

บทที่ 5

สรุปผล อภิปราย และข้อเสนอแนะ

5.1 สรุปผล

งานวิจัยนี้ได้เสนอวิธีการในการเพิ่มความต้องการที่ไม่ใช่เชิงฟังก์ชันหลักของระบบ (Non-Functional Requirement) ซึ่งเน้นเรื่องความต้องการด้านความปลอดภัย (Security) โดยได้เสนอวิธีการนำความต้องการด้านความปลอดภัยเพิ่มเติมลงไปแบบจำลองที่อิสระจากแพลตฟอร์ม (PIM) ได้ตั้งแต่ในช่วงวิเคราะห์และออกแบบระบบในกระบวนการพัฒนาซอฟต์แวร์แบบ Model-Driven Architecture หรือ MDA โดยมีจุดประสงค์เพื่อช่วยลดค่าใช้จ่ายที่จะเกิดขึ้นจากการที่นำความต้องการเรื่องความปลอดภัยไปเพิ่มเติมหลังจากที่พัฒนาแอปพลิเคชันเสร็จเรียบร้อยแล้ว

ในงานวิจัยนี้ได้เลือกใช้วิธีการเพิ่มคุณสมบัติด้านความปลอดภัยให้กับแบบจำลองที่อิสระจากแพลตฟอร์มโดยใช้วิธีการขยายเมตาโมเดลของ UML ซึ่งรองรับคุณสมบัติด้านความปลอดภัยครอบคลุม 3 ด้านคือการพิสูจน์ตัวตนจริง (Authentication) การรักษาความลับ (Confidentiality) และการรักษาความสมบูรณ์ (Integrity) โดยการขยายได้นิยามกลุ่มของอิลิเมนต์ที่แทนคุณสมบัติความปลอดภัยในเมตาโมเดลของ UML โดยใช้วิธีการวิเคราะห์จากความหมายและคำนิยามของความปลอดภัยแต่ละด้านจากแหล่งต่างๆ

ดังนั้นเพื่อทำการวัดผลว่าเมตาโมเดลของ UML ที่ทำการขยายให้มีคุณสมบัติด้านความปลอดภัยที่ได้นำเสนอในงานวิจัยนี้ สามารถนำไปใช้ในการออกแบบแบบจำลองการออกแบบที่อิสระจากแพลตฟอร์มที่มีคุณสมบัติด้านความปลอดภัยได้จริง จึงกำหนดให้มีวิธีการวัดผลด้วยวิธีการพัฒนาแอปพลิเคชันกรณีศึกษา โดยในงานวิจัยนี้ได้กำหนดให้แอปพลิเคชันกรณีศึกษาคือระบบงานย่อยของโครงการ One-Stop Services จำนวน 2 ระบบงานคือระบบการไฟฟ้า (PEA System) และระบบบริการชำระค่าไฟฟ้าออนไลน์ โดยนำความต้องการของระบบนี้มาวิเคราะห์และออกแบบแบบจำลอง PIM จากนั้นนำแบบจำลอง PIM เข้าสู่กระบวนการแปลงแบบจำลอง (Model Transformation) เพื่อสร้าง (Generate) เป็นแบบจำลองที่เฉพาะเจาะจงกับแพลตฟอร์ม (PSM) ที่รองรับคุณสมบัติด้านความปลอดภัยจำนวน 2 แพลตฟอร์มคือจาวาเว็บเซิร์ฟเวอร์ที่มีการรักษาความปลอดภัยโดยใช้มาตรฐาน WS-Security และจาวาเซิร์ฟเล็ตที่มีการพัฒนาส่วนการรักษาความปลอดภัยโดยใช้ข้อกำหนดของแพลตฟอร์ม J2EE

ซึ่งผลการพัฒนาแอปพลิเคชันกรณีศึกษาพบว่าแบบจำลอง PIM ที่ออกแบบโดยใช้เมตาโมเดลของ UML ที่มีการขยายให้มีคุณสมบัติด้านความปลอดภัยทั้ง 3 ด้านคือการพิสูจน์ตัวตนจริง (Authentication) การรักษาความลับ (Confidentiality) และการรักษาความสมบูรณ์ (Integrity) สามารถสร้างแอปพลิเคชันกรณีศึกษาที่มีคุณสมบัติด้านความปลอดภัยทั้ง 3 ด้านปฏิบัติตาม (Comply) ข้อกำหนดของการรักษาความปลอดภัยของเว็บเซอริวิส (WS-Security) และการรักษาความปลอดภัยของจาวาเซิร์ฟเล็ตตามข้อกำหนดของแพลตฟอร์ม J2EE ได้ ซึ่งสามารถดูรายละเอียดการสร้างซอร์สโค้ด การติดตั้ง และทดสอบแอปพลิเคชันได้ที่ภาคผนวก ค.

จากผลการวิจัยสามารถสรุปผลได้ดังนี้

1. ได้แนวทาง (Guideline) ในการนำความต้องการที่ไม่ใช่เชิงฟังก์ชันหลักของระบบ (Non-functional Requirement) โดยเฉพาะเรื่องความปลอดภัยเพิ่มเติมเข้าไปในกระบวนการพัฒนาซอฟต์แวร์แบบ MDA ได้ตั้งแต่ในขั้นตอนการวิเคราะห์และออกแบบระบบ ซึ่งสามารถใช้เป็นแนวทางนี้ในการพัฒนาความต้องการที่ไม่ใช่เชิงฟังก์ชันหลักของระบบด้านอื่นๆ ที่นอกเหนือจากเรื่องความปลอดภัยได้
2. สามารถนำเมตาโมเดลของแบบจำลอง PIM ที่มีการขยายให้มีคุณสมบัติด้านความปลอดภัย ในเรื่องการพิสูจน์ตัวตนจริง การรักษาความลับ การรักษาความสมบูรณ์ ที่ได้นำเสนอในงานวิจัยนี้ นำไปใช้ในกระบวนการพัฒนาแอปพลิเคชันที่มีการจัดการเรื่องความปลอดภัยได้จริง โดยช่วยให้ขั้นตอนการวิเคราะห์และออกแบบระบบในการพัฒนาซอฟต์แวร์แบบ MDA นั้น นักวิเคราะห์ระบบสามารถสร้างแบบจำลอง PIM ที่มีคุณสมบัติด้านความปลอดภัยได้ ซึ่งเป็นการเพิ่มความสะดวกให้กับนักวิเคราะห์และออกแบบระบบในการนำความต้องการที่ไม่ใช่เชิงฟังก์ชันหลักของระบบเพิ่มเติมให้กับแบบจำลองได้ตั้งแต่ช่วงเริ่มต้นของการพัฒนา
3. เครื่องมือที่พัฒนาขึ้นในงานวิจัยนี้ สามารถนำไปประยุกต์ใช้ในเชิงอุตสาหกรรมได้ กล่าวคือ นักพัฒนาสามารถสร้างซอฟต์แวร์คอมพิวเตอร์ประเภทจาวาเว็บเซอริวิส จาวาเซิร์ฟเล็ต หรือจาวาคลาสพื้นฐาน ที่มีคุณสมบัติด้านความปลอดภัยครบถ้วน ซึ่งคอมพิวเตอร์ที่ได้สามารถนำไปใช้งานจริงได้ หรือพัฒนาโค้ดเพิ่มเติมได้

5.2 อภิปราย

จากประสบการณ์ในการดำเนินการวิจัย สามารถสรุปประเด็นสำคัญที่เกี่ยวข้องกับการขยายแบบจำลองการออกแบบที่อิสระจากแพลตฟอร์มให้มีคุณสมบัติด้านความปลอดภัยได้ดังนี้

- การสร้างเมตาโมเดลของแบบจำลอง

ในการขยายแบบจำลองการออกแบบที่อิสระจากแพลตฟอร์ม (PIM) ให้มีคุณสมบัติด้านความปลอดภัยนั้น พบว่าการสร้างเมตาโมเดลสำหรับแบบจำลองดังกล่าวมีความยากมากกว่าการสร้างเมตาโมเดลสำหรับแบบจำลองที่เฉพาะเจาะจงกับแพลตฟอร์ม อย่างเช่นการรักษาความปลอดภัยของเว็บเซอวิส หรือการรักษาความปลอดภัยของจาวาเซิร์ฟเล็ต เนื่องจากการรักษาความปลอดภัยของเว็บเซอวิสและจาวาเซิร์ฟเล็ตมีข้อกำหนด (Specification) ที่เป็นมาตรฐานชัดเจน ซึ่งแตกต่างกับการขยายคุณสมบัติด้านความปลอดภัยในระดับของแบบจำลอง PIM ที่ใช้วิธีการนำคำจำกัดความหรือนิยามมาสร้างเป็นเมตาโมเดล ดังนั้นสามารถสรุปได้ว่าการสร้างเมตาโมเดลของแบบจำลองใดๆ ถ้ามีข้อกำหนดที่ชัดเจนก็สามารถสร้างเมตาโมเดลได้รวดเร็วและมีความยากน้อยลง ซึ่งถ้าไม่มีข้อกำหนดที่ชัดเจนการพัฒนาแอปพลิเคชันอาจจะใช้เวลาเท่ากันหรือมากกว่าการพัฒนาซอฟต์แวร์ที่ไม่ได้ใช้วิธีการแบบ MDA ก็ได้ ทำให้ทราบว่าความชัดเจนของแบบจำลองที่ต้องการสร้างมีผลต่อระยะเวลาและความยากง่ายในการสร้างเมตาโมเดลสำหรับแบบจำลองนั้นๆ และถือเป็นปัจจัยหนึ่งในการนำไปวิเคราะห์ว่าคุ้มค่าหรือไม่ในการที่จะเลือกวิธีการพัฒนาซอฟต์แวร์แบบ MDA เมื่อเทียบกับแนวทางการพัฒนาซอฟต์แวร์แบบอื่นๆ นอกจากนี้ยังมีปัจจัยอื่นๆ ที่สามารถที่จะเปรียบเทียบกับข้อดีในส่วนนี้ได้ด้วยเช่นกัน นั่นคือประเด็นเรื่องการนำกลับมาใช้ใหม่ (Reusability) ซึ่งในกรณีที่เลือกใช้วิธีการพัฒนาแบบ MDA ถึงแม้ว่าในการพัฒนาครั้งแรกใช้เวลามากกว่า แต่ถ้าต้องการให้ชิ้นงานเช่นเมตาโมเดลที่สร้างขึ้นสามารถนำกลับมาใช้งานได้อีกครั้งในการพัฒนาแอปพลิเคชันตัวใหม่ที่ใช้แพลตฟอร์มเดียวกัน ซึ่งวิธีการแบบนี้ก็จะลดระยะเวลาลงไปค่อนข้างมาก ดังนั้นปัจจัยที่ได้กล่าวถึงนี้สามารถที่จะนำมาพิจารณาส่วนได้ส่วนเสีย ก่อนที่จะเลือกวิธีการในการพัฒนาซอฟต์แวร์ได้ ซึ่งจะช่วยให้การตัดสินใจเลือกวิธีการพัฒนาแอปพลิเคชันได้เหมาะสมยิ่งขึ้น

- การสร้างกฎการแปลงระหว่างเมตาโมเดลของแบบจำลอง PIM และเมตาโมเดลของแบบจำลอง PSM

การนิยามกฎในการแปลงแบบจำลองจากแบบจำลอง PIM เป็นแบบจำลอง PSM ในส่วนของการจัดการด้านความปลอดภัยนั้น ก่อนที่จะนิยามกฎได้จะต้องทำการพิจารณาความสัมพันธ์ระหว่างเมตาโมเดลก่อน แล้วจับคู่ระหว่างอิลิเมนต์ของเมตาโมเดล PIM ที่เป็นแบบจำลองต้นทางกับเมตาโมเดลของแบบจำลอง PSM ที่เป็นแบบจำลองปลายทาง ซึ่งในงานวิจัยนี้ได้ใช้วิธีวิเคราะห์และออกแบบเมตาโมเดลโดยใช้คำนิยามและความหมายของความปลอดภัยมาสร้างเป็นเมตาโมเดลตามหลักการของ OOAD ซึ่งเมตาโมเดลที่ได้จะเป็นระดับนามธรรม ดังนั้นในการจับคู่กับเมตาโมเดลในระดับที่เฉพาะเจาะจงกับแพลตฟอร์มนั้น จะมีบางกรณีที่มีบางอิลิเมนต์ไม่สามารถจับคู่กับเมตาโมเดลของแบบจำลอง PSM ได้ เช่นในกรณีของการจับคู่ระหว่างเมตาโมเดลของแบบจำลอง PIM กับเมตาโมเดลของแบบจำลอง PSM ที่เป็นแพลตฟอร์มจาวาเว็บเซอวิส ในความปลอดภัยด้านการพิสูจน์ตัวตนจริง ไม่สามารถจับคู่ UserIdentity ประเภท SmartCard และ AuthenticationServer กับการใช้งาน UsernameToken ได้

- การเลือกใช้แพลตฟอร์มอื่นๆ ที่นอกเหนือจากที่ระบุในงานวิจัย

ในงานวิจัยนี้นำเสนอการสร้างแบบจำลองที่เฉพาะเจาะจงกับแพลตฟอร์มที่มีการจัดการเรื่องคุณสมบัติด้านความปลอดภัย มีพื้นฐานอยู่บนแพลตฟอร์มจาวา คือ จาวาเว็บเซอวิส และจาวาเซิร์ฟเล็ต ในงานวิจัยนี้ได้อ้างอิงข้อกำหนด (Specification) ของการรักษาความปลอดภัยของจาวาเซิร์ฟเล็ต เวอร์ชัน 2.4 ซึ่งถ้าในอนาคตต้องการที่จะเปลี่ยนไปใช้เซิร์ฟเล็ต เวอร์ชันที่ใหม่กว่า หรือเวอร์ชันอื่นๆ ทำได้โดยทำการตรวจสอบความแตกต่างเรื่องข้อกำหนดด้านความปลอดภัยของแต่ละเวอร์ชันแล้วถ้ามีการเปลี่ยนแปลงเกิดขึ้น ให้ทำการแก้ไขเมตาโมเดลในส่วนที่เปลี่ยนแปลง และหลังจากนั้นก็ให้เข้าไปแก้ไขกฎการแปลงแบบจำลองด้วย

ในกรณีที่เลือกใช้แพลตฟอร์มหรือเทคโนโลยีอื่นๆ ที่มีพื้นฐานบนแพลตฟอร์มจาวา อย่างเช่นถ้าต้องการพัฒนา EJB (Enterprise JavaBeans) การสร้างเมตาโมเดลของแบบจำลอง PSM จะไม่ซับซ้อนมากนัก สามารถที่จะนำเมตาโมเดลของจาวาพื้นฐานบางส่วนไปใช้ซ้ำได้ โดยทำการเปลี่ยนเฉพาะส่วนของคุณสมบัติด้านความปลอดภัยที่เป็นส่วนที่เฉพาะเจาะจงกับการจัดการความปลอดภัยของ EJB เท่านั้น แต่ถ้ามีการเลือกแพลตฟอร์มที่แตกต่างกันเช่น การพัฒนาแอปพลิเคชันโดยใช้แพลตฟอร์ม .NET ก็จำเป็นที่จะต้องสร้างเมตาโมเดลของแบบจำลอง PSM นี้ใหม่ทั้งหมด แต่

สามารถที่จะนำหลักการสร้างเมตาโมเดลที่ได้มีการกล่าวถึงในงานวิจัยนี้ นำไปใช้เป็นแนวทางในการวิเคราะห์และออกแบบเมตาโมเดลดังกล่าวได้

- การนำเมตาโมเดลของแบบจำลอง PIM ที่ได้ขยายให้มีคุณสมบัติด้านความปลอดภัยไปใช้งานบนเครื่องมือที่ใช้สำหรับการพัฒนาซอฟต์แวร์แบบ MDA

ในงานวิจัยนี้ได้พัฒนาเมตาโมเดลและขยายเมตาโมเดลให้มีคุณสมบัติด้านความปลอดภัย โดยใช้เครื่องมือ Eclipse Modeling Framework (EMF) ซึ่งเมตาโมเดลที่สร้างขึ้นนี้อยู่ในรูปแบบของ Ecore ดังนั้นการนำเมตาโมเดลดังกล่าวไปใช้งานได้นั้น ต้องเป็นเครื่องมือที่รองรับเมตาโมเดลแบบดังกล่าวด้วยเช่นเดียวกัน ซึ่งนอกเหนือจาก EMF ก็จะมีเครื่องมืออย่างเช่น oAW (open ArchitectureWare) ที่สามารถใช้งานเมตาโมเดลแบบ Ecore ได้เช่นเดียวกัน

5.3 ข้อเสนอแนะ

ในงานวิจัยได้เสนอการขยายแบบจำลองการออกแบบที่อิสระจากแพลตฟอร์มในประเด็นของความต้องการที่ไม่ใช่เชิงฟังก์ชันหลักของระบบเฉพาะด้านความปลอดภัยเท่านั้น ดังนั้นสามารถนำแนวคิดนี้ไปต่อยอดในการขยายแบบจำลองเพื่อรองรับความต้องการด้านอื่นๆ เพื่อให้รองรับการออกแบบแบบจำลองได้ครอบคลุมความต้องการที่ไม่ใช่เชิงฟังก์ชันหลักของระบบได้ครอบคลุมมากขึ้น

นอกจากนี้ ประเด็นเรื่องการแสดงผลของเครื่องมือ EMF ที่การในการสร้างแบบจำลอง PIM มีการแสดงผลอยู่ในรูปแบบของแผนภาพต้นไม้ (Tree) ซึ่งนักออกแบบบางส่วนไม่คุ้นเคยกับการแสดงผลแบบนี้ ดังนั้นเพื่อให้การสร้างแบบจำลองนั้นง่ายขึ้น สามารถทำได้โดยนำเมตาโมเดลดังกล่าวไปสร้างเป็นลักษณะที่เป็นกราฟิกได้เช่นเดียวกัน