 4.12 แสดงโครงสร้างไฟล์เมื่อสมาชิกแบ่งปันไฟล์

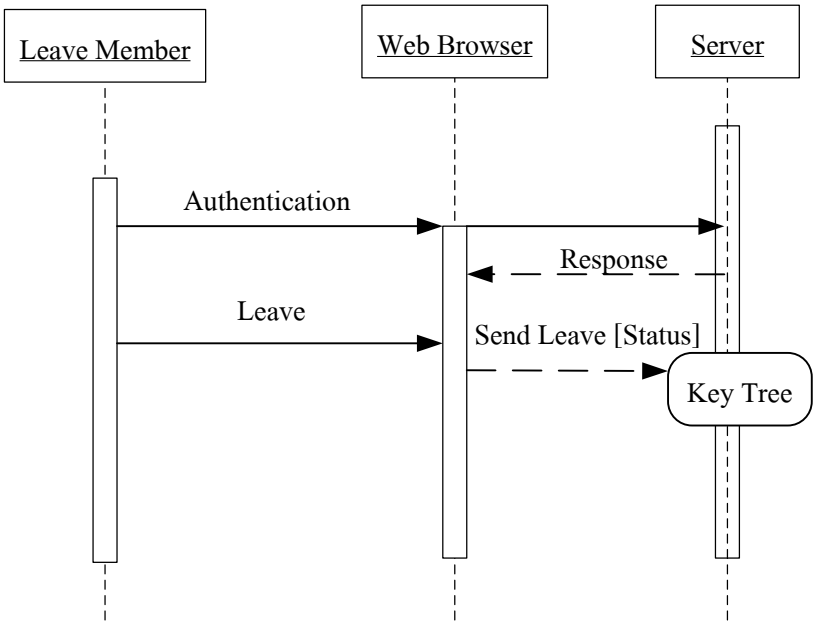
4.2.2 การจัดการโครงสร้างไฟล์เมื่อสมาชิกออกจากกลุ่ม

กรณีที่สมาชิกต้องการออกจากกลุ่ม หลังจากที่สมาชิกทออกจากกลุ่มแล้วจะไม่สามารถดูข้อมูลในกลุ่มที่ผ่านมาได้เนื่องจากคีย์กลุ่มจะถูกเปลี่ยนแปลง และสมาชิกในกลุ่มปัจจุบันเมื่อมีสมาชิกดำเนินการหรือออนไลน์จะเป็นผู้ดำเนินการในการคำนวณคีย์กลุ่มใหม่ เพื่อป้องกันความปลอดภัยของข้อมูลที่สื่อสารภายในกลุ่ม โดยเมื่อสมาชิกที่อยู่ภายในกลุ่มออนไลน์มากรณีที่อยู่เหนือหรืออยู่ด้านล่างของโหนดสมาชิกที่ออกจากกลุ่มจะใช้วิธีการคำนวณหาคีย์กลุ่มตามโครงสร้างของต้นไม้ตามหัวข้อที่ 3.2.3 ดังภาพที่ 4.13 แสดงขบวนการทำงานเมื่อสมาชิกออกจากกลุ่ม

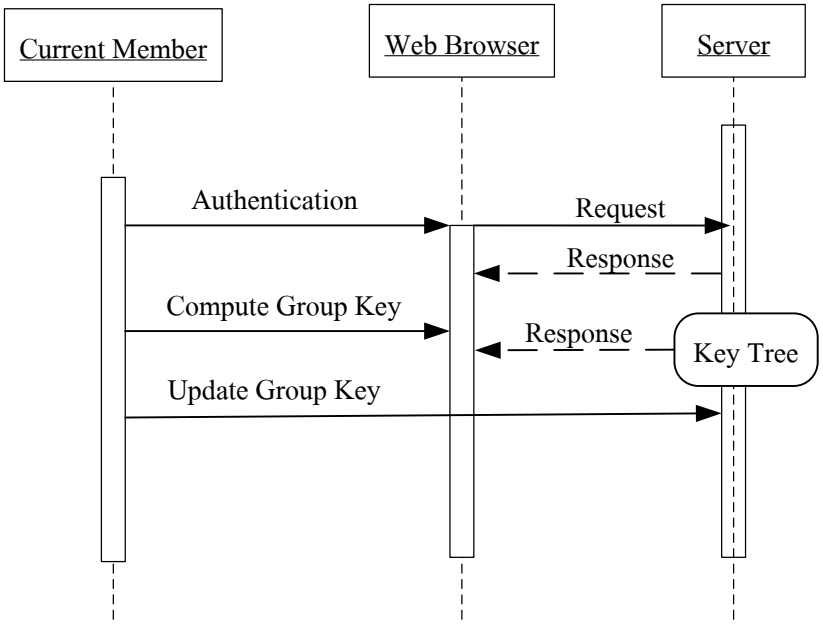


ภาพที่ 4.13 แสดง Diagram โครงสร้างไฟล์เมื่อสมาชิกออกจากกลุ่ม

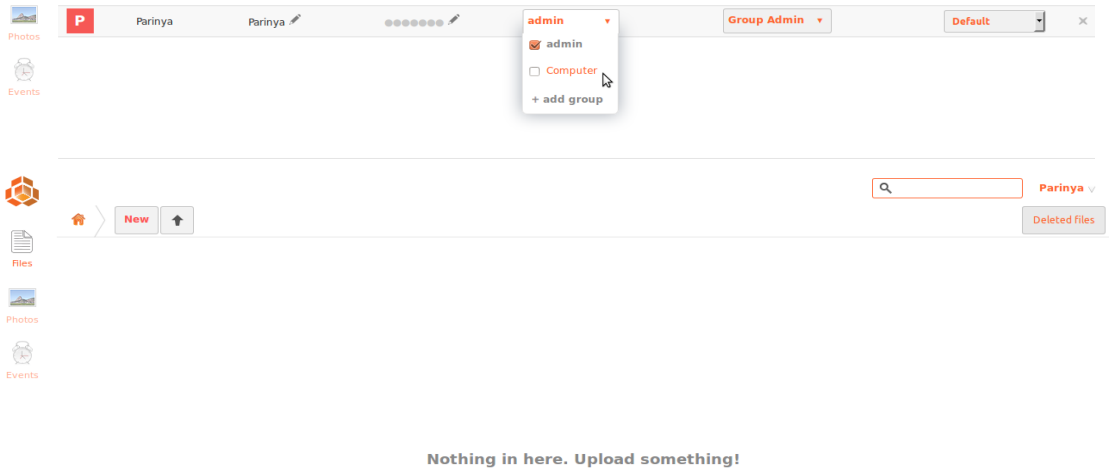
เมื่อสมาชิกออกจากกลุ่มแล้วสมาชิกจะไม่สามารถคำนวณคีย์กลุ่มเดิมได้ เพราะเมื่อสมาชิกที่อยู่ภายในกลุ่มออนไลน์ขึ้นมาจะดำเนินการปรับปรุงคีย์กลุ่มในโครงสร้างต้นไม้ทำให้สมาชิกที่ออกไปแล้วไม่ทราบคีย์กลุ่มใหม่ จึงไม่สามารถที่จะเปิดคีย์ไฟล์ที่เข้ารหัสด้วยคีย์กลุ่มได้ขบวนการทำงานเมื่อสมาชิกออกจากกลุ่มแสดงได้ดังภาพที่ 4.14 แสดง Sequence Diagram ของสมาชิกที่ต้องการออกจากกลุ่ม ส่วนภาพที่ 4.15 แสดง Sequence Diagram ของสมาชิกในกลุ่มเดิม และภาพที่ 4.16 แสดงตัวอย่างโปรแกรมเมื่อสมาชิกออกจากกลุ่ม



ภาพที่ 4.14 Sequence Diagram ของการทำงานเมื่อสมาชิกออกจากกลุ่ม



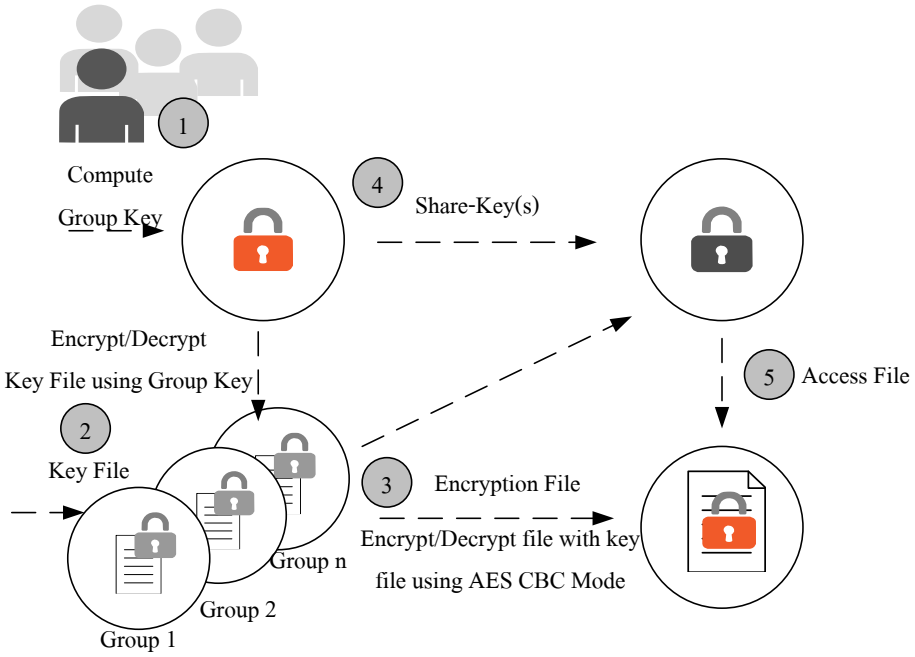
ภาพที่ 4.15 Sequence Diagram ของสมาชิกในกลุ่มเดิม



ภาพที่ 4.16 โครงสร้างไฟล์เมื่อสมาชิกออกจากกลุ่ม

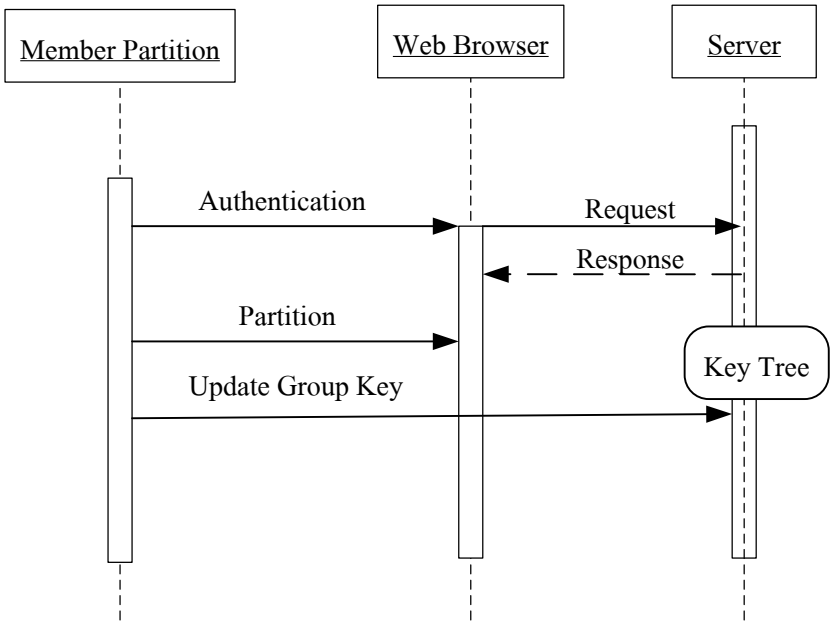
4.2.3 การจัดการโครงสร้างไฟล์เมื่อสมาชิกแยกกลุ่ม

เมื่อสมาชิกภายในกลุ่มต้องการแยกกลุ่มสื่อสารออกเป็นกลุ่มย่อยสมาชิกสามารถแยกไฟล์ข้อมูลออกจากกลุ่มเดิมโดยสมาชิกภายในกลุ่มจะดำเนินการสร้าง Group Directory สำหรับกลุ่มขึ้นมาใหม่จากนั้นสมาชิกที่ออนไลน์จะเป็นผู้ดำเนินการในการคำนวณหาคีย์กลุ่มตามโครงสร้างต้นไม้ดังหัวข้อที่ 3.2.3 โดยเมื่อสมาชิกได้ทำการแยกกลุ่มแล้วในแต่ละกลุ่มการสื่อสารของแต่ละสมาชิกจะมี Key File ของแต่ละกลุ่มแยกย่อยออกไป สมาชิกที่อยู่ในกลุ่มสื่อสารแต่ละกลุ่มจะต้องดำเนินการคำนวณหาคีย์กลุ่มเพื่อใช้ในการเปิดดูข้อมูลตาม Key File ซึ่งถ้าเป็นสมาชิกที่อยู่ภายในกลุ่มจะสามารถทำการเปิดดูข้อมูลนี้ได้ ซึ่งเมื่อสมาชิกที่อยู่ภายในกลุ่มสามารถที่จะเปิดดู Key File นี้ได้ก็จะทำให้สมาชิกนั้นสามารถเปิดดูข้อมูลได้ในลำดับต่อไป แต่ถ้าไม่เป็นสมาชิกที่อยู่ภายในกลุ่มสมาชิกดังกล่าวจะไม่สามารถคำนวณหาคีย์กลุ่มที่ใช้เปิดดูข้อมูล Key File ก็จะทำให้สามารถเปิดดูข้อมูลเหล่านั้นได้ ดังแสดงในภาพที่ 4.17 แสดง Diagram โครงสร้างไฟล์ข้อมูลกรณีเมื่อสมาชิกดำเนินการแยกกลุ่มสื่อสาร

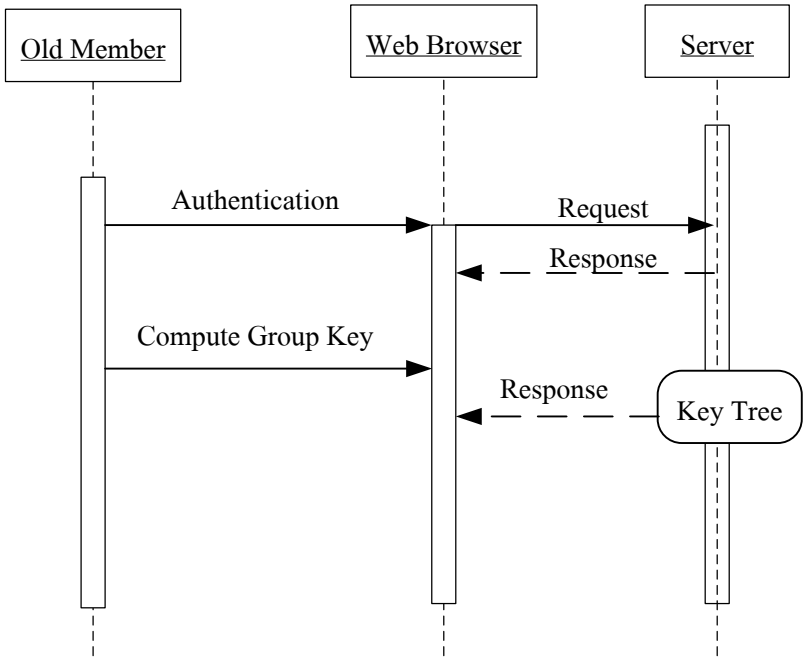


ภาพที่ 4.17 ขบวนการทำงานเมื่อมีการแยกกลุ่ม

เมื่อสมาชิกในกลุ่มต้องการแยกกลุ่มสื่อสารออกเป็นกลุ่มย่อยจะใช้หลักการเดียวกันเหมือนกับสมาชิกออกจากกลุ่มซึ่งโครงสร้างไฟล์ข้อมูลจะมีลักษณะเช่นเดียวกันการออกจากกลุ่มตามที่กล่าวถึงในบทที่ 3 โดยในคีย์ไฟล์จะมีไฟล์ที่ใช้สำหรับจัดเก็บของแต่ละกลุ่มสื่อสาร เมื่อสมาชิกคำนวณหาคีย์กลุ่มใหม่แล้วจะสามารถเปิดคีย์ไฟล์ที่ถูกเข้ารหัสด้วยคีย์กลุ่มใหม่ได้ เมื่อสมาชิกเปิดคีย์ไฟล์ได้ก็จะทำให้สามารถเข้าถึงไฟล์ได้ในลำดับถัดไป ภาพที่ 4.18 แสดง Sequence Diagram ของการทำงานเมื่อสมาชิกแยกกลุ่ม และภาพที่ 4.19 แสดง Sequence Diagram การทำงานของสมาชิกในกลุ่มเดิม



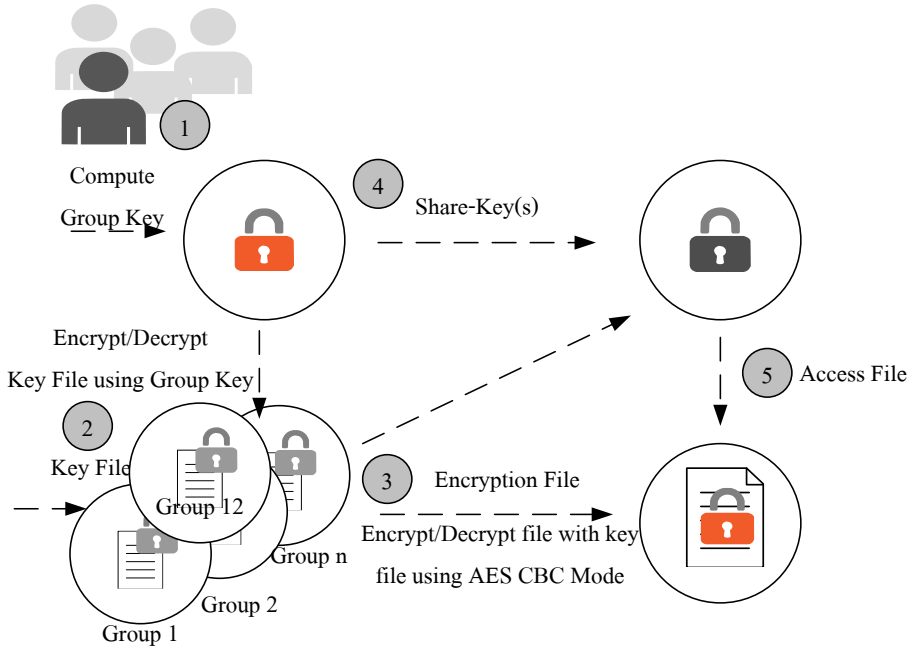
ภาพที่ 4.18 Sequence Diagram เมื่อมีสมาชิกแยกกลุ่ม



ภาพที่ 4.19 Sequence Diagram ของสมาชิกในกลุ่มเดิม

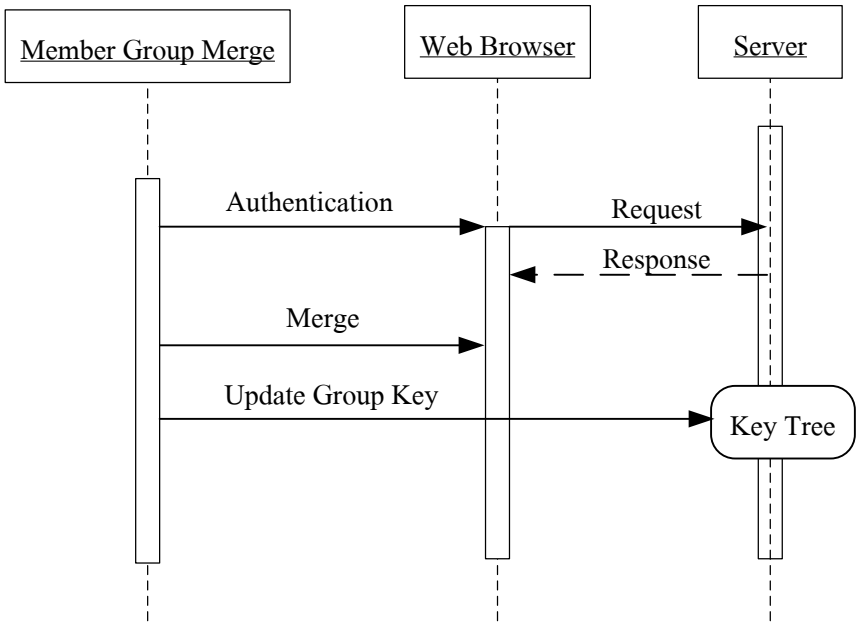
4.2.4 การจัดการโครงสร้างไฟล์เมื่อมีการรวมกลุ่ม

ในการพัฒนาระบบกรณีที่สมาชิกต้องการรวมกลุ่มสื่อสารไฟล์ข้อมูลที่อยู่ภายในกลุ่มสื่อสารจะต้องสามารถแบ่งปันข้อมูลระหว่างกลุ่มสื่อสารได้โดยมีวิธีกระบวนการคือเมื่อสมาชิกเข้ารวมกลุ่มและมีการแบ่งปันข้อมูลกันข้อมูลของสมาชิกภายในกลุ่มจะถูกจัดเก็บไว้ในไฟล์สำหรับแบ่งปันข้อมูลระหว่างกลุ่มนั่นคือจะต้องดำเนินการสร้าง Group Directory ขึ้นมาใหม่สำหรับจัดเก็บข้อมูลเกี่ยวกับกลุ่มสื่อสารโดยใน Group Directory นี้จะประกอบไปด้วยคีย์ไฟล์ซึ่งไฟล์นี้จะทำหน้าที่ในการชี้ตำแหน่งไปยังคีย์ไฟล์ที่เข้ารหัสสำหรับกลุ่มสื่อสารแต่ละกลุ่มและทำหน้าที่สำหรับเข้ารหัสไฟล์ที่อยู่ภายในกลุ่มสื่อสารแต่ละกลุ่มต่อไป ซึ่ง Key File นี้จะถูกเข้ารหัสด้วยคีย์กลุ่มซึ่งเมื่อสมาชิกที่ได้ทำการรวมกลุ่มสื่อสารแล้วสามารถคำนวณหาคีย์กลุ่มได้ตามข้อตกลงคีย์กลุ่มตามโครงสร้างต้นไม้ที่ได้นำเสนอตามกระบวนการรวมกลุ่มสื่อสารดังข้างต้น ซึ่งในขณะเดียวกันสมาชิกก็ยังสามารถที่จะเปิดดูข้อมูลที่อยู่ภายในกลุ่มสมาชิกเดิมได้เช่นกัน เพราะในการจัดเก็บของ Key File ของสมาชิกในกลุ่มก็ยังมีข้อมูลของสมาชิกเหล่านั้นอยู่ ดังแสดงในภาพที่ 4.20 แสดง Diagram ตัวอย่างโครงสร้างไฟล์กรณีที่สมาชิกรวมกลุ่มสื่อสาร

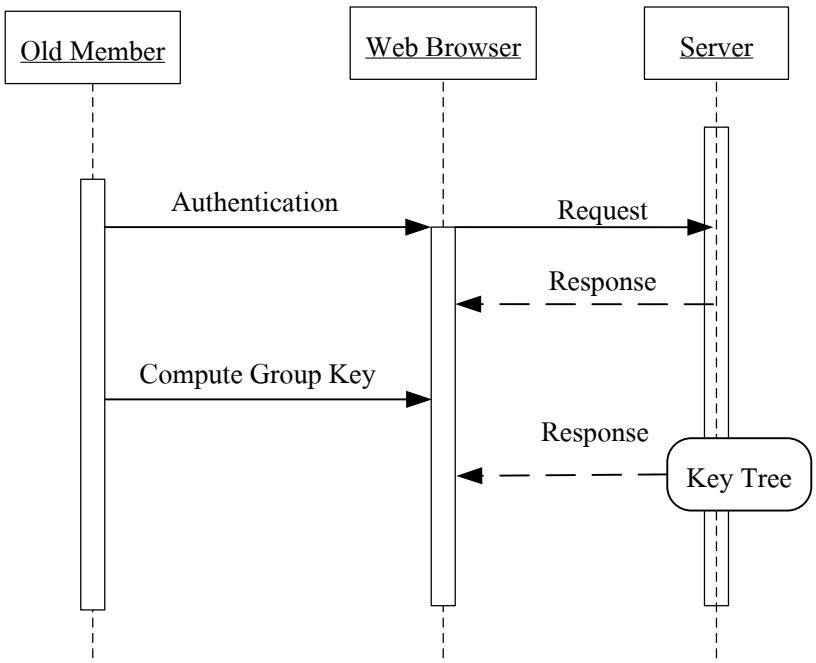


ภาพที่ 4.20 ขบวนการทำงานกรณีมีการรวมกลุ่ม

เมื่อสมาชิกต้องการรวมกลุ่มจะใช้หลักการทำงานเหมือนกับสมาชิกใหม่เข้าร่วมกลุ่ม กล่าวคือเมื่อมีการรวมกลุ่มสื่อสารแล้วสมาชิกภายในกลุ่มจะต้องคำนวณหาคีย์กลุ่มใหม่เพื่อใช้ในการเข้ารหัสและถอดรหัสคีย์ไฟล์ของกลุ่มใหม่อีกครั้ง โดยคีย์ไฟล์ของกลุ่มก็จะถูกสร้างขึ้นมาใหม่สำหรับการรวมกลุ่มสื่อสารซึ่งจะทำให้สมาชิกสามารถสื่อสารกันได้ภายในกลุ่มใหม่ที่เกิดจากการรวมกลุ่มเข้าด้วยกัน ภาพที่ 4.21 แสดง Sequence Diagram เมื่อสมาชิกรวมกลุ่ม และภาพที่ 4.22 แสดง Sequence Diagram ของสมาชิกในกลุ่มเดิมเมื่อมีการรวมกลุ่ม



ภาพที่ 4.21 Sequence Diagram เมื่อมีการรวมกลุ่ม



ภาพที่ 4.22 Sequence Diagram ของสมาชิกในกลุ่มเดิมเมื่อรวมกลุ่ม

บทที่ 5

สรุปผลการวิจัย และข้อเสนอแนะ

งานวิจัยนี้นำเสนอวิธีการสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆตามข้อตกลงคีย์กลุ่ม Diffie-Hellman เพื่อลดเวลาในการประมวลผลงานวิจัยนี้จึงได้ใช้โครงสร้างต้นไม้มาช่วยในขบวนการคำนวณคีย์กลุ่มซึ่งช่วยให้การทำงานมีความยืดหยุ่นต่อการเปลี่ยนแปลงของสมาชิกภายในกลุ่มสื่อสารเป็นอย่างมาก

จากการทดสอบโดยการจำลองการทำงานบนเครื่องเซิร์ฟเวอร์กุญแจที่ได้ประยุกต์การสร้างความปลอดภัยข้อมูลในการประมวลผลแบบกลุ่มเมฆตามข้อตกลงคีย์กลุ่ม เป็นไปได้อย่างมีประสิทธิภาพ โดยข้อมูลที่จัดเก็บในการประมวลผลแบบกลุ่มเมฆจะถูกเข้ารหัสด้วยกระบวนการเข้ารหัสแบบ AES ด้วยโหมด CBC ซึ่งไฟล์ที่จัดเก็บอยู่ในไดเร็กทอรี่จะถูกเข้ารหัสด้วยคีย์ของไฟล์ โดยคีย์ไฟล์นี้จะสามารถเปิดได้โดยใช้คีย์กลุ่มซึ่งสมาชิกที่อยู่ภายกลุ่มจะได้รับกุญแจส่วนตัวในการเปิดดูข้อมูลของตนเองและเมื่อสมาชิกต้องการติดต่อสื่อสารภายในกลุ่มสมาชิกจะสามารถแลกเปลี่ยนคีย์เพื่อใช้ในการคำนวณหาคีย์กลุ่มเพื่อติดต่อสื่อสารกันตามข้อตกลง Diffie-Hellman การประยุกต์ใช้โครงสร้างแบบต้นไม้มาช่วยในการคำนวณคีย์กลุ่มจะช่วยลดเวลาในการคำนวณคีย์ให้กับสมาชิกภายในกลุ่มสื่อสารได้อีกด้วย

เนื่องจากการทดลองได้พัฒนาระบบที่ให้บริการในรูปแบบของโปรแกรมเว็บเบราวเซอร์เท่านั้น ดังนั้นสิ่งที่ควรจะพัฒนาต่อไปคือ การพัฒนาระบบที่ให้บริการในรูปแบบอื่น ๆ เพื่อให้ตอบสนองการทำงานในทุกรูปแบบแฟลตฟอร์มของระบบซึ่งน่าจะตอบสนองความต้องการของผู้ใช้บริการได้มากขึ้น

บรรณานุกรม

Maggiani, Rich and Markoff, John. 2009. Cloud Computing Is Changing How We Communicate. **IEEE International**. 19 (July): 1-4.

Kim, Y.; Perrig, A. and Tsudik, G. 2004. Tree-based Group Key Agreement. **ACM Transaction on Information and System Security**. 7 (February): 60-96.

Rescorla, E. 1999. **Diffie-Hellman Key Agreement Method**. United States: RFC Editor.

Lam, I.; Szebeni, S. and Buttyan, L. 2012. Key Management for Dynamic Groups in an Asynchronous Communication Model. **IEEE International**. 10 (September): 269-276.

Blaze, M. 1993. A Cryptographic File System for UNIX. **ACM Conference on Computer and Communications Security**. 1 (December): 9-16.

Cattaneo, G.; Cauogno, L.; Sorbo, A.D. and Persiano, P. 2001. The Design and Implementation of a Transparent Cryptographic File System for UNIX. **ACM USENIX Annual Technical Conference**. 25 (June): 199-212.

Kevin E. Fu. 1999. **Group Sharing and Random Access in Cryptographic Storage File System**. Master's Thesis, Massachusetts Institute of Technology.

Harrington, A. and Jensen, C. 2003. Cryptographic Access Control in a Distributed File System. **ACM Symposium on Access Control Models and Technologies**. 2 (June): 158-165.

Goh, E.; Shacham, H.; Modadugu, N. and Boneh, D. 2003. Sirius: Securing Remote Untrusted Storage. **Network and Distributed Systems Security(NDSS)**. 7 (February): 131-145.

Sriram, V.; Narayan, G. and Gopinath, K. 2007. A Secure and Accountable Filesystem over Untrusted Storage. **IEEE International**. 27 (September): 34-45.

Geron, E. and Wool, A. 2009. Cryptographic Remote Untrusted Storage without Public Keys. **IEEE International**. 27 (September): 3-14.

Leghton, T. and Micali, S. 1993. Secret-key Agreement without Public Key Cryptography. **Springer Berlin Heidelberg**. 22 (August): 456-479.

Grolimund, D.; Meisser, L.; Schmid, S. and Wattenhofer, R. 2006. A Folder Tree Structure for Cryptographic File Systems. **IEEE International**. 2 (October): 189-198.

ประวัติผู้เขียน

ชื่อ ชื่อสกุล	นายปริญญา นาโท
ประวัติการศึกษา	บริหารธุรกิจบัณฑิต (ธุรกิจศึกษา-คอมพิวเตอร์) เกียรตินิยมอันดับ 2 มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ปีที่สำเร็จการศึกษา พ.ศ. 2549
ประสบการณ์การทำงาน	พ.ศ. 2551-2552 Programmer Wiansong CO., LTD. พ.ศ. 2552-ปัจจุบัน อาจารย์สอนประจำสาขาคอมพิวเตอร์ธุรกิจ หัวหน้าฝ่ายเทคโนโลยีการศึกษา วิทยาลัยอาชีวศึกษาดุสิตพณิชยการ