



Data Privacy Management System on Cloud According to Personal Data Protection Act

Kantapon Seshajoti and Thepparit Banditwattanawong

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

February 1, 2022

ระบบจัดการข้อมูลส่วนบุคคลบนคลาวด์ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล Data Privacy Management System on Cloud according to Personal Data Protection Act

บทคัดย่อ

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีผลบังคับให้ผู้ควบคุมข้อมูลส่วนบุคคลจำเป็นต้องขอความยินยอมการใช้ข้อมูลจากเจ้าของข้อมูลส่วนบุคคลเพื่อให้สามารถใช้งานได้ตามวัตถุประสงค์ ในอีกด้านหนึ่งภาคธุรกิจได้เปลี่ยนมาใช้บริการคลาวด์แทนที่ระบบแบบดั้งเดิมเพื่อลดค่าใช้จ่ายในการดูแลรักษาระบบและใช้ประโยชน์จากตัวแบบธุรกิจจ่ายตามปริมาณการใช้งานจริง งานวิจัยนี้จึงเสนอระบบจัดเก็บและให้สิทธิ์ข้อมูลส่วนบุคคลที่อาศัยบริการคลาวด์ แอมะซอนเว็บเซอร์วิส โดยเฉพาะบริการป้องกันการโจมตีเว็บไซต์ การพิสูจน์ตัวตน และการเข้ารหัสลับข้อมูล จากผลการประเมินโดยผู้ใช้งาน 21 คนพบว่าระบบสามารถช่วยสร้างความมั่นใจด้านความมั่นคงปลอดภัยให้แก่เจ้าของข้อมูล ผู้ประมวลผลข้อมูล และผู้ควบคุมข้อมูลส่วนบุคคล โดยมีความพึงพอใจในภาพรวมเท่ากับ 4.35

คำสำคัญ: พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โปรแกรมประยุกต์บนเว็บ ความเป็นส่วนตัวข้อมูล การคำนวณแบบคลาวด์

Abstract

Personal Data Protection Act As is now so effective that data controller must request the consents of personal data usage from data owners to meet usage purposes. On the other hand, business sectors have been adopting cloud services to replace traditional systems to reduce maintenance costs and to take benefit of pay-per-use business model. This paper proposes a system for storing personal data along with its usage authorization based on Amazon Web Services, especially web application firewall,

user authentication and data encryption services. Evaluation results by 21 users showed that the proposed system could have data owners, data processor, and data controller confident in the system's security with overall satisfaction score 4.35.

Keyword: PDPA, web application, data privacy, cloud computing.

1. บทนำ

ในปัจจุบันได้มีกฎหมายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Protection Act) มีผลบังคับใช้ เพื่อให้หน่วยงานมีมาตรฐานในการจัดการข้อมูลส่วนบุคคลอย่างมั่นคงปลอดภัย ทั้งการเข้ารหัสลับ การรักษาบูรณภาพข้อมูล และการรักษาภาวะพร้อมใช้งานของข้อมูลส่วนบุคคล [1] นอกจากนี้จำเป็นต้องมีการขอสิทธิ์การใช้ข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุล ที่อยู่ อีเมล เป็นต้น นอกจากนี้ยังมีข้อมูลส่วนบุคคลละเอียดอ่อน ที่จำเป็นต้องมีการควบคุมอย่างเข้มงวด เช่น เชื้อชาติ ประวัติอาชญากรรม หรือข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลส่วนบุคคล [2] ซึ่งการจัดเก็บข้อมูลที่ยืนยันตัวตนผ่านคลาวด์นั้น จำเป็นจะต้องมีการเข้ารหัสลับขั้นสูง เมื่อข้อมูลสำคัญเกิดรั่วไหล จะทำให้ไม่สามารถระบุตัวบุคคลได้ ดังนั้นควรเลือกระบบคลาวด์ที่มีความน่าเชื่อถือและมีมาตรฐานเพื่อปกป้องข้อมูลส่วนบุคคล ปัญหาด้านความมั่นคงปลอดภัยของข้อมูลและการปกป้องข้อมูลส่วนบุคคล มีอยู่ในวงจรชีวิตของข้อมูลตั้งแต่การสร้าง การถ่ายโอน การใช้ การแบ่งปัน การจัดเก็บแบบถาวร จนกระทั่งถูกทำลาย [3] ซึ่งระบบจัดการข้อมูลส่วนบุคคลควรเลือกเป็นประเภทคลาวด์แบบส่วนตัวเพื่อใช้งานระบบที่ต้องการความมั่นคงและความปลอดภัยของข้อมูลที่สูง [4]

บทความนี้จึงเสนอระบบจัดการข้อมูลส่วนบุคคลบนคลาวด์โดยทำการเข้ารหัสลับและจัดเก็บในฐานข้อมูลเชิงสัมพันธ์บนเครือข่ายเสมือนส่วนบุคคลผ่านคลาวด์ (Virtual Private Network)

2. เทคโนโลยีและงานวิจัยที่เกี่ยวข้อง

2.1 เทคโนโลยีที่เกี่ยวข้อง

บริการแพลตฟอร์มคลาวด์ (Platform as a Service) คือ บริการเพื่อการติดตั้งใช้งาน โปรแกรมประยุกต์ ผู้บริโภค สร้างขึ้นเองหรือได้มาลงบนโครงสร้างพื้นฐานคลาวด์ โดยโปรแกรมประยุกต์สร้างโดยใช้ภาษาหรือเครื่องมือที่ผู้ใช้บริการสนับสนุน โดยที่ผู้บริโภคไม่ต้องจัดหาหรือควบคุมโครงสร้างพื้นฐานคลาวด์ แต่ควบคุมโปรแกรมประยุกต์ได้ [12]

แอมะซอนอาร์ดีเอส (Amazon RDS) คือ บริการฐานข้อมูลเชิงสัมพันธ์ [14] ที่ผู้ใช้งานสามารถจัดการฐานข้อมูลได้โดยตรงผ่านเครื่องบริการฐานข้อมูลที่มีความยืดหยุ่น รองรับการระการประมวลผลและขนาดข้อมูลที่เพิ่มขึ้นหรือลดลงได้ และยังสำรองข้อมูลได้อัตโนมัติ

บริการอีซีทู (Amazon EC2) คือ บริการเครื่องเสมือน [8] ที่สามารถเลือกขนาดของ ซีพียู, หน่วยความจำหลัก และความจุของหน่วยเก็บข้อมูล ได้ตามต้องการ โดยมีการแบ่งทรัพยากรบนเครื่องบริการออกเป็นย่อยๆ และค่าใช้จ่ายเสียตามปริมาณทรัพยากรที่ใช้งานจริงเท่านั้น

เอพีไอเกตเวย์ (API Gateway) คือ บริการที่สามารถทำให้เผยแพร่ระบบเพื่อสำหรับการเรียกใช้งาน บำรุงรักษา เฝ้าติดตาม และรักษาความปลอดภัยของเอพีไอ [11] จัดการปริมาณการใช้งาน การอนุมัติจัดการการร้องขอ และการควบคุมการเข้าถึงก่อนส่งต่อไปยังเครื่องบริการอื่น

คลาวด์ฟรอนต์ (Cloudfront) [15] คือ บริการเครือข่ายการจัดส่งเนื้อหา (Content Delivery Network) ที่สามารถทำการรับส่งข้อมูลทั่วโลกอย่างมั่นคงปลอดภัยด้วยเวลาแฝง (Latency) ที่ต่ำ โดยส่งการร้องขอของผู้ใช้งานไปยังสถานที่ (Edge Location) และนำข้อมูลที่ถูกแคช (Cache) ไว้ในสถานที่นั้นส่งกลับไปยังผู้ใช้งานแทนการร้องขอข้อมูลจากระบบต้นทางที่อยู่

คอกนิโต้ (Cognito) คือ บริการสนับสนุนมาตรฐานการจัดการข้อมูลประจำตัวและการเข้าถึง [16] ที่ปรับขนาดได้สำหรับรองรับผู้ใช้ได้จำนวนมาก รองรับการพิสูจน์ตัวตนแบบหลายปัจจัย การเข้ารหัสลับข้อมูลทั้งระหว่างพักเก็บและระหว่างส่งผ่าน ควบคุมการเข้าถึงทรัพยากร โดยกำหนดบทบาทต่างๆ จับคู่ผู้ใช้งานและกำหนดการเข้าถึงเฉพาะผู้ใช้แต่ละรายได้

2.2 งานวิจัยที่เกี่ยวข้อง

งานวิจัย [6] เสนอเครื่องมือช่วยเหลือในการค้นหาข้อมูลส่วนบุคคลที่ระบุตัวตนได้ (Personally Identifiable Information) ค้นหาได้ทั้งเครื่องให้บริการส่วนบุคคลและที่จัดเก็บบนคลาวด์ เพื่อให้องค์กรค้นหาและจัดการข้อมูลส่วนบุคคลได้อัตโนมัติ โดยมีการเพิ่มนโยบายความเป็นส่วนตัวและปฏิบัติตามข้อกำหนดกฎหมายคุ้มครองข้อมูลส่วนบุคคล

งานวิจัยการเก็บข้อมูลบนคลาวด์และรักษาความเป็นส่วนตัว [7] เสนอให้มีการประมวลผลแบบคลาวด์ โดยนำเทคนิคการเข้ารหัสลับแบบโฮโมมอร์ฟิก (Homomorphic) ไปใช้รักษาความมั่นคงปลอดภัยของข้อมูลผู้ใช้งานที่ทำการใช้ร่วมกันข้อมูลเพื่อการวิเคราะห์ัญญาเจข้อมูล โดยไม่ต้องแปลงข้อมูลที่ถูกรหัสลับกลับเป็นข้อมูลปกติ กลไกนี้เพิ่มการรบกวนไปในข้อมูล เพื่อช่วยสร้างความเป็นส่วนตัวแก่ข้อมูลส่วนบุคคลในการวิเคราะห์เชิงสถิติ

งานวิจัยตัวแบบความมั่นคงปลอดภัยสำหรับการปรับปรุงความเป็นส่วนตัวในคลาวด์ [5] เสนอการจัดเก็บข้อมูลบนคลาวด์ที่มีขั้นตอนวิธีในการเข้ารหัสลับหลายระดับ โดยใช้ขั้นตอนวิธีอาร์เอสเอ (RSA) ในการเข้ารหัสลับระดับที่ 1 สำหรับข้อความและเพิ่มข้อมูลที่เกี่ยวข้อง ขั้นตอนถัดไปใช้ขั้นตอนวิธี เออีเอส (AES) เพื่อเข้ารหัสลับระดับที่ 2 ก่อนจะทำการจัดเก็บข้อความเข้ารหัสลับลงฐานข้อมูล

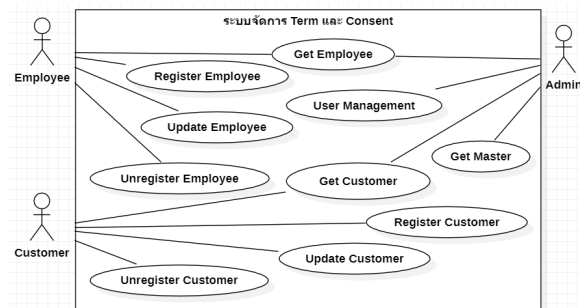
งานวิจัยจัดเก็บข้อมูลส่วนตัวบนคลาวด์ให้มีความปลอดภัยโดยการเข้ารหัสลับหลายัญญาเจ [13] เสนอขั้นตอนการแบ่งปันข้อมูลและการจัดเก็บข้อมูล ในระบบแบบกระจาย มีการนำขั้นตอนวิธีดีพีเค-อาร์อี (DPK-RE) มาให้ความปลอดภัยในการแบ่งปันข้อมูล โดยผู้ใช้

สามารถรวมกลุ่มกฎแฉลับได้หลายกลุ่ม กฎแฉรวมถูกเข้ารหัสลับใหม่ โดยสร้างเป็นกฎแฉส่วนบุคคลเป็นแบบคงที่ ที่ให้ความเป็นส่วนตัวในการแบ่งปันและการจัดเก็บ ซึ่งกฎแฉลับที่แยกจากกันจะถูกสร้างแบบพลวัตสำหรับไฟล์ๆหนึ่งและสร้างกฎแฉส่วนตัวใหม่โดยการเข้ารหัสลับกฎแฉรวมจะถูกเก็บไว้กับเจ้าของข้อมูล

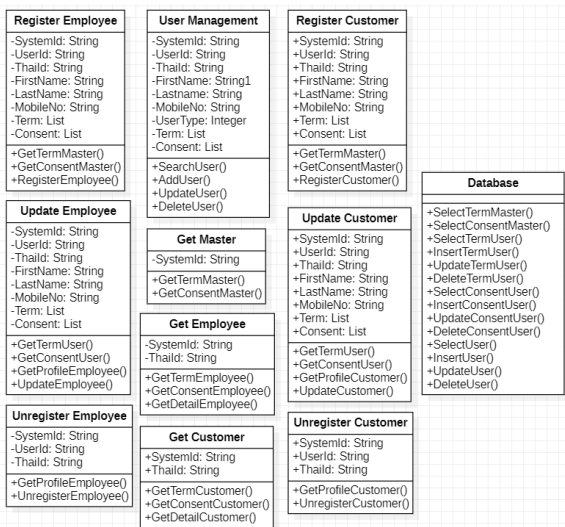
งานวิจัยแผนค้นหาคำสำคัญที่รักษาความเป็นส่วนตัวข้อมูลผ่านคลาวด์ที่เข้ารหัสลับด้วยการวิเคราะห์ที่กว้าง [9] เสนอให้อัจฉกรได้มีการจัดเก็บ ประมวลผล และวิเคราะห์ข้อมูลโดยการคำนวณแบบคลาวด์วิธีการปกป้องข้อมูลเป็นการเข้ารหัสลับข้อมูลก่อนทำการส่งไปเครื่องบริการระยะไกล มีการเข้ารหัสลับแบบค้นหาได้ โดยผู้ใช้งานมีการสร้างโทเค็น (Token) สำหรับการค้นหาเพื่อให้สามารถเรียกเนื้อหาที่มีการเข้ารหัสลับกลับมาใช้งานได้

3. วิธีการดำเนินงาน

แผนภาพยูสเคสสำหรับการจัดการหน้าที่และสิทธิ์การเข้าถึงของระบบ ประกอบด้วย 3 ผู้เกี่ยวข้องและ 10 ยูสเคส ดังภาพที่ 1

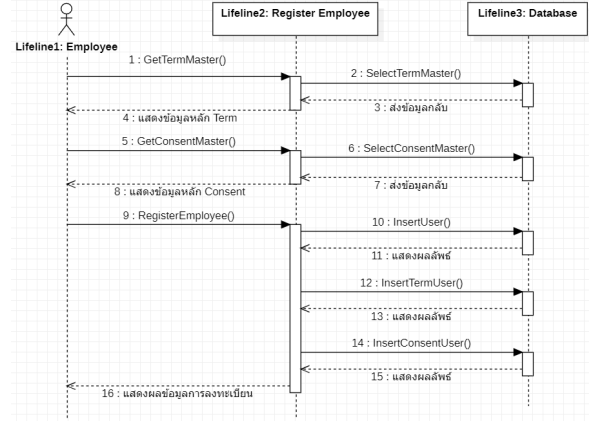


ภาพที่ 1: แผนภาพยูสเคสระบบจัดการข้อมูลส่วนบุคคล



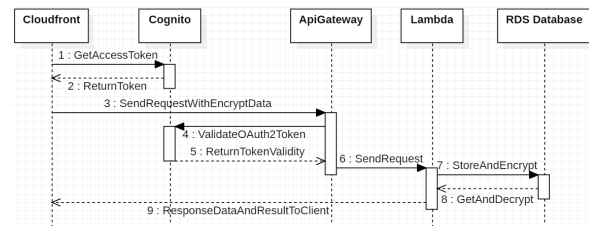
ภาพที่ 2: แผนภาพคลาสระบบจัดการข้อมูลส่วนบุคคล

ภาพที่ 2 ระบบที่เสนอประกอบไปด้วย 10 คลาส สำหรับการลงทะเบียนข้อมูลผู้ใช้งาน การยอมรับข้อกำหนดและเงื่อนไข การยินยอมการให้สิทธิ์ข้อมูลลงในเรื่องต่างๆ



ภาพที่ 3: แผนภาพลำดับการลงทะเบียนผู้ใช้งาน

ภาพที่ 3 อธิบายขั้นตอนการทำงานของระบบสำหรับการลงทะเบียนผู้ใช้งาน โดยมีมีการเรียกดูข้อมูล ข้อกำหนด และข้อตกลงฉบับล่าสุดก่อนให้ผู้ใช้งานลงทะเบียนข้อมูลส่วนบุคคลที่มีการให้ความยินยอมเงื่อนไขและข้อตกลง และสุดท้ายจะทำการแสดงผลการลงทะเบียน

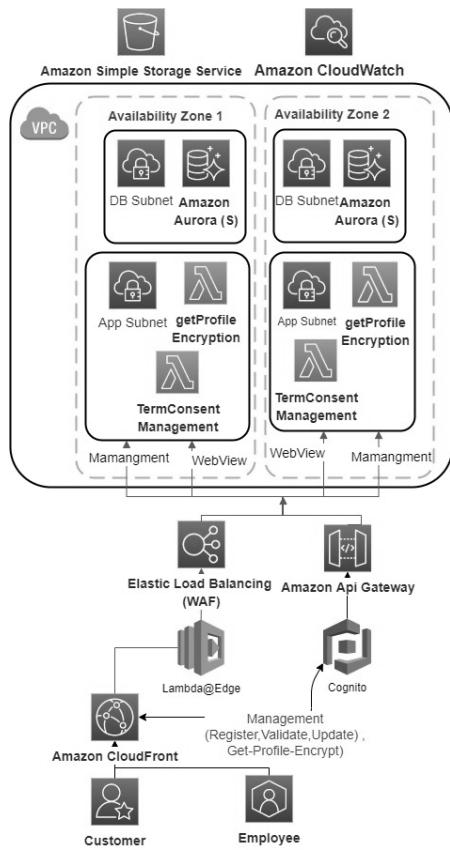


ภาพที่ 4 : แผนภาพลำดับขั้นตอนการทำงานของระบบ

ภาพที่ 4 อธิบายขั้นตอนการทำงานของระบบระหว่างส่วนติดต่อผู้ใช้งานและส่วนจัดการระบบ โดยในส่วนที่ 1 ทำการร้องขอโทเค็นจากคอกอนิโต โดยทำการสร้างโทเค็นใหม่แล้วส่งกลับไปยังส่วนที่ 2 ส่วนที่ 3 ส่งข้อมูลไปยังเอพียไอเกตเวย์ ตรวจสอบโทเค็นในส่วนที่ 4 ส่งผลกลับในส่วนที่ 5 และส่งข้อมูลไปประมวลผลในส่วนที่ 6 ทำการบันทึกรหัสลับข้อมูลในส่วนที่ 7 เรียกข้อมูลพร้อมถอดรหัสลับในส่วนที่ 8 และส่งผลกลับไปยังส่วนที่ 9

การเข้าใช้งานเว็บไซต์จากคลาวด์ฟรอนท์ผ่านแลมบ์ดา แอทเอจ (Lambda@Edge) ที่ทำการเพิ่มความปลอดภัยส่วนหัว [10] ก่อนส่งกลับไปยังผู้ใช้งานและผ่านการคัดกรองในส่วนบริการป้องกันการโจมตีเว็บไซต์ (Web Application Firewall) ใน ส่วนถัดไปผ่านการควบคุม

เครือข่ายตามกฎที่ระบุ เมื่อติดต่อในส่วนจัดการเว็บไซต์ จะต้องมีการพิสูจน์ตัวตนโดยใช้ คอกนิตีได้ โดยการสร้าง กฎแฉแบบพลวัตก่อนการเข้าถึง และทำการติดต่อไปยัง ส่วนจัดการเว็บไซต์ผ่านเอพีไอเกตเวย์ มีการควบคุมการ เข้าถึงก่อนส่งข้อมูลไปยังส่วนถัดไป ข้อมูลที่สำคัญจะ เข้ารหัสลับด้วยมาตราฐานขั้นสูงก่อนทำการติดต่อในส่วน จัดการเว็บไซต์เมื่อติดต่อสำเร็จในส่วนการทำงาน เบื้องหลังจะทำการถอดรหัสลับข้อมูลที่รับเข้ามาแล้ว นำไปทำการบวกรในส่วนถัดไป โดยมีการจัดการ การ ทำงานในส่วนการเรียกดู เพิ่ม แก้ไข ลบ ข้อมูลจากเจ้าของ ข้อมูลส่วนบุคคลรวมถึงข้อมูลการให้สิทธิ์ ข้อกำหนด เงื่อนไขและข้อตกลง และส่วนสุดท้ายการติดต่อไปยัง ฐานข้อมูลอาร์ดีเอส ที่วางอยู่ในเครือข่ายเสมือนแบบส่วน ตัวการเข้าถึงฐานข้อมูลจำเป็นต้องเข้าผ่านบริการอีซีทู ที่ อยู่ในวงเครือข่ายเสมือนวงเดียวกันเท่านั้น ดังภาพที่ 5



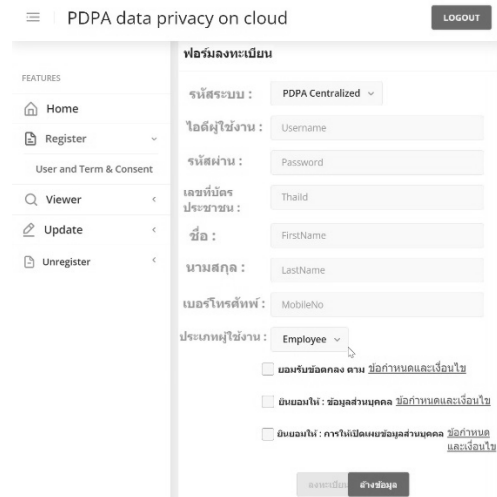
ภาพที่ 5: แผนภาพสถาปัตยกรรมระบบคลาวด์

4. ผลการดำเนินงาน

4.1 โปรแกรมประยุกต์

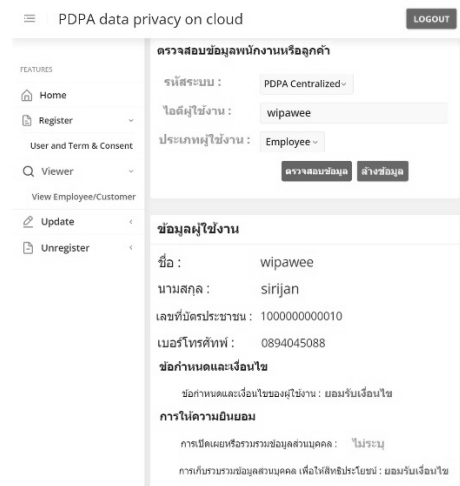
เว็บไซต์จัดการข้อมูลพนักงานและลูกค้าโดยผู้ดูแล ระบบสามารถลงทะเบียน แก้ไข เรียกดูข้อมูลให้กับเจ้าของ

ข้อมูลได้หรือเจ้าของข้อมูลส่วนบุคคลสามารถลงทะเบียน ด้วยตนเองได้ ในส่วนการลงทะเบียนให้ทำการกรอก รายละเอียดให้ครบถ้วน เลือกประเภทระบบและประเภท ผู้ใช้งาน โดยสามารถอ่านข้อกำหนดและเงื่อนไขก่อนทำ การยอมรับข้อตกลง โดยในส่วนข้อตกลงของผู้ใช้งาน จะ ให้ความยินยอมหรือไม่ก็ได้ แสดงดังภาพที่ 1



ภาพที่ 1 : เมนูการลงทะเบียน

เมนูการตรวจสอบข้อมูลส่วนบุคคลและแสดงสิทธิ์ ต่างๆของผู้ใช้งานตามระบบและประเภทที่ลงทะเบียน ข้อมูลส่วนบุคคล เช่น ชื่อ-นามสกุลและรหัสบัตร ประชาชน ถ้าเจ้าของข้อมูลส่วนบุคคลไม่ยินยอมให้ เปิดเผยข้อมูลส่วนบุคคล ระบบจะไม่ทำการแสดงผล ข้อมูลนั้นๆ ถ้าเป็นการเข้าสู่ระบบด้วยระดับผู้ใช้งานทั่วไป จะสามารถเรียกดูข้อมูลได้เฉพาะข้อมูลในส่วนของผู้ใช้งาน เท่านั้น เมนูการแก้ไขนั้นสามารถปรับเปลี่ยนความยินยอม การให้สิทธิ์ทางด้านต่างๆได้ตลอดเวลา แสดงดังภาพที่ 2



ภาพที่ 2 : เมนูการตรวจสอบข้อมูลและแก้ไขข้อมูล

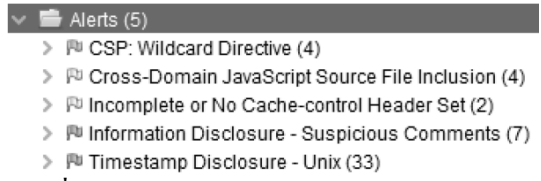
เมนูการยกเลิกความเป็นสมาชิกที่สามารถยกเลิกได้ตลอดเวลาเมื่อเจ้าของข้อมูลทำการร้องขอ โดยมีการตรวจสอบข้อมูลก่อนทำการยกเลิก การยกเลิกความเป็นสมาชิกนั้นระบบจะทำการลบข้อมูลส่วนบุคคลออกจากระบบทั้งหมด ทั้งข้อมูลการให้ความยินยอมในด้านต่างๆ และจะเก็บเป็นประวัติทำการ โดยที่ไม่สามารถระบุตัวตนของบุคคลนั้นได้ ในส่วนการทำงานของระบบจะมีการทำงานเพิ่มเติมเกี่ยวกับการตรวจสอบช่วงเวลารวมอายุ เมื่ออยู่ในระบบครบตามเวลาที่กำหนดหรือไม่มีการกระทำใดๆเกินเวลาที่กำหนด ระบบจะทำการออกจากระบบให้โดยอัตโนมัติ สิทธิในการเข้าถึงนั้นถ้าผู้ใช้งานเป็นระดับผู้ดูแลระบบจะเข้าถึงได้ทุกรายการเลือก แต่ถ้าผู้ใช้งานเป็นระดับทั่วไปจะเข้าถึงได้บางรายการเลือกเท่านั้นและเมื่อทำการรายการเสร็จสิ้นจะทำการบันทึกล็อก (log) ลงฐานข้อมูล เมื่อครบกำหนด 90 วัน ระบบจะทำการลบข้อมูลออกจากระบบ

การเก็บข้อมูลของเจ้าของข้อมูลส่วนบุคคล จะทำการเข้ารหัสลับด้วยขั้นตอนวิธีเอ็ไอเอส ด้วยขนาดกุญแจ 256 บิต ความยาวตัวอักษรกุญแจ 128 บิต และมีกุญแจลับในการเข้ารหัสลับร่วมด้วย และเมื่อต้องการนำข้อมูลกลับมาใช้งานก็จะทำการถอดรหัสลับด้วยการตั้งค่างกล่าว แสดงดังภาพที่ 3

SYSTEM_ID	USER_ID	PASSWORD	THAI_ID	FIRST_NAME	LAST_NAME	MOBILE_NO
01021001	adminkan...	K990981...	9e835a3de...	02b8a6392e...	5e45183a7e...	32e83e84cb...
01021001	kantapon10	B9987456*	473feaf19...	33a5658670...	2e45a1cf5f...	f82a84ccea2...
01021001	pichayamin	*198745x	062f67498...	e952ce5d09...	ebc18008b3...	7ce6ebe4e4...
01021001	wipawee	G134*dfg	fd5fbd03...	1d8ac04b93...	db176bccf53...	28e84cfcbf2...
01021001	wpmint01	Dcovk*01	2a11de003...	06262ca39a...	2eed05e3af...	1c76c5b33c...
01021002	kantaponso	805gs*๗	abf6e352fc...	1653e0c9ff...	7e1827a327...	c010e4d6c3...

ภาพที่ 3 : การเก็บข้อมูลส่วนบุคคลในฐานข้อมูลมีการเข้ารหัสลับ ผู้ทำวิจัยได้ทำการทดสอบหาช่องโหว่ระบบด้วยเครื่องมือโอดับเบิ้ลยูเอเอสพี แซบ (OWASP ZAP) [17] และได้ผลการทดสอบระบบ ประกอบด้วยผลการพบช่องโหว่ระดับปานกลาง ซึ่งเกี่ยวกับการตั้งค่านโยบายความปลอดภัยที่ไม่กระทบกับเว็บไซต์หลักเพราะไม่มีส่วนเกี่ยวข้องกับข้อมูลส่วนบุคคล และผลการพบช่องโหว่ระดับต่ำ เป็นส่วนข้อผิดพลาดที่ไม่เกี่ยวข้องกับเว็บไซต์หลักเนื่องจากเป็นผลมาจากคลังโปรแกรมของบุคคลที่สามและผลการพบช่องโหว่ที่เกี่ยวกับการควบคุมแคชพบว่าเว็บไซต์ในส่วนคลาวด์ฟรอนท์ ได้กำหนดไม่ให้เก็บ

แคชโดยจะทำการดาวน์โหลดหน้าเว็บไซต์ใหม่ทุกครั้งจึงไม่ได้รับผลกระทบดังกล่าว แสดงดังภาพที่ 4



ภาพที่ 4 : ผลทดสอบความปลอดภัยด้วยเครื่องมือ โอดับเบิ้ลยูเอเอสพี แซบ

ผู้ทำวิจัยวัดความพึงพอใจของผู้ใช้งานระบบจำนวน 21 คน ประกอบไปด้วยพนักงานเอกชน 10 คน ข้าราชการ 5 คน ผู้ทำงานอิสระ 4 คน และผู้ประกอบการ 2 คน หรือแบ่งเป็นผู้ควบคุมข้อมูลจำนวน 2 คน ผู้ประมวลผลข้อมูลจำนวน 5 คน และเจ้าของข้อมูลจำนวน 14 คนมีรายละเอียดผลการประเมิน ดังตารางที่ 1 โดยมีคะแนนเต็มแต่ละข้อเท่ากับ 5 พบค่าความพึงพอใจเฉลี่ยคิดเป็น 4.35 จัดอยู่ในระดับที่ดี และส่วนเบี่ยงเบนมาตรฐานอยู่ในระดับ 0.60

ตารางที่ 1: ผลการวัดความพึงพอใจของผู้ใช้งาน

เกณฑ์การประเมิน	\bar{X}	S.D.
1) ด้านสามารถทำงานได้ตามหน้าที่ (Function)	4.46	0.56
2) ด้านความถูกต้องและน่าเชื่อถือของระบบ (Accuracy)	4.31	0.63
3) ด้านความง่ายต่อการใช้งาน (Usability)	4.25	0.63
4) ด้านสมรรถนะ (Performance)	4.35	0.58
5) ด้านการรักษาความปลอดภัยของข้อมูล (Security)	4.37	0.59
6) ด้านความเข้าใจได้ของระบบ (Understandability)	4.32	0.61
ค่าเฉลี่ย	4.35	0.60

5. สรุป

งานวิจัยนี้มีวัตถุประสงค์เพื่อการศึกษาการออกแบบระบบจัดการข้อมูลส่วนบุคคลบนคลาวด์ที่มีการปกป้องข้อมูลก่อนส่งไปยังเครื่องบริการระยะไกล การจัดการสิทธิการให้ความยินยอมในการจัดเก็บข้อมูล การขอสิทธิใช้งานด้านต่างๆตามวัตถุประสงค์ การแก้ไขข้อมูล จนกระทั่งการทำลายข้อมูล เมื่อเจ้าของข้อมูลไม่ต้องการให้จัดเก็บข้อมูลส่วนบุคคลนั้นอีกต่อไป ผลการประเมินระบบพบว่า

เจ้าของข้อมูลส่วนบุคคลได้จัดเก็บข้อมูลบนคลาวด์ได้
อย่างมีความน่าเชื่อถือและปลอดภัย

เอกสารอ้างอิง

- [1] เบนญานา ช่างประดิษฐ์, (2561). “ระบบประมวลผลแบบคลาวด์ (Cloud Computing) : ข้อเสนอแนะเพื่อการยกระดับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย”. กรุงเทพฯ:มหาวิทยาลัยธรรมศาสตร์.
- [2] ราชกิจจานุเบกษา, “พระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562”. เล่ม 136.ตอนที่ 69.(พฤษภาคม 2562). น. 52.
- [3] สุนทรีย์ ส่งเสริม, “พร้อมรู้ PDPA”. กรุงเทพฯ:สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2564.
- [4] Amazon Web Services, (2561), “การใช้ AWS ในบริบทของการรักษาความเป็นส่วนตัวและการคุ้มครองข้อมูลทั่วไป” บริษัท Amazon Web Services , พฤษภาคม 2561.
- [5] Y. Sharma1, H. Gupta, S. K. Khatri, (2562) , “A Security Model for the Enhancement of Data Privacy in Cloud Computing,” Institute of Information Technology ,Amity University Campus.
- [6] S. Fugkeaw, A. Chaturasrivilai , P. Tasungnoen and W. Techaudomthaworn ,(2564) , “AP2I: Adaptive PII Scanning and Consent Discovery System,” Computer and Communication Technology (ICT) , Thammasat University.
- [7] S. Komawar , M. Batwal , S. Shah , S. Shahani and J. Abraham , (2561), “Privacy Preserving Data Aggregation on Secure Cloud,” Computer Engineering & IT , College of Engineering Pune.
- [8] Amazon Web Services. (2564). “Amazon Elastic Compute Cloud (EC2)“. [ออนไลน์] เข้าถึงได้จาก <https://aws.amazon.com/th/ec2/>. วันที่สืบค้น 2564, ธันวาคม 10.
- [9] P. Sreekumari , (2561) , “Privacy-Preserving Keyword Search Schemes over Encrypted Cloud Data An Extensive Analysis,” Department of Computer Science , Grambling State University.
- [10] Amazon Web Services. (2564). “HTTP-Security-Headers “. [ออนไลน์] เข้าถึงได้จาก <https://aws.amazon.com/th/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront> . วันที่สืบค้น 2564, มิถุนายน 2.
- [11] Amazon Web Services. (2564). “Amazon API Gateway“. [ออนไลน์] เข้าถึงได้จาก <https://aws.amazon.com/th/api-gateway/features/>. วันที่สืบค้น 2564, ธันวาคม 9.
- [12] เทพฤทธิ์ บัณฑิตวัฒนวงศ์, “พื้นฐานการคำนวณแบบคลาวด์ (Cloud Computing Fundamental)”, โรงพิมพ์ Protext บริษัทแดนเนิท์ อินเทอร์เน็ตเปอร์เซ้น จำกัด, กรุงเทพมหานคร, 2562
- [13] M. R. P, S. H. Manjula and V. K. R. , (2561) ,”Secured Privacy Data using Multi Key Encryption in Cloud Storage,” Department of Computer Science and Engineering , Bangalore University.
- [14] Amazon Web Services. (2564). “Amazon Relational Database Service (RDS)“. [ออนไลน์] เข้าถึงได้จาก <https://aws.amazon.com/th/rds/> . วันที่สืบค้น 2564, ธันวาคม 12.
- [15] Amazon Web Services. (2564). “Amazon CloudFront“. [ออนไลน์] เข้าถึงได้จาก <https://aws.amazon.com/th/cloudfront/>. วันที่สืบค้น 2564, ธันวาคม 9.
- [16] Amazon Web Services. (2564). “Amazon Cognito “. [ออนไลน์] เข้าถึงได้จาก <https://aws.amazon.com/th/cognito/>. วันที่สืบค้น 2564, ธันวาคม 8.
- [17] ZAP Dev Team. (2564). “Zed Attack Proxy Getting Started”, [ออนไลน์] เข้าถึงได้จาก <https://www.zaproxy.org/getting-started/> . วันที่สืบค้น 2564 , ธันวาคม 25.