การรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ

นายโมฮำหมัดชารีฟุดดิน สาและอารง

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2559

Securing Document in Untrusted Cloud-Based Environment

Mr. Mohammadshareefuddin Salash-arong

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Computer Science
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2016

หัวข้อวิทยานิพนธ์	การรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ
โดย	นายโมฮำหมัดชารีฟุดดิน สาและอารง
สาขาวิชา	วิทยาศาสตร์คอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	ผู้ช่วยศาสตราจารย์ ดร. ณัฐวุฒิ หนูไพโรจน์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(รองศาสตราจารย์ ดร. สุพจน์ เตชวรสินสกุล)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(ผู้ช่วยศาสตราจารย์ ดร. วีระ เหมืองสิน)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(ผู้ช่วยศาสตราจารย์ ดร. ณัฐวุฒิ หนูไพโรจน์)

.....กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร. เกริก ภิรมย์โสภา)

.....กรรมการภายนอกมหาวิทยาลัย

(อาจารย์ ดร. พงศ์ธวัช ชีพพิมลชัย)

โมฮำหมัดชารีฟุดดิน สาและอารง : การรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ (Securing Document in Untrusted Cloud-Based Environment) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: ผศ. ดร. ณัฐวุฒิ หนูไพโรจน์, 133 หน้า.

ในปัจจุบัน มีผู้ใช้งานคอมพิวเตอร์จำนวนไม่น้อยที่เลือกใช้ SaaS Application ในรูปแบบ Storage ในการเก็บข้อมูลของตน อาทิ เช่น เอกสารกูเกิ้ล เนื่องจากมีความสะดวกสบายในการเรียกใช้ข้อมูลนั้นๆ โดยปราศจากการนำ เครื่องบันทึกข้อมูลส่วนตัว ไว้ติดตัวตลอดเวลา ซึ่งผู้ใช้งานสามารถจัดการหรือเรียกใช้ข้อมูล ของตนที่เก็บไว้ใน SaaS Storage ได้จากเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ จากที่ไหนก็ได้บนโลกใบนี้ที่มีการเชื่อมต่ออินเตอร์เน็ต แต่ถ้าคำนึงถึงความปลอดภัยของข้อมูลแล้วการที่ผู้ใช้งานเลือกเก็บข้อมูลของตนไว้ที่อื่นที่ไม่ใช่ที่ของตนนั้นย่อมจะมีความเสี่ยงหรืออันตรายที่อาจจะเกิดขึ้นกับข้อมูลนั้นๆได้ ตลอดเวลาโดยเฉพาะอย่างยิ่งถ้าข้อมูลนั้นเกิดเป็นข้อมูลสำคัญหรือข้อมูลลับ ที่อาจส่งผล อันตรายต่อผู้เป็นเจ้าของเองหรือองค์กรได้ ถ้าข้อมูลสำคัญหรือข้อมูลลับเกิดมีการรั่วไหลไปยัง บุคคลอื่น ดังนั้นจำเป็นอย่างยิ่งที่จะต้องมีมาตราการสำคัญในการทำให้ SaaS Storage มีความปลอดภัยมากพอ ที่จะทำให้ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานมีความปลอดภัยสูงสุด ถึงแม้ว่า SaaS Storage ที่เปิดให้บริการ จะมีการนำเสนอถึงกระบวนการความปลอดภัยมากมาย อาทิเช่นการเข้ารหัสข้อมูลหรือการออกแบบระบบโดยวางอุปกรณ์ Firewall ที่ทำให้ไม่สามารถเจาะเข้าไปในระบบได้ง่ายเพื่อให้ผู้ใช้งานหรือลูกค้ามีความมั่นใจที่จะเลือกใช้งานการให้บริการของตนที่ไม่ใช่การเลือกใช้ผู้ให้บริการเจ้าอื่นซึ่งมาตรการเหล่านี้จะมุ่งเน้นที่การป้องกันอันเนื่องมาจากบุคคลอื่นที่มาจากภายนอกระบบที่ให้บริการ SaaS Storage เท่านั้นแต่ยังขาดการป้องกันประเด็นความเสี่ยง อันเนื่องมาจากตัวบุคคลหรือบุคคลากร ที่เกี่ยวข้องกับผู้ให้บริการ เช่น ผู้ดูแลระบบ ซึ่งบุคคลเหล่านี้สามารถที่จะเข้าถึงข้อมูล สำคัญหรือข้อมูลลับของผู้ใช้งานได้โดยไม่ยาก การนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิทยาศาสตร์คอมพิวเตอร์ ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

ปีการศึกษา 2559

5670946121 : MAJOR COMPUTER SCIENCE

KEYWORDS: GOOGLE DOCS ADD-ON, GOOGLE DOCS CRYPTOGRAPHY, UNTRUSTWORTHY CLOUD ENVIRONMENT, TRUSTED MODEL, MULTIPLE CLOUD SERVICE PROVIDER KEY DISTRIBUTION, CLIENT SIDE SECURITY

MOHAMMADSHAREEFUDDIN SALASH-ARONG: Securing Document in Untrusted Cloud-Based Environment. ADVISOR: ASST. PROF. NATAWUT NUPAIROJ, Ph.D., 133 pp.

SaaS applications such as Google Documents have been increasingly widely-used to handle user documents stored in cloud storage. To ensure secured access in untrustworthy cloud environment, all documents in cloud storage must be encrypted and protected from unauthorized stakeholders. There are several automated solutions available. However, most solutions are straight-forward encryption without providing the protection from the system administrators of the cloud storage providers. In this paper, we propose TrustDocs, a new client side cryptography Google Docs Add-on application has presented the security mechanism for being solved the user concernation about Untrusted Cloud Provideer by multi-cloud trusted model. Our proposed solution ciphers and deciphers user documents in Google Drive. Using multiple cloud service providers and key-distribution-like methodology, our proposed solution provides secured mechanism for protecting the risk of user data even from brute-force attack by system administrators of the cloud storage providers. Our method supports both real-time standalone and version control collaborative edition for ensuring the security, privacy and usability of user document and can protect user secret information in untrustworthy cloud-based environment.

Department: Computer Engineering Student's Signature .....

Field of Study: Computer Science Advisor's Signature .....

Academic Year: 2016

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลงด้วยความกรุณาอย่างสูงของ ผู้ช่วยศาสตราจารย์ ดร. ณัฐวุฒิ หนูไพโรจน์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่กรุณาให้คำปรึกษา แนะนำแนวทางการวิจัย ตรวจทานงานวิจัย และแนะแนวทางการแก้ไขปัญหาจากงานวิจัย ตลอดจนมีความเมตตาในการให้ความรู้ที่เป็นประโยชน์ในการทำงานวิจัย ทำให้งานวิจัยสำเร็จลุล่วงไปด้วยดี ขอขอบพระคุณอาจารย์เป็นอย่างสูง ณ ที่นี้

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร. วีระ เหมืองสิน ประธานกรรมการการสอบวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร. เกริก ภิรมย์โสภา กรรมการสอบวิทยานิพนธ์ และอาจารย์ ดร. พงศ์ธวัช ชีพพิมลชัย กรรมการสอบวิทยานิพนธ์ (ภายนอกมหาวิทยาลัย) ที่กรุณาให้ความรู้และคำแนะนำที่เป็นประโยชน์ในการทำวิทยานิพนธ์

ขอบพระคุณอาจารย์ทุกท่านที่ให้ความรู้ สั่งสอน และให้คำแนะนำที่เป็นประโยชน์จนสามารถนำมาใช้ในการทำวิทยานิพนธ์ได้

ขอบพระคุณบิดาและมารดาที่ให้โอกาส กำลังใจในการเรียน สั่งสอน และสนับสนุนให้ข้าพเจ้าหลาย ๆ ด้าน จนข้าพเจ้าประสบผลสำเร็จ

ขอบคุณเพื่อนนิสิต วิทยาศาสตร์คอมพิวเตอร์ วิศวกรรมซอฟต์แวร์ และ วิศวกรรมคอมพิวเตอร์ ที่คอยช่วยเหลือในหลาย ๆ เรื่อง เช่น ข่าวสารมหาวิทยาลัย แหล่งข้อมูลงานประชุมวิชาการ เป็นต้น

สารบัญ

หน้า

หน้า

หน้า

หน้า

หน้า

3.2.3.2 สถานะการกระจาย (Distribution State): หรือ [$ki1$] เป็นสถานะของค่ากุญแจลับที่มีการเรียกใช้งานจากโปรแกรมเสริม TrustDocs ในการกระทำการเข้ารหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานทั้งไฟล์เอกสารกูเกิ้ลที่สร้างใหม่ โปรแกรมเสริมเอกสารกูเกิ้ลจะเรียกใช้งาน [$ki0$] มาทำการเข้ารหัสลับกับข้อความดัมมี่ (Dummy Text) ที่ทางโปรแกรมเสริม TrustDocs เตรียมไว้เพื่อจับคู่ค่ากุญแจลับกับไฟล์เอกสารกูเกิ้ลใหม่ หลังจากโปรแกรมเสริม TrustDocs ได้ทำการเข้ารหัสลับข้อความดัมมี่และจับคู่ค่ากุญแจลับกับไฟล์เอกสารใหม่เรียบร้อยแล้ว โปรแกรมเสริม TrustDocs จะดำเนินการเปลี่ยนสถานะของค่ากุญแจลับ [$ki0$] (Origination State) กลายเป็น [$ki1$] (Distribution State) ที่อยู่ในสถานะกระจายนี้ และโปรแกรมเสริม TrustDocs ก็ทำการถอดรหัสข้อความดัมมี่เพื่อให้ทางผู้ใช้งานได้เห็น “Welcome to TrustDocs. Delete All then Start!” ซึ่งกระบวนการถอดรหัสลับข้อความดัมมี่ดังกล่าว โปรแกรมเสริม TrustDocs จะทำการเปลี่ยนสถานะของค่ากุญแจลับจาก [$ki1$] (Distribution State) กลายเป็นค่ากุญแจลับสถานะ [$ki2$] (Operation State) ซึ่งเป็นค่ากุญแจลับที่อยู่ในสถานะถัดไป 40

หน้า

หน้า

สารบัญตาราง

หน้า

สารบัญรูปภาพ

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน มีผู้ใช้งานคอมพิวเตอร์ (User) จำนวนไม่น้อยที่เลือกใช้ SaaS (Software as a Service) [1] ในรูปแบบ Storage ในการเก็บข้อมูลของตน เนื่องจากมีความสะดวกสบายในการเรียกใช้ข้อมูลนั้นๆ โดยปราศจากการนำ เครื่องบันทึกข้อมูลส่วนตัว ไว้ติดตัวตลอดเวลา อาทิเช่น แฟลชไดร์ฟ (Flash drive) หรือเครื่องคอมพิวเตอร์ แบบพกพาส่วนตัว (Computer Notebook) ซึ่งผู้ใช้งานสามารถจัดการหรือเรียกใช้ข้อมูล ของตนที่เก็บไว้ใน SaaS Storage ได้จากเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ จากที่ไหนก็ได้บนโลกใบนี้ที่มีการเชื่อมต่ออินเตอร์เน็ต (Internet) แต่ถ้าคำนึงถึงความปลอดภัยของข้อมูล (Data Security) แล้วการที่ผู้ใช้งานเลือกเก็บข้อมูลของตน ไว้ที่อื่นที่ไม่ใช่ที่ของตนนั้นย่อมจะมีความเสี่ยง(Risk) หรืออันตราย (Dangerous) ที่อาจจะเกิดขึ้นกับข้อมูลนั้นๆได้ ตลอดเวลาโดยเฉพาะอย่างยิ่งถ้าข้อมูลนั้นเกิดเป็นข้อมูลสำคัญหรือข้อมูลลับ (Sensitive Data) [2] ที่อาจส่งผล อันตรายต่อผู้เป็นเจ้าของเองหรือองค์กรได้ ถ้าข้อมูลสำคัญหรือข้อมูลลับเกิดมีการรั่วไหล (Data Leakage) ไปยัง บุคคลอื่น ดังนั้นจำเป็นอย่างยิ่งที่จะต้องมีมาตราการสำคัญในการทำให้ SaaS Storage มีความปลอดภัยมากพอ ที่จะทำให้ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานมีความปลอดภัยสูงสุด ถึงแม้ว่า SaaS Storage ที่เปิดให้บริการ จะมีการนำเสนอถึงกระบวนการความปลอดภัยมากมาย อาทิเช่น การเข้ารหัสข้อมูล (Data Encryption) หรือ การออกแบบระบบโดยวางอุปกรณ์ Firewall ที่ทำให้ไม่สามารถเจาะเข้าไปในระบบได้ง่ายเพื่อให้ผู้ใช้งานหรือ ลูกค้า (Customer) มีความมั่นใจที่จะเลือกใช้งานการให้บริการของตนที่ไม่ใช่การเลือกใช้ผู้ให้บริการ (Cloud Provider) เจ้าอื่นซึ่งมาตรการเหล่านี้จะมุ่งเน้นที่การป้องกันอันเนื่องมาจากบุคคลอื่นที่มาจากภายนอกระบบที่ให้บริการ SaaS Storage เท่านั้นแต่ยังขาดการป้องกันประเด็นความเสี่ยง อันเนื่องมาจากตัวบุคคลหรือบุคคลากร ที่เกี่ยวข้องกับผู้ให้บริการ เช่น ผู้ดูแลระบบ (System Administrator) ซึ่งบุคคลเหล่านี้สามารถที่จะเข้าถึงข้อมูล สำคัญหรือข้อมูลลับของผู้ใช้งานได้โดยไม่ยาก

จากงานวิจัยที่ผ่านมามีจำนวนหนึ่งที่ให้ความสำคัญเกี่ยวกับความปลอดภัย (Security) ป้องกันจาก ภัยคุกคาม (Threat) และนโยบายความเป็นส่วนตน (Privacy) ของการให้บริการในลักษณะคลาวด์ในรูปแบบ SaaS Storage โดยการนำเสนอหลักการหรือโมเดลการใช้วิทยาการรหัส

ลับ (Cryptography) และอื่นๆทั้งจัดเตรียมให้สำหรับฝั่งระบบหรือเซิร์ฟเวอร์ (Server side) และสำหรับฝั่งผู้ใช้งาน (Client side) มาแก้ไขปัญหาในส่วนนี้ แต่ปัญหาดังกล่าวก็ยังไม่สามารถถูกแก้ไขได้ทั้งหมด เนื่องจากในมุมมองของผู้ใช้งานนั้น ข้อมูลสำคัญหรือข้อมูลลับของตน นอกจากจะต้องมีความปลอดภัยแล้ว ยังจะต้องมีความเชื่อมั่นว่าข้อมูลของตนจะไม่ รั่วไหลไปถึงบุคคลใดบุคคลหนึ่ง ซึ่งไม่ใช่ตนเองหรือบุคคลที่ตนอนุญาตเท่านั้น ซึ่งงานวิจัยที่ผ่านมานั้น มีการใช้วิทยาการรหัสลับ ทั้งในรูปแบบที่ได้รับการจัดเตรียมจากผู้ให้บริการเอง และการจัดการการใช้วิทยาการรหัสลับที่ดำเนินการจากฝั่งของผู้ใช้งานเอง ซึ่งในปัจจุบัน ผู้ให้บริการ SaaS Storage ที่มีชื่อเสียงหลายราย ยังไม่มีการกล่าวถึงหรือนำเสนอการใช้วิทยาการ รหัสลับกับของตนอย่างเห็นได้ชัด ได้แค่กล่าวเพียงว่า SaaS Storage ของตนมีความปลอดภัยมากพอที่จะทำให้ ลูกค้าหรือผู้ใช้งานวางใจกับข้อมูลสำคัญหรือข้อมูลลับของตน ซึ่งหลักการความปลอดภัยดังกล่าวอาจมิใช่การใช้ วิทยาการรหัสลับซึ่งเป็นวิธีที่ปลอดภัยที่สุดสำหรับการปกปิดข้อมูลสำคัญหรือข้อมูลลับ และยังมีงานวิจัยที่มีการ นำเสนอการใช้วิทยาการรหัสลับที่ฝั่งของผู้ใช้งาน แต่ระบบการจัดการค่ากุญแจที่ไม่ดีพอ [3] เช่น มีการสร้าง ค่ากุญแจด้วยผู้ใช้งานเอง (Manual) และการกระจายค่ากุญแจ (Key Distribute) ไปยังผู้ใช้งานร่วมที่ยังไม่ดีพอ เช่น การโทรหาผู้ใช้งานร่วมเพื่อบอกค่ากุญแจนั้นๆ ซึ่งปัญหาที่อาจจะเกิดขึ้นนั้นอาจจะมาจากความยากลำบาก ในการจัดการค่ากุญแจดังกล่าว เช่น ลืมค่ากุญแจ ก็เป็นได้

ปัญหาที่ได้ระบุไว้ข้างต้นที่เกิดขึ้นในปัจจุบันเกิดจากการเลือกใช้ผู้ให้บริการ SaaS Storage เพียงแค่ รายเดียวในการเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน ซึ่งถ้าเราเลือกใช้ผู้ให้บริการเดียวในการเก็บข้อมูลสำคัญทั้งหมด ถึงแม้รูปแบบที่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะถูกเข้ารหัสลับแบบไม่สามารถใช้งานได้นั้น แต่ข้อมูลอื่นๆเช่น ค่ากุญแจต่างๆ ที่เกี่ยวข้อง ก็ยังอยู่ในการดูแลของผู้ให้บริการ ดังนั้นบุคคลที่เกี่ยวข้องเช่น ผู้ดูแลระบบก็สามารถที่จะนำค่ากุญแจต่างๆที่เกี่ยวข้องเพื่อถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำข้อมูลที่ได้มา เอาไปใช้งานที่สามารถก่อให้เกิดอันตรายต่อผู้ใช้งานได้ ดังนั้นการหากลไกรักษาความปลอดภัยของ เอกสารโดยการใช้ผู้ให้บริการ SaaS Storage มากกว่า 1 ราย มาทำงานร่วมกันเพื่อจัดเก็บข้อมูลสำคัญหรือ ข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้ วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง ในงานวิจัยนี้ ผู้วิจัยจึงนำเสนอหลักการหรือโมเดลใหม่ และกระบวนการ การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งาน (Client Side Cryptography) ที่สามารถตอบโจทย์ด้านความเหมาะสม และความปลอดภัยจากช่องโหว่ต่างๆ ที่อาจจะเกิดอันตรายต่อข้อมูลสำคัญ หรือข้อมูลลับ ขึ้นมาจากปัญหาดั่งกล่าว โดยจะเลือกใช้ทรัพยากร (Resource) ที่เป็นการประมวลผลแบบคลาวด์ (Cloud Computing) ในรูปแบบ SaaS ที่ให้บริการด้าน Storage จำนวน 2 รายเพื่อนำมาเป็นที่เก็บข้อมูลสำคัญหรือข้อมูลลับ (Data Repository) และเป็นที่เก็บค่ากุญแจ (Key Repository) ต่างๆที่เกี่ยวข้อง โดยการพัฒนาระบบต้นแบบที่ทำงานร่วมกับ

ระบบเอกสารกูเกิ้ล (Google Document) ในการจำลองการเป็นช่องทางการบริหารจัดการข้อมูลสำคัญ หรือข้อมูลลับของผู้ใช้งานทั่วไป ซึ่งจะใช้ Google Drive ในการจำลองเป็น Storage หรือ Data Repository ในการเก็บข้อมูล และใช้ ClearDB ในฐานะผู้ให้บริการ SaaS Storage ที่ให้บริการจัดเก็บข้อมูลในรูปแบบข้อมูล SQL Database อีกรายหนึ่งในการจำลองเป็น Key Repository ในการเก็บค่ากุญแจลับ (Session Key) ในส่วนกระบวนการ การใช้วิทยาการรหัสลับที่ฝังผู้ใช้งานนั้น ผู้วิจัยจะนำเสนอกระบวนการ ในรูปแบบในการเข้ารหัสลับข้อมูล (Data Encryption) การถอดรหัสลับข้อมูล (Data Decryption) และ การกระจายค่ากุญแจต่างๆ (Key Distribution) ในรูปแบบ ที่เป็นกระบวนการอัตโนมัติ (Automatic Process) เพื่อแก้ไขปัญหาในการใช้งานข้อมูลสำคัญ หรือข้อมูลลับ ที่เก็บไว้ที่ SaaS Storage ได้ง่ายและมีความปลอดภัยจากภัยคุกคามมากขึ้น

1.2 วัตถุประสงค์งานวิจัย

โครงงานวิจัยนี้มีวัตถุประสงค์เพื่อนำเสนอกระบวนการ หรือโมเดลใหม่ในการจัดการข้อมูลของผู้ใช้งาน SaaS Storage โดยการเลือกใช้ผู้ให้บริการด้าน SaaS Storage มากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญ หรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ

1.3 ขั้นตอนการวิจัย

การศึกษาและออกแบบการรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ มีขั้นตอนการดำเนินงานดังนี้

1.3.1 ศึกษางานวิจัยที่เกี่ยวข้อง

1.3.2 ศึกษาการเข้ารหัสและการถอดรหัสแบบสมมาตร (Symmetric Key Cryptography) และแบบอสมมาตร (Asymmetric Key Cryptography)

1.3.3 ศึกษา Google Docs API

1.3.4 ศึกษา Google Drive API

1.3.5 ศึกษา Google JDBC API

1.3.6 ศึกษาการพัฒนาโปรแกรมเสริม (Add-on) สำหรับ เอกสารกูเกิ้ล (Google Docs Add-on)

1.3.7 รวบรวมข้อมูลจากการทดลองและออกแบบ

1.3.8 พัฒนาระบบเข้ารหัสและถอดรหัสไฟลข้อมูลเอกสารกูเกิ้ล

1.3.9 ทดสอบการใช้งานและเก็บข้อมูล

1.3.10 วิเคราะห์ผลจากระบบ

1.3.11 ปรับปรุงข้อผิดพลาด

1.3.12 สรุปผลและเรียบเรียงวิทยานิพนธ์

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ผู้ใช้งานมีความมั่นใจในข้อมูลสำคัญมากขึ้นในการใช้งาน SaaS Storage โดยไร้ข้อกังวลใน เรื่องข้อมูลสำคัญหรือข้อมูลลับเหล่านั้นรั่วไหลไปยังบุคคลที่ไม่หวังดี

1.4.2 อาจจะเกิดแรงจูงใจจากผู้ใช้งานให้มีการใช้บริการทางด้าน SaaS Storage เพิ่มจำนวนมากขึ้น

1.4.3 การที่จัดการเก็บกุญแจลับ ไว้ไม่เป็นที่เดียวกัน เพื่อป้องกันไม่ให้บุคคลที่ไม่หวังดีสามารถนำมาใช้ในการถอดรหัสข้อมูลได้

1.4.4 หลักการทั้งหมดของการสนับสนุนความปลอดภัยอยู่ที่เครื่องของผู้ใช้งาน (Client Side Security)

1.4.5 ผู้ใช้งานทั้งเจ้าของไฟล์ และผู้ใช้งานร่วมสามารถใช้งานไฟล์แก้ไขข้อมูลไปพร้อมกันแบบ Version Control โดยความปลอดภัยก็ยังคงอยู่

1.5 ขอบเขตการวิจัย

การศึกษาออกแบบการรักษาความปลอดภัย ของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ กำหนดขอบเขตการดำเนินงานดังนี้

1.5.1 เลือกใช้ความสามารถของเอกสารกูเกิ้ล (Google Docs) ในการจำลองเป็นช่องทางในการบริหารจัดการข้อมูลสำคัญหรือข้อมูลลับ (D_i) ของผู้ใช้งานทั่วไป

1.5.2 เลือกใช้ Google Drive จำลองการเก็บข้อมูล สำคัญหรือข้อมูลลับ (Data Repository) ของผู้ใช้งาน ซึ่งข้อมูลเหล่านั้นจะต้องอยู่ในรูปที่เข้ารหัสลับ (Cipher Text) (D'_i) เรียบร้อยแล้ว

1.5.3 เลือกใช้ ClearDB ที่ให้บริการ SaaS Storage ในด้านการเก็บข้อมูลในรูปแบบโครงสร้างฐานข้อมูล (SQL Database) ในการจำลองการเก็บค่ากุญแจ (Key Repository) เพื่อ

จัดการเก็บค่ากุญแจลับ (Session Key) (K_{Di}) ของผู้ใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล (Google Docs Add-on)

1.5.4 พัฒนาโปรแกรมเสริม (Add-on) สำหรับ เอกสารกูเกิ้ล (Google Docs Add-on) เพื่อสนับสนุน การเข้าและถอดรหัสข้อมูลสำคัญ หรือข้อมูลลับ (Sensitive Data)

1.5.5 รองรับการเข้าและถอดรหัสข้อมูลไฟล์เอกสารกูเกิ้ลด้วยอัลกอริทึม AES-256

1.5.6 รองรับการเรียกใช้งานค่ากุญแจลับ (Session Key) (K_{Di}) จาก ClearDB ในช่องทางที่ปลอดภัย (Secure Channel) ด้วยโปรโตคอลเอสเอสแอล (SSL Protocol)

1.5.7 รองรับการจับคู่กับค่ากุญแจลับ (Mapping Session Key) รวมถึงการทำการสิ้นสุดการใช้งานค่ากุญแจลับเดิม (Expire Session Key)

1.5.8 รองรับการจับคู่กับค่ากุญแจใหม่ (Refresh Session Key) เมื่อครบ 1 รอบในการเข้า และถอดรหัสข้อมูลสำคัญหรือข้อมูลลับ โดยมีการจับคู่ค่ากุญแจใหม่ทุกครั้งที่มีการเข้ารหัสข้อมูลสำคัญหรือข้อมูลลับในครั้งต่อไป

1.5.9 รองรับการเรียกใช้งานค่ากุญแจลับร่วม (Collaborative Session Key) ในกรณีที่ต้องการแบ่งปันไฟล์เอกสารกูเกิ้ลไปให้กับผู้ใช้งานร่วมเพื่อแก้ไขข้อมูลแบบ Version Control โดยไม่สนับสนุนคุณสมบัติของการใช้งานเอกสารกูเกิ้ลในด้านการใช้งานในรูปแบบการแก้ไขร่วมกันแบบเรียลไทม์

1.5.10 ทดสอบประสิทธิภาพของระบบที่ได้นำเสนอ โดยใช้ตัวชี้วัด (Metrics) คือ ประสิทธิภาพทาง ด้าน เวลาเฉลี่ย (Average Time) ที่ใช้ไปดังต่อไปนี้

1.5.10.1 *เวลาเฉลี่ยที่ใช้ในการเข้ารหัสข้อมูลไฟล์เอกสารกูเกิ้ลด้วยอัลกอริทึม AES-256 ใน กรณีที่ผู้ใช้งานต้องการที่จะเขียนหรือแก้ไขข้อมูลไฟล์เอกสารกูเกิ้ลที่มีขนาดจำนวน 10 100 700 และ 7000 ตัวอักษรได้ก่อนที่จะถูกเก็บไว้ใน Google Drive*

1.5.10.2 *เวลาเฉลี่ยที่ใช้ในการการถอดรหัสข้อมูลไฟล์เอกสารกูเกิ้ลด้วยอัลกอริทึม AES-256 ในกรณีที่ผู้ใช้งานต้องการที่จะอ่านข้อมูลไฟล์เอกสารกูเกิ้ลที่มีขนาดจำนวน 10 100 700 และ 7000 ตัวอักษร*

1.6 ผลงานตีพิมพ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้รับการตีพิมพ์ในรายงานสืบเนื่องจากการประชุมวิชาการระดับนานาชาติเรื่อง “TrustDocs -- Google Docs add-on: Securing Document in Untrusted Cloud-based Environment”, Mohammadshareefuddin and Natawut Nupairoj, in Proceeding of 6th International Conference on Software and Computer Applications (ICSCA 2017), Pages 181-185, February 26-28, 2017 in Bangkok, Thailand.

บทที่ 2

ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎี

จากการศึกษาการวิเคราะห์และออกแบบ การรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือนั้น พบว่า ทฤษฎีที่เกี่ยวข้องและเป็นประโยชน์ในการวิจัย และพัฒนาประกอบด้วย ดังต่อไปนี้

2.1.1 ทฤษฎีที่เกี่ยวข้องและสถาปัตยกรรม Cloud Computing

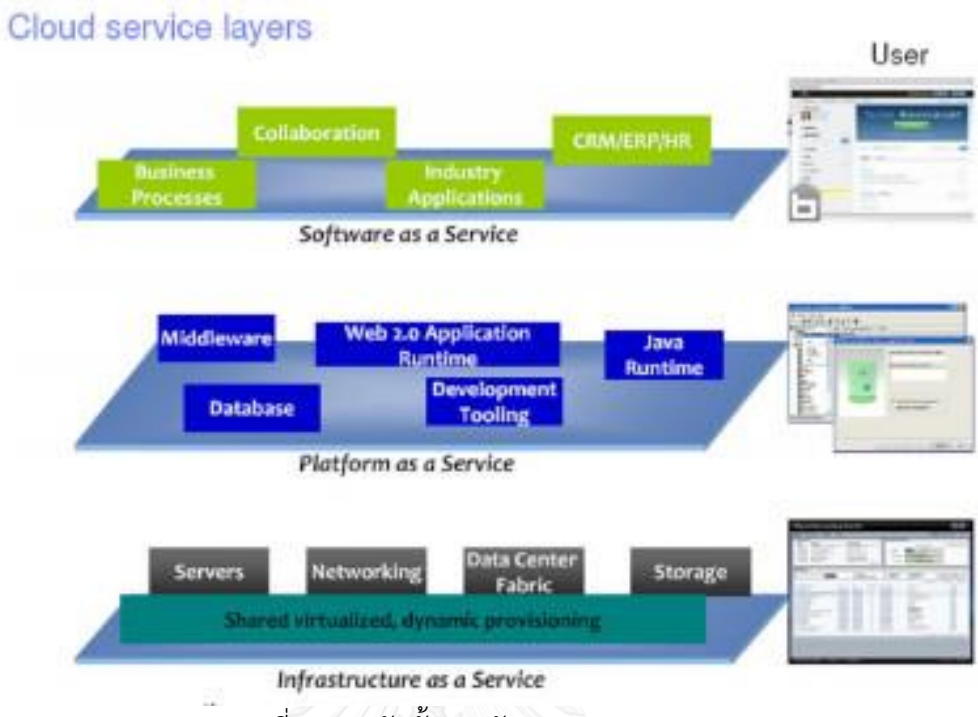
Cloud Computing [4] หมายถึง ระบบคอมพิวเตอร์รูปแบบหนึ่งที่ผู้ใช้บริการไม่จำเป็นต้องทราบ กระบวนการในการทำงานของระบบ ส่วนผู้ให้บริการจะนำทรัพยากรที่มีอยู่ในระบบที่มีความยืดหยุ่น นำมาจัดสรร เพื่อให้บริการในรูปแบบเทคโนโลยีคอมพิวเตอร์เสมือนเพื่อได้รับประโยชน์สูงสุด

รูปที่ 2.1 แสดงรูปแบบสถาปัตยกรรมของระบบ Cloud Computing นั้นจะแบ่งออกเป็นโมเดล ของการให้บริการหรือ Service layer ออกเป็น 3 ส่วน คือ

Software as a Service (SaaS) คือ ส่วนการให้บริการในส่วนของแอพลิเคชั่น หรือส่วนที่ติดต่อกับผู้ใช้ เช่น Google Drive, Dropbox, Sky Drive เป็นต้น

Platform as a Service (PaaS) คือ ส่วนการให้บริการในส่วนของ Platform หรือระบบพื้นฐาน ในการทำงาน เช่น การให้บริการ Database, Middleware หรือ Java Runtime เป็นต้น

Infrastructure as a Service (IaaS) คือ ส่วนการให้บริการในส่วนของฮาร์ดแวร์ เช่น การจัดการด้าน เซิร์ฟเวอร์ ระบบเครือข่าย การเก็บข้อมูล เป็นต้น

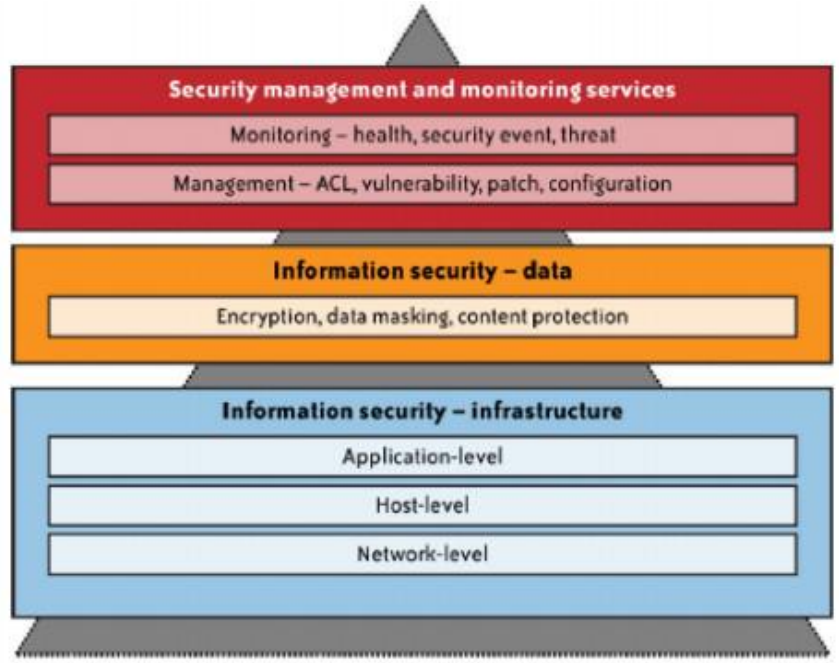


รูปที่ 2.1 ระดับชั้นสถาปัตยกรรมของ service layer [5]

2.2 ทฤษฎีที่เกี่ยวข้องกับการจัดการความปลอดภัยในระบบ Cloud Computing

ในระบบของ Cloud Computing นั้นเป็นรูปแบบเครือข่ายขนาดใหญ่ ที่ในส่วนต่างๆ แยกออกจากกันไม่ว่าจะเป็น ระบบ แอพพลิเคชั่น หรือข้อมูล โดยโมเดลการรักษาความปลอดภัยของระบบ Cloud Computing นั้นต้องสามารถตอบสนองต่อผู้ให้บริการหรือเจ้าของเครือข่ายได้ โดยคำถามแรกที่ผู้ดูแลรักษาความปลอดภัยในระบบ Cloud Computing มักจะตั้งไว้เป็นคำถามแรกในการรักษาความปลอดภัยให้กับระบบคือ เราจะทำย่างไรให้ข้อมูลที่มีการแชร์ในระบบ Cloud ของเราให้มีความปลอดภัย และคำถามที่สองคือ จะมีวิธีการจัดการกับผู้ใช้บริการในระบบ Cloud ของเราอย่างไร ไม่ว่าจะเป็นเรื่องสิทธิ์การเข้าใช้งานหรือความปลอดภัยของผู้เข้าใช้งาน เมื่อเข้าเชื่อมต่อกับระบบ สิ่งต่างๆ เหล่านี้ทำให้เราเกิดคำถามขึ้นมากมาย การที่จะตอบโจทย์ของการทำงานเหล่านั้น ได้นั้น ทำให้เราต้องทำการมองภาพรวมของระบบ เพื่อทำการกำหนดขอบเขตงาน เพื่อนำมาสร้าง ความปลอดภัยขึ้นมาในระบบ Cloud Computing ของเรา

หากเราต้องการที่จะทำการรับส่งข้อมูล หรือทำกิจกรรมอะไรสักอย่างที่มีการตอบโต้กับผู้ให้บริการในระบบ Cloud computing นั้นการโต้ตอบที่ได้รับก็จะมีความแตกต่างกันเนื่องจากระบบ Cloud นั้นอาจจะประกอบด้วยผู้ให้บริการหลายคน รวมทั้งอาจมีความหลากหลายในการให้บริการด้วย การเกิดความผิดพลาดหรือจุดบกพร่องในความปลอดภัยอาจเกิดได้จากหลายจุด



รูปที่ 2.2 Security management and monitoring scope [6]

2.3 จุดมุ่งหมายของความปลอดภัย (Security) ให้กับข้อมูลในเครื่องคอมพิวเตอร์ (Computer) บนระบบเครือข่าย (Internet) [7]

ในการทำธุรกรรมบน Internet นั้นต้องการที่จะพิสูจน์ตัวบุคคล และ เพิ่มความมั่นคง ความปลอดภัยให้กับข้อมูลบน Internet ทำให้บุคคลที่สามไม่สามารถเข้าถึงข้อมูลได้ ซึ่งจุดมุ่งหมาย ของการเพิ่มความปลอดภัยในคอมพิวเตอร์เครือข่าย ประกอบด้วย 5 ส่วนดังนี้

2.3.1 การรักษาความลับ (Confidentiality)

การรักษาความลับ หมายถึง การที่ผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงทรัพยากรหรือข้อมูลที่กำหนดไว้ได้ ผู้ที่ไม่มีสิทธิ์จะไม่สามารถล่วงรู้ข้อมูลนี้ได้ ตัวอย่างเช่น ข้อมูลผลการสอบหรือรายละเอียดส่วนตัวของนักศึกษาในมหาวิทยาลัย จัดว่าเป็นข้อมูลส่วนตัว ซึ่งผู้ที่มีสิทธิ์เข้าถึงข้อมูลนี้ควรเป็นนักศึกษาเจ้าของข้อมูลนี้ หรืออาจารย์ที่เกี่ยวข้อง ผู้อื่นที่ไม่เกี่ยวข้องไม่ควรเข้าถึงข้อมูลเหล่านี้ได้ เป็นต้น จุดมุ่งหมายข้อนี้เป็นเรื่องที่มีความสำคัญมากในบางวงการ เช่นการทางทหาร หรือความมั่นคงของชาติ

หลักการที่ใช้ในการรักษาความลับของข้อมูลคือ วิทยาการรหัสลับ (Cryptography) ซึ่งเป็นศาสตร์เก่าแก่ที่มีมาตั้งแต่สมัยโบราณ และได้รับการพัฒนาอย่างต่อเนื่องจนมาถึงในยุคปัจจุบัน โดยในสมัยก่อนวิทยาการรหัสลับใช้ในการทหารเป็นหลัก เพื่อป้องกันข้อมูลของชาติไม่ให้รั่วไหลไปถึง

ฝ่ายตรงข้าม หรือใช้ในการส่งข่าวสารสำคัญในภาวะสงคราม ในปัจจุบันวิทยาการรหัสลับจัดเป็นเทคนิคสำคัญที่มีนำมาใช้ปกป้องความเป็นส่วนตัวของการรับส่งผ่านข่าวสารโดยเฉพาะผ่านระบบเครือข่าย ในช่วงหลายสิบปีที่ผ่านมาได้มีการพัฒนาองค์ความรู้ทางด้านวิทยาการรหัสลับไว้จำนวนมาก

2.3.2 บูรณภาพ (Integrity)

บูรณภาพ หมายถึง การที่ทรัพยากรในระบบคอมพิวเตอร์สามารถถูกเปลี่ยนแปลงแก้ไขได้โดยผู้ที่มีสิทธิ์เท่านั้น ซึ่งทำให้ทรัพยากรนั้นมีความเชื่อถือได้นั้นเอง จุดมุ่งหมายข้อนี้แตกต่างจากการรักษาความลับ เพราะว่าข้อมูลบางประเภทไม่จำเป็นต้องเก็บไว้เป็นความลับ เนื่องจากเราสามารถประกาศให้ผู้อื่นทราบได้ เช่น ข้อมูลข่าวสารทางราชการซึ่งมีการประกาศทางเว็ปไซต์ต่างๆ สิ่งที่เราต้องการคือ ไม่ควรมีผู้อื่นเข้ามาดัดแปลงข้อความในเวปไซต์นี้ ซึ่งอาจให้ผู้อ่านสามารถเกิด ความเข้าใจผิดได้ หลักการที่ใช้ในการทำบูรณภาพคือ ข่าวสารย่อย (Message Digest) โดยเทคนิค อย่างหนึ่งของข่าวสารย่อยคือ ฟังก์ชันแฮช (Hash function)

2.3.3 การพิสูจน์ตัวจริง (Authentication)

การพิสูจน์ตัวจริง หมายถึง การพิสูจน์ว่าบุคคลที่ส่งข้อความหรือใช้ทรัพยากรคอมพิวเตอร์นั้น คือ บุคคลนั้นจริงๆ ไม่ใช่ผู้อื่นมาแปลกปลอม ตัวอย่างการพิสูจน์ตัวจริงที่เราพบเห็นในชีวิตประจำวัน คือ การใช้บัตรประชาชนหรือใบขับขี่ในการแสดงตัวตนว่า เป็นตนเอง ส่วนในระบบคอมพิวเตอร์นั้น เทคนิคการพิสูจน์ตัวจริงที่ใช้กันอย่างแพร่หลาย คือ การกำหนดชื่อผู้ใช้ (Login name) และรหัสผ่าน (Password) ของผู้ใช้แต่ละคน ผู้ใช้ต้องป้อนชื่อผู้ใช้และรหัสผ่านให้ ถูกต้องสอดคล้องตรงกัน จึงจะสามารถเข้าใช้คอมพิวเตอร์นั้นได้ นอกจากนี้ เทคนิคการพิสูจน์ตัวจริง ในคอมพิวเตอร์ที่กำลังได้รับความนิยมมากขึ้นเป็นลำดับ คือ การใช้ชีวมาตร (Biometric) ซึ่งหมายถึง การพิสูจน์ตัวจริง โดยพิจารณาจากอวัยวะของร่างกายมนุษย์ เช่น ลายนิ้วมือ และดวงตา เป็นต้น เนื่อง จากเทคโนโลยีด้านชีวมาตรมีราคาถูกลงและมีการใช้งานที่ง่ายขึ้น ดังนั้น เราจะเห็นอุปกรณ์ชีวมาตร ในชีวิตประจำวันมากขึ้นเรื่อยๆ เช่น โทรศัพท์มือถือ กุญแจสำนักงาน การเช็คการเข้าออกงาน และคอมพิวเตอร์โน้ตบุ๊ก เป็นต้น

2.3.4 การไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation)

การไม่สามารถปฏิเสธความรับผิดชอบ หมายถึง การที่ผู้ส่งหรือผู้รับข้อความไม่สามารถปฏิเสธได้ว่า ตนเองไม่ได้ส่งหรือรับข้อความนั้น ปัจจุบันเรื่องนี้กำลังได้รับความสนใจเป็นอย่างยิ่ง ในระบบอินเทอร์เน็ต เนื่องจากการทำธุรกิจทางอินเทอร์เน็ตกำลังได้รับความนิยมเพิ่มขึ้นเรื่อยๆ เช่น การสั่งซื้อสินค้าทางเว็ปไซต์ต่างๆ การโอนเงินหรือจัดการยอดบัญชีธนาคารทางอินเทอร์เน็ต เป็นต้น

ดังนั้น เวลาที่มีการโอนเงินหรือส่งข้อมูลการเงินให้กัน จึงต้องแน่ใจว่าอีกฝ่ายหนึ่งต้องรับผิดชอบในการกระทำของตนเอง โดยที่ไม่สามารถบิดพลิ้วหรือปฏิเสธการกระทำของตนเองได้ วิธีการที่ใช้ให้ ได้ตามจุดมุ่งหมายข้อนี้คือ การใช้ลายมือชื่อดิจิทัล (Digital signature)

2.3.5 สภาพพร้อมใช้งาน (Availability)

สภาพพร้อมใช้งาน หมายถึง การที่บุคคลผู้มีสิทธิสามารถเข้าถึงทรัพยากรที่ต้องการได้ในเวลาที่ต้องการ เช่น แพทย์ใน โรงพยาบาล ควรสามารถเข้าถึงข้อมูลของคนไข้ที่ตนเองกำลังรักษา อยู่ได้ในเวลาที่ต้องการ มิเช่นนั้นอาจเกิดความเสียหายหรือเป็นอันตรายต่อคนไข้ได้ เนื่องจากได้ ข้อมูลไม่ทันการ ทำให้ไม่สามารถรักษาได้ทันท่วงทีถ้าระบบคอมพิวเตอร์ไม่สามารถบรรลุจุดมุ่ง หมายข้อนี้อาจเกิดผลกระทบหลายอย่าง เช่น ในช่วงเทศกาลสำคัญ ถ้าลูกค้าธนาคารไม่สามารถ ใช้บริการตู้เอทีเอ็มเพื่อถอนเงินได้ อาจทำให้ลูกค้าเกิดความไม่พอใจ และหันไปใช้บริการของ ธนาคารคู่แข่งได้ ทำให้เกิดความเสียหายต่อธุรกิจ

2.4 เอกสารกูเกิ้ล (Google Docs) [8]

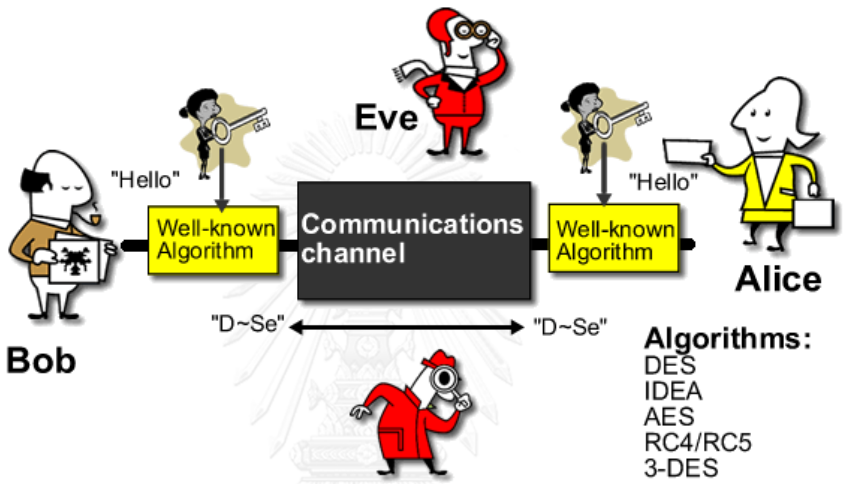
เอกสารกูเกิ้ล เป็นโปรแกรมประยุกต์บนเว็บฟรี ซึ่งสามารถสร้างเอกสาร แก้ไข และจัดเก็บแบบ ออนไลน์ สามารถเข้าถึงไฟล์เอกสารได้จากคอมพิวเตอร์ทุกครั้งที่เชื่อมต่อกับ อินเตอร์เน็ตและ Web browser ผู้ใช้เอกสารกูเกิ้ล สามารถนำเข้า สร้าง แก้ไข และปรับปรุงเอกสาร ฟอนต์และรูปแบบไฟล์ต่างๆ รวมข้อความเข้ากับสูตร excel ตาราง และภาพ เอกสารกูเกิ้ล ซึ่งสอด คล้องกับซอฟต์แวร์และ word processor ส่วนใหญ่ งานนี้สามารถเผยแพร่เป็นเว็บเพจหรือเพจ พร้อมพิมพ์ ผู้ใช้สามารถแบ่งปันไฟล์ให้กับผู้ใช้งานร่วม เพื่อการแก้ไขไฟล์ร่วมกันเป็นลักษณะ Real-time ได้ ดังนั้นเอกสารกูเกิ้ลมีประโยชน์อย่างยิ่ง และเป็นตัวเลือกใหม่ที่สำหรับผู้ที่ชื่นชอบหรือผู้ที่ ต้องใช้ในการทำงานเอกสารต่างๆ เป็นอย่างดี

2.5 ภาพรวมวิทยาการรหัสลับ [7]

2.5.1 วิทยาการรหัสลับชนิดกุญแจลับ

วิทยาการรหัสลับชนิดกุญแจลับมีหลักการทำงานดังนี้คือ สมมติให้อาลิซ (sender) มีความต้องการจะส่งข้อความบางอย่างไปให้บ๊อบ (receiver) ผ่านระบบเครือข่ายอินเทอร์เน็ต ขั้นแรก อาลิซจะต้องนำข้อความต้นฉบับ (Message) ที่ต้องการส่งให้บ๊อบไปผ่านการเข้ารหัสลับก่อนที่จะส่ง เข้าสู่ระบบเครือข่ายอินเทอร์เน็ตโดยใช้กุญแจลับในการเข้ารหัสซึ่งทั้งคู่ได้ตกลงกันไว้ล่วงหน้า และ ผลที่ได้จากการเข้ารหัสลับคือ ข้อความไซเฟอร์ (Cipher text) ที่มีรูปลักษณ์ซึ่งต่างไปจากข้อความ ต้นฉบับโดยสิ้นเชิง ดูรูปที่ 2.5.1 ประกอบ ฉะนั้นถึงแม้ว่าอีฟ (intruder) จะสามารถดักฟังและ ทราบข้อความ

ไซเฟอร์ที่ส่งผ่านจากอาลิซไปยังบ๊อบได้ครบทั้งหมด ก็ไม่ก่อให้เกิดประโยชน์อันใด เพราะอีฟไม่อาจคาดเดาหรือทราบได้ว่าข้อความต้นฉบับคืออะไร และเมื่อข้อความไซเฟอร์ถึงมือของ บ๊อบ บ๊อบจะใช้กุญแจดอกเดียวกับอาลิซที่ใช้ในการเข้ารหัสเพื่อถอดข้อความไซเฟอร์ให้กลับเป็น ข้อความต้นฉบับอีกครั้ง รูปแบบของการเข้ารหัสแบบนี้เรียกว่า วิทยาการรหัสลับชนิดกุญแจลับ (Secret key cryptography) หรือวิทยาการรหัสลับแบบสมมาตร (Symmetric cryptography)



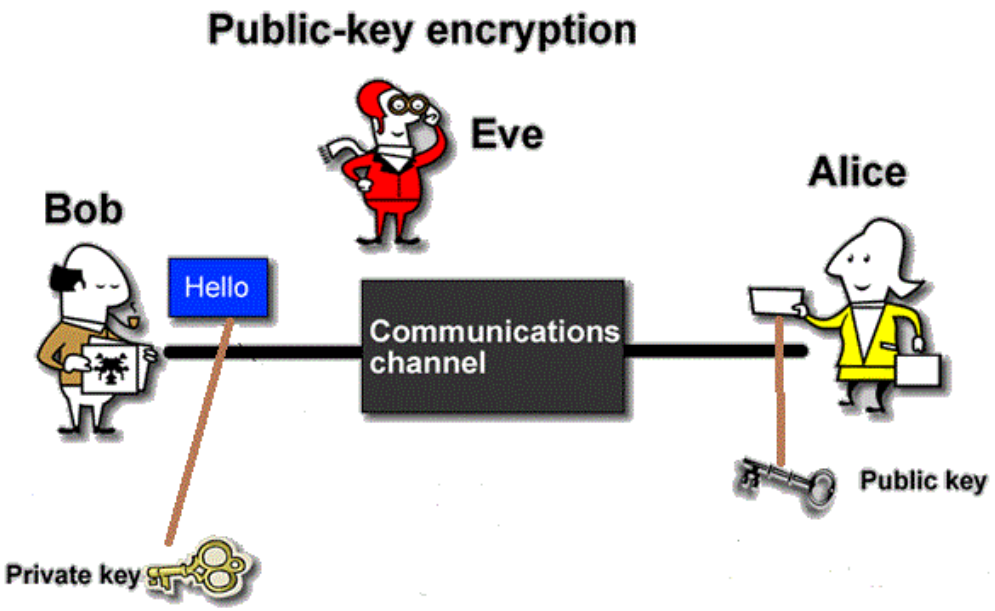
รูปที่ 2.5.1 โครงสร้างพื้นฐานของระบบการเข้ารหัสลับชนิดกุญแจลับร่วมกัน [9]

จากการอธิบายมาเมื่อพิจารณาในหลักการแล้วจะเห็นว่าตราบใดที่อีฟไม่ทราบค่ากุญแจลับที่บ๊อบและอาลิซใช้ร่วมกัน การส่งผ่านข้อความระหว่างบุคคลทั้งสองก็จะมีความปลอดภัย และในทางปฏิบัติหากกรรมวิธีการเข้ารหัสลับที่เลือกใช้มีขีดความสามารถสูง การเข้ารหัสลับประเภทนี้จัดว่ามีประสิทธิภาพและให้ความปลอดภัยในระดับที่น่าพอใจ ตัวอย่างของวิธีการเข้ารหัสลับชนิดนี้ที่สำคัญและใช้งานอย่างแพร่หลายเช่น DES (Data Encryption Standard) อย่างไรก็ตาม ข้อจำกัดของวิธีการแบบนี้อยู่ที่ขั้นตอนการตกลงกันระหว่างบ๊อบกับอาลิซถึงกุญแจลับที่จะใช้ร่วมกัน ในกรณีที่ทั้งคู่สามารถมาเจอกันซึ่งหน้าอย่างเป็นส่วนตัวหรือติดต่อกันผ่านระบบโทรศัพท์โดยรอดพ้นจากการดักฟังอีฟ การกำหนดค่าของกุญแจก็จะไม่เป็นปัญหาเลย อย่างไรก็ตาม สภาพการใช้งานในทางปฏิบัติที่จะต้องมีการกำหนดค่าของกุญแจลับให้กับผู้ใช้งานจำนวนมาก โดยผู้ใช้แต่ละรายเองก็จำเป็นต้องใช้กุญแจลับที่เปลี่ยนไปสำหรับการติดต่อกับผู้ใช้รายอื่นๆ ที่แตกต่างกันไปซึ่งหมายความว่า ผู้ใช้แต่ละรายจะต้องมีชุดกุญแจลับจำนวนมากที่ต้องคอยจัดการดูแล เห็นได้ชัดว่าขั้นตอนการตกลงค่าของ

กุญแจลับย่อมจะยุ่งยากซับซ้อนมาก ด้วยเหตุนี้ ปัญหาหลักของการใช้งานวิทยาการรหัสลับชนิดกุญแจลับจึงอยู่ที่การกำหนดกุญแจระหว่างบ๊อบและอาลิซโดยรอดพ้นจากอีฟนั้นจึงจัดว่าเป็นปัญหาหลักของวิธีการเข้ารหัสลับประเภทนี้

2.5.2 วิทยาการรหัสลับชนิดกุญแจสาธารณะ

วิทยาการรหัสลับชนิดกุญแจสาธารณะได้กำเนิดขึ้นในราวปี ค .ศ.1976 โดย Whitfield Diffie และ Martin Hellman ได้พัฒนาแนวคิดการเข้ารหัสรูปแบบใหม่ที่ต่างไปจากเดิมที่มีชื่อเรียกว่า วิทยาการรหัสลับชนิดกุญแจสาธารณะ (Public-key cryptography) เพื่อแก้ปัญหาระบบการจัดการกุญแจ (Key management) หลักการสำคัญของวิธีการใหม่นี้คือการเปลี่ยนจากการใช้กุญแจเพียงดอกเดียวสำหรับใช้ทั้งในขั้นตอนการเข้าและถอดรหัสมาเป็นการใช้กุญแจสองดอก กุญแจดอกแรกมีชื่อเรียกว่า กุญแจสาธารณะ (public key) มีไว้สำหรับใช้ในการเข้ารหัสลับข้อความ ส่วนกุญแจดอกที่สองเรียกว่า กุญแจส่วนตัว (private key) มีไว้สำหรับใช้ในกระบวนการถอดรหัสลับข้อความไซเฟอร์ ถ้าพิจารณาโครงสร้างพื้นฐานของระบบการเข้ารหัสลับชนิดใช้ทั้งกุญแจสาธารณะและกุญแจลับในรูปที่ 2.5.2 ในรูปเป็นสถาณการณ์ที่อาลิซมีความประสงค์จะส่งข้อความไปให้แก่บ๊อบ ในขั้นตอนแรกบ๊อบจะให้กำเนิดกุญแจขึ้นมาจำนวนสองดอก ดอกแรกคือกุญแจสาธารณะซึ่งจะประกาศให้แก่อาลิซเพื่อใช้ในการเข้ารหัสลับข้อความ เนื่องจากบ๊อบจะประกาศและเปิดเผยค่าของกุญแจดอกนี้ไปสู่สาธารณะ ดังนั้น อีฟเองก็จะทราบค่ากุญแจดอกนี้ด้วยเช่นกัน เมื่ออาลิซได้ใช้กุญแจดอกนี้ในการเข้ารหัสข้อความต้นฉบับเพื่อส่งต่อให้บ๊อบ และเช่นเคยข้อความไซเฟอร์ที่ได้จากการเข้ารหัสลับข้อความลับอาจจะถูกดักฟังโดยอีฟ อย่างไรก็ตาม อีฟจะไม่สามารถดึงข้อความต้นฉบับจากข้อความไซเฟอร์ได้ เพราะการถอดรหัสลับเพื่อแปลงข้อความไซเฟอร์ให้กลับมาเป็นข้อความต้นฉบับจะต้องอาศัยกุญแจอีกดอกหนึ่งที่เรียกว่ากุญแจส่วนตัว ซึ่งมีเพียงบ๊อบเท่านั้นที่ทราบ และแน่นอนว่าบ๊อบเองย่อมจะเก็บกุญแจส่วนตัวไว้เป็นความลับไม่เปิดเผย นอกจากนี้ให้สังเกตด้วยว่าการที่อีฟทราบค่ากุญแจสาธารณะจะไม่ช่วยให้ตนทราบกุญแจส่วนตัวได้เลย จากที่กล่าวมาทั้งหมดจะเห็นได้ว่าการเข้ารหัสประเภทนี้มีข้อดีกว่าแบบแรกคือตรงที่บ๊อบสามารถติดต่อกับอาลิซได้อย่างเป็นส่วนตัวโดยไม่ต้องมาพบเจอกันเลย กล่าวคือ ทั้งคู่ไม่จำเป็นต้องตกลงค่าของกุญแจลับที่ต้องใช้ร่วมกันก่อนการสื่อสารอีกต่อไป



รูปที่ 2.5.2 โครงสร้างพื้นฐานของระบบการเข้ารหัสลับชนิดใช้ทั้งกุญแจสาธารณะ [10]

อย่างไรก็ตาม ถ้าอีฟสามารถเข้ามาแทรกแซงการติดต่อสื่อสารระหว่างบ๊อบและอาลิซได้ อีฟอาจจะป้อนกุญแจสาธารณะของเธอให้แก่อาลิซแทน โดยที่ทางอาลิซเข้าใจว่าเป็นกุญแจสาธารณะของบ๊อบ ในกรณีเช่นนี้ข้อความต้นฉบับของอาลิซที่ผ่านการเข้ารหัสลับแล้วจะถูกถอดรหัสได้โดยอีฟด้วยกุญแจส่วนตัวของเธอเอง ดังนั้น การเข้ารหัสลับประเภทนี้ที่ใช้กุญแจสองดอกก็มีปัญหาของมันเองที่ต่างไปจากการเข้ารหัสแบบใช้กุญแจดอกเดียว นอกจากนี้ ในการสร้างกุญแจสาธารณะและกุญแจส่วนตัวขึ้นมาแต่ละคู่นั้น ค่าของกุญแจทั้งสองย่อมจะต้องเกี่ยวข้องและมีความสัมพันธ์กันในเชิงคณิตศาสตร์ ดังนั้น โดยหลักการแล้ว เป็นไปได้ที่อีฟน่าจะสามารถโจมตีระบบได้ โดยการค้นหาหรือคาดเดาค่าของกุญแจส่วนตัวจากค่าของกุญแจสาธารณะ ในทางปฏิบัติการป้องกันปัญหาที่ว่านี้สามารถทำได้โดยการสร้างความสัมพันธ์ทางคณิตศาสตร์ที่ซับซ้อนให้คำนวนยากที่สุดเท่าที่จะเป็นไปได้ ยกตัวอย่างเช่น ในการหาค่าของกุญแจส่วนตัวจากค่าของกุญแจสาธารณะ อีฟจะต้องแยกตัวประกอบตัวเลขจำนวนเต็มขนาดใหญ่มาก ซึ่งเราทราบว่าเป็นปัญหาที่ยากและมีความซับซ้อนสูงมาก แนวคิดนี้ได้มีการนำมาพัฒนาขึ้นเป็นระบบวิทยาการรหัสลับชนิดกุญแจสาธารณะรูปแบบหนึ่งที่ได้รับการยอมรับอย่างกว้างขวางในชื่อ RSA public-key cryptography

2.6 กูเกิ้ลไดรฟ์ (Google drive) [11]

กูเกิ้ลไดรฟ์ เป็นบริการจากกูเกิ้ลที่ ทำให้เราสามารถนำไฟล์ต่างๆ ไปฝากไว้กับ กูเกิ้ลซึ่งทำให้เราสามารถใช้ไฟล์เหล่านั้นจากที่ ไหนก็ได้ ไม่เพียงแค่ฝากไฟล์ได้เท่านั้นคุณยังสามารถแบ่งปันไฟล์กับ

คนที่ต้องการ และสามารถแก้ไขร่วมกันได้จากอุปกรณ์ หลายประเภท เช่น อุปกรณ์มือถือ อุปกรณ์แท็ปเลต หรือคอมพิวเตอร์ สำหรับพื้นที่ ๆ กูเกิ้ลให้เราใช้บริการฟรีนั้นอยู่ที่ 5 GB และหากต้องการพื้นที่มากขึ้น ก็สามารถซื้อพื้นพี่จัดเก็บข้อมูลเพิ่มได้ ส่วนราคาก็ขึ้นอยู่กับขนาดของพื้นที่ การจะใช้งานกูเกิ้ลไดรฟ์ หรือบริการต่าง ๆ ของกูเกิ้ล นั้น เราจำเป็นจะต้องมีบัญชีอีเมล์กับทาง จีเมล์ (Gmail) ก่อนถึงจะใช้งานได้ หากจะใช้บัญชี อีเมล์ที่ไม่ใช่ของจีเมล์ ก็จะใช้งานได้ไม่ครบถ้วนสมบูรณ์เหมือนกับการใช้บัญชีอีเมล์ของจีเมล์

2.7 ClearDB [12]

ClearDB คือ SaaS Application ที่ให้บริการทางด้านการเก็บข้อมูลในรูปแบบฐานข้อมูล (Database) โดยให้บริการ SQL Server ในรูปแบบการประมวลผลแบบคลาวด์ (Cloud Computing) เรียกว่า DBaaS (Database as a Service) อย่าง ClearDB นี้ใช้งานง่าย ซึ่งการเริ่มต้นการใช้งานนั้นไม่ต้องติดต่อเจ้าหน้าขององค์กรเจ้าของผู้ให้บริการแต่อย่างใด เหมือนกับ SaaS Application อื่นๆ เช่น กูเกิ้ล (Google) หรือ ดรอปบ็อกส์ (Dropbox) เป็นต้น

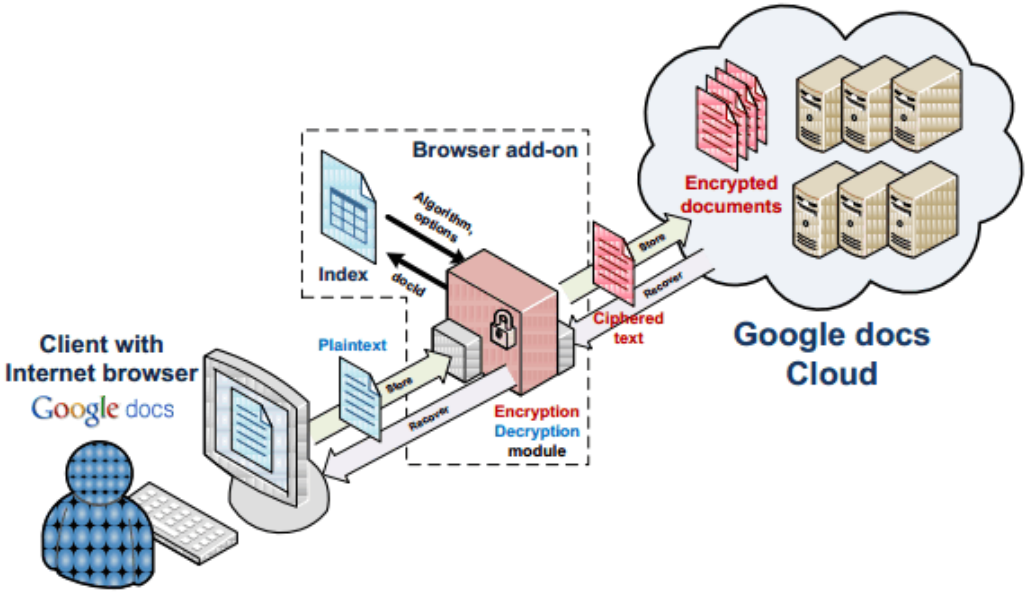
2.8 งานวิจัยที่เกี่ยวข้อง

แนวคิดการใช้วิทยาการรหัสลับฝั่งผู้ใช้งาน เพื่อความปลอดภัยในการใช้งาน SaaS Storage โดยเฉพาะ เอกสารกูเกิ้ลมี งานวิจัยที่เกี่ยวข้อง ดังนี้

2.8.1 Privacy for Google Docs: Implementing a Transparent Encryption Layer [13]

โดย Lilian Adkinson-Orellana, Daniel A. Rodríguez-Silva, Felipe Gil-Castiñeira และ Juan C. Burguillo-Rial, 2010

งานวิจัยฉบับนี้ได้นำเสนอ แนวคิดการใช้วิทยาการรหัสลับเพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล ด้วยการพัฒนา Firefox Extension (add-on) หรือโปรแกรมเสริม ที่สามารถนำวิทยาการรหัสลับเพื่อเข้ารหัส และถอดรหัสเอกสารกูเกิ้ลได้ ซึ่ง Firefox Extension นี้สร้างด้วย XUL และ Java script จึงทำให้สามารถติดตั้ง add-on นี้ได้ทุกระบบปฏิบัติการ ซึ่งกระบวนการทำงานจะเริ่มต้นจากการเปิดใช้งาน add-on หลังจากนั้นจะเริ่มมีการติดต่อสื่อสารและรับส่งข้อมูลไปยัง Google Docs server ด้วย API ซึ่งจะส่งการร้องขอ AJAX เพื่อการระบุตัวตนของผู้ใช้งาน และได้รับเอกสารกูเกิ้ลที่ผู้ใช้งานเป็นเจ้าของ หลังจากนั้นเมื่อผู้ใช้งานมีการแก้ไขเอกสาร add-on ก็จะมีการเข้ารหัสลับก่อนที่จะมีการบันทึกข้อมูลในเอกสารเหล่านั้นไปยัง Google Docs server และเมื่อผู้ใช้งานอ่านเอกสาร add-on ก็จะมีการถอดรหัสลับเพื่อให้ผู้ใช้งานสามารถอ่านเนื้อหาของเอกสารได้



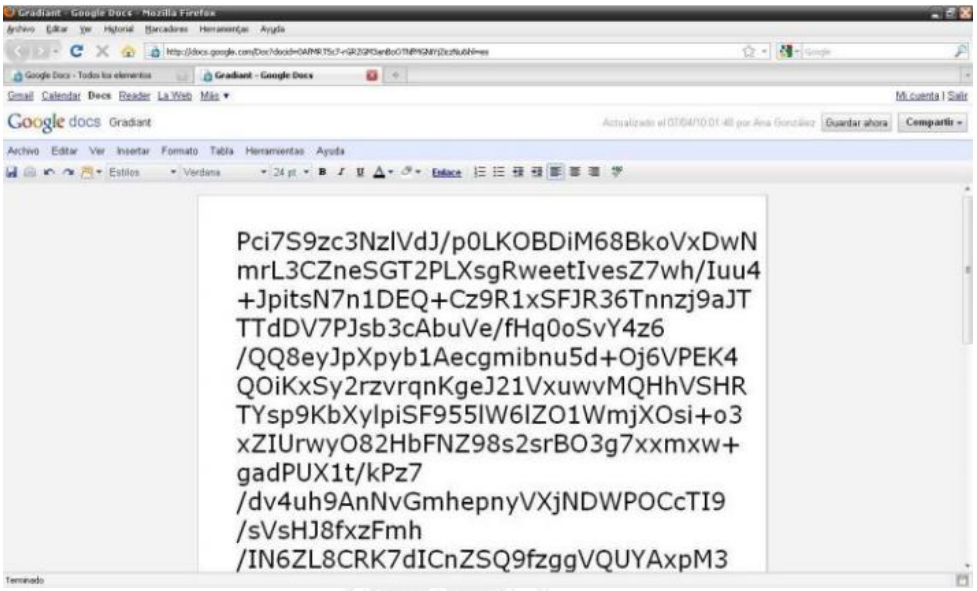
รูปที่ 2.8.1

งานวิจัยฉบับนี้ได้มีการนำวิทยาการรหัสลับแบบสมมาตร(Symmetric Key Algorithm) 7 อัลกอริทึม อันได้แก่ AES, DES, Triple DES, Blowfish, RC4, TEA และ xxTEA ซึ่งเป็นผลการทดลองจากผลงานวิจัย มาให้ผู้ใช้งานเลือกใช้ตามประสิทธิภาพด้านความปลอดภัยในการใช้งานเอกสารกูเกิ้ลที่ต่างกัน ซึ่งมีดังต่อไปนี้

	Name	Block size	Key size	Security	Speed	Speed depends on key size?
AES	Advanced Encryption Standard	128 bits	128, 192, 256 bits	Secure	Fast	Yes
DES	Data Encryption Standard	64 bits	56 bits	Insecure	Slow	-
Triple DES	Triple Data Encryption Algorithm	64 bits	56-168 bits	Moderately secure	Very Slow	No
Blowfish	-	64 bits	32-448 bits	Moderately secure	Fast	No
RC4	Rivest Cipher 4	64 bits	8-2048 bits	Insecure	Very fast	No
TEA	Tiny Encryption Algorithm	64 bits	128 bits	Insecure	Fast	No
xxTEA	Corrected Block TEA	arbitrary, (min 64 bits)	128 bits	Moderately secure	Fast	No

รูปที่ 2.8.2

การนำวิทยาการรหัสลับมาใช้เพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ลนั้น อัลกอริทึม AES มีประสิทธิภาพดี และเหมาะสมที่สุดในการนำมาใช้เข้าและถอดรหัสลับเพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล ซึ่งวัดประสิทธิภาพที่ความเร็ว (เวลาที่ใช้) ในการเข้าและถอดรหัสลับ และถ้าผู้ใช้งานได้มีการปิดadd-on ก็จะทำให้ไม่สามารถอ่านข้อความในเอกสารนั้นได้ตามรูปดังต่อไปนี้



รูปที่ 2.8.3

ปัญหาของงานวิจัยฉบับนี้ ยังขาดขั้นตอนสำคัญบางอย่าง นั้นก็คือ กระบวนการการแจกจ่ายกุญแจ(Key Distribution) ในกรณีที่มีการแชร์เอกสารให้กับเพื่อนเพื่อแก้ไขข้อมูลไปพร้อมๆ กัน

2.8.2 SHARING SECURE DOCUMENTS IN THE CLOUD: A Secure Layer for Google Docs [14]

โดย Lilian Adkinson-Orellana, Daniel A. Rodríguez-Silva, Felipe Gil-Castiñeira และ Francisco J. González-Castaño, 2011

งานวิจัยฉบับนี้ได้นำเสนอ แนวคิดการใช้วิทยาการรหัสลับเพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล ด้วยการพัฒนาเพิ่มเติมจากงานที่แล้วคือ Privacy for Google Docs: Implementing a Transparent Encryption Layer ซึ่งงานวิจัยฉบับนี้ได้มีการพัฒนาเพิ่มเติมในแนวคิดการใช้วิทยาการรหัสลับเพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ลในส่วนของการแบ่งปัน (Share) ไฟล์หรือโฟลเดอร์ ให้บุคคลอื่น แต่ยังคงไม่สนับสนุนคุณสมบัติของการใช้งานเอกสารกูเกิ้ลในด้านการใช้งานใน

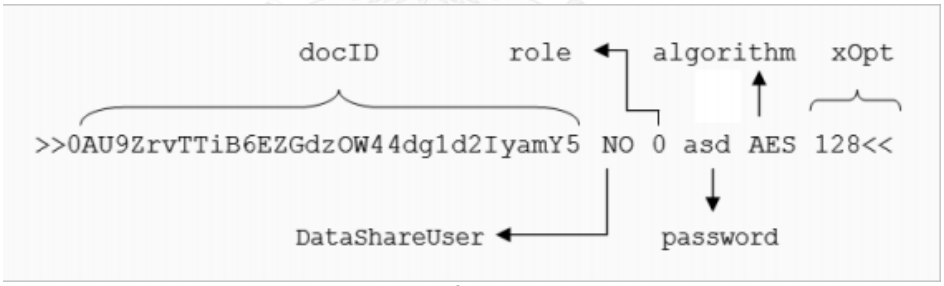
รูปแบบการแก้ไขร่วมกันแบบเรียลไทม์ (real time collaborative edition of online documents) ซึ่งได้ศึกษา Google Docs API ในการแบ่งปันไฟล์ไปยังบุคคลอื่น นั่นก็คือหลักการAccess Control List (ACL) Feed ซึ่งหลักการทำงานที่สามารถแสดงได้ว่าผู้ใช้งานร่วมคนใดสามารถที่จะเข้าถึงเอกสาร หรือโฟลเดอร์ของการใช้งานเอกสารกูเกิ้ลได้บ้าง ซึ่งผู้ใช้งานร่วมแต่ละรายมีสิทธิ์ (Role) ต่างกันดังต่อไปนี้

2.8.2.1 Owner ซึ่งเจ้าของไฟล์นั้นสามารถที่จะแก้ไขสิทธิ์ ACL feed เช่น ลบ หรือ แก้ไขเอกสารกูเกิ้ลได้

2.8.2.2 Writer สิทธิ์นี้ผู้ใช้งานร่วมสามารถแก้ไขข้อมูลในเอกสารกูเกิ้ลได้ แต่ไม่สามารถลบเอกสารกูเกิ้ลได้

2.8.2.3 Reader สิทธิ์นี้ผู้ใช้งานสามารถอ่านเอกสารกูเกิ้ลได้อย่างเดียว

2.8.2.4 และงานวิจัยฉบับนี้ก็ยังได้นำเสนอหลักการใช้วิทยาการรหัสลับเพื่อความปลอดภัยในการแบ่งปันการใช้งานเอกสารกูเกิ้ลให้แก่ผู้ใช้งานร่วม แต่ยังขาดคุณสมบัติของการใช้งานเอกสารกูเกิ้ลในด้านการใช้งานในรูปแบบการแก้ไขร่วมกันแบบเรียลไทม์ หมายถึง หลังจากที่เจ้าของไฟล์ได้มีการดำเนินการกระทำการแบ่งปันเรียบร้อยแล้ว ไฟล์ดังกล่าวที่ถูกส่งไปให้แก่ผู้ใช้งานร่วมจะกลายเป็นไฟล์ใหม่ทันที ถ้าไฟล์นั้นผ่านกระบวนการเข้ารหัส ซึ่งเอกสารกูเกิ้ลแต่ไฟล์จะมีเลขดัชนีเอกสาร (Index Document) ซึ่งโครงสร้างของเลขดัชนีเอกสารจะถูกกำกับไว้ดังรูป



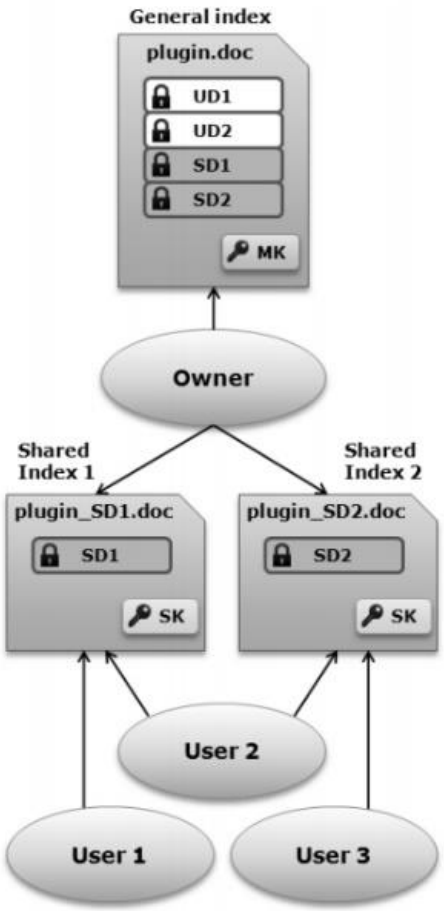
รูปที่ 2.8.4

เอกสารกูเกิ้ลแต่ละไฟล์นั้นจะถูกเข้ารหัสด้วย Master Password (Master Key) จะถูกเรียกว่า General Index และเมื่อต้องการแบ่งปันให้กับผู้ใช้งานร่วม เอกสารกูเกิ้ลนั้นก็จะสร้างเพิ่มขึ้นมาอีก 1 ไฟล์ ซึ่งไฟล์ที่ถูกสร้างใหม่จะเรียกว่า Shared Index ซึ่งจะถูกเข้ารหัสด้วย Shared Password (Shared Key) ตัวอย่างเช่น ไฟล์ชื่อว่า plugin.doc ซึ่งเป็น General Index และเมื่อต้องการที่จะแบ่งปันให้กับผู้ใช้งานร่วมก็จะสร้างไฟล์อีก 1 ไฟล์ชื่อว่า plugin_<docID>.doc ซึ่งเป็น Shared Index และ docID ใน plugin_<docID>.doc จะอ้างอิงถึงเลข DocID ของไฟล์ plugin.doc และ

เมื่อเจ้าของไฟล์ต้องการที่แบ่งปันไฟลในการใช้งานเอกสารกูเกิ้ลให้แก่ผู้ใช้งานร่วมเป็นครั้งแรก ก็จะมี popup แสดงขึ้นมาเพื่อให้เจ้าของไฟล์ได้ใส่รหัสใหม่ซึ่งหมายถึงกุญแจที่ต้องการเข้ารหัส Master Key ซึ่งอยู่ในข้อมูลดัชนี (Information Index) ในไฟล์ใหม่ เพื่อเข้ารหัสข้อมูลดัชนี ในไฟล์ใหม่ที่ถูกสร้างขึ้นด้วยอัลกอริทึม AES ขนาดกุญแจ 128 bit-key ซึ่งในตัวอย่างก็คือ ไฟล์plugin_<docID>.doc เมื่อเจ้าของไฟล์แบ่งปันไฟล์ไปยังผู้ใช้ร่วมแล้ว เจ้าของไฟล์จำเป็นที่จะต้องกำหนดช่องทางที่ปลอดภัยในการส่ง Master Key ไปยังผู้ใช้งานร่วมด้วย

จากการอธิบายข้างต้นในการแบ่งปันงานเอกสารกูลเกิ้ลไปยังผู้ใช้งานร่วมนั้น ไฟล์จะมีการสร้างไฟล์สำหรับการแบ่งปัน ซึ่งไฟล์เดิมจะถูกเรียกว่า General Index และไฟล์ที่ถูกสร้างใหม่จะถูกเรียกว่า Shared Index ซึ่งไฟล์ทั้งสองจะมีการ synchronize information index ตลอดเวลา shared index จะถูกส่งไปให้ผู้ใช้งานร่วม ซึ่งใน shared index นี้เองจะเก็บกุญแจลับที่ไว้เข้ารหัสข้อมูลในเอกสารกูเกิ้ลด้วย

การนำวิทยาการรหัสลับมาใช้เพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล และนำมาประยุกต์ใช้สำหรับการแบ่งปันให้แก่ผู้ใช้งานร่วม มีผลการทดลอง คือ เจ้าของไฟล์มีไฟล์ที่ต้องการแบ่งปันในการใช้งานเอกสารกูเกิ้ลเป็นจำนวน 2 ไฟล์ และต้องการแบ่งปันให้ผู้ใช้งานร่วมจำนวน 3 คน หลังจากนั้นไฟล์ที่ต้องการแบ่งปันก็จะสร้าง ไฟล์ (Hidden File) จำนวน 2 ไฟล์ ซึ่งจะถูกแบ่งปันให้กับผู้ใช้งานจำนวน 3 คนด้วยสิทธิ์ต่างกันดังนี้ user 1 สามารถใช้งานร่วมเอกสารกูเกิ้ลไฟล์ที่มีชื่อว่า plugin_SD1.doc user 2 สามารถใช้งานร่วมเอกสารกูเกิ้ลไฟล์ที่มีชื่อว่า plugin_SD1.doc และ plugin_SD2.doc และ user 3 สามารถใช้งานร่วมเอกสารกูเกิ้ลไฟล์ที่มีชื่อว่า plugin_SD2.doc อย่างเดียว ดังนั้นเจ้าของไฟล์จะต้องสร้าง Share Key จำนวน 2 key เพื่อส่งในช่องทางที่มีความปลอดภัยให้กับทั้ง 3 คนที่เกี่ยวข้อง หลังจากนั้นผู้ใช้งานร่วมทั้ง 3 คนก็สามารถใช้ Share Key ที่ได้รับจากเจ้าของไฟล์เพื่อถอดรหัสลับ plugin_SD1.doc และ plugin_SD2.doc เพื่อให้ได้ Master Key และสามารถนำ Master Key ไปถอดรหัสลับไฟล์ที่เจ้าของไฟล์ที่ได้แบ่งปันได้



รูปที่ 2.8.5

ปัญหาของงานวิจัยฉบับนี้ มีความปลอดภัยยังไม่เพียงพอในแง่ของผู้ดูแลระบบของทางกูเกิ้ลเอง เนื่องจากยังเก็บMaster Key อยู่ใน Google Drive ซึ่งไม่ได้มีการเข้ารหัสตัว Master Key ในการจัดเก็บเอกสารกูเกิ้ลใน Google Drive เพียงแค่เข้ารหัสลับ Master Key ในเวลาที่ต้องการแบ่งปันให้ผู้ใช้งานร่วมเท่านั้น เราสามารถสันนิฐานได้ว่าทางผู้ดูแลระบบของกูเกิ้ลสามารถที่จะเอา Master Key เพื่อถอดรหัสเอกสารกูเกิ้ล และสามารถอ่านได้

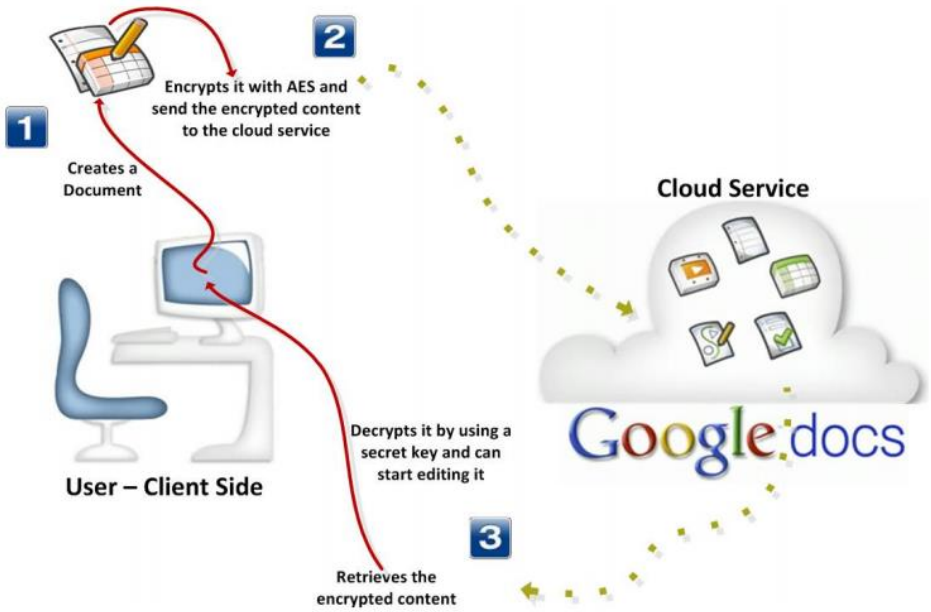
2.8.3 SecGOD Google Docs: Now I Feel Safer! [3]

โดย Antonis Michalas และ Menelaos Bakopoulos, 2012

งานวิจัยฉบับนี้ได้นำเสนอ แนวคิดการใช้วิทยาการรหัสลับเพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล ด้วยการพัฒนา Browser Extension ที่สามารถนำวิทยาการรหัสลับเพื่อเข้ารหัสลับ และถอดรหัสลับเอกสารกูเกิ้ลได้ ซึ่ง Browser Extension นี้สร้างด้วย Greasemonkey java-script ซึ่ง

การทำงานของ Browser Extension นี้จะใช้ลักษณะการเข้ารหัสลับเอกสารกูเกิ้ลแบบสมมาตร (Symmetric Key Encryption) และกระบวนการทำงานให้การใช้งานเอกสารกูเกิ้ลให้มีความปลอดภัยอยู่ที่เครื่องของผู้ใช้งานเอง ฉะนั้นผู้ใช้งานไม่ต้องกังวลถึงกระบวนการที่สนับสนุนความปลอดภัยในการใช้งานเอกสารกูเกิ้ลที่นำเสนอจากผู้ให้บริการ Google Provider แต่อย่างใด

กระบวนการที่นำเสนอจากนักวิจัยคือการพัฒนา Browser Extension ด้วย Greasemonkey java-script และได้นำอัลกอริทึมการเข้ารหัสลับแบบกุญแจดอกเดียวหรือการเข้ารหัสลับแบบสมมาตร คือ AES (Advanced Encryption Standard) แบบชนิดกุญแจขนาด 128, 192 และ 256 บิต ซึ่งมีการทำงานดังต่อไปนี้



รูปที่ 2.8.6

2.8.3.1 ผู้ใช้งานสร้างไฟล์เอกสารกูเกิ้ล

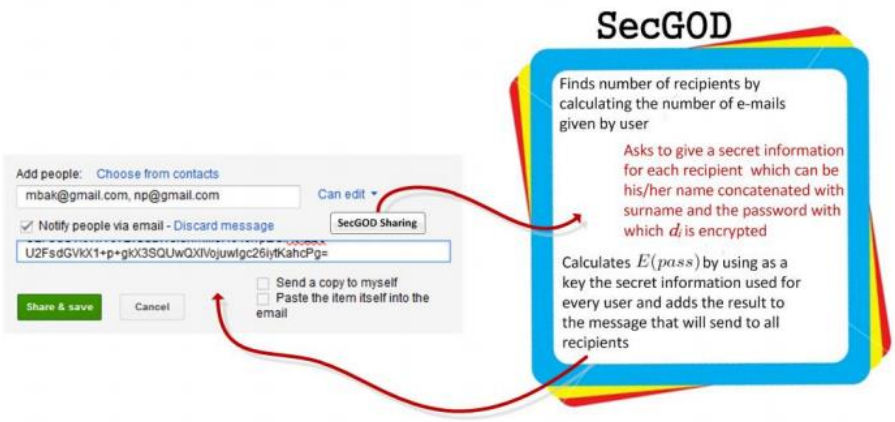
2.8.3.2 ผู้ใช้งานเลือกอัลกอริทึม AES ที่ต้องการเข้ารหัสข้อมูลเอกสารกูเกิ้ลด้วยขนาดกุญแจ คือ 128, 196 และ 256 บิต

2.8.3.3 ผู้ใช้งานใส่ค่ากุญแจ Master Key เพื่อใช้ในกระบวนการเข้ารหัสลับและถอดรหัสลับด้วยตัวเอง ตามที่ต้องการ

2.8.3.4 ไฟล์ข้อมูลในเอกสารกูเกิ้ลจะถูกเก็บใน Google Drive ในรูปแบบที่เข้ารหัสลับ (Cipher Text) หลังจากกดปุ่ม “Encrypt”

2.8.3.5 เมื่อผู้ใช้งานต้องการอ่านข้อมูลไฟล์เอกสารกูเกิ้ล ไฟล์ดังกล่าวก็จะเข้ากระบวนการถอดรหัสลับด้วยคุญแจค่าเดิม คือ Master Key ที่เคยใช้ในการเข้ารหัสลับ

2.8.3.6 ผู้ใช้งานสามารถอ่านและแก้ไขข้อมูลในไฟล์เอกสารกูเกิ้ลในรูปแบบที่ได้รับการถอดรหัสลับ (Plain Text) หลังจากการกดปุ่ม “Decrypt”



รูปที่ 2.8.7 SecGOD

2.8.3.7 ผู้ใช้งานที่เป็นเจ้าของไฟล์ต้องการแบ่งปันไฟล์ไปยังผู้ใช้งานร่วม หลังจากที่ได้กดปุ่ม “Share” แล้วจะปรากฏหน้าต่างเพื่อใส่ข้อมูลอีเมล์ (email) ของผู้ใช้งานร่วม และแสดงค่าของกุญแจ Shared Key ที่จะเอาไปทำกระบวนการเข้ารหัสลับกุญแจ Master Key

2.8.3.8 หลังจากนั้นระบบจะมีการนำเอาจำนวนอีเมล์ของผู้ใช้งานร่วมเพื่อปรากฏหน้าต่างเพื่อให้ใส่ข้อมูลเบื้องต้นของผู้ใช้งานหลังจากที่ได้กดปุ่ม “SecGOD Sharing” เช่น อีเมล์จำนวน 2 อีเมล์ก็จะปรากฏหน้าต่างมาให้เจ้าของไฟล์กรอกข้อมูลส่วนตัวของผู้ใช้งานร่วมจำนวน 2 หน้าต่าง

2.8.3.9 หลังจากที่เจ้าของไฟล์ได้ใส่ข้อมูลของผู้ใช้งานร่วมเรียบร้อยแล้ว ให้เลือกช่อง “Notify people via email” ให้กดปุ่ม “Share & save” ระบบจะนำเอาข้อมูลส่วนตัวของผู้ใช้งานร่วมที่ได้กรอกไว้ไปเข้ารหัสลับค่ากุญแจ Shared Key แล้วส่งผลจากการเข้ารหัสลับ Shared Key ให้กับผู้ใช้งานร่วมในช่องทางอีเมล์ต่อไป

2.8.3.10 ผู้ใช้งานร่วมได้รับค่ากุญแจ Shared Key ที่เข้ารหัสลับด้วยข้อมูลส่วนตัวของตนเอง หลังจากนั้นใช้ข้อมูลส่วนตัวของตนถอดรหัสลับ จะได้ค่าของกุญแจ Shared Key แล้วนำค่าของกุญแจ Shared Key มาเข้ากระบวนการถอดรหัสลับเพื่อได้ค่ากุญแจ Master Key

2.8.3.11 ผู้ใช้งานร่วมนำค่ากุญแจ Master Key มาเข้ากระบวนการถอดรหัสข้อมูลในไฟล์เอกสารกูเกิ้ล โดยจะมี popup ให้ใส่ค่าMKและสามารถที่จะอ่านและข้อมูลในไฟล์เอกสารกูเกิ้ลได้

- การนำวิทยาการรหัสลับมาใช้เพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล และนำมาประยุกต์ใช้สำหรับการแบ่งปันให้แก่ผู้ใช้งานร่วมนั้น ซึ่งผู้วิจัยได้การนำหลักการที่ได้จากการนำเสนอข้างต้นมาทำการทดลองการเข้าและถอดรหัสลับ ด้วยความแตกต่างของขนาดข้อมูลในไฟล์เอกสารกูเกิ้ลคือ จำนวน 799, 1437, 6945, 25980 และ 76526 ตัวอักษร และ ค่ากุญแจคือ 128, 192 และ 256 บิต นำมาหาค่ากุญแจที่มีประสิทธิภาพและเหมาะสมที่สุดในด้านความคุ้มค่า โดย มีผลการทดลองดังต่อไปนี้

- ข้อมูลไฟล์เอกสารกูเกิ้ลขนาดเล็ก จำนวน 799 ตัวอักษร

Cryptography Algorithm	Average Time (Encryption)	Average Time (Decryption)
AES 128	16ms	17ms
AES 192	19ms	18ms
AES 256	23ms	23ms

ตารางที่ 1 ผลการทดลองของข้อมูลไฟล์เอกสารกูเกิ้ลขนาดเล็ก จำนวน 799 ตัวอักษร

- ข้อมูลไฟล์เอกสารกูเกิ้ลขนาดใหญ่ จำนวน 76526 ตัวอักษร

Cryptography Algorithm	Average Time (Encryption)	Average Time (Decryption)
AES 128	143ms	156ms
AES 192	182ms	197ms
AES 256	201ms	213ms

ตารางที่ 2 ผลการทดลองของข้อมูลไฟล์เอกสารกูเกิ้ลขนาดใหญ่ จำนวน 76526 ตัวอักษร

ปัญหาของงานวิจัยฉบับนี้ ยังมีปัญหาอยู่ 2 ด้าน อันได้แก่

- ในเรื่องการสร้างค่ากุญแจลับ Master Key ที่จะนำมาเข้ากระบวนการเข้า และถอดรหัสลับข้อมูลในไฟล์เอกสารกูเกิ้ล เนื่องจากการสร้างค่ากุญแจลับ Master Key นั้นสร้างด้วยการคีย์ข้อมูลด้วยเจ้าของไฟล์ (Manual) เอง ซึ่งอาจจะไม่สะดวกหรือเหมาะสมในด้านการจัดการในกรณีที่เจ้าของไฟล์มีไฟล์เอกสารกูเกิ้ลเป็นจำนวนมาก ซึ่งถ้าเจ้าของไฟล์ต้องการที่จะใช้ค่ากุญแจรหัสลับของแต่ละไฟล์เอกสารกูเกิ้ลที่ต่างกันอาจจะทำให้เจ้าของไฟล์นั้นไม่สะดวกในการจำหรือจัดการค่ากุญแจดังกล่าว

- ในเรื่องของการแบ่งปันไฟล์เอกสารกูเกิ้ลไปยังผู้ใช้งานร่วม ค่ากุญแจลับ Shared Key ยังไม่เหมาะสมในด้านการจัดการอีกเช่นกันเนื่องจากเจ้าของไฟล์ยังต้องสร้างค่ากุญแจ (Passphrase) สำหรับเข้ารหัสลับตัว Shared Key ด้วยตัวเองอยู่(ข้อมูลส่วนตัวของผู้ใช้งานร่วม ถึงแม้ว่า กุญแจลับ Shared Key จะถูกสร้าง (Auto Generation) ด้วยระบบก็ตาม

บทที่ 3

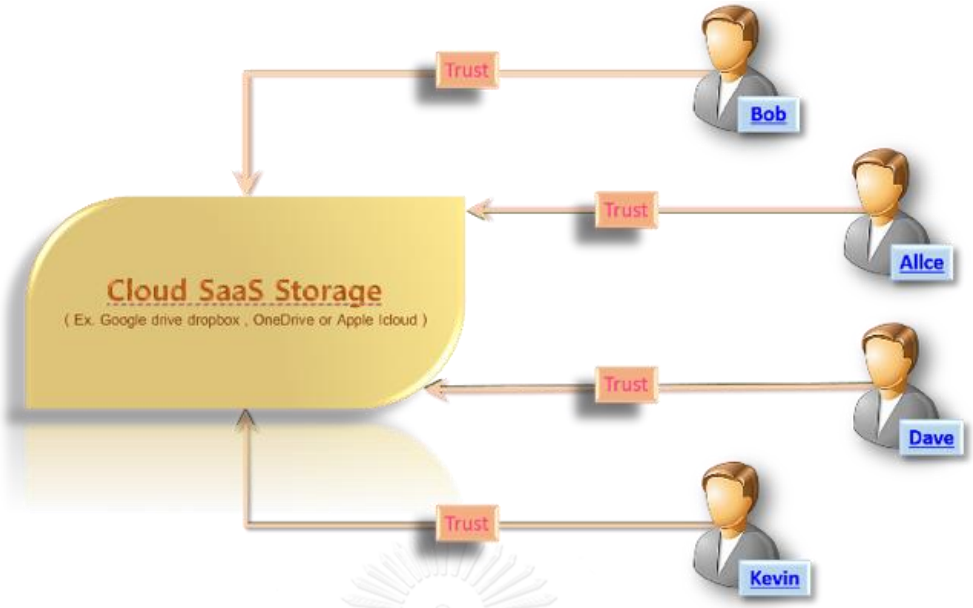
การรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ

การนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง ซึ่งถ้าเราเลือกใช้ผู้ให้บริการรายเดียวในการเก็บข้อมูลสำคัญทั้งหมด ถึงแม้รูปแบบที่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะถูกเข้ารหัสลับแบบไม่สามารถใช้งานได้นั้น แต่ข้อมูลอื่นๆเช่น ค่ากุญแจต่างๆ ที่เกี่ยวข้อง ก็อาจจะยังอยู่ในการดูแลของผู้ให้บริการ ดังนั้นบุคคลที่เกี่ยวข้องเช่น ผู้ดูแลระบบก็สามารถที่จะนำค่ากุญแจต่างๆที่เกี่ยวข้องเพื่อถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำข้อมูลที่ได้มา เอาไปใช้งานที่สามารถก่อให้เกิดอันตรายต่อผู้ใช้งานได้ ดังนั้นผู้วิจัยจึงได้นำเสนอกระบวนการหรือโมเดลใหม่ในการจัดการข้อมูลของผู้ใช้งาน ซึ่งมีใจความสำคัญ และภาพรวมของการนำเสนอแนวคิดและวิธีการดำเนินงาน ดังต่อไปนี้

3.1 รูปแบบการไว้ใจผู้ให้บริการในการใช้งาน SaaS Storage (SaaS Storage Provider Crypto Trusted Model – PCT Model)

SaaS Storage Provider Trusted Model ซึ่งเป็นหลักการหรือโมเดลใหม่ที่ต้องการนำเสนอหลักการวางใจและไว้ใจในการจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้บริการหรือผู้ใช้งานต่อผู้ให้บริการ โดยแบ่งแยกประเภทของความปลอดภัยของข้อมูลสำคัญหรือข้อมูลลับด้วยจำนวนของผู้ให้บริการ (Number of Cloud Provider) และสถานที่ ที่นำเสนอความปลอดภัยด้วยการเข้าและถอดรหัสข้อมูลสำคัญหรือข้อมูลลับ (Location of Crypto Mechanism) นั้น ผู้วิจัยขออณุญาตที่จะสรุปรูปแบบที่เกี่ยวกับหลักการ SaaS Storage Provider Crypto Trusted Model หรือ PCT Model ซึ่งมีดังต่อไปนี้

3.1.1 รูปแบบการไว้ใจผู้ให้บริการในการใช้งาน SaaS Storage ที่จัดเตรียมโดยผู้ให้บริการเพียงรายเดียว (Single Provider Server-side Cryptography – SPSC Model)



รูปที่ 3.1.1 Single Provider Server-side Cryptography Model

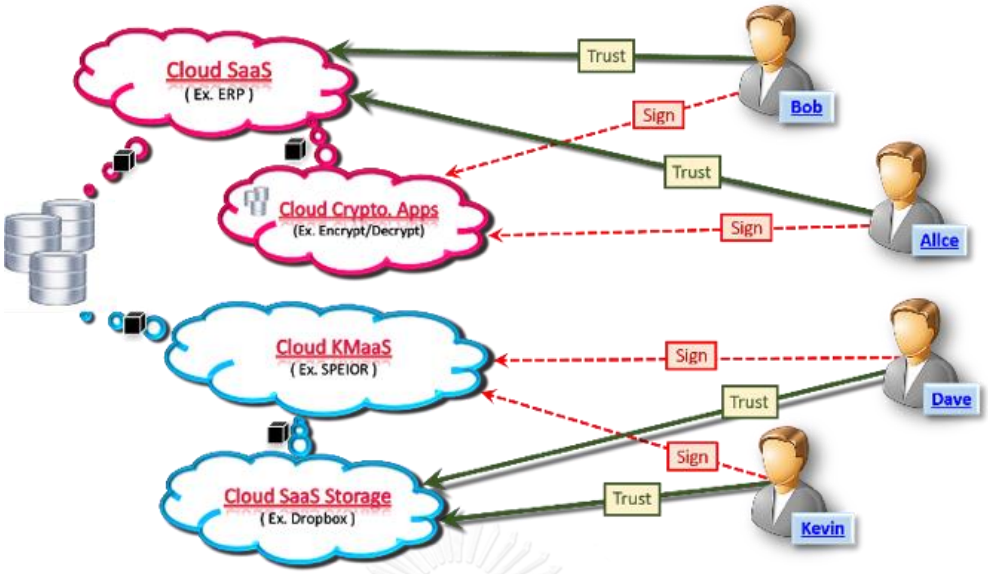
ปัจจุบันผู้ให้บริการด้าน SaaS Storage ส่วนใหญ่ยังคงนำเสนอหลักความปลอดภัยให้แก่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานด้วยหลักการหรือโมเดลนี้ ซึ่งอาจจะใช้ หรือไม่ใช้หลักการวิทยาการรหัสลับ หรือเลือกใช้วิธีอื่นๆ ที่สามารถปกป้องภัยคุกคาม หรืออันตรายต่อข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานได้ ซึ่งวิธีการของหลักการหรือโมเดลนี้เหมือนจะมีนโยบายเชิงบังคับให้ผู้ใช้งานจำเป็นจะต้องวางใจผู้ให้บริการอย่างปฏิเสธไม่ได้ถ้าผู้ใช้งานรายนั้นจำเป็นจะต้องใช้บริการของ SaaS Storage เนื่องจากข้อจำกัดด้านการนำเสนอความปลอดภัยของผู้ให้บริการเอง ซึ่งหลักการความปลอดภัยดังกล่าวอาจมิใช่การใช้วิทยาการรหัสลับซึ่งเป็นวิธีที่ปลอดภัยที่สุดสำหรับการปกปิดข้อมูลสำคัญหรือข้อมูล

จากตัวอย่างในภาพ ผู้ใช้งานทุกคนเช่น Bob, Alice, Dave และ Kevin จำเป็นต้องวางใจผู้ให้บริการหากต้องการใช้ SaaS Storage เช่น Google Drive, Dropbox หรือ OneDrive ดังนั้นพวกเขาเหล่านี้ไม่มีทางปฏิเสธการนำเสนอความปลอดภัยจากผู้ให้บริการได้

ข้อดี ผู้ใช้งานทั้งหมดสามารถใช้งาน SaaS Storage ด้วยวิธีที่ง่ายและรวดเร็ว

ข้อเสีย ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานอาจจะมีความเสี่ยงจากการละเมิดของผู้ให้บริการได้

3.1.2 รูปแบบการไว้ใจผู้ให้บริการในการใช้งาน SaaS Storage ที่จัดเตรียมโดยผู้ให้บริการหลายราย (Multiple Provider Server-side Cryptography – MPSC Model)



รูปที่ 3.1.2 Multiple Provider Server-side Cryptography Model

การนำเสนอการใช้วิทยาการรหัสลับที่ฝั่งผู้ให้บริการ และเลือกใช้และวางใจผู้ให้บริการ SaaS Storage หลายรายนั้น จะมี SaaS Provider อย่างน้อย 1 รายทำหน้าที่รักษาความปลอดภัยของข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานด้วยการเข้าและถอดรหัสก่อนที่จะมีการส่งข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานไปยัง SaaS Storage Provider รายอื่นในการจัดเก็บข้อมูลดังกล่าวในรูปแบบข้อมูลที่ได้รับการเข้ารหัสแล้ว และมีระบบการจัดการค่ากุญแจภายในฝั่งผู้ให้บริการที่เกี่ยวข้องโดยที่ผู้ใช้งานไม่ต้องสนใจหรือจัดการค่ากุญแจใดๆทั้งสิ้น

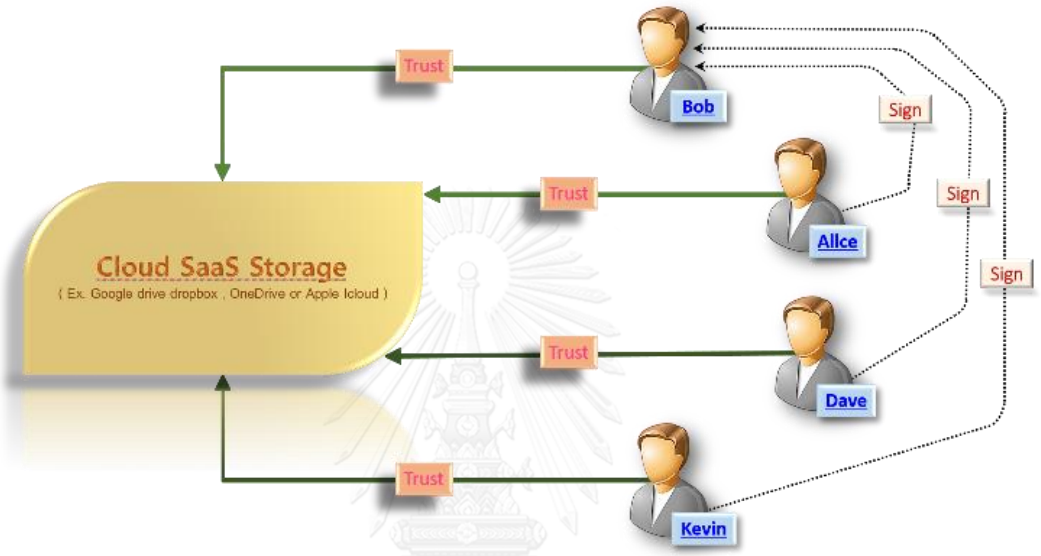
จากตัวอย่างในภาพ Bob และ Alice ใช้บริการ SaaS Storage คือ Dropbox ในการเก็บเอกสารกูเกิ้ล ซึ่ง Bob เลือกใช้หลักการวิทยาการรหัสลับฝั่งผู้ให้บริการหลายราย กล่าวคือเขาต้องการเก็บไฟล์ซึ่งมีข้อมูลสำคัญหรือข้อมูลลับ ใน เขาจะต้องใช้ SPEIOR (Cloud KMaaS) ด้วยทุกครั้งในการเข้าและถอดรหัสข้อมูลสำคัญหรือข้อมูลลับ เมื่อเขาได้แก้ไขข้อมูลในไฟล์ดังกล่าวเสร็จแล้ว เขาต้องการแบ่งปันหรือแชร์ไฟล์ซึ่งกันและกันในลักษณะการใช้งานร่วม SPEIOR ก็จะเป็นตัวจัดการค่ากุญแจที่เกี่ยวข้องในการใช้งานไฟล์ของทั้งคู่

ข้อดี ผู้ใช้งานทั้งหมดสามารถใช้งาน SaaS Storage ด้วยความปลอดภัยจากภัยคุกคามของผู้ให้บริการได้เนื่องจากผู้ให้บริการที่เกี่ยวข้องเท่านั้นที่มีสิทธิ์จัดการบริหารค่ากุญแจ เท่านั้น

ข้อเสีย -ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะต้องมีการเคลื่อนย้ายจากเครื่องตนเองไปยังผู้ให้บริการจำนวนหลายครั้ง อาจจะได้รับความเสี่ยงจากผู้ดักจับข้อมูลกลาง (Man-in-the-middle-attack) หรือจากสภาพแวดล้อมของผู้ให้บริการที่เกี่ยวข้องเกี่ยวกับความปลอดภัย (KMaaS

Environment) เอง กล่าวคือผู้ให้บริการสามารถที่จะทำการสำเนาข้อมูลสำคัญหรือของมูลลับของผู้ใช้งาน เช่น การล็อกกิ้ง (Logging) ก่อนที่จะมีเข้าเข้ารหัสข้อมูลดังกล่าว ก่อนที่จะส่งข้อมูลที่อยู่ในรูปแบบการเข้ารหัสไปยังผู้ให้บริการ SaaS Storage เพื่อจัดเก็บต่อไป

3.1.3 รูปแบบการไว้ใจผู้ให้บริการแค่รายเดียวในการใช้งาน SaaS Storage จัดเตรียมฝั่งผู้ใช้งาน (Single Provider Client-side Cryptography – SPCC Model)



รูปที่ 3.1.3 Single Provider Client-side Cryptography Model

งานวิจัยจำนวนหนึ่งมีการนำเสนอการใช้วิทยาการรหัสลับที่ฝั่งของผู้ใช้งาน และเลือกใช้และวางใจผู้ให้บริการ SaaS Storage เพียงรายเดียว และมีระบบการจัดการค่ากุญแจที่ไม่ดีพอ เช่น มีการสร้างค่ากุญแจด้วยผู้ใช้งานเอง (Manual) และการกระจายค่ากุญแจ (Key Distribute) ไปยังผู้ใช้งานร่วมที่ยังไม่ดีพอเช่น การโทรหาผู้ใช้งานร่วมเพื่อบอกค่ากุญแจนั้นๆ ซึ่งปัญหาที่อาจจะเกิดขึ้นนั้นอาจจะมาจากความยากลำบากในการจัดการค่ากุญแจดังกล่าว เช่น ลืมค่ากุญแจ ก็เป็นได้

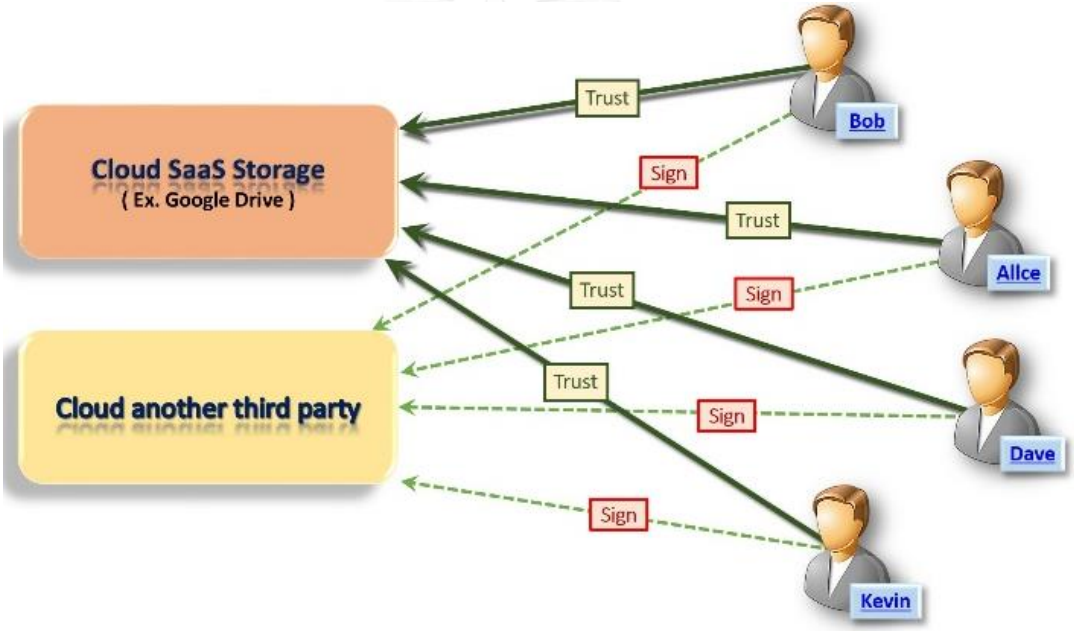
จากตัวอย่างในภาพ Bob ใช้บริการ SaaS Storage คือ Google Drive ในการเก็บเอกสารกูเกิ้ล ซึ่ง Bob เลือกใช้หลักการวิทยาการรหัสลับฝั่งผู้ใช้งานหรือฝั่งตนในรูปแบบของโปรแกรมเสริม (Plug-in) สำหรับเว็ปบราวส์เซอร์ กล่าวคือเขา ต้องการสร้างไฟล์เอกสารกูเกิ้ลใหม่ เขาจะต้องใส่ค่ากุญแจลับด้วยทุกครั้งในการใช้เอกสารกูเกิ้ล เมื่อเขาได้แก้ไขข้อมูลในไฟล์ดังกล่าวเสร็จแล้ว เขาต้องการแบ่งปันหรือแชร์ไฟล์ดังกล่าวไปยังผู้ใช้งานร่วมเช่น Alice และ Dave หลังจากเขาได้แชร์ไฟล์ดังกล่าวไปยังบุคคลที่เกี่ยวข้องแล้ว เขายังจะต้องหาช่องทางที่คิดว่าปลอดภัยในการบอกค่ากุญแจที่

เกี่ยวข้องด้วย เช่น อีเมล์ หรือ โทรศัพท์ และถ้า Alice ต้องการแชร์ไฟล์นั้นไปยัง Kevin หรือคนอื่นๆ ตนก็สามารถทำตามวิธีของ Bob ซึ่งเป็นเจ้าของไฟล์

ข้อดี ผู้ใช้งานทั้งหมดสามารถใช้งานSaaS Storage ด้วยความปลอดภัยจากภัยคุกคามของผู้ให้บริการได้

ข้อเสีย -จัดการค่ากุญแจและกระจายค่ากุญแจไม่เหมาะสม เนื่องจาก Bob สามารถลืมค่ากุญแจดังกล่าวได้ ถ้ากรณี Bob มีไฟล์เอกสารกูเกิ้ลจำนวนมาก และถ้า Bob เลือกกระจายค่ากุญแจด้วยช่องทางอีเมล์ ซึ่งในที่นี้หมายถึง Gmail ซึ่งเป็นช่องทางเดียวกันในแชร์ไฟล์เอกสารกูเกิ้ลดังกล่าว ผู้ให้บริการอย่าง Google สามารถดักจับค่ากุญแจในอีเมล์ดังกล่าว โดยไม่ยาก

3.1.4 รูปแบบการไว้ใจผู้ให้บริการหลายรายในการใช้งาน SaaS Storage จัดเตรียมฝั่งผู้ใช้งาน (Multiple Provider Client-side Cryptography – MPCC Model)



รูปที่ 3.1.4 Multiple Provider Client-side Cryptography Model

SaaS Storage Multiple-Provider Trusted Model เป็นหลักการหรือโมเดลการนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง ซึ่งถ้าเราเลือกใช้ผู้ให้บริการรายเดียวในการเก็บข้อมูลสำคัญทั้งหมด ถึงแม้รูปแบบที่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะถูกเข้ารหัสลับแบบไม่สามารถใช้งานได้นั้น แต่ข้อมูลอื่นๆเช่น ค่ากุญแจต่างๆ ที่เกี่ยวข้อง ก็ยังอยู่ในการดูแลของผู้ให้บริการ

ดังนั้นบุคคลที่เกี่ยวข้องเช่น ผู้ดูแลระบบก็สามารถที่จะนำค่ากุญแจต่างๆที่เกี่ยวข้องเพื่อถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำข้อมูลที่ได้มา เอาไปใช้งานที่สามารถก่อให้เกิดอันตรายต่อผู้ใช้งานได้ ผู้วิจัยต้องการนำเสนอและสนับสนุนหลักการหรือโมเดลนี้ และกระบวนการ การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งาน (Client Side Cryptography) ที่สามารถตอบโจทย์ด้านความเหมาะสมและความปลอดภัยจากช่องโหว่ต่างๆที่อาจจะเกิดอันตรายต่อข้อมูลสำคัญหรือข้อมูลลับ ขึ้นมาจากปัญหาดั่งกล่าว โดยจะเลือกใช้ทรัพยากร (Resource) ที่เป็นการประมวลผลแบบคลาวด์ (Cloud Computing) ในรูปแบบ SaaS ที่ให้บริการด้าน Storage จำนวน 2 รายเพื่อนำมาเป็นที่เก็บข้อมูลสำคัญหรือข้อมูลลับ (Data Repository) และ เป็นที่เก็บค่ากุญแจ (Key Repository) ต่างๆ ที่เกี่ยวข้อง

จากตัวอย่างในภาพ Bob ใช้ความสามารถของเอกสารกูเกิ้ลในการจำลองเป็นข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานทั่วไป จะใช้ Google Drive เป็น Storage หรือ Data Repository ในการเก็บข้อมูลสำคัญหรือข้อมูลลับ และใช้ ClearDB (Cloud another third Party) เป็น Key Repository ในการเก็บค่ากุญแจลับ (Session Key) ในส่วนกระบวนการ การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งานนั้น ถ้า Bob ต้องการแชร์ไฟล์ไปยังคนอื่นๆ เช่น Alice เขาก็สามารถแชร์ข้อมูลสำคัญที่เกี่ยวข้องใน SaaS Storage ทั้งหมดที่เป็นทั้ง Data Repository และ Key Repository ไปยัง Alice หรือคนอื่นๆ ด้วยการทำการผู้ใช้งานร่วมใน KRaaS หรือ ClearDB ว่ามีการมอบหมายสิทธิ์ในการใช้งานค่ากุญแจลับหรือไม่ ซึ่งโปรแกรมเสริมกูเกิ้ลเอกสาร จะทำหน้าที่ตรวจสอบสิทธิ์ก่อนที่จะมีการเรียกใช้งานค่ากุญแจลับดังกล่าวให้แก่ผู้ใช้งานร่วม เพื่อให้ผู้ใช้งานร่วมเลือกที่จะวางใจผู้ให้บริการ SaaS Storage ทั้งหมด

ข้อดี ผู้ใช้งานร่วมทั้งหมดสามารถใช้งาน SaaS Storage ด้วยความปลอดภัยจากภัยคุกคามของผู้ให้บริการได้

ข้อเสีย ความหน่วงขอเวลาที่จะเกิดขึ้นเมื่อมีการเรียกใช้งานไฟล์กูเกิ้ลเอกสาร เนื่องจากการทำการเข้าและถอดรหัสนั้น ซึ่งที่จะต้องแลกกับความปลอดภัยนี้คือ เวลาที่เพิ่มมากขึ้นในการอ่านหรือบันทึก ข้อมูลสำคัญหรือข้อมูลลับ เนื่องจากโปรแกรมเสริมกู้เกิ้ลเอกสารจะต้องใช้เวลาเพิ่มในการตรวจสอบสิทธิ์ผู้ใช้งาน และแต่ละค่ากุญแจลับปัจจุบันที่ถูกการจับคู่กับกูเกิ้ลเอการด้วย รวมถึงการทำการสิ้นสุดการใช้งานค่ากุญแจลับตัวเดิมเมื่อมีการใช้งานเข้าและถอดรหัสครบ 1 รอบของวิทยาการรหัสลับ และจับคู่ค่ากุญแจลับใหม่กับไฟล์กูเกิ้ลเอกสารดังกล่าว เพื่อป้องกันภัยคุกคามที่จะเกิดจากผู้ให้บริการ SaaS Storage ในแง่ของการพยายามที่จะคาดเดาค่ากุญแจลับ ซึ่งมีโอกาสเกิดขึ้นได้เสมอ

3.2 แนวความคิดของการรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมที่ผู้ให้บริการคลาวด์ไม่น่าเชื่อถือ

ในงานวิจัยนี้จะทำการเลือกใช้รูปแบบการไว้ใจผู้ให้บริการหลายรายในการใช้งาน SaaS Storage จัดเตรียมฝั่งผู้ใช้งาน (Multiple Provider Client-side Cryptography – MPCC Model) เนื่องจากกโมเดลนี้มีการใช้กระบวนการ วิทยาการรหัสลับที่ฝั่งผู้ใช้งาน(Client Side Cryptography) และใช้งานผู้ให้บริการด้าน Storage จำนวน 2 รายเพื่อนำมาเป็นที่เก็บข้อมูลสำคัญหรือข้อมูลลับ (Data Repository) และ เป็นที่เก็บค่ากุญแจ (Key Repository) ต่างๆ ที่เกี่ยวข้องที่สามารถตอบโจทย์ด้านความเหมาะสม และความปลอดภัยจากช่องโหว่ต่างๆที่อาจจะก่อให้เกิดอันตรายต่อข้อมูลสำคัญหรือข้อมูลลับ(Sensitive Data) ขึ้นมาจากปัญหาความไม่วางใจผู้ให้บริการ(Untrusted Cloud Provider) ซึ่งมีแนวคิดและวิธีการดำเนินงาน ดังนี้

จะเลือกใช้ทรัพยากร(Resource) ที่เป็นการประมวลผลแบบคลาวด์ (Cloud Computing) ในรูปแบบ SaaS (Software as a Service) ที่ให้บริการด้าน Storage และเป็นที่นิยมมากในการใช้งานของผู้ใช้งานในปัจจุบันคือ Google Drive และ ClearDB ซึ่งจะใช้ความสามารถของเอกสารกูเกิ้ลในการจำลองเป็นข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานทั่วไป จะใช้ Google Drive ในการจำลองเป็น Storage หรือ Data Repository ในการเก็บข้อมูลของผู้ใช้งาน และใช้ ClearDB จำลองเป็น Key Repository ในการเก็บค่ากุญแจลับ (Session Key)

จะนำเสนอกระบวนการ การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งาน (Client Side Cryptography) ซึ่งจะใช้อัลกอริทึมของวิทยาการรหัสลับแบบมาตรฐาน ทั้งวิทยาการรหัสลับที่ใช้กุญแจแบบสมมาตร (Symmetric Key Cryptography) หรือการใช้กุญแจดอกเดียว แบบ AES-256 บิต ในการเข้ารหัสและถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน ในที่นี้ก็คือ เอกสารในเอกสารกูเกิ้ลนั้นเอง และจะใช้โปรโตคอลเอสเอสแอล (SSL Protocol) ในการเข้ารหัส และถอดรหัสค่ากุญแจลับ (Session Key)

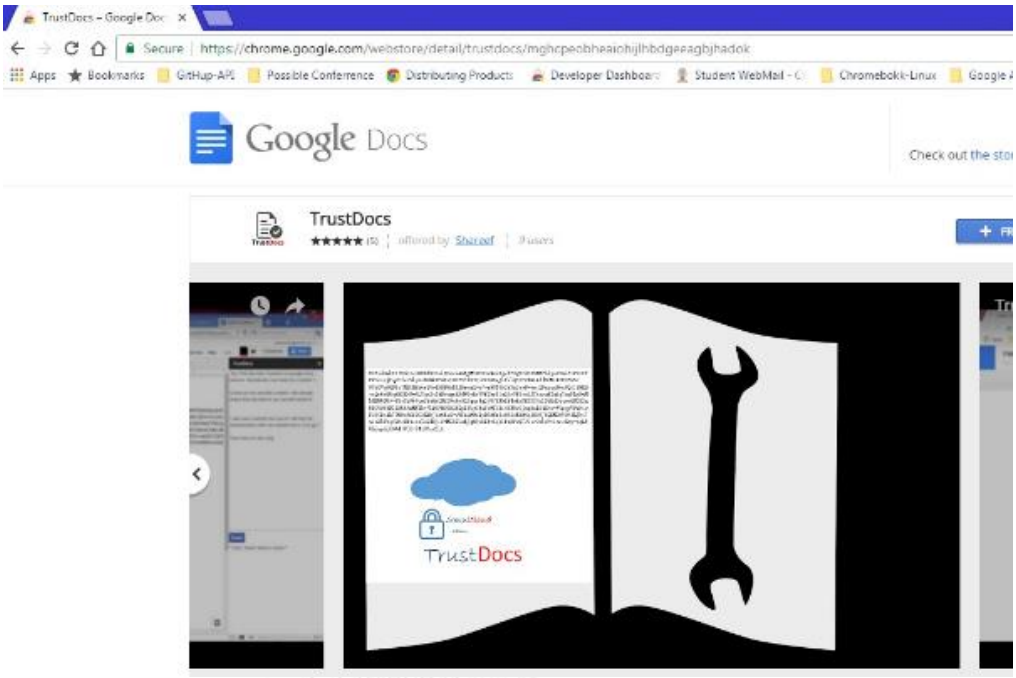
จะพัฒนาระบบต้นแบบเพื่อจำลองการทำงานของกระบวนการนำเสนอความปลอดภัยในการใช้งานของ SaaS Storage ด้วยการจัดทำโปรแกรมเสริม (Add-on) สำหรับ เอกสารกูเกิ้ล (Google Docs Add-on) เพื่อสนับสนุน การเข้าและถอดรหัสข้อมูลสำคัญ หรือข้อมูลลับ (Sensitive Data) ในไฟล์เอกสารกูเกิ้ล (Google Docs) และสนับสนุนการเรียกใช้งานค่ากุญแจลับ (Session Key) จาก ClearDB ที่ได้ออกแบบระบบและการทำงานในรูปแบบ Cloud Key Repository as a Service (KRaaS) ด้วยหลักการเสมือนการกระจายคีย์ (key-distribution-like) ในช่องทางการรับส่งที่ปลอดภัย (Secure Channel) ด้วยโปรโตคอลเอสเอสแอล (SSL Protocol) และจับคู่กับค่ากุญแจลับ

(Mapping Session Key) รวมถึงการทำการสิ้นสุดการใช้งานค่ากุญแจลับเดิม (Expire Session Key) เพื่อจับคู่กับค่ากุญแจใหม่ (Refresh Session Key) เมื่อครบ 1 รอบในการเข้า และถอดรหัสข้อมูลสำคัญหรือข้อมูลลับ ซึ่งมีรูปแบบการทำงานคล้าย One Time Pad Concept เพื่อแก้ไขปัญหาการพยายามการคาดเดาค่ากุญแจลับจากผู้ดูแลระบบ (Brute-Force Attack by System Administrator) ในส่วนของการสร้างค่ากุญแจลับ (Session Key) นั้น KRaaS Administrator จะมีหน้าที่สร้างค่ากุญแจ 256 บิต จำนวนมหาศาลเพื่อรองรับการใช้งานอย่างเพียงพอของผู้ใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล (Google Docs Add-on) รวมถึงความสามารถในการส่งไฟล์ดังกล่าว ไปยังผู้ใช้งานร่วมผ่านทาง Gmail และสุดท้ายคือกระบวนการบริหารการจัดการค่ากุญแจ (Key Management) หรือการกระจายค่ากุญแจ (Key Distribution) ไปยังบุคคลที่ต้องการแบ่งปันข้อมูลสำคัญหรือข้อมูลลับดังกล่าว

3.3 การพัฒนาระบบต้นแบบ TrustDocs – Google Docs Add-on

การที่ผู้วิจัยได้นำเสนอกระบวนการในรูปแบบในการเข้ารหัสลับข้อมูล (Data Encryption) การถอดรหัสลับข้อมูล (Data Decryption) การสร้างค่ากุญแจต่างๆ (Key Generation) และ การกระจายค่ากุญแจลับ (Session Key Distribution) ในรูปแบบที่เป็นกระบวนการอัตโนมัติ (Automatic Process) และการแก้ไขปัญหาในการใช้งานข้อมูลสำคัญหรือข้อมูลลับที่เก็บไว้ที่ SaaS Storage ได้ง่ายและมีความปลอดภัยจากภัยคุกคามมากขึ้น แต่ข้อเสียหรือจุดอ่อนของรูปแบบฯ ที่ได้นำมาใช้นี้ก็มีเช่นกัน กล่าวคือ การนำเสนอกระบวนการทั้งหมด ที่ได้กล่าวไว้ข้างต้นนั้น อาทิเช่น กระบวนการการเข้ารหัสลับและกระบวนการอื่นๆจะต้องถูกจัดการกระบวนบนเครื่องของผู้ใช้งาน ดังนั้นทรัพยากรของเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆของผู้ใช้งาน อาทิเช่น ขนาดหน่วยความจำ (RAM) ขนาดการประมวลผล (CPU Speed) จำเป็นต้องมีเพียงพอกับการใช้ในการสนับสนุนกระบวนการดังกล่าวทั้งสิ้น ที่สำคัญอีกอย่างหนึ่งที่หลีกเลี่ยงไม่ได้คือ ถ้า Second Cloud SaaS Storage เกิดเสีย (Failure) หรือไม่สามารถให้บริการได้ ผู้ใช้งานก็ไม่สามารถที่จะจัดการข้อมูลสำคัญหรือข้อมูลลับของตนได้ในขณะนั้นด้วยเช่นกัน ผู้วิจัยได้วิเคราะห์และออกแบบการพัฒนาระบบต้นแบบ TrustDocs – Google Docs Add-on ซึ่งมีดังต่อไปนี้

3.3.1 กลไกการใช้งานพื้นฐาน



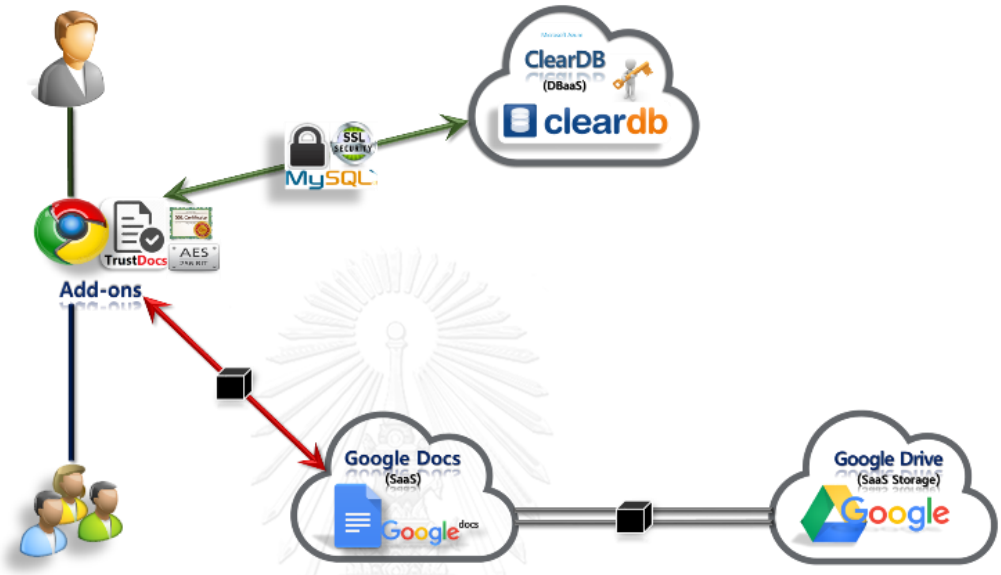
รูปที่ 3.2.1 TrustDocs – Google Docs Add-on

TrustDocs Google Docs Add-on คือโปรแกรมเสริมเอกสารกูเกิ้ลที่สามารถปกป้องข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจากผู้ดูแลระบบของกูเกิ้ล (Google Administrator) ด้วยการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานก่อนที่ผู้ใช้งานจะทำการสั่งให้มีการบันทึกข้อมูลดังกล่าวใน Google Drive และเมื่อผู้ใช้งานต้องการที่จะอ่านข้อมูลสำคัญหรือข้อมูลลับของตนที่อยู่ในไฟล์เอกสารกูเกิ้ล ก็สามารถสั่งด้วยการไปที่เมนู Add-ons >TrustDocs > Open โปรแกรมเสริมเอกสารกูเกิ้ลก็จะทำการถอดรหัสลับและแสดงผลข้อมูลสำคัญหรือข้อมูลลับในพื้นที่ Side Bar ซึ่งเป็นพื้นที่ๆไว้สนับสนุนให้ผู้ใช้งานได้มีการจัดการข้อมูลสำคัญหรือข้อมูลลับของตนทั้งการเขียน และอ่าน ซึ่งพื้นที่ Side Bar นี้ได้มีการทำงานและประมวลผลอยู่บนเว็ปบราวเซอร์ของผู้ใช้งานซึ่งสนับสนุนหลักการการนำเสนอความฝั่งปลอดภัยฝั่งผู้ใช้งาน (Client-side Security) ในการทำให้เกิดการไว้วางใจผู้ให้บริการ

3.3.2 สถาปัตยกรรมของ TrustDocs – Google Docs Add-on

ผู้วิจัยเสนอการเลือกใช้ทรัพยากร(Resource) ที่เป็นการประมวลผลแบบคลาวด์ (Cloud Computing) ในรูปแบบ SaaS (Software as a Service) ที่ให้บริการด้าน Storage และเป็นที่นิยม

มากในการใช้งานของผู้ใช้งานในปัจจุบันคือ Google Drive และ ClearDB ซึ่งจะใช้ความสามารถของเอกสารกูเกิ้ล ในการจำลองเป็นข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานทั่วไป จะใช้ Google Drive ในการจำลองเป็น Storage หรือ Data Repository ในการเก็บข้อมูลของผู้ใช้งาน และใช้ ClearDB จำลองเป็น Key Repository ในการเก็บค่ากุญแจลับ (Session Key)



รูปที่ 3.2.2 Solution Deployment Diagram

การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งาน (Client Side Cryptography) ซึ่งจะใช้อัลกอริทึมของวิทยาการรหัสลับแบบมาตรฐาน ทั้งวิทยาการรหัสลับที่ใช้กุญแจแบบสมมาตร (Symmetric Key Cryptography) หรือการใช้กุญแจดอกเดียว แบบ AES-256 บิต ในการเข้ารหัส และถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน ในที่นี้ก็คือ เอกสารในเอกสารกูเกิ้ลนั้นเอง และจะใช้โปรโตคอลเอสเอสแอล (SSL Protocol) ในการเข้ารหัส และถอดรหัสค่ากุญแจลับ (Session Key)

3.3.3 Key Distribution Life Cycle

การพัฒนาระบบต้นแบบเพื่อจำลองการทำงานของกระบวนการนำเสนอความปลอดภัยในการใช้งานของ SaaS Storage ด้วยการจัดทำโปรแกรมเสริม (Add-on) สำหรับ เอกสารกูเกิ้ล (Google Docs Add-on) เพื่อสนับสนุน การเข้าและถอดรหัสข้อมูลสำคัญ หรือข้อมูลลับ (Sensitive Data) ในไฟล์เอกสารกูเกิ้ล (Google Docs) และสนับสนุนการเรียกใช้งานค่ากุญแจลับ (Session Key) จาก ClearDB ที่ได้ออกแบบระบบและการทำงานในรูปแบบ Cloud Key Repository as a

Service (KRaaS) ด้วยหลักการเสมือนการกระจายคีย์ (key-distribution-like) ในช่องทางการรับส่งที่ปลอดภัย (Secure Channel) ด้วยโปรโตคอลเอสเอสแอล (SSL Protocol) และจับคู่กับค่ากุญแจลับ (Mapping Session Key) รวมถึงการทำการสิ้นสุดการใช้งานค่ากุญแจลับเดิม (Expire Session Key) เพื่อจับคู่กับค่ากุญแจใหม่ (Refresh Session Key) เมื่อครบ 1 รอบในการเข้า และถอดรหัสข้อมูลสำคัญหรือข้อมูลลับ ซึ่งมีรูปแบบการทำงานคล้าย One Time Pad Concept เพื่อแก้ไขปัญหาการพยายามการคาดเดาค่ากุญแจลับจากผู้ดูแลระบบ (Brute-Force Attack by System Administrator)

ต่อไปนี้จะเป็นนิยามของตัวย่อที่จะใช้ในการอธิบายขั้นตอนการทำงาน

Enc_{aes}^{256} [k][D] = เป็นการใช้กุญแจ k ในการเข้ารหัสเอกสาร D ด้วย AES 256 bit

Dec_{aes}^{256} [k][D] = เป็นการใช้กุญแจ k ในการถอดรหัสเอกสาร D ด้วย AES 256 bit

D_i^c = ไฟลเอกสารกูเกิ้ลที่มีข้อมูลสำคัญหรือข้อมูลลับปกติ (Google Docs with Plain Content)

D_{dum}^c = ไฟลเอกสารกูเกิ้ลข้อความดัมมี่ปกติ (Google Docs with Plain Dummy Text)

$D_i^{c\prime}$ = ไฟลเอกสารกูเกิ้ลที่มีข้อมูลสำคัญหรือข้อมูลลับในรูปแบบการเข้ารหัสลับ (Google Docs with Cypher Content)

$D_{dum}^{c\prime}$ = ไฟลเอกสารกูเกิ้ลข้อความดัมมี่ที่ได้รับการเข้ารหัสลับ (Google Docs with Cypher Dummy Text)

$[k_i^n]$ เป็นกุญแจลับ i ในสถานะต่างๆ โดยที่ n บ่งบอกสถานะของกุญแจลับซึ่งมีค่าตามสถานะดังนี้

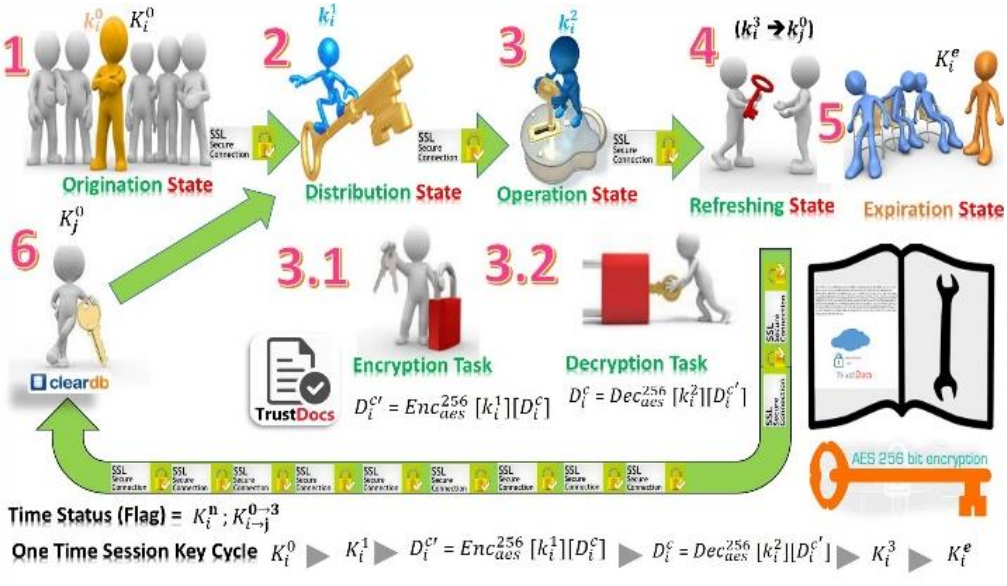
0 = ค่ากุญแจลับที่อยู่ในสถานะ Origination State

1 = ค่ากุญแจลับที่อยู่ในสถานะ Distribution State

2 = ค่ากุญแจลับที่อยู่ในสถานะ Operation State

3 = ค่ากุญแจลับที่อยู่ในสถานะ Refreshing State

4 = ค่ากุญแจลับที่อยู่ในสถานะ Expiration State



รูปที่ 3.2.3 Solution Deployment Diagram

ในส่วนของการสร้างค่ากุญแจลับ (Session Key) นั้น KRaaS Administrator จะมีหน้าที่สร้างค่ากุญแจ 256 บิต จำนวนมหาศาลเพื่อรองรับการใช้งานอย่างเพียงพอของผู้ใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล (Google Docs Add-on) รวมถึงความสามารถในการส่งไฟล์ดังกล่าว ไปยังผู้ใช้งานร่วมผ่านทาง Gmail และสุดท้ายคือกระบวนการบริหารการจัดการค่ากุญแจ (Key Management) หรือการกระจายค่ากุญแจ (Key Distribution) ไปยังบุคคลที่ต้องการแบ่งปันข้อมูลสำคัญหรือข้อมูลลับดังกล่าว สำหรับวงจรชีวิตของค่ากุญแจลับ (Session Key Life Cycle) สามารถแบ่งออกเป็น 5 สถานะ (State) ดังนี้

3.2.3.1 สถานะเริ่มต้น (Origination State): เป็นสถานะแรกของทุกๆค่ากุญแจลับใหม่ที่ถูกสร้างขึ้นมาด้วยผู้ดูแลระบบ KRaaS จะมีหน้าที่สร้างค่ากุญแจสำหรับอัลกอริทึม AES ขนาด 256 บิต จำนวนมหาศาลเพื่อรองรับการใช้งานอย่างเพียงพอของผู้ใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล เราจะใช้ชื่อ [k_i^0] แทนที่ค่ากุญแจต่างๆที่อยู่ในสถานะเริ่มต้น. เมื่อผู้ใช้งานได้มีการเปิดไฟล์เอกสารกูเกิ้ลที่มีการติดตั้งโปรแกรม TrustDocs เรียบร้อยแล้ว โปรแกรมเสริมจะมีการเช็กเอกสารกูเกิ้ลดังกล่าวว่าเคยมีในระบบ KRaaS หรือไม่ ถ้ายังไม่มี โปรแกรมเสริม TrustDocs จะทำการจับคู่ค่ากุญแจลับใน Original State กับไฟล์เอกสารกูเกิ้ลดังกล่าว

3.2.3.2 สถานะการกระจาย (Distribution State): หรือ [k_i^1] เป็นสถานะของค่ากุญแจลับที่มีการเรียกใช้งานจากโปรแกรมเสริม TrustDocs ในการกระทำการเข้ารหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานทั้งไฟล์เอกสารกูเกิ้ลที่สร้างใหม่ โปรแกรมเสริมเอกสารกูเกิ้ลจะเรียกใช้งาน [k_i^0] มาทำการเข้ารหัสลับกับข้อความดัมมี่ (Dummy Text) ที่ทางโปรแกรมเสริม TrustDocs เตรียมไว้เพื่อจับคู่ค่ากุญแจลับกับไฟล์เอกสารกูเกิ้ลใหม่ หลังจากโปรแกรมเสริม TrustDocs ได้ทำการเข้ารหัสลับข้อความดัมมี่ และจับคู่ค่ากุญแจลับกับไฟล์เอกสารใหม่เรียบร้อยแล้ว โปรแกรมเสริม TrustDocs จะดำเนินการเปลี่ยนสถานะของค่ากุญแจลับ [k_i^0] (Origination State) กลายเป็น [k_i^1] (Distribution State) ที่อยู่ในสถานะกระจายนี้ และโปรแกรมเสริม TrustDocs ก็ทำการถอดรหัสข้อความดัมมี่เพื่อให้ทางผู้ใช้งานได้เห็น “Welcome to TrustDocs. Delete All then Start!” ซึ่งกระบวนการถอดรหัสลับข้อความดัมมี่ดังกล่าว โปรแกรมเสริม TrustDocs จะทำการเปลี่ยนสถานะของค่ากุญแจลับจาก [k_i^1] (Distribution State) กลายเป็นค่ากุญแจลับสถานะ [k_i^2] (Operation State) ซึ่งเป็นค่ากุญแจลับที่อยู่ในสถานะถัดไป

3.2.3.3 สถานะการดำเนินการ (Operation State): หรือสถานะค่ากุญแจลับ [k_i^2] เป็นสถานะของค่ากุญแจลับที่ถูกเปลี่ยนแปลงหลังจากที่มีการเรียกใช้งานจากโปรแกรมเสริม TrustDocs ในการกระทำการถอดรหัสลับข้อความดัมมี่ และไฟล์เอกสาสารกูเกิ้ลเดิมที่ผู้ใช้งานได้สร้างและจัดการไปแล้วในการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน ในส่วนของไฟล์เอกสารกูเกิ้ลใหม่ โปรแกรมเสริมเอกสารกูเกิ้ลจะเรียกใช้งาน [k_i^1] มาทำการถอดรหัสลับกับข้อความดัมมี่ (Dummy Text) เพื่อแสดงให้ผู้ใช้งานได้เห็นข้อความดัมมี่ดังกล่าวในหน้า Side Bar หลังจากนั้นโปรแกรมเสริม TrustDocs จะดำเนินการทำการเปลี่ยนสถานะของค่ากุญแจลับ [k_i^1] (Distribution State) ให้กลายเป็น [k_i^2] (Operation State) และในส่วนของไฟล์เอกสารกูเกิ้ลเก่า โปรแกรมเสริม TrustDocs ก็ทำการเข้ารหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน ซึ่งโปรแกรมเสริม TrustDocs จะทำการเปลี่ยนสถานะของค่ากุญแจลับจาก [k_i^0] (Origination State) กลายเป็นค่ากุญแจลับสถานะ k_i^2 (Operation State) ซึ่งเป็นค่ากุญแจลับที่อยู่ในสถานะนี้

3.2.3.4 สถานะการพร้อมเริ่มต้นใหม่ (Refreshing State): หรือสถานะค่ากุญแจลับ k_i^3 คือสถานะค่ากุญแจลับที่โปรแกรมเสริม TrustDocs เรียกใช้งานครบวงจรจำนวน 1 รอบของวิทยาการรหัสลับ (a round of cryptographic task) คือการเข้าและถอดรหัสลับอย่างละ 1 ครั้งซึ่งโปรแกรมเสริม TrustDocs จัดทำการเตรียมการจับคู่ค่ากุญแจลับใหม่ และดำเนินการทำการสิ้นสุดหรือหมดอายุกับค่ากุญแจดังกล่าว

3.2.3.5 สถานการณ์หมดอายุ (Expiration State): หรือสถานะค่ากุญแจลับ k_i^e คือสถานะค่ากุญแจลับที่โปรแกรมเสริม TrustDocs ทำการจับคู่ค่ากุญแจลับใหม่ k_j^0 เพื่อเตรียมการการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับที่ได้ถูกแก้ไขข้อมูลจากผู้ใช้งานเรียบร้อยแล้ว ก่อนที่จะมีการสั่งให้บันทึกข้อมูลดังกล่าวลงสู่กูเกิ้ลไดร์ฟต่อไป

ข้อสรุปการดำเนินการของการเข้าและถอดรหัสลับ และการเปลี่ยนสถานะของค่ากุญแจลับ

- ไฟล์เอกสารกูเกิ้ลใหม่ (New Google Docs)

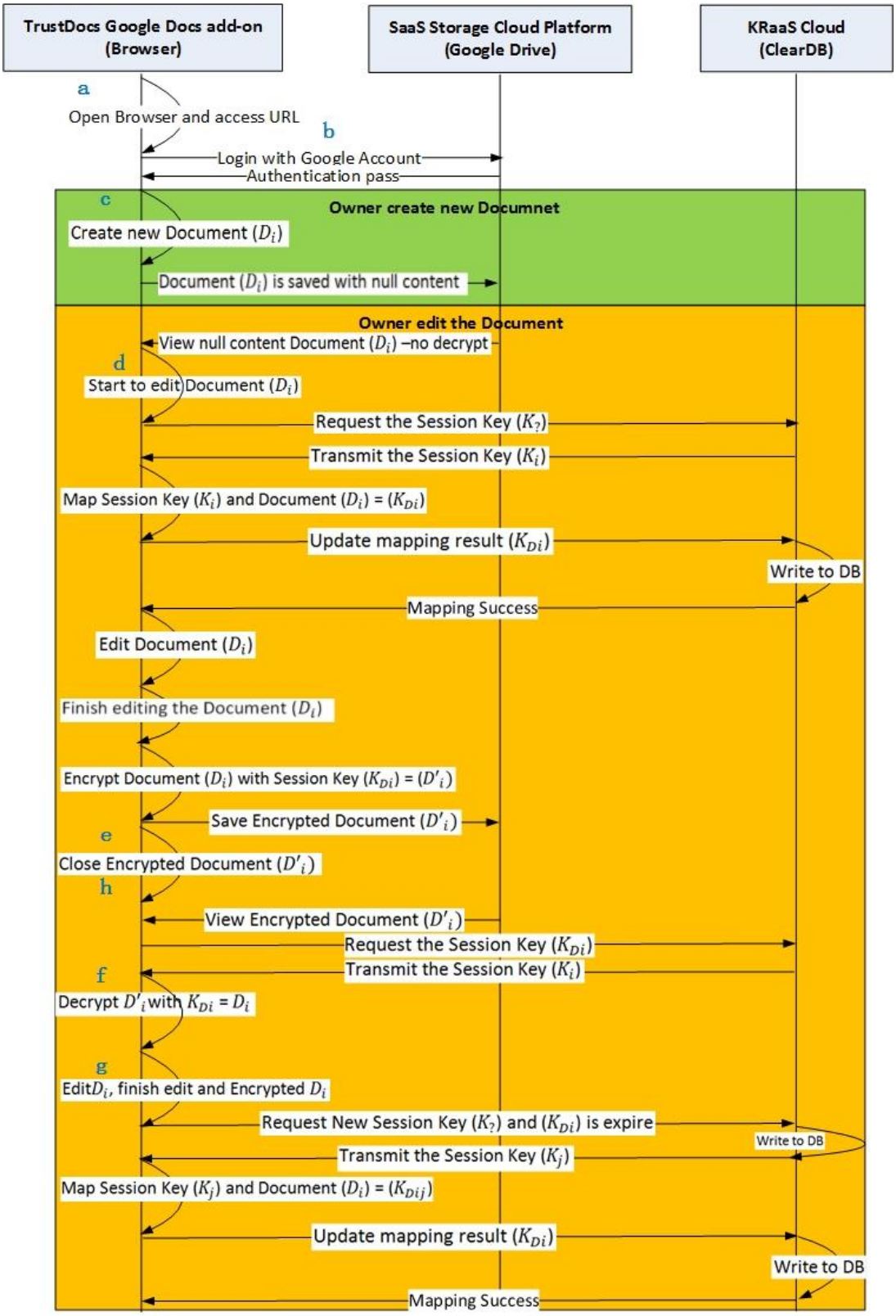
$$Encrypt\ New\ Document = D_{dum}^{c'} = Enc_{aes}^{256}\left[k_i^0\right][D_{dum}^{c}]$$
$$Decrypt\ New\ Document = D_{dum}^{c} = Dec_{aes}^{256}\left[k_i^1\right][D_{dum}^{c'}]$$
$$Encrypt\ New\ Document = \left[k_i^0\right] => \left[k_i^1\right]$$
$$Decrypt\ New\ Document = \left[k_i^1\right] => \left[k_i^2\right]$$

- ไฟล์เอกสารกูเกิ้ลเดิม (Old Google Docs)

$$Encrypt\ Old\ Document = D_i^{c'} = Enc_{aes}^{256}\left[k_i^0\right][D_i^c]$$
$$Decrypt\ Old\ Document = D_i^c = Dec_{aes}^{256}\left[k_i^2\right]\left[D_i^{c'}\right]$$
$$Encrypt\ Old\ Document = \left[k_i^0\right] => \left[k_i^2\right]$$
$$Decrypt\ Old\ Document = \left[k_i^2\right] => \left[k_i^2\right]$$

3.2.4 การสร้างและแก้ไขไฟล์เอกสารกูเกิ้ล (Google Docs Creation and Edition)

ก่อนที่จะมีการใช้งานเอกสารกูเกิ้ล ควรจะต้องติดตั้ง และเปิดใช้งาน โปรแกรมเสริม TrustDocs (TrustDocs – Google Docs Add-on) ก่อนทุกครั้ง สามารถดาวน์โหลดและติดตั้งจาก https://chrome.google.com/webstore/detail/trustdocs/mghcpeobheaiohijlhbdgeeagbjhadokโดยมีขั้นตอนดังต่อไปนี้



รูปที่ 3.2.4 TrustDocs – Google Docs Add-on Activity Diagram for Create and Edit

a) ผู้ใช้งานติดตั้งและเปิดใช้งานโปรแกรมเสริม TrustDocs

b) ผู้ใช้งานล็อกอินเพื่อเข้าสู่ระบบ ด้วยบัญชีของ Google

c) ผู้ใช้งานเปิดใช้งาน Google Drive และสร้างไฟล์เอกสารกูเกิ้ลใหม่ ($\boldsymbol{D_i}$) แล้วไปที่เมนู “Add-on > TrustDocs > Open” และรอโปรแกรมเสริม TrustDocs แสดงผลจนเสร็จสมบูรณ์ทำให้ผู้ใช้งานได้เห็น Side Bar พร้อม Dummy Text แสดงผลใน Text Area ในกระบวนการนี้ โปรแกรมเสริม TrustDocs ได้มีการเช็กเอกสารกูเกิ้ล และโปรไฟล์ผู้ใช้งาน ในระบบ KRaaS ในกรณีที่เป็นเอกสารใหม่ โปรแกรมเสริม TrustDocs มีการอัพเดตหมายเลขไฟล์เอกสารกูเกิ้ล และอีเมล์ผู้ใช้งานไปยัง KRaaS และมีการเรียกค่ากุญแจลับใหม่ $\boldsymbol{K_i}$ มาทำการเข้ารหัสลับกับข้อความดัมมี่และจับคู่กับไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) ดังกล่าว และโปรแกรมเสริม TrustDocs ทำการเรียก $\boldsymbol{K_i}$ ทำการถอดรหัสลับข้อความดัมมี่เพื่อให้ผู้ใช้งานสามารถเห็นและอ่านได้ใน Side Bar ได้

d) ผู้ใช้งานลบข้อความดัมมี่ทั้งหมด แล้วเริ่มต้นเขียนข้อมูลสำคัญหรือข้อมูลลับของตน แล้วกดปุ่ม “Save” โปรแกรมเสริม TrustDocs ทำการเรียกค่ากุญแจลับ $\boldsymbol{K_j}$ ที่ถูกจับคู่กับไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) จาก KRaaS เพื่อทำการเข้ารหัสลับขอมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน และทำการสิ้นสุดการใช้งานค่ากุญแจลับ $\boldsymbol{K_i}$ ก่อนที่จะบันทึกข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานในรูปแบบการถูกเข้ารหัสเรียบร้อยแล้วใน Google Drive

e) ผู้ใช้งานปิดเอกสารกูเกิ้ล

หลังจากที่ผู้ใช้งานได้ปิดเอกสารกูเกิ้ลหลังจากเสร็จสิ้นภาระกิจในการบริหารจัดการข้อมูลสำคัญหรือข้อมูลลับในไฟล์ที่มีการจัดเก็บบนการให้บริการคลาวด์ SaaS Storage นั้น เมื่อผู้ใช้งานต้องการแก้ไขข้อมูลสำคัญหรือข้อมูลลับในเอกสารกูเกิ้ล ผู้ใช้งานสามารถกระทำได้ทุกเวลา และทุกสถานที่ที่มีการเชื่อมต่ออินเตอร์เน็ต และทำการติดตั้งโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ซึ่งมีกระบวนการทำงานของการแก้ไขข้อมูลสำคัญหรือข้อมูลลับในไฟล์เอกสารกูเกิ้ลดังนี้

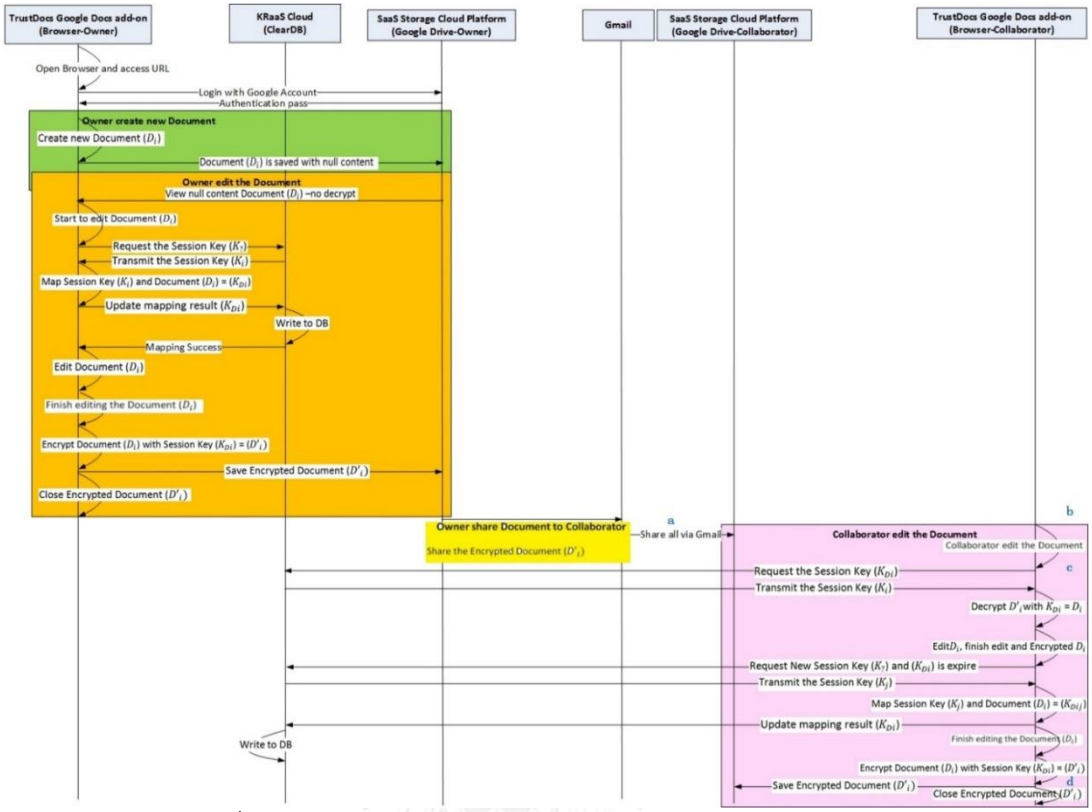
f) ผู้ใช้งานเปิดไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) ดังกล่าวแล้วไปที่เมนู “Add-on > TrustDocs > Open” และรอโปรแกรมเสริม TrustDocs แสดงผลจนเสร็จสมบูรณ์ทำให้ผู้ใช้งานได้เห็น Side Bar พร้อม ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน แสดงผลใน Text Area ในกระบวนการนี้ โปรแกรมเสริม TrustDocs ได้มีการเรียกค่ากุญแจลับ $\boldsymbol{K_j}$ ที่ถูกจับคู่กับไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) จากระบบ KRaaS มาทำการถอดรหัสลับข้อมูลสำคัญหรือข้อมูลลับเพื่อให้ผู้ใช้งานสามารถเห็นและอ่านได้ใน Side Bar ได้

g) ผู้ใช้งานแก้ไขข้อมูลสำคัญหรือข้อมูลลับของตน และเมื่อแก้ไขข้อมูลเสร็จสิ้นแล้ว ผู้ใช้งานทำการกดปุ่ม “Save” โปรแกรมเสริม TrustDocs ทำการเรียกค่ากุญแจลับใหม่ $\boldsymbol{K_k}$ มาจับคู่กับไฟล์เอกสารกูเกิ้ล $(\boldsymbol{D_i})$ จาก KRaaS เพื่อทำการเข้ารหัสลับขอมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน และทำการสิ้นสุดการใช้งานค่ากุญแจลับ $\boldsymbol{K_j}$ ก่อนที่จะบันทึกข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานในรูปแบบการถูกเข้ารหัสเรียบร้อยแล้วใน Google Drive

h) ผู้ใช้งานปิดเอกสารกูเกิ้ล

3.2.5 การแบ่งปันไฟล์เอกสารกูเกิ้ลให้กับผู้ใช้งานร่วมเพื่อแก้ไขข้อมูลร่วมกันแบบ Version Control (Collaborative Version Control Edition Sharing)

หลังจากที่ผู้ใช้งานในฐานะเจ้าของไฟล์ได้สร้างและแก้ไขข้อมูลไฟล์เอกสารกูเกิ้ลเรียบร้อยแล้ว และมีต้องการที่จะแบ่งปันไฟล์เอกสารกูเกิ้ลให้กับผู้ใช้งานร่วมเพื่อแก้ไขข้อมูลร่วมกันในลักษณะ Version Control เจ้าของไฟล์สามารถที่จะแบ่งปันไฟล์เอกสารกูเกิ้ลดังกล่าวไปให้ผู้ใช้งานร่วมได้ไม่จำกัดจำนวน และหลักการวิทยาการรหัสลับเพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล เพื่อป้องกันการถูกละเมิดความเป็นส่วนตัวจากเจ้าของผู้ให้บริการก็ยังคงสนับสนุน โดยมีขั้นตอนดังต่อไปนี้



รูปที่ 3.2.5 Collaborative Version Control Edition Sharing

โปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ยังคงสนับสนุนความสามารถในการแบ่งปันไฟล์เอกสารกูเกิ้ลไปให้กับผู้ใช้งานร่วมเพื่อแก้ไขข้อมูลในแบบ Version Control โดยไม่ สนับสนุนคุณสมบัติของการใช้งานเอกสารกูเกิ้ลในด้านการใช้งานในรูปแบบการแก้ไขร่วมกันแบบเรียลไทม์ (real time collaborative edition of online documents) ซึ่งมีกระบวนการงานดังต่อไปนี้

a) เจ้าของไฟล์แบ่งปันไฟล์ดังต่อไปนี้ให้กับผู้ใช้งานร่วมในช่องทางอีเมลของทาง Gmail และอีเมลโดเมนอื่นๆ ที่ได้รับการจดทะเบียนในการใช้งานเอกสารกูเกิ้ล

i. ไฟล์เอกสารกูเกิ้ลที่ได้รับการเข้ารหัสลับ ($\boldsymbol{D'_i}$) อัลกอริทึม AES ด้วยค่ากุญแจลับ 256 บิต ซึ่งข้อมูลส่วนนี้จะเป็น url

ii. เจ้าของไฟล์จะต้องทำการดำเนินการมอบหมายสิทธิ์ให้แก่ผู้ใช้งานร่วม เพื่อสามารถได้รับค่ากุญแจลับ ($\boldsymbol{K_{Di}}$) จากระบบ KRaaS เพื่อการถอดรหัสลับข้อมูลสำคัญหรือข้อมูลลับของตน โดยการใช้โปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ให้ไปที่เมนู “Add-on > TrustDocs > Share” และรอโปรแกรมเสริม TrustDocs แสดงผลจนเสร็จสมบูรณ์ทำให้ผู้ใช้งานได้เห็น Dialog Box เพื่อให้เจ้าของไฟล์กรอก email address ของผู้ใช้งานร่วมเพื่อสามารถใช้งานค่ากุญแจลับร่วมกัน ในกระบวนการนี้ โปรแกรมเสริม TrustDocs ได้มีการอัพเดตโปรไฟล์ผู้ใช้งานร่วม ไปยังระบบ KRaaS เพื่อสามารถใช้งานเอกสาร ($\boldsymbol{D_i}$) ดังกล่าวและค่ากุญแจลับ ทุกๆ ค่า $\boldsymbol{K_{i\rightarrow j}}$ ที่ถูกจับคู่กับเอกสาร ($\boldsymbol{D_i}$) นี้

iii. เจ้าของไฟล์จะต้องใช้เมนูการแบ่งปันไฟล์เอกสารกูเกิ้ลพื้นฐาน (Google Standard Feature) ในการแบ่งปันไฟล์ให้กับผู้ใช้งานร่วมเพื่อใช้งานไฟล์เอกสารร่วมกัน

b) ผู้ใช้งานร่วมสามารถรับไฟล์ดังกล่าวผ่านทาง Gmail หลังจากนั้นให้กดลิงค์เพื่อจัดการในการใช้งานร่วมไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) เมื่อผู้ใช้งานร่วมต้องการเปิดอ่านข้อมูลสำคัญหรือข้อมูลลับของเจ้าของไฟล์ ผู้ใช้งานร่วมจะต้องติดตั้งโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ก่อน และไปยังเมนู “Add-on > TrustDocs > Open” และรอโปรแกรมเสริม TrustDocs แสดงผลจนเสร็จสมบูรณ์ทำให้ผู้ใช้งานร่วมได้เห็น Side Bar พร้อม ข้อมูลสำคัญหรือข้อมูลลับของเจ้าของไฟล์ ซึ่งได้แสดงผลใน Text Area บน Side Bar ในกระบวนการนี้ โปรแกรมเสริม TrustDocs ได้มีการเรียกค่ากุญแจลับ $\boldsymbol{K_i}$ ที่ถูกจับคู่กับไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) จากระบบ KRaaS มาทำการถอดรหัสลับข้อมูลสำคัญหรือข้อมูลลับเพื่อให้ผู้ใช้งานร่วมสามารถเห็นและอ่านได้ใน Side Bar

c) ผู้ใช้งานร่วมแก้ไขข้อมูลสำคัญหรือข้อมูลลับของเจ้าของไฟล์ และเมื่อแก้ไขข้อมูลเสร็จสิ้นแล้ว ผู้ใช้งานร่วมทำการกดปุ่ม “Save” โปรแกรมเสริม TrustDocs ทำการเรียกค่ากุญแจลับใหม่ $\boldsymbol{K_j}$ มาจับคู่กับไฟล์เอกสารกูเกิ้ล ($\boldsymbol{D_i}$) จาก KRaaS เพื่อทำการเข้ารหัสลับขอมูลสำคัญหรือข้อมูล

ลับของผู้ใช้งาน และทำการสิ้นสุดการใช้งานค่ากุญแจลับ $\boldsymbol{K_i}$ ก่อนที่จะบันทึกข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานในรูปแบบการถูกเข้ารหัสเรียบร้อยแล้วใน Google Drive

d) ผู้ใช้งานร่วมปิดไฟล์เอกสารกูเกิ้ล และแจ้งเจ้าของไฟล์เกี่ยวกับการแก้ไขข้อมูลของตนให้แด่เจ้าของไฟล์ผ่านช่องทางที่ปลอดภัย

บทที่ 4

การพัฒนาเครื่องมือ

การนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง ซึ่งถ้าเราเลือกใช้ผู้ให้บริการรายเดียวในการเก็บข้อมูลสำคัญทั้งหมด ถึงแม้รูปแบบที่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะถูกเข้ารหัสลับแบบไม่สามารถใช้งานได้นั้น แต่ข้อมูลอื่นๆเช่น ค่ากุญแจต่างๆ ที่เกี่ยวข้อง ก็อาจจะยังอยู่ในการดูแลของผู้ให้บริการ ดังนั้นบุคคลที่เกี่ยวข้องเช่น ผู้ดูแลระบบก็สามารถที่จะนำค่ากุญแจต่างๆที่เกี่ยวข้องเพื่อถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำข้อมูลที่ได้มา เอาไปใช้งานที่สามารถก่อให้เกิดอันตรายต่อผู้ใช้งานได้ ดังนั้นผู้วิจัยจึงได้มีการพัฒนาเครื่องมือเพื่อสนับสนุนการทำงานของระบบความปลอดภัยจากภัยคุกคามในฝั่งผู้ให้บริการ ดังต่อไปนี้

4.1. การพัฒนาเครื่องมือในส่วนของโปรแกรมเสริม TrustDocs – Google Docs Add-on

ในการพัฒนาเครื่องมือในส่วนของฝั่งผู้ใช้งานนั้น ผู้วิจัยเลือกใช้โปรแกรมเสริมเอกสารกูเกิ้ล (Google Docs Add-on) ซึ่งเป็นส่วนเสริมของเอกสารกูเกิ้ลที่สามารถเพิ่มเติมความสามารถในการทำงานของเอกสารกูเกิ้ลตามที่เราต้องการ ซึ่งทางกูเกิ้ลเองอนุญาตให้นักพัฒนาโปรแกรม สามารถที่จะเขียนเพิ่มฟังก์ชั่น หรืออินติเกรทกับโปรแกรมของผู้พัฒนาเอง ซึ่งทางผู้ให้บริการได้เปิดช่องทางนี้ผ่าน Google Apps API ซึ่งภาษาคอมพิวเตอร์ที่ใช้เขียนโปรแกรมจะเป็นภาษาของทางกูเกิ้ลเอง คือ Google Apps Script ซึ่งลักษณะไวยกรณ์ (Syntax) จะคล้ายกับภาษา JavaScript หรือ JQuery จากการศึกษาคุณสมบัติของโปรแกรมเสริมเอกสารกูเกิ้ลถึงความเหมาะสมและได้สนับสนุนทางด้านความปลอดภัยในฝั่งผู้ใช้งาน (Client-side Security) เพื่อให้สอดคล้องกับสิ่งที่ผู้วิจัยต้องการที่จะนำเสนอการทำวิทยาการรหัสลับในฝั่งของผู้ใช้งาน (Client-side Cryptography) ดังนั้นผู้วิจัยจึงได้ทำการพัฒนาโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs เพื่อเป็นเครื่องมือในทำวิจัย ซึ่งรายละเอียดคร่าวๆ ดังต่อไปนี้

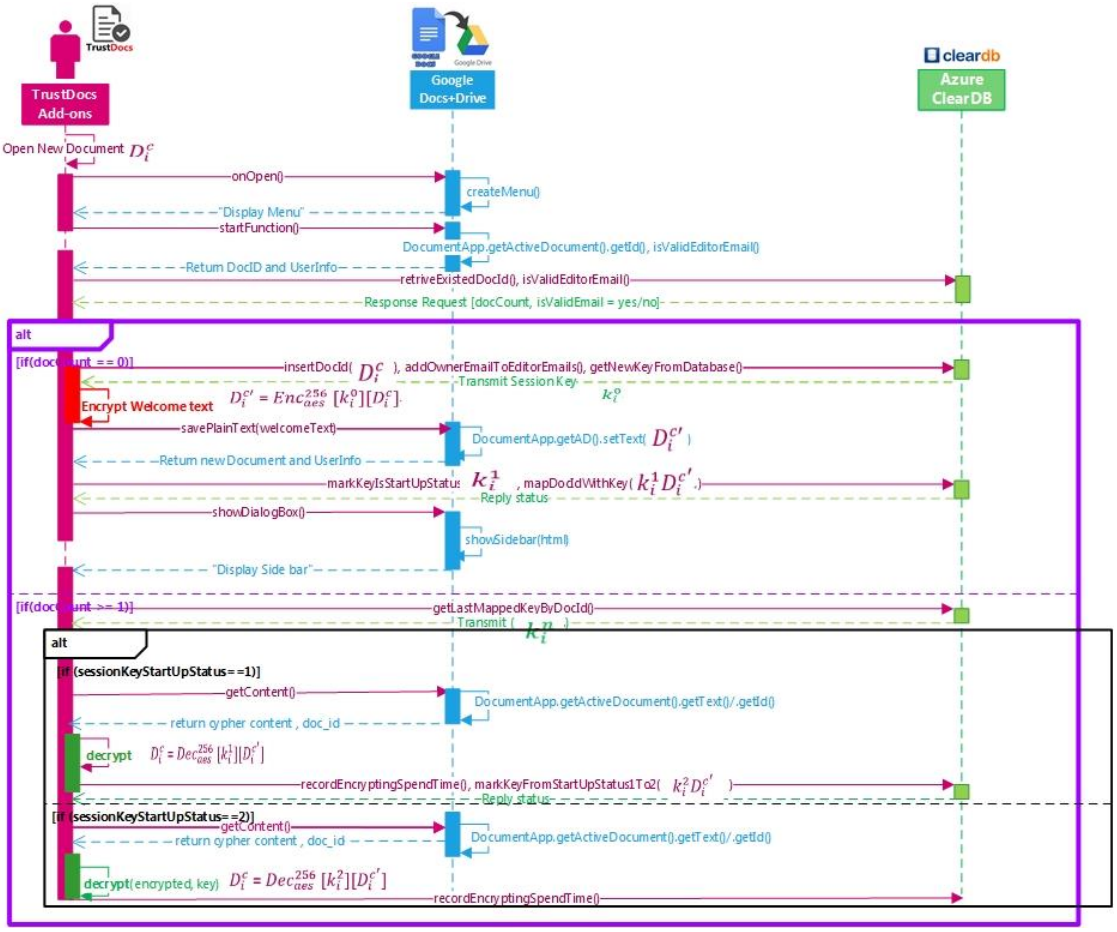
4.1.1 TrustDocs – Google Docs Add-on Execute Function Diagram

Execute Function Diagram คือไดอาแกรมที่อธิบายของการทำงานของฟังก์ชันต่างๆ ที่มีอยู่

ใน Source Code ซึ่งผู้วิจัยได้แบ่งแยกการทำงานของแต่ละฟังก์ชัน ได้ 3 สถานการณ์ดังนี้

4.1.1.1 สถานการณ์การสร้างไฟล์เอกสารกูเกิ้ลใหม่และการแก้ไข (New Google Docs Creation and Edition)

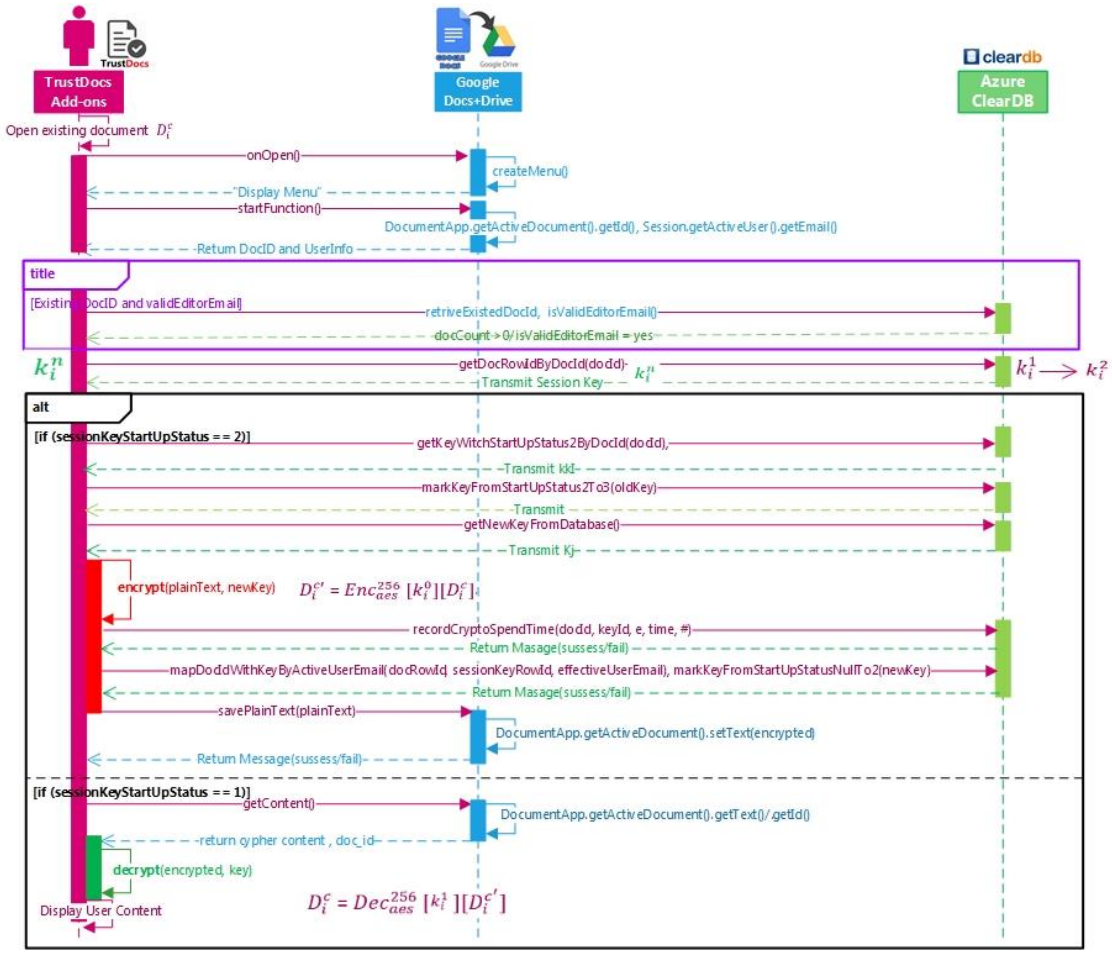
ในการทำงานของฟังก์ชั่นในสถานการณ์การสร้างไฟล์เอกสารกูเกิ้ลใหม่ ผู้ใช้งานจะต้องติดตั้งโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ก่อนที่จะมีการจัดการข้อมูลสำคัญหรือข้อมูลลับของตนให้ปลอดภัย ซึ่งการทำงานของฟังก์ชั่นต่างๆที่ผู้วิจัยได้พัฒนาโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ได้วิเคราะห์และออกแบบการทำงานดังต่อไปนี้



รูปที่ 4.1.1 Function Execution Activity Diagram for New Google Docs

4.1.1.2 Old Google Docs Edition

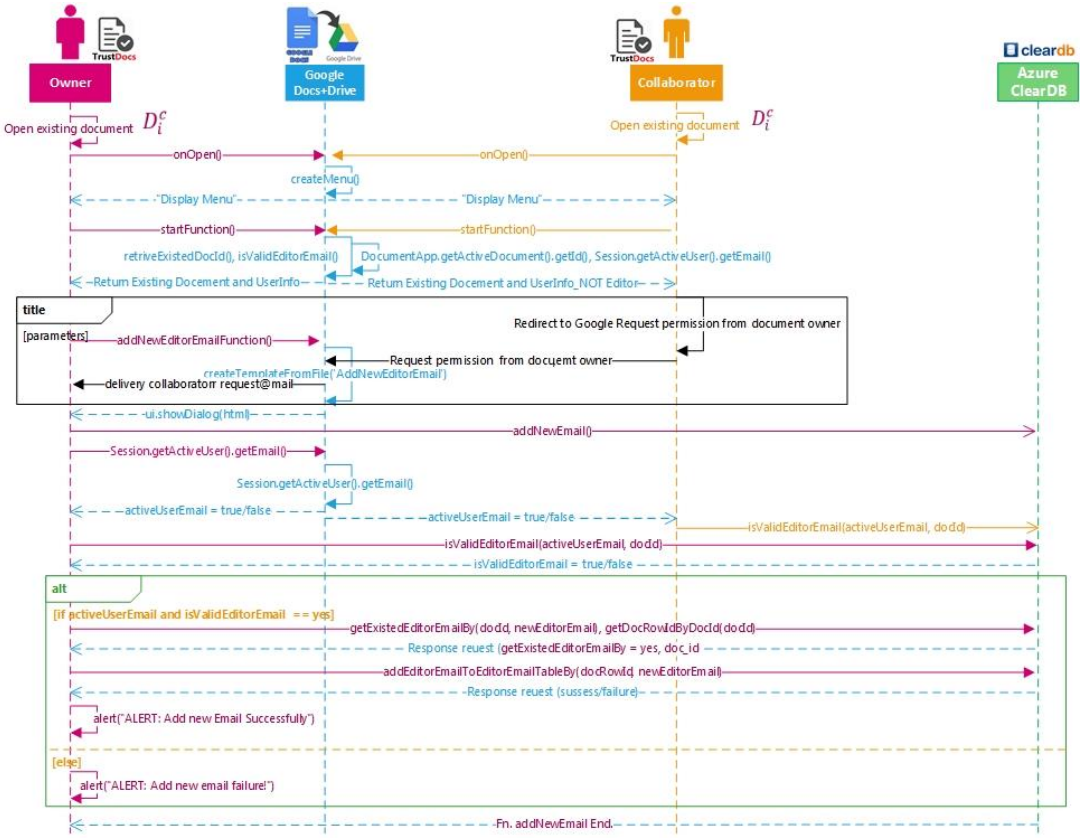
ในส่วนของสถานการณ์การจัดการแก้ไขไฟล์เอกสารกูเกิ้ลเก่า การทำงานของฟังก์ชั่นต่างๆ ยังคงคล้ายกับการจัดการไฟล์เอกสารกูเกิ้ลใหม่ อาจจะมีความแตกต่างกันเล็กน้อย การทำงานของฟังก์ชั่นมีการทำงานดังต่อไปนี้



รูปที่ 4.1.2 Function Execution Activity Diagram for Old Google Docs

4.1.1.3 Version Control Collaborative Environment

ในการทำงานของฟังก์ชั่นในสถานการณ์การ การจัดการไฟล์เอกสารกูเกิ้ลร่วมกัน ผู้ใช้งานร่วมทั้งหมดจะต้องติดตั้งโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ก่อนที่จะมีการจัดการข้อมูลสำคัญหรือข้อมูลลับของเจ้าของไฟล์ที่มีการแบ่งปันไฟล์เอกสารกูเกิ้ลเพื่อใช้งานร่วมกันให้ปลอดภัย ซึ่งการทำงานของฟังก์ชั่นต่างๆที่ผู้วิจัยได้พัฒนาโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ได้วิเคราะห์และออกแบบการทำงานดังต่อไปนี้



รูปที่ 4.1.3 Function Execution Activity Diagram for Google Docs in Collaborative

4.1.2 TrustDocs – Google Docs Add-on Function Description

4.1.2.1 New Google Docs Creation and Edition

onOpen() => Google Script API ที่ใช้สั่งการเปิดเอกสารกูเกิ้ล

createMenu() => Google Script API ที่ใช้สั่งสร้างเมนูใหม่เพิ่มเติมในเอกสารกูเกิ้ล

startFunction() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้เริ่มการทำงานของฟังก์ชั่นทั้งหมด

DocumentApp.getActiveDocument().getId(), isValidEditorEmail() => Google Script API ที่ใช้สั่งการรีเควสข้อมูลของเอกสารกูเกิ้ล คือ Doc_id และข้อมูลผู้เป็นเจ้าของไฟล์

retriveExistedDocId(), isValidEditorEmail() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กข้อมูลไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

[if(docCount == 0)], insertDocId(xx), addOwnerEmailToEditorEmails(), => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของไฟล์เอกสารกูเกิ้ลในฝั่ง KRaaS ถ้าไม่พบเอกสารดังกล่าวให้เพิ่มข้อมูลของเอกสารเข้าไป คือ Doc_id และ email ผู้เป็นเจ้าของไฟล์

getNewKeyFromDatabase() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีค่าการเรียกกุญแจลับใหม่ $\left[k_i^3\right]$ ==> $\left[k_j^0\right]$

savePlainText(welcomeText) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อสั่งให้มีการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับ ก่อนจะบันทึกข้อมูลดังกล่าวใน Google Drive

markKeyIsStartUpStatus1(), mapDocIdWithKey() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีค่าการเรียกกุญแจลับสถานะเริ่มต้น $\left[k_i^0\right] > \left[k_i^1\right]$

showDialogBox() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการสั่งให้แสดงหน้า Dialog Box

showSidebar(html) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการสั่งให้แสดงหน้า Side Bar

[if(docCount >= 1)], getLastMappedKeyByDocId() (), => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของไฟล์เอกสารกูเกิ้ลในฝั่ง KRaaS ถ้าพบเอกสารดังกล่าว ให้เรียกใช้งานค่ากุญแจลับที่ถูกจับคู่ไว้

[if (sessionKeyStartUpStatus==1)], getContent() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของค่ากุญแจลับไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

[if (sessionKeyStartUpStatus==2)], getContent() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของค่ากุญแจลับไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

DocumentApp.getActiveDocument().getText()/.getId() => Google Script API ที่ใช้สั่งการรีเควสข้อมูลของเอกสารกูเกิ้ล คือ Doc_id และข้อมูลสำคัญหรือข้อมูลลับ

4.1.2.2 Old Google Docs Edition

onOpen() => Google Script API ที่ใช้สั่งการเปิดเอกสารกูเกิ้ล

createMenu() => Google Script API ที่ใช้สั่งสร้างเมนูใหม่เพิ่มเติมในเอกสารกูเกิ้ล

startFunction() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้เริ่มการทำงานของฟังก์ชั่นทั้งหมด

DocumentApp.getActiveDocument().getId(), Session.getActiveUser().getEmail() => Google Script API ที่ใช้สั่งการรีเควสข้อมูลของเอกสารกูเกิ้ล คือ Doc_id และข้อมูลผู้เป็นเจ้าของไฟล์

retriveExistedDocId, isValidEditorEmail() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กข้อมูลไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

docCount >0/isValidEditorEmail = yes => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กข้อมูลไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

getDocRowIdByDocId(docId) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กข้อมูลไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

[if (sessionKeyStartUpStatus == 2)] => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของค่ากุญแจลับไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

getKeyWitchStartUpStatus2ByDocId(docId), => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีค่าการเรียกกุญแจลับสถานะดำเนินการ $\left[k_i^2\right]$ ที่ถูกจับคู่กับไฟล์เอกสารกูเกิ้ล $D_i^{c\prime}$ และผู้ใช้งานในฝั่ง KRaaS

markKeyFromStartUpStatus2To3(oldKey) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีค่าการเรียกกุญแจลับสถานะดำเนินการ $\left[k_i^2\right] > \left[k_i^3\right]$

getNewKeyFromDatabase() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีค่าการเรียกกุญแจลับใหม่ $\left[k_i^3\right] ==> \left[k_j^0\right]$

encrypt(plainText, newKey) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อสั่งให้มีการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับ

recordCryptoSpendTime(docId, keyId, e, time, #) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อสั่งให้มีการบันทึกเวลาเมื่อมีการเข้าหรือถอดรหัสลับข้อมูลสำคัญหรือข้อมูลลับ เพื่อเก็บผลทางการวิจัย

mapDocIdWithKeyByActiveUserEmail(docRowId, sessionKeyRowId, effectiveUserEmail), => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อสั่งให้มีการจับคู่ ค่ากุญแจลับใหม่ $\left[k_j^0\right]$ กับไฟล์เอกสารกูเกิ้ล $D_i^{c\prime}$ หลังจากมีการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับ

markKeyFromStartUpStatusNullTo2(newKey) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีค่าการเรียกกุญแจลับสถานะดำเนินการ $\left[k_i^0\right] > \left[k_i^2\right]$

savePlainText(plainText) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อสั่งให้มีการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับ ก่อนจะบันทึกข้อมูลดังกล่าวใน Google Drive

DocumentApp.getActiveDocument().setText(encrypted) => Google Script API และไลบรารี่ที่ผู้วิจัยขียนเอง ที่ใช้สั่งกเอกสารกูเกิ้ลเข้ารหัสลับและบันทึกข้อมูลสำคัญหรือข้อมูลลับในพื้นที่ Side Bar ลงสู่ Google Drive

[if (sessionKeyStartUpStatus == 1)] => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของค่ากุญแจลับไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

getContent() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการสั่งให้เอาข้อมูลใน Google Drive มาแสดงไฟล์เอกสารกูเกิ้ล

DocumentApp.getActiveDocument().getText()/.getId() => Google Script API ที่ใช้สั่งการรีเควสข้อมูลของเอกสารกูเกิ้ล คือ Doc_id และข้อมูลสำคัญหรือข้อมูลลับ

decrypt(encrypted, key) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อสั่งให้มีการถอดรหัสลับข้อมูลสำคัญหรือข้อมูลลับ

4.1.2.3 Collaborative Environment Edition

onOpen() => Google Script API ที่ใช้สั่งการเปิดเอกสารกูเกิ้ล

createMenu() => Google Script API ที่ใช้สั่งสร้างเมนูใหม่เพิ่มเติมในเอกสารกูเกิ้ล

startFunction() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้เริ่มการทำงานของฟังก์ชั่นทั้งหมด

DocumentApp.getActiveDocument().getId(), Session.getActiveUser().getEmail() => Google Script API ที่ใช้สั่งการรีเควสข้อมูลของเอกสารกูเกิ้ล คือ Doc_id และข้อมูลผู้เป็นเจ้าของไฟล์

retriveExistedDocId(), isValidEditorEmail() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กข้อมูลไฟล์เอกสารกูเกิ้ลและผู้ใช้งานในฝั่ง KRaaS

addNewEditorEmailFunction() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเพิ่มผู้ใช้งานร่วมในฝั่ง KRaaS

createTemplateFromFile('AddNewEditorEmail') => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการสั่งในการสร้างเมนูในการเพิ่มผู้ใช้งานร่วม

ui.showDialog(html) => Google Script API ที่ใช้สั่งการแสดง Dialog Box

addNewEmail() => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเพิ่มผู้ใช้งานร่วมในฝั่ง KRaaS

Session.getActiveUser().getEmail() => Google Script API ที่ใช้สั่งการเรียกข้อมูลเจ้าของไฟล์เอกสารกูเกิ้ล

isValidEditorEmail(activeUserEmail, docId) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็คผู้ใช้งาน และ doc_id ในฝั่ง KRaaS

[if activeUserEmail and isValidEditorEmail == yes] => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของผู้ใช้งานร่วมของไฟล์เอกสารกูเกิ้ลในฝั่ง KRaaS

getExistedEditorEmailBy(docId, newEditorEmail), getDocRowIdByDocId(docId) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเช็กสถานะของผู้ใช้งานร่วมของไฟล์เอกสารกูเกิ้ลในฝั่ง KRaaS

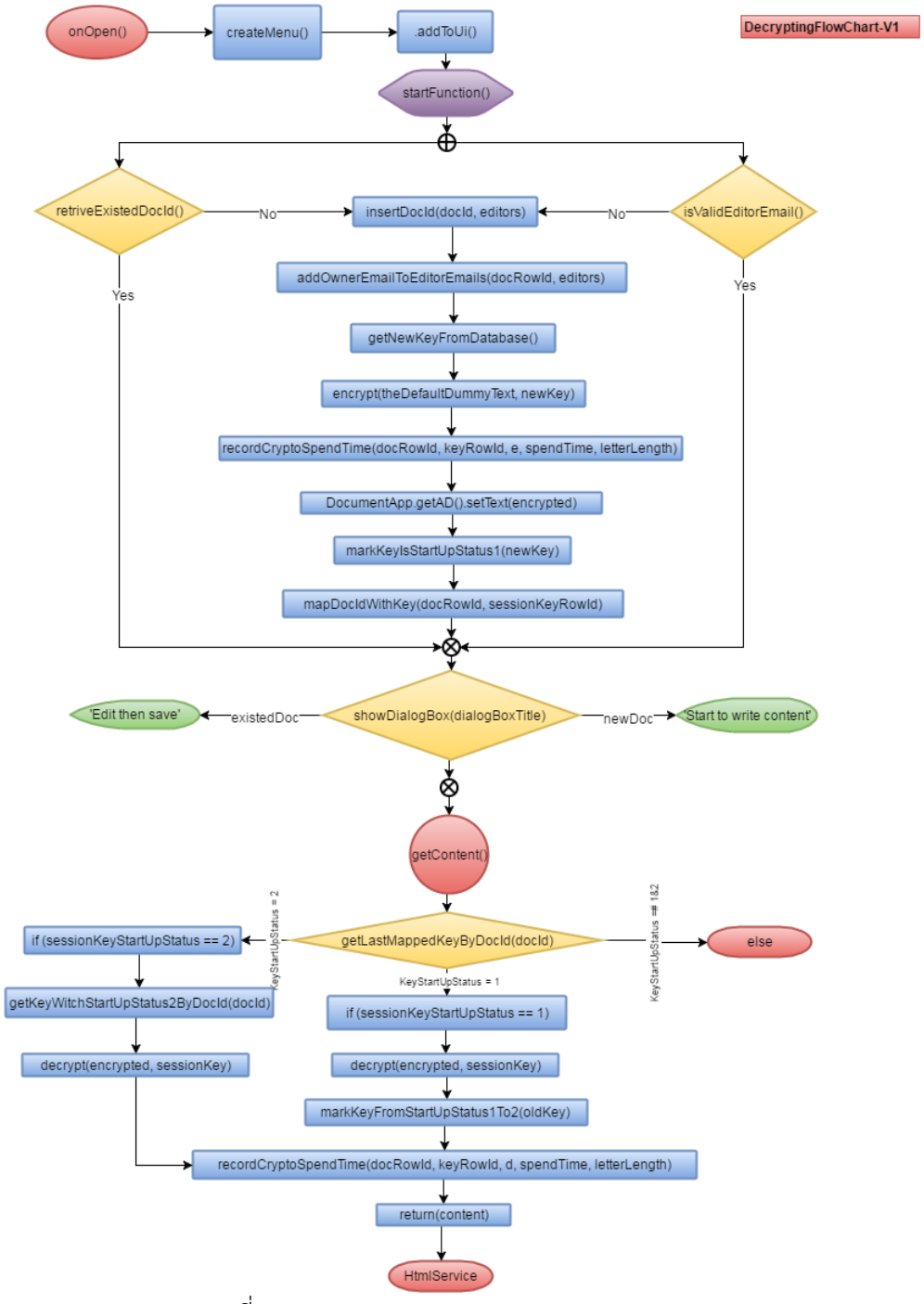
addEditorEmailToEditorEmailTableBy(docRowId, newEditorEmail) => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการเพิ่มผู้ใช้งานร่วมของไฟล์เอกสารกูเกิ้ลในฝั่ง KRaaS

alert("ALERT: Add new Email Successfully") => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการแจ้งเตือนเมื่อมีการเพิ่มผู้ใช้งานร่วมสำเร็จ

[else], alert("ALERT: Add new email failure!") => ไลบรารี่ที่ผู้วิจัยเขียนเองเพื่อให้มีการแจ้งเตือนเมื่อมีการเพิ่มผู้ใช้งานร่วมไม่สำเร็จ

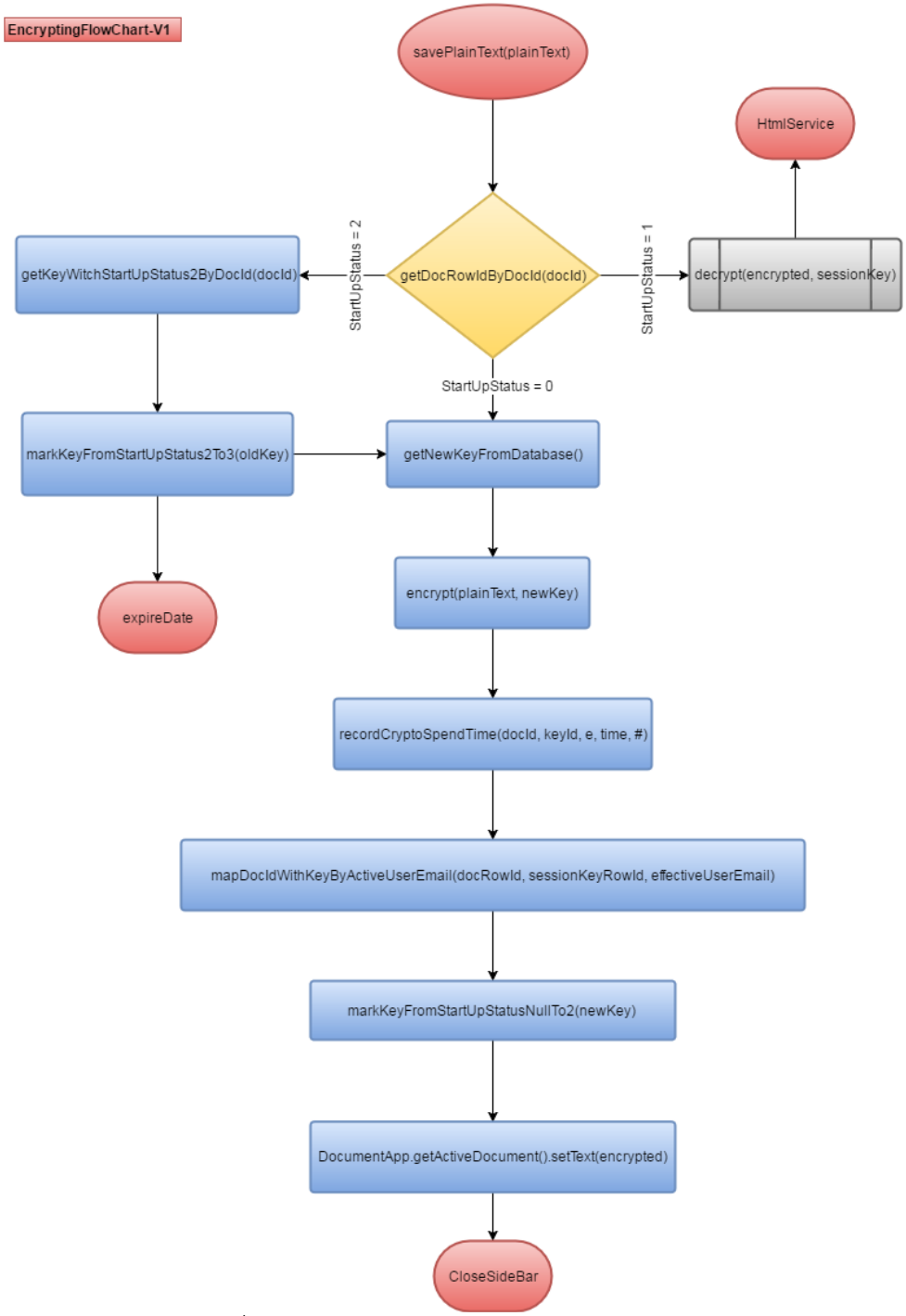
4.1.3 TrustDocs – Google Docs Add-on Function Flow Chart

4.1.3.1 Decryption Flow Chart



รูปที่ 4.1.3.1 Decryption Flow Chart Diagram

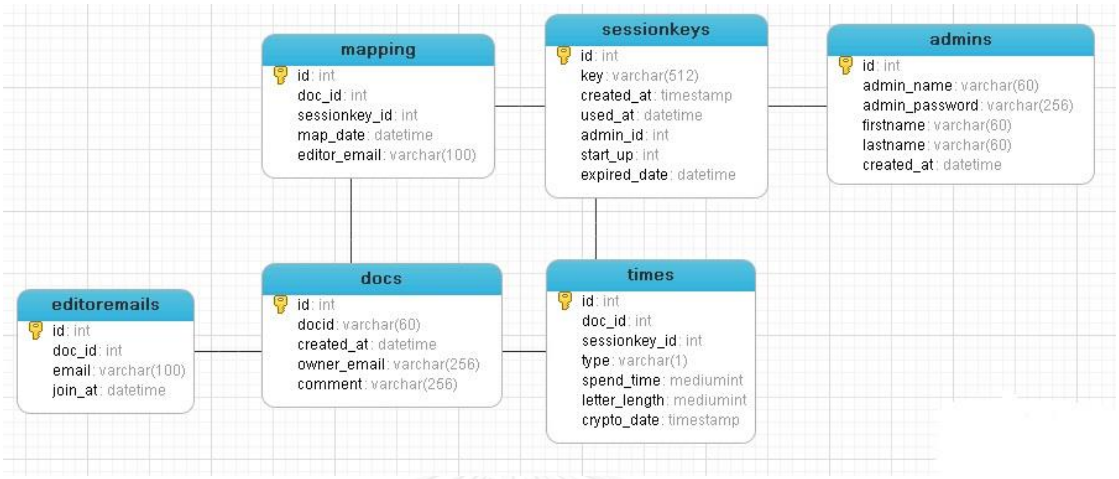
4.1.3.2 Encryption Flow Chart



รูปที่ 4.1.3.2 Encryption Flow Chart Diagram

4.2. การพัฒนาเครื่องมือในส่วนของ Cloud Key-Repository-as-a-Service

4.2.1 ER Diagram



รูปที่ 4.2.1 Key-Repository-as-a-Service ER-Diagram

4.2.2 Related Table and Parameter Description of KRaaS Database

4.2.2.1 ตาราง “admins” (Table name: admins)

ตารางชื่อ “admins” คือ ตารางที่ใช้เก็บข้อของผู้ดูแลระบบ KRaaS

- ตาราง admins ประกอบด้วย

id	คอลัมน์เก็บค่าไอดีของตาราง admins
admin_name	คอลัมน์เก็บ username ของผู้ดูแลระบบ KRaaS
admin_password	คอลัมน์เก็บ username ของผู้ดูแลระบบ KRaaS
firstname	คอลัมน์เก็บชื่อจริง ของผู้ดูแลระบบ KRaaS
lastname	คอลัมน์เก็บชื่อจริง ของผู้ดูแลระบบ KRaaS
create_at	คอลัมน์เก็บค่า date ที่มีการสร้างผู้ดูแลระบบ KRaaS

4.2.2.2 ตาราง “sessionkeys” (Table name: sessionkeys)

ตารางชื่อ “sessionkeys” คือ ตารางที่ใช้เก็บข้อมูลค่ากุญแจลับทั้งหมดเพื่อเตรียมในการเรียกใช้งานเพื่อทำการเข้าและถอดรหัสของไฟล์เอกสารกูเกิ้ลที่มีการงานผ่านโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

- ตาราง sessionkeys ประกอบด้วย

id	คอลัมน์เก็บค่าไอดีของตาราง sessionkeys
key	คอลัมน์เก็บค่าของค่ากุญแจลับขนาด 256 บิต
create_at	คอลัมน์เก็บค่า date ที่มีการสร้างหรือเอาค่ากุญแจเข้าระบบ KRaaS
used_at	คอลัมน์เก็บค่า date ที่มีการใช้ค่ากุญแจ
admin_id	คอลัมน์เก็บค่าไอดีของผู้ดูแลระบบ KRaaS
start_up	คอลัมน์เก็บค่า State หรือสถานะของค่ากุญแจลับ
expired_date	คอลัมน์เก็บค่า date ที่ค่ากุญแจหมดอายุ

4.2.2.3 ตาราง “mapping” (Table name: mapping)

ตารางชื่อ “mapping” คือ ตารางที่ใช้เก็บข้อมูลที่เกี่ยวกับการจับคู่ค่ากุญแจลับกับไฟล์เอกสารกูเกิ้ลสำหรับการเข้าและถอดรหัสของไฟล์เอกสารกูเกิ้ลที่มีการงานผ่านโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

- ตาราง times ประกอบด้วย

id	คอลัมน์เก็บค่าไอดีของตาราง mapping
key_id	คอลัมน์เก็บค่าไอดีของค่ากุญแจลับ
doc_id	คอลัมน์เก็บค่าไอดีของเอกสารกูเกิ้ล
map_date	คอลัมน์เก็บค่า date ที่มีการจับคู่
editor_email	คอลัมน์เก็บค่าอีเมลของผู้ใช้งานที่มีการแก้ไขเอกสารกูเกิ้ล

4.2.2.4 ตาราง “times” (Table name: times)

ตารางชื่อ “times” คือ ตารางที่ใช้เก็บข้อมูลที่เกี่ยวกับเวลาในการทำการเข้าและถอดรหัสของไฟล์เอกสารกูเกิ้ลที่มีการงานผ่านโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ซึ่งตารางนี้จัดเตรียมไว้ทำการเก็บค่าไว้ในส่วนการปรเมิณเท่านั้น ซึ่งเป็นส่วนหนึ่งในการทำวิจัย

- ตาราง times ประกอบด้วย

id	คอลัมน์เก็บค่าไอดีของตาราง times
doc_id	คอลัมน์เก็บค่าไอดีของเอกสารกูเกิ้ล
sessionkey_id	คอลัมน์เก็บค่าไอดีของค่ากุญแจลับ
type	คอลัมน์เก็บค่า ประเภทของการดำเนินการเข้าหรือถอดรหัสลับ
spend_time	คอลัมน์เก็บค่าระยะเวลาที่ใช้ในการเข้าหรือถอดรหัสลับ

letter_length คอลัมน์เก็บค่า จำนวนตัวอักษรในการเข้าหรือถอดรหัสลับ

crypto_date คอลัมน์เก็บค่า date ที่มีการเข้าหรือถอดรหัสลับ

4.2.2.5 ตาราง “docs” (Table name: docs)

ตารางชื่อ “docs” คือ ตารางที่ใช้เก็บข้อมูลที่เกี่ยวข้องเอกสารกูเกิ้ลที่มีการงานผ่านโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

- ตาราง docs ประกอบด้วย

id คอลัมน์เก็บค่าไอดีของตาราง docs

docid คอลัมน์เก็บค่าไอดีของเอกสารกูเกิ้ล

create_at คอลัมน์เก็บค่า date ที่มีการสร้างไฟล์เอกสารกูเกิ้ลด้วย TrustDocs

owner_email คอลัมน์เก็บค่าอีเมลของผู้ใช้งานผู้เป็นเจ้าของไฟล์เอกสารกูเกิ้ล

join_at คอลัมน์เก็บค่า date ที่มีการร่วมเข้ามาเป็นผู้ใช้งานร่วม

4.2.2.6 ตารางชื่อ “editoremail” (Table name: editoremail)

ตารางชื่อ “editoremail” คือ ตารางที่ใช้เก็บข้อมูลที่เกี่ยวข้องของผู้ใช้งานทั้งหมดที่ใช้งานร่วมกับไฟล์เอกสารกูเกิ้ล รายละเอียดข้อมูลแต่ละส่วนประกอบด้วย

- ตาราง editoremail ประกอบด้วย

id คอลัมน์เก็บค่าไอดีของตาราง editoremail

doc_id คอลัมน์เก็บค่าไอดีของเอกสารกูเกิ้ล

email คอลัมน์เก็บค่าอีเมลของผู้ใช้งานที่สามารถแก้ไขเอกสารกูเกิ้ล

join_at คอลัมน์เก็บค่า date ที่มีการร่วมเข้ามาเป็นผู้ใช้งานร่วมของเอกสารกูเกิ้ล

บทที่ 5

ผลการทดลอง

ในบทนี้จะกล่าวถึงผลการทดลอง โดยมีการเปรียบเทียบกับงานวิจัยที่มีการนำเสนอหลักการเพื่อให้เอกสารออนไลน์มีความปลอดภัยเหมือนกัน แต่แตกต่างการในเชิงหลักการ (Mechanism) และผลทางทดลองในเชิงเวลาที่เสียไป เมื่อมีการดำเนินการเข้า และถอดรหัสลับซึ่งมีรายละเอียดดังต่อไปนี้

5.1. การเปรียบเทียบด้านความสามารถ

ในปัจจุบันมีผู้พัฒนาซอฟต์แวร์หลายรายได้พัฒนาซอฟแวร์ในเชิงการค้าที่สนับสนุนการรักษาความลับให้กับเอกสารออนไลน์ที่ข้อมูลของผู้ใช้งานงานจะถูกเก็บอยู่ในความดูแลของผู้ให้บริการ SaaS Storage แต่ซอฟต์แวร์เหล่านั้นยังคงมีข้อจำกัดในด้านต่างๆ ที่ทำให้ผู้ใช้งานสามารถที่เลือกวางใจ หรือไม่วางใจต่อการใช้งาน SaaS Storage รวมถึงความยุ่งยากในการใช้งานที่ผู้ใช้งานจะต้องรับภาระเพิ่ม หากต้องการทำให้ข้อมูลสำคัญหรือข้อมูลของตนเกิดความปลอดภัย อาทิเช่น การจัดการค่ากุญแจลับด้วยตัวเอง ซึ่งแน่นอนว่าจะต้องมีเหตุการณ์ที่ผู้ใช้งานลืมค่ากุญแจลับของตนที่ทำการเข้ารหัสข้อมูลสำคัญหรือข้อมูลลับ โดยเหตุการณ์เช่นนี้ ผู้ใช้งานจะต้องสูญเสียข้อมูลสำคัญหรือข้อมูลลับของตนไปในกรณีการลืมค่ากุญแจลับแบบไม่สามารถกู้คืนได้

ดังนั้นผู้วิจัยได้มีการ survey ซอฟต์แวร์ในเชิงการค้าที่มีชื่อเสียง และเป็นที่นิยมที่สนับสนุนการรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมไม่เชื่อถือต่อผู้ให้บริการกูเกิ้ล ที่ใช้งาน SaaS Storage คือ Google Drive นำมาเปรียบเทียบรูปแบบ กับโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs (TrustDocs – Google Docs Add-on) อาทิเช่น DocSecrets ที่เป็นโปรแกรมเสริมเอกสารกูเกิ้ลเหมือนกัน แต่จุดมุ่งหมายที่ต้องการนำเสนอคือ ไม่ใช่ทุกคำในเอกสารกูเกิ้ลจะต้องเป็นความลับ จึงทำให้ DocSecrets มีความสามารถในการเลือกคำ หรือประโยคในการทำการเข้าและถอดรหัสลับได้ แต่ข้อเสียที่สำคัญก็ยังคงมีอยู่ ได้แก่ความยุ่งยากในการจัดการค่าคีย์ ซึ่งข้อเสียดังกล่าวยังเป็นข้อเสียของซอฟต์แวร์ในเชิงการค้าชื่อดังเจ้าอื่น เช่น BoxCrypto และ Fogpad ที่ลักษณะในเชิงกายภาพของซอฟต์แวร์จัดอยู่ในรูปแบบ Web Application ด้วยข้อเสียของซอฟต์แวร์ในเชิงการค้าทั้งหมดที่ได้กล่าวถึง นั่นคือเจ้าของไฟล์เอกสารจะต้องบริหารจัดการ หรือ จำค่ากุญแจลับด้วยตัวเอง ซึ่งมีความเสี่ยงอย่างมากในการลืมค่ากุญแจลับ และพฤติกรรมของผู้ใช้งานที่มักจะใช้ค่ากุญแจลับเดิมๆ ทุกครั้งหรือทุกไฟล์ที่มีการเข้าหรือถอดรหัสลับซึ่งจัดได้ว่ามีความเสี่ยงต่อการพยายามคาดเดาค่ากุญแจลับจากผู้ให้บริการ

ตารางที่ 3. Comparison table of service classification

Name	Utility Type	Key Management
TrustDocs	Google Add-on	Auto-Key gen and Distribution
TwinCloud	Software	Auto-Key gen and Distribution
DocsSecrets	Google Add-on	Manual-Key generation by user
Fogpad	Google App	Manual-Key generation by user
BoxCrypto.	Google App	Manual-Key generation by user

TwinCloud คืองานวิจัยที่นำเสนอหลักการรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมไม่เชื่อถือ ด้วยหลักการการเลือกใช้งานผู้ให้บริการมากกว่า 1 รายเหมือนกัน แต่แตกต่างที่รูปแบบความปลอดภัยที่นำเสนอ ซึ่งได้เปรียบเทียบอยู่ในตารางที่ 5

ตารางที่ 4. ตารางการเปรียบเทียบเชิงหลักการและกระบวนการของงานวิจัย

TWINCLOUD	TRUSTDOCS ADD-ON
1. มีการนำเสนอหลักการวิทยาการรหัสลับและการกระจายค่ากุญแจลับ ผ่านโปรโตคอล SSL ที่มีการสนับสนุนการเลือกใช้งานผู้ให้บริการ SaaS Storage มากกว่า 1 ราย ได้แก่ Google Drive และ Dropbox 2. มีการสนับสนันกลไกการสร้างค่ากุญแจลับด้วยหลักการการสุ่มที่มีประสิทธิภาพด้วยเครื่องมือ Java Key Generator ด้วยการนำข้อมูลส่วนตัวของผู้ใช้งานมาทำการสร้างค่าพาสเวิร์ดในการพิสูจน์ตัวตน SaaS Storage ของผู้ให้บริการทั้งสองราย และผู้ใช้งานไม่จำเป็นต้องมีการ Login เพื่อพิสูจน์ตัวตนทุกครั้งที่มีการใช้งาน TwinCloud 3. การกระจายค่ากุญแจลับจะเริ่มต้นก็ต่อเมื่อมีการลงทะเบียนระบบ SaaS storage เสร็จ	1. มีการนำเสนอหลักการวิทยาการรหัสลับและการกระจายค่ากุญแจลับ ผ่านโปรโตคอล SSL ที่มีการสนับสนุนการเลือกใช้งานผู้ให้บริการ SaaS Storage มากกว่า 1 ราย ได้แก่ Google Drive และ Cloud 3rd Party ได้แก่ ClearDB 2. มีการสนับสนุนหลักการการกระจายค่ากุญแจลับที่มีการทำงานคล้ายกับ KDC หรือ PKI ซึ่งผู้ใช้งานจะต้อง sign ระบบ KRaaS เพื่อให้เกิดความวางใจต่อผู้ให้บริการ สำหรับหลักการการสร้างค่ากุญแจลับนั้นผู้วิจัยไม่ได้ให้ความสำคัญมากกว่าหลักการอื่นๆ แต่ก็ยอมรับว่าหลักการการสร้างค่ากุญแจลับดังกล่าวมีสำคัญมาก 3. ผู้ดูแลระบบ Key-Repository-as-a-Service สามารถเห็นข้อมูลส่วนตัวของผู้ใช้งานได้ อาทิเช่น ค่ากุญแจลับต่างๆที่ถูกใช้งาน หมายเลขประจำตัวเอกสารกูเก้ิลหรือ ชื่อบัญชีกูเก้ิล แต่ผู้ดูแลระบบ

เรียบร้อยแล้วในลักษณะอัตโนมัติด้วยโปรโตคอล OAuth2.0 และ ฟังก์ชัน hash ในการเข้ากระบวนการพิสูจน์ตัวตนด้วยการนำข้อมูลส่วนตัวของผู้ใช้งานในการสร้างพาสเวิร์ดทำให้ผู้ใช้งานนั้นไม่ต้องทำการ login ใดๆทั้งสิ้นในการใช้งาน TwinCloud *งานวิจัยในอนาคต จะพัฒนาขีดความสามารถในวิทยาการรหัสลับด้วยอัลกอริทึมที่มีความเหมาะสมมากกว่า AES, และใช้หลักการ One-time pads มาช่วยเพิ่มประสิทธิภาพในความปลอดภัยด้านกระบวนการกระจายค่ากุญแจลับ นักวิจัยได้มีการหมายเหตุค่ากุญแจลับที่มีขนาดยาวจะมีผลต่อปัญหาในการเข้ากระบวนการวิทยาการรหัสลับเล็กน้อยและสามารถที่จะจัดเก็บค่ากุญแจลับเหล่านั้นในผู้บริการ Dropbox ได้ง่ายในการแบ่งปันค่ากุญแจลับเหล่านั้นในรูปแบบการใช้งานร่วมกัน ท้ายที่สุดนักวิจัยได้มีการวางแผนที่จะออกแบบการเลือกใช้ผู้ให้บริการมากกว่า 2 ในอนาคต	KRaaS ไม่สามารถที่จะเห็นข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานได้เนื่องจากไม่มีค่าพาสเวิร์ดของบัญชีกูเกิ้ลซึ่งกลไกความปลอดภัยนี้ได้รับความดูแลอย่างใกล้ชิดจากผู้ให้บริการทางกูเกิ้ลเอง **สิ่งที่สำคัญที่สุดในการนำเสนอหลักการและกลไกของการกระจายค่ากุญแจลับของผู้วิจัยนั้น ซึ่งได้นำเสนอหลักการการกระจายค่ากุญแจลับที่มีลักษณะการทำงานคล้ายหลักการ One-time pads (OTP) ในวงจรการกระจายค่ากุญแจลับในงานชิ้นนี้เรียบร้อยแล้ว แต่ละค่ากุญแจลับจะสามารถถูกนำมาใช้ในกระบวนการเข้ารหัสลับได้เพียง 1 ครั้งเท่านั้น ถ้ามีการสั่งให้มีการทำกระบวนการการเข้ารหัสลับอีกครั้ง โปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs จะทำการสั่งให้มีการสิ้นสุดการใช้งานค่ากุญแจลับดังกล่าว และมีการเรียกการใช้งานค่ากุญแจใหม่ทันทีในกระบวนการการเข้ารหัสทุกๆครั้ง ในส่วนของการถอดรหัสลับของมูลนั้น ตราบใดที่ผู้ใช้งานยังไม่มีการสั่งให้มีการเข้ารหัสลับครั้งใหม่ ค่ากุญแจลับที่จะถูกเรียกใช้งานในการถอดรหัสลับข้อมูลสำคัญหรือข้อมูลลับนั้นจะยังคงเป็นค่ากุญแจลับตัวเดิม

5.2 ผลการทดลองเชิงเวลา

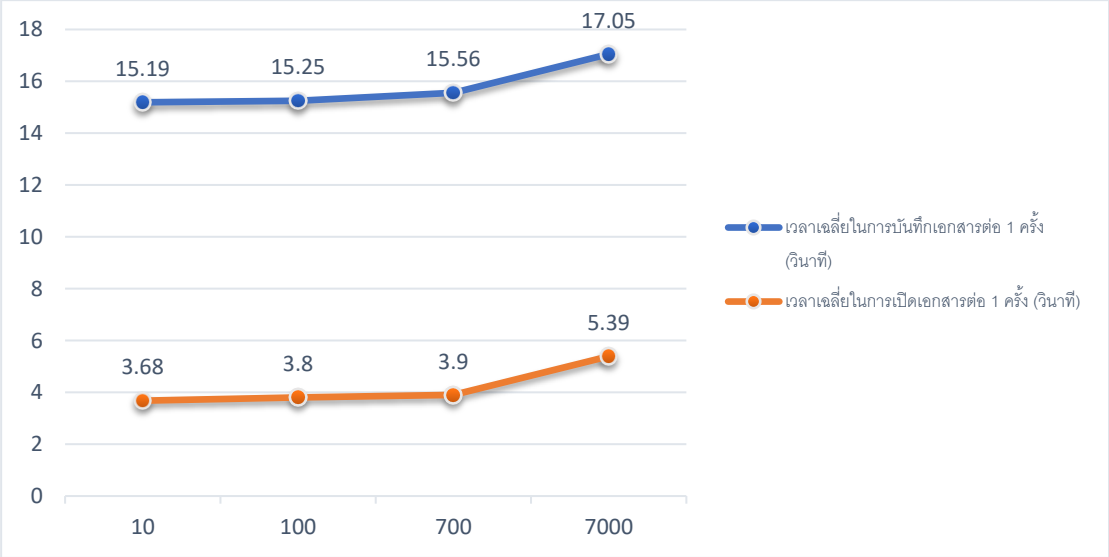
การนำวิทยาการรหัสลับมาใช้เพื่อความปลอดภัยในการใช้งานเอกสารกูเกิ้ล ซึ่งผู้วิจัยได้นำหลักการที่ได้จากการนำเสนอโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs มาทำการทดลองการเข้าและถอดรหัสลับ โดยมีการกระจายค่ากุญแจลับจาก KRaaS (ClearDB) ไปยังเว็ปบราวเซอร์(เครื่อง

คอมพิวเตอร์) ของผู้ใช้งานผ่านช่องทางที่ปลอดภัย คือ SSL-SQL ซึ่งจะทำให้เกิดการสูญเสียเวลามากขึ้น ซึ่งการเข้าและถอดรหัสลับ ผู้วิจัยออกแบบการทดลอง ด้วยความแตกต่างของขนาดข้อมูลในไฟล์เอกสารกูเกิ้ลคือ จำนวน 10, 100, 700 และ 70000 ตัวอักษร ด้วยค่ากุญแจลับอัลกอริทึม AES 256 บิต นำมาเข้าและถอดรหัสลับจำนวน 1000 ครั้ง ในแต่ละขนาดของตัวอักษร เพื่อหาค่าเฉลี่ยโดย มีผลการทดลองดังต่อไปนี้

5.2.1 ผลการทดลองประสิทธิภาพในเชิงเวลาทั้งกระบวนการของโปรแกรมเสริมกูเกิ้ล TrustDocs ในการเปิดเอกสารและการบันทึกเอกสารลงสู่กูเกิ้ลไดรฟ

ขนาดข้อมูลไฟล์เอกสารกูเกิ้ล	เวลาเฉลี่ยในการบันทึกเอกสาร	เวลาเฉลี่ยในการเปิดเอกสาร
10 ตัวอักษร	15.19 วินาที	3.68 วินาที
100 ตัวอักษร	15.25 วินาที	3.80 วินาที
700 ตัวอักษร	15.56 วินาที	3.90 วินาที
7000 ตัวอักษร	17.05 วินาที	5.39 วินาที

ตารางที่ 5 ผลการทดลองประสิทธิภาพในเชิงเวลาทั้งกระบวนการเปิดและบันทึกเอกสาร



รูปที่ 5.2.1 กราฟผลการทดลองประสิทธิภาพในเชิงเวลาทั้งกระบวนการเปิดและบันทึกเอกสาร

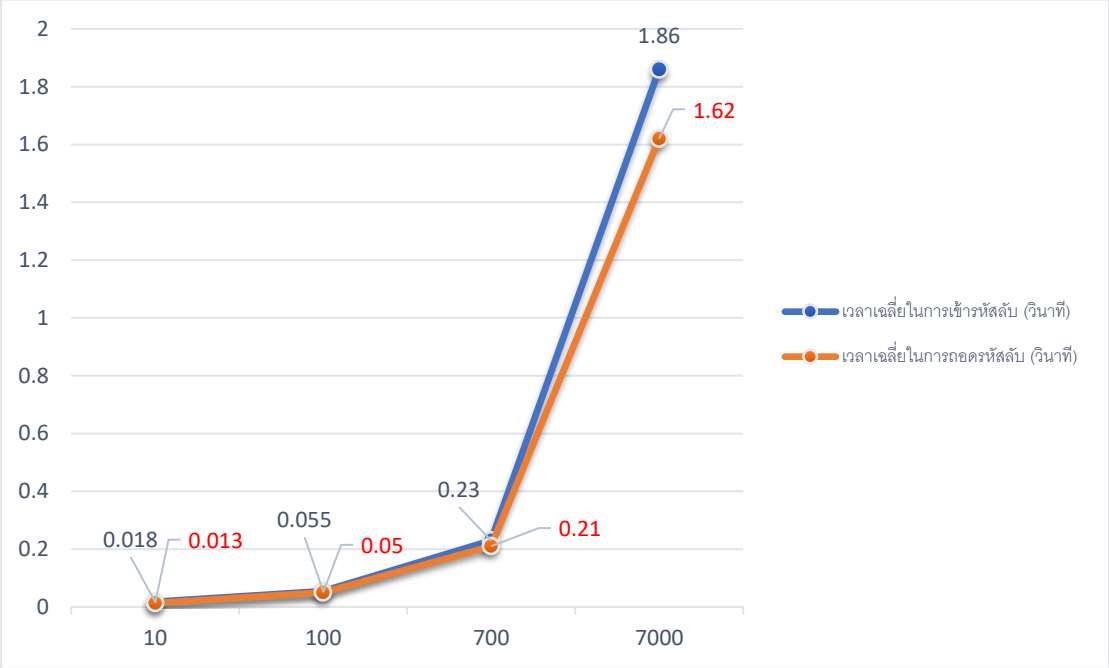
ในส่วนกระบวนการการบันทึกเอกสาร จะเสียประสิทธิภาพทางด้านเวลาสูงกว่ากระบวนการการเปิดเอกสาร เนื่องจากกระบวนการการบันทึกเอกสารจะประกอบกระบวนการย่อยที่มากกว่า อันได้แก่ การเข้ารหัสลับ การทำการเรียกใช้ค่ากุญแจลับใหม่ การทำการสิ้นสุดค่ากุญแจลับเดิม การจับคู่ค่ากุญแจลับใหม่ และการเปลี่ยนค่าสถานะค่ากุญแจลับหลังจากดำเนินการการเข้ารหัสลับเรียบร้อยแล้ว แต่ในส่วนของการเปิดเอกสารนั้น จะมีกระบวนการย่อยที่ก่อให้เกิดการสูญเสียประสิทธิภาพ

ทางด้านเวลาแค่กรณีการถอดรหัสลับ และการเรียกใช้งานค่ากุญแจลับจาก KRaaS เพื่อทำการถอดรหัสลับเท่านั้น ซึ่งเห็นได้ชัดว่า ประสิทธิภาพทางด้านเวลาของสองกระบวนการนั้นมีความแตกต่างอย่างสิ้นเชิง

5.2.2 ผลการทดลองประสิทธิภาพในเชิงเวลาในส่วนของการทำวิทยาการรหัสลับเท่านั่น

ขนาดข้อมูลไฟล์เอกสารกูเกิ้ล	เวลาเฉลี่ยในการเข้ารหัสลับ	เวลาเฉลี่ยในการถอดรหัสลับ
10 ตัวอักษร	0.018 วินาที	0.013 วินาที
100 ตัวอักษร	0.055 วินาที	0.050 วินาที
700 ตัวอักษร	0.230 วินาที	0.210 วินาที
7000 ตัวอักษร	1.860 วินาที	1.620 วินาที

ตารางที่ 6 ผลการทดลองประสิทธิภาพในเชิงเวลาในส่วนของการทำวิทยาการรหัสลับเท่านั่น



รูปที่ 5.2.2 กราฟผลการทดลองประสิทธิภาพในเชิงเวลาในส่วนของการทำวิทยาการรหัสลับเท่านั่น

เวลาเฉลี่ยในการทำวิทยาการรหัสลับสำหรับโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs จะแปรผันตรงกับขนาดของตัวอักษรที่เข้ากระบวนการ ซึ่งสามารถอธิบายได้ว่ายิ่งข้อมูลสำคัญหรือข้อมูลลับข้อผู้ใช้งานมีขนาดใหญ่มากเพียงใด ระยะเวลาในการทำวิทยาการรหัสลับก็จะต้องใช้จำนวนเวลามากขึ้นตามลำดับ

จากกราฟผลการทดลอง ประสิทธิภาพทางด้านเวลาของการทดลองประสิทธิภาพในเชิงเวลา ซึ่งผลการทดลองทั้งกระบวนการเปิดและบันทึกเอกสารนั้น จะสูญเสียประสิทธิภาพในเชิงเวลาเป็นจำนวนมากเนื่องจากการรับส่งข้อมูลในกระบวนการการกระจายค่ากุญแจลับ มีการรับส่งข้อมูลในช่องทางที่ปลอดภัยด้วยโปรโตคอลเอสเอสแอลประเภทข้อมูลในรูปแบบโครงสร้างฐานข้อมูล (SSL-SQL Database) ซึ่งเป็นกระบวนการรับที่ปลอดภัย แต่สิ่งที่จะต้องแลก (Trade-Off) คือระยะเวลาในการรับส่งข้อมูลที่เพิ่มมากขึ้นเป็นพิเศษ ดังนั้นเมื่อเปรียบเทียบผลการทดลองทางด้านประสิทธิภาพในเชิงเวลาระหว่าง การทดลองประสิทธิภาพในเชิงเวลาในส่วนของการทำวิทยาการรหัสลับเท่านั่น กับการทดลองประสิทธิภาพในเชิงเวลาทั้งกระบวนการเปิดเอกสารและการบันทึกเอกสารลงสู่กูเกิ้ลไดรฟจะมีความแตกต่างกันมากเป็นพิเศษ

5.2.3 การประเมินเชิงวิเคราะห์การค่าประสิทธิภาพในเชิงเวลา (Estimate Time Analysis)

สำหรับขนาดของข้อมูลที่มีการรับส่งไปมา ระหว่าง TrustDocs (Client Side) และ KRaaS ในกระบวนการการกระจายค่ากุญแจลับนั้น เป็นการรับส่งข้อมูลประเภท SQL Database (JDBC) จัดได้ว่าเป็นข้อมูลที่มีขนาดเล็กมาก และขนาดของข้อมูลเท่าๆกัน ในของแต่ละประเภทและระยะเวลาในการรับส่งข้อมูล อาทิเช่น ค่ากุญแจลับจะมีขนาด 32 Byte หรือการเปลี่ยนค่าสถานะของค่ากุญแจก็จะมีขนาดแค่ 1 Byte เป็นต้น จึงทำให้ไม่ส่งผลต่อประสิทธิภาพทางด้านเวลามากนัก กล่าวคือเวลาที่ใช้ในการรับส่งระหว่าง TrustDocs และ KRaaS จะมีขนาดและระยะเวลาเท่ากัน (Fix) ซึ่งเหตุการณ์ที่มีผลต่อประสิทธิภาพทางด้านเวลาจะแปรผันตรง (vary) คือขนาดของข้อมูลนั่นเอง

ขนาดหรือความเร็วของระบบเครือข่ายอินเตอร์เน็ตจัดได้ว่าเป็นปัจจัยอย่างหนึ่งที่มีผลกระทบต่อการประเมิณการค่าประสิทธิภาพในเชิงเวลาของการทำงานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs แต่ผู้วิจัยไม่ได้ทำการทดลองในปัจจัยดังกล่าวเนื่องจากข้อจำกัดทางด้านรีสอร์ท (Resource) ของผู้วิจัยเองไม่สามารถหาความเร็วอินเตอร์เน็ตที่หลากหลายในการทดลองได้ในการทำวิจัยในเฟสนี้

ไม่สามารถปฏิเสธได้ว่า ขนาดสเปกของเครื่องคอมพิวเตอร์นั้นมีผลกระทบต่อการประเมิณการค่าประสิทธิภาพในเชิงเวลาของการทำงานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ซึ่งแน่นอนว่าถ้าผู้วิจัยใช้เครื่องคอมพิวเตอร์ที่มีขนาดสเปกสูง ก็จะทำให้สามารถได้รับผลลัพธ์จากการทดลองประสิทธิภาพทางด้านเวลาที่ดีขึ้น และจากผลการทดลองของการทำการประเมิณค่าประสิทธิภาพในเชิงเวลาในการใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ได้ว่า เวลาเฉลี่ยในการทำวิทยาการรหัสลับสำหรับโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs จะแปรผันตรงกับขนาดของข้อมูลสำคัญหรือข้อมูลลับในการทำวิทยาการรหัสลับ

ผู้วิจัยได้วิเคราะห์และสรุปการประเมิณการค่าประสิทธิภาพในเชิงเวลาของการทำงานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ดังต่อไปนี้

5.2.3.1 การประเมิณการค่าประสิทธิภาพในเชิงเวลาของการเปิดเอกสารต่อจำนวน 1 ครั้ง

กระบวนการของการเปิดเอกสารกูเกิ้ลด้วยโปรแกรมเสริม TrustDocs นั้น จะสูญเสียค่าประสิทธิภาพเชิงเวลาในกระบวนการการถอดรหัสลับและกระบวนการกระจายค่ากุญแจลับจาก KRaaS ไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งานจำนวน 3 ครั้ง ผ่านช่องทางที่ปลอดภัย SSL-SQL ได้แก่

- เหตุการณ์การ Query ความถูกต้องของข้อมูลส่วนตัวของผู้ใช้งานใน KRaaS อาทิเช่น Doc_Id และ Email

- เหตุการณ์การ Query ที่มีต่อเนื่องจากเหตุการณ์ที่แล้ว ของข้อมูลที่เกี่ยวข้อง อาทิเช่น ค่ากุญแจลับ (Session Key) ที่ได้รับการจับคู่กับ Doc_Id
- เหตุการณ์การจากความต่อเนื่องจากเหตุการณ์ที่แล้ว ของค่าสถานะของค่ากุญแจลับที่ถูกจับคู่ ถ้าค่าสถานะของค่ากุญแจลับเท่ากับ 2 ให้มีการเรียกค่ากุญแจลับมาที่เครื่องของผู้ใช้งาน

สามารถสรุปเป็นสมการดังต่อไปนี้

$$t_{load} = 3 * (t_{network}) + t_{decrypt}\ (N_{text})$$

$$t_{network} = \frac{t_{load} - t_{decrypt}}{3}$$

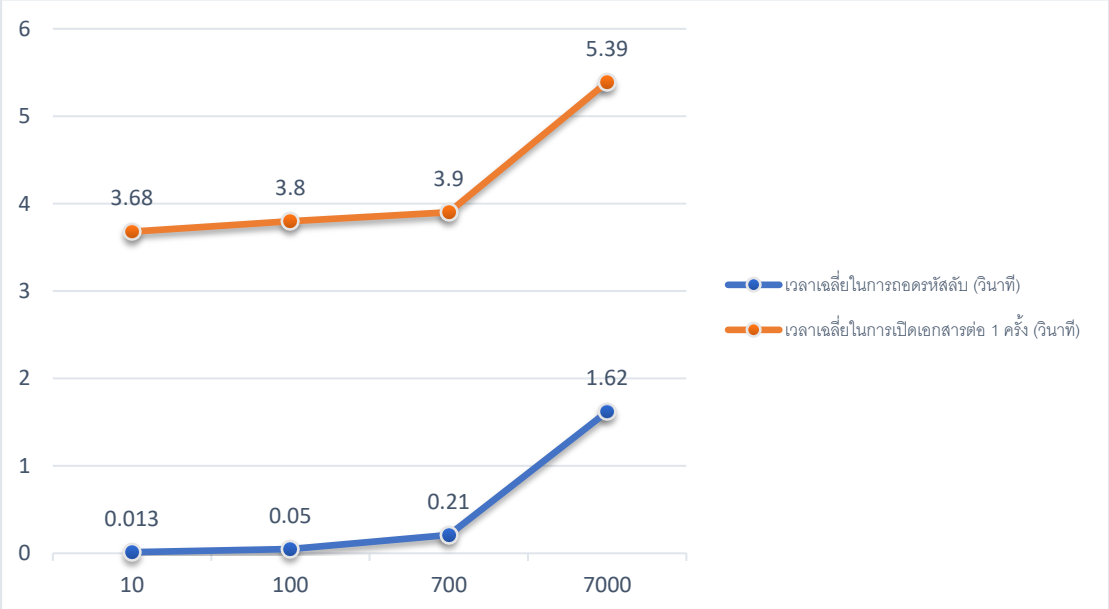
ซึ่งความหมายของแต่ละตัวแปรมีดังต่อไปนี้

t_{load} = ระยะเวลาที่ใช้ในการเปิดเอกสารต่อ 1 ครั้ง

$t_{network}$ = ระยะเวลาที่ใช้ในการกระจายค่ากุญแจลับจาก KRaaS ไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งาน

$t_{decrypt}$ = ระยะเวลาที่ใช้ในการถอดรหัสลับ

N_{text} = จำนวนตัวอักษรที่ใช้ในการถอดรหัสลับ



รูปที่ 5.2.3.1 กราฟการประเมินการค่าประสิทธิภาพในเชิงเวลาของการเปิดเอกสารต่อ 1 ครั้ง

5.2.3.2 <u>การประเมิณการค่าประสิทธิภาพในเชิงเวลาของการบันทึกเอกสารต่อจำนวน 1 ครั้ง</u>

กระบวนการของการเปิดเอกสารกูเกิ้ลด้วยโปรแกรมเสริม TrustDocs นั้น จะสูญเสียค่าประสิทธิภาพเชิงเวลาในกระบวนการการเข้ารหัสลับและกระบวนการกระจายค่ากุญแจลับจาก KRaaS ไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งานจำนวน 6 ครั้ง ผ่านช่องทางที่ปลอดภัย SSL-SQL ได้แก่

- เหตุการณ์การ Query ความถูกต้องของข้อมูลส่วนตัวของผู้ใช้งานใน KRaaS อาทิเช่น Doc_Id และ Email
- เหตุการณ์การ Query ที่มีต่อเนื่องจากเหตุการณ์ที่แล้ว ของข้อมูลที่เกี่ยวข้อง อาทิเช่น ค่ากุญแจลับ (Session Key) ที่ได้รับการจับคู่กับ Doc_Id
- เหตุการณ์การจากความต่อเนื่องจากเหตุการณ์ที่แล้ว ของค่าสถานะของค่ากุญแจลับที่ถูกจับคู่ ถ้าค่าสถานะของค่ากุญแจลับเท่ากับ 2 ให้มีการเปลี่ยนค่าสถานะของค่ากุญแจลับ จากค่าสถานะ 2 เปลี่ยนเป็นค่าสถานะ 3 เพื่อทำการสิ้นสุดการใช้งานค่ากุญแจดังกล่าว
- เหตุการณ์การเรียกค่ากุญแจลับใหม่จาก KRaaS มาที่เครื่องของผู้ใช้งาน
- เหตุการณ์การจับคู่ค่ากุญแจลับใหม่กับ Doc_Id
- เหตุการณ์การเปลี่ยนค่าสถานะของค่ากุญแจลับ จากค่าสถานะ 0 เปลี่ยนเป็นค่าสถานะ 2

สามารถสรุปเป็นสมการดังต่อไปนี้

t_{save} = 6 * ($t_{network}$) + $t_{encrypt}$ (N_{text})

$$t_{network} = \frac{t_{save} - t_{encrypt}}{6}$$

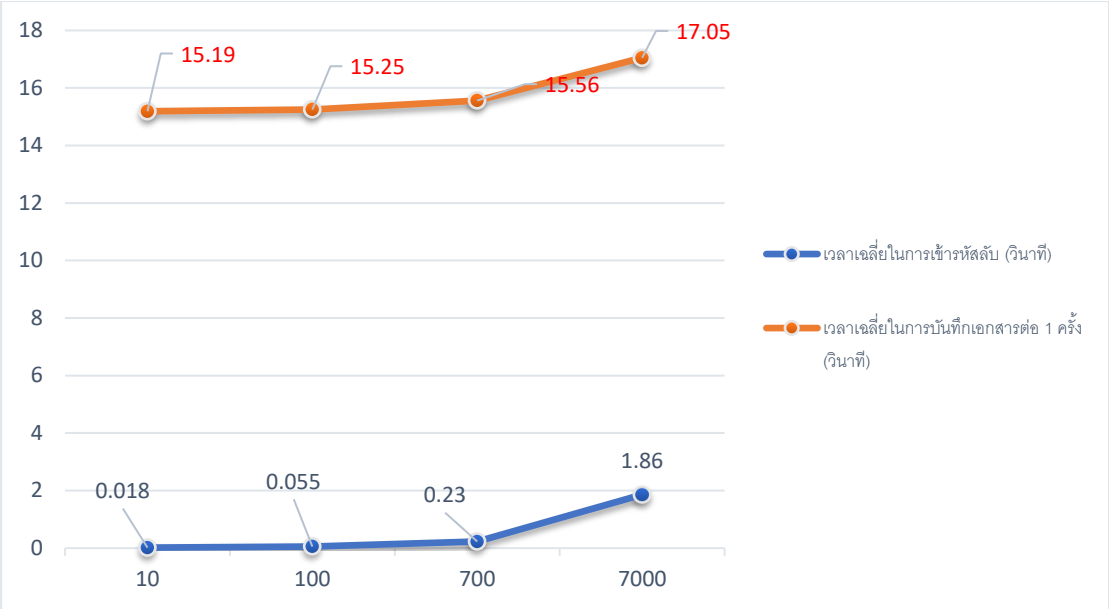
ซึ่งความหมายของแต่ละตัวแปรมีดังต่อไปนี้

t_{save} = ระยะเวลาที่ใช้ในการบันทึกเอกสารต่อ 1 ครั้ง

$t_{network}$ = ระยะเวลาที่ใช้ในการกระจายค่ากุญแจลับจาก KRaaS ไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งาน

$t_{encrypt}$ = ระยะเวลาที่ใช้ในการเข้ารหัสลับ

N_{text} = จำนวนตัวอักษรที่ใช้ในการถอดรหัสลับ



รูปที่ 5.2.3.2 กราฟการประเมินการค่าประสิทธิภาพในเชิงเวลาของการบันทึกเอกสารต่อ 1 ครั้ง

จากการวิเคราะห์และประเมินค่าประสิทธิภาพในเชิงเวลาของการใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs จะสูญเสียค่าประสิทธิภาพในเชิงเวลาซึ่งสามารถแบ่งแยกเป็นสองส่วน คือ กระบวนการทำวิทยาการรหัสลับ และกระบวนการกระจายค่ากุญแจลับ ซึ่งจากกราฟผลการทดลองค่าประสิทธิภาพเชิงเวลาจะมีผลต่อขนาดของตัวอักษรที่เข้าสู่กระบวนการทำวิทยาการรหัสลับ แต่จะไม่ผลต่อกระบวนการกระจายค่ากุญแจลับ กล่าวคือ ค่าประสิทธิภาพในเชิงเวลาของกระบวนการกระจายค่ากุญแจลับจะใช้ระยะเวลาเท่าๆกันซึ่งแบ่งแยกตามระยะเวลาการเข้าและถอดรหัสลับของการกระจายค่ากุญแจลับ

ซึ่งกล่าวได้ว่าค่าประสิทธิภาพในเชิงเวลานั้น จะมีผลต่อขนาดของข้อมูลในการทำวิทยาการรหัสลับอย่างมาก กล่าวคือ ยิ่งขนาดตัวอักษรมีขนาดใหญ่มากเท่าใด ระยะเวลาที่ใช้ในการทำวิทยาการรหัสลับหรือระยะเวลาในการทำการเปิด หรือบันทึกเอกสารในการใช้งานโปรแกรมเอกสารกูเกิ้ล TrustDocs ต่อจำนวน 1 ครั้ง มากขึ้นตามลำดับ

บทที่ 6

สรุปผลการวิจัย

ในบทนี้จะกล่าวถึงสรุปผลการวิจัย ข้อจำกัดของงานวิจัย งานวิจัยในอนาคตและผลงานตีพิมพ์จากวิทยานิพนธ์ โดยแต่ละส่วนที่กล่าวมานั้นมีรายละเอียดดังต่อไปนี้

6.1. สรุปผลการวิจัย

การนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง ซึ่งถ้าเราเลือกใช้ผู้ให้บริการรายเดียวในการเก็บข้อมูลสำคัญทั้งหมด ถึงแม้รูปแบบที่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะถูกเข้ารหัสลับแบบไม่สามารถใช้งานได้นั้น แต่ข้อมูลอื่นๆเช่น ค่ากุญแจต่างๆ ที่เกี่ยวข้อง ก็อาจจะยังอยู่ในการดูแลของผู้ให้บริการ ดังนั้นบุคคลที่เกี่ยวข้องเช่น ผู้ดูแลระบบก็สามารถที่จะนำค่ากุญแจต่างๆที่เกี่ยวข้องเพื่อถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำข้อมูลที่ได้มา เอาไปใช้งานที่สามารถก่อให้เกิดอันตรายต่อผู้ใช้งานได้

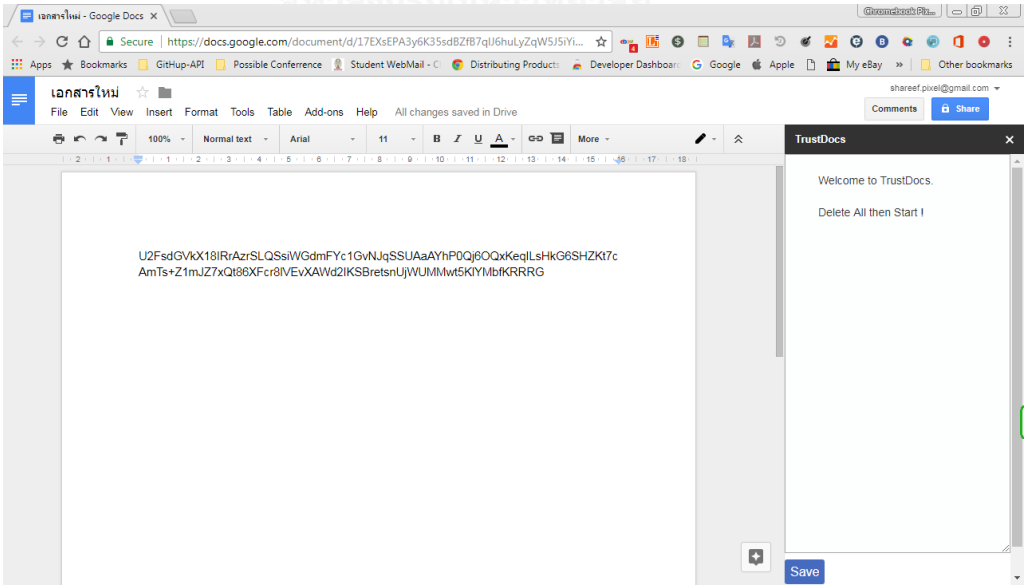
ปัญหาที่ได้ระบุไว้ข้างต้นที่เกิดขึ้นในปัจจุบันเกิดจากการเลือกใช้ผู้ให้บริการ SaaS Storage เพียงแค่ รายเดียวในการเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน ซึ่งถ้าเราเลือกใช้ผู้ให้บริการเดียวในการเก็บข้อมูลสำคัญ ทั้งหมด ถึงแม้รูปแบบที่ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานจะถูกเข้ารหัสลับแบบไม่สามารถใช้งานได้นั้น แต่ ข้อมูลอื่นๆเช่น ค่ากุญแจต่างๆ ที่เกี่ยวข้อง ก็ยังอยู่ในการดูแลของผู้ให้บริการ ดังนั้นบุคคลที่เกี่ยวข้องเช่น ผู้ดูแลระบบก็สามารถที่จะนำค่ากุญแจต่างๆที่เกี่ยวข้องเพื่อถอดรหัสข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำข้อมูลที่ได้มา เอาไปใช้งานที่สามารถก่อให้เกิดอันตรายต่อผู้ใช้งานได้ ดังนั้นการหากลไกลรักษาความปลอดภัยของ เอกสารโดยการใช้ผู้ให้บริการ SaaS Storage มากกว่า 1 ราย มาทำงานร่วมกันเพื่อจัดเก็บข้อมูลสำคัญหรือ ข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้ วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง ในงานวิจัยนี้ ผู้วิจัยจึงนำเสนอหลักการหรือโมเดลใหม่ และกระบวนการ การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งาน (Client Side Cryptography) ที่สามารถตอบโจทย์ด้านความเหมาะสม และความปลอดภัยจากช่องโหว่ต่างๆ ที่อาจจะเกิดอันตรายต่อข้อมูลสำคัญ หรือข้อมูลลับ ขึ้นมาจากปัญหาดั่งกล่าว โดยจะเลือกใช้ทรัพยากร (Resource) ที่เป็นการประมวลผลแบบคลาวด์ (Cloud Computing) ในรูปแบบ SaaS ที่ให้บริการด้าน Storage จำนวน 2 รายเพื่อนำมาเป็นที่เก็บข้อมูล สำคัญหรือข้อมูลลับ (Data Repository) และ

เป็นที่เก็บค่ากุญแจ (Key Repository) ต่างๆที่เกี่ยวข้อง โดย ได้พัฒนาระบบต้นแบบที่ทำงานร่วมกับระบบเอกสารกูเกิ้ล (Google Document) ในการจำลองเป็นข้อมูลสำคัญ หรือข้อมูลลับของผู้ใช้งานทั่วไป ซึ่งจะใช้ Google Drive ในการจำลองเป็น Storage หรือ Data Repository ในการเก็บข้อมูล และใช้ ClearDB ในฐานะผู้ให้บริการ SaaS Storage ที่ให้บริการจัดเก็บข้อมูลในรูปแบบข้อมูล SQL Database อีกรายหนึ่งในการจำลองเป็น Key Repository ในการเก็บค่ากุญแจลับ (Session Key) ในส่วนกระบวนการ การใช้วิทยาการรหัสลับที่ฝั่งผู้ใช้งานนั้น ผู้วิจัยจะนำเสนอกระบวนการ ในรูปแบบในการเข้ารหัสลับข้อมูล (Data Encryption) การถอดรหัสลับข้อมูล (Data Decryption) และ การกระจายค่ากุญแจต่างๆ (Key Distribution) ในรูปแบบ ที่เป็นกระบวนการอัตโนมัติ (Automatic Process) เพื่อแก้ไขปัญหาในการใช้งานข้อมูลสำคัญ หรือข้อมูลลับ ที่เก็บไว้ที่ SaaS Storage ได้ง่ายและมีความปลอดภัยจากภัยคุกคามมากขึ้น

6.2. ข้อจำกัดของงานวิจัย

6.2.1 หน้าตาอินเตอร์เฟสของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

ผู้ให้บริการ กูเกิ้ลไม่อนุญาตให้นักพัฒนาสามารถหยุดการทำงานเรียลทามในการบันทึกข้อมูลในกูเกิ้ลไดร์ฟ เมื่อใช้งานผ่านเอกสารกูเกิ้ล ดังนั้นผู้วิจัยจะต้องมีการพัฒนาโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ที่มีหน้าตาอินเตอร์เฟสในรูปแบบ Side Bar และรูปแบบ Side Bar เท่านั้นที่ทาง Google Add-on Advisor ตั้งข้อจำกัดให้นักพัฒนาออกแบบหน้าอินเตอร์เฟสของ Google Docs-Adon เพียงแค่รูปแบบ Side Bar ด้วยเหตุผลการจัดระเบียบหน้าตาภาพลักษณ์ของ Google Docs Ad-on

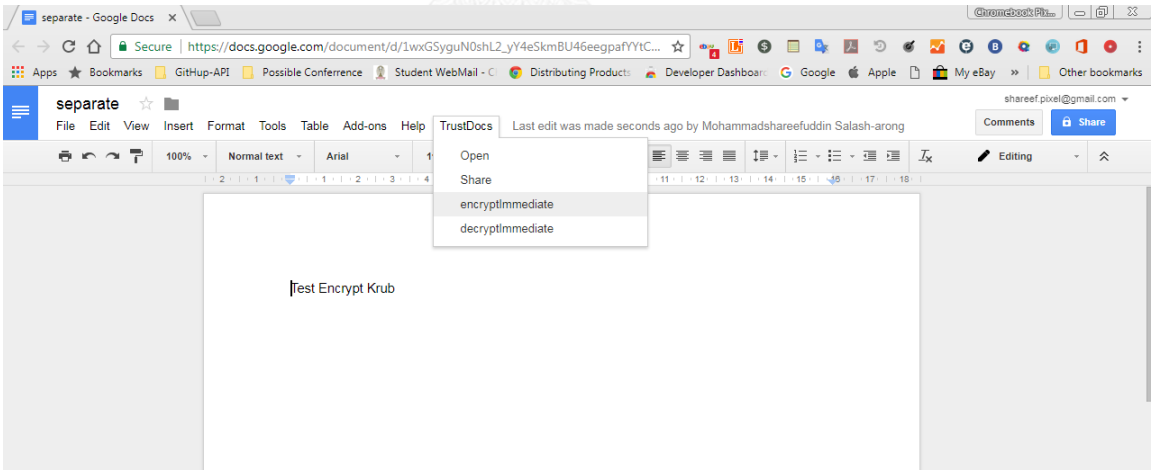


รูปที่ 6.2.1 TrustDocs – Google Docs Add-on GUI

6.2.2 ปัญหาจากการเลือกใช้หน้าตาอินเตอร์เฟสของเอกสารกูเกิ้ลในการดำเนินการวิทยาการรหัสลับ

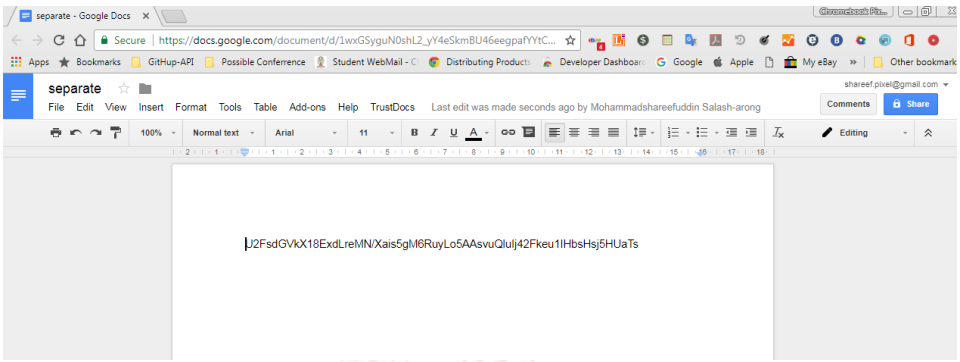
จากข้อจำกัดการไม่อนุญาตการหยุดการทำงานแบบเรียลทามข้างต้น ถ้านักพัฒนาต้องการใช้หน้า Standard GUI ของ Google Docs ในการจัดการข้อมูลสำคัญหรือข้อมูลลับ เวลาที่ผู้ใช้งานมีการพิมพ์ข้อมูลสำคัญหรือข้อมูลลับของตนลงพื้นที่ Text Area ในเอกสารกูเกิ้ล ข้อมูลสำคัญหรือข้อมูลลับทั้งหมดก็จะถูกบันทึกลง Google Drive โดยอัตโนมัต และถ้านักพัฒนาได้มีการใส่ฟังก์ชั่นเพิ่มในโปรแกรมเสริมเอกสารกูเกิ้ลให้มีการเข้าหรือถอดรหัสลับ โปรแกรมเสริมก็จะนำข้อมูลสำคัญหรือของมูลลับของผู้ใช้งานจากกูเกิ้ลไดร์ฟ มาทำการเข้ารหัสลับ และสั่งบันทึกเข้าไปในกูเกิ้ลไดร์ฟอีกครั้ง ซึ่งวิธีนี้จะไม่มีประโยชน์ในด้านการรักษาความปลอดภัยของเอกสารในสภาพแวดล้อมไม่เชื่อถือต่อผู้ให้บริการ เนื่องจากก่อนการทำการเข้ารหัสลับนั้น ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานถูกบันทึกลงสู่กูเกิ้ลไดร์ฟเรียบร้อยแล้ว ในรูปแบบ Plain Text ซึ่งถ้าผู้บริการได้ทำการ Logging ไว้ก็สามารถนำข้อมูลดังกล่าวไปใช้ได้

6.2.2.1 ผู้ใช้งานพิมพ์ข้อมูลสำคัญหรือข้อมูลลับของตนในพื้นที่ Text Area ในเอกสารกูเกิ้ล และทำการสั่งการทำการเข้ารหัสลับ



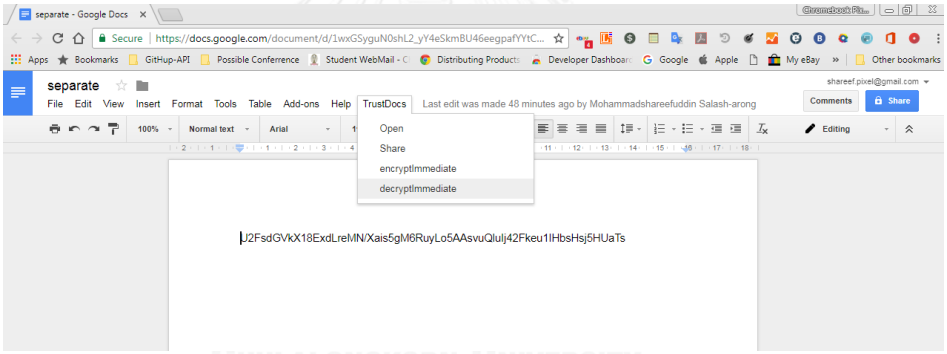
รูปที่ 6.2.2.1 Encrypt Content in Google Docs Text Area

6.2.2.2 ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานได้รับการเข้ารหัสลับ



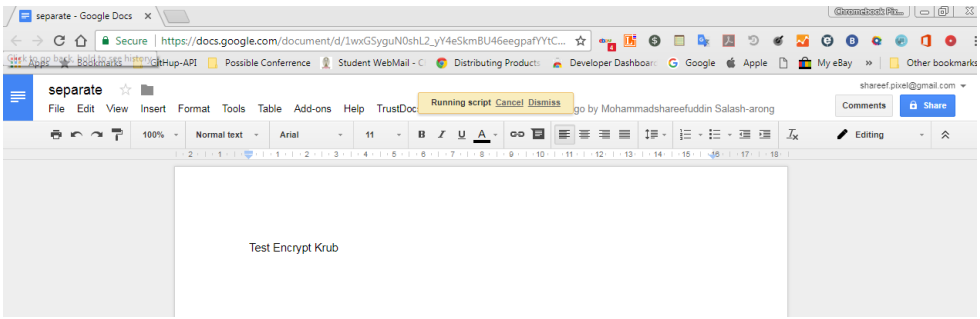
รูปที่ 6.2.2.2 Encrypted Content in Google Drive

6.2.2.3 ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานได้รับการเข้ารหัสลับ



รูปที่ 6.2.2.3 Decrypt Content in Google Docs Text Area

6.2.2.4 ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานได้รับการถอดรหัสลับ และข้อมูลดังกล่าวก็จะถูกบันทึกลงสู่กูเกิ้ลไดร์ฟอัตโนมัติ



รูปที่ 6.2.2.4 Plian Content in Google Drive

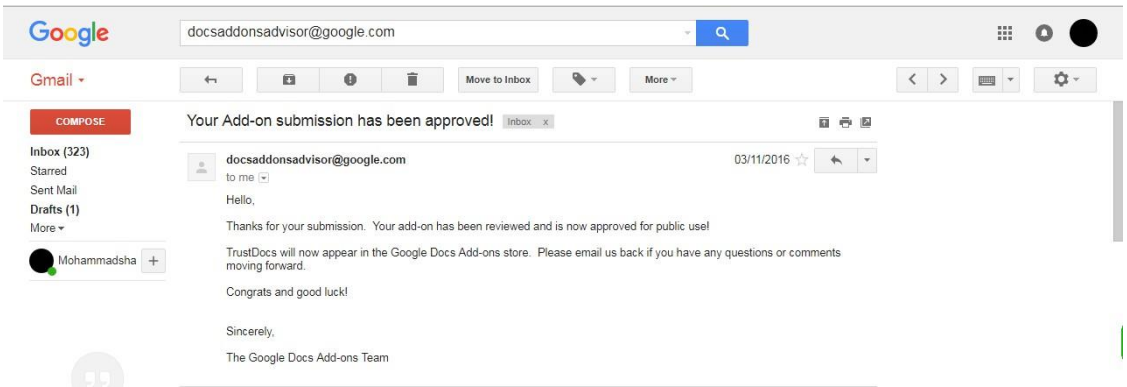
6.3. การอภิปรายในส่วนอื่นๆ ที่สำคัญของงานวิจัย

6.3.1 การวางใจการให้บริการของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

การนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ และกรณีที่ต้องการใช้วิทยาการรหัสลับเพื่อความปลอดภัยจากภัยคุกคามจะเกิดขึ้นจากผู้ให้บริการเอง แต่ถ้าคำนึงถึงประเด็นในการวางใจการให้บริการของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs นั้น ผู้ใช้งานจะมีความมั่นใจในความปลอดภัยจากพยันตรายในส่วนความปลอดภัยจากเหตุการณ์ Backdoors ในส่วนของ Source Code ของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ได้อย่างไรนั้น ผู้วิจัยขอสรุปได้ดังต่อไปนี้

6.3.1.1 การตรวจสอบความถูกต้อง และความปลอดภัยของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ในฝั่งของผู้ให้บริการกูเกิ้ล

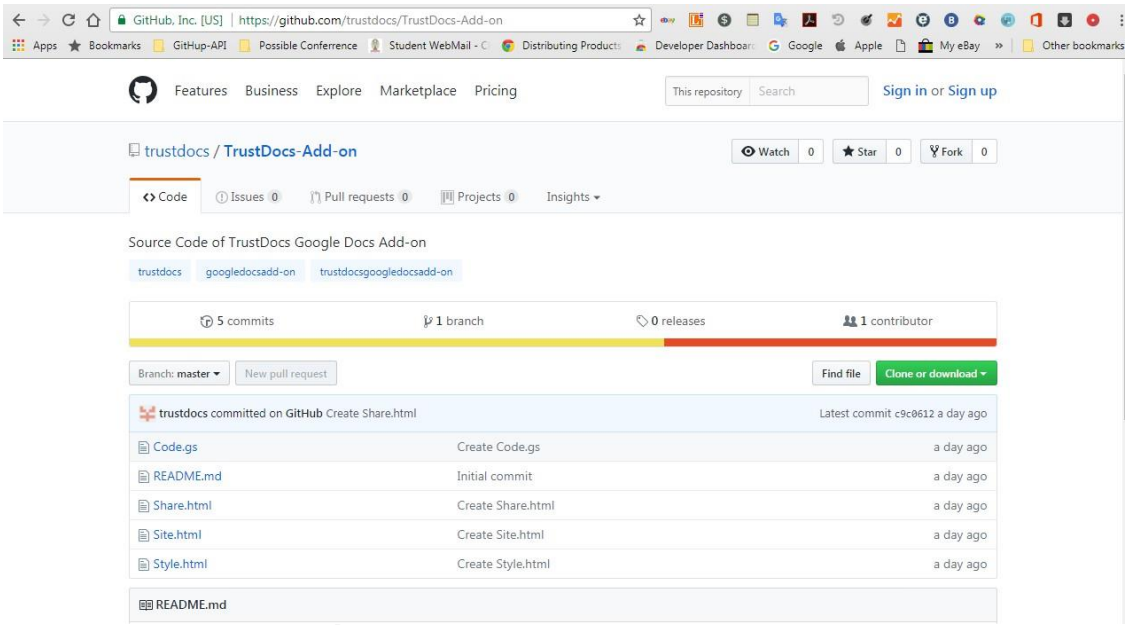
ก่อนที่จะมีการดำเนินการลงทะเบียนโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs หรือ โปรแกรมเสริมเอกสารกูเกิ้ลอื่นๆ สามารถวางจำหน่ายใน Google Docs Add-on Store เพื่อสามารถที่จะสนับสนุนให้ผู้ใช้งานสามารถทำการดาวน์โหลดเพื่อติดตั้ง โปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ก่อนที่จะใช้งานนั้น ต้องผ่านกระบวนการในการตรวจสอบความถูกต้อง และความปลอดภัยมากมายจากผู้ให้บริการกูเกิ้ล โดย Google Docs Add-on Advisor ซึ่งมีหน้าที่ที่สำคัญในการทำให้ลูกค้าของผู้ให้บริการกูเกิ้ลนั้น ไม่ต้องเผชิญหน้ากับความเสี่ยงจากความเสียหายของข้อมูลสำคัญ หรือข้อมูลลับของผู้ใช้งานในการใช้งานเอกสารกูเกิ้ลดังกล่าว ดังนั้น การที่โปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs มีวางจำหน่ายใน Google Docs Add-on Store ก็สามารถการันตีได้ว่า พยันตรายที่อาจขึ้นจากเหตุการณ์ Backdoors ในส่วนของ Source Code ของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs จะไม่เกิดขึ้น ทำให้ผู้ใช้งานสามารถใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ได้อย่างปลอดภัย



รูปที่ 6.3.1.1 Google Docs Add-on Advisor Approved Email

6.3.1.2 การดำเนินการทำโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ให้กลายเป็นซอฟต์แวร์ Open Source

เพื่อความปลอดภัยจากพยันตารายที่อาจขึ้นในเหตุการณ์ Backdoors ในส่วนของ Source Code ในการใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs และความต้องการให้มีแรงจูงใจในการต่อยอดในของงานวิจัย ในการพัฒนาโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ให้มีความปลอดภัยมากขึ้น ดังนั้น ผู้วิจัยได้มีการแบ่งปัน Source Code ให้แด่นักพัฒนาซอฟต์แวร์ หรือนักวิจัยทั้งหลาย สามารถที่จะดาวน์โหลด Source Code ทั้งหมดที่เกี่ยวข้อง ได้ที่ https://github.com/trustdocs/TrustDocs-Add-on



รูปที่ 6.3.1.2 TrustDocs Google Docs Add-on Open Source

6.3.2 การสร้างค่ากุญแจลับจำนวนมหาศาลใน KRaaS เพื่อสนับสนุนการใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

การนำเสนอการเลือกใช้ผู้ให้บริการมากกว่า 1 ราย เพื่อจัดเก็บข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานนั้น ซึ่งผู้วิจัยถือว่า ค่ากุญแจลับต่างๆที่ใช้ในการเข้ารหัสลับนั้น ถือว่าเป็นข้อมูลสำคัญหรือข้อมูลลับด้วยที่ไม่สมควรอย่างยิ่งที่จะเลือกเก็บค่ากุญแจลับไว้ที่เดียวกับข้อมูลสำคัญหรือข้อมูลลับเพื่อป้องกันผู้ให้บริการสามารถที่จะนำค่ากุญแจลับดังกล่าวมาทำการถอดรหัสลับแล้วก็สามารถที่จะนำข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานมากระทำการก่อให้เกิดความเสียหายต่อผู้ใช้งาได้ ดังนั้นผู้วิจัยได้มีการออกแบบระบบ Keys-Repository-as-a-Service (KRaaS) เพื่อแก้ปัญหาด้านความปลอดภัยดังกล่าว ซึ่งจุดมุ่งหมายของการออกแบบระบบ KRaaS เพื่อนำเสนอโมเดลใหม่ในรูปแบบการประมวลผลแบบคลาวด์ที่ไว้จัดเก็บและดูแลค่ากุญแจสำคัญของผู้ใช้งาน หรือ Cloud Keys-

Repository-as-a-Service (KRaaS) ซึ่งมีการทำงานคล้ายกับระบบ Cloud Keys-Management-as-a-Service (KMaaS) [15] แต่ต่างกันที่ KRaaS ไม่มีกลไกในการสร้างและบริหารจัดการค่ากุญแจ (Key Management Mechanism) ในส่วนของการวิจัยในเฟสแรกนี้ ซึ่งผู้วิจัยหวังเป็นอย่างว่างานวิจัยในอนาคตจะมีการให้ความสำคัญและพัฒนาต่อยอดในส่วนของการสร้างและจัดการค่ากุญแจให้มีประสิทธิภาพ อาทิเช่นการสร้างค่ากุญแจในขณะที่มีการเรียกใช้งานหรือการเข้ารหัสลับค่ากุญแจลับใน KRaaS เป็นต้น

การสร้างค่ากุญแจลับจำนวนมหาศาลใน KRaaS เพื่อสนับสนุนการใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs นั้นเป็นการออกแบบและพัฒนาเพื่อทำการทดลองเท่านั้น ถ้าคำนึงถึงด้านความปลอดภัยแล้วถือว่ายังไม่ดีพอ เนื่องจากยังมีช่องโหว่ที่ทำให้ผู้ไม่หวังดีสามารถใช้ในการโจมตีได้ กล่าวคือ ผู้ให้บริการเอกสารกูเกิ้ล ถ้าสามารถเข้าถึงระบบ KRaaS ได้ก็จะสามารถนำค่ากุญแจลับที่ถูกจับคู่กับเอกสารกูเกิ้ลของผู้ใช้งานมาทำการถอดรหัสลับเพื่ออ่านข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานดังกล่าวได้ ซึ่งช่องโหว่ดังกล่าวจะสามารถถูกโจมตีจากผู้ให้บริการเอกสารกูเกิ้ลเท่านั้น ในส่วนผู้ให้บริการ KRaaS และผู้ไม่หวังดีอื่นๆจะไม่สามารถโจมตีด้วยวิธีดังกล่าวได้เนื่องจากจะต้องผ่านการพิสูจน์ตัวตนในการเข้าใช้งานเอกสารกูเกิ้ล (Google Authentication)

6.3.3 การเปลี่ยนค่ากุญแจลับบ่อยครั้งของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

เพื่อหลีกเลี่ยงหรือป้องกันปัญหาที่อาจจะเกิดขึ้นในการพยายามการคาดเดาค่ากุญแจ (Brute Force Attack) การเปลี่ยนค่ากุญแจลับบ่อยครั้งของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs ก็เป็นการแก้ไขปัญหาที่ดีในแง่มุมของการไม่วางใจผู้ให้บริการ แต่ก็ยังมีช่องโหว่หรือความเสี่ยงอยู่ในส่วนของงานวิจัยเฟสนี้ กล่าวคือกลไกการเปลี่ยนค่ากุญแจนั้นจะเกิดขึ้นก็ต่อเมื่อผู้ใช้งานมีการดำเนินการแก้ไขข้อมูลสำคัญหรือข้อมูลลับของตน แต่ถ้าเอกสารกูเกิ้ลของผู้ใช้งานดังกล่าวไม่มีการแก้ไขเลย ได้แต่มีการถอดรหัสลับเพื่ออ่านข้อมูลสำคัญหรือข้อมูลลับเท่านั้น ค่ากุญแจลับก็จะไม่มีการเปลี่ยนเป็นค่ากุญแจลับใหม่ ซึ่งถ้าผู้ให้บริการกูเกิ้ลมีการพยายามที่จะคาดเดาค่ากุญแจลับจริงๆ ก็มีโอกาสที่จะดำเนินการนี้ได้สำเร็จ ดังนั้นผู้ใช้งานต้องตระหนักกับช่องโหว่หรือความเสี่ยงดังกล่าว ถ้าผู้ใช้งานกลัวว่าจะเกิดภัยคุกคามกับเอกสารกูเกิ้ลของตนที่มีข้อมูลสำคัญหรือข้อมูลลับในระดับลับสุดยอด ก็ควรจะมีการกระทำการแก้ไขอะไรบ้าง หรือแค่กดปุ่ม SAVE โดยมิต้องมีการแก้ไขข้อมูลใดๆทั้งสิ้น หลังจากผู้ใช้งานกดปุ่ม SAVE ก็จะเกิดกระบวนการเข้ารหัสลับที่ผนวกกับกระบวนการสิ้นสุดค่ากุญแจลับเดิมและมีการเรียกใช้ค่ากุญแจลับใหม่ในการดำเนินการการเข้ารหัสลับข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานในทุกๆครั้ง

6.3.4 ปัญหาที่อาจจะเกิดในกรณีที่มีการฝังค่าผู้ใช้งานในฝั่ง KRaaS ใน Source Code ของโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

ในส่วนของปัญหาที่อาจจะเกิดในกรณีที่มีการฝังค่าผู้ใช้งาน อาทิเช่น Host IP Addrress ค่า Username และค่า Password ในฝั่ง KRaaS ใน Source Code นั้น อาจเป็นช่องโหว่ต่อภัยคุกคามอย่างยิ่งในสภาวะที่ผู้ให้บริการกูเกิ้ลสามารถมองเห็นค่าดังกล่าวและสามารถทำการโจมตีด้วยการแอบเข้าถึงข้อมูลในฝั่ง KRaaS และสามารถนำค่ากุญแจลับต่างๆที่เกี่ยวข้องมาทำการถอดรหัสลับเพื่อได้ข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งานและนำไปใช้ซึ่งอาจก่อให้เกิดความเสียหายต่อผู้เป็นเจ้าของหรือองค์กรณ์ได้

วิธีการแก้ไขปัญหาดังกล่าว สามารถได้รับการแก้ไขโดยทำการซ่อน [16] ค่าที่สำคัญเหล่านั้นใน Source Code โดยเฉพาะอย่างยิ่ง ค่า Password เป็นต้น

รายการอ้างอิง

[1] Dave Wong. May 2013 http://www.hardwarezone.co.th/features/view/2218

[2] Top 10 2013-A6-Sensitive Data Exposure. https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure

[3] Michalas, Antonis, and Menelaos Bakopoulos. "SecGOD Google Docs: Now i feel safer!." Internet Technology And Secured Transactions, 2012 International Conference for. IEEE, 2012.

[4] Yutthapong, Amonfa. Bernerlee. Cloud Computing. March 2008 http://itm0151.blogspot.com/2009/03/itm640-internet-and-communication.html

[5] IMS Adoption of Service Oriented. September 2009 http://www.imsglobal.org/soa/soawpv1p0/imsSOAWhitePaper_v1p0.htm

[6] Tim Mather, Subra Kumaraswamy, and Shahed Latif. Cloud Security and Privacy: United States of America., September 2009

[7] ลัญฉกร วุฒิสิทธิกุลกิจ, ธงชัย โรจน์กังสดาล, วรากร ศรีเชวงทรัพย์, นพพล พรมภักษร, สุวิทย์ นาคพีรยุทธ .2543. วิทยาการรหัสลับเบื้องต้น.สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย :

[8] คู่มือการทำแบบสอบถามออนไลน์โดย Google Doc http://www1.si.mahidol.ac.th/km/sites/default/files/u2009/262f6285cf887a3025ec1d3543afdd43.pdf

[9] http://billatnapier.com/design_tips239.htm

[10] http://billatnapier.com/design_tips241.htm

[11] ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ กำแพงแสน มหาวิทยาลัยเกษตรศาสตร http://eng.kps.ku.ac.th/km-v57/stories/doc-download/57/km4/km4-manaul-google-drive.pdf

[12] https://www.cleardb.com

[13] L. Adkinson-Orellana, D. A. Rodr´ıguez-Silva, F. Gil-Castineira, and J. C. Burguillo-Rial. ˜ Privacy for Google Docs: Implementing a transparent encryption layer. In CloudViews2010 Conference, pages 41–48, Porto, 20th-21st May 2010. EuroCloud Portugal.

[14] Adkinson-Orellana, Lilian, et al. "Sharing Secure Documents in the Cloud-A Secure Layer for Google Docs." CLOSER. 2011.

[15] Lerman, L., Markowitch, O., Nakahara Jr, J., & Samarati, P. P. (2012, July). Key Management as a Service. In SECRYPT (pp. 276-281).

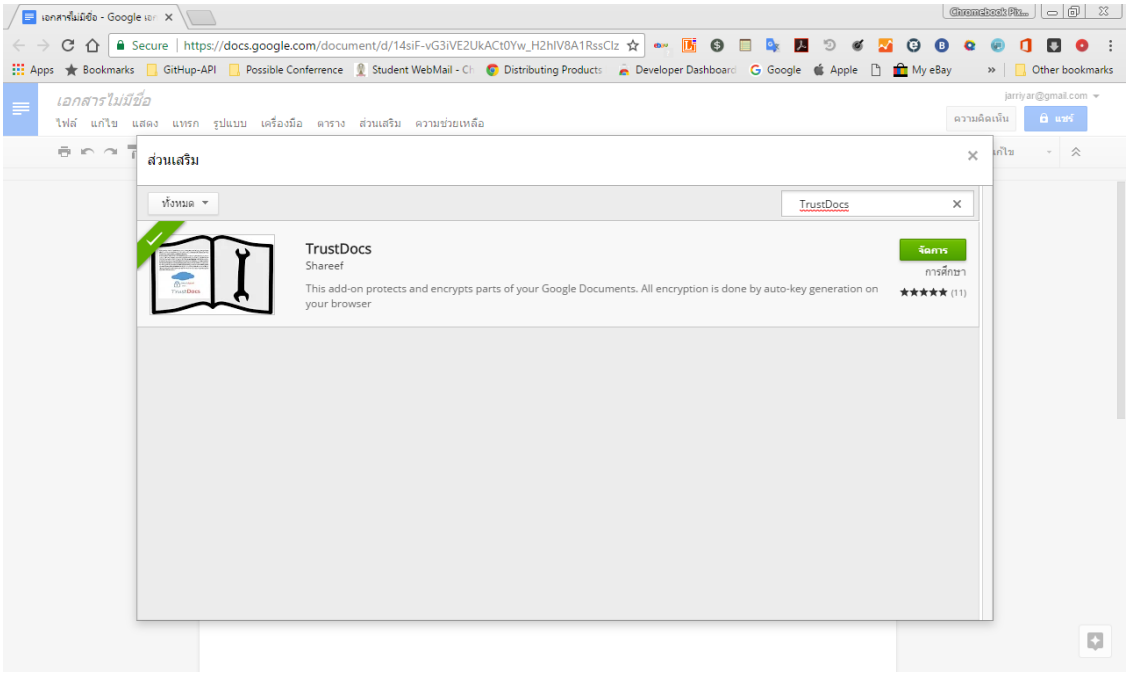
[16] http://www.codingforums.com/javascript-programming/177432-how-hide-javascript-login-password-source-code.html

ภาคผนวก

ภาคผนวก ก

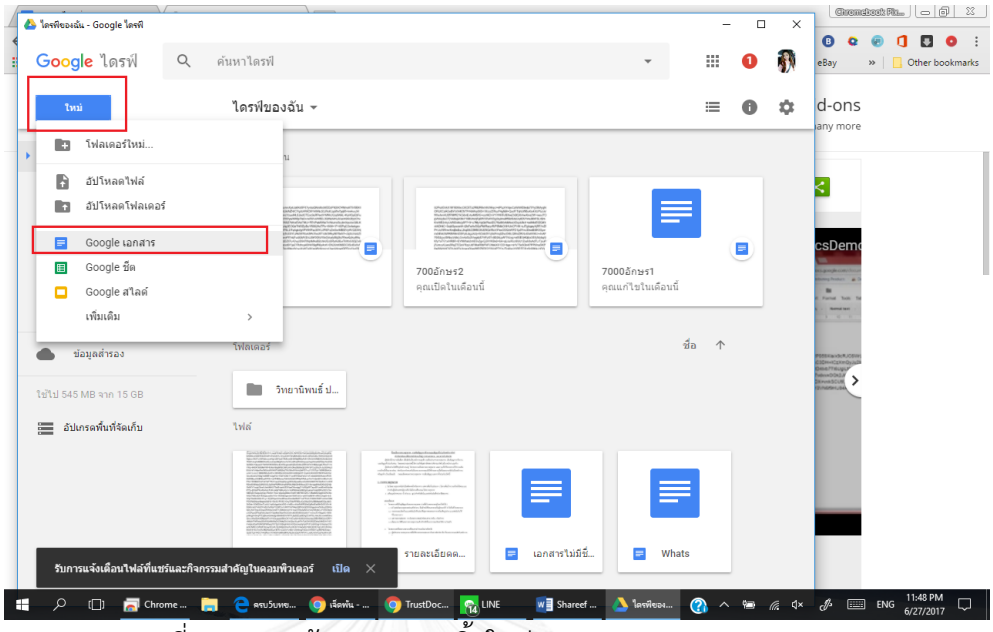
การดาวน์โหลดและติ้งตังเพื่อใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

1. ทำการดาวน์โหลดและติดตั้งโปรแกรมเสริมเอกสาร TrustDocs ได้ที่ Google Add-on Store หรือ https://chrome.google.com/webstore/detail/trustdocs/mghcpeobheaiohijlhbdgeeagbjhadok



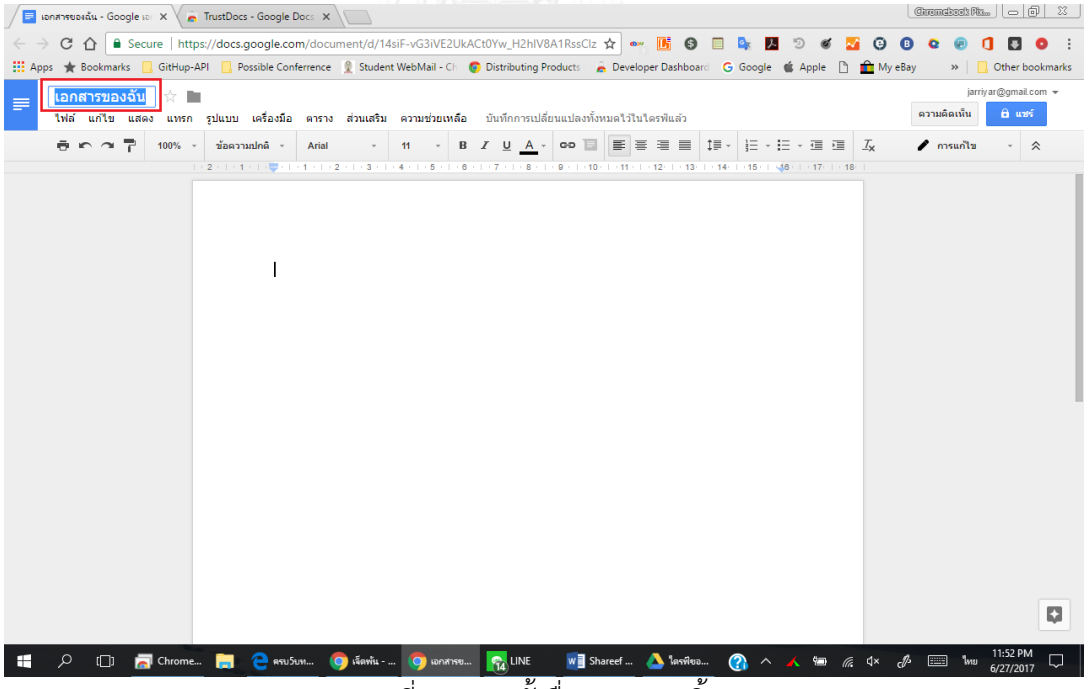
รูปที่ ก.1 การดาวน์โหลดและติดตั้งโปรแกรมเสริมเอกสาร TrustDocs ได้ที่ Google Store

1. สร้างเอกสารกูเกิ้ลใหม่ จาก Google Drive



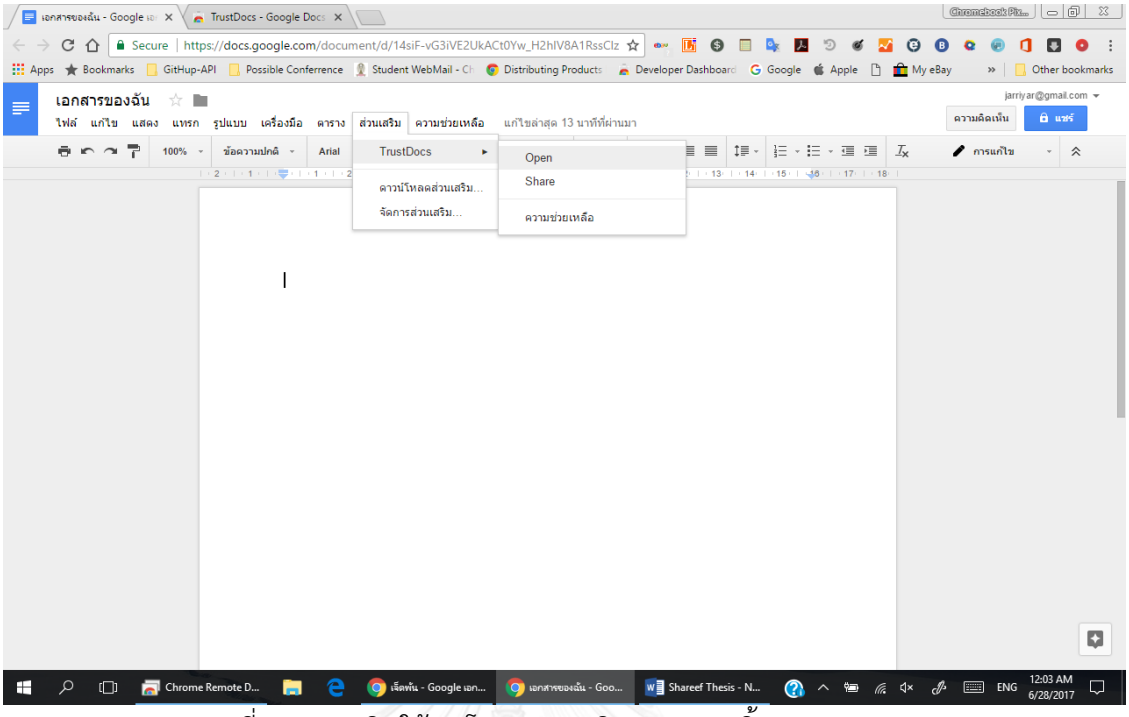
รูปที่ ก.2 การสร้างเอกสารกูเกิ้ลใหม่ จาก Google Drive

2. ตั้งชื่อไฟล์เอกสารกูเกิ้ล



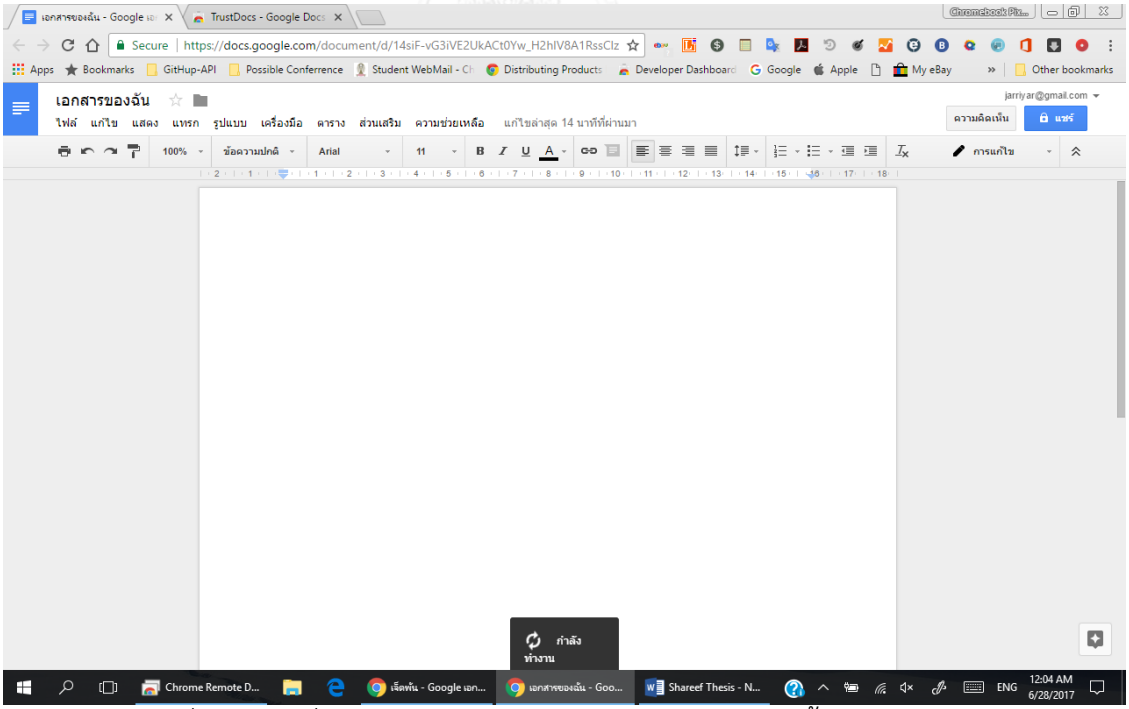
รูปที่ ก.3 การตั้งชื่อเอกสารกูเกิ้ล

3. ไปที่เมนู “ส่วนเสริม” > “TrustDocs” > “Open”



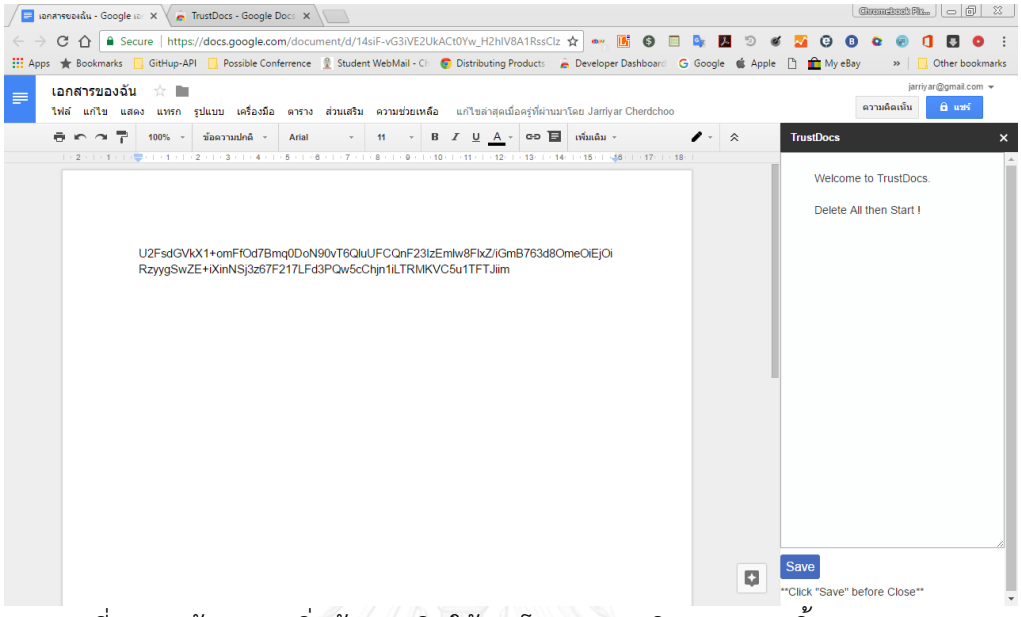
รูปที่ ก.4 การเปิดใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

4. รอโปรเซสการทำงานจนเสร็จ



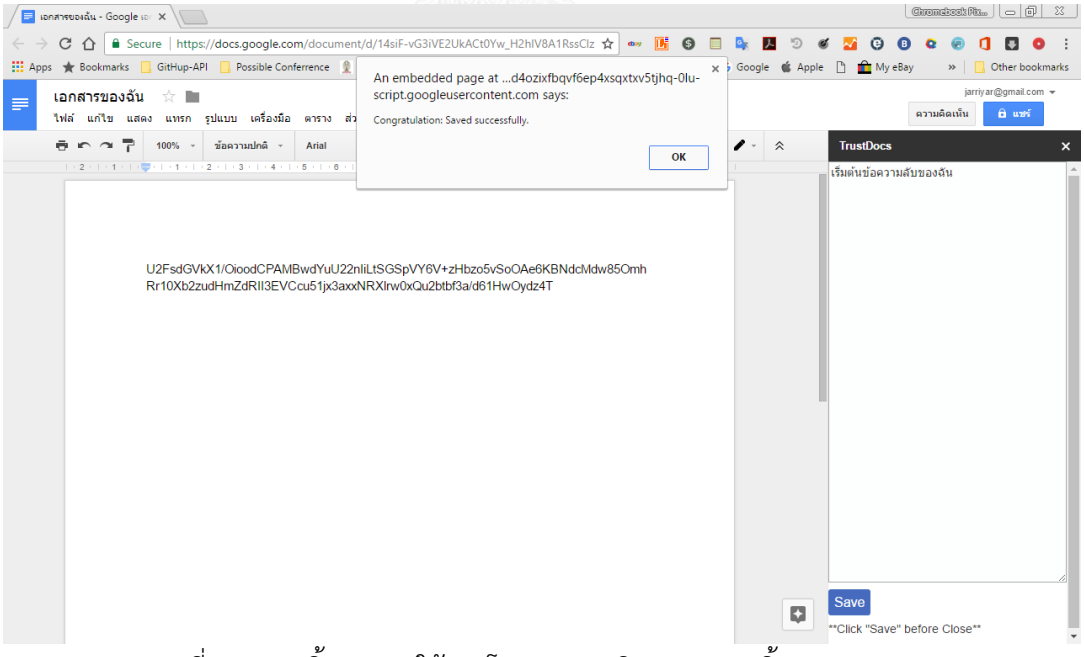
รูปที่ ก.5 การเริ่มต้นการเปิดใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

5. หลังจากโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocsได้ถูกเปิดเสร็จสมบูรณ์ ให้ผู้ใช้งานลบข้อความทั้งหมดใน Side Bar และเริ่มการเขียนข้อมูลสำคัญหรือข้อมูลลับของตน เมื่อการเขียนเสร็จสิ้นแล้ว ให้กดปุ่ม “SAVE” ให้โปรแกรมเสริมเอกสารกูเกิ้ลทำการเข้ารหัสลับข้อมูลทั้งหมดและบันทึกลงสู่กูเกิ้ลไดรฟ



รูปที่ ก.6 หน้าตาการเริ่มต้นการเปิดใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

6. ให้ผู้ใช้งานเปิดปุ่ม “OK” เพื่อสิ้นสุดการเข้ารหัสลับ และปิดเอกสารกูเกิ้ล



รูปที่ ก.7 การสิ้นสุดการใช้งานโปรแกรมเสริมเอกสารกูเกิ้ล TrustDocs

ภาคผนวก ข

TrustDocs – Google Docs Add-on Apps Script Code

ข.1 Code.gs

Source Code ส่วนใหญ่ในไฟล์ Code.gs จะใช้ภาษาไลบรารี่ของ Google Apps Script ที่ไว้ควบคุมการทำงานของเอกสารกูเกิ้ลโดยตรง จะมีการใช้ภาษาไลบรี่ JavaScript ในการควบคุมการทำงานของการเข้าและถอดรหัสลับ คือ Crypto.js ซึ่งเป็นภาษาไลบราลี่ของทางกูเกิ้ลเอง และสุดท้ายจะใช้ภาษาไลบรารี่ ของ Google JDBC ที่เป็นภาษาที่ไว้เชื่อมต่อกับฐานข้อมูลของ KRaaS ซึ่ง Source Code ทั้งหมดจะมีดังต่อไปนี้

```
function onOpen() {

  createMenu();
}

function createMenu() {

  ui.createMenu("TrustDocs")
    .addItem("Open", "startFunction")
    .addItem("Share", 'addNewEditorEmailFunction')
    .addToUi();
}



function startFunction() {

  var thisDoc = DocumentApp.getActiveDocument();
  var docId   = thisDoc.getId();
```

```
var docUrl  = thisDoc.getUrl();
var docName = thisDoc.getName();
var editors = thisDoc.getEditors();
var viewers = thisDoc.getViewers();
var activeUserEmail = Session.getActiveUser().getEmail();
var docCount = retriveExistedDocId();

if ( isValidEditorEmail(activeUserEmail, docId) ) {

} else {

}

if (docCount === 0) {

}
if (docCount > 0) {

  showDialogBox('TrustDocs');

  return;
}

if (editors.length === 1) {

}
else if (editors.length >= 1) {

} else {

}
```

```
  var docRowId          = insertDocId(docId, editors);

  var editorEmailRowId = addOwnerEmailToEditorEmails(docRowId, editors);

  var idAndNewKey       = getNewKeyFromDatabase();

  var sessionKeyRowid  = idAndNewKey[0];
  var newKey            = idAndNewKey[1];

  var start     = new Date();
  var encrypted = encrypt(theDefaultDummyText, newKey);
  var end       = new Date();

  recordEncryptingSpendTime(docRowId, sessionKeyRowid, 'e', (end - start),
theDefaultDummyText.length);
  DocumentApp.getActiveDocument().setText(encrypted);
  markKeyIsStartUpStatus1(newKey);
  mapDocIdWithKey(docRowId, sessionKeyRowid);
  showDialogBox('TrustDocs');
}

function createJdbcSSLConnection(dbUrl,  info) {

 var connection = Jdbc.getConnection( dbUrl, info );

  return connection;
}

function recordEncryptingSpendTime(docRowId, keyRowId, type, spendTime,
letterLength) {
```

```
  var timeRowId;
  var conn = createJdbcSSLConnection(dbUrl,  info);

  var stmt = conn.createStatement();
  var date = getDateTimeInMySQLFormat();
  var sql = ' INSERT INTO times ( doc_id, sessionkey_id, type, spend_time,
letter_length ) ' +
            " values ( '" + docRowId + "', '" + keyRowId + "', '" + type  + "', '" + spendTime
+ "', '" + letterLength + "' )";

  var count = stmt.executeUpdate(sql,1)
  var rs = stmt.getGeneratedKeys();

  rs.next();
  timeRowId = rs.getString(1);

  stmt.close();
  conn.close();

  return timeRowId;
}


function addNewEditorEmailFunction() {

    var html = HtmlService
     .createTemplateFromFile('Share')
     .evaluate()
     .setTitle('Add new editor email')
     .setWidth(354)
```

```
    .setHeight(300)
    .setSandboxMode(HtmlService.SandboxMode.IFRAME);

  ui.showDialog(html);
}

function isValidEditorEmail(activeUserEmail, docId) {

  var sql = " SELECT editoremails.email " +
            " FROM docs INNER JOIN editoremails " +
            "      ON docs.id = editoremails.doc_id " +
            " WHERE docs.docid = '" + docId + "' " +
            "       AND " +
            "       editoremails.email = '" + activeUserEmail + "' ";

  var connection = createJdbcSSLConnection(dbUrl,  info);
  var SQLstatement = connection.createStatement();
  var result = SQLstatement.executeQuery(sql);


  var isValid;
  if (result.next()) {

    isValid = true;
  } else {

    isValid = false;
  }

  result.close();
  SQLstatement.close();
```

```
  connection.close();

  return isValid;
}

function showDialogBox(dialogBoxTitle) {

  var html = HtmlService

     .createTemplateFromFile('Side')
     .evaluate()
     .setTitle(dialogBoxTitle)
     .setWidth(1000)
     .setHeight(900)
     .setSandboxMode(HtmlService.SandboxMode.IFRAME);

  ui.showSidebar(html);
}

function getContent( ) {

  var content;
  var docId      = DocumentApp.getActiveDocument().getId();
  var encrypted = DocumentApp.getActiveDocument().getText();
  var lastMappedKeyDatails;
  var docRowId;
  var sessionKeyRowId;
  var sessionKey;
  var sessionKeyStartUpStatus;
  var start;
  var end;
```

```
  lastMappedKeyDatails     = getLastMappedKeyByDocIdV2(docId);
  docRowId                 = lastMappedKeyDatails[0];
  sessionKeyRowId          = lastMappedKeyDatails[1];
  sessionKey               = lastMappedKeyDatails[2];
  sessionKeyStartUpStatus = lastMappedKeyDatails[3];

  if (sessionKeyStartUpStatus == 1) {

    start   = new Date();
    content = decrypt(encrypted, sessionKey);
    end     = new Date();

    recordEncryptingSpendTime(docRowId, sessionKeyRowId, 'd', (end - start),
content.length);
    markKeyFromStartUpStatus1To2(sessionKey);

  } else if (sessionKeyStartUpStatus == 2) {

    start   = new Date();
    content = decrypt(encrypted, sessionKey);
    end     = new Date();

    recordEncryptingSpendTime(docRowId, sessionKeyRowId, 'd', (end - start),
content.length);

  } else {

    content = "Illical error, because oldStartUpStatus = " + oldStartUpStatus;
  }
    return content;
```

```
}

function markKeyFromStartUpStatus1To2(oldKey) {

  var conn = createJdbcSSLConnection(dbUrl,  info);
  var date = getDateTimeInMySQLFormat();
  var stmt = conn.prepareStatement( 'UPDATE sessionkeys SET start_up = 2 WHERE
`key` = ? AND start_up = 1 ' );

  stmt.setString(1, oldKey);
  stmt.execute();
  stmt.close();
  conn.close();
}


function getKeyWithStartUpStatus2ByDocId(docId) {

  var connection = createJdbcSSLConnection(dbUrl,  info);

  var SQLstatement = connection.createStatement();

  var sql = " SELECT   sessionkeys.`key`, sessionkeys.start_up " +
            " FROM     docs " +
            "          INNER JOIN mapping ON docs.id = mapping.doc_id " +
            "          INNER JOIN sessionkeys ON sessionkeys.id = mapping.sessionkey_id "
+
            " WHERE    docs.docid = '" + docId + "' AND sessionkeys.start_up = 2 " +
            " ORDER BY mapping.map_date DESC " +
            " LIMIT    1 " ;
```

```
  var result = SQLstatement.executeQuery(sql);

  result.next();
  var key           = result.getString(1);
  var startUpStatus = result.getInt(2);

  result.close();
  SQLstatement.close();
  connection.close();

  return [key, startUpStatus];
}

function getLastMappedKeyByDocIdV2(docId) {

  var connection = createJdbcSSLConnection(dbUrl,  info);

  var SQLstatement = connection.createStatement();

  var sql = " SELECT docs.id, sessionkeys.id, sessionkeys.`key`, sessionkeys.start_up " +
            " FROM    docs " +
            "         INNER JOIN mapping ON docs.id = mapping.doc_id " +
            "         INNER JOIN sessionkeys ON sessionkeys.id = mapping.sessionkey_id " +
            " WHERE  docs.docid = '" + docId + "' " +
            " ORDER BY  mapping.map_date DESC " +
            " LIMIT 1 ";

  var result = SQLstatement.executeQuery(sql);

  result.next();
  var docRowId      = result.getInt(1);
```

```
  var sessionKeyId  = result.getInt(2);
  var sessionKey    = result.getString(3);
  var startUpStatus = result.getInt(4);

  result.close();
  SQLstatement.close();
  connection.close();

  return [docRowId, sessionKeyId, sessionKey, startUpStatus];
}


function getKeyWitchStartUpStatus1ByDocId (docId) {

  var connection = createJdbcSSLConnection(dbUrl,  info);

  var SQLstatement = connection.createStatement();

  var sql = " SELECT sessionkeys.`key`, sessionkeys.start_up " +
            " FROM docs INNER JOIN mapping ON docs.id = mapping.doc_id " +
            "            INNER JOIN sessionkeys ON sessionkeys.id = mapping.sessionkey_id "
+
            " WHERE docs.docid = '" + docId + "' AND sessionkeys.start_up = 1; ";

  var result = SQLstatement.executeQuery(sql);

  result.next();
  var key           = result.getString(1);
  var startUpStatus = result.getInt(2);

  result.close();
```

```
  SQLstatement.close();
  connection.close();

  return [key, startUpStatus];

}

function savePlainText(plainText) {

  var docId      = DocumentApp.getActiveDocument().getId();
  var docRowId  = getDocRowIdByDocId(docId);
  var editors = DocumentApp.getActiveDocument().getEditors();
  var viewers = DocumentApp.getActiveDocument().getViewers();
  var activeUserEmail = Session.getActiveUser().getEmail();
  var effectiveUserEmail = Session.getEffectiveUser().getEmail();
  var oldKeyAndStatus = getKeyWithStartUpStatus2ByDocId(docId);
  var oldKey =        oldKeyAndStatus[0];
  var oldKeyStatus = oldKeyAndStatus[1];

  markKeyFromStartUpStatus2To3(oldKey);

  var sessionKeyRowIdAndNewKey = getNewKeyFromDatabase();
  var sessionKeyRowId = sessionKeyRowIdAndNewKey[0];
  var newKey           = sessionKeyRowIdAndNewKey[1];
  var startTime = new Date();
  var encrypted = encrypt(plainText, newKey);
  var endTime   = new Date();
  recordEncryptingSpendTime(docRowId, sessionKeyRowId, 'e', (endTime - startTime),
plainText.length);

  mapDocIdWithKeyByEffectiveUserEmail(docRowId, sessionKeyRowId,
```

```
effectiveUserEmail);

  markKeyFromStartUpStatusNullTo2(newKey);

  DocumentApp.getActiveDocument().setText(encrypted);

}

function getDocRowIdByDocId(docId) {

  var docRowId;

  var connection = createJdbcSSLConnection(dbUrl,  info);
  var SQLstatement = connection.createStatement();

  var sql = " SELECT id FROM docs where docid = '" + docId + "' ; ";

  var result = SQLstatement.executeQuery(sql);

  result.next();
  docRowId     = result.getInt('id');

  result.close();
  SQLstatement.close();
  connection.close();

  return docRowId;
}

function retriveExistedDocId() {
```

```
  var docId = DocumentApp.getActiveDocument().getId();
  var connection = createJdbcSSLConnection(dbUrl,  info);
  var SQLstatement = connection.createStatement();
  var sql = " SELECT * FROM docs where docid = '" + docId + "' ; ";
  var result = SQLstatement.executeQuery(sql);

  var rowCount = 0;
  while( result.next() ) {
    var row_id     = result.getInt('id');
    var row_docid = result.getString('docid');

    rowCount++;
  }

  result.close();
  SQLstatement.close();
  connection.close();
  return rowCount;
}

function getDateTimeInMySQLFormat() {
  var date = new Date();
  date = date.getUTCFullYear() + '-' +
        ('00' + (date.getUTCMonth()+1)).slice(-2) + '-' +
        ('00' + date.getUTCDate()).slice(-2) + ' ' +
        ('00' + date.getUTCHours()).slice(-2) + ':' +
        ('00' + date.getUTCMinutes()).slice(-2) + ':' +
        ('00' + date.getUTCSeconds()).slice(-2);
  return date;
}
```

```
function insertDocId(docId, editors) {
  var docRowId;
  var conn = createJdbcSSLConnection(dbUrl,  info);
  var stmt = conn.createStatement();
  var date = getDateTimeInMySQLFormat();
  var sql = ' INSERT INTO docs (docid, created_at, owner_email) ' +
            " values ( '" + docId + "', '" + date + "', '" + editors + "' )";
  var count = stmt.executeUpdate(sql,1)
  var rs = stmt.getGeneratedKeys();

  rs.next();
  docRowId = rs.getString(1);
  stmt.close();
  conn.close();
  return docRowId;
}

function addOwnerEmailToEditorEmails(docRowId, editors) {

  var editorEmailRowId;
  var conn = createJdbcSSLConnection(dbUrl,  info);

  var stmt = conn.createStatement();
  var date = getDateTimeInMySQLFormat();
  var sql = ' INSERT INTO editoremails ( doc_id, email, join_at ) ' +
            " values ( '" + docRowId + "', '" + editors + "', '" + date + "' )";
  var count = stmt.executeUpdate(sql,1)
  var rs = stmt.getGeneratedKeys();

  rs.next();
  editorEmailRowId = rs.getString(1);
```

```
  stmt.close();
  conn.close();
  return editorEmailRowId;
}

function getNewKeyFromDatabase() {

  var id;
  var key;
  var conn = createJdbcSSLConnection(dbUrl,  info);

  var stmt = conn.createStatement();
  stmt.setMaxRows(10);

  var sql = " SELECT id, `key` " +
            " FROM sessionkeys " +
            " WHERE       used_at is NULL " +
            "       AND start_up is NULL " +
            " LIMIT 1 ";

  var results = stmt.executeQuery(sql);

  if (results.next()) {
     id  = results.getString(1);
     key = results.getString(2);
  }

  results.close();
  stmt.close();
  conn.close();
```

```
  return [id, key];
}


function markKeyFromStartUpStatus2To3(key) {

  var conn = createJdbcSSLConnection(dbUrl,  info);
  var expiredDate = getDateTimeInMySQLFormat();
  var sql = " UPDATE sessionkeys " +
            " SET    start_up = 3, expired_date = '" + expiredDate + "' " +
            " WHERE      `key` = ? " +
            "        AND start_up = 2 ; ";
  var stmt = conn.prepareStatement( sql );
  stmt.setString(1, key);
  stmt.execute();
  stmt.close();
  conn.close();
}


function markKeyFromStartUpStatusNullTo2(key) {

  var conn = createJdbcSSLConnection(dbUrl,  info);
  var usedDate = getDateTimeInMySQLFormat();
  var sql = " UPDATE sessionkeys " +
            " SET    start_up = 2 , used_at = '" + usedDate + "' " +
            " WHERE      `key` = ? " +
            "        AND start_up IS NULL ";
  var stmt = conn.prepareStatement(sql);
  stmt.setString(1, key);
  stmt.execute();
```

```
  stmt.close();
  conn.close();
}

function markKeyIsStartUpStatus1(newKey) {


  var conn = createJdbcSSLConnection(dbUrl,  info);
  var date = getDateTimeInMySQLFormat();
  var stmt = conn.prepareStatement( 'UPDATE sessionkeys SET used_at = ? , start_up
= 1 WHERE `key` = ? ' );
  stmt.setString(1, date);
  stmt.setString(2, newKey);
  stmt.execute();

  stmt.close();
  conn.close();
}

function mapDocIdWithKey(docRowId, sessionkeyRowId) {

  var conn = createJdbcSSLConnection(dbUrl,  info);
  var stmt = conn.prepareStatement('INSERT INTO mapping '
                                + '(doc_id, sessionkey_id, map_date) values (?, ?, ?)');
  stmt.setString(1, docRowId);
  stmt.setString(2, sessionkeyRowId);
  stmt.setString(3, getDateTimeInMySQLFormat());
  stmt.execute();
  stmt.close();
  conn.close();
```

```
}

function mapDocIdWithKeyByEffectiveUserEmail(docRowId, sessionKeyRowId,
effectiveUserEmail) {

  var mappingRowId;
  var conn = createJdbcSSLConnection(dbUrl,  info);
  var stmt = conn.createStatement();
  var date = getDateTimeInMySQLFormat();
  var sql = ' INSERT INTO mapping ' +
            ' (doc_id, sessionkey_id, map_date, editor_email) ' +
            " values ( '" + docRowId + "', '" + sessionKeyRowId + "', '" + date + "', '" +
effectiveUserEmail + "' )";

  var count = stmt.executeUpdate(sql,1)
  var rs = stmt.getGeneratedKeys();
  rs.next();
  mappingRowId = rs.getString(1);
  stmt.close();
  conn.close();
  return mappingRowId;
}

var CryptoJS=CryptoJS||function(h,r){var
k={},l=k.lib={},n=function(){},f=l.Base={extend:function(a){n.prototype=this;var b=new
n;a&&b.mixIn(a);b.hasOwnProperty("init")||(b.init=function(){b.$super.init.apply(this,argu
ments)});b.init.prototype=b;b.$super=this;return b},create:function(){var
a=this.extend();a.init.apply(a,arguments);return
a},init:function(){},mixIn:function(a){for(var b in
a)a.hasOwnProperty(b)&&(this[b]=a[b]);a.hasOwnProperty("toString")&&(this.toString=a.t
oString)},clone:function(){return this.init.prototype.extend(this)}},
```

j=l.WordArray=f.extend({init:function(a,b){a=this.words=a||[];this.sigBytes=b!=r?b:4*a.len
gth},toString:function(a){return(a||s).stringify(this)},concat:function(a){var
b=this.words,d=a.words,c=this.sigBytes;a=a.sigBytes;this.clamp();if(c%4)for(var
e=0;e<a;e++)b[c+e>>>2]|=(d[e>>>2]>>>24-8*(e%4)&255)<<24-8*((c+e)%4);else
if(65535<d.length)for(e=0;e<a;e+=4)b[c+e>>>2]=d[e>>>2];else
b.push.apply(b,d);this.sigBytes+=a;return this},clamp:function(){var
a=this.words,b=this.sigBytes;a[b>>>2]&=4294967295<<
32-8*(b%4);a.length=h.ceil(b/4)},clone:function(){var
a=f.clone.call(this);a.words=this.words.slice(0);return a},random:function(a){for(var
b=[],d=0;d<a;d+=4)b.push(4294967296*h.random()|0);return new
j.init(b,a)}}),m=k.enc={},s=m.Hex={stringify:function(a){var
b=a.words;a=a.sigBytes;for(var d=[],c=0;c<a;c++){var e=b[c>>>2]>>>24-
8*(c%4)&255;d.push((e>>>4).toString(16));d.push((e&15).toString(16))}return
d.join("")},parse:function(a){for(var
b=a.length,d=[],c=0;c<b;c+=2)d[c>>>3]|=parseInt(a.substr(c,
2),16)<<24-4*(c%8);return new j.init(d,b/2)}},p=m.Latin1={stringify:function(a){var
b=a.words;a=a.sigBytes;for(var
d=[],c=0;c<a;c++)d.push(String.fromCharCode(b[c>>>2]>>>24-8*(c%4)&255));return
d.join("")},parse:function(a){for(var
b=a.length,d=[],c=0;c<b;c++)d[c>>>2]|=(a.charCodeAt(c)&255)<<24-8*(c%4);return
new j.init(d,b)}},t=m.Utf8={stringify:function(a){try{return
decodeURIComponent(escape(p.stringify(a)))}catch(b){throw Error("Malformed UTF-8
data");}},parse:function(a){return p.parse(unescape(encodeURIComponent(a)))}},
q=l.BufferedBlockAlgorithm=f.extend({reset:function(){this._data=new
j.init;this._nDataBytes=0},_append:function(a){"string"==typeof
a&&(a=t.parse(a));this._data.concat(a);this._nDataBytes+=a.sigBytes},_process:function(
a){var
b=this._data,d=b.words,c=b.sigBytes,e=this.blockSize,f=c/(4*e),f=a?h.ceil(f):h.max((f|0)-
this._minBufferSize,0);a=f*e;c=h.min(4*a,c);if(a){for(var
g=0;g<a;g+=e)this._doProcessBlock(d,g);g=d.splice(0,a);b.sigBytes-=c}return new
j.init(g,c)},clone:function(){var a=f.clone.call(this);

a._data=this._data.clone();return
a},_minBufferSize:0});l.Hasher=q.extend({cfg:f.extend(),init:function(a){this.cfg=this.cfg.e
xtend(a);this.reset()},reset:function(){q.reset.call(this);this._doReset()},update:function(a)
{this._append(a);this._process();return
this},finalize:function(a){a&&this._append(a);return
this._doFinalize()},blockSize:16,_createHelper:function(a){return
function(b,d){return(new a.init(d)).finalize(b)}},_createHmacHelper:function(a){return
function(b,d){return(new u.HMAC.init(a,
d)).finalize(b)}}});var u=k.algo={};return k}(Math);

var CryptoJS=CryptoJS||function(u,p){var
d={},l=d.lib={},s=function(){},t=l.Base={extend:function(a){s.prototype=this;var c=new
s;a&&c.mixIn(a);c.hasOwnProperty("init")||(c.init=function(){c.$super.init.apply(this,argum
ents)});c.init.prototype=c;c.$super=this;return c},create:function(){var
a=this.extend();a.init.apply(a,arguments);return
a},init:function(){},mixIn:function(a){for(var c in
a)a.hasOwnProperty(c)&&(this[c]=a[c]);a.hasOwnProperty("toString")&&(this.toString=a.t
oString)},clone:function(){return this.init.prototype.extend(this)}},
r=l.WordArray=t.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=p?c:4*a.len
gth},toString:function(a){return(a||v).stringify(this)},concat:function(a){var
c=this.words,e=a.words,j=this.sigBytes;a=a.sigBytes;this.clamp();if(j%4)for(var
k=0;k<a;k++)c[j+k>>>2]|=(e[k>>>2]>>>24-8*(k%4)&255)<<24-8*((j+k)%4);else
if(65535<e.length)for(k=0;k<a;k+=4)c[j+k>>>2]=e[k>>>2];else
c.push.apply(c,e);this.sigBytes+=a;return this},clamp:function(){var
a=this.words,c=this.sigBytes;a[c>>>2]&=4294967295<<
32-8*(c%4);a.length=u.ceil(c/4)},clone:function(){var
a=t.clone.call(this);a.words=this.words.slice(0);return a},random:function(a){for(var
c=[],e=0;e<a;e+=4)c.push(4294967296*u.random()|0);return new
r.init(c,a)}}),w=d.enc={},v=w.Hex={stringify:function(a){var c=a.words;a=a.sigBytes;for(var
e=[],j=0;j<a;j++){var k=c[j>>>2]>>>24-
8*(j%4)&255;e.push((k>>>4).toString(16));e.push((k&15).toString(16))}return

e.join("")},parse:function(a){for(var
c=a.length,e=[],j=0;j<c;j+=2)e[j>>>3]|=parseInt(a.substr(j,
2),16)<<24-4*(j%8);return new r.init(e,c/2)}},b=w.Latin1={stringify:function(a){var
c=a.words;a=a.sigBytes;for(var
e=[],j=0;j<a;j++)e.push(String.fromCharCode(c[j>>>2]>>>24-8*(j%4)&255));return
e.join("")},parse:function(a){for(var
c=a.length,e=[],j=0;j<c;j++)e[j>>>2]|=(a.charCodeAt(j)&255)<<24-8*(j%4);return new
r.init(e,c)}},x=w.Utf8={stringify:function(a){try{return
decodeURIComponent(escape(b.stringify(a)))}catch(c){throw Error("Malformed UTF-8
data");}},parse:function(a){return b.parse(unescape(encodeURIComponent(a)))}},
q=l.BufferedBlockAlgorithm=t.extend({reset:function(){this._data=new
r.init;this._nDataBytes=0},_append:function(a){"string"==typeof
a&&(a=x.parse(a));this._data.concat(a);this._nDataBytes+=a.sigBytes},_process:function(
a){var
c=this._data,e=c.words,j=c.sigBytes,k=this.blockSize,b=j/(4*k),b=a?u.ceil(b):u.max((b|0)-
this._minBufferSize,0);a=b*k;j=u.min(4*a,j);if(a){for(var
q=0;q<a;q+=k)this._doProcessBlock(e,q);q=e.splice(0,a);c.sigBytes-=j}return new
r.init(q,j)},clone:function(){var a=t.clone.call(this);
a._data=this._data.clone();return
a},_minBufferSize:0});l.Hasher=q.extend({cfg:t.extend(),init:function(a){this.cfg=this.cfg.e
xtend(a);this.reset()},reset:function(){q.reset.call(this);this._doReset()},update:function(a)
{this._append(a);this._process();return
this},finalize:function(a){a&&this._append(a);return
this._doFinalize()},blockSize:16,_createHelper:function(a){return
function(b,e){return(new a.init(e)).finalize(b)}},_createHmacHelper:function(a){return
function(b,e){return(new n.HMAC.init(a,
e)).finalize(b)}}});var n=d.algo={};return d}(Math);
(function(){var u=CryptoJS,p=u.lib.WordArray;u.enc.Base64={stringify:function(d){var
l=d.words,p=d.sigBytes,t=this._map;d.clamp();d=[];for(var r=0;r<p;r+=3)for(var
w=(l[r>>>2]>>>24-8*(r%4)&255)<<16|(l[r+1>>>2]>>>24-
8*((r+1)%4)&255)<<8|l[r+2>>>2]>>>24-

8*((r+2)%4)&255,v=0;4>v&&r+0.75*v<p;v++)d.push(t.charAt(w>>>6*(3-
v)&63));if(l=t.charAt(64))for(;d.length%4;)d.push(l);return d.join("")},parse:function(d){var
l=d.length,s=this._map,t=s.charAt(64);t&&(t=d.indexOf(t),-1!=t&&(l=t));for(var
t=[],r=0,w=0;w<
l;w++)if(w%4){var v=s.indexOf(d.charAt(w-1))<<2*(w%4),b=s.indexOf(d.charAt(w))>>>6-
2*(w%4);t[r>>>2]|=(v|b)<<24-8*(r%4);r++}return
p.create(t,r)},_map:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01
23456789+/="})();
(function(u){function p(b,n,a,c,e,j,k){b=b+(n&a|~n&c)+e+k;return(b<<j|b>>>32-
j)+n}function d(b,n,a,c,e,j,k){b=b+(n&c|a&~c)+e+k;return(b<<j|b>>>32-j)+n}function
l(b,n,a,c,e,j,k){b=b+(n^a^c)+e+k;return(b<<j|b>>>32-j)+n}function
s(b,n,a,c,e,j,k){b=b+(a^(n|~c))+e+k;return(b<<j|b>>>32-j)+n}for(var
t=CryptoJS,r=t.lib,w=r.WordArray,v=r.Hasher,r=t.algo,b=[],x=0;64>x;x++)b[x]=42949672
96*u.abs(u.sin(x+1))|0;r=r.MD5=v.extend({_doReset:function(){this._hash=new
w.init([1732584193,4023233417,2562383102,271733878])},
_doProcessBlock:function(q,n){for(var a=0;16>a;a++){var
c=n+a,e=q[c];q[c]=(e<<8|e>>>24)&16711935|(e<<24|e>>>8)&4278255360}var
a=this._hash.words,c=q[n+0],e=q[n+1],j=q[n+2],k=q[n+3],z=q[n+4],r=q[n+5],t=q[n+6],
w=q[n+7],v=q[n+8],A=q[n+9],B=q[n+10],C=q[n+11],u=q[n+12],D=q[n+13],E=q[n+14],x
=q[n+15],f=a[0],m=a[1],g=a[2],h=a[3],f=p(f,m,g,h,c,7,b[0]),h=p(h,f,m,g,e,12,b[1]),g=p(g,h,
f,m,j,17,b[2]),m=p(m,g,h,f,k,22,b[3]),f=p(f,m,g,h,z,7,b[4]),h=p(h,f,m,g,r,12,b[5]),g=p(g,h,f,
m,t,17,b[6]),m=p(m,g,h,f,w,22,b[7]),
f=p(f,m,g,h,v,7,b[8]),h=p(h,f,m,g,A,12,b[9]),g=p(g,h,f,m,B,17,b[10]),m=p(m,g,h,f,C,22,b[11]
),f=p(f,m,g,h,u,7,b[12]),h=p(h,f,m,g,D,12,b[13]),g=p(g,h,f,m,E,17,b[14]),m=p(m,g,h,f,x,22,b
[15]),f=d(f,m,g,h,e,5,b[16]),h=d(h,f,m,g,t,9,b[17]),g=d(g,h,f,m,C,14,b[18]),m=d(m,g,h,f,c,20
,b[19]),f=d(f,m,g,h,r,5,b[20]),h=d(h,f,m,g,B,9,b[21]),g=d(g,h,f,m,x,14,b[22]),m=d(m,g,h,f,z,2
0,b[23]),f=d(f,m,g,h,A,5,b[24]),h=d(h,f,m,g,E,9,b[25]),g=d(g,h,f,m,k,14,b[26]),m=d(m,g,h,f,
v,20,b[27]),f=d(f,m,g,h,D,5,b[28]),h=d(h,f,
m,g,j,9,b[29]),g=d(g,h,f,m,w,14,b[30]),m=d(m,g,h,f,u,20,b[31]),f=l(f,m,g,h,r,4,b[32]),h=l(h,f,
m,g,v,11,b[33]),g=l(g,h,f,m,C,16,b[34]),m=l(m,g,h,f,E,23,b[35]),f=l(f,m,g,h,e,4,b[36]),h=l(h,f
,m,g,z,11,b[37]),g=l(g,h,f,m,w,16,b[38]),m=l(m,g,h,f,B,23,b[39]),f=l(f,m,g,h,D,4,b[40]),h=l(h

,f,m,g,c,11,b[41]),g=l(g,h,f,m,k,16,b[42]),m=l(m,g,h,f,t,23,b[43]),f=l(f,m,g,h,A,4,b[44]),h=l(h
,f,m,g,u,11,b[45]),g=l(g,h,f,m,x,16,b[46]),m=l(m,g,h,f,j,23,b[47]),f=s(f,m,g,h,c,6,b[48]),h=s(
h,f,m,g,w,10,b[49]),g=s(g,h,f,m,
E,15,b[50]),m=s(m,g,h,f,r,21,b[51]),f=s(f,m,g,h,u,6,b[52]),h=s(h,f,m,g,k,10,b[53]),g=s(g,h,f,
m,B,15,b[54]),m=s(m,g,h,f,e,21,b[55]),f=s(f,m,g,h,v,6,b[56]),h=s(h,f,m,g,x,10,b[57]),g=s(g,h
,f,m,t,15,b[58]),m=s(m,g,h,f,D,21,b[59]),f=s(f,m,g,h,z,6,b[60]),h=s(h,f,m,g,C,10,b[61]),g=s(g
,h,f,m,j,15,b[62]),m=s(m,g,h,f,A,21,b[63]);a[0]=a[0]+f|0;a[1]=a[1]+m|0;a[2]=a[2]+g|0;a[3]=a
[3]+h|0},_doFinalize:function(){var
b=this._data,n=b.words,a=8*this._nDataBytes,c=8*b.sigBytes;n[c>>>5]|=128<<24-
c%32;var e=u.floor(a/
4294967296);n[(c+64>>>9<<4)+15]=(e<<8|e>>>24)&16711935|(e<<24|e>>>8)&427825
5360;n[(c+64>>>9<<4)+14]=(a<<8|a>>>24)&16711935|(a<<24|a>>>8)&4278255360;b.si
gBytes=4*(n.length+1);this._process();b=this._hash;n=b.words;for(a=0;4>a;a++)c=n[a],n
[a]=(c<<8|c>>>24)&16711935|(c<<24|c>>>8)&4278255360;return
b},clone:function(){var b=v.clone.call(this);b._hash=this._hash.clone();return
b}});t.MD5=v._createHelper(r);t.HmacMD5=v._createHmacHelper(r)})(Math);
(function(){var
u=CryptoJS,p=u.lib,d=p.Base,l=p.WordArray,p=u.algo,s=p.EvpKDF=d.extend({cfg:d.exte
nd({keySize:4,hasher:p.MD5,iterations:1}),init:function(d){this.cfg=this.cfg.extend(d)},co
mpute:function(d,r){for(var
p=this.cfg,s=p.hasher.create(),b=l.create(),u=b.words,q=p.keySize,p=p.iterations;u.lengt
h<q;){n&&s.update(n);var n=s.update(d).finalize(r);s.reset();for(var
a=1;a<p;a++)n=s.finalize(n),s.reset();b.concat(n)}b.sigBytes=4*q;return
b}});u.EvpKDF=function(d,l,p){return s.create(p).compute(d,
l)}})();
CryptoJS.lib.Cipher||function(u){var
p=CryptoJS,d=p.lib,l=d.Base,s=d.WordArray,t=d.BufferedBlockAlgorithm,r=p.enc.Base6
4,w=p.algo.EvpKDF,v=d.Cipher=t.extend({cfg:l.extend(),createEncryptor:function(e,a){re
turn this.create(this._ENC_XFORM_MODE,e,a)},createDecryptor:function(e,a){return
this.create(this._DEC_XFORM_MODE,e,a)},init:function(e,a,b){this.cfg=this.cfg.extend(b);t
his._xformMode=e;this._key=a;this.reset()},reset:function(){t.reset.call(this);this._doRese

t()},process:function(e){this._append(e);return this._process()},
finalize:function(e){e&&this._append(e);return
this._doFinalize()},keySize:4,ivSize:4,_ENC_XFORM_MODE:1,_DEC_XFORM_MODE:2,_cre
ateHelper:function(e){return{encrypt:function(b,k,d){return("string"==typeof
k?c:a).encrypt(e,b,k,d)},decrypt:function(b,k,d){return("string"==typeof
k?c:a).decrypt(e,b,k,d)}}}});d.StreamCipher=v.extend({_doFinalize:function(){return
this._process(!0)},blockSize:1});var b=p.mode={},x=function(e,a,b){var
c=this._iv;c?this._iv=u:c=this._prevBlock;for(var d=0;d<b;d++)e[a+d]^=
c[d]},q=(d.BlockCipherMode=l.extend({createEncryptor:function(e,a){return
this.Encryptor.create(e,a)},createDecryptor:function(e,a){return
this.Decryptor.create(e,a)},init:function(e,a){this._cipher=e;this._iv=a}})).extend();q.Encry
ptor=q.extend({processBlock:function(e,a){var
b=this._cipher,c=b.blockSize;x.call(this,e,a,c);b.encryptBlock(e,a);this._prevBlock=e.slic
e(a,a+c)}});q.Decryptor=q.extend({processBlock:function(e,a){var
b=this._cipher,c=b.blockSize,d=e.slice(a,a+c);b.decryptBlock(e,a);x.call(this,
e,a,c);this._prevBlock=d}});b=b.CBC=q;q=(p.pad={}).Pkcs7={pad:function(a,b){for(var
c=4*b,c=c-
a.sigBytes%c,d=c<<24|c<<16|c<<8|c,l=[],n=0;n<c;n+=4)l.push(d);c=s.create(l,c);a.conca
t(c)},unpad:function(a){a.sigBytes-=a.words[a.sigBytes-
1>>>2]&255}};d.BlockCipher=v.extend({cfg:v.cfg.extend({mode:b,padding:q}),reset:func
tion(){v.reset.call(this);var
a=this.cfg,b=a.iv,a=a.mode;if(this._xformMode==this._ENC_XFORM_MODE)var
c=a.createEncryptor;else
c=a.createDecryptor,this._minBufferSize=1;this._mode=c.call(a,
this,b&&b.words)},_doProcessBlock:function(a,b){this._mode.processBlock(a,b)},_doFin
alize:function(){var
a=this.cfg.padding;if(this._xformMode==this._ENC_XFORM_MODE){a.pad(this._data,this.
blockSize);var b=this._process(!0)}else b=this._process(!0),a.unpad(b);return
b},blockSize:4});var
n=d.CipherParams=l.extend({init:function(a){this.mixIn(a)},toString:function(a){return(a||t
his.formatter).stringify(this)}}),b=(p.format={}).OpenSSL={stringify:function(a){var

b=a.ciphertext;a=a.salt;return(a?s.create([1398893684,
1701076831]).concat(a).concat(b):b).toString(r)},parse:function(a){a=r.parse(a);var
b=a.words;if(1398893684==b[0]&&1701076831==b[1]){var
c=s.create(b.slice(2,4));b.splice(0,4);a.sigBytes-=16}return
n.create({ciphertext:a,salt:c})}},a=d.SerializableCipher=l.extend({cfg:l.extend({format:b})
,encrypt:function(a,b,c,d){d=this.cfg.extend(d);var
l=a.createEncryptor(c,d);b=l.finalize(b);l=l.cfg;return
n.create({ciphertext:b,key:c,iv:l.iv,algorithm:a,mode:l.mode,padding:l.padding,blockSiz
e:a.blockSize,formatter:d.format})},
decrypt:function(a,b,c,d){d=this.cfg.extend(d);b=this._parse(b,d.format);return
a.createDecryptor(c,d).finalize(b.ciphertext)},_parse:function(a,b){return"string"==typeof
a?b.parse(a,this):a}}),p=(p.kdf={}).OpenSSL={execute:function(a,b,c,d){d||(d=s.random(8)
);a=w.create({keySize:b+c}).compute(a,d);c=s.create(a.words.slice(b),4*c);a.sigBytes=4*b
;return
n.create({key:a,iv:c,salt:d})}},c=d.PasswordBasedCipher=a.extend({cfg:a.cfg.extend({kdf:
p}),encrypt:function(b,c,d,l){l=this.cfg.extend(l);d=l.kdf.execute(d,
b.keySize,b.ivSize);l.iv=d.iv;b=a.encrypt.call(this,b,c,d.key,l);b.mixIn(d);return
b},decrypt:function(b,c,d,l){l=this.cfg.extend(l);c=this._parse(c,l.format);d=l.kdf.execute
(d,b.keySize,b.ivSize,c.salt);l.iv=d.iv;return a.decrypt.call(this,b,c,d.key,l)}})}();
(function(){for(var
u=CryptoJS,p=u.lib.BlockCipher,d=u.algo,l=[],s=[],t=[],r=[],w=[],v=[],b=[],x=[],q=[],n=[],a
=[],c=0;256>c;c++)a[c]=128>c?c<<1:c<<1^283;for(var e=0,j=0,c=0;256>c;c++){var
k=j^j<<1^j<<2^j<<3^j<<4,k=k>>>8^k&255^99;l[e]=k;s[k]=e;var
z=a[e],F=a[z],G=a[F],y=257*a[k]^16843008*k;t[e]=y<<24|y>>>8;r[e]=y<<16|y>>>16;w[e
]=y<<8|y>>>24;v[e]=y;y=16843009*G^65537*F^257*z^16843008*e;b[k]=y<<24|y>>>8;
x[k]=y<<16|y>>>16;q[k]=y<<8|y>>>24;n[k]=y;e?(e=z^a[a[a[G^z]]],j^=a[a[j]]):e=j=1}var
H=[0,1,2,4,8,
16,32,64,128,27,54],d=d.AES=p.extend({_doReset:function(){for(var
a=this._key,c=a.words,d=a.sigBytes/4,a=4*((this._nRounds=d+6)+1),e=this._keySchedul
e=[],j=0;j<a;j++)if(j<d)e[j]=c[j];else{var k=e[j-
1];j%d?6<d&&4==j%d&&(k=l[k>>>24]<<24|l[k>>>16&255]<<16|l[k>>>8&255]<<8|l[k&2

55]):(k=k<<8|k>>>24,k=l[k>>>24]<<24|l[k>>>16&255]<<16|l[k>>>8&255]<<8|l[k&255],k^=H[j/d|0]<<24);e[j]=e[j-d]^k}c=this._invKeySchedule=[];for(d=0;d<a;d++)j=a-d,k=d%4?e[j]:e[j-4],c[d]=4>d||4>=j?k:b[l[k>>>24]]^x[l[k>>>16&255]]^q[l[k>>>8&255]]^n[l[k&255]]},encryptBlock:function(a,b){this._doCryptBlock(a,b,this._keySchedule,t,r,w,v,l)},decryptBlock:function(a,c){var d=a[c+1];a[c+1]=a[c+3];a[c+3]=d;this._doCryptBlock(a,c,this._invKeySchedule,b,x,q,n,s);d=a[c+1];a[c+1]=a[c+3];a[c+3]=d},_doCryptBlock:function(a,b,c,d,e,j,l,f){for(var m=this._nRounds,g=a[b]^c[0],h=a[b+1]^c[1],k=a[b+2]^c[2],n=a[b+3]^c[3],p=4,r=1;r<m;r++)var q=d[g>>>24]^e[h>>>16&255]^j[k>>>8&255]^l[n&255]^c[p++],s=d[h>>>24]^e[k>>>16&255]^j[n>>>8&255]^l[g&255]^c[p++],t=d[k>>>24]^e[n>>>16&255]^j[g>>>8&255]^l[h&255]^c[p++],n=d[n>>>24]^e[g>>>16&255]^j[h>>>8&255]^l[k&255]^c[p++],g=q,h=s,k=t;q=(f[g>>>24]<<24|f[h>>>16&255]<<16|f[k>>>8&255]<<8|f[n&255])^c[p++];s=(f[h>>>24]<<24|f[k>>>16&255]<<16|f[n>>>8&255]<<8|f[g&255])^c[p++];t=(f[k>>>24]<<24|f[n>>>16&255]<<16|f[g>>>8&255]<<8|f[h&255])^c[p++];n=(f[n>>>24]<<24|f[g>>>16&255]<<16|f[h>>>8&255]<<8|f[k&255])^c[p++];a[b]=q;a[b+1]=s;a[b+2]=t;a[b+3]=n},keySize:8});u.AES=p._createHelper(d)})();

var CryptoJS=CryptoJS||function(e,m){var p={},j=p.lib={},l=function(){},f=j.Base={extend:function(a){l.prototype=this;var c=new l;a&&c.mixIn(a);c.hasOwnProperty("init")||(c.init=function(){c.$super.init.apply(this,arguments)});c.init.prototype=c;c.$super=this;return c},create:function(){var a=this.extend();a.init.apply(a,arguments);return a},init:function(){},mixIn:function(a){for(var c in a)a.hasOwnProperty(c)&&(this[c]=a[c]);a.hasOwnProperty("toString")&&(this.toString=a.toString)},clone:function(){return this.init.prototype.extend(this)}},n=j.WordArray=f.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=m?c:4*a.length},toString:function(a){return(a||h).stringify(this)},concat:function(a){var c=this.words,q=a.words,d=this.sigBytes;a=a.sigBytes;this.clamp();if(d%4)for(var b=0;b<a;b++)c[d+b>>>2]|=(q[b>>>2]>>>24-8*(b%4)&255)<<24-8*((d+b)%4);else if(65535<q.length)for(b=0;b<a;b+=4)c[d+b>>>2]=q[b>>>2];else

c.push.apply(c,q);this.sigBytes+=a;return this},clamp:function(){var
a=this.words,c=this.sigBytes;a[c>>>2]&=4294967295<<
32-8*(c%4);a.length=e.ceil(c/4)},clone:function(){var
a=f.clone.call(this);a.words=this.words.slice(0);return a},random:function(a){for(var
c=[],b=0;b<a;b+=4)c.push(4294967296*e.random()|0);return new
n.init(c,a)}}),b=p.enc={},h=b.Hex={stringify:function(a){var c=a.words;a=a.sigBytes;for(var
b=[],d=0;d<a;d++){var f=c[d>>>2]>>>24-
8*(d%4)&255;b.push((f>>>4).toString(16));b.push((f&15).toString(16))}return
b.join("")},parse:function(a){for(var
c=a.length,b=[],d=0;d<c;d+=2)b[d>>>3]|=parseInt(a.substr(d,
2),16)<<24-4*(d%8);return new n.init(b,c/2)}},g=b.Latin1={stringify:function(a){var
c=a.words;a=a.sigBytes;for(var
b=[],d=0;d<a;d++)b.push(String.fromCharCode(c[d>>>2]>>>24-8*(d%4)&255));return
b.join("")},parse:function(a){for(var
c=a.length,b=[],d=0;d<c;d++)b[d>>>2]|=(a.charCodeAt(d)&255)<<24-8*(d%4);return
new n.init(b,c)}},r=b.Utf8={stringify:function(a){try{return
decodeURIComponent(escape(g.stringify(a)))}catch(c){throw Error("Malformed UTF-8
data");}},parse:function(a){return g.parse(unescape(encodeURIComponent(a)))}},
k=j.BufferedBlockAlgorithm=f.extend({reset:function(){this._data=new
n.init;this._nDataBytes=0},_append:function(a){"string"==typeof
a&&(a=r.parse(a));this._data.concat(a);this._nDataBytes+=a.sigBytes},_process:function(
a){var
c=this._data,b=c.words,d=c.sigBytes,f=this.blockSize,h=d/(4*f),h=a?e.ceil(h):e.max((h|0)
-this._minBufferSize,0);a=h*f;d=e.min(4*a,d);if(a){for(var
g=0;g<a;g+=f)this._doProcessBlock(b,g);g=b.splice(0,a);c.sigBytes-=d}return new
n.init(g,d)},clone:function(){var a=f.clone.call(this);
a._data=this._data.clone();return
a},_minBufferSize:0});j.Hasher=k.extend({cfg:f.extend(),init:function(a){this.cfg=this.cfg.ex
tend(a);this.reset()},reset:function(){k.reset.call(this);this._doReset()},update:function(a){
this._append(a);this._process();return
this},finalize:function(a){a&&this._append(a);return

this._doFinalize()},blockSize:16,_createHelper:function(a){return
function(c,b){return(new a.init(b)).finalize(c)}},_createHmacHelper:function(a){return
function(b,f){return(new s.HMAC.init(a,
f)).finalize(b)}}});var s=p.algo={};return p}(Math);
(function(){var
e=CryptoJS,m=e.lib,p=m.WordArray,j=m.Hasher,l=[],m=e.algo.SHA1=j.extend({_doRese
t:function(){this._hash=new
p.init([1732584193,4023233417,2562383102,271733878,3285377520])},_doProcessBloc
k:function(f,n){for(var
b=this._hash.words,h=b[0],g=b[1],e=b[2],k=b[3],j=b[4],a=0;80>a;a++){if(16>a)l[a]=f[n+a]
|0;else{var c=l[a-3]^l[a-8]^l[a-14]^l[a-
16];l[a]=c<<1|c>>>31}c=(h<<5|h>>>27)+j+l[a];c=20>a?c+((g&e|~g&k)+1518500249):40>
a?c+((g^e^k)+1859775393):60>a?c+((g&e|g&k|e&k)-1894007588):c+((g^e^
k)-
899497514);j=k;k=e;e=g<<30|g>>>2;g=h;h=c}b[0]=b[0]+h|0;b[1]=b[1]+g|0;b[2]=b[2]+e|0;
b[3]=b[3]+k|0;b[4]=b[4]+j|0},_doFinalize:function(){var
f=this._data,e=f.words,b=8*this._nDataBytes,h=8*f.sigBytes;e[h>>>5]|=128<<24-
h%32;e[(h+64>>>9<<4)+14]=Math.floor(b/4294967296);e[(h+64>>>9<<4)+15]=b;f.sigB
ytes=4*e.length;this._process();return this._hash},clone:function(){var
e=j.clone.call(this);e._hash=this._hash.clone();return
e}});e.SHA1=j._createHelper(m);e.HmacSHA1=j._createHmacHelper(m)})();

(function(){var
e=CryptoJS,f=e.lib.WordArray,e=e.enc;e.Utf16=e.Utf16BE={stringify:function(b){var
d=b.words;b=b.sigBytes;for(var
c=[],a=0;a<b;a+=2)c.push(String.fromCharCode(d[a>>>2]>>>16-8*(a%4)&65535));return
c.join("")},parse:function(b){for(var
d=b.length,c=[],a=0;a<d;a++)c[a>>>1]|=b.charCodeAt(a)<<16-16*(a%2);return
f.create(c,2*d)}};e.Utf16LE={stringify:function(b){var d=b.words;b=b.sigBytes;for(var
c=[],a=0;a<b;a+=2)c.push(String.fromCharCode((d[a>>>2]>>>16-
8*(a%4)&65535)<<8&4278255360|(d[a>>>

2]>>>16-8*(a%4)&65535)>>>8&16711935));return c.join("")},parse:function(b){for(var d=b.length,c=[],a=0;a<d;a++){var e=c,g=a>>>1,j=e[g],h=b.charCodeAt(a)<<16-16*(a%2);e[g]=j|h<<8&4278255360|h>>>8&16711935}return f.create(c,2*d)}}})();

(function(){var h=CryptoJS,j=h.lib.WordArray;h.enc.Base64={stringify:function(b){var e=b.words,f=b.sigBytes,c=this._map;b.clamp();b=[];for(var a=0;a<f;a+=3)for(var d=(e[a>>>2]>>>24-8*(a%4)&255)<<16|(e[a+1>>>2]>>>24-8*((a+1)%4)&255)<<8|e[a+2>>>2]>>>24-8*((a+2)%4)&255,g=0;4>g&&a+0.75*g<f;g++)b.push(c.charAt(d>>>6*(3-g)&63));if(e=c.charAt(64))for(;b.length%4;)b.push(e);return b.join("")},parse:function(b){var e=b.length,f=this._map,c=f.charAt(64);c&&(c=b.indexOf(c),-1!=c&&(e=c));for(var c=[],a=0,d=0;d<e;d++)if(d%4){var g=f.indexOf(b.charAt(d-1))<<2*(d%4),h=f.indexOf(b.charAt(d))>>>6-2*(d%4);c[a>>>2]|=(g|h)<<24-8*(a%4);a++}return j.create(c,a)},_map:"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/="}})();

var address = 'ap-cdbr-azure-east-c.cloudapp.net';
var user = 'b6f144a4d170db';
var userPwd = '3c53e10dbe73613';
var db = 'smulcloud';
var dbUrl = 'jdbc:mysql://' + address + '/' + db + '?useSSL=true';

var ui = DocumentApp.getUi();

var theDefaultDummyText = "\n Welcome to TrustDocs. Your Content\n is encrypted with Auto-Generate Key.\n This activity is done on your Browser.\n\n Only YOU can see and edit your text\n but non-Realtime edit (Version Control)\n\n Do NOT change directly in Google Docs.\n Only this page, you can edit as follow:\n\n Single editor step:\n 1. Delete this all text on this page\n 2. Start

write your text\n 3. Finish then Click 'Save' before Close\n Multiple editor step:\n 1. Menu Add ons>TrustDocs>Share\n 2. Enter Your Collaborator Email\n 3. Click 'Add' and 'Ok' then close dialog\n 4. Menu File>Share.. finish this step\n\n This Instruction be shown only this time !\n\n Delete All then Start !"

var _serverSslCertificate = '-----BEGIN CERTIFICATE-----
\nMIIEBzCCAu+gAwIBAgIJAPs/TPnO24QSMA0GCSqGSIb3DQEBBQUAMIGZMQswCQYD\n
VQQGEwJVUzEOMAwGA1UECAwFVGV4YXMxDTALBgNVBAcMBFdhY28xHTAbBgNVBAoM
\nFFN1Y2Nlc3NCcmlja3MgSW5jIENBMRQwEgYDVQQLDAtFbmdpbmVlcmluZzESMBAG\
nA1UEAwwJQ0EgTWFzdGVyMSIwIAYJKoZIhvcNAQkBFhNzdXBwb3J0QGNsZWFyZGlu\nY
29tMB4XDTExMDgwOTE5NTcxOVoXDTM4MTIyNDE5NTcxOVowgZkxCzAJBgNVBAYT\nAl
VTMQ4wDAYDVQQIDAVUZXhhczENMAsGA1UEBwwEV2FjbzEdMBsGA1UECgwUU3Vj\nY2
Vzc0JyaWNrcyBJbmMgQ0ExFDASBgNVBAsMC0VuZ2luZWVyaW5nMRIwEAYDVQQD\nDAl
DQSBNYXN0ZXIxIjAgBgkqhkiG9w0BCQEWE3N1cHBvcnRAY2xlYXJkYi5jb20w\nggEiMA0GC
SqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDl3xOV5yj2XkwCgMZ2H3AV\nTZrGf/LhuX1E
ByOaoYeutBQfzb049wp4olmFhcL7ZXmsBJb3/7fYwyxs6rbJ0diz\nnGFATOaEWE7yNm14
glagL6xb+Arqh9TrlF77Wts32RHIQvCAt1Sw8VeoBhWKLp96\ngCC1ZRSHEdh0qaTOFXRgE
UGXOmtPtwiNaDwVsaYN82a9AfhKqdygRMzAPYZk29cr\njZy13CMgz8JZIGEKRxTqbl8ClR
+A6aW3Opgf6hD/vASGigGfgbjNNPeEHUUYHj8y\nW3OWn7CrItdm/2TXG0xdks5VPJonHY
5KdhSLobJZCyR9Oc00bT4gSOsDEKO4+t3J\nAgMBAAGjUDBOMB0GA1UdDgQWBBRs1gy
V3ammzQYMNt78zZpXDz74GzAfBgNVHSME\nGDAWgBRs1gyV3ammzQYMNt78zZpXDz
74GzAMBgNVHRMEBTADAQH/MA0GCSqGSIb3\nDQEBBQUAA4IBAQATIQy8MJ9aZ4z6our
kHeY/RmkfMF2lfpknsPWkab/DpTkfQ4Zt\nAv8ZP+lCYzdoBm98FJoOhLNJxgI4M1jHg4ub
ccoL6r+MWBUMCT5KW6zFyom9p1wY\nD8dpIdzV8cTmsJTt3vrUWkC+aP2Dz3EaMHzH1
4JyLRxqhoOOr456y6HD4SXEwzW3\n8n8N9J15Rpp6Am/y+dVEXquUf0Qj7l67ElIgDByBit
V4AVUnmmu7C/Kn+GzTKFet\nyLGbEXgbgalggtnUltm4nFIrcOh51xxnTNtWDNktD06/0Os
s5OY901VVwSm0JmV0\nLtNgymxXhQAJVDVaIAn4C0/Hh8GudcAs/QKv\n-----END
CERTIFICATE-----';

var _clientSslCertificate = '-----BEGIN CERTIFICATE-----
\nMIIEEjCCAvqgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBmTELMAkGA1UEBhMCVVMx\nDj

AMBgNVBAgMBVRleGFzMQ0wCwYDVQQHDARXYWNvMR0wGwYDVQQKDBRTdWNjZXNz
\nQnJpY2tzIEluYyBDQTEUMBIGA1UECwwLRW5naW5lZXJpbmcxEjAQBgNVBAMMCUNB\
nIE1hc3RlcjEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBjbGVhcmRiLmNvbTAeFw0x\nNTEy
MTAwNTUzMDhaFw00MzA0MjYwNTUzMDhaMIGsMQswCQYDVQQGEwJVUzEQMA4G\nA
1UECAwHQmFuZ2tvazEQMA4GA1UEBwwHQmFuZ2tvazEQMA4GA1UECgwHQ2xlYXJE\n
QjEUMBIGA1UECwwLRW5naW5lZXJpbmcxKjAoBgNVBAMMIU1vaGFtbWFkc2hhcmVl\nZ
nVkZGluIFNhbGFzaC1hcm9uZzElMCMGCSqGSIb3DQEJARYWbW9tby5zaGFyZWVm\nQG
dtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANg8j1w2\nSWN2
46niC3vZ0/bT6zRzMetfgz8tYrtY/1c4wpHtmNpbg+lttl731A8geVpUejOQ\nqmv7xeMuAC
Tuzr3arZODJpM1IcAPcAckXBu8Jltb8i3u4njQdxFJXhV4zLdApyBd\nmw5po8PyTM/WQug
fDWhINvlsraAFHxpRp3xp8l8Ac60cx/liWrTBobQyjoSvfATd\nOPReHeMEH6XyGe133i+3Cc
ZyHdTz8oBwDB7GqGFjvLH0kZxzX3aw92mMDS1Z+cH8\n5cl1BdQqgeAlGtgNXdCa0asQ
uIgnrCe9TtVe5rq+7sbC5UMS1XAhCZrUjgRRdLCi\nBCnuboWsa79jdX8CAwEAAaNQME4w
HQYDVR0OBBYEFFIOjgb6luwZ+UuQPZ9CcyDR\nrDgnMB8GA1UdIwQYMBaAFGzWDJXdq
abNBgw23vzNmlcPPvgbMAwGA1UdEwQFMAMB\nAf8wDQYJKoZIhvcNAQELBQADggEBA
K+Row60Xh1zcK0CZAn7nI1+TDBHY0o+pH2l\nFV0sTawKQkIFEZvWp+lm9tsasJq3mONv
Xa9BodO9QJeYjZl+0bWM2X/+9qnSUlND\n6HXrKN3V3qGOBnC9XTqlz5lM9o63FPhedE/
o0e5uQuDZ0K79VEM/vuy4UowcBKTR\n+B65fe3l9Hcv3Ijcjvy/14PVdbKrFzsjtlLRbe91XxF
gmmCfxAWTaQ2cx9Px1Wl3\ngXyfp+M6ojfUuvtaZbIUdpQ37NBGGNyEZafAfJK2vL/gaM0
9bLB5J7Esbk+mpnfA\nzCJfMWWwfZqbLKKv+OUXCfeYEIX3OsLMbNCuDYuC/2WeyHvb
OMk=\n-----END CERTIFICATE-----';

var _clientSslKey = '-----BEGIN PRIVATE KEY-----
\nMIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQDYPI9cNkljduOp\n4gt72
dP20+s0czHrX4M/LWK7WP9XOMKR7ZjaW4PpbbZe99QPIHlaVHozkKpr+8Xj\nLgAk7s69
2q2TgyaTNSHAD3AHJFwbvCSLW/It7uJ40HcRSV4VeMy3QKcgXZsOaaPD\n8kzP1kLoHw1
oSDb5bK2gBR8aUad8afJfAHOtHMf5Ylq0waG0Mo6Er3wE3Tj0Xh3j\nBB+l8hntd94vtwnG
ch3U8/KAcAwexqhhY7yx9JGcc192sPdpjA0tWfnB/OXJdQXU\nKoHgJRrYDV3QmtGrELiIJ6
wnvU7VXua6vu7GwuVDEtVwIQma1I4EUXSwogQp7m6F\nrGu/Y3V/AgMBAAECggEBAIWg
xydBFRE2g3KUkmwzLN44D/4Vwh+mosEEFyOX2BPa\nq8Lqha9LJrW2ayE9HftLIjNESVBc
cjTRHnVKFCS+v1xsKyAhyFDoYLcD00NWoOUy\n25KTe5IPMj1e9nXkVRQH1trYRW+m6Q

97EQ0iS32U9zvjFLIBDpgNJS7ie1oUY+Bp\npV5UdXBff8o8mBDkjCNWOE9cSCQFLAHW0u
R8jPhoXX1k0NrrezluK45EAlowarRZ\n465uQsb1drXFlSbdEDVq8eABSro+e0l+n3YLwTH+
lY7hOT3GWdlqiUuMDYdXzuG+\n5flCrd1tL4C2r1YI+pfVSdZxcQxi5i0OxxyD0xGKmSECgY
EA+e7EGtKu4QnzBjGV\nTr8wY51BhF75Do7ykEJXr/unswN5WlJE5CVc0/UZfvGvdfHNwi0
1tYUYBJoXNwM9\nkbjhEfOzSPFcu1Azm++CVGoAXhoobOZS+/2dJR0VTWRloEN3+4sTj6
5ROW8sH07U\nYHlEvq+bRMI5ZaZnLegvYP2QPnUCgYEA3XxiwT7TcP/+UlQdpyDJDapw
4NCP8dEj\nHC7SztpsPsb8lE0feu538LhwOsgAwGuYy3ON7COUrut55hPp/B0qq3YCWl8+
qUxQ\nWbUNXmZxjYCJsMau8evTFNvhVnlHAXdXtly/K2oXhy3l895yWuW9nSTajHv5TZS
D\nW4wMm19ozaMCgYEAsqzjPVnI89CtEIx59SXxbgWKRRuwaZwABOmozoLWTL/7DXsr\
nDP848b6TT5Fwop0PP/YaI37WwNN4LTf/2CGXpcHXNhp29OJNQvli7v4o7R0+MTwn\nr0
aMBXBZPk676GrTZ9zxSxKPtsOng2pTofSQFNJt6iX/6o+fy83lsS0U5dECgYEA\nmb/c9fTc5
pZuP0xxATF7H+dvUEC3i8/4JXpDkKCDf9i2QWSAM+ASlqlSFlv8WZbX\njHP80y2n6v0/s3
2jcgX1Nu1GmOGBKBj3ti4+x4cp0GaoLnTdwMZJ0zMH6/VoWxYz\nZz5e3o5ZItezx2Rl0b+
lrs6Ef/0XhMlRnl1L6xeCMy0CgYAuBivEpiG0W8dFuHRn\njwmrKM3MUkkH+vKuDa9Ts+iH
9MzwAlkj1SFPl2+6G5xlHSKBeaUdriMb8m7ZxdSw\n+9QY3CiqmOVOOODolVlZaqqs+im
D1/+0CAso+gtqctn9qyq+ZZVqYhxrbWWvvWAv\nFW5egyO6l9rrp0Yaup5Wz4sgwA==\n
-----END PRIVATE KEY-----';

var useJDBCCompliantTimeZoneShift = false;


```
var info = {
        password    : userPwd,
        user        : user,

        useJDBCCompliantTimeZoneShift :  useJDBCCompliantTimeZoneShift,
        _serverSslCertificate : _serverSslCertificate,
        _clientSslCertificate : _clientSslCertificate,
        _clientSslKey : _clientSslKey
};

function encrypt(plainText, key) {
```

```
  var encrypted;

  encrypted = CryptoJS.AES.encrypt( plainText, key);
  encrypted = encrypted + '';

  return encrypted;
}

function decrypt(encrypted, key) {
  var content;
  var decrypted;

  decrypted = CryptoJS.AES.decrypt(encrypted, key);
  content = CryptoJS.enc.Utf8.stringify(decrypted);

  return content;
}

function addNewEmail(newEditorEmail) {

  newEditorEmail        = newEditorEmail.trim();
  var addedSuccess      = false;
  var editorEmailRowId = -1;

  var docId             = DocumentApp.getActiveDocument().getId();
  var activeUserEmail   = Session.getActiveUser().getEmail();

  if ( isValidEditorEmail(activeUserEmail, docId) ) {

  } else {
```

```
    return addedSuccess;
  }

  var docRowIdAndEmailBoolean = getExistedEditorEmailBy(docId, newEditorEmail);
  var docRowId = docRowIdAndEmailBoolean[0];
  var existedEmailBoolean = docRowIdAndEmailBoolean[1];

  if ( existedEmailBoolean == true ) {

    return addedSuccess;

  } else if ( existedEmailBoolean == false ) {

    editorEmailRowId = addEditorEmailToEditorEmailTableBy(docRowId,
newEditorEmail);
  } else {

  }

  if (editorEmailRowId != -1) {
    addedSuccess = true;
  }

  return addedSuccess;

function getExistedEditorEmailBy(docId, newEditorEmail) {

  var docRowId = getDocRowIdByDocId(docId);

   var sql2 = ' SELECT editoremails.email ' +
              ' FROM    editoremails   ' +
```

```
            ' WHERE        editoremails.doc_id = "' + docRowId + '" ' +
            '         AND ' +
            '              editoremails.email  = "' + newEditorEmail + '" ';

  var connection = createJdbcSSLConnection(dbUrl,  info);
  var SQLstatement = connection.createStatement();
  var result = SQLstatement.executeQuery(sql2);



  var existedEmailBoolean;
  if (result.next()) {

     existedEmailBoolean = true;
  } else {

     existedEmailBoolean = false;
  }

  result.close();
  SQLstatement.close();
  connection.close();

  return [docRowId, existedEmailBoolean];
}

function addEditorEmailToEditorEmailTableBy(docRowId, newEditorEmail) {

  var editorEmailRowId;

  var conn = createJdbcSSLConnection(dbUrl,  info);
  var stmt = conn.createStatement();
```

```
  var date = getDateTimeInMySQLFormat();

  var sql = " INSERT INTO editoremails (doc_id, email, join_at ) " +
          " values ( '" + docRowId + "', '" + newEditorEmail + "', '" + date + "' ) ";

  var count = stmt.executeUpdate(sql,1)
  var rs = stmt.getGeneratedKeys();

  rs.next();
  editorEmailRowId = rs.getString(1);
  stmt.close();
  conn.close();

  return editorEmailRowId;
  }
}
```

ข.2 Side.html

Source Code ส่วนใหญ่ในไฟล์ Side.html จะใช้ภาษาไลบรารี่ของ HTML ที่ไว้ควบคุมการทำงานของเอกสารกูเกิ้ลในส่วนหน้าบ้าน หรือบนหน้าเว็ปบราวเซอร์ที่แสดงผลเป็น Side Bar บนเอกสารกูเกิ้ลที่สนับสนุนการทำงานการจัดการกับข้อมูลสำคัญหรือข้อมูลลับของผู้ใช้งาน

```
<!DOCTYPE html>
<html>
 <head>
  <base target="_top">
  <script
src="https://ajax.googleapis.com/ajax/libs/jquery/1.12.4/jquery.min.js"></script>
  <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css"
  integrity="sha384-
BVYiiSIFeK1dGmJRAkycuHAHRg32OmUcww7on3RYdg4Va+PmSTsz/K68vbdEjh4u"
crossorigin="anonymous">
  <link rel="stylesheet"
href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap-
```

```
theme.min.css"
   integrity="sha384-
rHyoN1iRsVXV4nD0JutlnGaslCJuC7uwjduW9SVrLvRYooPp2bWYgmgJQIXwl/Sp"
crossorigin="anonymous">
   <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js"
   integrity="sha384-
Tc5IQib027qvyjSMfHjOMaLkfuWVxZxUPnCJA7l2mCWNIpG9mGCD8wGNIcPD7Txa"
crossorigin="anonymous"></script>
   <script
src="https://cdnjs.cloudflare.com/ajax/libs/Trumbowyg/2.3.0/trumbowyg.min.js"
   integrity="sha256-bmGihvwwwjimzKboiicxTaciToROxZrEwOMCjPSGlvE="
crossorigin="anonymous"></script>
   <script
src="https://cdnjs.cloudflare.com/ajax/libs/Trumbowyg/2.3.0/langs/sv.min.js"
   integrity="sha256-2CvGlJbXM6ls7tR5HV3gASa69xGMJ1RAcr9Orybd9AA="
crossorigin="anonymous"></script>
   <link rel="stylesheet"
href="https://cdnjs.cloudflare.com/ajax/libs/Trumbowyg/2.3.0/ui/trumbowyg.min.c
ss" crossorigin="anonymous">
 </head>
 <body>
   <form>
    <div id="trumbowyg-icons">
     <svg xmlns="http://www.w3.org/2000/svg">
     <symbol id="trumbowyg-blockquote" viewBox="0 0 72 72">
     <path d="M21.3 31.9h-.6c.8-1.2 1.9-2.2 3.4-3.2 2.1-1.4 5-2.7 9.2-3.3l-1.4-8.9c-
4.7.7-8.5 2.1-11.7 4-2.4 1.4-4.3 3.1-5.8 4.9-2.3 2.7-3.7 5.7-4.5 8.5-.8 2.8-1 5.4-1 7.5 0
2.3.3 4 .4 4.8 0 .1.1.3.1.4 1.2 5.4 6.1 9.5 11.9 9.5 6.7 0 12.2-5.4 12.2-12.2s-5.5-12-
12.2-12zM49.5 31.9h-.6c.8-1.2 1.9-2.2 3.4-3.2 2.1-1.4 5-2.7 9.2-3.3l-1.4-8.9c-4.7.7-
8.5 2.1-11.7 4-2.4 1.4-4.3 3.1-5.8 4.9-2.3 2.7-3.7 5.7-4.5 8.5-.8 2.8-1 5.4-1 7.5 0 2.3.3
4 .4 4.8 0 .1.1.3.1.4 1.2 5.4 6.1 9.5 11.9 9.5 6.7 0 12.2-5.4 12.2-12.2s-5.5-12-12.2-
12z"/></symbol><symbol id="trumbowyg-bold" viewBox="0 0 72 72"><path
d="M51.1 37.8c-1.1-1.4-2.5-2.5-4.2-3.3 1.2-.8 2.1-1.8 2.8-3 1-1.6 1.5-3.5 1.5-5.3 0-2-
.6-4-1.7-5.8-1.1-1.8-2.8-3.2-4.8-4.1-2-.9-4.6-1.3-7.8-1.3h-16v42h16.3c2.6 0 4.8-.2
6.7-.7 1.9-.5 3.4-1.2 4.7-2.1 1.3-1 2.4-2.4 3.2-4.1.9-1.7 1.3-3.6 1.3-5.7.2-2.5-.5-4.7-2-
6.6zM40.8 50.2c-.6.1-1.8.2-3.4.2h-9V38.5h8.3c2.5 0 4.4.2 5.6.6 1.2.4 2 1 2.7 2 .6.9 1
2 1 3.3 0 1.1-.2 2.1-.7 2.9-.5.9-1 1.5-1.7 1.9-.8.4-1.7.8-2.8 1zm2.6-20.4c-.5.7-1.3 1.3-
2.5 1.6-.8.3-2.5.4-4.8.4h-7.7V21.6h7.1c1.4 0 2.6 0 3.6.1s1.7.2 2.2.4c1 .3 1.7.8 2.2
1.7.5.9.8 1.8.8 3-.1 1.3-.4 2.2-.9 3z"/></symbol><symbol id="trumbowyg-close"
viewBox="0 0 72 72"><path d="M57 20.5l-5.4-5.4-15.5 15.5-15.6-15.5-5.4 5.4L30.7
36 15.1 51.5l5.4 5.4 15.6-15.5 15.5 15.5 5.4-5.4L41.5 36z"/></symbol><symbol
id="trumbowyg-create-link" viewBox="0 0 72 72"><path d="M31.1 48.9l-6.7 6.7c-
.8.8-1.6.9-2.1.9s-1.4-.1-2.1-.9L15 50.4c-1.1-1.1-1.1-3.1 0-4.2l6.1-6.1.2-.2 6.5-6.5c-1.2-
.6-2.5-.9-3.8-.9-2.3 0-4.6.9-6.3 2.6L11 41.8c-3.5 3.5-3.5 9.2 0 12.7l5.2 5.2c1.7 1.7 4
```

2.6 6.3 2.6s4.6-.9 6.3-2.6l6.7-6.7c2.5-2.6 3.1-6.7 1.5-10l-5.9 5.9zM38.7 22.5l6.7-6.7c.8-.8 1.6-.9 2.1-.9s1.4.1 2.1.9l5.2 5.2c1.1 1.1 1.1 3.1 0 4.2l-6.1 6.1-.2.2L42 38c1.2.6 2.5.9 3.8.9 2.3 0 4.6-.9 6.3-2.6l6.7-6.7c3.5-3.5 3.5-9.2 0-12.7l-5.2-5.2c-1.7-1.7-4-2.6-6.3-2.6s-4.6.9-6.3 2.6l-6.7 6.7c-2.7 2.7-3.3 6.9-1.7 10.2l6.1-6.1c0 .1 0 .1 0 0z"/><path d="M44.2 30.5c.2-.2.4-.6.4-.9 0-.3-.1-.6-.4-.9l-2.3-2.3c-.3-.2-.6-.4-.9-.4-.3 0-.6.1-.9.4L25.9 40.6c-.2.2-.4.6-.4.9 0 .3.1.6.4.9l2.3 2.3c.2.2.6.4.9.4.3 0 .6-.1.9-.4l14.2-14.2zM49.9 55.4h-8.5v-5h8.5v-8.9h5.2v8.9h8.5v5h-8.5v8.9h-5.2v-8.9z"/></symbol><symbol id="trumbowyg-del" viewBox="0 0 72 72"><path d="M45.8 45c0 1-.3 1.9-.9 2.8-.6.9-1.6 1.6-3 2.1s-3.1.8-5 .8c-2.1 0-4-.4-5.7-1.1-1.7-.7-2.9-1.7-3.6-2.7-.8-1.1-1.3-2.6-1.5-4.5l-.1-.8-6.7.6v.9c.1 2.8.9 5.4 2.3 7.6 1.5 2.3 3.5 4 6.1 5.1 2.6 1.1 5.7 1.6 9.4 1.6 2.9 0 5.6-.5 8-1.6 2.4-1.1 4.3-2.7 5.6-4.7 1.3-2 2-4.2 2-6.5 0-1.6-.3-3.1-.9-4.5l-.2-.6H44c0 .1 1.8 2.3 1.8 5.5zM29 28.9c-.8-.8-1.2-1.7-1.2-2.9 0-.7.1-1.3.4-1.9.3-.6.7-1.1 1.4-1.6.6-.5 1.4-.9 2.5-1.1 1.1-.3 2.4-.4 3.9-.4 2.9 0 5 .6 6.3 1.7 1.3 1.1 2.1 2.7 2.4 5.1l.1.9 6.8-.5v-.9c-.1-2.5-.8-4.7-2.1-6.7s-3.2-3.5-5.6-4.5c-2.4-1-5.1-1.5-8.1-1.5-2.8 0-5.3.5-7.6 1.4-2.3 1-4.2 2.4-5.4 4.3-1.2 1.9-1.9 3.9-1.9 6.1 0 1.7.4 3.4 1.2 4.9l.3.5h11.8c-2.3-.9-3.9-1.7-5.2-2.9zm13.3-6.2zM22.7 20.3zM13 34.1h46.1v3.4H13z"/></symbol><symbol id="trumbowyg-em" viewBox="0 0 72 72"><path d="M26 57l10.1-42h7.2L33.2 57H26z"/></symbol><symbol id="trumbowyg-fullscreen" viewBox="0 0 72 72"><path d="M25.2 7.1H7.1v17.7l6.7-6.5 10.5 10.5 4.5-4.5-10.4-10.5zM47.2 7.1l6.5 6.7-10.5 10.5 4.5 4.5 10.5-10.4 6.7 6.8V7.1zM47.7 43.2l-4.5 4.5 10.4 10.5-6.8 6.7h18.1V47.2l-6.7 6.5zM24.3 43.2L13.8 53.6l-6.7-6.8v18.1h17.7l-6.5-6.7 10.5-10.5z"/><path fill="currentColor" d="M10.7 28.8h18.1V11.2l-6.6 6.4L11.6 7.1l-4.5 4.5 10.5 10.5zM60.8 28.8l-6.4-6.6 10.5-10.6-4.5-4.5-10.5 10.5-6.7-6.9v18.1zM60.4 64.9l4.5-4.5-10.5-10.5 6.9-6.7H43.2v17.6l6.6-6.4zM11.6 64.9l10.5-10.5 6.7 6.9V43.2H11.1l6.5 6.6L7.1 60.4z"/></symbol><symbol id="trumbowyg-h1" viewBox="0 0 72 72"><path d="M6.4 14.9h7.4v16.7h19.1V14.9h7.4V57h-7.4V38H13.8v19H6.4V14.9zM47.8 22.5c1.4 0 2.8-.1 4.1-.4 1.3-.2 2.5-.6 3.6-1.2 1.1-.5 2-1.3 2.8-2.1.8-.9 1.3-1.9 1.5-3.2h5.5v41.2h-7.4v-29H47.8v-5.3z"/></symbol><symbol id="trumbowyg-h2" viewBox="0 0 72 72"><path d="M1.5 14.9h7.4v16.7H28V14.9h7.4V57H28V38H8.8v19H1.5V14.9zM70.2 56.9H42c0-3.4.9-6.4 2.5-9s3.8-4.8 6.6-6.7c1.3-1 2.7-1.9 4.2-2.9 1.5-.9 2.8-1.9 4-3 1.2-1.1 2.2-2.2 3-3.4.8-1.2 1.2-2.7 1.2-4.3 0-.7-.1-1.5-.3-2.4s-.5-1.6-1-2.4c-.5-.7-1.2-1.3-2.1-1.8-.9-.5-2.1-.7-3.5-.7-1.3 0-2.4.3-3.3.8s-1.6 1.3-2.1 2.2-.9 2-1.2 3.3c-.3 1.3-.4 2.6-.4 4.1h-6.7c0-2.3.3-4.4.9-6.3.6-1.9 1.5-3.6 2.7-5 1.2-1.4 2.7-2.5 4.4-3.3 1.7-.8 3.8-1.2 6.1-1.2 2.5 0 4.6.4 6.3 1.2 1.7.8 3.1 1.9 4.1 3.1 1 1.3 1.8 2.6 2.2 4.1.4 1.5.6 2.9.6 4.2 0 1.6-.3 3.1-.8 4.5-.5 1.3-1.2 2.6-2.1 3.7-.9 1.1-1.8 2.2-2.9 3.1-1.1.9-2.2 1.8-3.4 2.7-1.2.8-2.4 1.6-3.5 2.4-1.2.7-2.3 1.5-3.3 2.2-1 .7-1.9 1.5-2.6 2.3-.7.8-1.3 1.7-1.5 2.6h20.1v5.9z"/></symbol><symbol id="trumbowyg-h3" viewBox="0 0 72 72"><path d="M1.4 14.5h7.4v16.7h19.1V14.5h7.4v42.1h-7.4v-19H8.8v19H1.4V14.5zM53.1 32.4c1.1 0 2.2 0 3.3-.2 1.1-.2 2.1-.5 2.9-1 .9-.5 1.6-1.2 2.1-2 .5-.9.8-1.9.8-3.2 0-1.8-.6-3.2-1.8-4.2-1.2-1.1-2.7-1.6-4.6-1.6-1.2 0-2.2.2-3.1.7-.9.5-1.6 1.1-2.2 1.9-.6.8-1 1.7-1.3 2.7-.3 1-.4 2-.4 3.1h-6.7c.1-2 .5-3.9 1.1-5.6.7-1.7 1.6-3.2 2.7-4.4s2.6-2.2 4.2-2.9c1.6-.7 3.5-1.1 5.6-1.1 1.6 0 3.2.2 4.7.7 1.6.5 2.9 1.2 4.2 2.1 1.2.9 2.2 2.1 3 3.4.7 1.4 1.1 3 1.1 4.8 0 2.1-.5 3.9-1.4 5.4-.9 1.6-2.4 2.7-4.4 3.4v.1c2.4.5 4.2 1.6 5.5 3.5 1.3 1.9 2 4.1

2 6.8 0 2-.4 3.7-1.2 5.3-.8 1.6-1.8 2.9-3.2 3.9-1.3 1.1-2.9 1.9-4.7 2.5-1.8.6-3.6.9-5.6.9-2.4 0-4.5-.3-6.3-1s-3.3-1.7-4.5-2.9c-1.2-1.3-2.1-2.8-2.7-4.5-.6-1.8-1-3.7-1-5.9h6.7c-.1 2.5.5 4.6 1.9 6.3 1.3 1.7 3.3 2.5 5.9 2.5 2.2 0 4.1-.6 5.6-1.9 1.5-1.3 2.3-3.1 2.3-5.4 0-1.6-.3-2.9-.9-3.8-.6-.9-1.5-1.7-2.5-2.2-1-.5-2.2-.8-3.4-.9-1.3-.1-2.6-.2-3.9-.1v-5.2z"/></symbol><symbol id="trumbowyg-h4" viewBox="0 0 72 72"><path d="M1.5 14.9h7.4v16.7H28V14.9h7.4V57H28V38H8.9v19H1.5V14.9zM70.5 47.2h-5.3V57h-6.4v-9.8H41.2v-6.7l17.7-24.8h6.4v26.2h5.3v5.3zm-24.2-5.3h12.5V23.7h-.1L46.3 41.9z"/></symbol><symbol id="trumbowyg-horizontal-rule" viewBox="0 0 72 72"><path d="M9.1 32h54v8h-54z"/></symbol><symbol id="trumbowyg-insert-image" viewBox="0 0 72 72"><path d="M64 17v38H8V17h56m8-8H0v54h72V9z"/><path d="M17.5 22C15 22 13 24 13 26.5s2 4.5 4.5 4.5 4.5-2 4.5-4.5-2-4.5-4.5-4.5zM16 50h27L29.5 32zM36 36.2l8.9-8.5L60.2 50H45.9S35.6 35.9 36 36.2z"/></symbol><symbol id="trumbowyg-italic" viewBox="0 0 72 72"><path d="M26 57l10.1-42h7.2L33.2 57H26z"/></symbol><symbol id="trumbowyg-justify-center" viewBox="0 0 72 72"><path d="M9 14h54v8H9zM9 50h54v8H9zM18 32h36v8H18z"/></symbol><symbol id="trumbowyg-justify-full" viewBox="0 0 72 72"><path d="M9 14h54v8H9zM9 50h54v8H9zM9 32h54v8H9z"/></symbol><symbol id="trumbowyg-justify-left" viewBox="0 0 72 72"><path d="M9 14h54v8H9zM9 50h54v8H9zM9 32h36v8H9z"/></symbol><symbol id="trumbowyg-justify-right" viewBox="0 0 72 72"><path d="M9 14h54v8H9zM9 50h54v8H9zM27 32h36v8H27z"/></symbol><symbol id="trumbowyg-link" viewBox="0 0 72 72"><path d="M30.9 49.1l-6.7 6.7c-.8.8-1.6.9-2.1.9s-1.4-.1-2.1-.9l-5.2-5.2c-1.1-1.1-1.1-3.1 0-4.2l6.1-6.1.2-.2 6.5-6.5c-1.2-.6-2.5-.9-3.8-.9-2.3 0-4.6.9-6.3 2.6L10.8 42c-3.5 3.5-3.5 9.2 0 12.7l5.2 5.2c1.7 1.7 4 2.6 6.3 2.6s4.6-.9 6.3-2.6l6.7-6.7C38 50.5 38.6 46.3 37 43l-6.1 6.1zM38.5 22.7l6.7-6.7c.8-.8 1.6-.9 2.1-.9s1.4.1 2.1.9l5.2 5.2c1.1 1.1 1.1 3.1 0 4.2l-6.1 6.1-.2.2-6.5 6.5c1.2.6 2.5.9 3.8.9 2.3 0 4.6-.9 6.3-2.6l6.7-6.7c3.5-3.5 3.5-9.2 0-12.7l-5.2-5.2c-1.7-1.7-4-2.6-6.3-2.6s-4.6.9-6.3 2.6l-6.7 6.7c-2.7 2.7-3.3 6.9-1.7 10.2l6.1-6.1z"/><path d="M44.1 30.7c.2-.2.4-.6.4-.9 0-.3-.1-.6-.4-.9l-2.3-2.3c-.2-.2-.6-.4-.9-.4-.3 0-.6.1-.9.4L25.8 40.8c-.2.2-.4.6-.4.9 0 .3.1.6.4.9l2.3 2.3c.2.2.6.4.9.4.3 0 .6-.1.9-.4l14.2-14.2z"/></symbol><symbol id="trumbowyg-ordered-list" viewBox="0 0 72 72"><path d="M27 14h36v8H27zM27 50h36v8H27zM27 32h36v8H27zM11.8 15.8V22h1.8v-7.8h-1.5l-2.1 1 .3 1.3zM12.1 38.5l.7-.6c1.1-1 2.1-2.1 2.1-3.4 0-1.4-1-2.4-2.7-2.4-1.1 0-2 .4-2.6.8l.5 1.3c.4-.3 1-.6 1.7-.6.9 0 1.3.5 1.3 1.1 0 .9-.9 1.8-2.6 3.3l-1 .9V40H15v-1.5h-2.9zM13.3 53.9c1-.4 1.4-1 1.4-1.8 0-1.1-.9-1.9-2.6-1.9-1 0-1.9.3-2.4.6l.4 1.3c.3-.2 1-.5 1.6-.5.8 0 1.2.3 1.2.8 0 .7-.8.9-1.4.9h-.7v1.3h.7c.8 0 1.6.3 1.6 1.1 0 .6-.5 1-1.4 1-.7 0-1.5-.3-1.8-.5l-.4 1.4c.5.3 1.3.6 2.3.6 2 0 3.2-1 3.2-2.4 0-1.1-.8-1.8-1.7-1.9z"/></symbol><symbol id="trumbowyg-p" viewBox="0 0 72 72"><path d="M47.8 15.1H30.1c-4.7 0-8.5 3.7-8.5 8.4s3.7 8.4 8.4 8.4v25h7V19.8h3v37.1h4.1V19.8h3.7v-4.7z"/></symbol><symbol id="trumbowyg-redo" viewBox="0 0 72 72"><path d="M10.8 51.2c0-5.1 2.1-9.7 5.4-13.1 3.3-3.3 8-5.4 13.1-5.4H46v-12L61.3 36 45.9 51.3V39.1H29.3c-3.3 0-6.4 1.3-8.5 3.5-2.2 2.2-3.5 5.2-3.5 8.5h-6.5z"/></symbol><symbol id="trumbowyg-removeformat" viewBox="0 0 72 72"><path d="M58.2 54.6L52 48.5l3.6-3.6 6.1 6.1 6.4-6.4 3.8 3.8-6.4 6.4 6.1 6.1-3.6 3.6-6.1-6.1-6.4 6.4-3.7-3.8 6.4-6.4zM21.7 52.1H50V57H21.7zM18.8

15.2h34.1v6.4H39.5v24.2h-7.4V21.5H18.8v-6.3z"/></symbol><symbol id="trumbowyg-strikethrough" viewBox="0 0 72 72"><path d="M45.8 45c0 1-.3 1.9-.9 2.8-.6.9-1.6 1.6-3 2.1s-3.1.8-5 .8c-2.1 0-4-.4-5.7-1.1-1.7-.7-2.9-1.7-3.6-2.7-.8-1.1-1.3-2.6-1.5-4.5l-.1-.8-6.7.6v.9c.1 2.8.9 5.4 2.3 7.6 1.5 2.3 3.5 4 6.1 5.1 2.6 1.1 5.7 1.6 9.4 1.6 2.9 0 5.6-.5 8-1.6 2.4-1.1 4.3-2.7 5.6-4.7 1.3-2 2-4.2 2-6.5 0-1.6-.3-3.1-.9-4.5l-.2-.6H44c0 .1 1.8 2.3 1.8 5.5zM29 28.9c-.8-.8-1.2-1.7-1.2-2.9 0-.7.1-1.3.4-1.9.3-.6.7-1.1 1.4-1.6.6-.5 1.4-.9 2.5-1.1 1.1-.3 2.4-.4 3.9-.4 2.9 0 5 .6 6.3 1.7 1.3 1.1 2.1 2.7 2.4 5.1l.1.9 6.8-.5v-.9c-.1-2.5-.8-4.7-2.1-6.7s-3.2-3.5-5.6-4.5c-2.4-1-5.1-1.5-8.1-1.5-2.8 0-5.3.5-7.6 1.4-2.3 1-4.2 2.4-5.4 4.3-1.2 1.9-1.9 3.9-1.9 6.1 0 1.7.4 3.4 1.2 4.9l.3.5h11.8c-2.3-.9-3.9-1.7-5.2-2.9zm13.3-6.2zM22.7 20.3zM13 34.1h46.1v3.4H13z"/></symbol><symbol id="trumbowyg-strong" viewBox="0 0 72 72"><path d="M51.1 37.8c-1.1-1.4-2.5-2.5-4.2-3.3 1.2-.8 2.1-1.8 2.8-3 1-1.6 1.5-3.5 1.5-5.3 0-2-.6-4-1.7-5.8-1.1-1.8-2.8-3.2-4.8-4.1-2-.9-4.6-1.3-7.8-1.3h-16v42h16.3c2.6 0 4.8-.2 6.7-.7 1.9-.5 3.4-1.2 4.7-2.1 1.3-1 2.4-2.4 3.2-4.1.9-1.7 1.3-3.6 1.3-5.7.2-2.5-.5-4.7-2-6.6zM40.8 50.2c-.6.1-1.8.2-3.4.2h-9V38.5h8.3c2.5 0 4.4.2 5.6.6 1.2.4 2 1 2.7 2 .6.9 1 2 1 3.3 0 1.1-.2 2.1-.7 2.9-.5.9-1 1.5-1.7 1.9-.8.4-1.7.8-2.8 1zm2.6-20.4c-.5.7-1.3 1.3-2.5 1.6-.8.3-2.5.4-4.8.4h-7.7V21.6h7.1c1.4 0 2.6 0 3.6.1s1.7.2 2.2.4c1 .3 1.7.8 2.2 1.7.5.9.8 1.8.8 3-.1 1.3-.4 2.2-.9 3z"/></symbol><symbol id="trumbowyg-subscript" viewBox="0 0 72 72"><path d="M32 15h7.8L56 57.1h-7.9L44.3 46H27.4l-4 11.1h-7.6L32 15zm-2.5 25.4h12.9L36 22.3h-.2l-6.3 18.1zM58.7 59.9c.6-1.4 2-2.8 4.1-4.4 1.9-1.3 3.1-2.3 3.7-2.9.8-.9 1.3-1.9 1.3-3 0-.9-.2-1.6-.7-2.2-.5-.6-1.2-.9-2.1-.9-1.2 0-2.1.5-2.5 1.4-.3.5-.4 1.4-.5 2.5h-4c.1-1.8.4-3.2 1-4.3 1.1-2.1 3-3.1 5.8-3.1 2.2 0 3.9.6 5.2 1.8 1.3 1.2 1.9 2.8 1.9 4.8 0 1.5-.5 2.9-1.4 4.1-.6.8-1.6 1.7-3 2.6L66 57.7c-1 .7-1.7 1.2-2.1 1.6-.4.3-.7.7-1 1.1H72V64H57.8c0-1.5.3-2.8.9-4.1z"/></symbol><symbol id="trumbowyg-superscript" viewBox="0 0 72 72"><path d="M32 15h7.8L56 57.1h-7.9l-4-11.1H27.4l-4 11.1h-7.6L32 15zm-2.5 25.4h12.9L36 22.3h-.2l-6.3 18.1zM49.6 28.8c.5-1.1 1.6-2.3 3.4-3.6 1.5-1.1 2.5-1.9 3-2.4.7-.7 1-1.6 1-2.4 0-.7-.2-1.3-.6-1.8-.4-.5-1-.7-1.7-.7-.7 0-1.7.4-2.1 1.1-.2.4-.3 1.1-.4 2.1H49c.1-1.5.3-2.6.8-3.5.9-1.7 2.5-2.6 4.8-2.6 1.8 0 3.2.5 4.3 1.5 1.1 1 1.6 2.3 1.6 4 0 1.3-.4 2.4-1.1 3.4-.5.7-1.3 1.4-2.4 2.2l-1.3 1c-.8.6-1.4 1-1.7 1.3-.3.3-.6.6-.8.9h7.4v3H48.8c0-1.3.3-2.4.8-3.5z"/></symbol><symbol id="trumbowyg-table" viewBox="0 0 72 72"><path d="M25.686 51.38v-6.347q0-.462-.297-.76-.298-.297-.761-.297H14.04q-.463 0-.761.297-.298.298-.298.76v6.346q0 .463.298.76.298.298.761.298h10.589q.463 0 .76-.298.298-.297.298-.76zm0-12.692v-6.346q0-.463-.297-.76-.298-.298-.761-.298H14.04q-.463 0-.761.298-.298.297-.298.76v6.346q0 .462.298.76.298.297.761.297h10.589q.463 0 .76-.297.298-.298.298-.76zm16.94 12.691v-6.346q0-.462-.297-.76-.298-.298-.761-.298H30.98q-.463 0-.76.297-.299.298-.299.76v6.346q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76zm-16.94-25.383v-6.345q0-.463-.297-.76-.298-.298-.761-.298H14.04q-.463 0-.761.298-.298.297-.298.76v6.345q0 .463.298.76.298.298.761.298h10.589q.463 0 .76-.298.298-.297.298-.76zm16.94 12.691v-6.346q0-.463-.297-.76-.298-.298-.761-.298H30.98q-.463 0-.76.298-.299.297-.299.76v6.346q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76zm16.94-12.691v-6.345q0-.463-.297-.76-.298-.298-.761-.298H47.92q-.463 0-.76.298-.299.297-.299.76v6.345q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76z"/></symbol><symbol id="trumbowyg-table-add" viewBox="0 0 72 72"><path d="M25.686 51.38v-6.347q0-.462-.297-.76-.298-.297-.761-.297H14.04q-.463 0-.761.297-.298.298-.298.76v6.346q0 .463.298.76.298.298.761.298h10.589q.463 0 .76-.298.298-.297.298-.76zm0-12.692v-6.346q0-.463-.297-.76-.298-.298-.761-.298H14.04q-.463 0-.761.298-.298.297-.298.76v6.346q0 .462.298.76.298.297.761.297h10.589q.463 0 .76-.297.298-.298.298-.76zm16.94 12.691v-6.346q0-.462-.297-.76-.298-.298-.761-.298H30.98q-.463 0-.76.297-.299.298-.299.76v6.346q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76zm-16.94-25.383v-6.345q0-.463-.297-.76-.298-.298-.761-.298H14.04q-.463 0-.761.298-.298.297-.298.76v6.345q0 .463.298.76.298.298.761.298h10.589q.463 0 .76-.298.298-.297.298-.76zm16.94 12.691v-6.346q0-.463-.297-.76-.298-.298-.761-.298H30.98q-.463 0-.76.298-.299.297-.299.76v6.346q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76zm16.94-12.691v-6.345q0-.463-.297-.76-.298-.298-.761-.298H47.92q-.463 0-.76.298-.299.297-.299.76v6.345q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76z"/></symbol>

.463.297.76.298.298.761.298h10.588q.463 0 .761-.298.298-.297.298-.76zm-16.94-25.383v-6.345q0-.463-.297-.76-.298-.298-.761-.298H30.98q-.463 0-.76.297-.299.298-.299.76v6.346q0 .463.298.76.298.298.761.298h10.588q.463 0 .76-.298.299-.297.299-.76zm16.94 12.692v-6.346q0-.463-.297-.76-.298-.298-.761-.298H47.92q-.463 0-.76.298-.298.297-.298.76v6.346q0 .462.297.76.298.297.761.297h10.588q.463 0 .761-.297.298-.298.298-.76zm0-12.692v-6.345q0-.463-.297-.76-.298-.298-.761-.298H47.92q-.463 0-.76.297-.298.298-.298.76v6.346q0 .463.298.76.298.298.761.298h10.588q.463 0 .761-.298.298-.297.298-.76zm4.236-10.576v35.96q0 2.18-1.555 3.734-1.555 1.553-3.739 1.553H14.04q-2.184 0-3.739-1.553-1.555-1.555-1.555-3.735V15.42q0-2.181 1.555-3.735 1.555-1.553 3.739-1.553h44.468q2.184 0 3.739 1.553 1.555 1.554 1.555 3.735z"/></symbol><symbol id="trumbowyg-underline" viewBox="0 0 72 72"><path d="M36 35zM15.2 55.9h41.6V59H15.2zM21.1 13.9h6.4v21.2c0 1.2.1 2.5.2 3.7.1 1.3.5 2.4 1 3.4.6 1 1.4 1.8 2.6 2.5 1.1.6 2.7 1 4.8 1 2.1 0 3.7-.3 4.8-1 1.1-.6 2-1.5 2.6-2.5.6-1 .9-2.1 1-3.4.1-1.3.2-2.5.2-3.7V13.9H51v23.3c0 2.3-.4 4.4-1.1 6.1-.7 1.7-1.7 3.2-3 4.4-1.3 1.2-2.9 2-4.7 2.6-1.8.6-3.9.9-6.1.9-2.2 0-4.3-.3-6.1-.9-1.8-.6-3.4-1.5-4.7-2.6-1.3-1.2-2.3-2.6-3-4.4-.7-1.7-1.1-3.8-1.1-6.1V13.9z"/></symbol><symbol id="trumbowyg-undo" viewBox="0 0 72 72"><path d="M61.2 51.2c0-5.1-2.1-9.7-5.4-13.1-3.3-3.3-8-5.4-13.1-5.4H26.1v-12L10.8 36l15.3 15.3V39.1h16.7c3.3 0 6.4 1.3 8.5 3.5 2.2 2.2 3.5 5.2 3.5 8.5h6.4z"/></symbol><symbol id="trumbowyg-unlink" viewBox="0 0 72 72"><path d="M30.9 49.1l-6.7 6.7c-.8.8-1.6.9-2.1.9s-1.4-.1-2.1-.9l-5.2-5.2c-1.1-1.1-1.1-3.1 0-4.2l6.1-6.1.2-.2 6.5-6.5c-1.2-.6-2.5-.9-3.8-.9-2.3 0-4.6.9-6.3 2.6L10.8 42c-3.5 3.5-3.5 9.2 0 12.7l5.2 5.2c1.7 1.7 4 2.6 6.3 2.6s4.6-.9 6.3-2.6l6.7-6.7C38 50.5 38.6 46.3 37 43l-6.1 6.1zM38.5 22.7l6.7-6.7c.8-.8 1.6-.9 2.1-.9s1.4.1 2.1.9l5.2 5.2c1.1 1.1 1.1 3.1 0 4.2l-6.1 6.1-.2.2-6.5 6.5c1.2.6 2.5.9 3.8.9 2.3 0 4.6-.9 6.3-2.6l6.7-6.7c3.5-3.5 3.5-9.2 0-12.7l-5.2-5.2c-1.7-1.7-4-2.6-6.3-2.6s-4.6.9-6.3 2.6l-6.7 6.7c-2.7 2.7-3.3 6.9-1.7 10.2l6.1-6.1z"/><path d="M44.1 30.7c.2-.2.4-.6.4-.9 0-.3-.1-.6-.4-.9l-2.3-2.3c-.2-.2-.6-.4-.9-.4-.3 0-.6.1-.9.4L25.8 40.8c-.2.2-.4.6-.4.9 0 .3.1.6.4.9l2.3 2.3c.2.2.6.4.9.4.3 0 .6-.1.9-.4l14.2-14.2zM41.3 55.8v-5h22.2v5H41.3z"/></symbol><symbol id="trumbowyg-unordered-list" viewBox="0 0 72 72"><path d="M27 14h36v8H27zM27 50h36v8H27zM9 50h9v8H9zM9 32h9v8H9zM9 14h9v8H9zM27 32h36v8H27z"/></symbol><symbol id="trumbowyg-view-html" viewBox="0 0 72 72"><path fill="none" stroke="currentColor" stroke-width="8" stroke-miterlimit="10" d="M26.9 17.9L9 36.2 26.9 54M45 54l17.9-18.3L45 17.9"/></symbol><symbol id="trumbowyg-base64" viewBox="0 0 72 72"><path d="M64 17v38H8V17h56m8-8H0v54h72V9z"/><path d="M29.9 28.9c-.5-.5-1.1-.8-1.8-.8s-1.4.2-1.9.7c-.5.4-.9 1-1.2 1.6-.3.6-.5 1.3-.6 2.1-.1.7-.2 1.4-.2 1.9l.1.1c.6-.8 1.2-1.4 2-1.8.8-.4 1.7-.5 2.7-.5.9 0 1.8.2 2.6.6.8.4 1.6.9 2.2 1.5.6.6 1 1.3 1.2 2.2.3.8.4 1.6.4 2.5 0 1.1-.2 2.1-.5 3-.3.9-.8 1.7-1.5 2.4-.6.7-1.4 1.2-2.3 1.6-.9.4-1.9.6-3 .6-1.6 0-2.8-.3-3.9-.9-1-.6-1.8-1.4-2.5-2.4-.6-1-1-2.1-1.3-3.4-.2-1.3-.4-2.6-.4-3.9 0-1.3.1-2.6.4-3.8.3-1.3.8-2.4 1.4-3.5.7-1 1.5-1.9 2.5-2.5 1-.6 2.3-1 3.8-1 .9 0 1.7.1 2.5.4.8.3 1.4.6 2 1.1.6.5 1.1 1.1 1.4 1.8.4.7.6 1.5.7 2.5h-4c0-1-.3-1.6-.8-2.1zm-3.5 6.8c-.4.2-.8.5-1 .8-.3.4-.5.8-.6 1.2-.1.5-.2 1-.2 1.5s.1.9.2 1.4c.1.5.4.9.6 1.2.3.4.6.7 1 .9.4.2.9.3 1.4.3.5 0 1-.1 1.3-.3.4-.2.7-.5 1-.9.3-.4.5-.8.6-1.2.1-.5.2-.9.2-1.4 0-.5-.1-1-.2-1.4-.1-.5-.3-.9-.6-1.2-.3-.4-.6-.7-1-.9-.4-.2-.9-.3-1.4-.3-.4 0-.9.1-1.3.3zM36.3 41.3v-

3.8l9-12.1H49v12.4h2.7v3.5H49v4.8h-4v-4.8h-8.7zM45 30.7l-5.3 7.2h5.4l-.1-7.2z"/></symbol><symbol id="trumbowyg-back-color" viewBox="0 0 72 72"><path d="M36.5 22.3l-6.3 18.1H43l-6.3-18.1z"/><path d="M9 8.9v54.2h54.1V8.9H9zm39.9 48.2L45 46H28.2l-3.9 11.1h-7.6L32.8 15h7.8l16.2 42.1h-7.9z"/></symbol><symbol id="trumbowyg-fore-color" viewBox="0 0 72 72"><path d="M32 15h7.8L56 57.1h-7.9l-4-11.1H27.4l-4 11.1h-7.6L32 15zm-2.5 25.4h12.9L36 22.3h-.2l-6.3 18.1z"/></symbol><symbol id="trumbowyg-emoji" viewBox="0 0 72 72"><path d="M36.05 9C21.09 9 8.949 21.141 8.949 36.101c0 14.96 12.141 27.101 27.101 27.101 14.96 0 27.101-12.141 27.101-27.101S51.01 9 36.05 9zm9.757 15.095c2.651 0 4.418 1.767 4.418 4.418s-1.767 4.418-4.418 4.418-4.418-1.767-4.418-4.418 1.767-4.418 4.418-4.418zm-19.479 0c2.651 0 4.418 1.767 4.418 4.418s-1.767 4.418-4.418 4.418-4.418-1.767-4.418-4.418 1.767-4.418 4.418-4.418zm9.722 30.436c-14.093 0-16.261-13.009-16.261-13.009h32.522S50.143 54.531 36.05 54.531z"/></symbol><symbol id="trumbowyg-insert-audio" viewBox="0 0 8 8"><path d="M3.344 0L2 2H0v4h2l1.344 2H4V0h-.656zM5 1v1c.152 0 .313.026.469.063H5.5c.86.215 1.5.995 1.5 1.938a1.99 1.99 0 0 1-2 2.001v1a2.988 2.988 0 0 0 3-3 2.988 2.988 0 0 0-3-3zm0 2v2l.25-.031C5.683 4.851 6 4.462 6 4c0-.446-.325-.819-.75-.938v-.031h-.031L5 3z"/></symbol><symbol id="trumbowyg-noembed" viewBox="0 0 72 72"><path d="M31.5 33.6V25l11 11-11 11v-8.8z"/><path d="M64 17v38H8V17h56m8-8H0v54h72V9z"/></symbol><symbol id="trumbowyg-preformatted" viewBox="0 0 72 72"><path d="M10.3 33.5c.4 0 .9-.1 1.5-.2s1.2-.3 1.8-.7c.6-.3 1.1-.8 1.5-1.3.4-.5.6-1.3.6-2.1V17.1c0-1.4.3-2.6.8-3.6s1.2-1.9 2-2.5c.8-.7 1.6-1.2 2.5-1.5.9-.3 1.6-.5 2.2-.5h5.3v5.3h-3.2c-.7 0-1.3.1-1.8.4-.4.3-.8.6-1 1-.2.4-.4.9-.4 1.3-.1.5-.1.9-.1 1.4v11.4c0 1.2-.2 2.1-.7 2.9-.5.8-1 1.4-1.7 1.8-.6.4-1.3.8-2 1-.7.2-1.3.3-1.7.4v.1c.5 0 1 .1 1.7.3.7.2 1.3.5 2 .9.6.5 1.2 1.1 1.7 1.9.5.8.7 2 .7 3.4v11.1c0 .4 0 .9.1 1.4.1.5.2.9.4 1.3s.6.7 1 1c.4.3 1 .4 1.8.4h3.2V63h-5.3c-.6 0-1.4-.2-2.2-.5-.9-.3-1.7-.8-2.5-1.5s-1.4-1.5-2-2.5c-.5-1-.8-2.2-.8-3.6V43.5c0-.9-.2-1.7-.6-2.3-.4-.6-.9-1.1-1.5-1.5-.6-.4-1.2-.6-1.8-.7-.6-.1-1.1-.2-1.5-.2v-5.3zM61.8 38.7c-.4 0-1 .1-1.6.2-.6.1-1.2.4-1.8.7-.6.3-1.1.7-1.5 1.3-.4.5-.6 1.3-.6 2.1v12.1c0 1.4-.3 2.6-.8 3.6s-1.2 1.9-2 2.5c-.8.7-1.6 1.2-2.5 1.5-.9.3-1.6.5-2.2.5h-5.3v-5.3h3.2c.7 0 1.3-.1 1.8-.4.4-.3.8-.6 1-1 .2-.4.4-.9.4-1.3.1-.5.1-.9.1-1.4V42.3c0-1.2.2-2.1.7-2.9.5-.8 1-1.4 1.7-1.8.6-.4 1.3-.8 2-1 .7-.2 1.3-.3 1.7-.4v-.1c-.5 0-1-.1-1.7-.3-.7-.2-1.3-.5-2-.9-.6-.4-1.2-1.1-1.7-1.9-.5-.8-.7-2-.7-3.4V18.5c0-.4 0-.9-.1-1.4-.1-.5-.2-.9-.4-1.3s-.6-.7-1-1c-.4-.3-1-.4-1.8-.4h-3.2V9.1h5.3c.6 0 1.4.2 2.2.5.9.3 1.7.8 2.5 1.5s1.4 1.5 2 2.5c.5 1 .8 2.2.8 3.6v11.6c0 .9.2 1.7.6 2.3.4.6.9 1.1 1.5 1.5.6.4 1.2.6 1.8.7.6.1 1.2.2 1.6.2v5.2z"/></symbol><symbol id="trumbowyg-upload" viewBox="0 0 72 72"><path d="M64 27v28H8V27H0v36h72V27h-8z"/><path d="M32.1 6.7h8v33.6h-8z"/><path d="M48 35.9L36 49.6 24 36h24z"/></symbol></svg>

      <textarea id="mytextarea" >.....decrypting.....</textarea>

```
      <div>
        <span id="saveButton" class="button blueButton" >Save</span>
        <p></p>
        <p></p>
        <p>**Click "Save" before Close**</p>
      </div>
    </div>
    </form>
  </body>
  <script>
</script>
<?!= HtmlService.createHtmlOutputFromFile('Style').getContent();  ?>
<script src="//code.jquery.com/jquery-1.11.3.min.js"></script>
<script>
  $(document).ready(function(){
    $('#saveButton').click(savePlainText);
    google.script.run.withSuccessHandler(function(valueOfReturn){
       $('#mytextarea').html(valueOfReturn);
    }).getContent();
  });
    function savePlainText() {
     console.log("fn. savePlainText was called");
     google.script.run.withSuccessHandler(function(){
     console.log('console: Saved successfully.');
     alert("ALERT: Saved successfully.");
     var modal = $('.modal-dialog');
     modal.style.display = 'none';
   }).savePlainText( $('#mytextarea').val() );
  }
</script>
</html>
```

ข.3 Style.html

Source Code ส่วนใหญ่ในไฟล์ Style.html จะใช้ภาษาไลบรารี่ของ CSS ทำงานร่วมกับไฟล์ Side.html และ Share.html ที่ไว้ควบคุมความสวยงามข้อหน้าตาอินเตอร์เฟสของ Side Bar บนเอกสารกูเกิ้ล เช่น ขนาดและสีต่างๆของตัวอักษร และปุ่มต่างๆ เป็นต้น

```
<style type="text/css">
  #wrapper {
    color: #334489;

  }
```

```
.sectionHeader {

}

.sectionContent {

}

.sectionFooter {
   margin-top: 8px;
}

.add-underline {
  padding-bottom: 10px;
  border-bottom: 1px solid #999;
}

.add-underline2 {
  padding-bottom: 10px;
  border-bottom: 1px solid #eee;
  margin-bottom: 10px;
}

#new-email-label {
  color: #cccccc;
  text-align: center;
  border: 2px #000;
  border-radius: 5px;
  display: inherit;
}


#mytextarea{
  background: #FDFEFE;
   width: 100%;
   height: 500px;
}

.centerer {
   text-align: center;
}
```

```
#newemail {
  margin-right: 12px;
  padding-left: 10px;
  background: #FDFEFE;
  font-size: 14px;
  line-height: 25px;
  width: 320px;
}

#addNewEmailButton{
float:right;
margin-top: 10px;
margin-right: 5px;
width: 320px;
text-align: center;
}


.button {
 color: #ffffff;
 font-size: 16px;
 moz-border-radius: 3px;
 -webkit-border-radius: 3px;
 padding: 7px;
 border: 0;
}

.blueButton {
 background-color: #456abe;
}
.button:hover {
 opacity: 0.87;
 cursor: pointer;
 cursor: hand;
}

</style>
```


ข.4 Share.html

Source Code ส่วนใหญ่ในไฟล์ Share.html จะใช้ภาษาไลบรารี่ของ HTML ที่ไว้ควบคุมการทำงานของเอกสารกูเกิ้ลในส่วนหน้าบ้าน หรือบนหน้าเว็ปบราวเซอร์ที่แสดงผลเป็น Dialog Box

บนเอกสารกูเกิ้ลที่สนับสนุนการทำงานการใส่ email address ของผู้ใช้งานร่วมในกรณีที่เจ้าของไฟล์เอกสารกูเกิ้ลต้องการแบ่งปันไฟล์ของตนให้กับผู้ใช้งานร่วมได้เปิดอ่านข้อมูลสำคัญหรือข้อมูลลับของตน

```
<div id="wrapper">

 <center><img src="https://cdn0.iconfinder.com/data/icons/follower/154/follower-
man-user-login-round-512.png"
 style="width:120px;height:120px;padding-bottom: 20px;"> </center>

 <div class="sectionContent" >
    <div class="centererxx">
       <input id="newemail" type="text" style="color:#888;"
  value="Enter editor email" onfocus="inputFocus(this)" onblur="inputBlur(this)"/>
       <br>
       <span id="addNewEmailButton" class="button blueButton">Add</span>
    </div>
 </div>

 <div class="sectionFooter" >
    <div>

    </div>
 </div>
</div>

<script>
function inputFocus(i){
   if(i.value==i.defaultValue){ i.value=""; i.style.color="#000"; }
}
function inputBlur(i){
   if(i.value==""){ i.value=i.defaultValue; i.style.color="#888"; }
}
</script>

<?!= HtmlService.createHtmlOutputFromFile('Style').getContent();  ?>

<script src="//code.jquery.com/jquery-1.11.3.min.js"></script>

<script>

 $(document).ready(function(){
```

```
  $('#addNewEmailButton').click(addNewEmail);

});

function addNewEmail() {

  console.log("fn. addNewEmail was called");

  google.script.run.withSuccessHandler(function(addedSuccess){

    if (addedSuccess) {

      console.log('console: Add new Email Successfully');
      alert("Congratulation: Add new collaborative email successfully");
    } else {

      console.log('console: Add new email failure');
      alert("Try again: Add new collaborative email failure!");
    }

  }).addNewEmail( $('#newemail').val() );

}
</script
```

ประวัติผู้เขียนวิทยานิพนธ์

นายโมฮำหมัดชารีฟุดดิน สาและอารง เกิดเมื่อวันที่ 8 มิถุนายน พ.ศ. 2529 ที่จังหวัดยะลา สำเร็จการศึกษาระดับปริญญาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ สำนักวิชาเทคโนโลยีสารสนเทศ จากมหาวิทยาลัยแม่ฟ้าหลวง และได้ศึกษาต่อหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาศาสตร์คอมพิวเตอร์ ภาควิชาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย