

บทที่ 5

สรุปและข้อเสนอแนะ

การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อใช้สำหรับเผยแพร่ข้อมูลบนเว็บไซต์ ทางคณะผู้จัดทำได้ทำการประเมินการใช้งานเว็บไซต์จากผู้ใช้งานทั่วไป เพื่อสรุปผลการจัดทำโครงการ ข้อจำกัดของเว็บไซต์ ปัญหาและอุปสรรคต่าง ๆ ของการจัดทำโครงการ และข้อเสนอแนะเพื่อพัฒนาโครงการต่อไป ดังนี้

5.1 บทสรุปโครงการ

จากการศึกษา และจัดทำโครงการวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 เพื่อใช้สำหรับเผยแพร่ข้อมูลบนเว็บไซต์ ผู้จัดทำได้ทำการศึกษา และรวบรวมข้อมูลในทางทฤษฎี (CRISP-DM) , (Classification) การตัดสินใจแบบต้นไม้ (Decision Tree) , (Data Visualization) รวมไปถึงขั้นตอนการออกแบบพัฒนาเว็บไซต์โดยเริ่มจากการศึกษาภาษาที่ใช้สำหรับการพัฒนา คือ พีเอชพี (PHP) ภาษาซีเอสเอส (CSS) ภาษาเอชทีเอ็มแอล (HTML) และภาษาจาวาสคริปต์ (JavaScript) ทำการวิเคราะห์ และออกแบบฐานข้อมูล ออกแบบหน้าจอส่วนต่อประสานกับผู้ใช้งาน พร้อมกับการเขียนเว็บไซต์ จนกระทั่งเสร็จสมบูรณ์

จากการการพัฒนาเว็บไซต์การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในปี 2019-2021 สามารถนำเว็บไซต์การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ในไปเผยแพร่ข้อมูลบนเว็บไซต์ ผลการวิเคราะห์สามารถนำไปใช้งานได้จริง รวมไปถึงการออกรายงานต่าง ๆ ได้หลายรูปแบบตามการทำงานของเว็บไซต์การวิเคราะห์ข้อมูล ภัยคุกคามการโจมตีทางด้านไซเบอร์บนเว็บไซต์ ซึ่งสามารถนำมาใช้ได้จริงบนเว็บไซต์ สมาชิกสามารถหาความรู้จากชุดข้อมูล หรือการเพิ่มอัปโหลดข้อมูลภัยคุกคามบนเว็บไซต์ใหม่ๆ เข้ามาได้ จากผลการวิเคราะห์ข้อมูล ด้วยการจำแนกแบบ Decision Tree การคำนวณด้วยมือนี้ ผู้วิเคราะห์ข้อมูลได้ผลลัพธ์ว่า โมเดลต้นไม้ตัดสินใจ Root node ที่คือ แอตทริบิวต์ Type และได้ interior node คือ แอตทริบิวต์ Country , แอตทริบิวต์ Web server และ leaf node คือ แอตทริบิวต์ Os ซึ่งไม่สามารถสร้างกิ่งแต่ละโหนดต่อไปได้ เนื่องจากไม่มีความสัมพันธ์กับแอตทริบิวต์ใด ก็จะได้ผลลัพธ์ที่ แอตทริบิวต์ Os linux , nginx และ แอตทริบิวต์ Country United States , Spain , Germany และ Thailand จากโปรแกรมที่ใช้เลือกทำเหมืองข้อมูล

เพื่อนำเสนอ คือ โปรแกรม Weka ในการสร้างโมเดล Decision Tree และตรวจสอบข้อมูลผ่านทางโปรแกรม RapidMiner Studio เพื่อความแม่นยำ เมื่อนำไปเปรียบเทียบกับผลการคำนวณ โมเดล Decision Tree ด้วยตัวเอง ทางผู้วิเคราะห์ข้อมูลพบว่าทั้ง 3 โมเดลได้ผลลัพธ์ความแม่นยำของโมเดลที่เหมือนกัน และสามารถนำโมเดลไปใช้งานได้ และประเมินประสิทธิภาพของโมเดล ซึ่งมีค่าความถูกต้องเฉลี่ยในทุกโมเดลเท่ากับ 75.55% จำนวนทั้งสิ้น 42,414 รายการ เมื่อเปรียบเทียบกับงานวิจัยการพัฒนาแบบจำลองของ วนิตา พงษ์สงวน , ทิพยา ถินสูงเนิน , มาโนช ถินสูงเนิน (2559) การพัฒนาแบบจำลองปัจจัยที่มีผลต่อการเป็นโรคเบาหวานด้วยเทคนิคต้นไม้ตัดสินใจ จำนวนทั้งสิ้น 44,002 รายการ พบว่าโมเดลแบบจำลองมีค่าความถูกต้องเฉลี่ยที่ใกล้เคียงกันที่ 76.14% ซึ่งเป็นค่าที่สามารถยอมรับได้ในการทดสอบประสิทธิภาพของ Model ด้วยวิธี Self- Consistency Test และทุกโมเดลพบว่ามีผลลัพธ์ตรงกันอยู่ในระดับค่อนข้างดี ดังนั้นจึงเหมาะนำมาใช้งานกับการวิเคราะห์ข้อมูลสารสนเทศได้เป็นอย่างดี

จากคะแนนในแต่ละด้านที่กลุ่มผู้เข้าใช้งานเว็บไซต์ ได้ประเมินผ่านแบบสอบถามความพึงพอใจในการวิเคราะห์ข้อมูล ได้คะแนนเฉลี่ย รวม 3.93 คะแนน อยู่ในระดับพึงพอใจมาก ซึ่งสามารถที่จะนำผลการวิเคราะห์แนวโน้มของการโจมตีบนเว็บไซต์ไปใช้งานในด้านของการเฝ้าระวังและป้องกันภัยคุกคาม และคะแนนในแต่ละด้านการเข้าเยี่ยมชมเว็บไซต์ ได้ประเมินผ่านแบบสอบถามความพึงพอใจในการเข้าเยี่ยมชมเว็บไซต์ ได้คะแนนเฉลี่ย รวม 4.01 คะแนน อยู่ในระดับพึงพอใจมาก ซึ่งเหมาะสมกับการนำเว็บไซต์ไปเผยแพร่และสร้างชุมชนให้กับผู้ที่มีความสนใจในเรื่องของภัยคุกคามที่เกิดขึ้นบนเว็บไซต์

5.2 ข้อจำกัดของเว็บไซต์

5.2.1 การอัปเดตชุดข้อมูลต้องมีการปรับ ให้ตรงกับฐานข้อมูล

5.2.2 การเพิ่มข้อมูลทีนอกเหนือจากข้อมูลภัยคุกคามบนเว็บไซต์จะทำให้ชุดข้อมูล ฐานข้อมูลที่ผิด และเสียรูปแบบของการจัดเก็บข้อมูล

5.2.3 ถ้ามีการใช้งานที่ผิดไปจากคู่มือของเว็บไซต์อาจทำให้ การอัปเดตของสมาชิกผิดพลาดได้

5.2.4 การแปลภาษาของเว็บไซต์ อาจจะไม่ได้อีกต้อง ร้อยเปอร์เซ็นต์ ตามหลักหลักไวยากรณ์ภาษา เพราะใช้ API google translate เข้ามาใช้งาน

5.3 ปัญหาและอุปสรรคของโครงการ

5.3.1 เนื่องจากบางครั้งแบ่งงานกันทำ ทำให้เกิดการดำเนินงานซ้ำซ้อนกันในส่วนของการทำ (CRISP-DM) การแก้ไข ลบของชุดข้อมูลที่ได้มา

5.3.2 เกิดโรคระบาด COVID-19 ทำให้การติดต่อระหว่างการทำงานร่วมกันในโปรเจกต์มีความยากลำบากในบางส่วน

5.3.3 การวิเคราะห์ข้อมูล มีการคำนวณที่ผิดพลาดและไม่ถูกต้องหลายครั้ง จึงใช้เวลามากในส่วนนี้เพื่อศึกษาการทำ decision tree

5.3.4 การใช้เครื่องมือที่ไม่ชำนาญ ในการทำเหมืองข้อมูล ปัญหาการใช้งานของโปรแกรม weka และ rapid miner จึงต้องมีการศึกษาการใช้งานต่าง ๆ เพิ่มเติม

5.3.5 การเขียนโปรแกรมบางส่วนของงานเกิดปัญหาในการไม่คุ้นชินการเขียน หรือรวมไปถึงหลักการการทำงานจึงทำให้ล่าช้าบ้างในการหาวิธีแก้ไข หรือศึกษาการเขียน การใช้งาน เป็นต้น

5.3.6 ผู้จัดทำจำเป็นต้องมีความรู้ความเข้าใจใน ในเรื่องของ เทคนิคการแฮก (hacking technical) เป็นส่วนหนึ่ง เพราะตัวข้อมูลที่นำมาทำการวิเคราะห์เป็นเรื่องเกี่ยวกับการ Hack เว็บไซต์จึงใช้เวลาค่อนข้างมาก

5.3.7 ในการพัฒนาเว็บไซต์ ผู้จัดทำจำเป็นต้องมีความรู้ความเข้าใจใน ในเรื่องของ ความปลอดภัยของเว็บแอปพลิเคชัน (web application security) เป็นส่วนหนึ่ง เพราะเว็บไซต์นำเสนอในเรื่องเกี่ยวกับการวิเคราะห์ข้อมูล การแฮกเว็บไซต์ จึงต้องสร้างเว็บไซต์ที่มีการป้องกันช่องโหว่ที่เจออยู่ในอันดับ ต้นๆ ของภัยคุกคาม เพื่อให้เกิดความเชื่อมั่นของบุคคลทั่วไปที่เข้ามาใช้งานเว็บ

5.4 ข้อเสนอแนะ

5.4.1 เว็บไซต์ควรเพิ่มการแจ้งเตือนเมื่อสมาชิกอัปโหลดชุดข้อมูลเข้ามายังเว็บไซต์ ให้กับผู้ดูแลเว็บไซต์

5.4.2 เว็บไซต์ใช้ Backend เป็น ภาษา PHP ควรใช้ Framework มาช่วยในการพัฒนา เช่น Laravel , CodeIgniter เป็นต้น เพราะจะได้ช่วยในเรื่องของ Security ที่ผู้เขียนตกหล่น มากขึ้น

5.4.3 เว็บไซต์ควรเพิ่มแบบทดสอบ เรื่องของภัยคุกคามบนเว็บไซต์และ สอนวิธีการป้องกันของภัยคุกคามบนเว็บไซต์

5.4.4 ข้อมูลรายงานนำเสนอ Visualization อัจฉริยะแบบเรียลไทม์

5.4.5 ผลการวิเคราะห์ข้อมูลด้วยเทคนิคต้นไม้ตัดสินใจ ที่ได้ผลลัพธ์ออกมา สามารถที่จะนำผลลัพธ์ของภัยคุกคามที่จะเกิดขึ้น ไปศึกษานำไปใช้ในการป้องกันภัยคุกคามบนเว็บไซต์ และนำไปอบรมให้ความรู้เกี่ยวกับภัยคุกคามนั้นได้