การแบ่งกุญแจลับเป็นหลายส่วนโดยใช้เทคนิคการเข้ารหัสเครือข่ายสำหรับผู้ให้บริการการจัดการลิขสิทธิ์ดิจิทัลแบบคลาวด์

ภานุวัฒน์ พรหมศิริ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
คณะวิศวกรรมศาสตร์ มหาวิทยาลัยบูรพา
พฤษภาคม 2560

คณะกรรมการควบคุมวิทยานิพนธ์ และคณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาวิทยานิพนธ์ของ ภานุวัฒน์ พรหมศิริ ฉบับนี้แล้ว เห็นสมควรรับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า ของมหาวิทยาลัยบูรพาได้

คณะกรรมการควบคุมวิทยานิพนธ์

.....อาจารย์ที่ปรึกษาหลัก
(ดร. อภิรัฐ ลิ่มมณี)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธาน
(ผู้ช่วยศาสตราจารย์ ดร. วิมล แสนอุ้ม)

.....กรรมการ
(รองศาสตราจารย์ วิรุฬห์ ศรีบริรักษ์)

.....กรรมการ
(ดร. อภิรัฐ ลิ่มมณี)

.....กรรมการ
(รองศาสตราจารย์ ดร. ณกร อินทร์พยุง)

คณะวิศวกรรมศาสตร์อนุมัติให้รับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมไฟฟ้า ของมหาวิทยาลัยบูรพา

.....คณบดีคณะวิศวกรรมศาสตร์
(ดร. อาณัติ ดีพัฒนา)
วันที่ 30 เดือน พฤษภาคม พ.ศ. 2560

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงด้วยการได้รับความกรุณาให้คำปรึกษาเสนอแนะแนวทางที่ถูกต้อง และตรวจแก้ไขข้อบกพร่องต่าง ๆ อย่างดียิ่งจาก ดร.อภิรัฐ ลิ่มมณี อาจารย์ที่ปรึกษาหลัก ที่ให้คำแนะนำ ชี้แนะแนวทาง และ รองศาสตราจารย์ วิรุฬห์ ศรีบริรักษ์ ที่สนับสนุนช่วยเหลือและเป็นกำลังใจ ประธานคณะกรรมการสอบวิทยานิพนธ์ คณะกรรมการสอบวิทยานิพนธ์ ที่ให้คำแนะนำ ผู้วิจัยรู้สึกซาบซึ้งและขอกราบขอบพระคุณทุกท่านเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบพระคุณบริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน) ที่ให้ความช่วยเหลือในการพัฒนาระบบบนการทำงานแบบกลุ่มเมฆ

ขอขอบพระคุณผู้ทรงคุณวุฒิทุกท่านที่ได้กรุณาตรวจสอบความสมบูรณ์และให้คำแนะนำแก้ไขเครื่องมือในการวิจัย รวมทั้งผู้เชี่ยวชาญทุกท่าน

ท้ายที่สุดผู้วิจัยขอกราบขอบพระคุณ บิดา มารดา พี่ น้อง และเพื่อน ๆ ที่ได้ให้ความช่วยเหลือและกำลังใจ ตลอดจนผู้ที่เกี่ยวข้องทุกท่านที่มิได้กล่าวถึงในที่นี้

คุณค่า และประโยชน์ของวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบเป็นกตัญญูกตเวทิตาแด่บิดา มารดา ครู อาจารย์ และผู้มีพระคุณทุกท่าน ที่ได้อบรมสั่งสอน และให้กำลังใจแก่ผู้วิจัยเสมอมา

ภานุวัฒน์ พรหมศิริ

55910293: สาขาวิชา: วิศวกรรมไฟฟ้า; วศ.ม. (วิศวกรรมไฟฟ้า)
คำสำคัญ: DIGITAL RIGHTS MANAGEMENT/ SECRET KEY SHARING/ NETWORK CODING/ KEY MANAGEMENT/ OPEN CLOUD

ภานุวัฒน์ พรหมศิริ: การแบ่งกุญแจลับเป็นหลายส่วนโดยใช้เทคนิคการเข้ารหัสเครือข่ายสำหรับผู้ให้บริการ การจัดการลิขสิทธิ์ดิจิทัลแบบคลาวด์ (MULTIPLE SECRET KEY SHARING BASED ON THE NETWORK CODING TECHNIQUE FOR AN OPEN CLOUD DRM SERVICE PROVIDER) คณะกรรมการควบคุมวิทยานิพนธ์: อภิรัฐ ลิ่มมณี, ปร.ด. 44 หน้า. ปี พ.ศ. 2560.

จากอัตราการเติบโตของอินเทอร์เน็ตและยอดการจำหน่ายอุปกรณ์พกพาอิเล็กทรอนิกส์ในปัจจุบันมีการขยายตัวอย่างต่อเนื่อง ส่งผลให้ตลาดสื่อสิ่งพิมพ์ดิจิทัลอยู่ในทิศทางการเจริญเติบโตในแนวเดียวกัน ดังนั้นเพื่อให้ตลาดสื่อสิ่งพิมพ์ดิจิทัลสามารถดำเนินต่อไปได้ด้วยความราบรื่นกอปรกับการเพิ่มขึ้นของนักเขียนอิสระในปัจจุบัน การป้องกันลิขสิทธิ์ดิจิทัลจึงมีความสำคัญเป็นอย่างยิ่ง ในงานวิจัยฉบับนี้ได้มีการพัฒนาระบบให้บริการป้องกันลิขสิทธิ์ดิจิทัลที่มีการทำงานในลักษณะ On-the-fly ที่ไม่มีการเก็บบันทึกข้อมูลใด ๆ ไว้ในระบบทั้งต้นฉบับและไฟล์ข้อมูลที่ได้รับการเข้ารหัส โดยข้อมูลดังกล่าวจะถูกเก็บบันทึกกับลงไปยังพื้นที่เก็บข้อมูลแบบกลุ่มเมฆส่วนบุคคลของเจ้าของลิขสิทธิ์ ในส่วนกุญแจที่ใช้ในการเข้ารหัสลับนั้นงานวิจัยฉบับนี้ได้นำเสนอวิธีการกระจายและรวบรวมชิ้นส่วนกุญแจรหัสลับด้วยเทคนิคการเข้ารหัสเครือข่ายแบบปลอดภัย โดยการทดสอบใช้การทดสอบระยะเวลาในการประมวลผลในระบบต่าง ๆ จากการประเมินผลพบว่าการประมวลผลการกระจายกุญแจรหัสลับเพื่อไปเก็บยังเครื่อง VM-Based server ต่าง ๆ หลังจากที่มีการลงทะเบียนข้อมูลสินค้าเข้าสู่ระบบจากเจ้าของลิขสิทธิ์มีระยะเวลาในการดำเนินการเฉลี่ย 5.14 และ 8.88 วินาที ที่การกระจาย 4 และ 8 เครื่องตามลำดับ โดยมีจำนวนผู้เข้าใช้งานพร้อมกันได้มากถึง 10,000 ผู้ใช้งาน และการเก็บรวบรวมกุญแจรหัสลับเมื่อผู้ซื้อสินค้าต้องการดาวน์โหลดสินค้าในแต่ละครั้ง ใช้ระยะเวลาเฉลี่ย 1.20 และ 1.28 วินาที ที่การรวบรวมจาก 4 และ 8 เครื่องตามลำดับ ดังนั้นระบบจึงมีความเหมาะสมและสามารถรองรับปริมาณผู้ใช้งานเมื่อเข้ามาใช้งานระบบในเวลาเดียวกันได้มากพอ ที่จะสามารถนำไปใช้ได้ในสถานการณ์จริง

55910293: MAJOR: ELECTRICAL ENGINEERING; M.Eng. (ELECTRICAL ENGINEERING)
KEYWORD: DIGITAL RIGHTS MANAGEMENT/ SECRET KEY SHARING/ NETWORK CODING/ KEY MANAGEMENT/ OPEN CLOUD
PANUWAT PROMSIRI: MULTIPLE SECRET KEY SHARING BASED ON THE NETWORK CODING TECHNIQUE FOR AN OPEN CLOUD DRM SERVICE PROVIDER. ADVISORY COMMITTEE: APIRATH LIMMANEE, Ph.D. 44 P. 2017.

Today's continuous growth of the eBook market coincides with the increase in the number of Internet and Smart devices. One of the important service providers is the Digital Rights Management (DRM) service that provides copyrights security to the system. In this research, we present an open cloud DRM service provider to protect the digital content's copyright. The proposed architecture enables the service providers to use an on-the-fly DRM technique with symmetric-key encryption. Unlike other similar works, our system does not keep the encrypted digital content but lets the content creators do so in their own cloud storage. Moreover, the key used for symmetric encryption are managed in an extremely secure way by means of the key fission engine and the key fusion engine. The ideas behind the two engines are taken from the works in secure network coding and secret sharing. The performance of key fission engine after content creator registered their eBook to our system varies with average at 5.14 seconds in case of 4 VM-based servers and 8.88 seconds in case of 8 VM-based servers. We also measured the operating time of key fusion engine in 4 and 8 VM-based servers varies with average at 1.20 and 1.28 seconds respectively in each VM-based server. The experimental results demonstrate that our proposal is feasible for the real eBook market, especially for individual businesses.

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

ตารางที่ หน้า

สารบัญภาพ

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันทิศทางการเติบโตของตลาดสื่อสิ่งพิมพ์ดิจิทัล (Digital content) อยู่ในทิศทางการเจริญเติบโตสูงขึ้นกอปรกับยอดการจำหน่ายอุปกรณ์พกพาอิเล็กทรอนิกส์ (Smart device) ที่มีการขยายตัวจึงส่งผลให้เกิดการเจริญเติบโตอย่างรวดเร็วของตลาดสื่อสิ่งพิมพ์ดิจิทัลดังที่ได้กล่าวมาข้างต้น ซึ่งเป็นไปในทางเดียวกันกับทิศทางการเจริญเติบโตของตลาดการให้บริการบนกลุ่มเมฆ ทั้งการให้บริการระบบประมวลผลบนกลุ่มเมฆ หรือการให้บริการแหล่งเก็บข้อมูลบนกลุ่มเมฆแบบส่วนบุคคล โดยจากทิศทางการเจริญเติบโตของของกลุ่มธุรกิจทั้ง 3 ส่วน จึงก่อให้เกิดตลาดที่น่าจับตามองดังต่อไปนี้

1. ส่วนร้านค้าสื่อสิ่งพิมพ์ดิจิทัล (eBook store) ที่มีองค์ประกอบในการบริหารจัดการสื่อสิ่งพิมพ์ดิจิทัลที่วางขายภายในร้านค้าอิเล็กทรอนิกส์ การบริหารจัดการลูกค้า และการบริหารจัดการเรื่องการเงินภายในร้านค้า
2. ส่วนการให้บริการแหล่งเก็บข้อมูลบนกลุ่มเมฆส่วนบุคคล ที่มีการใน 2 ลักษณะ ได้แก่การให้บริการแบบเปิด (Public cloud) และการให้บริการแบบส่วนบุคคล (Private cloud) มีทั้งรูปแบบที่ให้ใช้งานได้ฟรี และคิดค่าใช้บริการ
3. ส่วนการให้บริการป้องกันลิขสิทธิ์ดิจิทัล ที่มีองค์ประกอบในการบริหารจัดการและป้องกันลิขสิทธิ์ดิจิทัลด้วยวิธีการต่าง ๆ

ส่วนการให้บริการที่มีความสำคัญมากที่สุดในกลุ่มตลาดทั้ง 3 กลุ่ม ได้แก่ ส่วนการให้บริการป้องกันลิขสิทธิ์ดิจิทัล ด้วยเหตุผลที่ว่ากระบวนการดังกล่าวสามารถที่จะป้องกันการคัดลอกข้อมูลสินค้าโดยไม่ได้รับอนุญาตได้ ทั้งข้อมูลที่ถูกเก็บอยู่ภายในแหล่งข้อมูลหรือระหว่างการส่งข้อมูลภายในเครือข่าย อย่างไรก็ตามจากการขยายตัวของตลาดสื่อสิ่งพิมพ์ดิจิทัลจึงก่อให้เกิดกลุ่มนักเขียนอิสระเพิ่มขึ้นอย่างมากมาย ทว่าการที่กลุ่มนักเขียนอิสระเหล่านี้ต้องมีการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัลขึ้นมานั้นเป็นเรื่องที่เกิดขึ้นได้ยาก อันเป็นผลมาจากค่าใช้จ่ายและความซับซ้อนของขั้นตอนในการพัฒนา ดังนั้นกลุ่มนักเขียนต้องหันไปใช้บริการการป้องกันลิขสิทธิ์ดิจิทัลจากทางสำนักพิมพ์รายใหญ่ที่มีศักยภาพมากพอในการพัฒนาระบบขึ้นมาใช้งานภายในองค์กร และการมีอยู่ของบุคคลกลางนี้ส่งผลให้ต้นทุนของสินค้ามีราคาที่เพิ่มสูงขึ้น รวมไปถึงความคุ้มทุนที่ทางสำนักพิมพ์ต้องคำนึงในการวางจำหน่ายสินค้าที่มาจากกลุ่มนักเขียน

รายย่อยที่ยังไม่เป็นกลุ่มนักเขียนชั้นนำในตลาด และยังสร้างความไม่สะดวกกับผู้ใช้งานที่ต้องทำการติดตั้งโปรแกรมที่มาจากหลากหลายสำนักพิมพ์ในอีกทางหนึ่งด้วย

นอกจากนี้แล้วความต้องการของนักเขียนหรือเจ้าของลิขสิทธิ์ส่วนใหญ่ย่อมมีความต้องการที่จะเก็บข้อมูลสินค้า อาทิเช่น PDF และ ePub ไว้ภายในแหล่งเก็บข้อมูลที่เชื่อถือได้ เช่น Dropbox และ Google Drive ที่อนุญาตให้เจ้าของชิ้นงานมีสิทธิเต็มที่ในการควบคุมการเข้าถึงข้อมูลจากทุกที่และทุกเวลา นอกไปจากนี้แล้วของเจ้าของลิขสิทธิ์ทั้งหลายยังคงมีความต้องการที่จะป้องกันการรั่วไหลของสินค้าในช่องทางต่าง ๆ ผ่านทางการใช้งานผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัลที่สามารถควบคุมการรั่วไหลของสินค้าได้ รวมไปถึงสามารถส่งต่อให้ยังผู้ใช้งานโดยไม่มีการเก็บข้อมูลใด ๆ ของสินค้าไว้ที่ผู้ให้บริการ

ในปัจจุบันได้มีงานวิจัยที่มีการพัฒนาเพื่อให้เป็นผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัล แต่ละงานวิจัยจะมีจุดสนใจลงไปศึกษาที่แตกต่างกัน เช่น มีความสนใจในเรื่องการเพิ่มความสามารถของการให้บริการป้องกันลิขสิทธิ์ดิจิทัลโดยการแก้ไขเพิ่มเติมไฟล์ใบอนุญาต โดยที่ยังคงรายละเอียดของเนื้อหาที่ได้รับการป้องกันลิขสิทธิ์ไว้แล้วตามเดิม อย่างไรก็ตามค่าใช้จ่ายในการติดตั้งระบบยังคงมีความสูงอยู่ หรือในบางงานวิจัยนั้นเป็นการพัฒนามาตรฐานที่ใช้กับการป้องกันลิขสิทธิ์ดิจิทัลขึ้นมาที่อนุญาตให้นักเขียนหรือเจ้าของลิขสิทธิ์สามารถที่จะควบคุมจำนวนหรือการคัดลอกข้อมูลจากลูกค้าได้ อย่างไรก็ตามงานวิจัยดังกล่าวยังคงครอบคลุมเฉพาะบางกลุ่มสินค้า อาทิเช่น เกมส์ เสียงเรียกเข้า เพลง วีดีโอ หรือ เนื้อหาสตรีมมิ่ง (Streaming media) เป็นต้น

ดังนั้นเมื่อวิเคราะห์จากปัจจัยต่าง ๆ ที่ได้กล่าวมาข้างต้นหัวข้องานวิจัยที่น่าสนใจจึงเป็นงานวิจัยเกี่ยวกับการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัลที่ข้อมูลทั้งหมดของสินค้ายังคงถูกเก็บไว้ยังแหล่งเก็บข้อมูลบนกลุ่มเมฆส่วนบุคคลของเจ้าของลิขสิทธิ์ โดยที่ระบบของผู้ให้บริการจำเป็นต้องไปอ่านข้อมูลจากแหล่งดังกล่าว แล้วนำมาป้องกันลิขสิทธิ์ดิจิทัล จากนั้นจึงส่งข้อมูลที่ได้รับการเข้ารหัสเป็นที่เรียบร้อยแล้ว กลับไปเก็บยังแหล่งเก็บข้อมูลที่เจ้าของลิขสิทธิ์เอง และในอีกส่วนหนึ่งที่มีความสำคัญที่สุดของระบบ ได้แก่ การบริหารจัดการกุญแจรหัสลับที่ใช้ในการเข้ารหัสสินค้า และเพื่อเป็นการป้องกันกุญแจรหัสลับดังกล่าว จึงมีการนำเสนอระบบขึ้นมาใช้งานในอีก 2 ส่วน ได้แก่ ระบบการกระจายกุญแจรหัสลับ ที่ใช้แนวความคิดทางด้านการกระจายความลับ เพื่อส่งต่อไปรักษายังเครื่องแม่ข่ายเสมือนเครื่องต่าง ๆ และส่วนการเก็บรวบรวมกุญแจรหัสลับเพื่อนำกลับมาใช้งานต่อไป และถึงแม้ว่าเรื่องของการกระจายความลับจะไม่ใช่เรื่องใหม่ แต่งานวิจัยฉบับนี้จะมีการนำเอาแนวคิดทางด้านการเข้ารหัสเครือข่าย (Network coding) มาประยุกต์ใช้งานกับการกระจายความลับต่อไป

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาและพัฒนาระบบให้บริการป้องกันลิขสิทธ์ดิจิทัลสำหรับผู้ให้บริการที่ข้อมูลสินค้าถูกจัดเก็บไว้ยังแหล่งเก็บข้อมูลบนกลุ่มเมฆส่วนบุคคล (Personal cloud storage) ของเจ้าของลิขสิทธิ์

2. เพื่อศึกษาและพัฒนาระบบการจัดการการแบ่งกุญแจรหัสลับเป็นหลายส่วนด้วยการใช้แนวคิดการเข้ารหัสเครือข่าย (Network coding)

ขอบเขตของการวิจัย

การศึกษานี้เป็นการศึกษาเทคโนโลยีการป้องกันลิขสิทธิ์ดิจิทัลด้วยกระบวนการการเข้ารหัสข้อมูลสินค้าที่ไม่มีการเก็บข้อมูลสินค้าไว้ภายในส่วนผู้ให้บริการ รวมไปถึงมาตรการในการรักษาความปลอดภัยด้วยการแบ่งการเก็บกุญแจรหัสลับไว้เป็นหลายส่วน โดยมีขอบเขตการวิจัยดังต่อไปนี้

1. พัฒนาระบบให้บริการป้องกันลิขสิทธิ์ดิจิทัล ที่ทำงานอยู่บนการประมวลผลแบบกลุ่มเมฆ

2. การเชื่อมต่อกันระหว่างระบบป้องกันลิขสิทธิ์ดิจิทัล และแหล่งเก็บข้อมูลบนกลุ่มเมฆส่วนบุคคล มีการทดสอบการใช้งานอยู่บนแหล่งเก็บข้อมูล Dropbox

3. การพัฒนาระบบการจัดเก็บกุญแจรหัสลับแบ่งการพัฒนาออกเป็น 2 ส่วน ได้แก่ ส่วนการกระจายกุญแจรหัสลับ และส่วนการรวบรวมกุญแจรหัสลับ

4. การจัดเก็บกุญแจรหัสลับ มีการใช้งานอยู่บนระบบคอมพิวเตอร์เสมือน (Virtual machine server) จำนวน 4 และ 8 เครื่อง ตามลำดับ

ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถพัฒนา และให้บริการระบบป้องกันลิขสิทธ์ดิจิทัลสำหรับผู้ให้บริการ ที่ทำงานอยู่บนการประมวลผลแบบกลุ่มเมฆได้

2. สามารถเข้าใจถึงแนวทางในการพัฒนาระบบที่มีการเชื่อมต่อกันระหว่างระบบป้องกันลิขสิทธิ์ดิจิทัล และแหล่งเก็บข้อมูลบนกลุ่มเมฆส่วนบุคคล

3. สามารถเข้าใจแนวคิดการเข้ารหัสเครือข่าย และประยุกต์ใช้งานกับการแบ่งกุญแจรหัสลับเป็นหลายส่วนได้

ขั้นตอนและวิธีการดำเนินการวิจัย

1. ศึกษารูปแบบการการจัดทำระบบป้องกันลิขสิทธิ์ดิจิทัล และการกระจายและรวบรวมกุญแจรหัสลับ

2. ออกแบบการทดลอง และเขียนโปรแกรมเพื่อทดสอบประสิทธิภาพการกระจายกุญแจรหัสลับที่สภาพแวดล้อมต่าง ๆ

3. สรุปผลการทำงานเพื่อนำมาวิเคราะห์ และหารูปแบบการกระจายกุญแจรหัสลับที่เหมาะสม

บทที่ 2
เอกสารและงานวิจัยที่เกี่ยวข้อง

การบริหารจัดการลิขสิทธิ์ดิจิทัล

Prihandoko, Litow and Ghodosi, (2012) ได้อธิบายไว้ว่าการบริหารจัดการลิขสิทธิ์ดิจิทัล มีความสำคัญอย่างยิ่ง อันเนื่องมาจากการเจริญเติบโตของอินเทอร์เน็ต รวมไปถึงยอดการจำหน่าย ที่เพิ่มขึ้นอย่างรวดรวดของตลาดอุปกรณ์พกพาอิเล็กทรอนิกส์ (Smart device) ในปัจจุบัน ที่รวบรวมข้อมูลโดยบริษัทสำรวจข้อมูล International Data Corporation (IDC) จึงส่งไปให้ ตลาดสื่อสิ่งพิมพ์ดิจิทัลมีการเจริญเติบโตขึ้นอย่างรวดเร็วทั้งในต่างประเทศ และรวมถึงภายในพื้นที่ ประเทศไทย ข้อมูลดิจิทัลเป็นชนิดของข้อมูลมีประสิทธิภาพสูงในการขนส่ง การจัดเก็บข้อมูลที่ไม่ จำเป็นต้องมีพื้นที่กักเก็บสินค้าที่มีขนาดใหญ่หรือเทียบเท่าคลังสินค้า และสามารถแจกจ่ายไปได้ อย่างรวดเร็ว มีต้นทุนที่ต่ำ จากประสิทธิภาพที่กล่าวมาข้างต้น ทำให้ตลาดสื่อสิ่งพิมพ์ดิจิทัลนั้น เติบโตได้อย่างรวดเร็วอย่างมีนัยสำคัญ อย่างไรก็ตามภายใต้ประสิทธิภาพและความสะดวกสบายนี้ กลับแฝงไปด้วยภัยร้ายมากมาย อาทิเช่น ความง่ายในการคัดลอกที่เป็นช่องโหว่ให้ผู้ไม่ประสงค์ดี นำข้อมูลออกไปแจกจ่ายต่อสาธารณะโดยไม่ได้รับอนุญาต ซึ่งก่อให้เกิดความสูญเสียต่อตลาด ในภาพรวม รวมถึงสูญเสียผลประกอบการทางธุรกิจต่อผู้ครอบครองลิขสิทธิ์เป็นอย่างมาก ดังนั้น เพื่อเป็นการป้องกันสิ่งที่จะเกิดขึ้นกับผู้ครอบครองลิขสิทธิ์ ปัจจุบันจึงได้มีแนวทางการป้องกันด้วย เทคโนโลยีสมัยใหม่ ซึ่งเทคโนโลยีนั้นได้แก่ เทคโนโลยีการป้องกันลิขสิทธิ์ดิจิทัล

Liu, Safavi-Naini and Sheppard, (2003) ได้ระบุไว้ว่าการจัดการลิขสิทธิ์ดิจิทัล (Digital right management หรือเรียกสั้น ๆ ว่า DRM) เป็นเทคโนโลยีที่ใช้โดยผู้ครอบครองลิขสิทธิ์ เพื่อที่ จะนำมาเป็นอาวุธที่ใช้ในการป้องกันและปกป้องผลประโยชน์ที่ตนเองควรได้รับจาก กลุ่มผู้ไม่ประสงค์ดีที่ก่อให้เกิดความสูญเสีย อาทิเช่น การป้องกันการคัดลอกและเผยแพร่ข้อมูล เป็นบางส่วน หรือทั้งหมด การควบคุมกำหนดขอบเขตการเข้าถึง การควบคุมวิธีใช้งานตามแต่ ผู้ครอบครองลิขสิทธิ์จะกำหนดไว้ ซึ่งตามปกติแล้วแนวทางการป้องกันลิขสิทธิ์ดิจิทัลนั้น มีหลายแนวทาง เช่น ในเชิงของความปลอดภัยของข้อมูล ข้อมูลทั้งหมดก็จะถูกเข้ารหัสลับป้องกัน ไว้ ส่งผลให้เมื่อผู้ที่ได้รับมีความต้องการเปิดข้อมูลขึ้นมา จำเป็นต้องใช้โปรแกรมหรือซอร์ฟแวร์ ที่ได้รับอนุญาตเท่านั้น แต่ในปัจจุบันเรื่องของลิขสิทธิ์ดิจิทัลไม่เฉพาะเจาะจงลงไปในเรื่องของ การเข้ารหัสข้อมูลเท่านั้น แต่ยังคงมีวิธีการควบคุมต่าง ๆ มากมาย เช่น การขอยืนยันตัวบุคคล ในการเข้าถึงด้วยการใช้ชื่อผู้ใช้งานและรหัสผ่านหรือการควบคุมด้วยลายนิ้วมือ การติดตาม

การส่งต่อข้อมูล การใส่ลายน้ำเพื่อปกป้องข้อมูลสำคัญ การไม่อนุญาตในการคัดลอกข้อมูลจากบุคคลบางกลุ่ม เป็นต้น

ตามปกติแล้วผู้ครอบครองสิทธิ์ดิจิทัลนั้นไม่ได้ถูกจำกัดความว่าจะต้องเป็นเพียงเฉพาะผู้ครอบครองสิทธิ์ในสื่อสิ่งพิมพ์ดิจิทัลเท่านั้น แต่การครอบครองสิทธิ์นั้นครอบคลุมไปถึงไฟล์จำพวกเพลง วีดีโอ หรือกระทั่งเกมส์ต่าง ๆ

ทั่วไปแล้วในการป้องกันลิขสิทธิ์ดิจิทัลมีข้อควรคำนึงถึงดังต่อไปนี้

1. การทำงานร่วมกัน

ด้วยความหลากหลายของชนิดเนื้อหาดิจิทัล อาทิเช่น เสียง เพลง วิดีโอ ภาพ หรือสื่อสิ่งพิมพ์ดิจิทัล และด้วยความหลากหลายของแพลตฟอร์มที่ใช้งาน เช่น พีซี แล็ปท็อป โทรศัพท์เคลื่อนที่ และอื่น ๆ ดังที่กล่าวมาข้างต้น เห็นได้ว่าสิ่งสำคัญที่นักพัฒนาหรือผู้ครอบครองลิขสิทธิ์จะต้องคำนึงถึง ได้แก่ การป้องกันจุดอ่อนจากการทำงานร่วมกัน

2. ความปลอดภัย

เมื่อการป้องกันลิขสิทธิ์ดิจิทัลได้ถูกพัฒนาขึ้นมา จึงเป็นที่หลีกเลี่ยงไม่ได้ที่จะมีผู้ไม่ประสงค์ดีเกิดความต้องการที่จะโจมตีระบบ ดังนั้นในการพัฒนาจึงควรต้องพัฒนาระบบโดยให้มีความสามารถในการทนทานต่อการถูกโจมตีได้

3. ความเป็นส่วนบุคคล

โดยปกติทั่วไปแล้วระบบการป้องกันลิขสิทธิ์ดิจิทัลนั้นถูกนำไปใช้งานกับกลุ่มธุรกิจพาณิชย์อิเล็กทรอนิกส์ ที่จำเป็นจะต้องมีการเก็บข้อมูลของลูกค้าไว้ ดังนั้นเพื่อให้เกิดความน่าเชื่อถือที่สุดการจัดเก็บข้อมูลดังกล่าวต้องห้ามเปลี่ยนแปลงข้อมูลส่วนใดส่วนหนึ่งอย่างเด็ดขาด

4. ความสมดุลกันของความซับซ้อน และความมีประสิทธิภาพ

ข้อสำคัญในการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัลขึ้นมานั้นอีกสิ่งสำคัญที่ต้องคำนึงถึงได้แก่ ความสมดุลกันของความซับซ้อน และประสิทธิภาพ เช่น ระบบที่มีความซับซ้อนสูงค่าใช้จ่ายในการพัฒนาย่อมสูงขึ้นตาม และจะส่งผลเสียโดยตรงกับลูกค้าที่เข้ามาใช้งาน เนื่องจากต้นทุนในการผลิตที่สูงขึ้น และถึงแม้ว่าระบบที่มีความซับซ้อนสูงจะมีประสิทธิภาพสูงก็ตาม แต่ในบางกรณีระบบที่มีความซับซ้อนไม่มากนักก็สามารถทนทานต่อการถูกโจมตีได้เช่นกัน

ความสำคัญของระบบป้องกันลิขสิทธิ์ดิจิทัล

ระบบป้องกันลิขสิทธิ์ดิจิทัลเป็นช่องทางที่ก่อให้เกิดความเชื่อมโยงกันระหว่างเจ้าของลิขสิทธิ์ และผู้ใช้งาน Dingledy and Matamoros, (2016) ระบุว่า การป้องกันลิขสิทธิ์ดิจิทัล เป็นกระบวนการที่เกิดขึ้นมาเพื่อคั่นกลาง เพื่อควบคุมในการเข้าถึงข้อมูลดิจิทัล หรือควบคุมระหว่างการขนถ่ายข้อมูลและการใช้งาน หรือให้ความหมายอีกนัยนึงว่า เป็นเครื่องมือที่เจ้าของลิขสิทธิ์ใช้ในการควบคุมการเข้าถึงข้อมูลต่าง ๆ ของผู้ได้รับอนุญาต โดยในการควบคุมต่าง ๆ สามารถแบ่งได้ดังนี้

1. การควบคุมการเข้าถึง (Access control)

ในการควบคุมการเข้าถึงของข้อมูลของระบบป้องกันลิขสิทธิ์ดิจิทัลมีหลากหลายรูปแบบในปัจจุบัน แต่เป้าหมายในการทำงานทั้งหมดยังคงอยู่ที่การจำกัดช่องทางทั้งการเข้าถึงข้อมูล หรือจะจัดการกับข้อมูลอย่างไรตามที่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์ด้วยระบบจัดการสิทธิ์การเข้าถึง (Permission management) ดังรายละเอียดต่อไปนี้

1.1 การยินยอมให้เข้าใช้งานด้วยการใช้รหัส (Software license and key) ในปัจจุบันการที่ผู้ใช้งานสามารถเข้าใช้งานโปรแกรมคอมพิวเตอร์ที่ถูกลิขสิทธิ์ได้นั้น ผู้ใช้งานจำเป็นต้องได้รับรหัสชนิดหนึ่ง ซึ่งภายในประกอบไปด้วยอักขระจำนวนหนึ่งที่ผู้ใช้งานต้องระบุก่อนเริ่มต้นใช้งานโปรแกรม โดยในขั้นตอน โปรแกรมคอมพิวเตอร์ทำการส่งรหัสดังกล่าวเพื่อไปยืนยันกับผู้ผลิตผ่านทางเครือข่ายอินเทอร์เน็ตต่อไป หรือในอีกแนวทางหนึ่งทางผู้ผลิตสามารถกำหนดช่องทางให้ผู้ใช้งานสามารถติดต่อกลับเพื่อขอเปิดใช้งานโปรแกรมได้

1.2 การเข้าใช้งานระบบด้วยการยืนยันตัวบุคคล (User Authentication) เป็นกระบวนการเพื่อควบคุมการเข้าถึงที่ได้รับความนิยมมากในปัจจุบัน เนื่องจากเป็นระบบที่สามารถยืนยันได้ตัวบุคคลที่เข้ามาใช้งานได้ว่าเป็นบุคคลที่มีตัวตนจริง และมีสิทธิในการเข้าถึงระบบจริง ไม่ว่าจะมาจากการซื้อขายสินค้า หรือส่งมอบด้วยวิธีการอื่นใด ตามที่ Dingledy and Matamoros, (2016) ได้ระบุว่า โดยปกติแล้วการยืนยันตัวบุคคลนั้นมี 3 แนวทางที่ใช้กันอย่างแพร่หลาย ดังนี้

1.2.1 การใช้ข้อมูลเพื่อยืนยันตัวบุคคลจากสิ่งที่ผู้ใช้งานรู้อยู่แต่เดิม (Something you know) ที่พบเห็นกันบ่อย ๆ ได้แก่ การใช้งานรหัสผ่าน หรือการตั้งคำถามที่คำตอบจะมีแต่เพียงตัวบุคคลนั้น ๆ เท่านั้นที่สามารถรู้คำตอบของคำถามได้ ซึ่งรวมถึงการใช้รหัสบัตรและรหัสผ่านที่เกี่ยวข้อง

1.2.2 การใช้ข้อมูลเพื่อยืนยันตัวบุคคลจากสิ่งที่ผู้ใช้งานมี (Something you have) เช่น การใช้งานโทรศัพท์มือถือ เพื่อยืนยันตัวบุคคล โดยวิธีที่พบเห็นได้อย่างแพร่หลาย ได้แก่ การที่

เจ้าของลิขสิทธิ์ส่งข้อความตัวอักขระบางอย่างให้กับผู้ใช้งานผ่านทางเครือข่ายโทรศัพท์มือถือส่วนบุคคล

1.2.3 การใช้ข้อมูลเพื่อยืนยันตัวบุคคลจากสิ่งที่ผู้ใช้งานย่อมมีอยู่โดยเฉพาะบุคคล (Something you are) อาทิเช่น การยืนยันตัวบุคคลจากลายนิ้วมือ การยืนยันตัวบุคคลจากม่านตา เป็นต้น

1.3 การควบการเข้าถึงข้อมูลด้วยลักษณะทางภูมิศาสตร์ (Regional restriction) ในปัจจุบันข้อมูลดิจิทัลที่อยู่ในรูปแบบของข้อมูลที่ให้ความบันเทิง อาทิ การซื้อขายภาพยนตร์ เพลง รายการโทรทัศน์ หรือหนังสือในบางรูปแบบ สามารถควบคุมการจำหน่ายหรือการใช้งานได้ตามลักษณะทางภูมิศาสตร์ เช่น การเข้าถึงข้อมูลได้จากบางประเทศ โดยหลังจากที่ผู้ใช้งานยืนยันตัวบุคคลกับระบบเรียบร้อยแล้วนั้น ในขั้นตอนถัดไประบบทำการตรวจสอบที่อยู่ไอพี (IP Address) ของคอมพิวเตอร์ที่ใช้งาน หากไม่ได้รับอนุญาตให้ใช้งาน ผู้ใช้งานจะไม่สามารถใช้งานข้อมูลนั้นได้

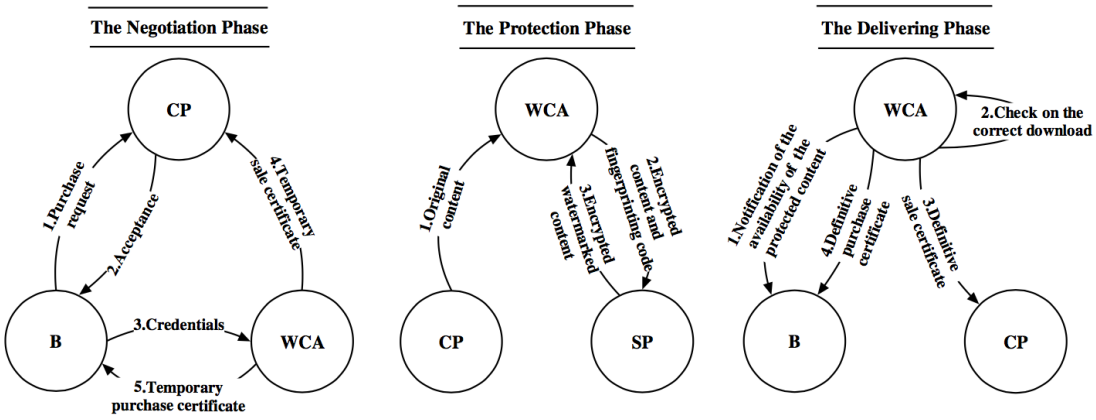
1.4 การควบคุมการเข้าถึงข้อมูลด้วยการจำกัดประเภทอุปกรณ์ หรือโปรแกรมที่ใช้งาน (Trusted computing) ในหลากหลายอุปกรณ์ที่ผู้ผลิตได้กำหนดว่าการที่จะใช้ข้อมูลดิจิทัลนั้น ๆ จำเป็นต้องใช้งานผ่านทางอุปกรณ์ หรือโปรแกรมที่ผู้ผลิตระบุได้อย่างชัดเจน เช่น เครื่องเล่นเกมส์ต่าง ๆ ที่จำเป็นต้องใช้งานกับอุปกรณ์ที่เฉพาะเจาะจง หรือโปรแกรมอ่านหนังสืออิเล็กทรอนิกส์ที่การใช้งานสินค้านั้น ๆ จำเป็นต้องใช้โปรแกรมที่เฉพาะเจาะจงเพื่อการอ่านเท่านั้น เนื่องจากในไฟล์หนังสืออิเล็กทรอนิกส์บางประเภทนั้นมีการเข้ารหัสสินค้าด้วยการใช้กุญแจรหัสลับ เป็นต้น

2. การป้องกันการคัดลอกข้อมูลดิจิทัล (Copy protection)

นอกเหนือจากการที่ระบบป้องกันลิขสิทธิ์ดิจิทัลใช้งานในป้องกันการเข้าถึงข้อมูลแล้วนั้น อีกหนึ่งความสำคัญ ได้แก่ การป้องกันการคัดลอกข้อมูลดิจิทัลโดยบุคคลผู้ไม่พึงประสงค์ดีกับลิขสิทธิ์ของเจ้าของอันพึงจะมี ในการป้องกันการคัดลอกข้อมูลดิจิทัลนั้น ในปัจจุบันมีการนำเสนอเทคโนโลยีหลากหลายรูปแบบมาช่วยในกระบวนการดังกล่าว Frattolillo and Landolfi, (2008) กล่าวว่า “การบริหารจัดการลิขสิทธิดิจิทัลเป็นการป้องกันและบังคับ ให้เกิดการใช้งานที่ถูกกฎหมายในการกระจายข้อมูลดิจิทัลบนเครือข่ายอินเทอร์เน็ต” ดังมีรูปแบบชนิดการป้องกันการคัดลองข้อมูลดิจิทัลดังนี้

2.1 การสร้างลายน้ำเพื่อป้องกันลิขสิทธิ์ดิจิทัล (Digital Watermarking) Dingledy and Matamoros, (2016) กล่าวว่าการสร้างลายน้ำเพื่อป้องกันลิขสิทธิ์นั้นได้มีผู้คิดริเริ่มมาตั้งแต่การใช้ข้อมูลบนกระดาษ โดยผู้ส่งสารได้ทำการใส่ลายน้ำที่สามารถมองเห็นได้เมื่อส่องกระดาษไว้ใกล้กับเทียนไข ดังนั้นด้วยการประยุกต์ตามแนวทางทฤษฎีเดียวกันการใส่ลายน้ำดิจิทัลจึงเริ่มได้รับความแพร่หลายด้วยการใส่ชุดข้อมูลดิจิทัลบางอย่างที่เจ้าของลิขสิทธิ์แต่เพียงผู้เดียว

ที่สามารถรู้ตำแหน่งในการใส่ลายน้ำ และในกรณีที่เจ้าของลิขสิทธิ์ได้ทำการระบุข้อมูลที่แตกต่างกันในการส่งมอบข้อมูลแต่ละครั้ง ย่อมเป็นเหตุให้ระบุได้ว่าข้อมูลชุดดังกล่าวออกมาจากบุคคลหรือหน่วยงานใด ซึ่งสามารถส่งผลให้เจ้าของลิขสิทธิ์สามารถดำเนินการตามกฎหมายต่อไปได้



ภาพที่ 2-1 โปรโตคอลการทำลายน้ำ

จากภาพที่ 2-1 Frattolillo and Landolfi, (2008) ได้นำเสนอระบบป้องกันลิขสิทธิ์ดิจิทัลสำหรับป้องกันสื่อผสมต่าง ๆ ที่ต้องการนำไปกระจายบนเครือข่ายอินเทอร์เน็ตด้วยการนำเทคโนโลยีลายน้ำมาประยุกต์ใช้ โดยแบ่งการทำงานออกเป็น 3 ส่วน ได้แก่ ส่วนการต่อรอง (The negotiation phase) ส่วนการป้องกัน (The protection phase) และส่วนการส่งข้อมูล (The delivering phase) โดยหลังจากที่ผู้ซื้อได้เสร็จสิ้นกระบวนการซื้อสื่อผสมดิจิทัลจากทางเจ้าของลิขสิทธิ์แล้ว ผู้ซื้อจำเป็นต้องติดต่อไปยังส่วนการยืนยันตัวบุคคลของระบบสร้างลายน้ำเพื่อส่งข้อมูลจำเพาะไปยังระบบ และส่งต่อไปยังผู้ขาย หรือเจ้าของลิขสิทธิ์ต่อไป จากนั้นระบบเข้าสู่ส่วนการทำงานของส่วนการป้องกันข้อมูล ทางเจ้าของลิขสิทธิ์เริ่มดำเนินการส่งข้อมูลจำเพาะเพื่อสร้างลายน้ำให้กับระบบ และเข้าสู่ส่วนการส่งข้อมูลต่อไป เพื่อส่งข้อมูลต่าง ๆ ให้กับผู้ใช้งาน โดยระบบที่นำเสนอนี้ ผู้วิจัยเห็นว่าส่วนที่สำคัญที่สุดในกระบวนการ ได้แก่ การยืนยันตัวบุคคลและสร้างลายน้ำ จะทำอย่างไรเพื่อให้สามารถแยกแยะได้ว่าสินค้าที่ออกไปในระบบนั้นบุคคลหรือหน่วยงานใดเป็นผู้ที่ติดต่อซื้อหรือได้รับการแจกจ่ายจากเจ้าของลิขสิทธิ์ โดยที่บุคคลหรือหน่วยงานนั้นสามารถยืนยันได้ว่ามีตัวตน

2.2 การเข้ารหัสข้อมูลเพื่อป้องกันลิขสิทธิ์ดิจิทัล (Digital content encryption) สำหรับการป้องกันลิขสิทธิ์ดิจิทัลในรูปแบบนี้ Dingledy and Matamoros, (2016) ได้ระบุไว้ว่า สื่อผสม

ดิจิทัลนั้นถูกเขียนขึ้นมาใหม่ด้วยชุดคำสั่งที่สามารถอ่านได้จากอุปกรณ์ หรือโปรแกรมประยุกต์ที่ได้กำหนดไว้แล้วเท่านั้น ด้วยการใช้กุญแจรหัสลับที่ทราบกันเพียงเจ้าของลิขสิทธิ์ และอุปกรณ์หรือโปรแกรมประยุกต์ดังกล่าวในการเข้ารหัสให้ไฟล์ข้อมูลเกิดการเปลี่ยนแปลงไปในรูปแบบที่ไม่สามารถเข้าใจได้ กระทั่งผ่านเข้าสู่กระบวนการถอดรหัสข้อมูลให้ย้อนกลับมาเป็นข้อมูลที่ไม่มีการปกปิดต่อไป

ในปัจจุบันเทคโนโลยีในการเข้ารหัสข้อมูลเพื่อป้องกันลิขสิทธิ์ดิจิทัลมีมากมายหลายรูปแบบทั้งที่อยู่ในรูปแบบของการเข้ารหัสแบบสมมาตร (Symmetric encryption) และการเข้ารหัสแบบอสมมาตร (Asymmetric encryption)

การเข้ารหัสแบบสมมาตร (Symmetric encryption) เป็นการเข้ารหัสข้อมูล และถอดรหัสด้วยการใช้กุญแจรหัสลับตัวเดียวกันระหว่างผู้ส่งสารและผู้รับสาร ดังนั้นเพื่อให้กระบวนการสามารถทำงานได้ถูกต้อง ระหว่างผู้รับสาร และผู้ส่งสาร จำเป็นต้องได้รับข้อตกลงเพื่อแลกเปลี่ยนกุญแจรหัสลับระหว่างกัน หรือในอีกนัยหนึ่ง โปรแกรมประยุกต์ที่สามารถนำมาใช้งานได้นั้นจำเป็นต้องมีการเก็บกุญแจรหัสลับไว้ภายในระบบ การนำวิธีการเข้ารหัสแบบสมมาตรมาประยุกต์ใช้งานสามารถเลือกใช้ได้ตามความเหมาะสม เนื่องจากการเข้ารหัสแบบสมมาตรมีหลากหลายอัลกอริทึมในการใช้งาน อาทิ การเข้ารหัสด้วยมาตรฐาน DES และ การเข้ารหัสด้วยมาตรฐาน AES

การเข้ารหัสแบบอสมมาตร (Asymmetric encryption) เป็นการเข้ารหัสข้อมูลที่มีความแตกต่างกับการเข้าแบบสมมาตรโดยสิ้นเชิง เนื่องจากกุญแจรหัสลับที่ใช้ในการเข้ารหัสนั้นใช้ความสามารถในการแลกเปลี่ยนกุญแจสาธารณะ (Public key) ระหว่างกันผ่านทางเครือข่าย และในกระบวนการถอดรหัสจะใช้กุญแจส่วนตัว (Private key) ในการถอดรหัสข้อมูล เห็นได้ชัดเจนว่าการเข้ารหัสข้อมูลด้วยเทคโนโลยีการเข้ารหัสแบบอสมมาตร มีข้อได้เปรียบกว่าการเข้ารหัสแบบสมมาตร เนื่องจากผู้ส่งสาร และผู้รับสาร สามารถแลกเปลี่ยนกุญแจสาธารณะกันได้ตลอด เพื่อเป็นการป้องกันผู้ไม่ประสงค์ดีกับระบบ

จากข้อมูลในส่วนต่าง ๆ ที่ผ่านมา เห็นได้ว่าการป้องกันลิขสิทธิ์ดิจิทัลเป็นส่วนสำคัญที่ส่งให้การค้าในตลาดธุรกิจดิจิทัลสามารถดำเนินต่อไปได้ และในการป้องกันลิขสิทธิ์นั้นมีหลายส่วนที่ต้องให้ความสำคัญไม่ว่าจะเป็นชนิดของข้อมูล การยืนยันตัวบุคคล และการป้องกันการคัดลอกลิขสิทธิ์ ดังนั้นงานวิจัยฉบับนี้จึงมีแนวคิดริเริ่มในการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัลขึ้นมาดังรายละเอียดต่อไป

ระบบการประมวลผลแบบกลุ่มเมฆ

ภาคภูมิ อุทัยเลิศ, (2553) กล่าวว่า ระบบประมวลผลแบบกลุ่มเมฆ (Cloud computing) เป็นระบบที่ได้รับความนิยมมาระยะหนึ่ง และมีแนวโน้มเป็นที่สนใจในหลายองค์กรในประเทศไทย เนื่องจากประสิทธิภาพในการประมวลผล และลดค่าใช้จ่ายในการบำรุงรักษาอุปกรณ์ ระบบประมวลผลแบบกลุ่มเมฆ เป็นระบบการประมวลผลที่อ้างอิงตามการใช้งานของผู้ใช้ ทั้งในเรื่องค่าใช้จ่าย การจัดสรรทรัพยากรต่าง ๆ ที่สามารถเพิ่มลดได้โดยมีผลกระทบกับผู้ใช้บริการน้อยที่สุด

ลักษณะจำเพาะของระบบประมวลผลแบบกลุ่มเมฆ

Abbasov, (2014) ได้กล่าวไว้ว่าข้อมูลที่ใช้บ่งบอกลักษณะจำเพาะของระบบประมวลผลแบบกลุ่มเมฆนั้นแบ่งได้เป็น 5 ลักษณะจำเพาะดังนี้

1. การกำหนดความต้องการด้วยตนเอง (On-demand self-service) ในระบบการประมวลผลแบบกลุ่มเมฆ สิ่งที่ขาดไม่ได้ ได้แก่ การกำหนดความต้องการทรัพยาการของเครื่องแม่ข่ายเสมือนที่ให้บริการได้ด้วยต้นเอง เช่น ระยะเวลาในการใช้งาน ขนาดของเครือข่าย ขนาดของพื้นที่การเก็บข้อมูล โดยการทำงานทั้งหมด ระบบต้องสามารถทำได้โดยอัตโนมัติปราศจากการใช้บุคคลในการให้บริการ

2. การเข้าถึงเครือข่าย (Broad network access) ระบบการประมวลผลแบบกลุ่มเมฆอีกสิ่งสำคัญที่ขาดไม่ได้อีกหนึ่งสิ่ง ได้แก่ การเข้าถึงเครือข่ายอินเทอร์เน็ต เนื่องจากการเข้าถึงบริการต่าง ๆ รวมถึงการเข้าถึงข้อมูลในเชิงลึกของผู้ดูแลระบบ จำเป็นต้องมีการเชื่อมต่อไปยังเครื่องแม่ข่ายเสมือน อาทิ การเข้าถึงผ่านช่องทางเทอร์มินอล จากอุปกรณ์คอมพิวเตอร์ หรือสมาร์ทโฟนต่าง ๆ

3. การจัดสรรทรัพยากร (Resource pooling) ในการประมวลผลต่าง ๆ ของระบบประมวลผลแบบกลุ่มเมฆ จำเป็นต้องมีการแบ่งปันการใช้ทรัพยากรของเครื่องแม่ข่ายหลัก ไปยังกลุ่มผู้ใช้งานหลายกลุ่ม โดยในการแบ่งปันนั้นระบบบริหารจัดการต้องสามารถจัดสรรทรัพยากรเสมือนไปยังกลุ่มเครื่องแม่ข่ายเสมือนต่าง ๆ ได้ตามที่ได้รับความต้องการมาโดยอัตโนมัติ โดยที่ผู้ใช้บริการไม่มีความจำเป็นต้องทราบถึงปริมาณทรัพยาทั้งหมดที่มี ยกเว้นในส่วนของประเทศที่ตั้งหรือสถานที่ตั้งของศูนย์ข้อมูล โดยในส่วนทรัพยากรที่สามารถจัดสรรได้นั้น ประกอบไปด้วยทรัพยากรต่าง ๆ ดังนี้ พื้นที่ในการเก็บข้อมูล หน่วยประมวลผล หน่วยความจำ และความเร็วโครงข่าย

4. ความยืดหยุ่น (Rapid elasticity) สำหรับทรัพยากรที่ระบบได้ทำการจัดสรรให้กับผู้ใช้งานนั้น ต้องมีความสามารถในการลดหรือเพิ่มได้อย่างยืดหยุ่นอย่างเหมาะสมตามความต้องการใช้งาน โดยที่ผู้บริโภคสามารถขยายหรือลดขนาดได้ตลอดเวลา

5. การควบคุมและวัดผล (Monitored and Measured service) ทรัพยากรต่าง ๆ ของระบบต้องสามารถควบคุมและปรับปรุงประสิทธิภาพได้โดยอัตโนมัติ ด้วยเครื่องมือตามที่ระบบได้จัดสรรไว้ตามประเภทของการให้บริการ เช่น การให้บริการทางด้านการเก็บบันทึกข้อมูล หน่วยประมวลผล โครงข่าย หรือ จำนวนผู้ใช้งาน โดยระบบดังกล่าวต้องสามารถรายงานผลต่าง ๆ ไปยังผู้ให้บริการ และผู้รับบริการได้เพื่อความโปร่งใสของระบบ

ประเภทการให้บริการของระบบบริการแบบกลุ่มเมฆ

ระบบการประมวลผลแบบกลุ่มเมฆเป็นระบบที่รวบรวมเอาการประมวลผล พื้นที่จัดเก็บข้อมูล และอื่น ๆ อีกมากมายที่เกี่ยวข้องมารวบรวมเพื่อจัดทำเป็นการให้บริการให้กับผู้ใช้งานโดยเสียค่าบริการตามการใช้งานจริงผ่านทางเครือข่ายอินเทอร์เน็ต สามารถเพิ่ม หรือลดขนาดการบริการได้โดยอัตโนมัติตามความต้องการในการใช้งาน โดยยังคงเสถียรภาพสูง ง่ายต่อการเข้าถึง และช่วยลดค่าใช้จ่ายของการดูแลระบบ โดยมีวิวัฒนาการดังนี้

ในปี 2503 John MaCarthy นำเสนอวิธีการประมวลผลค่าบริการต่าง ๆ ที่ถูกส่งต่อไปยังผู้บริโภค อาทิ ค่าไฟฟ้า ค่าน้ำ และค่าแก๊ส

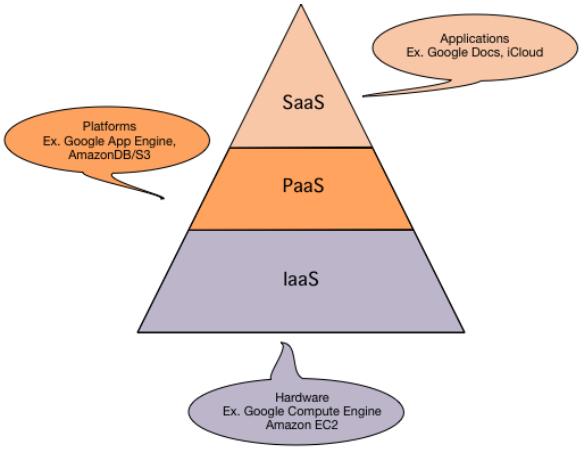
ในปี 2533 ระบบประมวลผลแบบกลุ่มเมฆได้ถูกริเริ่มขึ้นมาโดยรู้จักกันในรูปแบบของระบบ ATM

ในปี 2549 Eric Schmidt ผู้บริหารของบริษัทกูเกิ้ล ได้นำเสนอคำว่าระบบประมวลผลแบบกลุ่มเมฆขึ้นมา (Cloud computing) เพื่ออธิบายถึงลักษณะโครงสร้างทางธุรกิจของบริษัท

นับจากนั้นเป็นต้นมา คำว่าระบบประมวลผลแบบกลุ่มเมฆจึงได้รับความนิยม และเป็นที่สนใจของตลาดในวงกว้าง ตามคำกล่าวของ Weinhardt et al. (2009) จึงส่งผลให้ระบบการให้บริการของการประมวลผลแบบกลุ่มเมฆในปัจจุบันสามารถแบ่งได้ออกเป็น 3 ประเภทการบริการดังภาพที่ 2-2 โดยมีรายละเอียดดังต่อไปนี้

1. การให้บริการเชิงซอร์ฟแวร์ (Software as a Service:SaaS) การให้บริการในลักษณะนี้เป็นการให้บริการเพื่อให้ผู้ใช้งานสามารถใช้บริการได้โดยที่ไม่จำเป็นต้องติดตั้งโปรแกรมประยุกต์ใด ๆ ภายในระบบ ตามคำกล่าวของ Rani and Ranjan, (2014) ด้วยเหตุดังกล่าว การใช้งานการให้บริการในลักษณะนี้จำเป็นต้องใช้งานผ่านโปรแกรมประยุกต์จำพวกเว็บเบาร์เซอร์ (Web Browser) เพื่อควบคุมระบบ การทำงานจำพวกการให้บริการลักษณะนี้เป็นการให้บริการที่เน้นในด้านความง่ายของระบบ ความเร็วในการใช้งาน ความปลอดภัย การดูแลรักษาต่าง ๆ

และราคาในการให้บริการที่มีอัตราที่ต่ำกว่าการให้บริการในรูปแบบอื่น ๆ ตามคำกล่าวของ Kulkarni, Chavan, Bankar, Koli and Waykule, (2012) ตัวอย่างสำหรับการให้บริการเชิงซอร์ฟแวร์ที่พบเห็นได้ทั่วไปนั้น ได้แก่ SaleForce.com, Google Mail, Google Docs เป็นต้น



ภาพที่ 2-2 ประเภทการให้บริการของระบบประมวลผลแบบกลุ่มเมฆ

2. การให้บริการเชิงแพลทฟอร์ม (Platform as a Service:PaaS) การให้บริการเชิงแพลทฟอร์ม เป็นการให้บริการในลักษณะที่ระบบมีการพัฒนาโครงสร้าง และสภาพแวดล้อมพื้นฐานไว้เรียบร้อยแล้ว เพื่อให้ผู้รับบริการสามารถเช่าใช้งาน และพัฒนาโปรแกรมประยุกต์หรือการบริการต่อยอดได้ ซึ่งแตกต่างกับการให้บริการเชิงซอร์ฟแวร์ที่เป็นการให้บริการในลักษณะของโปรแกรมประยุกต์ที่ได้รับการพัฒนาครบถ้วนสมบูรณ์เรียบร้อยเท่านั้น และในอีกนัยยะหนึ่งการให้บริการเชิงแพลทฟอร์ม เป็นการให้บริการที่ผู้รับบริการไม่จำเป็นต้องวางแผนในการจัดการเรื่องโครงสร้างพื้นฐานใด ๆ ทั้งสิ้นตามกำกล่าวของ Karada, Pipliya, Thakur and Kamdar, (2013) สำหรับการคิดค่าบริการในส่วนของการให้บริการเชิงแพลทฟอร์มนั้น เกิดจากการคำนวณอัตราการโอนถ่ายข้อมูลต่อชั่วโมง อัตราการใช้งานส่วนรับและส่งข้อมูล (I/O) และการใช้งานโครงข่าย เป็นต้น ตัวอย่างงานบริการในลักษณะเชิงแพลทฟอร์มที่เห็นได้ชัดเจนในปัจจุบัน ได้แก่ Google App Engine

3. การให้บริการเชิงโครงสร้างพื้นฐาน (Infrastructor as a service:IaaS) ในรูปแบบการให้บริการลักษณะนี้เป็นการให้บริการในระดับโครงสร้างพื้นฐานของระบบไอที ได้แก่ หน่วยการประมวลผล พื้นที่จัดเก็บข้อมูล โครงข่าย และทรัพยากรพื้นฐานของการประมวลผล

การให้บริการทั้งหมดเปรียบเสมือนว่าผู้รับบริการมีเครื่องแม่ข่ายเสมือนเป็นของตน หรือที่รู้จักกันในชื่อ Virtual Private Server:VPS ตามคำกล่าวของ Hofer and Karagiannis, (2011) ในการดำเนินการในลักษณะนี้ส่งผลให้การให้บริการเครื่องแม่ข่ายเสมือนเป็นการให้บริการอย่างคลอบคลุมที่สุดของการให้บริการเชิงโครงสร้างพื้นฐานเพื่อให้ง่ายต่อการเพิ่มเติม หรือลดการใช้ทรัพยากรของผู้รับบริการ ซึ่งเป็นไปในแนวทางเดียวกับราคาการใช้งานที่เกิดขึ้นที่คำนวณตามการใช้งานจริง การติดตั้งโปรแกรมประยุกต์ หรือการให้บริการต่าง ๆ สามารถดำเนินได้ตามความต้องการของผู้รับบริการได้อย่างเต็มรูปธรรม เนื่องจากผู้รับบริการสามารถควบคุมได้ตั้งแต่ในระดับจำนวนหน่วยประมวลผล จำนวนหน่วยความจำ พื้นที่ในการเก็บข้อมูล ระบบปฏิบัติการ การควบคุม การเข้าถึงเครือข่าย สามารถขยาย หรือลดขนาดได้ตามความต้องการ เป็นต้น ตัวอย่างการให้บริการเชิงโครงสร้างพื้นฐานที่เห็นได้ชัดเจนในปัจจุบัน ได้แก่ AmazonEc2, Google Cloud Service เป็นต้น

โครงสร้างลำดับชั้นการให้บริการระบบประมวลผลแบบกลุ่มเมฆ

Abbasov, 2014 ระบุว่าสถาปัตยกรรมของการให้บริการระบบประมวลผลแบบกลุ่มเมฆนั้นสามารถแบ่งออกได้เป็น 4 ส่วน ดังต่อไปนี้ ส่วนของฮาร์ดแวร์ ส่วนของโครงสร้างพื้นฐาน ส่วนของระบบแพลทฟอร์ม และส่วนของโปรแกรมประยุกต์ดังแสดงในตารางที่ 2-1

ตารางที่ 2-1 โครงสร้างลำดับชั้นการให้บริการประมวลผลแบบกลุ่มเมฆ

ประเภทการบริการ	การจัดการทรัพยากรและบริการ	กลุ่มตัวอย่าง
การให้บริการเชิงซอร์ฟแวร์	โปรแกรมประยุกต์สำเร็จรูปเว็บเซอร์วิส และสื่อผสมต่าง ๆ **โปรแกรมประยุกต์**	Google Docs, iCloud Youtube เป็นต้น
การให้บริการแพลทฟอร์ม	โครงสร้างพื้นฐานของซอร์ฟแวร์ หรือ พื้นที่เก็บข้อมูล **แพลทฟอร์ม**	Google App Engine, Force.com, Amazon DB/S3 เป็นต้น

ตารางที่ 2-1 (ต่อ)

ประเภทการบริการ	การจัดการทรัพยากรและบริการ	กลุ่มตัวอย่าง
การให้บริการเชิงโครงสร้างพื้นฐาน	การประมวลผล พื้นที่เก็บข้อมูล	Google Compute Engine, Amazon EC2
	โครงสร้างพื้นฐาน	
	หน่วยประมวลผล	ศูนย์ข้อมูล
	หน่วยความจำ ดิสก์	
	ฮาร์ดแวร์	

ในส่วนของลำดับชั้นฮาร์ดแวร์ Abbasov, (2014) ระบุว่าเป็นการอ้างอิงถึงทรัพยากรพื้นฐานของระบบให้บริการแบบกลุ่มเมฆ ประกอบไปด้วย เครื่องแม่ข่ายและอุปกรณ์เครือข่าย การจัดการด้านพลังงาน ระบบระบายความร้อน โดยในลำดับชั้นนี้การดำเนินการทั้งหมด จะอยู่ภายใต้การดำเนินการของศูนย์ข้อมูล ประกอบไปด้วยเครื่องแม่ข่ายจำนวนมากที่เชื่อมต่อกันเป็นโครงข่าย

ลำดับชั้นโครงสร้างพื้นฐาน หรือในความเป็นจริงนั้นอยู่ในส่วนของโครงสร้างพื้นฐานเสมือน ที่ควบคุมการใช้งานฮาร์ดแวร์คอมพิวเตอร์ต่าง ๆ โดยจัดสรรการใช้งานจากทรัพยากรที่มีอยู่จริงของเครื่องแม่ข่ายด้วยเทคนิคของการทำระบบเสมือน

ลำดับชั้นแพลทฟอร์มหรือลำดับชั้นฐานงาน เป็นลำดับชั้นที่รวมถึงระบบปฏิบัติการและพื้นฐานโปรแกรมประยุกต์ต่าง ๆ การทำงานในลำดับชั้นนี้มีเป้าหมายในการลดขั้นตอนการดำเนินการของผู้รับบริการให้สามารถเข้าถึงการทำงานให้น้อยลง โดยไม่จำเป็นต้องติดตั้งระบบตั้งแต่จุดเริ่มต้น

ลำดับชั้นโปรแกรมประยุกต์ เป็นลำดับชั้นสูงสุดของระบบการให้บริการแบบกลุ่มเมฆที่ประกอบไปด้วยโปรแกรมประยุกต์ในรูปแบบต่าง ๆ ที่สามารถเข้าถึงได้ง่าย เช่น ผ่านทางเว็บเบาร์เซอร์ เป็นต้น แต่ยังคงประสิทธิภาพในการให้บริการ และค่าใช้จ่ายที่ต่ำกว่าลำดับชั้นอื่น ๆ

ลักษณะของระบบประมวลผลแบบกลุ่มเมฆ

ลักษณะของการประมวลผลแบบกลุ่มเมฆที่พบเห็นได้ในปัจจุบัน Karada, Pipliya, Thakur and Kamdar, (2013) ได้รวบรวมไว้ว่าประกอบไปด้วย 4 ลักษณะ ดังนี้

1. ระบบประมวลผลแบบกลุ่มเมฆส่วนภายใน (Private cloud) โครงสร้างพื้นฐานของการให้บริการในลักษณะนี้ เกิดขึ้นภายในองค์กรที่ต้องการประสิทธิภาพการทำงานที่สูง ด้วยการใช้ทรัพยากรที่มีอยู่ภายในองค์กร หรือองค์กรที่ต้องการความปลอดภัยของข้อมูลในระดับสูง หรือในระดับการศึกษาที่ต้องการพัฒนาสำหรับงานวิจัยต่าง ๆ เป็นต้น ในการเข้าถึงข้อมูลที่อยู่ภายในระบบดังกล่าว อาจจำเป็นต้องมีการเข้าถึงจากเครือข่ายภายในองค์กรเท่านั้น

2. ระบบประมวลผลแบบกลุ่มเมฆแบบสาธารณะ (Public cloud) ในปัจจุบัน การให้บริการระบบประมวลผลแบบกลุ่มเมฆแบบสาธารณะ เป็นการให้บริการที่มีบทบาทสำคัญในปัจจุบัน โดยทรัพยากรทั้งหมดเป็นของผู้ให้บริการระบบการประมวลผลแบบกลุ่มเมฆ ผู้ใช้บริการสามารถกำหนดเงื่อนไขการใช้งานต่าง ๆ ได้ โดยยึดตามค่าบริการที่เรียกเก็บจากผู้รับบริการเป็นหลักที่คำนวณ ตามอัตราการใช้งานจริงของระบบ ระบบประมวลผลแบบกลุ่มเมฆแบบสาธารณะที่เห็นได้ในปัจจุบัน ได้แก่ Google Cloud Compute Engin, Google App Engine, Amazon EC2 เป็นต้น

3. ระบบประมวลผลแบบกลุ่มเมฆแบบเครือข่าย (Community cloud) การให้บริการในลักษณะนี้ เป็นลักษณะที่พัฒนามากจากการให้บริการแบบส่วนภายใน โดยมีข้อแตกต่างที่การให้บริการในลักษณะนี้สามารถเกิดการแบ่งปันทรัพยากรต่าง ๆ ร่วมกับองค์กรหรือหน่วยงานอื่น ๆ ได้ เพื่อให้เกิดการขยายประสิทธิภาพการบริการ หรือประสิทธิภาพทางด้านเศรษฐศาสตร์

4. ระบบประมวลผลแบบกลุ่มเมฆแบบผสม (Hybrid cloud) เน้นการรวบรวมนำเอาลักษณะการให้บริการในรูปแบบต่าง ๆ เข้าด้วยกัน มากกว่า 2 รูปแบบขึ้นไป ก่อให้เกิดการให้บริการที่เป็นลักษณะใหม่ เหมาะสำหรับองค์กรที่ต้องการปรับปรุงประสิทธิภาพของระบบ โดยโยกย้ายการบริการต่าง ๆ ที่ไม่มีความกังวลในเรื่องความปลอดภัยของข้อมูลมากนัก หรือข้อมูลที่ไม่มีกฎหมายบังคับให้การเก็บข้อมูลต้องเก็บไว้ภายในองค์กรเท่านั้น

จากการรวบรวมข้อมูลที่ผ่านมาเห็นได้ชัดว่า ระบบประมวลผลแบบกลุ่มเมฆ เป็นอีกหนึ่งแนวเทคโนโลยีที่ได้รับความสนใจเป็นอย่างสูงในปัจจุบัน เนื่องจากเป็นเทคโนโลยีที่ให้ประสิทธิภาพ และเสถียรภาพการทำงานของระบบในระดับสูง

มาตรฐานการยืนยันตัวบุคคล

ปัจจุบันมาตรฐานการยืนยันตัวบุคคลที่ได้รับความนิยมในปัจจุบันมีอยู่หลากหลายมาตรฐานดังนี้

OpenID

OpenID เป็นโปรโตคอลที่ได้รับการพัฒนาขึ้นมาโดย Brad Fitzpatrick ในปี 2548 เพื่อให้เป็นระบบการยืนยันตัวบุคคลสำหรับการเข้าถึงการบริการต่าง ๆ ของเว็บในปัจจุบัน ทั้งในลักษณะของการเข้าถึงเนื้อหาในเว็บไซต์ หรือการเข้าถึงเว็บเซอร์วิสต่าง ๆ การทำงานของ OpenID เป็นลักษณะของการทำงานแบบเปิด หรือในอีกนัยยะหนึ่งหมายความว่า การทำงานของ OpenID เป็นการอนุญาตให้เว็บไซต์ที่ได้รับการพัฒนาขึ้นมาใหม่ในอนาคตสามารถใช้งานระบบฐานข้อมูลสมาชิกร่วมกันกับระบบที่ได้รับการพัฒนามาก่อนหน้าได้ จึงเป็นอีกแนวทางหนึ่งที่เข้ามาช่วยผู้พัฒนาระบบ และผู้ใช้งานให้มีความสะดวกมากยิ่งขึ้น

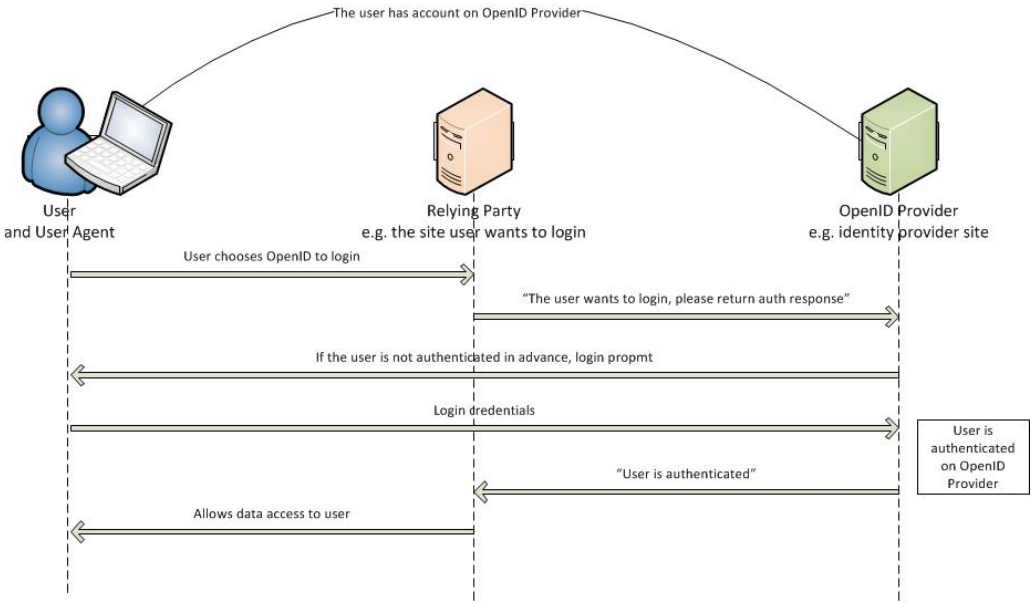
กระบวนการทำงานของ OpenID เป็นกระบวนการทำงานที่เป็นลักษณะของการทำงานแบบ SSO (Single Sign On) ในปัจจุบันมีการพัฒนาจนถึงเวอร์ชั่นที่ 2.0 ประกอบไปด้วย 3 ส่วนในการทำงานดังนี้

1. ส่วนผู้ใช้งาน (User Agent:UA) เป็นการทำงานของผู้ใช้งาน หรือบุคคลทั่วไปที่ต้องการเข้าสู่ระบบ

2. โปรแกรมประยุกต์ฝั่งผู้ให้บริการ (Relying Party:RelP) ทำหน้าที่ในการให้บริการเนื้อหาต่าง ๆ โดยที่การบริการในแต่ละครั้งจำเป็นต้องมีการขออนุญาตในการเข้าถึงข้อมูลในส่วนต่าง ๆ

3. ผู้ให้บริการระบบยืนยันตัวบุคคล (OpenID provider) เป็นฝั่งผู้ให้บริการข้อมูลในการเข้าสู่ระบบด้วยโปรโตรคอล OpenID พร้อมทั้งเป็นส่วนที่ให้บริการข้อมูลต่าง ๆ ของผู้ใช้งาน ให้กับโปรแกรมประยุกต์ฝั่งผู้ให้บริการ

การยืนยันตัวบุคคลแบบ OpenID นั้นผู้ใช้งานจำเป็นต้องมีการลงทะเบียนข้อมูลไว้กับผู้ให้บริการระบบยืนยันตัวบุคคลสำหรับการยืนยันตัวบุคคลที่อาจเกิดขึ้นในภายหลังได้ สำหรับกระบวนการในการยืนยันตัวบุคคลแบบ OpenID มีกระบวนการดังภาพที่ 2-3



ภาพที่ 2-3 กระบวนการทำงานของ OpenID

Kisin, (2013) ระบุไว้ว่ากระบวนการทำงานต่าง ๆ ของ OpenID มีรายละเอียดดังต่อไปนี้

1. ผู้ใช้งานระบุข้อมูลสำหรับยืนยันตัวบุคคลยังหน้าโปรแกรมประยุกต์ของฝั่งผู้ให้บริการ และเลือกการยืนยันตัวบุคคลในรูปแบบของ OpenID และส่งข้อมูลเพื่อเริ่มต้นกระบวนการ

2. โปรแกรมประยุกต์เริ่มทำการตรวจสอบ และจัดเตรียมข้อมูลที่ผู้ใช้งานได้ระบุไว้ก่อนหน้า ให้อยู่ในรูปแบบมาตรฐานเพื่อเตรียมส่งต่อข้อมูลให้ระบบสำหรับยืนยันตัวบุคคล

3. โปรแกรมประยุกต์ฝั่งผู้ให้บริการ และผู้ให้บริการยืนยันตัวบุคคลสร้างกุญแจรหัสลับสำหรับการแลกเปลี่ยนข้อมูลระหว่างกัน

4. โปรแกรมประยุกต์ฝั่งผู้ให้บริการเริ่มต้นทำการเปลี่ยนหน้าต่างข้อมูลที่ฝั่งผู้ใช้บริการไปยังหน้าต่างของผู้ให้บริการยืนยันตัวบุคคล พร้อมทั้งแนบที่อยู่สำหรับการย้อนกลับไปยังหน้าต่างของผู้ให้บริการโปรแกรมประยุกต์หลังจากที่การยืนยันตัวบุคคลสำเร็จเป็นที่เรียบร้อย

5. ผู้ให้บริการยืนยันข้อมูลส่วนบุคคลทำการตรวจสอบข้อมูลตามกระบวนการปกติโดยขึ้นอยู่กับแต่ละผู้ให้บริการ

6. ในกรณีที่กระบวนการการยืนยันตัวบุคคลสามารถยืนยันได้ ระบบยืนยันตัวบุคคลเริ่มทำการเปลี่ยนหน้าต่างของผู้ใช้งานให้กลับสู่หน้าต่างของโปรแกรมประยุกต์ฝั่งผู้ให้บริการพร้อมทั้งข้อมูลยืนยันที่ระบุว่าผู้ใช้งานได้รับการยืนยันเป็นที่เรียบร้อยแล้ว

7. โปรแกรมประยุกต์ฝั่งผู้ให้บริการยืนยันข้อมูลที่ได้รับไปยังฝั่งผู้ให้บริการยืนยันตัวบุคคลอีก หากการยืนยันสำเร็จสมบูรณ์ผู้ใช้งานสามารถให้งานระบบได้ต่อไป

OAuth2.0

OAuth2.0 ได้รับการพัฒนาขึ้นในปี 2545 โดย Hardt โดยเป็นการพัฒนามาจาก OAuth1.0 เป็นอีกมาตรฐานที่ได้รับการกำหนดขึ้นมาสำหรับการยืนยันตัวบุคคลด้วยการอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลต่างให้กับโปรแกรมประยุกต์ โดยที่โปรแกรมประยุกต์นั้น ๆ ไม่จำเป็นต้องทราบชื่อผู้ใช้ และรหัสผ่านของผู้ใช้งาน การทำงานของ OAuth2.0 เป็นการดำเนินงานที่ควบคุมการเข้าถึงข้อมูลผ่านทางบุคคลที่ 3 ที่ต้องการเรียกใช้งานโปรโตคอล HTTP ร่วมกับอุปกรณ์ที่ได้รับอนุญาต หรือเป็นการทำงานผ่าน APIs ที่เป็นช่องทางการให้บริการต่าง ๆ ด้วยชุดข้อมูลชุดหนึ่งที่เรียกว่า แอคเซสโทคเค่น (Access Token) แทนการใช้งานรหัสผ่าน ผู้ให้บริการ OAuth ที่พบเห็นได้ในปัจจุบันนั้นมีอยู่หลากหลาย ที่พบเห็นได้ทั่วไป ได้แก่ Facebook, Google, Twitter และอื่น ๆ ตามคำกล่าวของ Boyd, (2012)

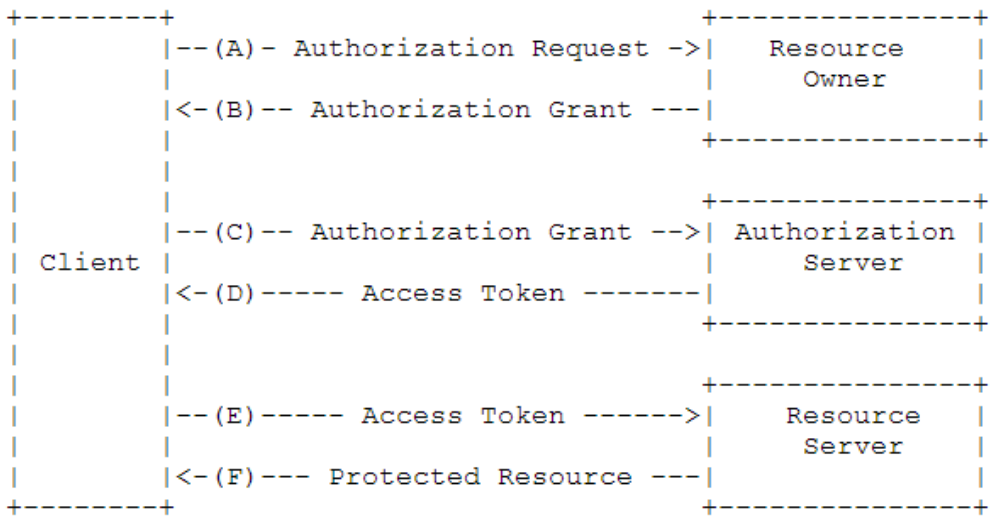
Darwish and Ouda, (2015) ระบุว่าองค์ประกอบที่สำคัญของระบบการยืนยันตัวบุคคลด้วย OAuth นั้นประกอบไปด้วยส่วนต่าง ๆ ดังต่อไปนี้

1. โปรแกรมประยุกต์ (Client application) เป็นโปรแกรมประยุกต์ที่ต้องการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูลหรือผู้ใช้งานโปรแกรมประยุกต์

2. เจ้าของข้อมูล (Resource owner) เป็นส่วนของผู้ใช้งานโปรแกรมประยุกต์ ที่จำเป็นต้องมีการอนุญาตให้โปรแกรมประยุกต์สามารถเข้าถึงข้อมูลต่าง ๆ ของตนเองที่ถูกเก็บบันทึกไว้ยังเครื่องแม่ข่ายของผู้เก็บบันทึกข้อมูล อาทิ เครื่องแม่ข่ายสำหรับการเก็บข้อมูลส่วนบุคคลของ Facebook เป็นต้น

3. เครื่องแม่ข่ายสำหรับการเก็บบันทึกข้อมูลส่วนบุคคล (Resource server) เป็นเครื่องแม่ข่ายที่ทำหน้าที่ให้การเก็บรักษาข้อมูลส่วนบุคคลต่าง ๆ ให้มีความปลอดภัย โดยในการทำงานนั้น เครื่องดังกล่าวเป็นเครื่องที่ให้บริการ APIs เพื่อการเข้าถึงข้อมูลที่ถูกบันทึกไว้ภายในระบบ

4. เครื่องแม่ข่ายสำหรับการให้อนุญาตการเข้าถึงข้อมูล (Authorisation server) เป็นเครื่องแม่ข่ายที่มีหน้าที่ในการอนุญาตการเข้าถึงข้อมูลจากเจ้าของข้อมูล และทำหน้าที่ในการสร้างแอคเซสโทคเค่น และส่งกลับไปยังโปรแกรมประยุกต์ โดยปกติแล้วเครื่องแม่ข่ายในการอนุญาตการเข้าถึงข้อมูลนั้นสามารถเป็นเครื่องเดียวกับเครื่องแม่ข่ายสำหรับการเก็บบันทึกข้อมูลส่วนบุคคลได้



ภาพที่ 2-4 กระบวนการทำงานพื้นฐานของ OAuth 2.0

จากภาพที่ 2-4 Sendor, Lehmann, Serme and Oliveira, (2014) กล่าวว่ากระบวนการทำงานพื้นฐานของ OAuth2.0 สามารถแบ่งออกได้เป็น 6 กระบวนการสำคัญดังต่อไปนี้

1. ในกรณีที่โปรแกรมประยุกต์ต้องการเข้าถึงข้อมูลส่วนบุคคลของเจ้าของข้อมูล โปรแกรมประยุกต์ต้องทำการร้องขอข้อมูลดังกล่าวเจ้าของข้อมูล

2. เจ้าของข้อมูลอนุญาตการเข้าถึงข้อมูลชุดดังกล่าว

3. โปรแกรมประยุกต์นำการอนุญาตที่ได้รับส่งไปยังเครื่องแม่ข่ายสำหรับการให้อนุญาตการเข้าถึงข้อมูลเพื่อร้องขอการเข้าถึงข้อมูลที่ได้รับการบันทึกไว้

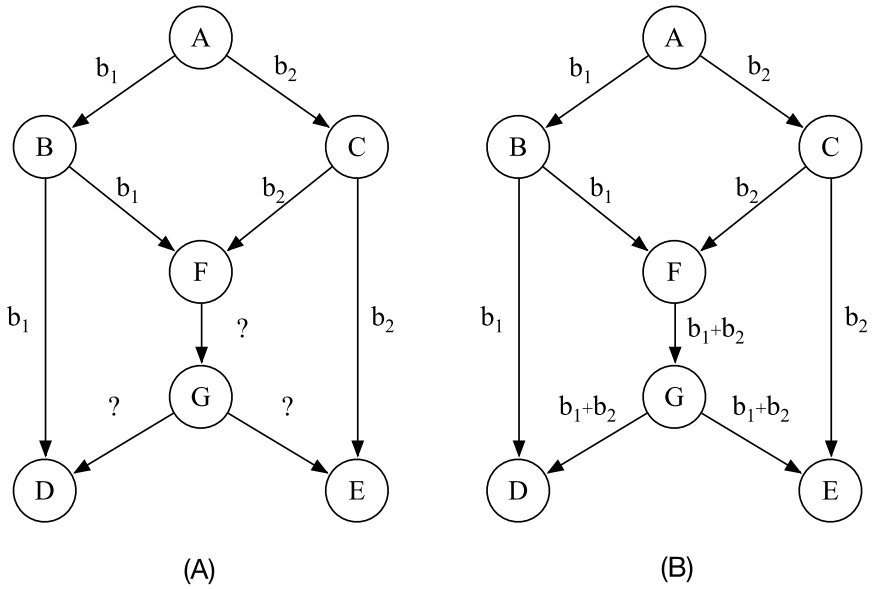
4. เครื่องแม่ข่ายสำหรับการให้อนุญาตการเข้าถึงข้อมูลทำการแลกเปลี่ยนข้อมูลการอนุญาตในการเข้าถึงกับแอคเซสโทคเค่น

5. โปรแกรมประยุกต์ใช้เอคเซสโทคเค่นที่ได้รับร้องขอการเข้าถึงข้อมูลไปยังเครื่องแม่ข่ายสำหรับการเก็บบันทึกข้อมูลส่วนบุคคล

6. เครื่องแม่ข่ายสำหรับการเก็บบันทึกข้อมูลส่วนบุคคลอนุญาตให้โปรแกรมประยุกต์สามารถเข้าถึงข้อมูลได้ โดยการเข้าถึงทั้งหมดจะถูกจำกัดไว้ในขณะที่ แอคเซสโทคเค่นยังสามารถใช้งานได้

การเข้ารหัสเครือข่าย

การเข้ารหัสเครือข่าย (Network coding) ได้รับการคิดค้นในปี 2543 โดย Ahlswede เป็นเทคนิคหนึ่งในการเพิ่มประสิทธิภาพและศักยภาพในการส่งข้อมูลต่าง ๆ ผ่านทางเครือข่าย หรือช่องทางทั่วไป เพื่อให้เกิดการส่งข้อมูลที่ดีขึ้น โดยมีการเข้ารหัสข้อมูลที่ได้รับมาแทนที่การคัดลอกข้อมูลและส่งต่อข้อมูลไปตามขั้นตอนปกติ โดยมีจุดมุ่งหมายหลักในการพัฒนาเพื่อให้สามารถส่งสัญญาณแบบมัลติคาสต์ออกไปในเครือข่ายได้

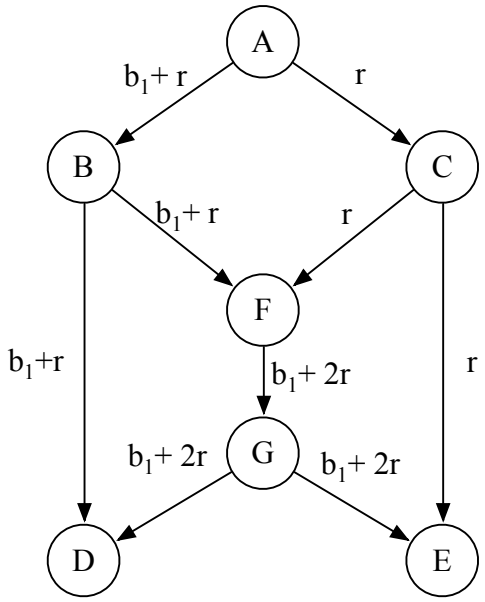


ภาพที่ 2-5 การเข้ารหัสเครือข่าย

จากภาพที่ 2-5 (A) เห็นได้ว่าเมื่อต้องการส่งข้อมูลใด ๆ จากโหนด A ไปยัง โหนด D และ E ตามลำดับ การส่งข้อมูลทั้งหมดจะเกิดภาวะคอขวดที่โหนด F ในกรณีที่โหนด F ต้องการส่งต่อสัญญาด้วยเทคนิคแบบปกติ แต่ด้วยเทคนิคการทำงานของการเข้ารหัสเครือข่ายที่สามารถนำสัญญาณต่าง ๆ มารวมกันเป็นอีกหนึ่งสัญญาณได้ดังภาพที่ 2-5 (B) เมื่อโหนด D ได้รับข้อมูลจากโหนด B และ G แล้วนั้น โหนด D จึงมีความสามารถในการแยกแยะสัญญาณและถอดรหัสเพื่อหาค่า b_1 และ b_2 ได้ ซึ่งเป็นกรณีเดียวกับการทำงานในโหนด E

จากภาพที่ 2-5 (B) เห็นได้ว่าการส่งสัญญาณที่เกิดขึ้นในระบบเป็นการส่งสัญญาณที่ช่วยให้ความเร็วและประสิทธิภาพในการส่งนั้นรวดเร็วขึ้น จึงเหมาะสำหรับการส่งสัญญาณที่ไม่ต้องการความปลอดภัยของข้อมูลมากนัก หากโหนดหนึ่งโหนดใดในระบบเกิดการดังฟังข้อมูลจาก

ผู้ไม่ประสงค์ดี ข้อมูลดังกล่าวสามารถถูกเปิดเผยออกไปได้ในบางส่วนของข้อมูล เช่น เกิดการดักฟังที่เส้นเชื่อม CE ผู้ไม่ประสงค์ดีกับระบบสามารถเห็นข้อมูล B_2 ได้ในทันที



ภาพที่ 2-6 การเข้ารหัสเครือข่ายที่มีความปลอดภัย

ในการแก้ปัญหาดังกล่าวของการเข้ารหัสเครือข่าย ในปัจจุบันได้มีการพัฒนาแนวคิดการเข้ารหัสเครือข่ายขึ้นมา เป็นการเข้ารหัสเครือข่ายที่มีความปลอดภัย (Secure network coding) ด้วยการเพิ่มสัญญาณแบบสุ่ม (r) เข้ามาในระบบ เมื่อใดก็ตามที่โหนด A ต้องการส่งข้อมูลไปยังโหนด D และ E ตามลำดับ ดังนั้นเมื่อใดที่ผู้ไม่ประสงค์ดีต้องการดักฟังข้อมูลจำเป็นต้องมีการดักฟังที่ 2 สายข้อมูลขึ้นไป จึงจะได้รับสัญญาณ b_1 แต่การดำเนินการในลักษณะนี้เป็นการดำเนินการโดยการเพิ่มข้อมูลสุ่มเข้ามาในระบบจึงส่งผลให้การส่งข้อมูลในหนึ่งครั้งสามารถส่งข้อมูลได้เพียงข้อมูลเดียว ดังนั้นจึงเกิดความล่าช้าของระบบมากขึ้น แต่แลกมาด้วยความปลอดภัยที่มากขึ้นเช่นกัน

จากการศึกษาข้อมูลของ Feldman, Malkin, Servedio and Stein, (2004) ที่กล่าวถึงการเข้ารหัสเครือข่ายแบบปลอดภัย โดยใช้รหัสข้อมูลแบบมัลติคาสต์ เพื่อส่งข้อมูลแบบปลอดภัยผ่านทางเครือข่ายที่มีการบุกรุกปรากฏอยู่ด้วยหลักการ การเข้ารหัสเครือข่ายแบบเชิงเส้น โดยใช้การจำลองเครือข่ายให้อยู่ในรูปของกราฟ $G = (V, E)$ โดยที่ V เป็นเซตของโหนด และ E เป็นเซตของเส้นเชื่อม ในหลักการของการเข้ารหัสเครือข่ายแบบเชิงเส้นนั้นสามารถอธิบายได้ด้วยการเขียนสมการในลักษณะเชิงเส้น ดังนั้นคำตอบของปัญหาการเข้ารหัสเครือข่ายจึงสามารถอธิบาย

ได้ในลักษณะของเวกเตอร์ $\boldsymbol{v}[e]$ บนเส้นเชื่อม $e \in E_G$ ใด ๆ โดยข้อมูลที่ส่งไปตามเส้นเชื่อม e จะมีค่าเป็น $\boldsymbol{v}[e] \cdot m$ เมื่อ m เป็นเวกเตอร์ของข้อมูลที่ส่งมาจากแหล่งกำเนิด

การส่งข้อมูลผ่านทางเครือข่ายของ Feldman, Malkin, Servedio and Stein, (2004) ได้มีการใช้ขั้นตอนการเข้ารหัสข้อมูลเบื้องต้นที่แหล่งกำเนิดก่อนที่จะส่งออกมาผ่านทางเครือข่าย ด้วยการเพิ่มเวกเตอร์สุ่มเข้ามาในระบบ โดยให้ $\boldsymbol{y} = (\boldsymbol{x}, \boldsymbol{r})$ โดยที่ $\boldsymbol{x} = (x_1, x_2, \dots, x_{n-l})$ เป็นเวกเตอร์ของข้อมูลที่ต้องการส่ง $\boldsymbol{r} = (r_1, r_2, \dots, r_l)$ เป็นเวกเตอร์สุ่ม ซึ่งสามารถอธิบายได้ด้วยสมการดังต่อไปนี้

$$E(\boldsymbol{x}, \boldsymbol{r}) = \quad \boldsymbol{y}\boldsymbol{M}^{-1} \tag{2-1}$$

โดยที่ $\boldsymbol{M}$ เป็น nxn เมทริกซ์ที่อินเวอร์สได้

Cai and Yeung, (2002) แนะนำเทคนิคการเข้ารหัสเครือข่ายแบบปลอดภัย โดยมีเงื่อนไขดังต่อไปนี้

1. $n > l \geq k$ เมื่อ n เป็นจำนวนเส้นที่เชื่อมกับโหนดปลายทางแต่ละตัว และ k เป็นจำนวนเส้นเชื่อมที่ถูกดักฟัง

2. x_i, r_i เป็นสมาชิกของฟิลด์จำกัดที่มีขนาด $\mathrm{q} > \left(\frac{|E_G|}{k}\right)$ โดยที่ $|E_G|$ คือจำนวนเส้นเชื่อมทั้งหมด

ดังนั้นข้อมูลที่ถูกส่งออกมาถึงเส้นเชื่อม e จะมีค่าเป็น $\boldsymbol{y}\boldsymbol{M}^{-1}\boldsymbol{v}[e]$

ในการถอดรหัสข้อมูลเวกเตอร์ของข้อมูลที่ได้รับการเข้ารหัส $E(\boldsymbol{x}, \boldsymbol{r})$ นั้นมีเงื่อนไขในการถอดรหัสดังนี้ สำหรับทุก ๆ $\boldsymbol{x}, \boldsymbol{x}'$ โดยที่ $\boldsymbol{x} \neq \boldsymbol{x}'$ จะได้ $E(\boldsymbol{x}, \boldsymbol{r}) \neq E(\boldsymbol{x}', \boldsymbol{r}')$ สำหรับทุก ๆ $\boldsymbol{r}, \boldsymbol{r}'$

สำหรับเงื่อนไขความปลอดภัยของการเข้ารหัสเครือข่ายนั้นมีต้องมีการกำหนดจำนวน k เมื่อ k คือจำนวนเส้นเชื่อมที่ต้องการให้ถูกดักฟังได้สูงสุดในขณะที่ข้อมูล x ยังคงมีความปลอดภัยจากการถูกดักฟัง สำหรับทุก ๆ เวกเตอร์ $a = (a_1, a_2, \dots, a_{k'}) \in GF(q^{k'})$ ซึ่ง k' เป็นข้อมูลในสายที่ถูกดักฟัง ถ้าให้

$$R(\boldsymbol{x}, \boldsymbol{a}) \quad = \quad \{r \in GF(q^l) | E(\boldsymbol{x}, \boldsymbol{r}) \cdot \boldsymbol{v}[e_i] = a_i\} \tag{2-2}$$

โดยที่ $R(\boldsymbol{x}, \boldsymbol{a})$ เป็นเซตของเวกเตอร์สุ่ม r ที่เป็นไปได้ที่จะทำให้เกิดค่าเวกเตอร์ที่ถูกดักฟังเป็น $\boldsymbol{a}$ โดยเงื่อนไขความปลอดภัยจะเป็น $|R(\boldsymbol{x}, \boldsymbol{a})| = |R(\boldsymbol{x}', \boldsymbol{a})|$ สำหรับทุก ๆ $\boldsymbol{x}, \boldsymbol{x}' \in GF(q^{n-l})$ กล่าวคือ ศัตรูจะไม่มีทางทราบข้อมูลความลับ $\boldsymbol{x}$ แม้จะรู้ $\boldsymbol{a}$

จากสมการที่ (2-1) ในการเข้ารหัสข้อมูลเพื่อทำการเข้ารหัสเครือข่ายที่มีความปลอดภัย นั้นเมทริกซ์ $\boldsymbol{M}$ ต้องเป็น nxn เมทริกซ์ที่สามารถอินเวอร์สได้ โดยต้องมีเงื่อนไขตามข้อกำหนดดังต่อไปนี้

1. เป็นเวกเตอร์ที่ไม่ขึ้นต่อกันในเชิงเส้น (Linearly independent) กับกลุ่มของเวกเตอร์ $\{v[e]\}_{e\in E_G}$

2. ทุก ๆ ชุดตัวเลข ของเวกเตอร์จากคอลัมน์ $n-l$ ของ $\boldsymbol{M}$ ต้องไม่ขึ้นต่อกันในเชิงเส้น (Linearly independent)

การกระจายความลับ

Shamir, (1979) กล่าวว่าการเก็บรักษากุญแจรหัสลับในที่เดียว อาทิ เครื่องคอมพิวเตอร์ ความจำของมนุษย์ หรือในสถานที่ปลอดภัยใด ๆ ย่อมมีความน่าเชื่อถือน้อย เนื่องจากถ้ามีการสูญเสีย เช่น เครื่องคอมพิวเตอร์เสีย ผู้เก็บรักษาข้อมูลเสียชีวิต หรือมีการก่อวินาศกรรม ย่อมส่งผลให้ข้อมูลนั้น ๆ ไม่สามารถเข้าถึงได้ ในอีกทางหนึ่งการคัดลอกข้อมูลไว้ยังหลายสถานที่สามารถป้องกันการสูญเสียดังกล่าวได้ แต่ย่อมแลกมาด้วยความปลอดภัยของข้อมูลที่ลดลง

ดังนั้น Shamir, (1979) ได้แสดงถึงการแบ่งกุญแจรหัสลับออก b ออกเป็นจำนวน n ส่วน ได้แก่ $b_1,\ b_2, \dots, b_n$ โดยมีเงื่อนไขดังต่อไปนี้

1. เมื่อสามารถเข้าถึงข้อมูลได้เท่ากับ k ตัว หรือมากกว่า ชิ้นส่วน b_i จะส่งผลให้ข้อมูล b สามารถคำนวณออกมาได้ง่าย

2. เมื่อสามารถเข้าถึงข้อมูลได้เท่ากับ $k-1$ ตัว หรือน้อยกว่า ชิ้นส่วน b_i จะส่งผลให้ข้อมูล b ไม่สามารถคาดเดาได้

โดยแบบแผนการกระจายนี้เรียกว่า (k,n) Threshold scheme ประสิทธิภาพของการกระจายความลับดังแบบแผนนี้สามารถนำไปช่วยในการเก็บรักษากุญแจรหัสลับได้

ในส่วนของแบบแผน (k,n) Threshold scheme นั้นใช้หลักการของการประมาณค่าในเชิงพหุนาม (Polynomial interpolation) โดยให้ k อยู่ในจุดพิกัด 2 มิติ $(x_1,y_1), \dots, (x_k,y_k)$ โดยที่ x_i นั้นแตกต่างกันโดยสิ้นเชิง เพื่อให้ง่ายต่อการคำนวณ และแบ่งข้อมูลลับ สามารถกำหนดให้ b เป็นข้อมูลตัวเลขได้ ด้วยสมการดังต่อนี้

$$q(x) = y \tag{2-3}$$

$$q(x) = \sum_{i=0}^{k-1} a_i x^i \tag{2-4}$$

$$q(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} \tag{2-5}$$

โดยที่ $a_0 = b$ และ $a_1, a_2, \dots, a_{k-1}$ เป็นข้อมูลตัวเลขสุ่ม

จากสมการที่ (2-5) ให้ทำการแบ่งความลับออกเป็นจำนวน n ชิ้นเพื่อนำไปเก็บบันทึกยังสถานที่ต่าง ๆ ได้ดังนี้ $b_1 = q(1), \dots, b_i = q(i), \dots, b_n = q(n)$

จากสมการที่ (2-5) เมื่อต้องการคำนวณหาข้อมูลความลับให้ทำการนำชิ้นส่วนข้อมูลความลับผ่านกระบวนการของพหุนามลากรองจ์ดังนี้

$$q(x) = \sum_{i=0}^{k-1} y_i \ell_i(x) \quad (2\text{-}6)$$

โดยที่

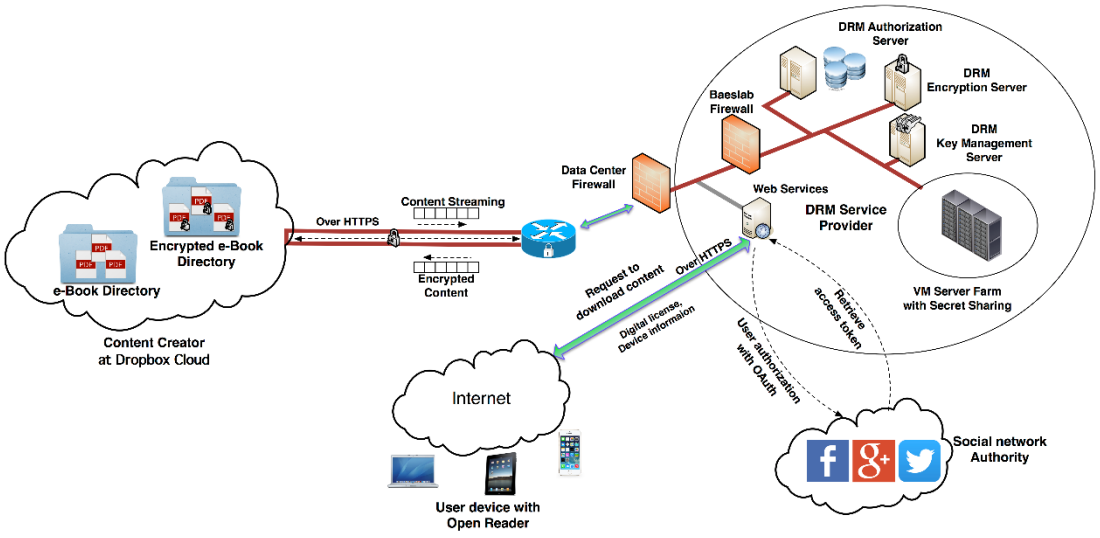
$$\ell_i(x) = \prod_{\substack{0 \le m \le k-1 \\ m \ne k-1}} \frac{x - x_m}{x_i - x_m} \quad (2\text{-}7)$$

จากการศึกษางานวิจัยของ Shamir, (1979) พบว่าการแบ่งความลับตามแบบแผนนั้นช่วยให้เข้าใจถึงหลักการแบ่งความลับ และเงื่อนไขของการกระจายความลับเพื่อเป็นการกำหนดเงื่อนไขในการเข้าถึงชิ้นส่วนความลับได้ และจากการศึกษาในเรื่องของการเข้ารหัสเครือข่ายจึงสามารถนำมาประยุกต์ใช้งานกับการเก็บรักษากุญแจรหัสลับ และเพื่อนำมาสร้างสมการสำหรับการกระจายความลับโดยที่ไม่มีการข้อมูลความลับทั้งหมดไว้ภายในสัมประสิทธิ์เพียงตัวเดียวของสมการ

บทที่ 3
ขั้นตอนและวิธีดำเนินงาน

ภาพรวมของระบบ

ระบบการให้บริการป้องกันลิขสิทธิ์ดิจิทัล เป็นระบบที่จำเป็นต้องใช้ความสามารถของทรัพยากรระบบอย่างเต็มที่ ในการพัฒนานั้นเพื่อให้สามารถทำงานได้อย่างเต็มประสิทธิภาพ ความสามารถของเครื่องมือจึงเป็นสิ่งสำคัญ และควรเป็นเครื่องมือ หรือเทคโนโลยีที่มีเสถียรภาพและความปลอดภัยสูง มีการประมวลผลที่รวดเร็ว สามารถเชื่อมต่อกับเครือข่ายได้ตลอดเวลา ซึ่งเทคโนโลยีดังกล่าว ได้แก่ เทคโนโลยีการประมวลผลแบบกลุ่มเมฆ ที่ตามปกแล้วพื้นฐานการทำงานทั้งหมดจะอยู่ภายใต้เครือข่ายของศูนย์ข้อมูลขนาดใหญ่ที่มีการรักษาความปลอดภัยอย่างเข้มงวด สามารถระบุได้ชัดเจนว่า เครื่องแม่ข่ายใด สามารถเข้าถึงได้จากเครือข่ายภายใน และเครื่องแม่ข่ายใดสามารถเข้าถึงได้จากทุกเครือข่าย รวมไปถึงการติดต่อกันระหว่างเครือข่ายต่าง ๆ ควรเป็นการติดต่อกันผ่านทางช่องทางที่น่าเชื่อถือ อาทิเช่น HTTPS เป็นต้น



ภาพที่ 3-1 ภาพรวมของระบบการป้องกันลิขสิทธิ์ดิจิทัล

จากภาพที่ 3-1 เป็นการแสดงภาพรวมของระบบป้องกันลิขสิทธิ์ดิจิทัลที่ได้มีการนำเสนอขึ้นมา โดยประกอบไปด้วย 3 ส่วนสำคัญได้แก่ ส่วนของนักเขียนหรือเจ้าของลิขสิทธิ์ (Content ll

creator) ส่วนของผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัล (DRM service provider) และส่วนของผู้ใช้งาน (Users)

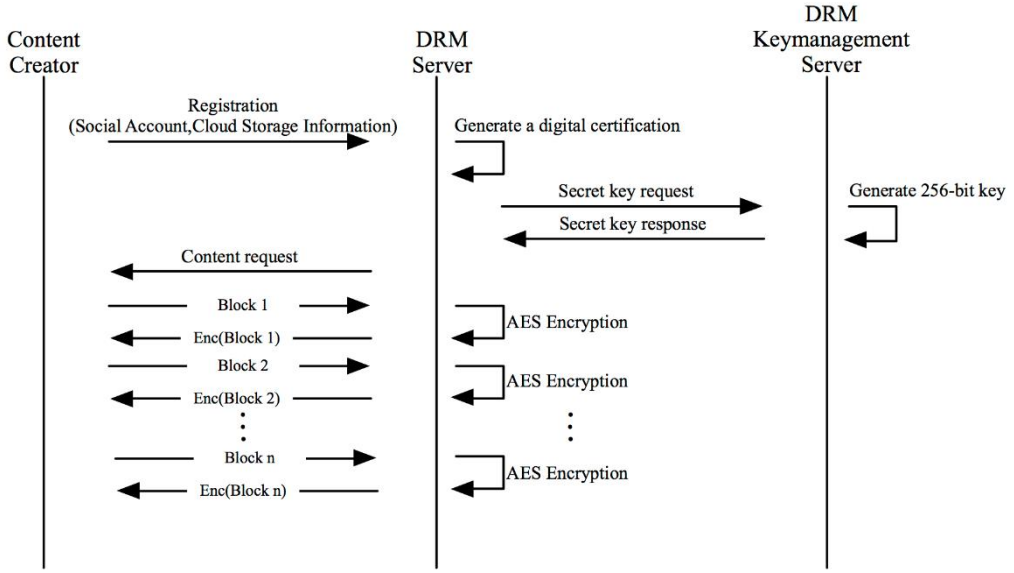
1. นักเขียนหรือเจ้าของผู้ครอบครองลิขสิทธิ์ (Content creator or Authorized proprietor) เป็นผู้สร้าง หรือผู้ครอบครองไฟล์สื่อสิ่งพิมพ์ดิจิทัล (eBook) อาทิ PDF หรือ ePub โดยมีหน้าที่ในการเก็บรักษาสื่อสิ่งพิมพ์ดังกล่าวไว้ภายในแหล่งเก็บข้อมูลแบบกลุ่มเมฆส่วนบุคคล (Personal cloud storage) อาชิเช่น Dropbox เป็นต้น โดยประกอบไปด้วย 2 ส่วนย่อยหลัก ๆ ได้แก่ แหล่งการเก็บข้อมูลสื่อสิ่งพิมพ์ดิจิทัล และแหล่งการเก็บข้อมูลสื่อสิ่งพิมพ์ดิจิทัลที่ได้รับการเข้ารหัสพร้อมทั้งหนังสือรับรองลิขสิทธิ์ดิจิทัล

2. ผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัล (DRM service provider) เป็นส่วนที่มีความสำคัญที่สุดต่อภาพรวมของระบบ เนื่องจากมีหน้าที่ความรับผิดชอบในการป้องกันข้อมูลเนื้อหา ทั้งระหว่างการเก็บรักษา และการเคลื่อนย้ายข้อมูลภายใต้เงื่อนไขลิขสิทธิ์ที่กำหนด หลังจากที่ระบบได้รับการลงทะเบียนสื่อสิ่งพิมพ์ดิจิทัลเข้ามาเรียบร้อยแล้ว ระบบการให้บริการจะดำเนินการสร้างหนังสือรับรองลิขสิทธิ์ดิจิทัล เพื่อไว้เป็นการยืนยันตัวบุคคลผู้ครองต่อไป ในขณะเดียวกันระบบจะทำการเรียกไปยังแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์ เพื่อขอการสตรีมมิ่งข้อมูลมาทำการเข้ารหัส และบันทึกกลับไปยังแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์ดังเดิม ซึ่งกระบวนการดังกล่าวนั้นเป็นกระบวนการที่ไม่มีการเก็บข้อมูลใด ๆ ไว้ยังฝั่งผู้ให้บริการทั้งสิ้น นอกจากนั้น ฝั่งผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัลยังคงมีการพัฒนาส่วนการบริหารจัดการกุญแจรหัสลับที่ใช้ในการเข้ารหัสไฟล์ข้างต้น ด้วยเทคนิคการเข้ารหัสเครือข่าย และในส่วนประกอบย่อยอีกส่วนหนึ่งที่มีความสำคัญ ได้แก่ การยืนยันตัวบุคคลที่เข้ามาร้องไฟล์สื่อสิ่งพิมพ์ดิจิทัลจากทางผู้ให้บริการด้วยการใช้การยืนยันตัวบุคคลผ่านกระบวนการการยืนยันตัวบุคคลที่ 3 ตามมาตรฐานที่แพร่หลายและรู้จักกันทั่วไปในส่วนของสังคมออนไลน์ที่เรียกว่ามาตรฐาน OAuth 2.0

3. ส่วนของผู้ใช้งาน (Users) หลังจากที่ผู้ใช้งานได้มีการติดต่อซื้อขายสื่อสิ่งพิมพ์ดิจิทัลกับทางผู้ครอบครองลิขสิทธิ์เรียบร้อยแล้วนั้น ทางผู้ครอบครองลิขสิทธิ์จะดำเนินการส่งข้อมูลการยืนยันตัวบุคคลจากเครือข่ายสังคมออนไลน์ อาทิเช่น Facebook, Google plus เป็นต้น ไปยังผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัลเพื่อดำเนินการสร้างใบอนุญาตดิจิทัล จากนั้นจะมีการส่งใบอนุญาตดิจิทัลจากทางผู้ให้บริการกลับไปยังผู้ครอบครองลิขสิทธิ์ และส่งต่อไปยังผู้ใช้งานเพื่อเป็นการยืนยันว่าเป็นผู้มีสิทธิในสื่อสิ่งพิมพ์นั้นจริง เมื่อผู้ใช้งานได้รับใบอนุญาตดิจิทัล จากนั้นเปิดด้วยโปรแกรมที่พัฒนามาให้รองรับกับระบบการป้องกันลิขสิทธิ์ดิจิทัลที่ข้างต้น ระบบจะทำการร้องขอการเปิดอ่านไฟล์สื่อสิ่งพิมพ์นั้นต่อไป

กระบวนการดำเนินงาน

ในส่วนของการออกแบบกระบวนการดำเนินงานของระบบนั้นสามารถแบ่งออกได้เป็น 2 ส่วนหลัก ๆ ได้แก่ กระบวนการป้องกันลิขสิทธิ์ดิจิทัล และกระบวนการการร้องขอข้อมูลสินค้าจากผู้ใช้งาน



ภาพที่ 3-2 กระบวนการป้องกันลิขสิทธิ์ดิจิทัล

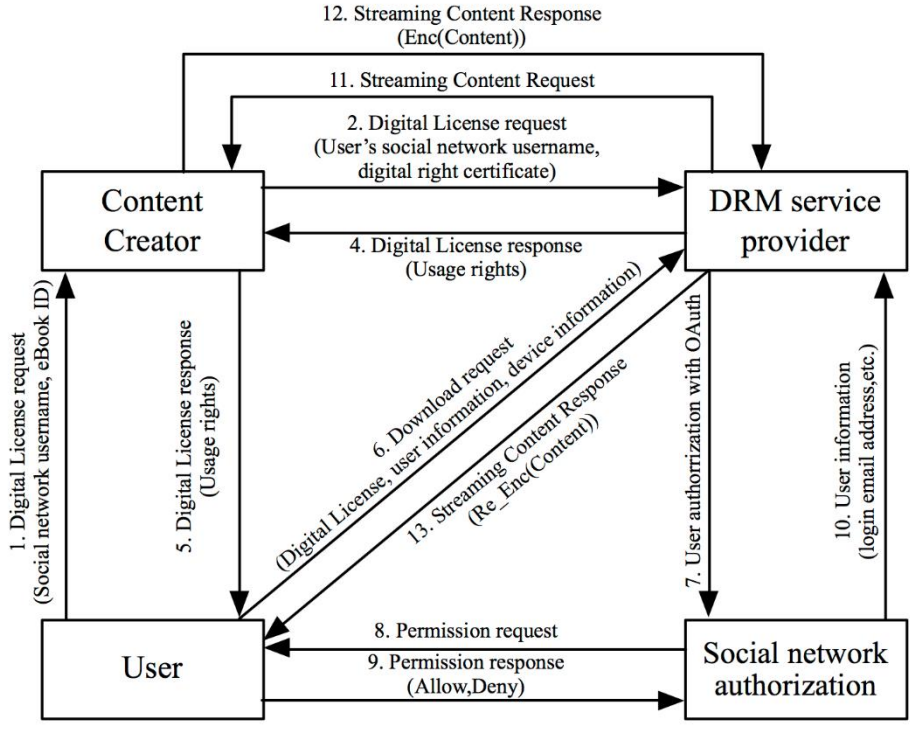
จากภาพที่ 3-2 เป็นกระบวนการการป้องกันลิขสิทธิ์ดิจิทัลที่เกิดขึ้นในช่วงจังหวะเวลาที่ผู้ครอบครองลิขสิทธิ์ได้ทำการลงทะเบียนสื่อสิ่งพิมพ์ดิจิทัลเข้ามาในระบบ เมื่อผู้ให้บริการได้รับข้อมูลดังกล่าวแล้วจะมีการส่งใบรับรองลิขสิทธิ์ดิจิทัลกลับไปยังผู้ครอบครองลิขสิทธิ์เพื่อใช้สำหรับยืนยันตัวบุคคลในอนาคต และในขณะเดียวกันระบบจะทำการเรียกไปยังแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์ เพื่อขอการสตรีมมิ่งข้อมูลมาทำการเข้ารหัสด้วยเทคนิคการเข้ารหัสแบบ AES และบันทึกกลับไปยังแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์ดังเดิม จากกระบวนการดังกล่าวจะเห็นได้ว่าไม่มีการเก็บข้อมูลใด ๆ ของสื่อสิ่งพิมพ์ดิจิทัลไว้ที่ผู้ให้บริการ โดยสามารถแบ่งเป็นกระบวนการทำงานได้ดังต่อไปนี้

1. ผู้ครอบครองลิขสิทธิ์เปิดเข้าไปที่หน้าเว็บไซต์ของผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัลเพื่อขอลงทะเบียนสื่อสิ่งพิมพ์ดิจิทัลเข้าสู่ระบบการเข้ารหัส โดยข้อมูลที่ต้องระบุระหว่างการลงทะเบียนได้แก่ ชื่อผู้ใช้งานสื่อสังคมออนไลน์ และข้อมูลของแหล่งเก็บข้อมูลแบบกลุ่มเมฆ เช่น Dropbox

2. หลังจากที่ผู้ครอบครองลิขสิทธิ์ดิจิทัลลงทะเบียนสื่อสิ่งพิมพ์เรียบร้อยแล้ว ระบบการให้บริการทำการสร้างไฟล์ใบรับรองลิขสิทธิ์ดิจิทัลที่ประกอบไปด้วย ชื่อสื่อสิ่งพิมพ์ดิจิทัล APIs ของแหล่งเก็บข้อมูลแบบกลุ่มเมฆ สถานที่เก็บข้อมูล และสิทธิการเข้าใช้งาน เป็นต้น

3. เครื่องแม่ข่ายของผู้ให้บริการทำการติดต่อไปยังเครื่องบริหารจัดการกุญแจรหัสลับที่ตั้งอยู่ภายในเครือข่ายส่วนบุคคลของผู้ให้บริการ เพื่อร้องขอการสร้างกุญแจรหัสลับแบบสมมาตรจำนวน 256 บิต (256-bit AES-based symmetric key) ขึ้นมาเพื่อจับคู่กับไฟล์สื่อสิ่งพิมพ์ดิจิทัลแต่ละไฟล์ สำหรับรายละเอียดของการสร้างกุญแจรหัสลับจะกล่าวถึงในส่วนถัดไป

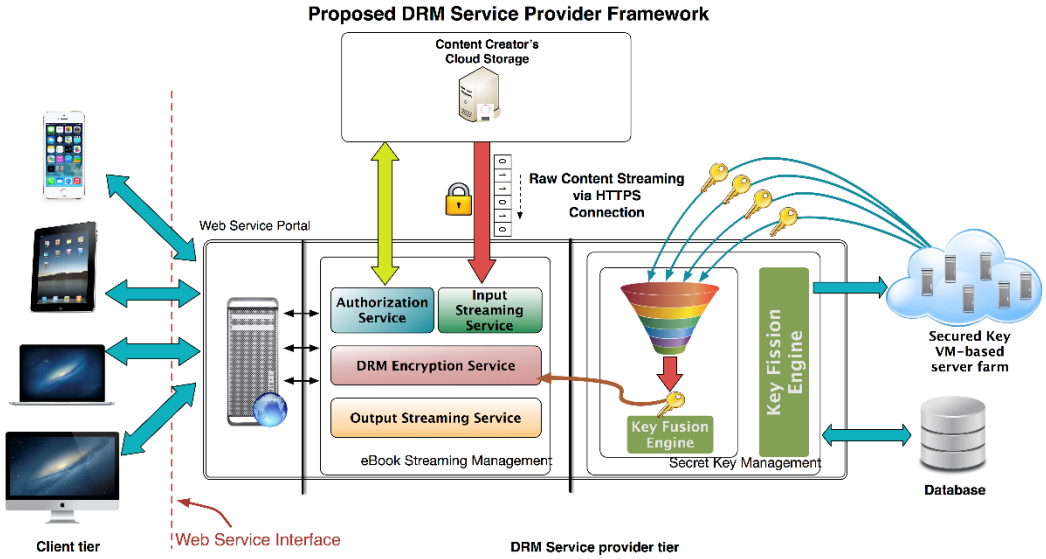
4. หลังจากที่เครื่องแม่ข่ายได้รับกุญแจรหัสลับเรียบร้อยแล้ว จะดำเนินการร้องขอการเข้าสู่สื่อสิ่งพิมพ์ดิจิทัลที่บันทึกอยู่ภายในแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์ และทำการแบ่งข้อมูลออกเป็นส่วน ๆ เพื่อนำมาทำการเข้ารหัสข้อมูลสินค้าและบันทึกกลับลงไปยังแหล่งข้อมูลดังเดิม



ภาพที่ 3-3 กระบวนการร้องขอข้อมูลสื่อสิ่งพิมพ์ดิจิทัลจากผู้ใช้งาน

จากภาพที่ 3-3 เป็นกระบวนการร้องขอข้อมูลสิ่งพิมพ์ดิจิทัลจากผู้ใช้งาน หลังจากที่ผู้ใช้งานได้เสร็จสิ้นกระบวนการซื้อขายกับผู้ครอบครองลิขสิทธิ์แล้วนั้น ไม่ว่าจะผ่านทางการชำระเงินแบบออนไลน์ หรือการโอนเงิน ผู้ครอบครองลิขสิทธิ์ดำเนินการส่งข้อมูล สื่อสังคมออนไลน์ของผู้ใช้งานพร้อมทั้งใบรับรองลิขสิทธิ์ดิจิทัลไปยังผู้ให้บริการเพื่อร้องขอการสร้างใบอนุญาตเข้าถึงข้อมูลสื่อสิ่งพิมพ์ของผู้ใช้งานที่ประกอบไปด้วย สิทธิ์การเข้าถึงข้อมูลสื่อสิ่งพิมพ์เพียงผู้ใช้งานเดียว เป็นต้น จากนั้นผู้ครอบครองลิขสิทธิ์ดำเนินการส่งใบอนุญาตดังกล่าวกลับไปยังผู้ใช้งาน ซึ่งจะเป็นฝ่ายที่ใช้งานโปรแกรมสำหรับอ่านที่เข้ากันได้กับผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัล และร้องขอการเข้าอ่านสื่อสิ่งพิมพ์ต่อไป

โครงแบบการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัล



ภาพที่ 3-4 โครงแบบการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัล

จากภาพที่ 3-4 เป็นโครงแบบการพัฒนาระบบป้องกันลิขสิทธิ์ดิจิทัลที่ประกอบไปด้วย 3 ส่วนหลัก ๆ ได้แก่ ระบบการติดต่อกับอุปกรณ์ภายนอก (Web service portal) ระบบบริหารจัดการการป้องกันลิขสิทธิ์ดิจิทัล และระบบการบริหารจัดการกุญแจรหัสลับ

1. ระบบการติดต่อกับอุปกรณ์ภายนอก (Web service portal) เป็นส่วนการให้บริการที่รองรับการติดต่อระหว่างอุปกรณ์ภายนอกอาทิเช่น อุปกรณ์พกพาอิเล็กทรอนิกส์ (Smart device) ของผู้ใช้งาน กับเครือข่ายของผู้ให้บริการป้องกันลิขสิทธิ์ดิจิทัล ซึ่งตามปกติแล้วผู้ใช้งานไม่สามารถ

ที่จะติดต่อกับส่วนการบริการจัดการป้องกันลิขสิทธิ์ดิจิทัลได้โดยตรง ต้องกระทำผ่านทางช่องทางนี้เท่านั้น

2. ส่วนการบริหารจัดการป้องกันลิขสิทธิ์ดิจิทัล เป็นส่วนที่มีหน้าที่ความรับผิดชอบในการเข้ารหัสข้อมูลสินค้าจากทางผู้ครอบครองลิขสิทธิ์ก่อนที่จะทำการส่งสินค้าดังกล่าวให้กับผู้ใช้งาน ซึ่งภายในจะประกอบไปด้วย 4 ส่วนย่อยสำคัญ ได้แก่ ส่วนบริการนำเข้าข้อมูล (Input streaming service) ส่วนบริการเข้ารหัสความปลอดภัยของข้อมูล (DRM encryption service) ส่วนบริการข้อมูลออก (Output streaming service) และส่วนบริการการยืนยันผู้ใช้งาน (Authorisation service)

2.1 ส่วนบริการนำเข้าข้อมูลสินค้า (Input streaming service) เป็นส่วนที่มีหน้าที่ความรับผิดชอบในการรับข้อมูลสินค้าจากผู้ครอบครองลิขสิทธิ์ ก่อนที่จะส่งต่อข้อมูลดังกล่าวไปยังส่วนถัดไปได้แก่ ส่วนบริการเข้ารหัสความปลอดภัยของข้อมูล

2.2 ส่วนบริการเข้ารหัสความปลอดภัยของข้อมูล (DRM encryption service) เป็นส่วนที่เกี่ยวข้องกับการป้องกันเนื้อหาดิจิทัลใน 2 ส่วนย่อย ได้แก่ การลงทะเบียนสื่อสิ่งพิมพ์ดิจิทัล และการรองรับการร้องข้อสื่อสิ่งพิมพ์ดิจิทัลจากผู้ใช้งาน โดยขั้นตอนการลงทะเบียนสื่อสิ่งพิมพ์ดิจิทัลนั้น ส่วนบริการเข้ารหัสข้อมูลจะมีการติดต่อกับส่วนการบริหารจัดการกุญแจรหัสลับเพื่อร้องขอกุญแจรหัสลับ และนำมาทำการเข้ารหัสสินค้า และส่งสื่อสิ่งพิมพ์ดิจิทัลที่ได้รับการเข้ารหัสแล้วกลับไปยังแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์ต่อไปผ่านทางส่วนบริการข้อมูลออก และเมื่อได้รับการร้องขอสื่อสิ่งพิมพ์ดิจิทัลจากผู้ใช้งาน ส่วนบริการเข้ารหัสข้อมูลจะทำการร้องขอไปยังแหล่งเก็บข้อมูลอีกครั้งเพื่อนำข้อมูลกลับมาเข้าสู่ระบบผ่านทางส่วนบริการนำเข้าข้อมูลสินค้า

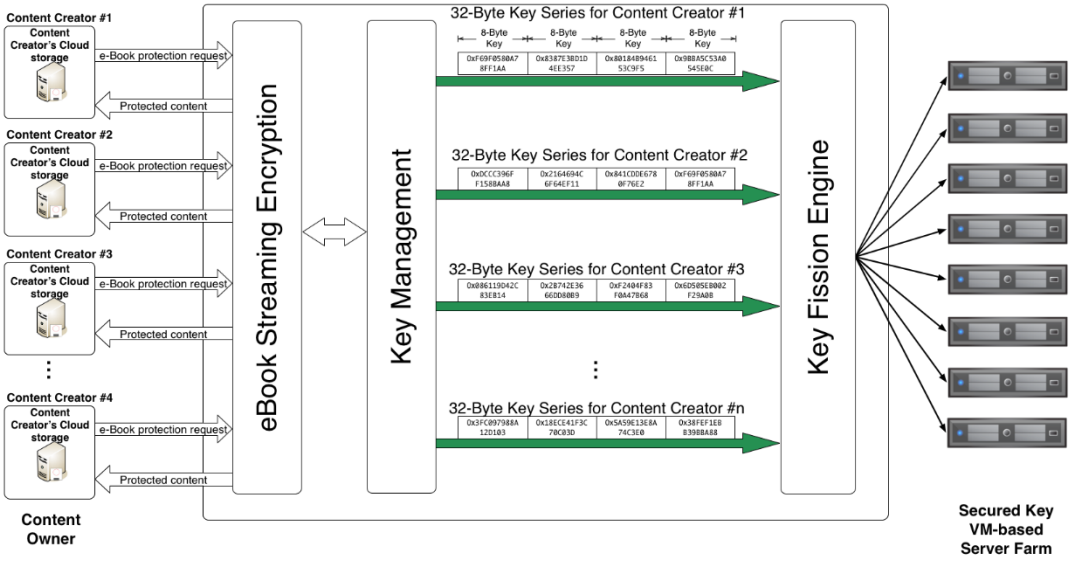
2.3 ส่วนบริการข้อมูลออก (Output streaming service) เป็นส่วนที่รองรับการทำงานเกี่ยวกับเรื่องการส่งข้อมูลที่ได้รับการเข้ารหัสแล้วออกไปยังแหล่งเก็บข้อมูลของผู้ครอบครองลิขสิทธิ์หรือผู้ใช้งาน

2.4 ส่วนบริการการยืนยันผู้ใช้งาน (Authorisation Service) เป็นส่วนที่ทำหน้าที่ในการยืนยันตัวบุคคล รวมไปถึงอุปกรณ์ที่มีการใช้งานระบบ

3. ส่วนการบริหารจัดการกุญแจรหัสลับ เป็นส่วนที่มีหน้าที่ในการจัดการกุญแจรหัสลับทั้งหมดในระบบ ทั้งการสร้างกุญแจรหัสลับ การกระจายกุญแจรหัสลับไปยังเครื่องแม่ข่ายเสมือนด้วยกลไกการกระจายกุญแจ (Key fission engine) และเมื่อต้องการใช้งานกุญแจดังกล่าว ส่วนการบริการจัดการกุญแจรหัสลับจะทำการรวบรวมกุญแจทั้งหมดที่เกี่ยวข้องผ่านทางกลไกการรวบรวมกุญแจ (Key fusion engine) และในรายละเอียดจะกล่าวถึงในส่วนถัดไป

การบริหารจัดการกุญแจรหัสลับด้วยเทคนิคการเข้ารหัสเครือข่าย

การบริหารจัดการกุญแจรหัสลับในระบบป้องกันลิขสิทธิ์ดิจิทัล เพื่อเป็นการเพิ่มความปลอดภัยให้กับระบบ การบริหารจัดการกุญแจจึงได้นำเทคนิคการเข้ารหัสเครือข่ายเข้ามาใช้งานในการกระจายกุญแจรหัสลับไปเก็บยังเครื่องแม่ข่ายเสมือนเครื่องต่าง ๆ ในกรณีที่มีผู้ไม่หวังดีเข้าถึงเครื่องแม่ข่ายเสมือนได้ไม่ครบทุกเครื่อง ผู้ไม่หวังดีนั้นจะหมดสิทธิในการได้กุญแจลับทั้งหมดไปโดยปริยาย โดยกลไกของระบบการบริหารจัดการกุญแจรหัสลับสามารถแบ่งได้เป็น 2 ส่วน ได้แก่ กลไกการกระจายกุญแจรหัสลับ (Key fission engine) และกลไกการรวบรวมกุญแจรหัสลับ (Key fusion engine)



ภาพที่ 3-5 กลไกการกระจายกุญแจรหัสลับ

1. กลไกการกระจายกุญแจรหัสลับ (Key fission engine)

จากภาพที่ 3-5 เป็นกลไกการทำงานของระบบการกระจายกุญแจรหัสลับ ที่มีการใช้กระบวนการของการเข้ารหัสเครือข่ายเพื่อกระจายกุญแจรหัสลับออกเป็นส่วน ๆ และกระจายไปเก็บยังเครื่องแม่ข่ายเสมือนเครื่องต่าง ๆ โดยในการออกแบบการทำงานของระบบสามารถแบ่งออกได้เป็น 2 ส่วน ได้แก่ การกระจายกุญแจรหัสลับไปยังเครื่องคอมพิวเตอร์เสมือนจำนวน 4 และ 8 เครื่องตามลำดับ

1.1 เงื่อนไขปัญหาพื้นฐานสำหรับการเข้ารหัสเครือข่าย

เมื่อให้ n เป็นจำนวนเครื่องแม่ข่าย และกุญแจรหัสลับถูกแทนที่ด้วยเวกเตอร์ของสนามจำกัด $GF(q^{n-k})$ เมื่อ q เป็นขอบเขตจำกัด และ k เป็นเงื่อนไขการเข้าถึงได้ จะทำอย่างไรให้เมื่อทำการเข้ารหัสเครือข่ายเรียบร้อยแล้วสามารถกระจายกุญแจไปยังสถานที่ต่าง ๆ ตามเงื่อนไขดังต่อไปนี้

1.1.1 หากผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องแม่ข่ายได้ไม่เกิน k เครื่องจะไม่ได้ข้อมูลใด ๆ กลับออกไป

1.1.2 หากผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องแม่ข่ายได้มากกว่า k เครื่องแต่ไม่ถึง n เครื่องจะได้ข้อมูลออกไปเพียงบางส่วน

1.1.3 แต่ในกรณีที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องแม่ข่ายได้ทั้งหมด n เครื่อง ผู้ไม่ประสงค์ดีนั้นจะสามารถได้ข้อมูลทั้งหมดออกไป

1.2 เงื่อนไขปัญหาพิเศษสำหรับการเข้ารหัสเครือข่าย

หลังจากที่ได้ทราบปัญหาพื้นฐานของการเข้ารหัสเครือข่ายเรียบร้อยแล้วเพื่อที่จะสามารถหาคำตอบของปัญหาทั้งหมดได้จำเป็นต้องมีการกำหนดค่าให้กับตัวแปรต่าง ๆ ดังต่อไปนี้ ให้ q = 8 เนื่องมาจากว่าต้องมีการประมวลผลในระดับไบต์ สำหรับตัวแปร n และ q สามารถแบ่งได้เป็น 2 ส่วนดังนี้

1.2.1 n = 4, k = 2 เพื่อกำหนดให้ถ้าผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องแม่ข่ายได้ 2 เครื่องจากเครื่องแม่ข่ายทั้งหมด 4 เครื่อง ข้อมูลทั้งหมดจะปลอดภัย

1.2.2 n = 8, k = 4 เพื่อกำหนดให้ถ้าผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องแม่ข่ายได้ 4 เครื่องจากเครื่องแม่ข่ายทั้งหมด 8 เครื่อง ข้อมูลทั้งหมดจะปลอดภัย

1.3 การแก้ไขปัญหาพื้นฐานสำหรับการเข้ารหัสเครือข่าย

ในคำตอบของการแก้ไขปัญหาการเข้ารหัสเครือข่าย ทุกไบต์ของเวกเตอร์กุญแจรหัสลับจะถูกจัดกลุ่มรวมเข้าไปกับเวกเตอร์สุ่ม แล้วนำเวกเตอร์ที่ได้จากการจัดกลุ่มไปคูณเข้ากับเมทริกซ์ที่อินเวอร์สได้ M^{-1} และทุก ๆ ผลลัพธ์ที่ได้จาการคูณจะถูกกระจายไปเก็บยังเครื่องแม่ข่ายต่าง ๆ ต่อไป ดังตัวอย่างที่จะแสดงในการแก้ไขปัญหาพิเศษสำหรับการเข้ารหัสเครือข่าย

1.4 การแก้ไขปัญหาพิเศษสำหรับการเข้ารหัสเครือข่าย

1.4.1 n = 4, k = 2 ในกรณีนี้ให้ทำการแบ่งเวกเตอร์กุญแจรหัสลับออกเป็น 2 ส่วน ได้แก่ b_1และ b_2 และในกรณีของเวกเตอร์สุ่ม r_1 และ r_2 ก็กระทำในลักษณะเดียวกัน จากนั้นจึงนำไปคูณกับเมทริกซ์ที่อินเวอร์สได้ M^{-1} ดังนี้

$$E(\boldsymbol{b},\boldsymbol{r}) = [b_1, b_2, r_1, r_2] \cdot M^{-1} \quad (3\text{-}1)$$

$$= [b_1, b_2, r_1, r_2] \cdot \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 1 \\ 0 & 1 & -1 & 0 \end{bmatrix} \quad (3\text{-}2)$$

$$= [r_1, r_2, b_1 - r_1 - r_2, b_1 + r_1 + r_2] \quad (3\text{-}3)$$

$$= [s_1, s_2, s_3, s_4] \quad (3\text{-}4)$$

หลังจากที่ได้ผ่านกระบวนการเข้ารหัสเครือข่ายเรียบร้อยแล้วจะเห็นว่าแต่ละผลลัพธ์ที่อยู่ในเวกเตอร์ที่ (3-4) จะถูกกระจายไปเก็บยังเครื่องแม่ข่ายเครื่องต่าง ๆ ตัวอย่างเช่น $b_1 - r_1 - r_2$ ถูกส่งไปเก็บยังเครื่องแม่ข่ายเครื่องที่ 3 และ $b_1 + r_1 + r_2$ ถูกส่งไปเก็บยังเครื่องแม่ข่ายเครื่องที่ 4 ดังนั้นถ้าในกรณีที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องแม่ข่ายไม่มากกว่า 2 เครื่องจะไม่สามารถนำข้อมูลไปถอดรหัสกลับมาได้ b_1 และ b_2 ถ้าในกรณีที่ผู้ไม่หวังดีสามารถเข้าถึงเครื่องแม่ข่ายได้จำนวน 3 เครื่อง เช่นสามารถเข้าเครื่องที่เก็บข้อมูล $r_1, r_1, b_1 + r_1 + r_2$ เขาจะได้ข้อมูลไปเพียงครึ่งเดียวเท่านั้น ได้แก่ b_1 ดังนั้นเมื่อนำการแก้ไขปัญหานี้ไปใช้งานกับการเก็บกุญแจรหัสลับก็จะสามารถป้องกันการโจมตีจากผู้ไม่หวังดีได้ ค่า M^{-1} ที่ใช้ในตัวอย่างนั้นเป็นเพียงตัวอย่างหนึ่งของค่าที่คำนวณมาได้

1.4.2 $n = 8, k = 4$ ในกรณีนี้ให้ทำการแบ่งเวกเตอร์กุญแจรหัสลับออกเป็น 4 ส่วน ในลักษณะที่คล้ายกันกับในกรณีแรก นอกไปจากนี้ในกรณีของเวกเตอร์สุ่มก็ต้องแบ่งออกเป็น 4 ส่วนให้อยู่ลักษณะเดียวกัน จากนั้นจึงนำไปคูณกับเมทริกซ์ที่อินเวอร์สได้ M^{-1} ดังนี้

$$E(\boldsymbol{b},\boldsymbol{r}) = [b_1, b_2, b_3, b_4, r_1, r_2, r_3, r_4] \cdot M^{-1} \quad (3\text{-}5)$$

$$= [b_1, b_2, b_3, b_4, r_1, r_2, r_3, r_4] \cdot \begin{bmatrix} 0 & 0 & 0 & 0 & 23 & 1 & -3 & -4 \\ 0 & 0 & 0 & 0 & 1 & -14 & 8 & 5 \\ 0 & 0 & 0 & 0 & -3 & 8 & -7 & 2 \\ 0 & 0 & 0 & 0 & -4 & 5 & 2 & -3 \\ 1 & 0 & 0 & 0 & 4 & -5 & -2 & 3 \\ 0 & 1 & 0 & 0 & 3 & -8 & 7 & -2 \\ 0 & 0 & 1 & 0 & -1 & 14 & -8 & -5 \\ 0 & 0 & 0 & 1 & -23 & -1 & 3 & 4 \end{bmatrix} \quad (3\text{-}6)$$

$$= \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ r_4 \\ 23b_1 + b_2 - 3b_3 - 4b_4 + 4r_1 + 3r_2 - r_3 - 23r_4 \\ b_1 - 14b_2 + 8b_3 + 5b_4 - 5r_1 - 8r_2 + 14r_3 - r_4 \\ -3b_1 + 8b_2 - 7b_3 + 2b_4 - 2r_1 + 7r_2 - 8r_3 + 3r_4 \\ -4b_1 + 5b_2 + 2b_3 - 3b_4 + 3r_1 - 2r_2 - 5r_3 + 4r_4 \end{bmatrix}^T \quad (3\text{-}7)$$

$$= [s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8] \quad (3\text{-}8)$$

จากผลลัพธ์ที่ได้ในสมการที่ (3-8) นั้นสามารถนำข้อมูลที่ได้รับทั้งหมดไปกระจายเก็บยังเครื่องแม่ข่ายเครื่องต่าง ๆ โดยในการแก้ไขปัญหาดังกล่าวข้อมูลทั้งหมดจะปลอดภัยเมื่อผู้ไม่หวังดีสามารถโจมตีได้ไม่เกิน 4 เครื่อง จากทั้งหมด 8 เครื่อง

2. กลไกการรวบรวมกุญแจรหัสลับ (Key fusion engine)

กลไกการรวบรวมกุญแจรหัสลับเป็นกระบวนการย้อนกลับของกลไกการกระจายกุญแจรหัสลับ มีหน้าที่ความรับผิดชอบในการรวบรวมกุญแจและทำการถอดรหัสข้อมูลเพื่อให้ได้กุญแจรหัสลับที่ถูกต้องออกมา

จากสมการที่ (3-4) และ (3-8) รหัสเครือข่ายที่ได้คือ s_i เมื่อ i = 1, 2, 3, 4 ในปัญหาที่ 1 และ i = 1, 2, …, 8 ในปัญหาที่ 2 สามารถถูกแก้ไขได้โดยกลไกการรวบรวมกุญแจรหัสลับ ที่จะทำการแก้ไขสมการเชิงเส้นที่ (3-2) หรือ (3-6) เพื่อให้ได้กุญแจกลับคืนมาทั้งหมด และนำไปใช้สำหรับการเข้ารหัสต่อไป

บทที่ 4
ผลการวิจัย

เครื่องมือที่ใช้ในงานวิจัย

การพัฒนาโปรแกรมประยุกต์และทดสอบประสิทธิภาพการทำงานของระบบในงานวิจัยฉบับนี้พัฒนาด้วยโปรแกรมภาษา HTML, Javascript, CSS และ Java ที่ดำเนินการอยู่ภายใต้สถาปัตยกรรมแบบกลุ่มเมฆ ที่มีจำนวนซีพียู 4, 8, 16 และ 20 คอร์ตามลำดับ ด้วยระบบปฏิบัติการ Ubuntu 14.04LTS

วิธีการทดสอบ

การทดสอบแนวคิดและกระบวนการทำงานของระบบให้บริการป้องกันลิขสิทธิ์ดิจิทัลแบบคลาวด์ ที่ซึ่งนำเอาเทคนิคการแบ่งกุญแจลับออกเป็นหลายส่วน ด้วยเทคนิคการเข้ารหัสเครือข่ายดังกล่าวมาข้างต้นมาประยุกต์ใช้งานนั้น ภายในงานวิจัยฉบับนี้ มีการนำเสนอผลการดำเนินงานออกเป็น 2 ส่วน ได้แก่ การทดสอบประสิทธิภาพการทำงานของระบบ และการพัฒนาระบบฝั่งผู้ใช้งาน

1. การทดสอบประสิทธิภาพการทำงานของระบบ

ในการทดสอบประสิทธิภาพการทำงานของระบบนั้นสามารถแบ่งการทดสอบออกได้เป็น 2 ส่วน ได้แก่ การทดสอบประสิทธิในการกระจายและรวบรวมกุญแจรหัสลับ และการทดสอบระยะเวลาในกระบวนการทำ On-the-fly Encryption และ On-the-fly Decryption

1.1 การทดสอบประสิทธิภาพในการกระจายและรวบรวมกุญแจรหัสลับ

ในการทดสอบระยะเวลาในการกระจายและรวบรวมกุญแจรหัสลับนั้น งานวิจัยฉบับนี้ใช้การทดสอบการกระจายและรวมรวมกุญแจรหัสลับดังสมการ (3-8) ด้วยการวัดระยะเวลาขณะที่ประมวลผลตั้งแต่เริ่มกระบวนกระบวนการสร้างกุญแจรหัสลับ จนกระทั่งสามารถกระจายกุญแจรหัสลับไปยังเครื่องต่าง ๆ เพื่อเก็บบันทึกข้อมูล โดยทดสอบจากจำนวนผู้ใช้งาน (Concurrencies) ของระบบตั้งแต่ 100 1,000 2,000 3,000 4,000 5,000 6,000 7,000 8,000 9,000 และ 10,000 ตามลำดับ โดยแบ่งการทดสอบรอบละ 10 ครั้ง ด้วยเครื่อง VM-Based Server ที่มีจำนวนหน่วยประมวลผล 4, 8, 16, 20 คอร์ ตามลำดับ และประเมินหาค่าเฉลี่ยของระยะเวลาในกระบวนการทั้งหมด โดยการทดสอบการรวบรวมกุญแจรหัสลับนั้นสามารถกระทำได้ในลักษณะ

เดียวกัน โดยวัดผลตั้งแต่กระบวนการอ่านค่ากุญแจรหัสลับจากเครื่องต่าง ๆ จนกระทั่งสิ้นสุดกระบวนการสร้างกุญแจรหัสลับขึ้นมาใหม่ตามสมการการรวบรวมกุญแจ

1.2 การทดสอบประสิทธิภาพในกระบวนการทำ On-the-fly Encryption และ On-the-fly Decryption

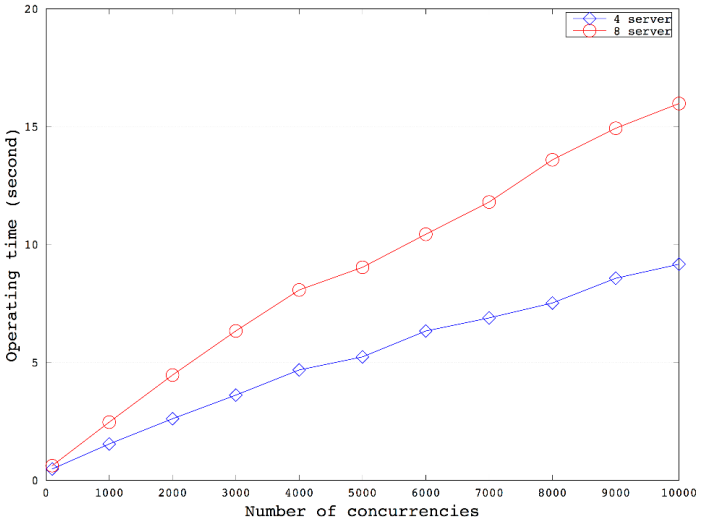
ในการทดสอบประสิทธิภาพการทำงานของกระบวนการทำ On-the-fly Encryption และ On-the-fly Decryption นั้น งานวิจัยฉบับได้ทำการรวบรวมข้อมูลการทำงานของการเข้ารหัสและถอดรหัสไฟล์ PDF ที่มีขนาด 100MB (อ้างอิงจากขนาดไฟล์เฉลี่ยที่พบได้ในระบบ eBook ของบริษัท ซีเอ็ดยูเคชั่น จำกัด (มหาชน)) จำนวน 10,000 ตัวอย่าง โดยใช้วัดผลเป็นหน่วยระยะเวลาในการดำเนินกระบวนการ

2. การพัฒนาระบบสำหรับฝั่งผู้ใช้งาน

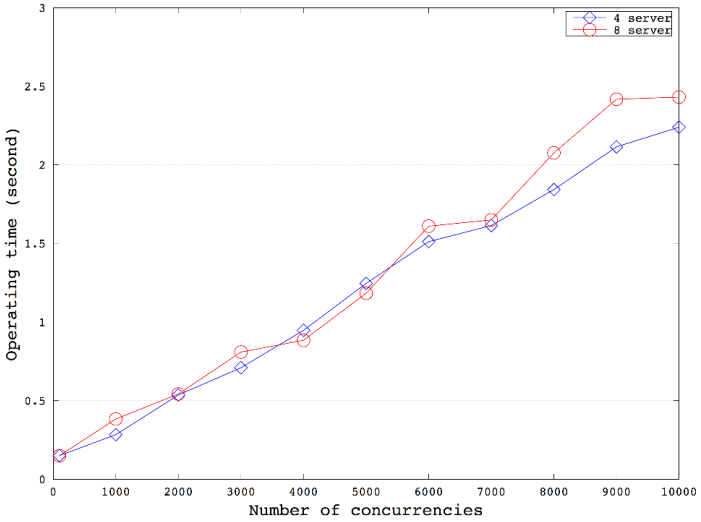
ในส่วนการพัฒนาระบบฝั่งผู้ใช้งาน นั้นงานวิจัยฉบับนี้เน้นการพัฒนาออกเป็น 2 ส่วน ได้แก่ การพัฒนาส่วนระบบสำหรับเจ้าของลิขสิทธิ์เพื่อใช้งานระบบให้บริการป้องกันลิขสิทธิ์ดิจิตัล และการพัฒนาส่วน Android SDK สำหรับผู้อ่านที่ได้ทำการติดต่อเพื่อซื้อขายหรือขอแจกจ่ายจากเจ้าของลิขสิทธิ์

ผลการทดสอบ

จากหัวข้อที่ 1 การทดสอบประสิทธิภาพการทำงานของระบบ โดยวัดผลการทดสอบจากระยะเวลาการประมวลผลดังภาพที่ 4-1 และ 4-2



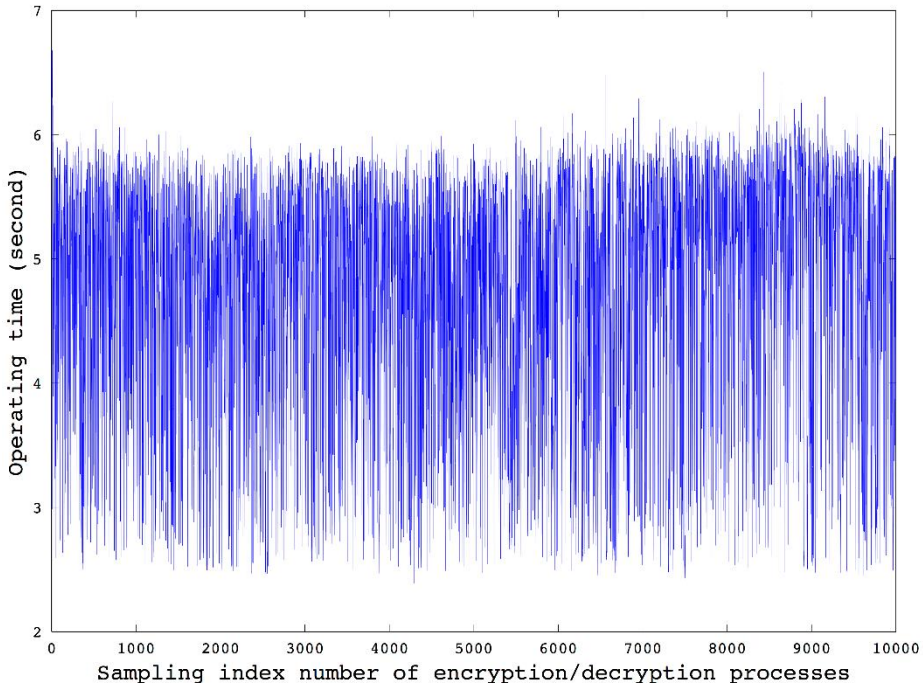
ภาพที่ 4-1 เวลาเฉลี่ยในการประมวลผลเพื่อกระจายกุญแจรหัสลับ



ภาพที่ 4-2 เวลาเฉลี่ยในการประมวลผลเพื่อรวบรวมกุญแจรหัสลับ

จากภาพที่ 4-1 แสดงการวัดผลเวลาที่เกิดขึ้นระหว่างประมวลผลเพื่อกระจายกุญแจรหัสลับตามสมการที่ (3-8) โดยเปรียบเทียบระหว่างจำนวนผู้ใช้งานเมื่อเข้ามาพร้อม ๆ กันกับเวลาในการประมวล ผลตั้งแต่เริ่มสร้างกุญแจกระทั่งกระจายไปเก็บยังเครื่องต่าง ๆ ที่มี 4 และ 8 เครื่องตามลำดับ โดยในกระบวนการดังกล่าวมีการทำงานเพียงครั้งเดียวเมื่อเจ้าของลิขสิทธิ์ลงทะเบียนเพื่อนำสินค้าเข้าสู่ระบบ จากการวัดผลเห็นได้ว่าการการเพิ่มขึ้นของเวลาในทั้งสองกรณีมีแนวโน้มเพิ่มขึ้นในลักษณะเชิงเส้น แต่ในกรณีที่กระจายชิ้นส่วนกุญแจรหัสลับทั้งหมด 8 เครื่องจะใช้เวลาในการประมวลผลที่นานกว่ากรณี 4 เครื่อง

จากภาพที่ 4-2 แสดงการวัดผลเวลาที่เกิดขึ้นระหว่างประมวลผลเพื่อรวบรวมชิ้นส่วนกุญแจรหัสลับ กระทั่งสามารถสร้างเป็นกุญแจได้ดังเดิม โดยเปรียบเทียบในลักษณะเดียวกับการวัดผลในการกระจายชิ้นส่วนกุญแจรหัสลับ จากการวัดผลเห็นได้ว่า ประสิทธิภาพในการทำงานของระบบทั้งสองรูปแบบมีความใกล้เคียงกัน แต่ช่วงที่ระบบรับจำนวนผู้ใช้งานมากกว่า 7,000 ในเวลาพร้อมกันนั้น เห็นได้ว่ามีเวลาที่ใช้ในการประมวลสูงขึ้น อย่างไรก็ตามความปลอดภัยจากการกระจายและรวบรวมชิ้นส่วนกุญแจรหัสลับจากเครื่องทั้ง 8 เครื่อง จำเป็นต้องแรกมากับระยะเวลาในการประมวลผลที่ยาวนานกว่าเดิม



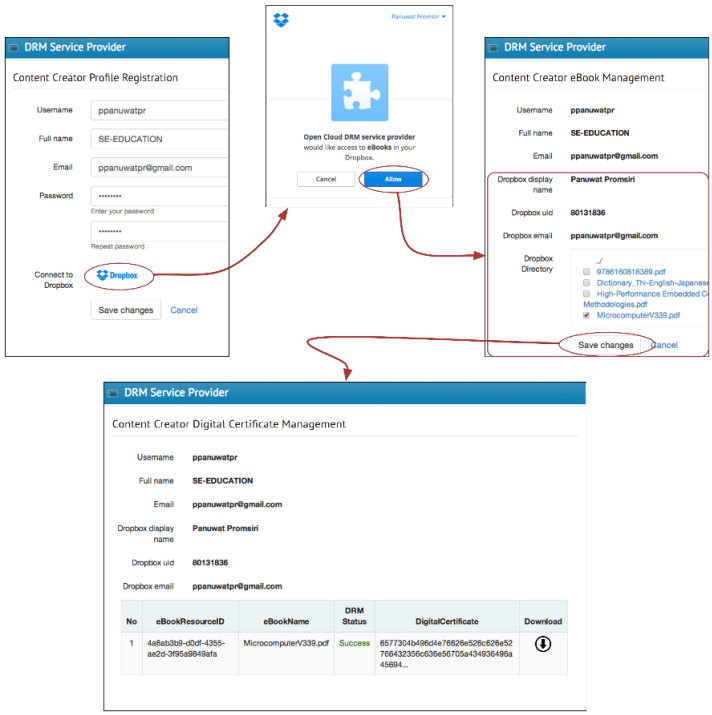
ภาพที่ 4-3 เวลาในการทำ On-the-fly Encryption และ On-the-fly Decryption

จากภาพที่ 4-3 แสดงการวัดผลช่วงเวลาที่เกิดขึ้นระหว่างประมวลผลไฟล์ PDF ขนาด 100MB จำนวน 10,000 รอบเพื่อทำ On-the-fly Encryption และ On-the-fly Decryption เห็นได้ว่าประสิทธิภาพในการประมวลผลอยู่ในช่วงระหว่าง 2.5 – 6.7 วินาที โดยมีค่าเฉลี่ย อยู่ที่ 4.69 วินาที ซึ่งสามารถแปรผันได้จากการทำงานของ I/O และการทำงานของเครือข่าย หลังจากเสร็จสิ้นกระบวนการทั้งสอง ผู้ใช้งานสามารถเริ่มอ่าน PDF ผ่านทางโปรแกรมอ่านหนังสืออิเล็กทรอนิกส์ตามที่ระบบให้บริการต่อไปโดยไม่มีการเก็บไฟล์หนังสืออิเล็กทรอนิกส์ไว้ภายในโปรแกรม

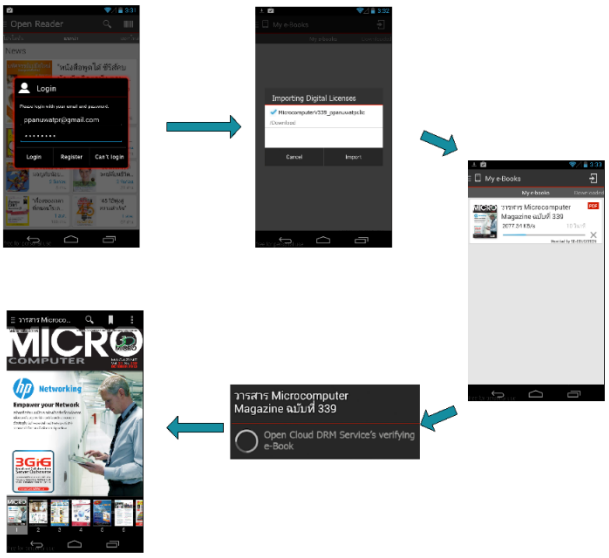
การพัฒนาโปรแกรมประยุกต์สำหรับบริหารจัดการข้อมูลไฟล์หนังสืออิเล็กทรอนิกส์ เมื่อเจ้าของลิขสิทธิ์ต้องการใช้ระบบบริการป้องกันลิขสิทธิ์ดิจิทัล เจ้าของลิขสิทธิ์ต้องลงทะเบียนเล่มหนังสือที่ต้องการเพื่อทำการสร้างใบรับรองดิจิทัล ดังแสดงในภาพที่ 4-4 หลังจากเสร็จสิ้นกระบวนการลงทะเบียน ระบบจะเริ่มกระบวนการเข้ารหัสไฟล์แบบ On-the-fly ด้วยกุญแจที่สร้างขึ้นมาจากระบบบริหารจัดการกุญแจรหัสลับ และบันทึกไฟล์ที่ได้รับการเข้ารหัสกลับไปยังศูนย์เก็บข้อมูลของเจ้าของลิขสิทธิ์ต่อไป

โปรแกรมประยุกต์ต้นแบบบนระบบปฏิบัติการ Android ที่รองรับการทำงานของระบบป้องกันลิขสิทธิ์ดิจิทัลตามงานวิจัยฉบับนี้ หลังจากที่เสร็จสิ้นกระบวนการติดตั้งและเข้าสู่ระบบ

ผู้ใช้งานต้องนำเข้าใบรับรองดิจิทัลเพื่อแสดงรายการหนังสืออิเล็กทรอนิกส์และเริ่มต้นในงานต่อไป ดังภาพที่ 4-5



ภาพที่ 4-4 ระบบบริหารจัดการข้อมูลสำหรับเจ้าของลิขสิทธิ์



ภาพที่ 4-5 โปรแกรมอ่านไฟล์หนังสืออิเล็กทรอนิกส์บนระบบปฏิบัติการ Android

บทที่ 5
สรุปผล อภิปรายผล และข้อเสนอแนะ

สรุปผลการศึกษา

จากการเจริญเติบโตของตลาดหนังสืออิเล็กทรอนิกส์ ส่งผลให้ระบบป้องกันลิขสิทธิ์ดิจิทัลเริ่มเข้ามามีความสำคัญเป็นอย่างมาก เพื่อการปกป้องผลประโยชน์ที่สมควรได้รับของเจ้าของลิขสิทธิ์ แต่ทว่าปัญหาในการพัฒนาหรือการเช่าใช้บริการ ยังคงมีค่าใช้จ่ายที่สูงเนื่องจากการลงทุนทางด้านอุปกรณ์เป็นหลัก

ในงานวิจัยฉบับนี้ได้เสนอแนวทางการแก้ไขปัญหาข้างต้นเพื่อช่วยเจ้าของลิขสิทธิ์ลดต้นทุนด้านการพัฒนาระบบด้วยการเสนอใช้ Cloud storage สาธารณะเป็นสถานที่ในการเก็บข้อมูล และให้ระบบป้องกันลิขสิทธิ์ดิจิทัลเข้าไปทำการปกป้องลิขสิทธิ์เนื้อหาต่าง ๆ ด้วยการเข้ารหัสแบบ On-the-fly และเพิ่มประสิทธิภาพด้านความปลอดภัยจากการเก็บกุญแจรหัสลับไว้ในสถานที่เดียวด้วยการกระจายกุญแจรหัสลับเก็บไว้ยังเครื่องแม่ข่ายต่าง ๆ โดยใช้เทคนิคตามทฤษฎีการเข้ารหัสเครือข่าย รวมไปถึงการนำเสนอ Android SDK ที่สามารถนำมาใช้งานกับระบบป้องกันข้อมูลลิขสิทธิ์ดิจิทัลตามงานวิจัยฉบับนี้ได้อย่างมีประสิทธิภาพ จากการประเมินผลพบว่าระบบมีความยืดหยุ่นมากพอที่จะสามารถนำไปใช้ได้ในสถานการณ์จริง

ข้อเสนอแนะแนวทางในอนาคต

จากการทดสอบด้านประสิทธิภาพระบบพบว่าในการใช้งานระบบป้องกันลิขสิทธิ์ดิจิทัลที่ประยุกต์ใช้เทคโนโลยีการเข้ารหัสเครือข่ายเพื่อกระจายชิ้นส่วนกุญแจรหัสลับไปยังเครื่องแม่ข่ายเสมือนที่มีจำนวน 4 และ 8 เครื่องตามลำดับ โดยที่ประสิทธิภาพการทำงานของระบบนั้นให้ผลที่ดีทั้งด้านการเข้ารหัสข้อมูลไฟล์ PDF และการกระจายชิ้นส่วนกุญแจรหัสลับที่เพิ่มความปลอดภัยของข้อมูลในกรณีที่เกิดการบุกรุกที่เครื่องแม่ข่าย แต่ในกรณีที่ต้องการความปลอดภัยของข้อมูลในระดับที่สูงขึ้น อาจมีการเปลี่ยนแปลงโมเดลในการกระจายกุญแจรหัสลับในรูปแบบอื่น ๆ หรือเพิ่มจำนวนเครื่องแม่ข่ายในการเก็บข้อมูลลับให้มากขึ้น

บรรณานุกรม

ภาคภูมิ อุทัยเลิศ (2553). *การจัดการข้อมูลจราจรบนระบบประมวลผลแบบกลุ่มเมฆจาลองโดยใช้โปรแกรมจูมลา.* กรุงเทพมหานคร: มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

Abbasov, B. (2014). *Cloud Computing: State Of The Art Reseach Issues.* Application of Information and Communication Technologies (AICT).

Boyd, R. (2012). *Getting Started with OAuth 2.0.* O'Reilly Media.

Cai, N., & Yeung, R. W. (2002). *Secure Network Coding.* Proceedings IEEE International Symposium on Information Theory.

Darwish, M., & Ouda, A. (2015). *Evaluation of an OAuth 2.0 Protocol Implementation for Web Server Applications.*

Dingledy, F., & Matamoros, A. B. (2016). *What is Digital Rights Management?*

Feldman, J., Malkin, T., Servedio, R. A., & Stein, C. (2004). *On the Capacity of Secure Network Coding.*

Frattolillo, F., & Landolfi, F. (2008). *Designing a DRM System.* The Fourth International Conference on Information Assurance and Security.

Gourkhede, M. H., & Theng, D. P. (2014). *Analysing Security and Privacy Management for Cloud Computing Environment.* Communication Systems and Network Technologies (CSNT).

Hofer, C., & Karagiannis, G. (2011). *Cloud computing services: taxonomy and comparison.*

Karada, O. P., Pipliya, A., Thakur, P., & Kamdar, N. (2013). *Analytical Survey Model on Consumption of Cloud Service Models.*

Kisin, B. B. (2013). *OPENID WITH CERTIFICATE-BASED USER AUTHENTICATION ON SMARTCARD.*

Kulkarni, G., Chavan, P., Bankar, H., Koli, K., & Waykule, V. (2012). *A new approach to Software as Service Cloud.* th International Conference on Telecommunication Systems, Services, and Applications (TSSA).

Liu, Q., Safavi-Naini, R., & Sheppard, N. P. (2003). *Digital Rights Management for Content Distribution.* Adelaide, Australia: Australasian Information Security Workshop 2003 (AISW2003).

Prihandoko, A. C., Litow, B., & Ghodosi, H. (2012). *DRM's Rights Protection Capability: A Review.* Medan, Indonesia: 1st International Conference on Computational Science and Information Management.

Rani, D., & Ranjan, R. K. (2014). *A Comparative Study of SaaS, PaaS and IaaS in Cloud Computing.* IJARCSSE.

Sendor, J., Lehmann, Y., Serme, G., & Oliveira, A. S. (2014). *Platform-level support for Authorization in Cloud Services with OAuth 2.* EEE International Conference on Cloud Engineering.

Shamir, A. (1979). *How to Share a Secret.* Communication of the ACM.

Weinhardt, C., Anandasivam, A., Benjamin, B., Borissov, N., Meinl, T., Michalk, W., & Stoß̈er, J. (2009). *Cloud Computing A Classification, Business Models,.* Business & Information Systems Engineering.

Zhang, J., Li, Q., Gong, X., & Fang, J. (2010). *A Novel DRM for Service Provider in Digital Reading.* Wuhan, China: International Conference on Information Engineering and Computer Science (ICIECS).