Pseudonymization for the protection of personal data necessary to conduct corporate transactions using encryption and tokenization Methods

***Nontawatt Saraman*[1], *Surasak Mungsing*[2]**
[1] Cyber Innovation Promotion Association of Technology
[2] Faculty of Information Technology, Sripatum University

Abstract

Personal data is any information that can be directly or indirectly linked to an individual. It is the information that is necessary to carry out the transaction. The best way to protect personal information is to make that information become anonymous without the identity of the person anymore and cannot be reversed regardless of any additional information. This article objective is to present presents methods for creating pseudonymisation for protecting personal information by means of encryption and tokenization.

Keywords: Personal data, Anonymization, Encryption, Tokenization, Pseudonymisation

Revised: 10 May 2022, Revise: 25 July 2022, Accepted: 30 September 2022

Correspondence: Surasak Mungkasing, Department of Computing, Faculty of Information Technology, Sripatum University, 2410/2 Phahonyothin Road, Chatuchat District, Bangkok 10900, E-mail: surasak.mu@spu.ac.th

การทำข้อมูลแฝงเพื่อการปกป้องข้อมูลส่วนบุคคลที่จำเป็นต่อการดำเนินธุรกรรมขององค์กรด้วยเทคนิคการเข้ารหัสและการสร้างโทเค็น

นนทวัตต์ สาระมาน[1], สุรศักดิ์ มังสิงห์[2]

[1] สมาคมส่งเสริมนวัตกรรมเทคโนโลยีไซเบอร์

[2] คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

บทคัดย่อ

ข้อมูลส่วนบุคคลคือข้อมูลใดๆที่สามารถเชื่องโยงไปถึงตัวบุคคลไม่ว่าทางตรงหรือทางอ้อม เป็นข้อมูลที่จำเป็นต่อการดำเนินการธุรกรรม วิธีที่ดีที่สุดในการปกป้องข้อมูลส่วนบุคคล คือการทำให้ข้อมูลนั้นกลายเป็นข้อมูลนิรนาม (Anonymization) โดยไม่สามารถระบุตัวตนของบุคคลได้อีกต่อไปอย่างถาวร (Anonymized data) และไม่สามรถที่จะย้อนกลับไปได้ไม่ว่าจะมีข้อมูลใดๆมาเพิ่มเติม บทความนี้มีวัตถุประสงค์เพื่อนำเสนอวิธีการในการสร้างข้อมูลแฝง (Pseudonymisation) สำหรับการปกป้องข้อมูลส่วนบุคล โดยวิธีการเข้ารหัส (Encryption) และการทำให้เป็นโทคเคน (Tokenization)

คำสำคัญ: ข้อมูลส่วนบุคคล, ไม่ระบุชื่อ, การเข้ารหัส, การสร้างโทเค็น, ข้อมูลแฝง

วันที่รับต้นฉบับ: 10 พฤษภาคม 2565, วันที่แก้ไข: 25 กรกฎาคม 2565, วันที่ตอบรับ: 30 กันยายน 2565

บทนำ

ข้อมูลส่วนบุคคล (Personally identifiable information) คือข้อมูลใดๆที่สามารถเชื่องโยงไปถึงตัวบุคคลไม่ว่าทางตรงหรือทางอ้อม [8] องค์กรต่างๆ ไม่ว่าใหญ่หรือเล็ก มีความจำเป็นต้องจัดเก็บข้อมูลส่วนบุคคลเพื่อดำเนินการทางธุรกิจอย่างหลีกเลี่ยงไม่ได้ การปกป้องข้อมูลส่วนบุคคลจึงเข้ามามีส่วนสำคัญในการออกแบบระบบการจัดเก็บข้อมูลภายในองค์กร วิธีที่ดีที่สุดในการปกป้องข้อมูลส่วนบุคคล คือการทำให้ข้อมูลนั้นกลายเป็นข้อมูลนิรนาม (Anonymization) หรือก็คือการทำให้ข้อมูลไม่สามารถระบุตัวตนของบุคคลได้อีกต่อไปอย่างถาวร (Anonymized data) และไม่สามรถที่จะย้อนกลับไปได้ไม่ว่าจะมีข้อมูลใดๆ มาเพิ่มเติม แต่การทำข้อมูลเป็นข้อมูลนิรนามก็ไม่สามารถทำได้เสมอไป เนื่องจากการดำเนินการทางธุรกิจอาจจำเป็นต้อใช้ข้อมูลส่วนนั้น ยกตัวอย่างเช่น ฐานข้อมูลผู้ป่วยภายในโรงพยาบาล ในกรณีนี้ โรงพยาบาลมีความจำเป็นต้องเก็บข้อมูลตัวตนของผู้ป่วย และต้องสามารถเชื่อมโยงข้อมูลนั้นกับอาการที่อยู่และอื่นๆ ได้ หากนำข้อมูลส่วนนี้ไปทำให้เป็นข้อมูลนิรนามโรงพยาบาลก็ไม่สามารถดำเนินการได้อีกต่อไป เพราะฉะนั้นจึงจำเป็นต้องใช้วิธีอื่นแทน ที่ยังคงความสามารถในการทำงานของธุรกิจนั้นๆ อยู่

ผู้นิพนธ์ประสานงาน: สุรศักดิ์ มังสิงห์, คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม 2410/2 ถนนพหลโยธิน เขตจตุจัตร กรุงเทพฯ 10900 E-mail: surasak.mu@spu.ac.th

ข้อมูลแฝง

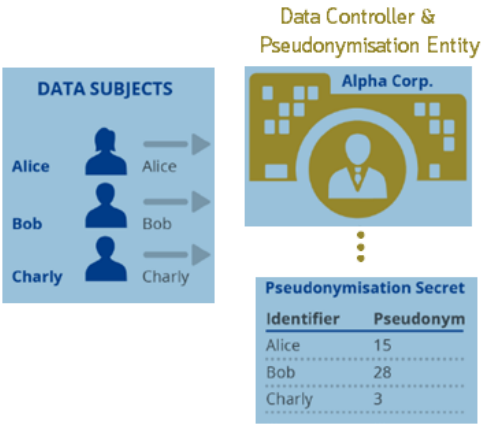
การใช้ข้อมูลแฝงเป็นกระบวนการไม่ระบุตัวตน (de-identification process) ซึ่งได้รับความสนใจหลังจากที่มีกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation – GDPR) ออกมาเพื่อคุ้มครองประชาชนในกลุ่มประเทศสหภาพยุโรป และที่ประเทศไทยจะประกาศใช้ คือพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act – PDPA) [8] จากการที่ความเป็นส่วนตัวและข้อมูลส่วนบุคคลถูกล่วงละเมิดมากขึ้นในโลกยุคใหม่ที่ขับเคลื่อนด้วยข้อมูลมาใช้ โดยอ้างอิงเป็นทั้งการรักษาความปลอดภัยและการปกป้องข้อมูลโดยกลไกการออกแบบ นอกจากนี้ ในบริบทของ GDPR และ PDPA การใช้ข้อมูลแฝงสามารถกระตุ้นการผ่อนคลายภาระผูกพันทางกฎหมายของผู้ควบคุมข้อมูลได้ในระดับหนึ่ง หากนำไปใช้อย่างเหมาะสม [1]

ข้อมูลแฝง (Pseudonymized data) คือข้อมูลที่ไม่สามารถระบุตัวตนของบุคคลได้ แต่สามารถที่จะย้อนกลับมาเพื่อเป็นข้อมูลที่ระบุตัวตนได้อีกครั้งเมื่อมีข้อมูลเพิ่มเติม การทำข้อมูลแฝง (Pseudonymization) ที่ถูกวิธีกับเป้าหมายที่ถูกต้องเท่านั้นจึงจะให้ผลลัพท์ออกมาเป็นข้อมูลแฝง วิธีการทำข้อมูลแฝงมีหลายวิธี แต่สิ่งทุกวิธีการมีเหมือนกันคือการปิดบังข้อมูลส่วนที่ใช้ระบุตัวตนบุคคล ด้วยวิธีการบางอย่าง โดยจะสามารถย้อนกลับมาเป็นข้อมูลเดิมได้ก็ต่อเมื่อมีข้อมูลอีกส่วนเท่านั้น ข้อมูลทั้งสองส่วนต้องแยกจากกันอย่างชัดเจน เนื่องจากข้อมูลจะยังคงเป็นข้อมูลแฝงก็ต่อเมื่อข้อมูลทั้งสองแยกจากกันเท่านั้น หากข้อมูลทั้งสองส่วนหลุดออกไปพร้อมกันก็ยังคงถือว่าเป็นข้อมูลส่วนบุคคล

สถานการณ์การใช้ข้อมูลแฝง

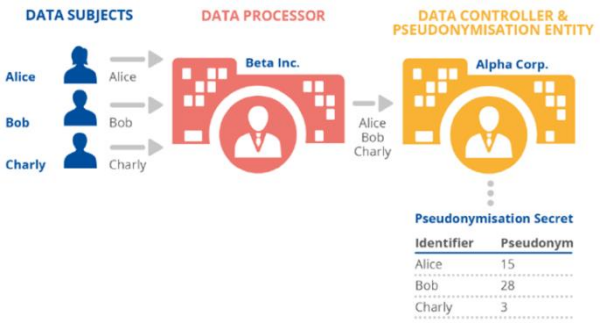
สถานการณ์การใช้ข้อมูลแฝงในทางปฏิบัติ แบ่งได้เป็น 6 กรณี ดังนี้

1. **กรณีข้อมูลแฝงสำหรับการใช้งานภายในองค์กร** (รูปที่ 1) ผู้ควบคุมข้อมูล (Data Controller) ขององค์กรมีบทบาทในการระบุข้อมูลแฝง การเลือกและกำหนดข้อมูลแฝงให้กับตัวระบุ จะต้องชี้ให้เห็นว่าเจ้าของข้อมูลไม่จำเป็นต้องรู้หรือเรียนรู้ข้อมูลแฝงเฉพาะของตน และเป็นที่รู้จักเฉพาะในองค์กรเท่านั้น ทั้งนี้เพิ่มความปลอดภัยของข้อมูลส่วนบุคคลสำหรับการใช้งานภายใน [2]



รูปที่ 1 ข้อมูลแฝงสำหรับการใช้งานภายในองค์กร [2]

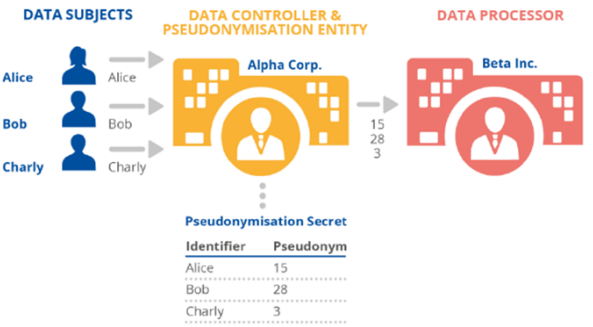
2. **กรณีที่มีผู้ประมวลผลขององค์กรอื่นมาเกี่ยวข้อง** (รูปที่ 2) ในกรณีผู้ประมวลผลข้อมูลเฉพาะ ที่ ได้รับมอบหมายให้รวบรวมตัวระบุจากเจ้าของข้อมูลและส่งต่อข้อมูลนี้ไปยังผู้ควบคุมข้อมูลขององกรณ์ ซึ่งดำเนินการโดยใช้ข้อมูลแฝงในที่สุด สถานการณ์ดังกล่าวอาจเป็นผู้ให้บริการระบบคลาวด์ที่โฮสต์บริการรวบรวมข้อมูลในนามของผู้ควบคุมข้อมูล ซึ่งผู้ควบคุมยังคงรับผิดชอบการใช้ข้อมูลแฝงของข้อมูลก่อนดำเนินการใดๆ ต่อไป เป้าหมายสำหรับการใช้ข้อมูลแฝงเหมือนกับในสถานการณ์ที่ 1 (แต่คราวนี้ผู้ประมวลผล มีส่วนร่วมในกระบวนการด้วย)



รูปที่ 2 กรณีที่มีผู้ประมวลผลของนิติบุคคลอื่นมาเกี่ยวข้อง [2]

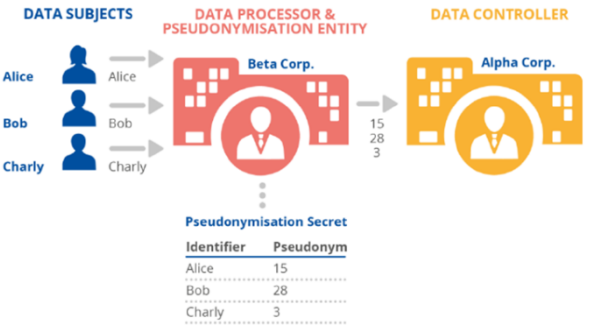
3. **กรณีส่งข้อมูลโดยใช้ข้อมูลแฝงไปยังผู้ประมวลผลของนิติบุคลอื่น** (รูปที่ 3)

ผู้ควบคุมข้อมูลขององค์กรที่รวบรวมข้อมูลและดำเนินงานของข้อมูลข้อมูลแฝง ส่งต่อข้อมูลข้อมูลแฝงไปยังผู้ประมวลผลข้อมูลขององค์กรอื่น เช่น สำหรับการวิเคราะห์ทางสถิติ หรือการจัดเก็บข้อมูลแบบต่อเนื่อง ในสถานการณ์สมมตินี้เป้าหมายการป้องกันโดยการใช้ข้อมูลแฝงของข้อมูลสามารถเปิดเผยได้ เพราะองค์กรที่ได้รับข้อมูลแฝงไปใช้ในการประมวลผล ไม่ได้เรียนรู้ตัวระบุของเจ้าของข้อมูล จึงไม่สามารถระบุบุคคลที่อยู่เบื้องหลังข้อมูลได้โดยตรง



รูปที่ 3 กรณีส่งข้อมูลโดยใช้ข้อมูลแฝงไปยังผู้ประมวลผลของนิติบุคลอื่น [2]

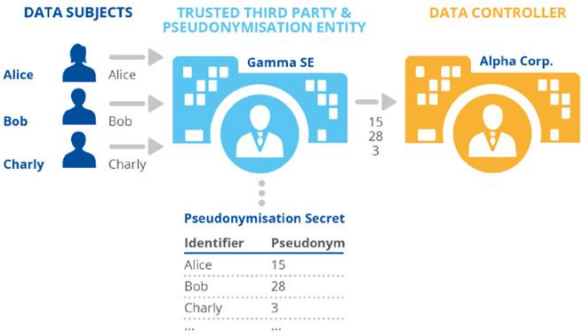
4. **กรณีผู้ประมวลผลในฐานะนิติบุคคลข้อมูลแฝง** (รูปที่ 4) แม้ผู้ประมวลผลต้องรับผิดชอบในการประมวลผลตัวระบุเป็นข้อมูลแฝงโดยใช้ฟังก์ชันข้อมูลแฝง แต่ความรับผิดชอบสำหรับกระบวนการสร้างข้อมูลแฝงทั้งหมด (และสำหรับการดำเนินการประมวลผลข้อมูลทั้งหมดโดยทั่วไป) ก็ยังเป็นของผู้ควบคุมข้อมูล



รูปที่ 4 กรณีผู้ประมวลผลในฐานะนิติบุคคลข้อมูลแฝง [2]

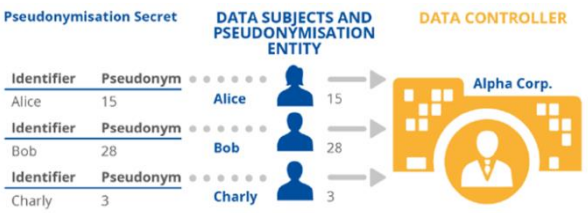
5. **กรณีบุคคลที่สามในฐานะนิติบุคคลข้อมูลแฝง** (รูปที่ 5) ในสถานการณ์นี้อาจมีความเกี่ยวข้องอย่างมากกับกรณีของการควบคุมร่วมกัน โดยที่หนึ่งในผู้ควบคุมกำลังดำเนินการโดยใช้ข้อมูลแฝง (ทำหน้าที่เป็นบุคคลที่สามที่เชื่อถือได้ - TTP ในรูปที่ 5) และอีกรายหนึ่งได้รับเฉพาะข้อมูลข้อมูลแฝงสำหรับการประมวลผลต่อไป สถานการณ์นี้อาจมีความเกี่ยวข้องอย่างมากกับกรณีของการ

ควบคุมร่วมกัน โดยที่หนึ่งในผู้ควบคุมกำลังดำเนินการโดยใช้ข้อมูลแฝง และอีกรายหนึ่งได้รับเฉพาะข้อมูลข้อมูลแฝงสำหรับการประมวลผลต่อไป



รูปที่ 5 กรณีบุคคลที่สามในฐานะนิติบุคคลข้อมูลแฝง [2]

6. กรณีเจ้าของข้อมูลในฐานะนิติบุคคลข้อมูลแฝง (รูปที่ 6) เป็นกรณีพิเศษของการใช้นามแฝงที่เจ้าของข้อมูลสร้างนามแฝงขึ้นมาเอง ซึ่งเป็นส่วนหนึ่งของกระบวนการสร้างข้อมูลแฝงโดยรวม เจ้าของข้อมูลแต่ละคนสร้างนามแฝงของตนเอง จากนั้นจึงส่งต่อข้อมูลแฝงนี้เป็นต้นไป ซึ่งนามแฝงอาจอยู่ในรูปแบบของกุญแจส่วนตัวและกุญแจสาธารณะโดยที่เจ้าของข้อมูลเก็บรักษากุญแจส่วนตัวไว้สำหรับถอดรหัสข้อมูลที่ต้องการอนุญาตเท่านั้น เช่น ระบบ Trusty[3]



รูปที่ 6 กรณีเจ้าของข้อมูลในฐานะนิติบุคคลข้อมูลแฝง [2]

การสร้างข้อมูลแฝง

การสร้างข้อมูลแฝงทำได้หลายวิธี เช่น การเข้ารัส (Encryption[1] และการทำให้เป็นโทเค็น(Tokenization) [2] การใช้อัลกอริทึม Rule-base [4] การใช้เทคนิคผสมผสาน [5] เป็นต้น

การเข้ารหัสข้อมูล (Encryption) คือ รูปแบบการจัดการข้อมูลอย่างหนึ่ง โดยการเข้ารหัสให้เป็น Cipher text ซึ่งคนทั่วไปอ่านไม่เข้าใจ ผู้ที่ได้รับอนุญาตหรือมีกุญแจเท่านั้นที่จะสามารถถอดรหัสกลับคืนมาเป็นข้อมูลธรรมดาที่สามารถอ่านเข้าใจได้อีกครั้งหนึ่ง

การสร้างข้อมูลแฝงโดยการเข้ารหัสข้อมูล (Encryption) เพื่อปกป้องข้อมูลส่วนบุคคล คือการแปลงข้อมูลส่วนบุคคลที่เป็น Plain text ให้กลายเป็นข้อมูลที่ไม่สามารถเข้าใจได้ หรือ Cipher text โดยใช้ข้อมูลบางอย่างเป็นกุญแจ (Key) ในการเข้ารหัสหรือถอดรหัส ดังในรูปที่ 7

รูปที่ 7 การสร้างข้อมูลแฝงโดยการเข้ารหัส [7]

ในรูปที่ 7 แสดงวิธีการสร้างข้อมูลแฝงรูปแบบหนึ่งโดยการเข้ารหัสข้อมูลส่วนบุคคลที่สามารถอ่านหรือเข้าใจได้ ซึ่งเป็นข้อมูลส่วนที่จะต้องได้รับการคุ้มครองตามพระราชบัญญัติคุ้มครองข้อมูล พ.ศ. 2562 [8] วิธีการที่ใช้คือการเข้ารหัสโดยใช้กุญแจลับหรือคีย์สำหรับเข้ารหัสแล้ว เพื่อเปลี่ยนข้อมูลที่ต้องการปกป้องคุ้มครองเป็นข้อมูลที่ไม่สามารถอ่านเข้าใจได้ (cipher text)

เมื่อนำข้อมูลส่วนบุคคลที่ต้องการปกป้องมาทำการเข้ารหัส (Plain text) จะได้ข้อมูลที่เป็น Cipher text) โดยในอุดมคติผู้ที่จะสามารถย้อนกลับการเข้ารหัสได้จำเป็นต้องรู้วิธีการเข้ารหัสและกุญแจเท่านั้น แต่ในสถานะการจริง รู้เพียงวิธีการเข้ารหัส และมีกำลังการคำนวณที่เพียงพอก็เป็นไปได้ที่จะย้อนการเข้ารหัสได้ วิธีการการเข้ารหัสที่เป็นที่นิยมส่วนมากถูกพิสูจน์ทางคณิตศาสตร์แล้วว่าเป็นไปได้ยากมากที่กำลังการคำนวณในปัจจุบันจะสามารถถอดรหัสได้โดยไม่ใช้กุญแจ แต่ตราบใดที่ Cipher text มีข้อมูลเดิมอยู่ภายใน ในอนาคตก็ยังคงมีความเสี่ยงที่จะถูกถอดรหัสได้หากกำลังการคำนวณของคอมพิวเตอร์เพิ่มขึ้น หรือค้นพบวิธีการถอดรหัสแบบใหม่

นาย ก	CipherText A	CipherText D
นาง ข	CipherText B	CipherText E
นาย ค	CipherText C	CipherText F

Key

Key

รูปที่ 8 ข้อมูลส่วนบุคคลถูกเข้ารหัสโดยใช้กุญแจลับ (Key) จะได้ Cipher text

การสร้างข้อมูลแฝงอีกรูปแบบหนึ่งคือใช้กระบวนการแปลงข้อมูลเป็นโทเค็น (Tokenization) โทเค็น (Token) ที่ได้คือชุดข้อมูลเสมือนที่ถูกเข้ารหัสโดยการสุ่มเพื่อใช้แทนข้อมูลที่ต้องการความปลอดภัยสูงและหลีกเลี่ยงการแลกเปลี่ยนข้อมูลนั้นโดยตรง การสร้างโทเค็นมีวัตถุประสงค์เพื่อซ่อนข้อมูลส่วนบุคคล ได้แก่ ชื่อ หมายเลขบัตรประชาชน เบอร์โทรศัพท์ และข้อมูลอ่อนไหวที่มีความสำคัญ ได้แก่ หมายเลขบัตรเครดิตร ข้อมูลสุขภาพ โทเค็นจะเกิดจากการนำข้อมูลบนตารางบนฐานข้อมูลเพื่อนำค่าที่ต้องการซ่อน โดยเลือกได้ว่าต้องการให้เป็น Data Masking หรือ Pseudonymization

การทำ Data masking เป็นเฉพาะส่วนที่แสดงข้อมูลขาออกเพื่อเผยแพร่ต่อสาธารณะ ส่วน Pseudonymization จะเป็นขาที่ต่อเชื่อมระหว่างตารางในฐานข้อมูลและการส่งข้อมูลเข้าออกแบบ Real time เพื่อฐานข้อมูลได้ทำการอ่านและเขียนพร้อมๆกันได้อย่างต่อเนื่อง ทำให้การทำงานระหว่างผู้รับจ้างเขียนโปรแกรมที่เป็น Out source หรือ ผู้ไม่ประสงค์ดีในการดักรับข้อมูล (Sniffer) จะมองเห็นข้อมูลส่วนบุคคล และข้อมูลอ่อนไหวที่สำคัญให้ปลอดภัยจากการละเมิดข้อมูล (Data Breach) ได้

การสร้างข้อมูลแฝงโดยการทำให้เป็นโทเค็น (Tokenization) จึงเป็นการสลับข้อมูลจริงกับข้อมูลที่สร้างขึ้นมาแบบสุ่ม (โทเค็น) โดยความสัมพันธ์ข้อมูลที่สุ่มขึ้นมากับข้อมูลจริงจะถูกเก็บไว้ในที่ปลอดภัย แยกจากข้อมูลในส่วนแรก และตราบใดที่ไม่มีข้อมูลทั้งสองอยู่ในการครอบครอง ก็เป็นไปไม่ได้ที่จะรู้ความสัมพันธ์ของข้อมูลกับโทเค็น เนื่องจากในโทเค็นไม่ได้มีข้อมูลเดิมอยู่ภายในการทำโทเค็นจึงมีความได้เปรียบมากกว่าการเข้ารหัสในส่วนนี้ แต่การเก็บความสัมพันธ์ของโทเค็นกับข้อมูลเดิมจะใช้พื้นที่ที่เพิ่มขึ้นเรื่อยๆตามจำนวนข้อมูลที่ถูกทำให้เป็นโทเค็น เสมือนกับการมีฐานข้อมูลถึงสองที่ที่จำเป็นต้องดูแลรักษาความปลอดภัย และเก็บรักษาให้แยกจากกันอย่างสมบูรณ์ (รูปที่ 9 และรูปที่ 10)ความได้เปรียบของการทำโทเค็นอีกอย่างหนึ่งคือความสามารถในการควบคุมลักษณะของโทเค็นให้เป็นไปตามที่ต้องการ เช่น โทเค็นที่ถูกสร้างขึ้นมาเพื่อแทนที่ชื่อคน อาจจะถูกสุ่มขึ้นมาให้เป็นลักษณะคล้ายชื่อคนจริง เพื่อให้ผู้ที่อ่านข้อมูลที่ถูกทำให้เป็นโทเค็นแล้วเข้าใจข้อมูลได้ง่ายยิ่งขึ้น

นาย ก	Token A	Token D
นาง ข	Token B	Token E
นาย ค	Token C	Token F

Token A	ข้อมูลส่วนบุคคลของนาย ก
Token B	ข้อมูลส่วนบุคคลของนาย ข
Token C	ข้อมูลส่วนบุคคลของนาย ค
Token D	ข้อมูลอ่อนไหวของนาย ก
Token E	ข้อมูลอ่อนไหวของนาย ข
Token F	ข้อมูลอ่อนไหวของนาย ค

รูปที่ 9 ข้อมูลในส่วนแรกที่ข้อมูลส่วนบุคคลถูกทำให้เป็นโทเค็น
รูปที่ 10 ข้อมูลส่วนที่ 2 ความสัมพันธ์ข้อมูลที่สุ่มขึ้นมากับข้อมูล

สรุปและอภิปราย

วิธีการทำข้อมูลแฝงทั้งสองวิธีมีข้อดีและข้อเสียที่แตกต่างกัน ผู้ออกแบบระบบควรเลือกวิธีการที่เหมาะสมที่สุดต่อ การใช้งานข้อมูล ระดับความเสียหายหากข้อมูลรั่วไหล และทรัพยากรที่มีรวมถึงการควบคุมการเข้าถึงข้อมูลโดยผู้ที่มีสิทธิการเข้าถึง โดยต้องมีการยืนยันตัวตนซึ่งต้องใช้เรื่อง Digital Identity มาใช้ในระบบที่ต้องการรู้ตัวตนผู้เข้าถึงระบบได้จริงซึ่งเราสามารถทำโดยใช้การยืนยันตัวตนตามมาตรฐานเกี่ยวกับแนวทางการใช้ดิจิทัลไอดี Identity Assurance Level (IAL) ซึ่งสามารถทำได้หลายวิธี หนึ่งในวิธีที่กำลังได้รับความนิยม และสอดคล้องกับบทวิจัยนี้ คือการนำเทคโนโลยีบล็อกเชน เช่นกรณีการนำ Trusty sign[3] ในการยืนยันตัวตนก่อนเข้าสู่ระบบที่สำคัญ และการจัดเก็บบันทึกการเข้าถึงข้อมูลดิจิทัลที่เป็นลักษณะ Log files[4] จะช่วยให้เราตรวจสอบความผิดปกติที่เกิดขึ้นได้

ในการป้องกันการละเมิดข้อมูล Data Breach ส่วนที่สำคัญอย่างหนึ่งคือการที่ไม่มีการยืนยันตัวตนเพื่อเข้าถึงระบบ ซึ่งการยืนยันตัวตนมีหลายรูปแบบ สำหรับการยืนยันตัวตนที่ระบุได้ว่าเป็นคนคนนั้นได้จริง ต้องมีการทำการยืนยันมากกว่าการรู้รหัสผ่านหรือ passwordless (Multi- Factor Authenthication) เช่น การใช้ One-Time Password (OTP) จาก SMS หรือ Authenticator Application ต่างๆ การใช้ Mobile Authenticator อาทิ การใส่รหัส PIN, การตรวจสอบลายนิ้วมือ, การตรวจสอบ Face ID และการทำ Device Binding การใช้ Transaction Signing อาทิ การสร้าง e-Signature ขึ้นมา เพื่อให้ผู้ใช้งานสามารถทำการยืนยัน Transaction นั้นๆ และสามารถใช้งาน E-Signature กับเอกสารต่างๆ บนอุปกรณ์ Smartphone ได้ด้วย การใช้ Card Reader อาทิ การยืนยันตัวตนผ่านบัตร Smart Card

การใช้เทคโนโลยี Passwordless Authentication จำเป็นต้องผ่านการทำ Digital KYC (Digital Know-Your-Customer) ก่อนที่จะทำการเข้ายืนยันตัวตน ซึ่งส่วนนี้มีกรณีศึกษา โดยใช้ ซอฟต์แวร์ที่ชื่อ Trusty Sign ซึ่งจะเปลี่ยนการนำค่า Certificate CA ที่เป็น Private Key ติดตั้งเพื่อยืนยันตัวตนกับแอพพลิเคชั่นมือถือ ซึ่งจะทำให้การยืนยันต้องมี อย่างน้อย 2 อย่างคือ รหัสผ่าน และเครื่องมือถือ ที่ทำ QRcode เป็นต้น

สำหรับ Log files ถือว่าเป็นส่วนสำคัญที่สุดในการสืบหาต้นตนหรือสาเหตุเมื่อพบเหตุการณ์ที่ไม่คาดฝัน เช่น การถูกโจมตีทางไซเบอร์ผ่านระบบเครือข่าย การมีลักษณะบุกรุกอย่างต่อเนื่อง เช่น การทำ Brute force ต่อเนื่อง การพยายามเข้าถึงระดับสิทธิผู้ดูแลระบบ อย่างต่อเนื่อง หรือการแชร์ไฟล์ ในระดับเครือข่ายคอมพิวเตอร์องค์กรที่มีความผิดปกติ เช่น การ Share SMB Protocol ใน version ที่มีความเสี่ยงต่อโปรแกรมเรียกค่าไถ่ Ransomware เป็นต้น

การเข้ารหัส (Encryption) เป็นเทคนิคที่เข้ามาตอบโจทย์ในประเด็นที่ข้อมูลหลุดหรือถูกขโมยออกไปก็จะไม่สามารถนำไปใช้ประโยชน์ต่อได้ อย่างไรก็ตามการเข้ารหัสข้อมูลแบบทั่วไปที่ใช้กันอยู่มักส่งผลให้ Format ของข้อมูลเปลี่ยนแปลงไป ทำให้เป็นเรื่องยากที่องค์กรจะนำข้อมูลที่เข้ารหัส แล้วไปใช้ต่อเหมือนตอนที่เป็นข้อมูลที่เป็น Plain text สำหรับ Tokenization ซึ่งสามารถแทนที่ข้อมูลสำคัญด้วยตัวอักษรหรือข้อความใหม่ 6 Pseudonymization) ในขณะที่ยังคงรักษา Format เดิมของข้อมูลไว้ได้ จึงมีประโยชน์สำหรับการใช้ Cloud Applications เนื่องจากข้อมูลจะถูกแทนที่ด้วยข้อความใหม่ก่อนส่งออกไปยังระบบ Cloud ช่วยให้เจ้าของข้อมูลยังคงรักษาความคล่องตัวในการใช้งาน Cloud Applications ในขณะที่ยังคงดำเนินงานตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลได้ แต่จะต้องมีการจัดการว่าทั้งสองส่วน (โทเคนและความสัมพันธ์ของโทเคนกับข้อมูลที่ต้องการปกป้อง) ไม่อยู่ในการครอบครองของผู้ไม่ประสงค์ดี

เอกสารอ้างอิง

[1] H. C. Van Tilborg and S. Jajodia, Encyclopedia of cryptography and security, Springer Science & Business Media, 2014.

[2] Athena, Prokopios Drogkaris, Ioannis Agrafiotis. PSEUDONYMISATION TECHNIQUES AND BEST PRACTICES NOVEMBER 2019. European Union Agency for Cybersecurity (ENISA).

[3] TrustySign Co. Ltd., Trusty Sign – your only digital identity. https://www.trustysign.net, 25 September 2021.

[4] Hercules Dalianis, Pseudonymisation of Swedish Electronic Patient Records Using a Rule-based Approach, Proceeding of the Workshop on NLP and Pseudonymisation, pages 16-23, Turku, Finland, 30 September 2019.

[5] Johannes Heurix, Michael Karlinger, Michael Schrefl and Thomas Neubauer, A HYBRID APPROACH INTEGRATING ENCRYPTION AND PSEUDONYMIZATION FOR PROTECTING ELECTRONIC HEALTH REC April 2011

[6] Log management, SRAN Log ที่มีคุณภาพนั้นเป็นอย่างไร https://bit.ly/3kYVySY, 18 April 2018.

[7] Pseudonymization according to the GDPR [definitions and examples] https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/, download: 28 Sep 2021.

[8] พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF, download: 28 Sep 2021.