การรักษาความมั่นคงในการจัดเก็บข้อมูลแบบกลุ่มเมฆโดยใช้วิธีการแบ่งปันความลับ

Cloud Storage Security using Shamir's Secret Sharing

ธนพล แก้วเบญจโชติ[1] (Thanaphon Kaewbenjachot)[1], สมชาย ปราการเจริญ (Sornchai Prakancharoen)[2]

[1,2]ภาควิชาวิทยาการคอมพิวเตอร์และสารสนเทศ คณะวิทยาศาสตร์ประยุกต์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
1518 ถ.พิบูลสงคราม เขตบางซื่อ กรุงเทพฯ 10800 โทรศัพท์ : 0-2913-2500 ต่อ 4617
E-mail: onlinethai@gmail.com[1], spk@kmutnb.ac.th[2]

บทคัดย่อ

งานวิจัยนี้นำเสนอการรักษาความมั่นคงในการจัดเก็บข้อมูลแบบกลุ่มเมฆด้วยวิธีการแบ่งปันความลับ โดยมีวัตถุประสงค์เพื่อรักษาความมั่นคงในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน เพื่อใช้เก็บข้อมูลที่สำคัญ และต้องการปกปิด โดยใช้วิธีการเข้ารหัสแบบกุญแจสมมาตร ด้วยมาตรฐานการเข้ารหัสลับขั้นสูง และวิธีการแบ่งปันความลับ [1] เพื่อแบ่งข้อมูลความลับออกเป็นหลายส่วนและกระจายการจัดเก็บ

คำสำคัญ: การจัดเก็บข้อมูลแบบกลุ่มเมฆ การเข้ารหัสข้อมูลแบบกุญแจสมมาตร ความมั่นคง การกระจายการจัดเก็บข้อมูล การเข้ารหัสข้อมูล การถอดรหัสข้อมูล

Abstract

This paper presents security of cloud storage system protocol which could guarantees confidentiality, integrity and availability for store sensitive and important information. The designed protocol use Symmetric-key cryptography schemes, Advanced Encryption Standard (AES) and Shamir's Secret Sharing to share confidential information into several parts of distributed to storages.

Keywords: Cloud Storage, Symmetric-key Cryptography, Security, Data Distribute, Encryption, Decryption

1. คำนำ

การจัดเก็บข้อมูลในปัจจุบันมีการพัฒนาเป็นอย่างมากโดยเฉพาะการจัดเก็บข้อมูลแบบกลุ่มเมฆ (Cloud Storage) ซึ่งมีพื้นที่จัดเก็บข้อมูลแบบกระจายและมีการควบคุมดูแลโดยผู้ดูแลฐานข้อมูลหลายคน ทำให้การจัดเก็บข้อมูลในลักษณะนี้มีความมั่นคงและความเป็นส่วนตัวน้อยเกินกว่าจะเก็บข้อมูลที่มีความสำคัญและต้องการความมั่นคงสูง

งานวิจัยนี้จึงได้นำเสนอวิธีการจัดเก็บข้อมูลให้มีความมั่นคงและมีความเป็นส่วนตัวสูง โดยใช้วิธีการเข้ารหัสข้อมูลแบบกุญแจสมมาตร (Symmetric-key cryptography) [2, 3] และวิธีการแบ่งปันความลับ (Shamir's Secret Sharing) [1] ในการแยกส่วนข้อมูลออกเป็นหลายส่วนเพื่อกระจายการจัดเก็บและสามารถสร้างข้อมูลกลับมาใหม่ได้ หากมีจำนวนข้อมูลความลับที่มีจำนวนมากพอตามที่กำหนดไว้

วิธีนี้จึงสามารถนำไปประยุกต์ใช้กับข้อมูลสำคัญที่ต้องการปกปิด เช่น เอกสารทางราชการ หรือ ข้อมูลสำคัญทางการเงิน เป็นต้น

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 Cloud Storage [4 ,8]

เทคโนโลยีแบบกลุ่มเมฆ (Cloud Technology) มีคำจำกัดความว่าเป็นการให้บริการผ่านระบบอินเตอร์เน็ตที่สามารถรองรับการใช้งานได้ตามต้องการ และยังคงมี

เสถียรภาพแม้ว่ามีผู้ใช้งานจำนวนมาก ซึ่งปัจจุบันได้รับความนิยมอย่างแพร่หลาย เนื่องจากเป็นการบริหารทรัพยากรอย่างคุ้มค่า ประกอบกับปัจจุบันอินเตอร์เน็ตมีความเร็วสูงทำให้เทคโนโลยีแบบกลุ่มเมฆได้รับความนิยมสูง ประเภทของการให้บริการมี 3 ประเภทได้แก่

1. Software as a Service (SaaS)
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

การให้บริการ Cloud Service มีหลายรูปแบบ อาทิ เช่น การให้บริการอีเมล์ (Electronic Mail) การให้บริการเครือข่ายสังคม (Social Network) การให้บริการพื้นที่จัดเก็บข้อมูล (Storage)

2.2 Secret Sharing Schemes [1]

Secret sharing schemes ถูกคิดค้นโดย Blakley และ Adi Shamir แนวคิดของ Secret Sharing คือการแบ่งข้อมูลออกเป็นส่วนๆ และจัดสรรให้กับบุคคลต่างๆ ซึ่งบุคคลที่ได้รับข้อมูลแต่ละส่วนไปนั้นจะสามารถกู้คืนข้อมูลได้โดยไม่จำเป็นต้องมีครบทุกส่วน แต่จะต้องข้อมูลความลับที่มีจำนวนมากพอตามที่กำหนดไว้

2.3 HMAC [6]

Hash-based Message Authentication Code เป็นการเข้ารหัสโดยใช้ฟังก์ชัน MD5 หรือ SHA-1 ซึ่งมีการใช้งานรหัสลับ (Secret Key) เข้ามาร่วมกับฟังก์ชัน Hash เพื่อให้ปลายทางสามารถตรวจสอบได้ตามหลักการลายเซ็นดิจิตอล [8] ว่าต้นทางเป็นผู้ส่งข้อมูลนั้นมาจริง

การเข้ารหัสลับมาตรฐานขั้นสูง (Advanced Encryption Standard) ได้รับการรับรองโดยรัฐบาลสหรัฐในปี 1997 โดยสถาบัน National Institute of Standards and Technology (NIST) อัลกอริทึมนี้เป็นแบบ Block Cipher โดยใช้บล็อกข้อมูลขนาด 128 บิต 196 บิต และ 256 บิต โดยสามารถใช้คีย์ได้ยาวถึง 128 บิต 196 บิต และ 256 บิต อัลกอริทึมนี้ได้รับการออกแบบให้มีการทำงานที่เหมาะสมกับโพรเซสเซอร์รุ่นใหม่และใช้งานกับ Smart Card ได้

2.4 Symmetric-key cryptography [2, 3]

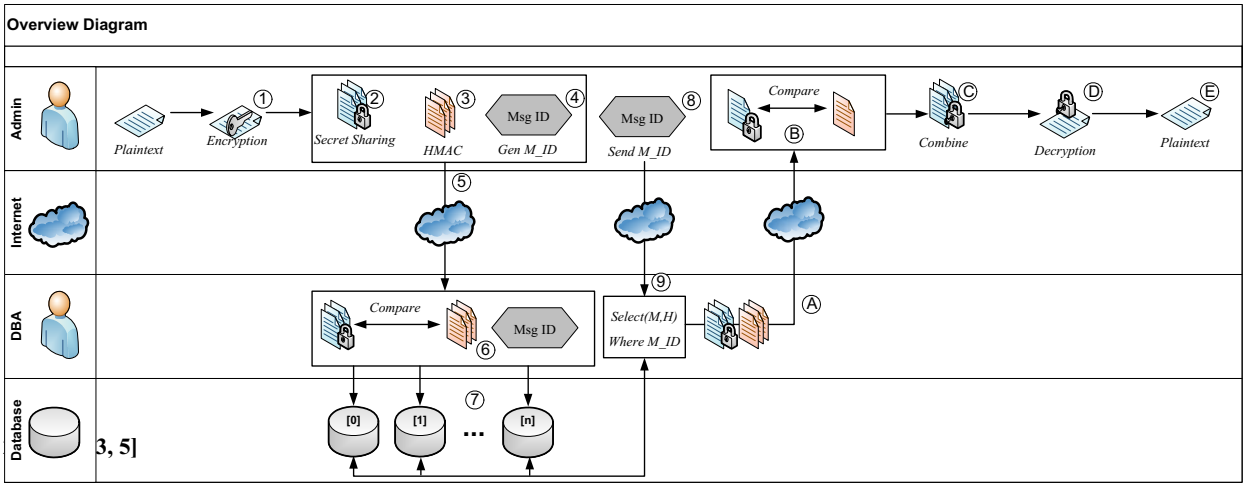
การเข้ารหัสแบบกุญแจสมมาตรเป็นการเข้ารหัสข้อมูลโดยการใช้ Secret Key หรือรหัสลับในการเข้ารหัสและถอดรหัสข้อมูลโดยทั้งผู้ส่งและผู้รับจะต้องใช้รหัสลับเดียวกัน

ข้อดี คือ สามารถเข้ารหัสและถอดรหัสได้อย่างรวดเร็ว แต่ไม่เหมาะกับการใช้งานในกลุ่มคนขนาดใหญ่ซึ่งจะยากต่อการบริหารจัดการรหัสลับ

3. ขั้นตอนวิธีการดำเนินการวิจัย

งานวิจัยนี้ได้ออกแบบวิธีการรักษาความมั่นคงในการจัดเก็บข้อมูลแบบกลุ่มเมฆโดยใช้วิธีการแบ่งปันความลับโดยออกแบบ 2 ส่วน คือ

1. ส่วนเข้ารหัสแล้วแบ่งปันความลับเพื่อส่งข้อมูลไปเก็บแบบกระจาย
2. ส่วนค้นหาและเลือกข้อมูลเพื่อนำมาควบรวมความลับแล้วถอดรหัส



3, 5]

ภาพที่ 1: ภาพรวมการทำงานของระบบ

จากภาพที่ 1 ภาพรวมการทำงานของระบบ สามารถอธิบายขั้นตอนการดำเนินการได้ดังนี้

(1) ผู้ดูแลระบบเข้ารหัสข้อมูล โดยใช้การเข้ารหัสแบบกุญแจสมมาตร *Encrypt* จะได้ *Ciphertext*

(2) จากนั้นนำ *Ciphertext* มาแยกส่วนโดยใช้การแบ่งปันความลับ *SecretSharing*

(3) เมื่อได้ข้อมูลความลับก็นำแต่ละส่วนมาเข้าฟังก์ชันแฮชด้วยกุญแจความลับโดยใช้ *HMAC*

(4) จากนั้นสร้าง *MessageID*

(5) ข้อมูลจะถูกแบ่งเป็นชุดข้อมูลโดยจะมี *MessageID* ข้อมูลความลับและข้อมูลที่แฮชแล้ว ข้อมูลทั้ง 3 นี้จะถูกส่งแบบกระจายไปยังผู้ดูแลข้อมูลแต่ละคน

(6) เมื่อผู้ดูแลข้อมูลได้รับข้อมูลก็จะทำการนำข้อมูลความลับมาเข้าฟังก์ชันแฮชด้วยกุญแจความลับซึ่งเป็นกุญแจเดียวกันกับผู้ดูแลระบบ แล้วทำการเปรียบเทียบเพื่อตรวจสอบความถูกต้องของข้อมูลว่าไม่ถูกเปลี่ยนระหว่างการส่งด้วยฟังก์ชัน *Compare*

(7) หากตรวจสอบข้อมูลถูกต้องแล้วจึงทำการจัดเก็บข้อมูล

(8) เมื่อผู้ดูแลระบบต้องการข้อมูลจะทำการร้องขอไปยังผู้ดูแลข้อมูลโดยส่ง *MessageID* ไปร้องขอยังผู้ดูแลฐานข้อมูลทุกคน

(9) ผู้ดูแลข้อมูลทุกคนนำ *MessageID* ไปค้นหาข้อมูล

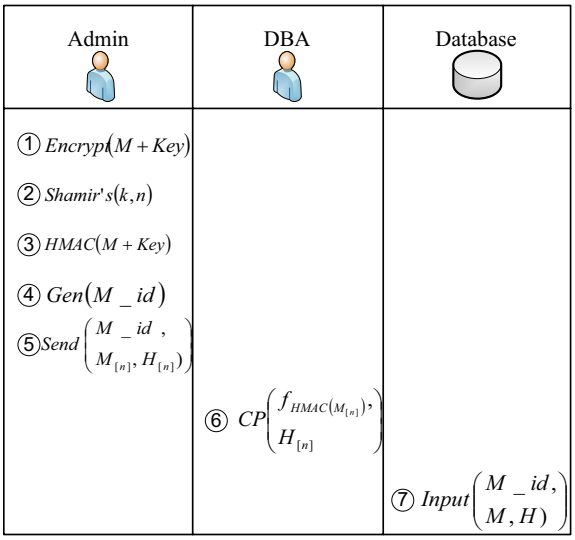
(A) ผู้ดูแลข้อมูลส่งข้อมูลความลับและข้อมูลแฮชที่ได้จากฐานข้อมูลกลับไปยังผู้ดูแลระบบ

(B) เมื่อผู้ดูแลระบบได้รับข้อมูลก็จะทำการนำข้อมูลความลับมาเข้าฟังก์ชันแฮชด้วยกุญแจความลับซึ่งเป็นกุญแจความลับเดิมโดยใช้ *HMAC* เพื่อตรวจสอบความถูกต้องของข้อมูลว่าไม่ถูกเปลี่ยนระหว่างการส่ง *Compare*

(C) เมื่อตรวจสอบเสร็จทำการควบรวมข้อมูลความลับ *Combine* ซึ่งจะได้ *Ciphertext*

(D) จากนั้นนำ *Ciphertext* มาถอดรหัส *Decrypt* แบบกุญแจสมมาตร $Symmetric-key$ ซึ่งจะใช้รหัสลับเดียวกันกับตอนเข้ารหัสในครั้งแรก

(E) เมื่อถอดรหัสด้วยรหัสลับแล้วจะได้ข้อความต้นฉบับ *Plaintext* กลับคืนมา



ภาพที่ 2: การเข้ารหัส แบ่งปันความลับและเก็บข้อมูล

3.1 การเข้ารหัส แบ่งปันความลับและเก็บข้อมูล สามารถอธิบายได้จาก**ภาพที่ 2** ดังนี้

(1) $Encrypt(M+Key)$ คือ ฟังก์ชันการเข้ารหัสข้อมูลซึ่งใช้ Symmetric-key แบบ AES

(2) $Shamir's(k,n)$ คือ ฟังก์ชันการแบ่งปันความลับซึ่งต้องกำหนดค่าจำนวนความลับทั้งหมด n และค่าจำนวนความลับที่จะใช้ในการกู้คืนได้ k

(3) $HMAC(M+Key)$ คือ ฟังก์ชันการแฮชแบบใช้กุญแจความลับเพื่อยืนยันตัวตนของผู้ส่งและตรวจสอบความถูกต้องของข้อมูลว่าไม่ถูกเปลี่ยนระหว่างการส่ง

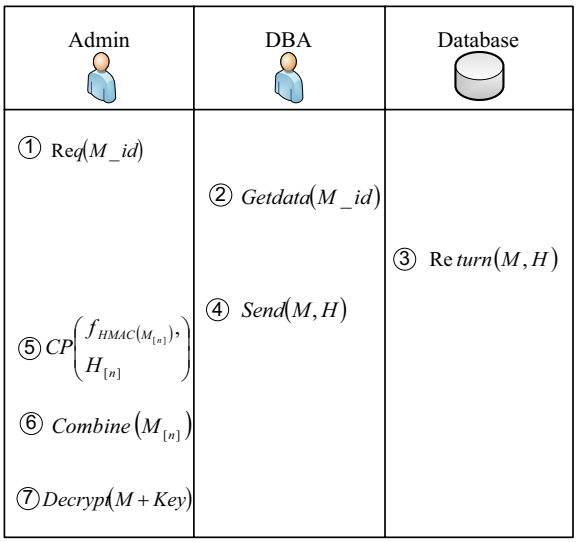
(4) $Gen(M\_id)$ คือ ฟังก์ชันการสร้าง *MessageID* ซึ่งใช้เวลาปัจจุบันในการสร้าง โดยใช้ฟังก์ชัน $DateNow(yyyyMMddHH\ mmssffff)$

(5) $Send\begin{pmatrix}M\_id,\\M_{[n]},H_{[n]}\end{pmatrix}$ คือ ฟังก์ชันการส่งข้อมูลไปยังผู้ดูแลข้อมูลทั้งหมด

(6) ผู้ดูแลข้อมูลตรวจสอบความถูกต้องของข้อมูลว่าไม่ถูกเปลี่ยนระหว่างการส่งและยืนยันตัวตนของผู้ส่งว่าข้อความถูกส่งมาโดยผู้ดูแลระบบจริง โดยใช้ฟังก์ชัน

$$Compare\begin{pmatrix}f_{HMAC(M_{[n]})},\\H_{[n]}\end{pmatrix}\Rightarrow ?\ True\ :\ False$$

(7) $Input\begin{pmatrix} M\_id, \\ M, H \end{pmatrix}$ คือ ฟังก์ชันการจัดเก็บข้อมูลลงฐานข้อมูล



ภาพที่ 3: การเลือกข้อมูล ควบรวมข้อมูลและถอดรหัส

3.2 การเลือกข้อมูล ควบรวมและถอดรหัสข้อมูล สามารถอธิบายได้จาก**ภาพที่ 3** ดังนี้

(1) $\mathrm{Re}\,q(M\_id)$ คือ ฟังก์ชันการร้องขอข้อมูลโดยส่ง $MessageID$ ไปยังผู้ดูแลฐานข้อมูลทุกคน

(2) ผู้ดูแลฐานข้อมูลทำการเลือกข้อมูลในฐานข้อมูลโดยใช้ $MessageID$ เป็นเงื่อนไขในการเลือก $Getdata(M\_id)$

(3) เมื่อพบข้อมูลตามเงื่อนไขที่ต้องการฐานข้อมูลจะ $\mathrm{Re}\,turn(M,H)$ ข้อมูลไปให้ผู้ดูแลฐานข้อมูล

(4) $Send(M,H)$ คือ ฟังก์ชันที่ผู้ดูแลฐานข้อมูลส่งข้อมูลไปยังผู้ดูแลระบบ

(5) ผู้ดูแลระบบตรวจสอบความถูกต้องของข้อมูลว่าไม่ถูกเปลี่ยนระหว่างการส่งและยืนยันตัวตนผู้ส่งว่าข้อความส่งโดยผู้ดูแลฐานข้อมูลจริง โดยใช้ฟังก์ชัน

$$Compare\begin{pmatrix} f_{HMAC}(M_{[n]}), \\ H_{[n]} \end{pmatrix} \Rightarrow ?\,True\ :\ False$$

(6) $Combine(M_{[n]})$ คือ ฟังก์ชันการควบรวมข้อมูล เมื่อควบรวมข้อมูลแล้วจะได้ $Ciphertext$ กลับคืนมา

(7) $Decrypt(M + Key)$ คือ ฟังก์ชันการถอดรหัส โดยใช้การเข้ารหัสแบบกุญแจสมมาตรซึ่งจะใช้รหัสลับเดียวกันกับตอนเข้ารหัส

4. ผลการดำเนินการวิจัย

ในงานวิจัยนี้ได้เสนอการรักษาความมั่นคงในการจัดเก็บข้อมูลแบบกลุ่มเมฆโดยใช้วิธีการแบ่งปันความลับ ผู้วิจัยได้พัฒนาโปรแกรมการเข้ารหัสแบบกุญแจสมมาตร ด้วยมาตรฐานการเข้ารหัสลับขั้นสูงโดยใช้รหัสลับที่กำหนดไว้แล้วใช้ฟังก์ชันแบ่งปันความลับด้วย Shamir's Secret Sharing ซึ่งผู้วิจัยได้กำหนดให้แบ่งข้อมูลความลับเป็น 3 ส่วนและจัดเก็บข้อมูลแบบกระจายไปยังฐานข้อมูลจำนวน 3 ชุด ซึ่งสามารถทำงานได้อย่างมีประสิทธิภาพ โดยข้อมูลความลับแต่ละส่วนได้ถูกจัดเก็บอย่างถูกต้องครบถ้วน

ในขั้นตอนการนำข้อมูลความลับแต่ละส่วนมาควบรวมแล้วถอดรหัส ผู้วิจัยได้พัฒนาโปรแกรมให้รับค่า Message ID เพื่อนำไปค้นหาและเลือกข้อมูลตามเงื่อนไข ข้อมูลความลับที่ได้มานั้นไม่จำเป็นต้องครบทั้งหมดก็สามารถควบรวมได้ ในที่นี้ผู้วิจัยได้กำหนดให้ใช้ข้อมูล 2 ใน 3 ส่วนก็สามารถทำการควบรวมข้อมูลความลับกลับคืนเป็น Ciphertext และทำการถอดรหัสด้วยมาตรฐานการเข้ารหัสลับขั้นสูงโดยใช้รหัสลับที่กำหนดไว้ซึ่งเป็นรหัสลับเดียวกันกับการเข้ารหัสในขั้นตอนแรก เมื่อถอดรหัสแล้วจะได้ข้อมูล Plaintext ต้นฉบับกลับคืนมาซึ่งผลการทำงานถูกต้องครบถ้วน

5. บทสรุป

การรักษาความมั่นคงในการจัดเก็บข้อมูลแบบกลุ่มเมฆโดยใช้วิธีการแบ่งปันความลับ วิธีการนี้มีความมั่นคงในด้านของการรักษาความลับ (Confidentaility) และความพร้อมใช้งาน (Availiability) ซึ่งหลักการทำงานไม่ซับซ้อน ผู้วิจัยจึงได้เพิ่มขั้นตอนของการเข้ารหัสโดยใช้การเข้ารหัสแบบกุญแจสมมาตร ด้วยมาตรฐานการเข้ารหัสลับขั้นสูงโดยใช้รหัสลับเดียวกัน และเพิ่มขั้นตอนของการตรวจสอบความถูกต้องของข้อมูลโดยใช้วิธีแฮชฟังก์ชันแบบ Hash-based Message Authentication Code (HMAC) ซึ่งจะใช้ในการตรวจสอบความ

ถูกต้องของข้อมูลเพื่อให้มั่นใจได้ว่าข้อมูลที่รับมาไม่ถูกเปลี่ยนระหว่างการส่งผ่านเครือข่าย เพื่อเพิ่มความมั่นคงในด้านความสมบูรณ์ (Integrity) ทำให้งานวิจัยนี้สามารถรักษาความมั่นคงได้ครบทั้ง 3 ด้าน

เอกสารอ้างอิง

[1] Adi Shamir, "How to share a secret," CACM Communications of the ACM Volume 22(11): 612-613, 1979

[2] วิทยาการเข้ารหัสลับ [ออนไลน์] ม.ป.ป. [อ้างเมื่อ 7 เมษายน 2555] จาก http://th.wikipedia.org/wiki/วิทยาการเข้ารหัสลับ.

[3] Hans Delfs and Helmut Knebl, "Symmetric-Key Encryption, Introduction to Cryptography: Principles and Applications, Second Edition," ISBN-13 978-3-540-49243-6, 11-25.

[4] Miller H.G. และ Veiga J. 2009. Cloud Computing: Will Commodity Services Benefit Users Long Term?. IT Professional (11): 57-59.

[5] Christof Paar, Jan Pelzl, "The Advanced Encryption Standard", Chapter 4 of "Understanding Cryptography, A Textbook for Students and Practitioners". (Companion web site contains online lectures on AES), Springer, 2009.

[6] Hash-based message authentication code [ออนไลน์] ม.ป.ป. [อ้างเมื่อ 27 เมษายน 2555] จาก http://en.wikipedia.org/wiki/Hash-based_message_authentication_code.

[7] S. Prakancharoen, "Sys-Log Database Manipulation Security Protocol," ICACTE'3, V2-367, 2010.

[8] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21(2): 120–126, 1978.

[9] กนธร จินดารักษ์, "ระบบเก็บข้อมูลแบบกลุ่มเมฆ," บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์, 2552.