การค้นหาผู้ให้บริการคลาวด์ที่สอดคล้องด้านความมั่นคงกับเมตริกซ์ควบคุมคลาวด์แบบเชิงความหมาย

นายจักรินทร์ ทวีจินดา

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์
คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2556

SEMANTIC SEARCH FOR CLOUD PROVIDERS WITH SECURITY CONFORMANCE TO CLOUD CONTROLS MATRIX

Mr. Jakarin Thaweejinda

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Science Program in Software Engineering
Department of Computer Engineering
Faculty of Engineering
Chulalongkorn University
Academic Year 2013

หัวข้อวิทยานิพนธ์	การค้นหาผู้ให้บริการคลาวด์ที่สอดคล้องด้านความมั่นคงกับเมตริกซ์ควบคุมคลาวด์แบบเชิงความหมาย
โดย	นายจักรินทร์ ทวีจินดา
สาขาวิชา	วิศวกรรมซอฟต์แวร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีคณะวิศวกรรมศาสตร์

(ศาสตราจารย์ ดร.บัณฑิต เอื้ออาภรณ์)

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(อาจารย์ ดร.ยรรยง เต็งอำนวย)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา)

.....กรรมการภายนอกมหาวิทยาลัย

(ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์)

จักรินทร์ ทวีจินดา : การค้นหาผู้ให้บริการคลาวด์ที่สอดคล้องด้านความมั่นคงกับเมตริกซ์ควบคุมคลาวด์แบบเชิงความหมาย. (SEMANTIC SEARCH FOR CLOUD PROVIDERS WITH SECURITY CONFORMANCE TO CLOUD CONTROLS MATRIX) อ.ที่ปรึกษาวิทยานิพนธ์หลัก: รศ. ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา, 86 หน้า.

กลุ่มลูกค้าที่จะใช้บริการคลาวด์จะพิจารณาคุณลักษณะเชิงคุณภาพของผู้ให้บริการคลาวด์เมื่อจะทำการเลือกใช้บริการคลาวด์ ความมั่นคงเป็นคุณลักษณะเชิงคุณภาพที่สำคัญ ที่มักจะถูกนำมาใช้เพื่อเปรียบเทียบความแตกต่างระหว่างข้อเสนอบริการของผู้ให้บริการหลายราย องค์กรความมั่นคงของคลาวด์ได้นำเสนอเมตริกซ์ควบคุมคลาวด์ ซึ่งประกอบด้วยหลักการปฏิบัติทางด้านความมั่นคงและหลักการที่ผู้ให้บริการคลาวด์ควรปฏิบัติตามเพื่อให้บริการคลาวด์มีความมั่นคง งานวิจัยนี้นำเสนอต้นแบบเครื่องมือการค้นหาเชิงความหมาย สำหรับใช้ค้นหาบริการคลาวด์ที่สอดคล้องกับแนวทางการควบคุมด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ ในต้นแบบเครื่องมือนั้น ได้มีการสร้างออนโทโลจีด้านความมั่นคงจากเมตริกซ์ควบคุมคลาวด์ และออนโทโลจีทางด้านความมั่นคงนี้ สามารถนำมาใช้อ้างอิงในการสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ได้ โปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ซึ่งนำเสนอหลักฐานที่เกี่ยวข้อง สอดคล้องกับแนวทางการควบคุมด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ จะถูกใช้ในการค้นหาและจัดลำดับตามการค้นหาของผู้ใช้บริการคลาวด์ ผู้ใช้บริการคลาวด์จึงสามารถตรวจสอบและเปรียบเทียบระดับความสอดคล้องของบริการคลาวด์ตามเมตริกซ์ควบคุมคลาวด์ได้ ในการทดลองพบว่าการค้นหาเชิงความหมายจะให้ผลการค้นหาที่มีประโยชน์ต่อผู้ใช้บริการมากกว่าการค้นหาแบบปกติ

ภาควิชา วิศวกรรมคอมพิวเตอร์ ลายมือชื่อนิสิต .....

สาขาวิชา วิศวกรรมซอฟต์แวร์ ลายมือชื่อ อ.ที่ปรึกษาวิทยานิพนธ์หลัก .....

ปีการศึกษา 2556

5570968921 : MAJOR SOFTWARE ENGINEERING
KEYWORDS: CLOUD COMPUTING / SECURITY / SERVICE DISCOVERY / ONTOLOGY

JAKARIN THAWEEJINDA: SEMANTIC SEARCH FOR CLOUD PROVIDERS WITH SECURITY CONFORMANCE TO CLOUD CONTROLS MATRIX. ADVISOR: ASSOC. PROF. TWITTIE SENIVONGSE, Ph.D., 86 pp.

Prospective cloud consumers consider several quality attributes of cloud providers when selecting a cloud service. Security is a major quality attribute that is often used to differentiate between service offers from different cloud providers. Cloud Security Alliance has published the Cloud Controls Matrix (CCM) which contains security best practices and principles where cloud providers can follow to provide secure cloud services. This research presents a semantic search prototype for discovering cloud services which conform to the security controls in the CCM. In this prototype a security ontology is constructed from the CCM. Based on this security ontology, provider profiles can be built. A provider profile which presents relevant evidence of conformance to CCM security controls is then searched and ranked against a cloud consumer's query. Cloud consumers can then determine and compare the degree of conformance of the cloud services to the CCM. From the experiment, the semantic search gives the search results that are more useful to the consumers than normal text search.

Department: Computer Engineering Student's Signature .....
Field of Study: Software Engineering Advisor's Signature .....
Academic Year: 2013

กิตติกรรมประกาศ

ขอกราบขอบพระคุณ รองศาสตราจารย์ ดร.ทวิตีย์ เสนีวงศ์ ณ อยุธยา อาจารย์ที่ปรึกษาวิทยานิพนธ์เป็นอย่างสูง ที่ได้เสียสละเวลาให้ความรู้และคำแนะนำในการทำวิทยานิพนธ์ ตลอดจนความเมตตาและความอดทนในการตรวจผลงานของข้าพเจ้า ได้แก่ โครงร่างวิทยานิพนธ์ ผลงานวิจัยภาษาไทย และวิทยานิพนธ์ ทำให้ผลงานทุกชิ้นสำเร็จไปด้วยดี

ขอกราบขอบพระคุณ อาจารย์ ดร.ยรรยง เต็งอำนวย ประธานกรรมการสอบวิทยานิพนธ์ และ ผู้ช่วยศาสตราจารย์ ดร.ชวลิต ศรีสถาพรพัฒน์ กรรมการสอบวิทยานิพนธ์ ที่กรุณาสละเวลาให้คำแนะนำ ชี้แนะแนวทางที่เป็นประโยชน์ เพื่อให้วิทยานิพนธ์นี้มีความถูกต้อง สมบูรณ์

ขอกราบขอบพระคุณ คณาจารย์ทุกท่าน ที่ให้ความรู้และคำแนะนำที่เป็นประโยชน์ในการทำวิทยานิพนธ์ในครั้งนี้

ขอขอบคุณ เพื่อนร่วมชั้นเรียนหลักสูตรวิศวกรรมซอฟแวร์ ภาคนอกเวลาราชการทุกคน สำหรับกำลังใจและความช่วยเหลือในเรื่องต่าง ๆ ในการทำวิทยานิพนธ์

สุดท้ายนี้ ขอบกราบขอพระคุณ คุณย่า บิดา มารดา และสมาชิกทุกคนในครอบครัวที่ให้การสนับสนุนและให้กำลังใจที่ดีเสมอมา จนทำให้ข้าพเจ้ามีผลงานที่สำเร็จได้

สารบัญ

หน้า

หน้า

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

บริการคลาวด์เป็นบริการที่กำลังได้รับความนิยมเป็นอย่างมาก เนื่องจากเป็นรูปแบบการบริการที่สามารถส่งมอบทรัพยากรทางด้านไอที ที่ผู้ใช้บริการรู้สึกได้ว่ากำลังใช้บริการทรัพยากรที่มีอยู่อย่างไม่จำกัดได้ เช่น เมื่อมีความต้องการใช้งานระบบคอมพิวเตอร์ที่มีปริมาณเพิ่มมากขึ้น ทำให้ศูนย์คอมพิวเตอร์ต้องดูแลรักษาคอมพิวเตอร์เซิร์ฟเวอร์เป็นจำนวนมาก หลายองค์กรจึงมองหาวิธีที่ช่วยประหยัดค่าใช้จ่ายในการดูแลและซ่อมบำรุงรักษาฮาร์ดแวร์ซึ่งเป็นทรัพย์สินอันมีค่าขององค์กร ดังนั้นการซื้อบริการการประมวลผลที่มีประสิทธิภาพโดยไม่จำเป็นที่จะต้องซื้อเครื่องใหม่ เพียงแค่จ่ายเงินสำหรับการใช้งานที่เพียงพอต่อการใช้งานของเราเท่านั้น จึงเป็นวิธีช่วยประหยัดค่าใช้จ่ายได้ ในท้องตลาดมีผู้ให้บริการคลาวด์อยู่มากมายหลายราย เช่น ไอบีเอ็ม จะมีบริการ “Smart Business Development and Test on the IBM Cloud”, Amazon ก็จะมีบริการ Amazon Web Services (AWS) เป็นต้น และเนื่องจากเรื่องความมั่นคงของระบบและข้อมูลนั้นมีความเสี่ยงสูง เพราะด้วยเหตุผลที่ว่าจะให้บุคคลที่สามเข้ามาจัดการระบบและข้อมูลที่เป็นความลับขององค์กรนั้นต้องเป็นเรื่องที่ต้องระมัดระวังเป็นพิเศษ นั่นจึงเป็นเหตุผลหลักที่ทำไมองค์การต่าง ๆ จึงให้ความสำคัญกับความมั่นคงเป็นอย่างมาก

เช่นเดียวกับการใช้บริการด้านอื่นนั้น ผู้ใช้บริการคลาวด์จำเป็นต้องมีการพิจารณาเลือกผู้ให้บริการคลาวด์ก่อนการตัดสินใจใช้บริการ ข้อมูลที่ผู้ใช้บริการคลาวด์นำมาใช้ประกอบการพิจารณามักจะอยู่ในหน้าเว็บ ผู้ใช้บริการคลาวด์ส่วนมากจะทำการค้นหาข้อมูลของผู้ให้บริการคลาวด์ด้วยตัวเองจากเครื่องมือการค้นหาทั่วไป เช่น Google ซึ่งจะคืนค่าผลลัพธ์เป็นยูอาร์แอลมาเป็นจำนวนมาก จากนั้นก็จะเข้าไปพิจารณาตามยูอาร์แอลเหล่านั้น ซึ่งทำให้เสียเวลามากเนื่องจากบางยูอาร์แอลอาจไม่มีเนื้อหาที่เกี่ยวข้องกับข้อมูลที่ผู้ใช้บริการคลาวด์ต้องการเลยก็ได้ ในปัจจุบันมีเว็บไซต์ตัวกลาง เช่น clouddir [1] ซึ่งทำการจัดหมวดหมู่ผู้ให้บริการคลาวด์ตามโดเมนการให้บริการและมีการให้คะแนนผู้ให้บริการโดยผู้ที่เคยใช้บริการ แต่คะแนนยังไม่ได้บ่งบอกอย่างชัดเจนถึงคุณภาพแต่ละด้านของผู้ให้บริการคลาวด์รวมทั้งคุณภาพด้านความมั่นคง แต่เป็นเพียงคะแนนโดยรวม

จากประเด็นดังกล่าว งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อนำเสนอต้นแบบของระบบที่ช่วยผู้ใช้บริการคลาวด์ค้นหาและสนับสนุนการตัดสินใจเลือกผู้ให้บริการคลาวด์ที่ตรงกับความต้องการ โดยพิจารณาเฉพาะความต้องการที่ไม่ใช่หน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์ตามเมตริกซ์ควบคุมคลาวด์ (Cloud Controls Matrix) [2] ที่จัดทำโดยองค์กรความมั่นคงของคลาวด์หรือซีเอสเอ (Cloud Security Alliance: CSA) ซึ่งกำหนดความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่ผู้ให้บริการคลาวด์จำเป็นต้องตอบสนองไว้ 16 ด้าน ร่วมกับการใช้แบบสอบถามการประเมินที่เป็นที่

เห็นพ้องต้องกัน (Consensus Assessments Initiative Questionnaire) [3] ซึ่งระบุคำถามที่ใช้ตรวจสอบการปฏิบัติตามความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงทั้ง 16 ด้านที่ระบุไว้ในเมตริกซ์ควบคุมคลาวด์ ความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงที่เมตริกซ์ควบคุมคลาวด์ได้กำหนดไว้ มีดังนี้

1. ความมั่นคงของโปรแกรมประยุกต์และส่วนต่อประสาน (Application & Interface Security)
2. การรับรองการตรวจสอบและการปฏิบัติตาม (Audit Assurance & Compliance)
3. การจัดการความต่อเนื่องทางธุรกิจและความยืดหยุ่นเชิงปฏิบัติการ (Business Continuity Management & Operational Resilience)
4. การควบคุมการเปลี่ยนแปลงและการจัดการโครงแบบ (Change Control & Configuration Management)
5. ความมั่นคงของข้อมูลและการจัดการวัฏจักรชีวิตสารสนเทศ (Data Security & Information Lifecycle Management)
6. ความมั่นคงของศูนย์ข้อมูล (Datacenter Security)
7. การเข้ารหัสลับและการจัดการกุญแจ (Encryption & Key Management)
8. วิธีการปกครองและการจัดการความเสี่ยง (Governance and Risk Management)
9. ทรัพยากรมนุษย์ (Human Resources)
10. เอกลักษณ์และการจัดการการเข้าถึง (Identity & Access Management)
11. โครงสร้างพื้นฐานและความมั่นคงของเทคโนโลยีเสมือน (Infrastructure & Virtualization Security)
12. การทำงานร่วมกันและใช้ได้หลายระบบ (Interoperability & Portability)
13. ความมั่นคงของระบบเคลื่อนที่ (Mobile Security)
14. การจัดการเหตุการณ์ด้านความมั่นคง การค้นพบอิเล็กทรอนิกส์ และกระบวนการทางกฎหมายของคลาวด์ (Security Incident Management, E-Discovery & Cloud Forensics)
15. การจัดการสายโซ่อุปทาน ความโปร่งใส และภาระรับผิดชอบ (Supply Chain Management, Transparency and Accountability)
16. การคุกคามและการจัดการจุดอ่อน (Threat and Vulnerability Management)

การวิจัยจะใช้เมตริกซ์ควบคุมคลาวด์เป็นหลักและแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันเป็นส่วนเสริม เพื่อนำมาสร้างองค์ความรู้ด้านความมั่นคงของคลาวด์โดยใช้ออนโทโลจี (Ontology) [4] ซึ่งเป็นองค์ความรู้ที่ระบุคำศัพท์และความสัมพันธ์ของคำศัพท์ในโดเมนหนึ่ง ออนโทโลจีความมั่นคงของคลาวด์ที่ได้จะใช้อ้างอิงในการสร้างโปรไฟล์ความมั่นคงให้กับผู้ให้บริการคลาวด์ การค้นหาผู้ให้บริการคลาวด์จะเป็นการค้นหาเชิงความหมายตามโปรไฟล์ของผู้ให้บริการว่าสามารถตอบสนองความต้องการด้านความมั่นคงที่ระบุไว้ในเมตริกซ์ควบคุมคลาวด์ในด้านใดบ้าง เพื่อนำมาประกอบการตัดสินใจเลือกใช้บริการ

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อออกแบบและพัฒนาออนโทโลจีความมั่นคงของคลาวด์โดยอิงเมตริกซ์ควบคุมคลาวด์

1.2.2 เพื่อออกแบบและพัฒนาต้นแบบระบบค้นหาผู้ให้บริการคลาวด์เชิงความหมายโดยอิงออนโทโลจีความมั่นคงของคลาวด์

1.3 ขอบเขตของการวิจัย

1.3.1 พัฒนาออนโทโลจีความมั่นคงของคลาวด์ โดยอิงเมตริกซ์ควบคุมคลาวด์ ร่วมกับการพิจารณาคำถามในแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

1.3.2 พัฒนาโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ โดยอิงออนโทโลจีความมั่นคงของคลาวด์ที่สร้างขึ้น

1.3.3 โปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์จะสร้างจากข้อมูลหน้าเว็บของผู้ให้บริการโดยเป็นการสร้างด้วยมือ

1.3.4 พัฒนาต้นแบบของระบบค้นหาผู้ให้บริการคลาวด์ จากโปรไฟล์ด้านความมั่นคง

1.3.5 การพัฒนาออนโทโลจี ทำโดยใช้ออนโทโลจีเอดิเตอร์ เช่น Protégé ส่วนการพัฒนาต้นแบบของระบบค้นหาทำโดยใช้ภาษาจาวา

1.3.6 ประเมินผลการค้นหาของต้นแบบระบบโดยเปรียบเทียบกับผลการค้นหาด้วยมือ โดยใช้ข้อมูลผู้ให้บริการคลาวด์10 รายเป็นอย่างน้อย

1.4 ขั้นตอนการวิจัย

1.4.1 ศึกษาและทำความเข้าใจทฤษฎีที่เกี่ยวข้อง

1.4.2 ศึกษาและทดลองใช้เครื่องมือในการสร้างออนโทโลจี

1.4.3 วิเคราะห์และกำหนดภาพรวมของงานวิจัย

1.4.4 ออกแบบ กำหนดเป้าหมาย และขอบเขตของงานวิจัย

1.4.5 พัฒนาระบบ

1.4.6 ทดสอบและประเมินผลการวิจัย

1.4.7 สรุปผลการวิจัยและนำผลที่ได้ไปปรับปรุงงานวิจัย

1.4.8 จัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ได้ออนโทโลจีความมั่นคงของคลาวด์สำหรับใช้ในการค้นหาเชิงความหมายโดยอิงเมตริกซ์ควบคุมคลาวด์ ซึ่งสามารถนำไปใช้ในบริบทอื่นต่อไปได้

1.5.2 ได้ต้นแบบของระบบที่ช่วยในการค้นหาผู้ให้บริการคลาวด์ที่ตรงตามมาตรฐานด้านความมั่นคงของคลาวด์

1.6 ผลงานตีพิมพ์

ส่วนหนึ่งของวิทยานิพนธ์นี้ได้ตีพิมพ์และนำเสนอในการประชุมวิชาการต่อไปนี้

1.6.1 บทความเรื่อง Semantic Search for Cloud Providers with Security Conformance to Cloud Controls Matrix โดยผู้แต่งคือ Jakarin Thaweejinda และ Twittie Senivongse ในการประชุมวิชาการ The 11th International Joint Conference on Computer Sciences and Software Engineering (JCSSE 2014), Pattaya City , Thailand (May14-16, 2014): 286–291

บทที่ 2
ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดและทฤษฎีที่เกี่ยวข้อง

2.1.1 มาตรฐานความมั่นคงและความต้องการที่ไม่ใช่เชิงหน้าที่ของการคำนวณแบบคลาวด์

มีหลากหลายองค์กรที่นำเสนอมาตรฐานความมั่นคงรวมถึงความต้องการที่ไม่ใช่เชิงหน้าที่ด้านอื่น ๆ ที่จำเป็นในการให้บริการคลาวด์ เช่น องค์กรความมั่นคงของคลาวด์หรือซีเอสเอ (Cloud Security Alliance) ซึ่งเป็นองค์กรที่เกิดจากการร่วมมือกันระหว่างภาคอุตสาหกรรม บริษัท และสมาคมต่าง ๆ โดยมีวัตถุประสงค์เพื่อสนับสนุนแนวทางปฏิบัติที่ดี สำหรับการสร้างความเชื่อมั่นในด้านต่าง ๆ ของความต้องการที่ไม่ใช่เชิงหน้าที่ในการให้บริการคลาวด์ โดยได้ให้ความสำคัญกับการนำมาตรฐานความมั่นคงที่ถูกนิยามโดยองค์กรที่มีมาตรฐานและเชื่อถือได้ดังต่อไปนี้ มาประยุกต์ใช้กับบริการคลาวด์ [2]

1. ISO (International Organization for Standardization) ได้เสนอมาตรฐานหนึ่งที่มีความสำคัญต่อหลายองค์กร คือ ISO 27001 เพราะปัญหาและความเสี่ยงในเรื่องของการรั่วไหลของข้อมูลที่มีความสำคัญ ทำให้มีปัญหาต่าง ๆ ตามมามากมาย เช่นการเสียเปรียบทางการค้า เป็นต้น ดังนั้น ISO จึงได้ทำการกำหนดมาตรฐานนี้ขึ้นมา เพื่อเป็นแบบจำลองการกำหนดนโยบาย กระบวนการดำเนินการ การบำรุงรักษา และการปรับปรุงระบบจัดการความมั่นคงสารสนเทศ (Information Security Management System: ISMS) ซึ่งมาตรฐานนี้เป็นมาตรฐานที่เน้นไปที่การปฏิบัติ จึงสามารถนำไปอ้างอิงเพื่อใช้ในการประเมินและขอรับการรับรองมาตรฐานต่อไปได้

2. ISACA (Information Systems Audit and Control Association) เป็นองค์กรที่เกิดจากการรวมตัวของกลุ่มบริษัทเอกชนโดยมีความต้องการรวมข้อมูลให้เป็นศูนย์กลาง (Centralized) และให้แนวทางในด้านการควบคุมการตรวจสอบระบบคอมพิวเตอร์ ปัจจุบัน ISACA นำเสนอแนวทางและกรอบด้านต่าง ๆ ในระบบสารสนเทศ เช่น การกำกับดูแลเทคโนโลยีสารสนเทศ การควบคุมและให้ความเชื่อมั่นด้านความมั่นคง ISACA นำเสนอ COBIT (Control Objectives for Information and Related Technology) ซึ่งเป็นกรอบการกำกับดูแลเทคโนโลยีสารสนเทศโดยมีชุดเครื่องมือสำหรับกลุ่มผู้บริหารเพื่อเชื่อมโยงช่องว่างระหว่างการควบคุมความต้องการ ประเด็นทางเทคนิคและความเสี่ยงทางธุรกิจ นอกจากนี้ยังนำเสนอนโยบายและแนวทางปฏิบัติที่ดีสำหรับการควบคุมเทคโนโลยีสารสนเทศเพื่อช่วยเพิ่มมูลค่าทางธุรกิจให้แก่องค์กร

3. Payment Card Industry (PCI) Security Standards Council เป็นฟอรัมเปิดขนาดใหญ่ที่ถูกจัดตั้งขึ้นในปี ค.ศ. 2006 เพื่อวัตถุประสงค์ในการพัฒนา จัดการ ให้ความรู้เกี่ยวกับความมั่นคง โดยได้จัดทำมาตรฐานความมั่นคงที่ชื่อว่า PCI DSS (Payment Card Industry Data

Security Standard) ซึ่งเป็นมาตรฐานที่รวบรวมความต้องการที่ไม่ใช่เชิงหน้าที่ด้านการจัดการความมั่นคง นโยบาย ขั้นตอน สถาปัตยกรรมเครือข่าย การออกแบบซอฟต์แวร์ และความต้องการที่ไม่ใช่เชิงหน้าที่ด้านอื่น ๆเพื่อช่วยให้องค์กรที่มีการเก็บข้อมูล หรือประมวลผลข้อมูลทางบัตรเครดิตสามารถป้องกันการโจรกรรมข้อมูลทางบัตรเครดิต โดยการควบคุมข้อมูลและช่องโหว่ต่าง ๆ ให้มีความรัดกุมมากขึ้น

4. NIST (National Institute of Standards and Technology) เป็นหน่วยงานหนึ่งของกระทรวงพาณิชย์สหรัฐฯ ก่อตั้งในปี ค.ศ. 1901 โดยภารกิจของ NIST คือ การสนับสนุนการพัฒนาและสร้างความสามารถทางอุตสาหกรรมของสหรัฐอเมริกา อีกทั้งยังได้จัดตั้งมาตรฐานในด้านต่าง ๆ รวมถึงมาตรฐานความมั่นคงของคลาวด์ซึ่งมีวัตถุประสงค์เพื่อสร้างมาตรฐานความมั่นคงและนโยบายความเป็นส่วนตัวสำหรับการใช้งานคลาวด์สาธารณะ

5. HIPAA (Health Information Portability and Accountability Act) ซึ่งเป็นองค์กรที่จัดทำนโยบายความเป็นส่วนตัวของข้อมูลผู้ป่วย (Personal Health Information) ได้แก่ ชื่อที่อยู่หมายเลขโทรศัพท์หมายเลขบัตรประชาชนประวัติการเจ็บป่วยผลการตรวจ และข้อมูลอื่น ๆ ที่มีความเกี่ยวข้องกับผู้ป่วย ซึ่งผู้ที่มีส่วนเกี่ยวข้องเท่านั้นที่มีสิทธิดำเนินการกับข้อมูลอย่างเป็นไปตามมาตรฐาน เพื่อป้องกันการรั่วไหลของข้อมูล เช่น การส่งข้อมูลผ่านทางอีเมล ก็จะต้องมีการเข้ารหัสข้อมูล (Encryption) เป็นต้น

จากที่กล่าวมา องค์กรข้างต้นมีวัตถุประสงค์เดียวกันคือ เพื่อสร้างมาตรฐานในการควบคุมกระบวนการของการให้บริการ ให้เป็นไปตามความต้องการที่ไม่ใช่เชิงหน้าที่ด้านต่าง ๆ ทั้งนี้ องค์กรความมั่นคงของคลาวด์หรือซีเอสเอ ได้จัดทำเอกสารเมตริกซ์ควบคุมคลาวด์ (Cloud Controls Matrix) [2] กับการใช้แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน (Consensus Assessments Initiative Questionnaire) [3] ดังตารางที่ 2.1 และ 2.2 เพื่อนำมาใช้ในการประเมินผู้ให้บริการคลาวด์ ทั้งนี้เอกสารเมตริกซ์ควบคุมคลาวด์ ปัจจุบันเป็นเวอร์ชัน 3.0 ซึ่งมีทั้งหมด 16 หมวด แต่ละหมวดแบ่งออกเป็นหมวดย่อย ดังนี้

1. Application & Interface Security
2. Audit Assurance & Compliance
3. Business Continuity Management & Operational Resilience
4. Change Control & Configuration Management
5. Data Security & Information Lifecycle Management
6. Datacenter Security
7. Encryption & Key Management
8. Governance and Risk Management

9. Human Resources
10. Identity & Access Management
11. Infrastructure & Virtualization Security
12. Interoperability & Portability
13. Mobile Security
14. Security Incident Management, E-Discovery & Cloud Forensics
15. Supply Chain Management, Transparency, and Accountability
16. Threat and Vulnerability Management

เอกสารเมตริกซ์ควบคุมคลาวด์จะอธิบายหลักการรักษาความมั่นคง เพื่อให้คำแนะนำแก่ผู้ให้บริการคลาวด์ที่จะให้บริการคลาวด์ที่มีความมั่นคงและช่วยลูกค้าในการประเมินความเสี่ยงด้านความมั่นคงโดยรวมของผู้ให้บริการคลาวด์ ส่วนแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน เป็นเอกสารที่ควบคู่มากับเอกสารเมตริกซ์ควบคุมคลาวด์โดยเป็นกลุ่มของคำถามเกี่ยวกับการปฏิบัติเพื่อให้สอดคล้องกับเอกสารเมตริกซ์ควบคุมคลาวด์ ขณะนี้แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันยังไม่ได้ปรับตามเมตริกซ์ควบคุมคลาวด์เวอร์ชัน 3.0 โดยยังคงเป็นเวอร์ชัน 1.1 อยู่ซึ่งมีทั้งหมด 11 หมวด แต่ยังสามารถใช้งานได้อยู่เพราะเนื้อหาในเมตริกซ์ควบคุมคลาวด์เวอร์ชัน 1.1 ส่วนใหญ่ยังคงอยู่ในเวอร์ชัน 3.0 ในปัจจุบันผู้ให้บริการคลาวด์หลายราย ได้ทำการเผยแพร่รายงานการประเมินตนเอง (Self-Assessment) ลงในคลังข้อมูลของซีเอสเอ ที่มีชื่อว่าสตาร์ (Security, Trust & Assurance Registry (STAR)) [4] เพื่อช่วยให้ผู้ใช้บริการคลาวด์ที่กำลังค้นหาผู้ให้บริการคลาวด์สามารถทำการพิจารณาว่าผู้ให้บริการรายใดได้ปฏิบัติตามมาตรฐานด้านความมั่นคงขององค์กรความมั่นคงของคลาวด์หรือซีเอสเอ โดยใช้การตอบคำถามในแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันในการพิจารณา ดังตัวอย่างในตารางที่ 2.3

ตารางที่ 2.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์

Control Domain	Control ID	Control Specification
Application & Interface Security *Application Security*	AIS-01	Applications and interfaces (APIs) shall be designed, developed, and deployed in accordance with industry acceptable standards and adhere to applicable legal, statutory, or regulatory compliance obligations.

ตารางที่ 2.2 ตัวอย่างของแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

Control Domain	CGID	CID	Consensus Assessment Question
Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?
Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?
		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?
		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?
		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?

ตารางที่ 2.3 ตัวอย่างของการตอบแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

Control Domain	CAIQ Question	Provider's Response
Audit Assurance & Compliance *Audit Planning*	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	The Statement on Auditing Standards No. 70 (SAS 70) is an auditing standard issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) and provides guidance to auditors whom assess the internal controls of a service provider in order to produce an independent audit report. SAS70 has been replaced by the Statements on Standards for Attestation Engagements No. 16 (SSAE16) as of 2011. Acquia has completed its first SSAE16 SOC 1 Type I audit in June, 2012 covering its corporate controls and its Acquia Managed Cloud PaaS platform and will complete its first SOC 1 Type II audit in early 2013 which will cover the last half of the 2012 calendar year. Acquia will continue to conduct annual SSAE16 SOC 1 Type II audits annually going forward. Acquia is happy to provide the audit reports to our customers and prospective customers.
Audit Assurance & Compliance *Independent Audits*	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?	Yes. Acquia utilizes Qualys Web Application Scanning platform to conduct vulnerability scans on Acquia sites as well customer sites on an ad hoc basis. Note that web application vulnerability scans are not inclusive as part of Acquia Cloud service but we do offer ad hoc scans to assist customers as well as a Professional Services security audit.

2.1.2 ออนโทโลจี

ออนโทโลจี (Ontology) [5] คือ แบบจำลองของแนวคิดหรือองค์ความรู้เกี่ยวกับโดเมน (Domain) หนึ่ง ๆ รวมไปถึงความสัมพันธ์ในโดเมนเหล่านั้นด้วย โดยทั่วไปออนโทโลจีจะถูกนำไปใช้ประโยชน์ในการกำหนด ให้นิยาม หรือให้คำจำกัดความของโดเมนนั้น ๆ ออนโทโลจีมีองค์ประกอบ (Components) หลัก ๆ ดังนี้

- อินดิวิดวล (Individuals) เป็นองค์ประกอบพื้นฐานของออนโทโลจี หมายถึงอ็อบเจกต์ (Object) หนึ่ง ๆ ของโดเมน เช่น คน สัตว์ สิ่งของต่างๆ เป็นต้น
- คลาส (Classes) คือกลุ่มของอ็อบเจกต์ที่มีลักษณะประจำร่วมกัน สามารถจัดให้อยู่ภายในคลาสเดียวกันได้
- แอตทริบิวต์ (Attributes) เป็นลักษณะประจำของคลาส ๆ หนึ่ง
- ความสัมพันธ์ (Relationships) หมายถึงความเกี่ยวข้องกันระหว่างอ็อบเจกต์ภายในออนโทโลจี

การอธิบายองค์ความรู้ในรูปของออนโทโลจีที่นิยมในปัจจุบันทำได้โดยการใช้ภาษาออนโทโลจี เช่น ภาษาอาร์ดีเอฟ ภาษาอาร์ดีเอฟสกีมา และภาษาอาวล์ ซึ่งทั้งหมดนี้ ได้ถูกประยุกต์มาจากภาษาเอกซ์เอ็มแอล (XML) ที่มีการกำหนดความหมายไว้เป็นอย่างดี การพัฒนาออนโทโลจีประกอบไปด้วย 6 ขั้นตอนดังนี้

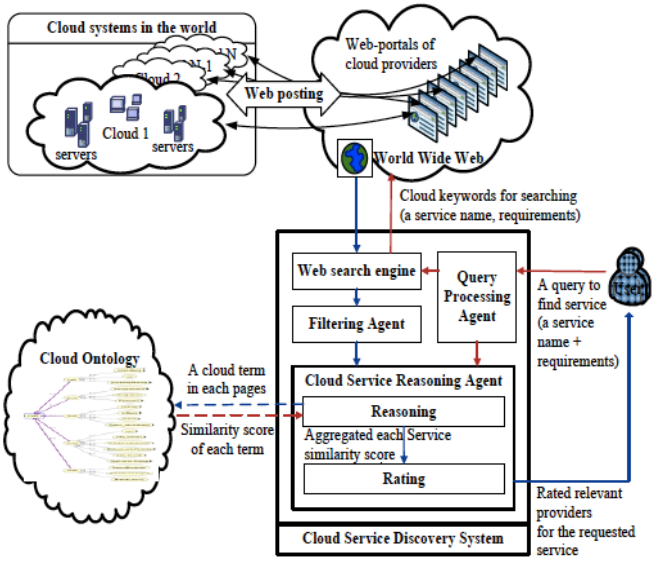
1. การตรวจสอบและกำหนดขอบเขตของโดเมน
2. การพิจารณาการนำกลับมาใช้ใหม่ของออนโทโลจีที่มีอยู่
3. การแจกแจงเทอมต่าง ๆ ในออนโทโลจี
4. การกำหนดคลาส
5. การกำหนดความสัมพันธ์
6. การสร้างอินสแตนซ์

2.2 เอกสารและงานวิจัยที่เกี่ยวข้อง

2.2.1 An Ontology-Enhanced Cloud Service Discovery System [6]

งานวิจัยนี้ได้นำเสนอเครื่องมือที่ชื่อว่า “Cloud Service Discovery System” หรือที่เรียกว่าระบบ CSDS ดังภาพที่ 2.1 โดยมีจุดมุ่งหมายเพื่อช่วยให้ผู้ใช้บริการคลาวด์สามารถค้นหาบริการคลาวด์ที่ตรงกับความต้องการของผู้ใช้บริการคลาวด์มากที่สุด โดยงานวิจัยนี้ได้ทำการออกแบบและพัฒนาออนโทโลจีของคลาวด์ ซึ่งประกอบไปด้วยหมวดหมู่ และขอบเขตเชิงหน้าที่ตามหลักการของระบบคลาวด์ เช่น การแบ่งหมวดหมู่เป็น IaaS, PaaS และ SaaS และคุณสมบัติของบริการในแต่ละหมวดหมู่ ได้แก่ โดเมนของบริการ ทรัพยากร สภาพแวดล้อมการให้บริการ เป็นต้น เพื่อที่จะช่วยในการหาความสัมพันธ์ระหว่างบริการคลาวด์ได้

เมื่อผู้ใช้ทำการค้นหาบริการคลาวด์โดยระบุความต้องการเชิงหน้าที่ที่ผู้ใช้ต้องการ ระบบ CSDS จะให้ผลลัพธ์ที่ใกล้เคียงกับความต้องการของผู้ใช้มากที่สุดและผลลัพธ์ที่แนะนำจะมีการจัดลำดับมาให้ผู้ใช้พิจารณาเลือกด้วย



ภาพที่ 2.1 ระบบ CSDS

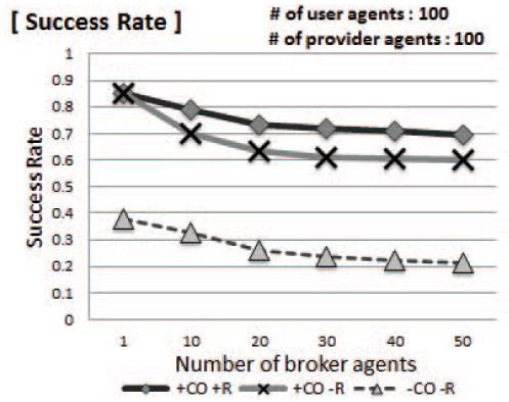
2.2.2 Toward Agents and Ontology for Cloud Service Discovery [7]

งานวิจัยนี้เป็นงานต่อเนื่องจาก [6] โดยได้นำเสนอระบบการค้นหาผู้ให้บริการคลาวด์แบบ Agent-Based และโพรโทคอลสำหรับการติดต่อสื่อสารระหว่าง Agent ซึ่งเรียกว่า “Agent-Based Cloud Service Discovery Protocol” งานวิจัยได้นำออนโทโลจีซึ่งประกอบไปด้วยหมวดหมู่และขอบเขตเชิงหน้าที่ตามหลักการของระบบคลาวด์มาประยุกต์ใช้เพื่อการค้นหาเชิงความหมาย ระบบ Agent-Based นี้ประกอบไปด้วย Agent 3 ประเภทคือ User Agent, Provider Agent และ Broker Agent โดยที่ Broker Agent มีขั้นตอนการทำงาน 4 ขั้นตอนดังนี้

1. Selection Stage ในขั้นตอนนี้ Broker Agent จะทำการเปรียบเทียบระหว่างความต้องการของผู้ใช้บริการซึ่งติดต่อผ่าน User Agent กับคำโฆษณาของผู้ให้บริการซึ่งติดต่อผ่าน Provider Agent เพื่อทำการคัดผู้ให้บริการที่ไม่มีความสามารถตรงตามความต้องการขั้นต่ำของผู้ใช้บริการออก
2. Evaluation Stage ในขั้นตอนนี้จะทำการจัดลำดับผู้ให้บริการโดยพิจารณาความคล้ายคลึง (Similarity Reasoning) ระหว่างความสามารถเชิงหน้าที่ของผู้ให้บริการกับความต้องการของผู้ใช้บริการ และพิจารณาราคาและเวลาของการให้บริการ (Price and Timeslot Utilities Matching)

3. Filtering Stage ในขั้นตอนนี้ได้ทำการคัดผู้ให้บริการที่มีคะแนนต่ำกว่าค่าที่ได้ตั้งไว้ออก
4. Recommendation Stage หากไม่มีผู้ให้บริการที่ตรงกับความต้องการของผู้ใช้บริการเลย Broker Agent จะทำการค้นหา Broker Agent อื่นซึ่งน่าจะมีข้อมูลผู้ให้บริการรายอื่นอยู่ และแนะนำผู้ใช้บริการให้ติดต่อ Broker Agent รายอื่นนั้นต่อไป

ผลลัพธ์ของงานวิจัยนี้กล่าวว่าเมื่อ Broker Agent ได้ใช้ออนโทโลจีของคลาวด์ด้วย จะมีประสิทธิภาพในการค้นหาบริการคลาวด์ที่เหมาะสมมากกว่าเมื่อ Broker Agent ไม่ได้ใช้ออนโทโลจีของคลาวด์ ดังภาพที่ 2.2 อย่างไรก็ตามออนโทโลจีที่ใช้ยังกล่าวถึงเฉพาะความสามารถเชิงหน้าที่ของผู้ให้บริการคลาวด์เป็นหลัก



ภาพที่ 2.2 ผลลัพธ์จากการใช้ออนโทโลจีของคลาวด์ในการค้นหา

2.2.3 An Ontology-Based System for Cloud Infrastructure Service' Discovery [8]

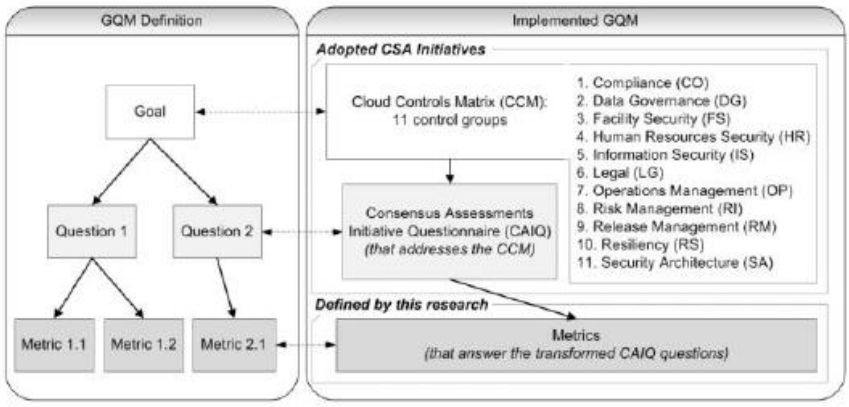
งานวิจัยนี้ได้นำเสนอออนโทโลจีเพื่อที่จะอธิบายข้อมูลความสามารถเชิงหน้าที่และไม่ใช่เชิงหน้าที่ของ IaaS Services โดยไม่พิจารณา PaaS และ SaaS ออนโทโลจีนี้อธิบายลักษณะของการให้บริการในหมวดหมู่ Compute, Storage และ Network และอธิบายคุณสมบัติเชิงหน้าที่ เช่น ข้อมูลทรัพยากร ข้อกำหนดโครงแบบ (Configuration) และคุณสมบัติที่ไม่ใช่เชิงหน้าที่ เช่น ชื่อผู้ให้บริการ ราคา คิวโอเอส (QoS) ด้านสมรรถนะ นอกจากนี้งานวิจัยนี้ได้นำออนโทโลจีที่ได้สร้างขึ้นไปประยุกต์ใช้กับระบบที่เรียกว่า CloudRecommender เพื่อใช้ในการแนะนำบริการคลาวด์ประเภท IaaS Services แต่ในงานวิจัยนี้จะทำการสร้างอินสแตนซ์โดยเก็บข้อมูลลงใน MySQL และใช้คำสั่ง SQL ในการจับคู่ระหว่างคำค้นข้อมูลและคำอธิบายบริการ (Service Description) จึงยังไม่ใช่การค้นหาเชิงความหมาย อีกทั้งยังไม่ครอบคลุมประเด็นด้านความมั่นคง

2.2.4 Semantic Security Policy Matching in Service Oriented Architectures [9]

งานวิจัยนี้ได้นำเสนอวิธีการจับคู่เชิงความหมายระหว่างนโยบายความมั่นคง (Security Policy) ของผู้ให้บริการเว็บเซอร์วิซกับนโยบายความมั่นคงของผู้ใช้บริการ นโยบายความมั่นคงจะถูกกำหนดโดยใช้ออนโทโลจีนโยบาย (Policy Ontology) ซึ่งระบุความต้องการและความสามารถด้านความมั่นคง โดยอ้างอิงออนโทโลจีความมั่นคง (Security Ontology) อีกต่อหนึ่ง ออนโทโลจีความมั่นคงจะกำหนดคอนเซปต์โดยทั่วไป เช่น Objective, Algorithm, Protocol และ Credential แบบต่าง ๆ ในโดเมนความมั่นคง นโยบายความมั่นคงที่ได้จะเป็นเอกสารที่ถูกอ้างถึงผ่านการใช้งาน WS-Policy ซึ่งกำหนดแท็กมาตรฐานที่ใช้ในการระบุนโยบายใด ๆ ที่เกี่ยวข้องกับเว็บเซอร์วิซในการจับคู่เชิงความหมาย งานวิจัยนี้จะใช้การจับคู่ 4 แบบ ได้แก่ Perfect Match, Close Match, Possible Match และ No Match

2.2.5 An Assessment of Security Requirements Compliance of Cloud Providers [10]

งานวิจัยนี้ได้นำเสนอวิธีการประเมินผู้ให้บริการคลาวด์ โดยใช้วิธีเป้าหมาย คำถาม ตัววัด (Goal Question Metric) หรือจีคิวเอ็ม เพื่อนำเสนอแบบจำลองการคำนวณแบบถ่วงน้ำหนักสำหรับประเมินผู้ให้บริการคลาวด์ในด้านการปฏิบัติตามความต้องการด้านความมั่นคง โดยที่เป้าหมายด้านความมั่นคงและคำถามที่สะท้อนถึงการบรรลุเป้าหมายนั้นนำมาจากเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันซึ่งได้กำหนดไว้โดยองค์กรความมั่นคงของคลาวด์ โดยที่แบบสอบถามนั้นจะถูกแปลงเป็นคำถามที่ละเอียดขึ้นเพื่อให้สามารถกำหนดตัววัดเชิงปริมาณสำหรับที่จะตอบคำถามเหล่านั้นได้ ดังภาพที่ 2.3 ตัววัดจะอยู่ในรูปของหลักฐานการปฏิบัติตามความต้องการด้านความมั่นคงซึ่งแบ่งออกเป็น Product และ Activity ที่ปฏิบัติตามความต้องการนั้น ๆ



ภาพที่ 2.3 ความสัมพันธ์ของเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันกับวิธีจีคิวเอ็ม

2.2.6 Matchmaking and Ranking of Semantic Web Services Using Integrated Service Profile [11]

งานวิจัยนี้นำเสนอแบบจำลองคำอธิบายเว็บเซอร์วิซเชิงความหมายเรียกว่า เซอร์วิซโปรไฟล์รวม (Integrated Service Profile) ซึ่งอธิบายความสามารถในการให้บริการของเซอร์วิซในรูปของโครงสร้างการให้บริการ พฤติกรรมของเซอร์วิซแบบมีกฎ รวมไปถึงคุณลักษณะอย่างง่ายและคุณลักษณะเชิงความหมายของเซอร์วิซ และนำเสนออัลกอริทึมในการจับคู่บริการกับความต้องการของผู้ใช้บริการ โดยผลการค้นหาและจับคู่นั้นนำมาจัดลำดับ (Ranking) ความใกล้เคียงกับความต้องการด้วย โดยเซอร์วิซโปรไฟล์รวมประกอบด้วย 2 ส่วนคือ

1. สารสนเทศเชิงแอตทริบิวต์ (Attribute-Based Information) คือ กลุ่มของแอตทริบิวต์ที่ใช้อธิบายเว็บเซอร์วิซที่สนใจซึ่งเป็นข้อมูลอย่างง่าย เช่น ข้อมูลผู้ให้บริการ
2. สารสนเทศเชิงความสามารถ (Capability-Based Information) คือ ลักษณะของเว็บเซอร์วิซที่ซับซ้อนขึ้น โดยแบ่งออกเป็น 3 แอตทริบิวต์ ดังนี้
   - โครงสร้างของบริการ (Service Structure) แสดงโครงสร้างความรู้ (Knowledge Structure) ของเว็บเซอร์วิซ ซึ่งผู้ใช้บริการคาดว่าจะรู้ก่อนการตัดสินใจใช้บริการ เช่น ผลิตภัณฑ์ของบริการ รายละเอียดการขาย และการส่งของ
   - พฤติกรรมของบริการ (Service Behaviour) แสดงสารสนเทศที่เกี่ยวกับพฤติกรรมของเว็บเซอร์วิซ เช่น ต้องการข้อมูลเข้าบางอย่างเพื่อสั่งซื้อสินค้า
   - เงื่อนไขของบริการ (Service Constraint) แสดงเงื่อนไขของบริการในรูปของกฎ

อัลกอริทึมที่ใช้ในการจับคู่นั้น จะพิจารณาระหว่างเซอร์วิซโปรไฟล์รวมกับข้อคำถาม (Query) ของผู้ใช้บริการ โดยจะมีการจับคู่ทั้งหมดเป็น 6 แบบได้แก่

- การจับคู่คอนเซปต์เชิงความหมาย (Matching Ontological Concepts)
- การจับคู่เงื่อนไขเชิงตัวเลข (Matching Numerical Constraints)
- การจับคู่กลุ่มของค่าเชิงความหมาย (Matching Sets of Ontological Values)
- การจับคู่เงื่อนไขของบริการ (Matching Service Constraints)
- การจับคู่โปรไฟล์พฤติกรรม (Matching Behaviour Profiles)
- การจับคู่แอตทริบิวต์อย่างง่าย (Matching Simple Attributes)

จากเอกสารงานวิจัยที่เกี่ยวข้อง สามารถสรุปได้ดังตารางที่ 2.4

ตารางที่ 2.4 สรุปเอกสารงานวิจัยที่เกี่ยวข้อง

หัวข้อวิจัย	ประเด็นงานวิจัย	แนวคิดงานวิจัย	ความแตกต่างจากงานของผู้วิจัย
An Ontology-Enhanced Cloud Service Discovery System [6]	สามารถช่วยให้ผู้ใช้บริการคลาวด์สามารถค้นหาบริการคลาวด์ที่ตรงกับความต้องการของผู้ใช้บริการคลาวด์มากที่สุด	ออกแบบและพัฒนาออนโทโลจีของคลาวด์ซึ่งประกอบไปด้วยหมวดหมู่ และขอบเขตเชิงหน้าที่ตามหลักการของระบบคลาวด์ เช่น การแบ่งหมวดหมู่เป็น IaaS, PaaSและ SaaS	ระบบพิจารณาเฉพาะความต้องการเชิงหน้าที่ของระบบคลาวด์
Toward Agents and Ontology for Cloud Service Discovery [7]	เป็นงานวิจัยต่อจากงานวิจัยก่อนหน้า	นำออนโทโลจีซึ่งประกอบไปด้วยหมวดหมู่และขอบเขตเชิงหน้าที่ตามหลักการของระบบคลาวด์มาประยุกต์ใช้เพื่อการค้นหาเชิงความหมายโดยใช้ระบบ Agent-Based ซึ่งประกอบไปด้วย Agent 3 ประเภท คือ User Agent, Provider Agent และ Broker Agent	ระบบยังคงพิจารณาเฉพาะความต้องการเชิงหน้าที่ของระบบคลาวด์อยู่

ตารางที่ 2.4 สรุปเอกสารงานวิจัยที่เกี่ยวข้อง (ต่อ)

หัวข้อวิจัย	ประเด็นงานวิจัย	แนวคิดงานวิจัย	ความแตกต่างจากงานของผู้วิจัย
An Ontology-Based System for Cloud Infrastructure Service' Discovery [8]	สร้างระบบที่แนะนำบริการคลาวด์ประเภท IaaS Services	สร้างออนโทโลจีเพื่อที่จะอธิบายข้อมูลความสามารถเชิงหน้าที่และไม่ใช่เชิงหน้าที่ของ IaaS Services โดยไม่พิจารณา PaaSและ SaaS	สร้างอินสแตนซ์โดยเก็บข้อมูลลงใน MySQL และใช้คำสั่ง SQL ในการจับคู่ระหว่างคำค้นข้อมูลและคำอธิบายบริการ (Service Description)
Semantic Security Policy Matching in Service Oriented Architectures [9]	นำเสนอวิธีการจับคู่เชิงความหมายระหว่างนโยบายความมั่นคง	นำเสนอวิธีการจับคู่เชิงความหมายระหว่างนโยบายความมั่นคง (Security Policy) ของผู้ให้บริการเว็บเซอร์วิซกับนโยบายความมั่นคงของผู้ใช้บริการ	ออนโทโลจีความมั่นคงจะกำหนดคอนเซปต์ทั่วไป
An Assessment of Security Requirements Compliance of Cloud Providers [10]	ประเมินผู้ให้บริการคลาวด์ โดยใช้วิธีจีคิวเอ็ม (Goal Question Metric)	การประเมินด้านความมั่นคงโดยมีการให้คะแนนหลักฐาน ซึ่งพิจารณาจากคุณภาพและปริมาณของหลักฐาน	ไม่ได้นำเสนอระบบการค้นหาผู้ให้บริการคลาวด์ที่สอดคล้องกับเมตริกซ์ควบคุมคลาวด์แบบเชิงความหมาย
Matchmaking and Ranking of Semantic Web Services Using Integrated Service Profile [11]	นำเสนอแบบจำลองคำอธิบายเว็บเซอร์วิซเชิงความหมาย	สร้างเซอร์วิซโปรไฟล์รวม และนำเสนออัลกอริทึมในการจับคู่บริการกับความต้องการของผู้ใช้บริการ	เซอร์วิซโปรไฟล์ใช้สำหรับเว็บเซอร์วิสและไม่ได้พิจารณาด้านความมั่นคง

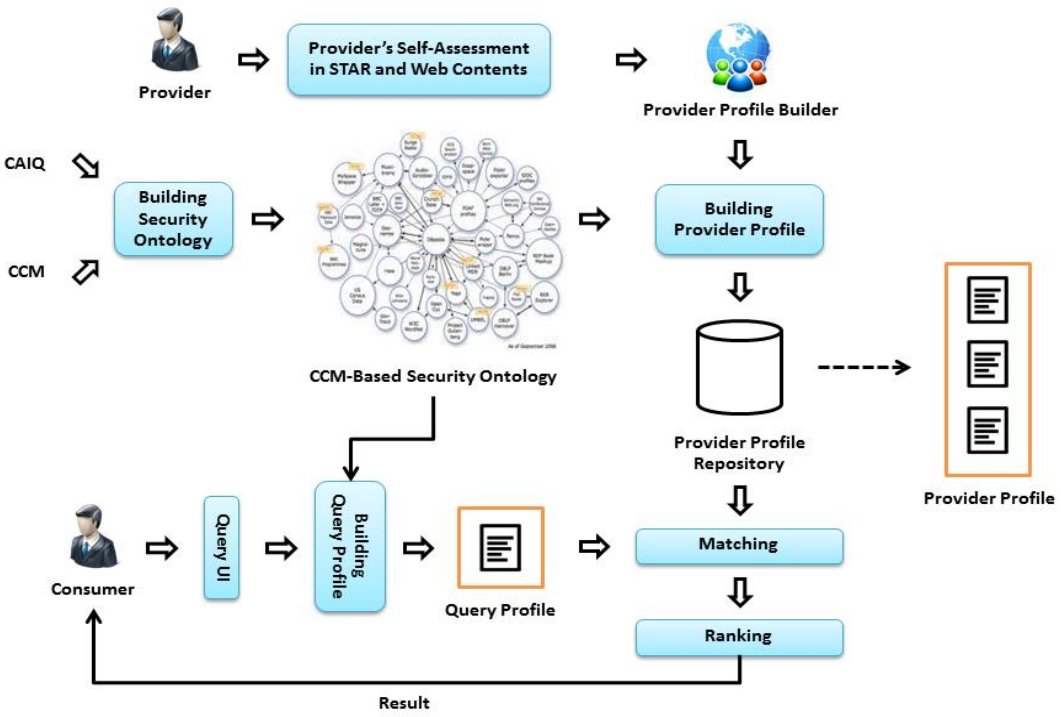
โดยงานวิจัย An Ontology-Enhanced Cloud Service Discovery System [6] ผู้วิจัยเห็นว่า แนวคิดของงานวิจัยชิ้นนี้สามารถเป็นแนวทางในการสร้างเครื่องมือการค้นหาผู้ให้บริการคลาวด์ ที่ตรงกับความต้องการของผู้ใช้บริการคลาวด์ แต่ผู้วิจัยจะพิจารณาเฉพาะความต้องการที่ไม่ใช่เชิงหน้าที่ด้านความมั่นคงของผู้ให้บริการคลาวด์ตามเมตริกซ์ควบคุมคลาวด์ โดยใช้หลักการออนโทโลจี มาเป็นแนวทางในการพัฒนา ทั้งนี้ผู้วิจัยจะใช้แนวคิดการออกแบบนโยบายความมั่นคงจากงานวิจัย Semantic Security Policy Matching in Service Oriented Architectures [9] มาใช้ในการออกแบบโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ รวมทั้งใช้แนวทางเกี่ยวกับการจับคู่ ส่วนออนโทโลจีด้านความมั่นคงที่จะเสนอนั้นจะอิงแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ แทนการกำหนดองค์ความรู้ด้านความมั่นคงโดยทั่วไป และทำการประยุกต์ใช้เมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันดังงานวิจัย An Assessment of Security Requirements Compliance of Cloud Providers [10] นำมาประยุกต์กับออนโทโลจี โดยนำมาสร้างองค์ความรู้ทางด้านความมั่นคงของคลาวด์ เพื่อใช้ในการค้นหาเชิงความหมาย โดยข้อมูลของผู้ให้บริการคลาวด์จะพิจารณาจากข้อมูลที่เปิดเผยบนหน้าเว็บ และคลังข้อมูลสตาร์ของซีเอสเอ (Security, Trust & Assurance Registry (STAR)) [4] เพื่อนำข้อมูลการตอบคำถามในแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันในการพิจารณาคำศัพท์ในการสร้างออนโทโลจี ทั้งนี้ยังใช้แนวทางการสร้างโปรไฟล์ของผู้ให้บริการและอัลกอริทึมการจับคู่คอนเซปต์เชิงความหมาย จากงานวิจัย Matchmaking and Ranking of Semantic Web Services Using Integrated Service Profile [11] มาใช้ในการสร้างโปรไฟล์ด้านความมั่นคงของผู้ให้บริการคลาวด์และพิจารณาการจับคู่ระหว่างโปรไฟล์ของผู้ให้บริการคลาวด์กับข้อคำถามที่ผู้วิจัยสร้างขึ้นได้

สรุปได้ว่าการค้นหาบริการคลาวด์ส่วนมากจะเป็นการค้นหาบริการคลาวด์ เฉพาะความต้องการเชิงหน้าที่ของระบบคลาวด์ โดยที่ยังไม่พิจารณาความต้องการที่ไม่ใช่เชิงหน้าที่ ออนโทโลจีที่ใช้ส่วนมากเป็นออนโทโลจีความมั่นคงที่มีคอนเซปต์ทั่วไป เช่น IaaS, PaaS และ SaaS แต่ก็ยังไม่ได้พิจารณาความต้องการเชิงหน้าที่ด้านความมั่นคง ซึ่งเป็นเรื่องที่มีความสำคัญต่อองค์กรเป็นอย่างยิ่ง ทั้งนี้การค้นหาเชิงความหมายจะใช้คอนเซปต์ของการจับคู่เชิงความหมายเพื่อช่วยในการเปรียบเทียบคำศัพท์

บทที่ 3
การค้นหาผู้ให้บริการคลาวด์เชิงความหมายโดยอิงออนโทโลจีความมั่นคงของคลาวด์

งานวิจัยนี้เสนอวิธีการค้นหาผู้ให้บริการคลาวด์ที่ตรงตามมาตรฐานด้านความมั่นคงของคลาวด์ พร้อมทั้งระบบต้นแบบสำหรับช่วยในการค้นหา ภาพรวมของงานวิจัยเป็นดังภาพที่ 3.1 โดยมีส่วนประกอบหลักเป็นออนโทโลจีด้านความมั่นคงโดยอิงกับเอกสารเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน โปรไฟล์ของผู้ให้บริการคลาวด์ โปรไฟล์ข้อคำถาม การจับคู่ความหมาย และการจัดลำดับ รายละเอียดของวิธีการดำเนินการวิจัยมีขั้นตอนอยู่ 7 ขั้นตอน คือ

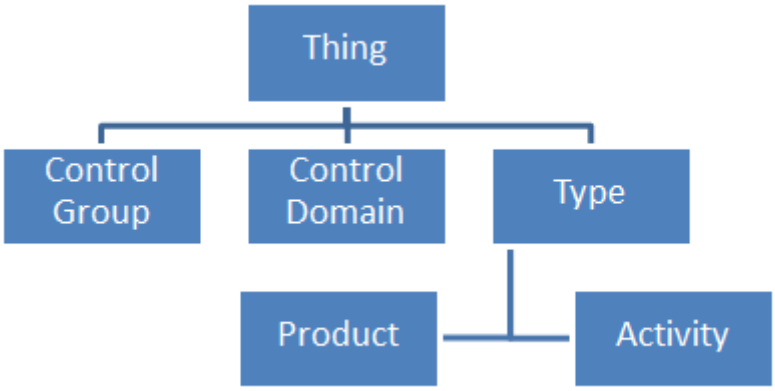
1) ขั้นตอนการพัฒนาออนโทโลจีความมั่นคงของคลาวด์ที่อิงมาตรฐานซีเอสเอ
2) ขั้นตอนการพัฒนาโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์
3) ขั้นตอนการพัฒนาโปรไฟล์ข้อคำถาม
4) ขั้นตอนการจับคู่เชิงความหมาย
5) ขั้นตอนการจัดลำดับของการจับคู่เชิงความหมาย
6) ขั้นตอนการพัฒนาต้นแบบของระบบค้นหาผู้ให้บริการคลาวด์
7) ขั้นตอนการทดสอบ



ภาพที่ 3.1 ภาพรวมของระบบค้นหาผู้ให้บริการคลาวด์

3.1 ขั้นตอนการพัฒนาออนโทโลจีความมั่นคงของคลาวด์ที่อิงมาตรฐานซีเอสเอ

ผู้วิจัยได้ใช้เอกสารเมตริกซ์ควบคุมคลาวด์ (Cloud Controls Matrix) [2] เป็นหลัก และใช้แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน (Consensus Assessments Initiative Questionnaire) [3] เป็นส่วนเสริม เพื่อมาทำการวิเคราะห์ว่าเนื้อหาส่วนใดในเอกสารที่สำคัญ จากนั้นนำมาสร้างความสัมพันธ์ระหว่างคำศัพท์ในเอกสารให้อยู่ในรูปของออนโทโลจีภาษาอาวล์ด้วยโปรแกรม Protégé Editor โดยจะมีโครงสร้างออนโทโลจี ดังภาพที่ 3.2 และคำอธิบายดังตารางที่ 3.1

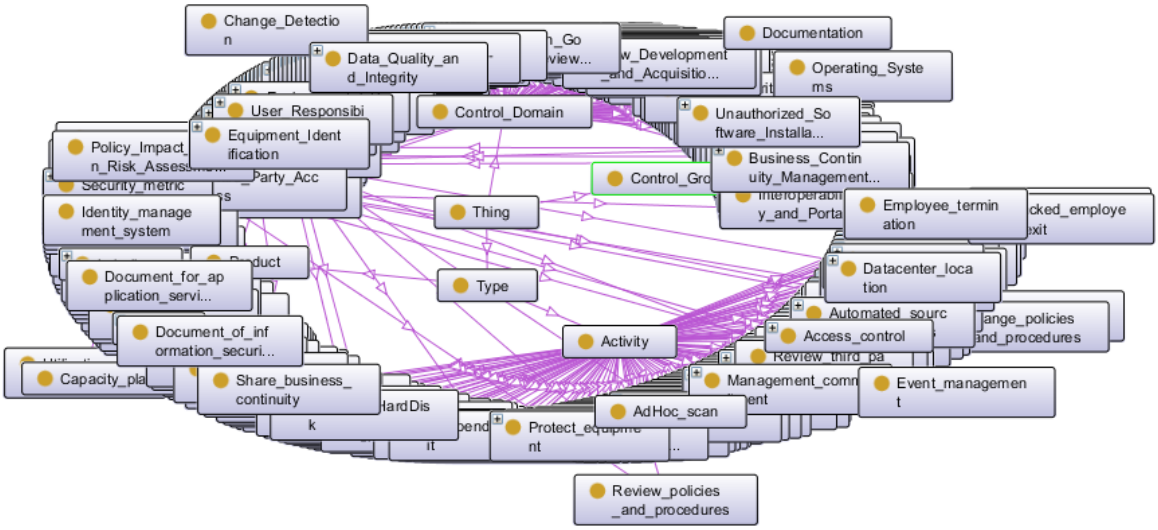


ภาพที่ 3.2 โครงสร้างออนโทโลจี

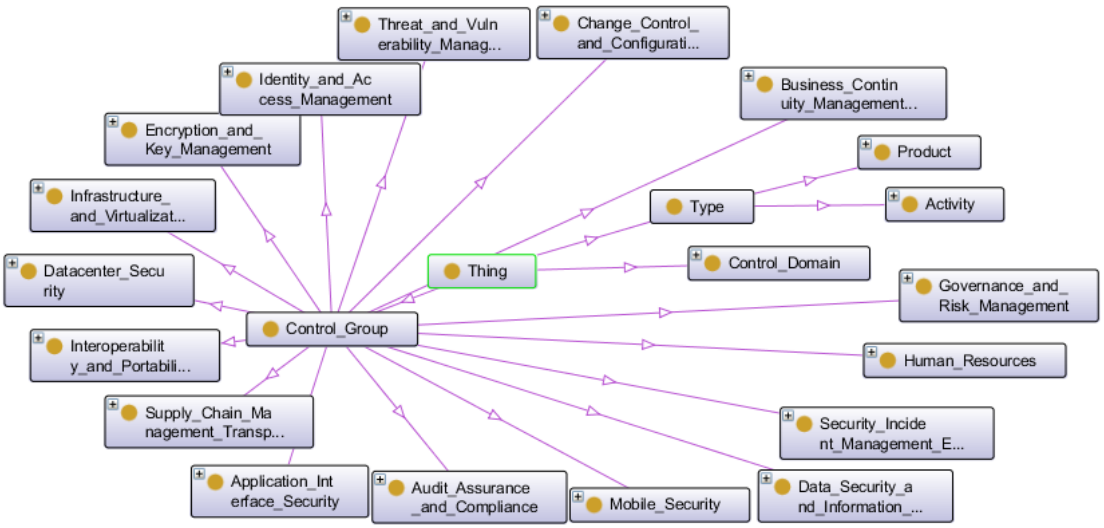
ตารางที่ 3.1 คำอธิบายคำศัพท์โครงสร้างออนโทโลจี

คำศัพท์	ความหมาย
Thing	คำศัพท์ที่จะนำมาสร้างออนโทโลจี
Control Group	แนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์
Control Domain	หมวดย่อยของแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์
Type	ประเภทของคำ ซึ่งสามารถแบ่งเป็น Activity, Product
Activity	กิจกรรมที่แนวการปฏิบัติด้านหนึ่ง ๆ ระบุให้กระทำ
Product	สิ่งที่เป็นผลผลิตจากการดำเนินการตามแนวปฏิบัติด้านหนึ่ง ๆ

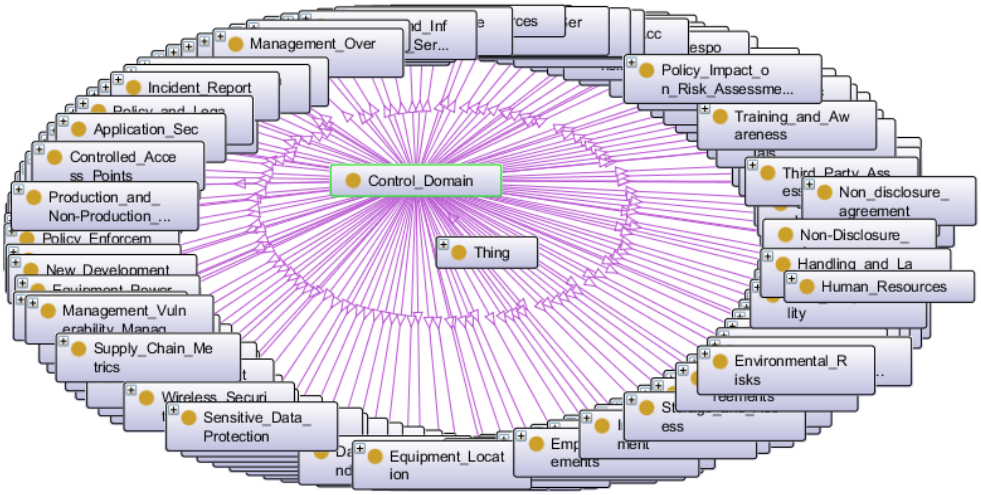
ตัวอย่างภาพรวมของออนโทโลจีความมั่นคงของคลาวด์แสดงในภาพที่ 3.3 ซึ่งประกอบด้วยคำศัพท์ที่เกี่ยวกับ Control Group, Control Domain และ Type รวม 396 คำ ภาพที่ 3.4 แสดงตัวอย่างออนโทโลจีในส่วนของ Control Group รวม 16 คำ ภาพที่ 3.5 แสดงตัวอย่างออนโทโลจีในส่วนของ Control Domain รวม 131 คำ ภาพที่ 3.6 แสดงตัวอย่างออนโทโลจีในส่วนของ Activity รวม 167 คำ ภาพที่ 3.7 แสดงตัวอย่างออนโทโลจีในส่วนของ Product รวม 82 คำ สำหรับคำศัพท์ในออนโทโลจีทั้งหมดแสดงไว้ในภาคผนวก ก และ ข



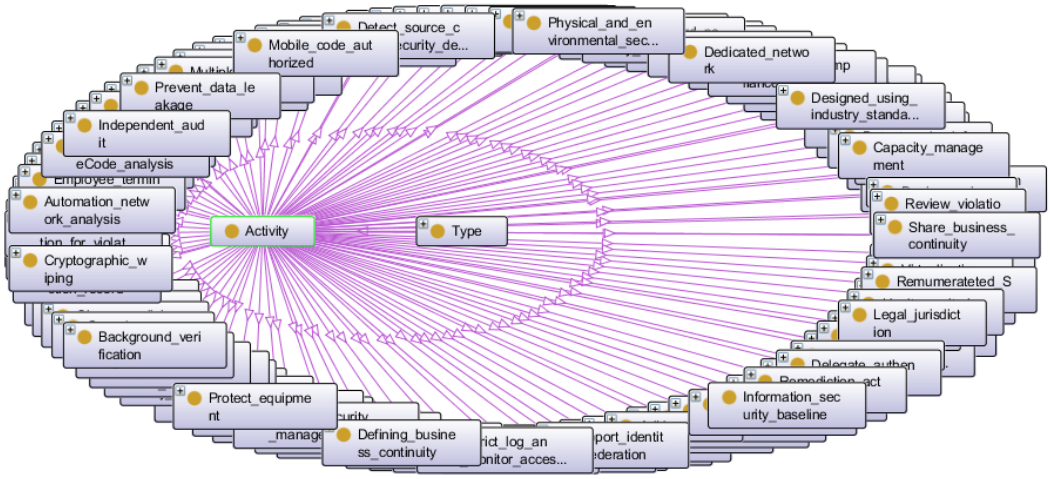
ภาพที่ 3.3 ภาพรวมของออนโทโลจี



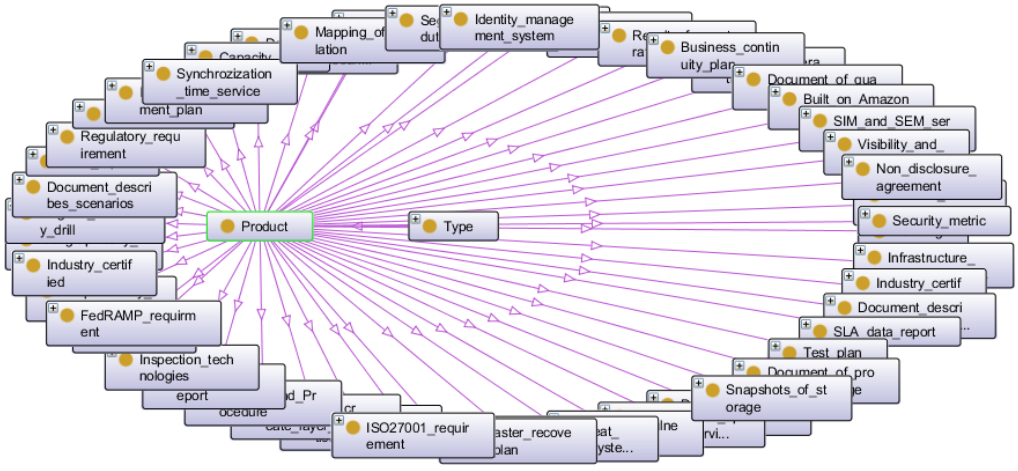
ภาพที่ 3.4 ออนโทโลจีในส่วนของ Control Group



ภาพที่ 3.5 ออนโทโลจีในส่วนของ Control Domain



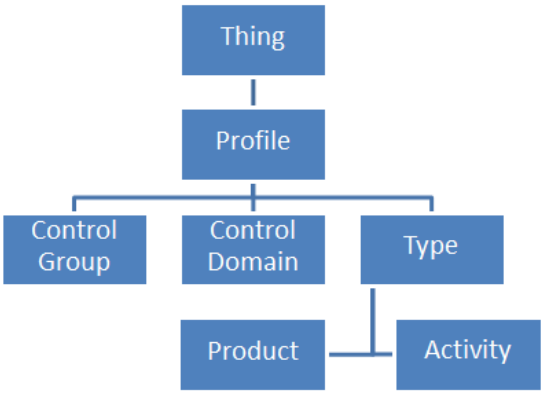
ภาพที่ 3.6 ออนโทโลจีในส่วนของ Activity



ภาพที่ 3.7 ออนโทโลจีในส่วนของ Product

3.2 ขั้นตอนการพัฒนาโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์

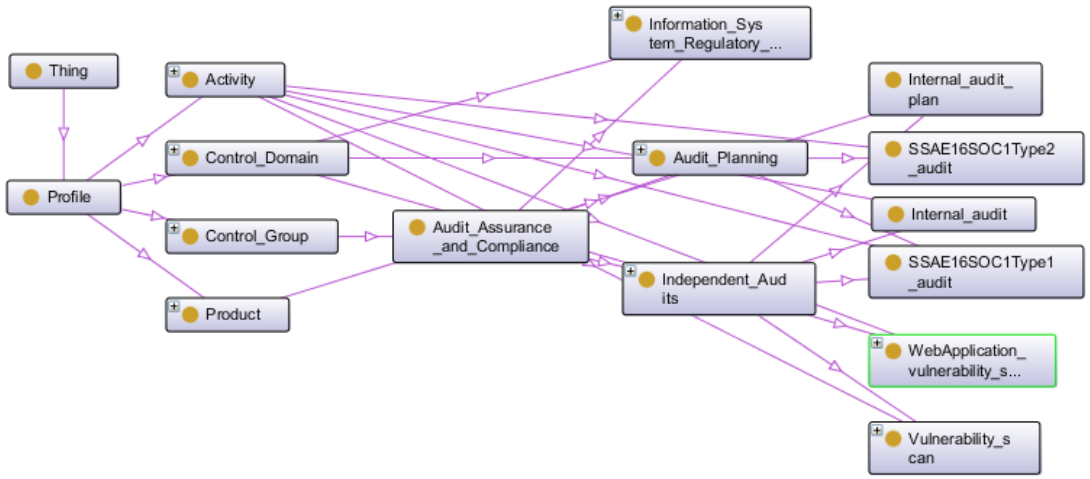
ผู้วิจัยจะนำเอาออนโทโลจีที่ได้ทำการสร้างไว้จากขั้นตอนที่ 3.1 มาใช้เป็นออนโทโลจีหลักเพื่อนำมาสร้างออนโทโลจีสำหรับโปรไฟล์ความมั่นคงเชิงความหมายของผู้ให้บริการคลาวด์แต่ละรายให้สามารถนำไปใช้ได้ โดยนำมาสร้างความสัมพันธ์ระหว่างคำศัพท์ในเอกสารให้อยู่ในรูปของออนโทโลจีภาษาอาวล์ด้วยโปรแกรมที่พัฒนาขึ้นมาเพื่อช่วยในการสร้างโปรไฟล์ความมั่นคงเชิงความหมายของผู้ให้บริการคลาวด์ ซึ่งโปรไฟล์ความมั่นคงเชิงความหมายของผู้ให้บริการคลาวด์ จะมีโครงสร้างคล้ายกับออนโทโลจีความมั่นคงของคลาวด์ ดังตัวอย่างในภาพที่ 3.8 และคำอธิบายดังตารางที่ 3.2



ภาพที่ 3.8 โครงสร้างโปรไฟล์ความมั่นคงเชิงความหมายของผู้ให้บริการคลาวด์

ตารางที่ 3.2 คำอธิบายคำศัพท์โครงสร้างโปรไฟล์ความมั่นคงเชิงความหมายของผู้ให้บริการคลาวด์

คำศัพท์	ความหมาย
Thing	คำศัพท์ที่จะนำมาสร้างออนโทโลจี
Profile	เอกสารอาวล์ประเภทโปรไฟล์
Control Group	แนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ที่ผู้ให้บริการทำตาม
Control Domain	หมวดย่อยของแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ที่ผู้ให้บริการทำตาม
Type	ประเภทของคำ ซึ่งสามารถแบ่งเป็น Activity, Product
Activity	กิจกรรมตามแนวการปฏิบัติด้านหนึ่ง ๆ ที่ผู้ให้บริการทำตาม
Product	สิ่งที่เป็นผลผลิตจากการที่ผู้ให้บริการดำเนินการตามแนวปฏิบัติด้านหนึ่ง ๆ



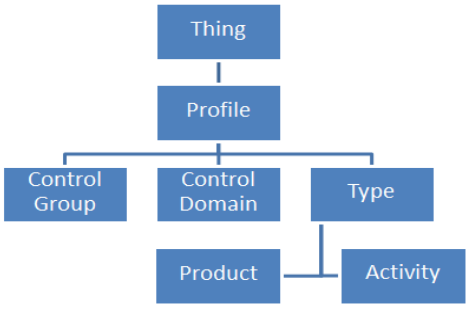
ภาพที่ 3.9 ตัวอย่างโปรไฟล์ของผู้ให้บริการคลาวด์เฉพาะส่วน Audit Assurance and Compliance

จากภาพที่ 3.9 เป็นตัวอย่างโปรไฟล์เชิงความหมายของผู้ให้บริการคลาวด์ที่ชื่อว่า Acquia โดยมีรายละเอียดคือ ผู้ให้บริการที่ชื่อว่า Acquia ได้ทำการปฏิบัติตามมาตรฐานของเมตริกซ์ควบคุมคลาวด์ในหมวดที่ชื่อว่า Audit Assurance and Compliance ซึ่งในส่วนนี้ Acquia ได้ปฏิบัติตามหมวดย่อย Audit Planning โดยมีกิจกรรมที่ดำเนินการคือ Internal audit และมีผลผลิตที่ได้คือเอกสาร SSAE16SOC1Type2 Audit นอกจากนี้ Acquia ยังได้ทำตามหมวดย่อย Information System Regulatory Mapping และ Independent Audits และมีกิจกรรมและผลผลิตอื่น จากหมวดย่อยเหล่านี้ด้วย ในการสร้างโปรไฟล์ของผู้ให้บริการคลาวด์นั้น ผู้วิจัยได้พิจารณาข้อมูลจากหน้าเว็บร่วมกับข้อมูลการประเมินตนเองของผู้ให้บริการคลาวด์ ตามแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันเวอร์ชัน 1.1 ซึ่งเก็บอยู่ในสตาร์ ดังนั้นเวลาสร้างโปรไฟล์ของผู้ให้บริการคลาวด์ ผู้วิจัยจะทำการเชื่อมโยง Control Domain ตามข้อมูลเวอร์ชัน 1.1 ในสตาร์ เข้ากับ Control Domain ของออนโทโลจีความมั่นคงของคลาวด์ ซึ่งเป็นเวอร์ชัน 3.0 ด้วย

3.3 ขั้นตอนการพัฒนาโปรไฟล์ข้อคำถาม

ในส่วนนี้ผู้วิจัยจะนำเอาออนโทโลจีที่ได้ทำการสร้างไว้จากขั้นตอนที่ 3.1 มาช่วยในการสร้างโปรไฟล์ข้อคำถาม โดยที่ผู้ใช้บริการจะทำการค้นหาข้อมูลที่ต้องการผ่านทางส่วนต่อประสานผู้ใช้ (User Interface) ที่ได้จัดทำไว้ให้ การค้นหาที่สามารถทำได้ ได้แก่ ค้นหาว่าผู้ให้บริการคลาวด์รายใดได้ปฏิบัติตามเมตริกซ์ควบคุมคลาวด์ในด้านใดบ้าง ค้นหาว่าผู้ให้บริการคลาวด์รายใด มีหลักฐานการปฏิบัติตามเมตริกซ์ควบคุมคลาวด์หรือไม่ ค้นหาหมวดหมู่ใน Control Group หรือ Control Domain ว่ามีผู้ให้บริการรายใดบ้างที่ได้ปฏิบัติตามหมวดหมู่นั้นของเมตริกซ์ควบคุมคลาวด์ เป็นต้น

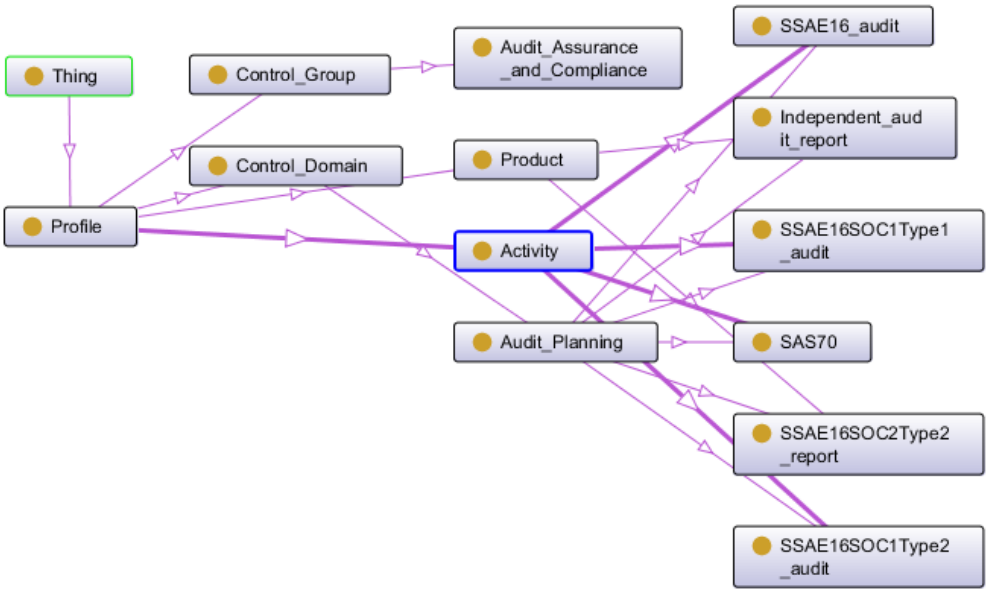
โปรไฟล์ข้อคำถามจะถูกสร้างให้อยู่ในรูปของออนโทโลจีภาษาอาวล์ด้วยโปรแกรมที่ประยุกต์ขึ้นมาเพื่อระบุคำศัพท์และความสัมพันธ์ระหว่างคำศัพท์ที่อ้างอิงจากออนโทโลจีความมั่นคงของคลาวด์ ซึ่งผู้ใช้บริการต้องการค้นหา โปรไฟล์ข้อคำถามเชิงความหมาย จะมีโครงสร้างคล้ายกับออนโทโลจีความมั่นคงของคลาวด์ ดังตัวอย่างในภาพที่ 3.10 และคำอธิบายดังตารางที่ 3.3



ภาพที่ 3.10 โครงสร้างโปรไฟล์ข้อคำถาม

ตารางที่ 3.3 คำอธิบายคำศัพท์โครงสร้างโปรไฟล์ข้อคำถาม

คำศัพท์	ความหมาย
Thing	คำศัพท์ที่จะนำมาสร้างออนโทโลจี
Profile	เอกสารอาวล์ประเภทโปรไฟล์
Control Group	แนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ ที่ต้องการค้นหา
Control Domain	หมวดย่อยของแนวปฏิบัติด้านความมั่นคงตามเมตริกซ์ควบคุมคลาวด์ ที่ต้องการค้นหา
Type	ประเภทของคำ ซึ่งสามารถแบ่งเป็น Activity, Product
Activity	กิจกรรมตามแนวการปฏิบัติด้านหนึ่ง ๆ ที่ต้องการค้นหา
Product	สิ่งที่เป็นผลผลิตจากการดำเนินการตามแนวปฏิบัติด้านหนึ่ง ๆ ที่ต้องการค้นหา



ภาพที่ 3.11 ตัวอย่างโปรไฟล์ข้อคำถาม

ภาพที่ 3.11 เป็นตัวอย่างโปรไฟล์ข้อคำถามที่ต้องการค้นหาผู้ให้บริการที่ได้ทำการปฏิบัติตามมาตรฐานของเมตริกซ์ควบคุมคลาวด์ตาม Control Group ที่ชื่อว่า “Audit Assurance and Compliance” ภายใต้ Control Domain ที่ชื่อว่า Audit Planning โดยมีการทำกิจกรรมและมีเอกสารต่าง ๆ ประกอบ เช่น SSAE16SOC1Type1 Audit, SSAE16SOC1Type2 Audit เป็นต้น

3.4 ขั้นตอนการจับคู่เชิงความหมาย

การจับคู่เชิงความหมายนั้น เป็นการเปรียบเทียบระหว่างสองนิพจน์ความสัมพันธ์ โดยอันหนึ่งอยู่ในโปรไฟล์ข้อคำถาม หรือ Q และอีกอันอยู่ในโปรไฟล์ของผู้ให้บริการคลาวด์ หรือ P กำหนดให้โปรไฟล์ข้อคำถามประกอบด้วย n นิพจน์ความสัมพันธ์ และโปรไฟล์ของผู้ให้บริการคลาวด์ประกอบด้วย m นิพจน์ความสัมพันธ์ และแต่ละนิพจน์ความสัมพันธ์จะอยู่ในรูปแบบของ <subject, property, object> โดยที่ subject หมายถึงโปรไฟล์ข้อคำถามหรือโปรไฟล์ของผู้ให้บริการคลาวด์ property หมายถึงคำศัพท์ที่เป็นคอนเซปต์ในเมตริกซ์ควบคุมคลาวด์ที่ต้องการเปรียบเทียบ และ object หมายถึงค่าของ property ดังสมการที่ (1) และ (2)

$$Q = \{hasProperty(q_1), ..., hasProperty(q_n)\} \quad (1)$$

$$P = \{hasProperty(p_1), ..., hasProperty(p_m)\} \quad (2)$$

โดยที่ hasProperty จะหมายถึง hasControlGroup, hasControlDomain, hasActivity, หรือ hasProduct เป็นต้น

การจับคู่เชิงความหมายนั้นเราจะจับคู่กันระหว่าง ค่า object ของ property ในโปรไฟล์ Q และโปรไฟล์ P ซึ่งจะมีระดับของการจับคู่อยู่ 4 แบบ ซึ่งแต่ละแบบมีคะแนนการจับคู่ (similarity score) ลดหลั่นกันไป ดังสมการที่ (3)

$$sim(q_i, p_j) = \begin{cases} 3 \ \ if \ \ p_j \equiv q_i \ \ (exact\ match) \\ 2 \ \ if \ \ p_j \sqsubseteq q_i \ (specialized\ match) \\ 1 \ \ if \ \ q_i \sqsubseteq p_j \ (generalized\ match) \\ 0 \ \ otherwise\ (\ failed\ match) \end{cases} \quad (3)$$

1. ถ้า $p_j \equiv q_i$ แล้ว q_i จะเป็นการจับคู่อย่างถูกต้อง (Exact Match) กับ p_j โดย $\equiv$ หมายถึง ว่ามีค่าเท่าเทียมกับ ดังตัวอย่างภาพที่ 3.11 โปรไฟล์ Q มีออนโทโลจีเทอมเป็นคำว่า SSAE16SOC1Type2Audit จะถือว่าเป็นการจับคู่อย่างถูกต้องกับ โปรไฟล์ P ที่มีออนโทโลจีเทอมเป็นคำว่า SSAE16SOC1Type2Audit เหมือนกัน ดังตัวอย่างภาพที่ 3.9
2. ถ้า $p_j \sqsubseteq q_i$ แล้ว p_j จะเป็นการจับคู่อย่างเจาะจง (Specialized Match) กับ q_i โดย $\sqsubseteq$ หมายถึง ถูกครอบคลุมโดย (Subsumed By) ซึ่งในกรณีนี้คือ p_j เป็นคำที่มีความหมายเฉพาะเจาะจงกว่าของ q_i ดังตัวอย่างภาพที่ 3.11 โปรไฟล์ Q มีออนโทโลจีเทอมเป็นคำว่า Audit Planning จะถือว่าเป็นการจับคู่ที่เจาะจงกับ โปรไฟล์ P ที่มีออนโทโลจีเทอมเป็นคำว่า SSAE16SOC1Type2Audit ดังตัวอย่างภาพที่ 3.9
3. ถ้า $q_i \sqsubseteq p_j$ แล้ว q_i จะเป็นการจับคู่ทั่วไป (Generalized Match) กับ p_j โดย $\sqsubseteq$ หมายถึง ถูกครอบคลุมโดย (Subsumed By) ซึ่งในกรณีนี้คือ q_i เป็นคำที่มีความหมายเฉพาะเจาะจงกว่าของ p_j ดังตัวอย่างภาพที่ 3.11 โปรไฟล์ Q มีออนโทโลจีเทอมเป็นคำว่า SSAE16SOC1Type2Audit จะถือว่าเป็นการจับคู่แบบทั่วไปกับ โปรไฟล์ P ที่มีออนโทโลจีเทอมเป็นคำว่า Audit Planning ดังตัวอย่างภาพที่ 3.9
4. ถ้าไม่มีความสัมพันธ์ตรงกับที่กล่าวมาด้านบนแล้ว q_i จะไม่จับคู่ (Failed Match) กับ p_j

3.5 ขั้นตอนการจัดลำดับของการจับคู่เชิงความหมาย

คะแนนความคล้ายคลึงกันของการจับคู่ ระหว่างโปรไฟล์ข้อคำถาม และโปรไฟล์ของผู้ให้บริการคลาวด์ คำนวณโดย

$$psim = \sum_{i=1}^{n} sim(q_i, p_j). \quad (4)$$

ผลของการค้นหานั้นมีเพียงผู้ให้บริการที่มีนิพจน์ความสัมพันธ์ที่จับคู่อย่างถูกต้อง จับคู่อย่างเจาะจง หรือจับคู่ทั่วไป กับอย่างน้อยหนึ่งนิพจน์ความสัมพันธ์ในโปรไฟล์ข้อคำถาม โดยมีการจัดลำดับของคะแนน psim (Profile Similarity) เพื่อเรียงลำดับผู้ให้บริการที่มีคะแนนมากที่สุดเรียงไปหาน้อย คะแนน psim (Profile Similarity) นั้นสะท้อนให้เห็นถึงระดับของความโปร่งใสของความมั่นคง (Security Transparency) ของผู้ให้บริการคลาวด์ กล่าวคือผู้ให้บริการที่เผยแพร่ข้อมูลการรักษาความมั่นคงอย่างครบถ้วนและเพียงพอ จะได้คะแนนสูงกว่าผู้ที่เปิดเผยข้อมูลน้อยกว่า

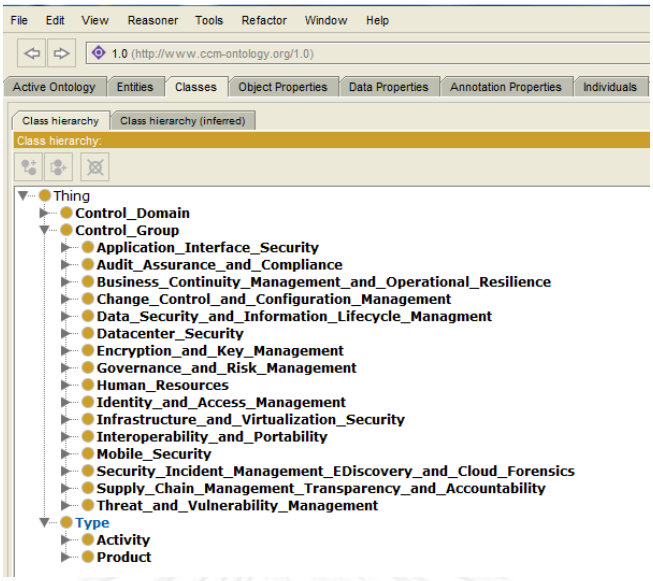
3.6 ขั้นตอนการพัฒนาต้นแบบของระบบค้นหาผู้ให้บริการคลาวด์

3.6.1 เครื่องมือที่ใช้ในการพัฒนา

- NetBeans ใช้สำหรับการพัฒนาต้นแบบของระบบค้นหาผู้ให้บริการคลาวด์
- Jena API ใช้สำหรับค้นหาความสัมพันธ์ระหว่างสองนิพจน์
- Protégé ใช้สำหรับสร้างออนโทโลจีความมั่นคงของคลาวด์

3.6.2 ขั้นตอนในการพัฒนาต้นแบบของระบบค้นหา

1. ขั้นตอนการพัฒนาออนโทโลจีที่อิงมาตรฐานจากซีเอสเอ โดยผู้วิจัยทำการวิเคราะห์เอกสารเมตริกซ์ควบคุมคลาวด์เป็นหลัก และเสริมด้วยการวิเคราะห์แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน และนำคำตอบที่ได้จากการประเมินจากผู้ให้บริการคลาวด์แล้วมาพิจารณาร่วมด้วย เพื่อสกัดเนื้อหาส่วนสำคัญมาใช้ในการสร้างความสัมพันธ์ระหว่างคำศัพท์ในเอกสารให้อยู่ในรูปของออนโทโลจีความมั่นคงของคลาวด์โดยผ่านเครื่องมือที่ชื่อว่า Protégé ดังภาพที่ 3.12



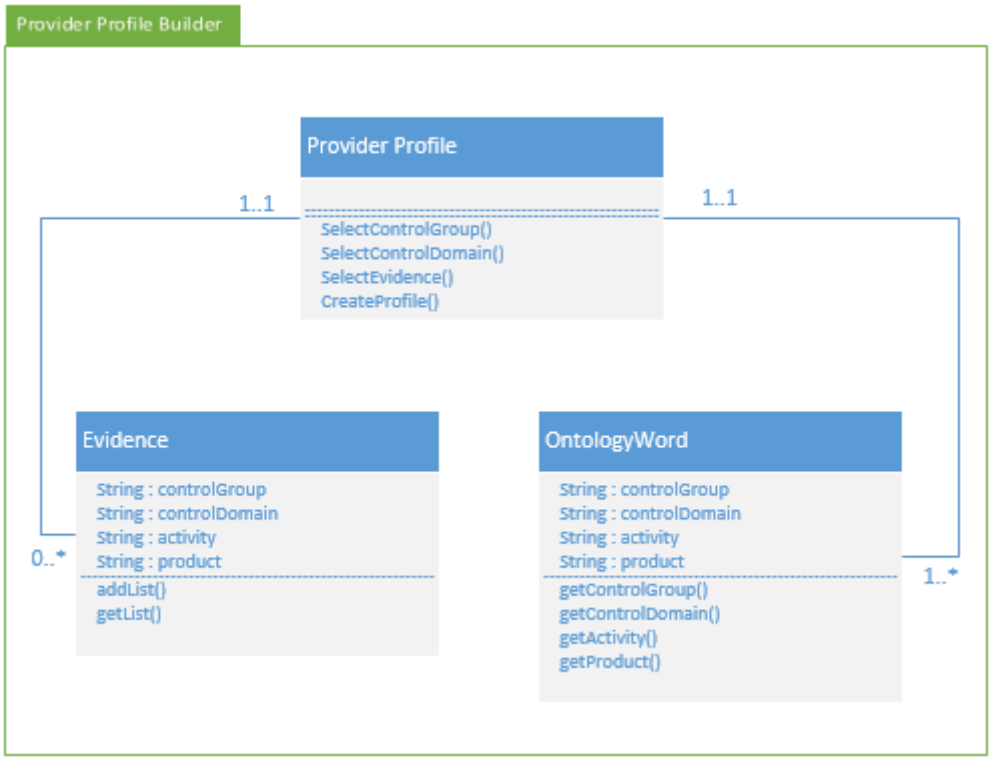
ภาพที่ 3.12 เครื่องมือ Protégé

จากภาพที่ 3.12 ผู้วิจัยได้นำคำศัพท์ที่ได้ทำการพิจารณาแล้วมาทำการเพิ่มเป็น MainClass และSubClass ลงไปในโครงสร้างออนโทโลจี ที่ได้กำหนดไว้แต่แรก (Control Group, Control Domain, Activity, Product) ซึ่งคำศัพท์สามารถดูเพิ่มเติมได้ใน ภาคผนวก ก และ ข

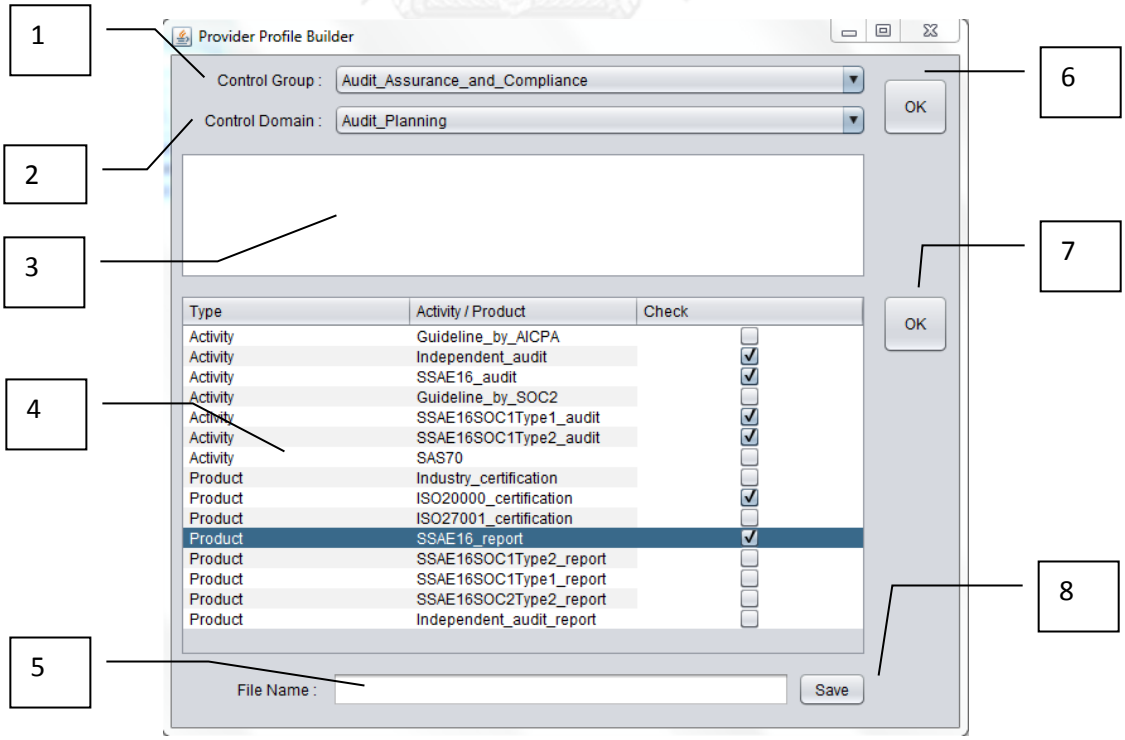
2. ขั้นตอนการพัฒนาโปรแกรมเพื่อสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ (Provider Profile Builder) เป็นโปรแกรมที่เอาไว้ช่วยสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ เนื่องจากมีคำศัพท์ในออนโทโลจีที่นำมาใช้สร้างโปรไฟล์ได้จำนวนมาก จึงอาจทำให้ลำบากในการสร้างด้วยมือหรือใช้ โปรแกรมอย่างเช่น Protégé สร้าง แผนภาพ Class Diagram ของโปรแกรม Provider Profile Builder เป็นดังภาพที่ 3.13 คำอธิบายแผนภาพ Class Diagram ของโปรแกรม Provider Profile Builder ดังตารางที่ 3.4 ส่วนต่อประสานผู้ใช้ของโปรแกรม Provider Profile Builder เป็นดังภาพที่ 3.14 และคำอธิบายส่วนต่อประสานผู้ใช้แสดงดังตารางที่ 3.5

ตารางที่ 3.4 คำอธิบายแผนภาพ Class Diagram ของโปรแกรม Provider Profile Builder

หัวข้อ	คำอธิบาย
Provider Profile	ทำหน้าที่ด้านการจัดการหลักในการสร้างโปรไฟล์ของผู้ให้บริการ
Evidence	ทำหน้าที่ในการจัดเก็บคำศัพท์ตามออนโทโลจีความมั่นคงซึ่งผู้ให้บริการระบุไว้ว่าได้ปฏิบัติตาม
OntologyWord	ทำหน้าที่ในการค้นหาคำศัพท์ในออนโทโลจีมาแสดง



ภาพที่ 3.13 แผนภาพ Class Diagram ของโปรแกรม Provider Profile Builder

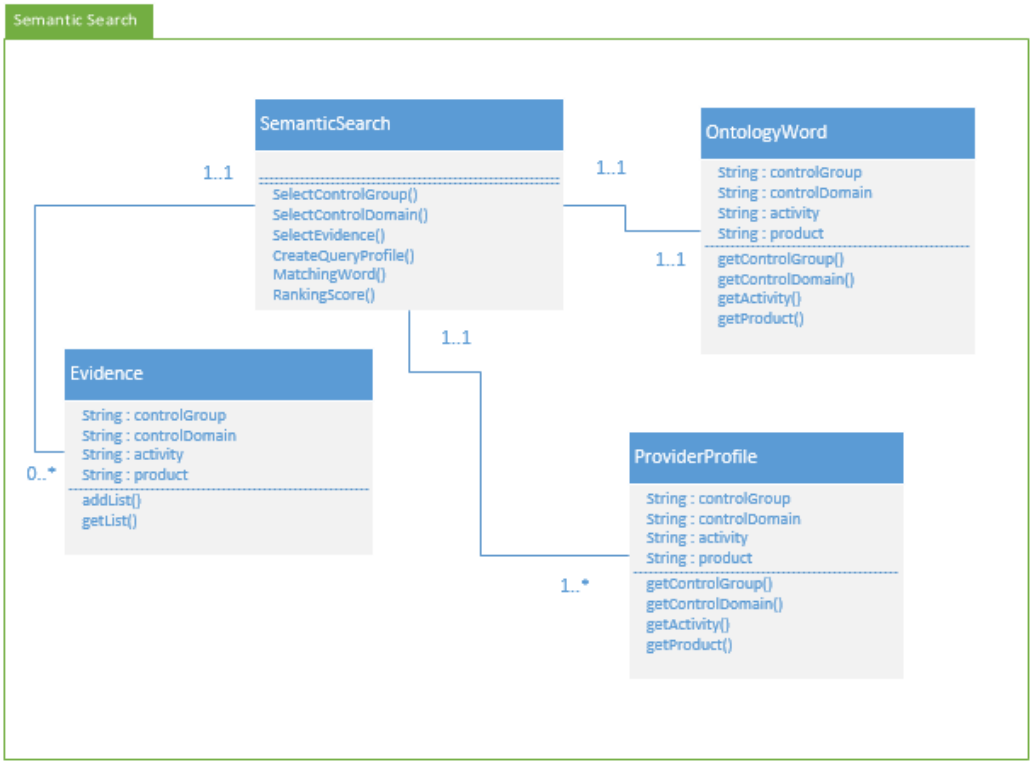


ภาพที่ 3.14 ส่วนต่อประสานผู้ใช้ของโปรแกรม Provider Profile Builder

ตารางที่ 3.5 คำอธิบายส่วนต่อประสานผู้ใช้ของโปรแกรม Provider Profile Builder

หมายเลขที่	ความหมาย
1	คำศัพท์ของ Control Group
2	คำศัพท์ของ Control Domain
3	ส่วนแสดงข้อมูล Activity หรือ Product ที่ได้เลือก
4	ส่วนแสดงข้อมูล Activity หรือ Product สำหรับให้เลือกภายใต้ Control Group และ Control Domain
5	พิมพ์ชื่อไฟล์
6	ยืนยันการเลือก Control Group และ Control Domain เพื่อคัดกรอง เฉพาะ Activity และ Product ที่เกี่ยวข้อง
7	ยืนยันการเลือก Activity หรือ Product ตามที่ระบุไว้สำหรับโปรไฟล์
8	บันทึกไฟล์โปรไฟล์

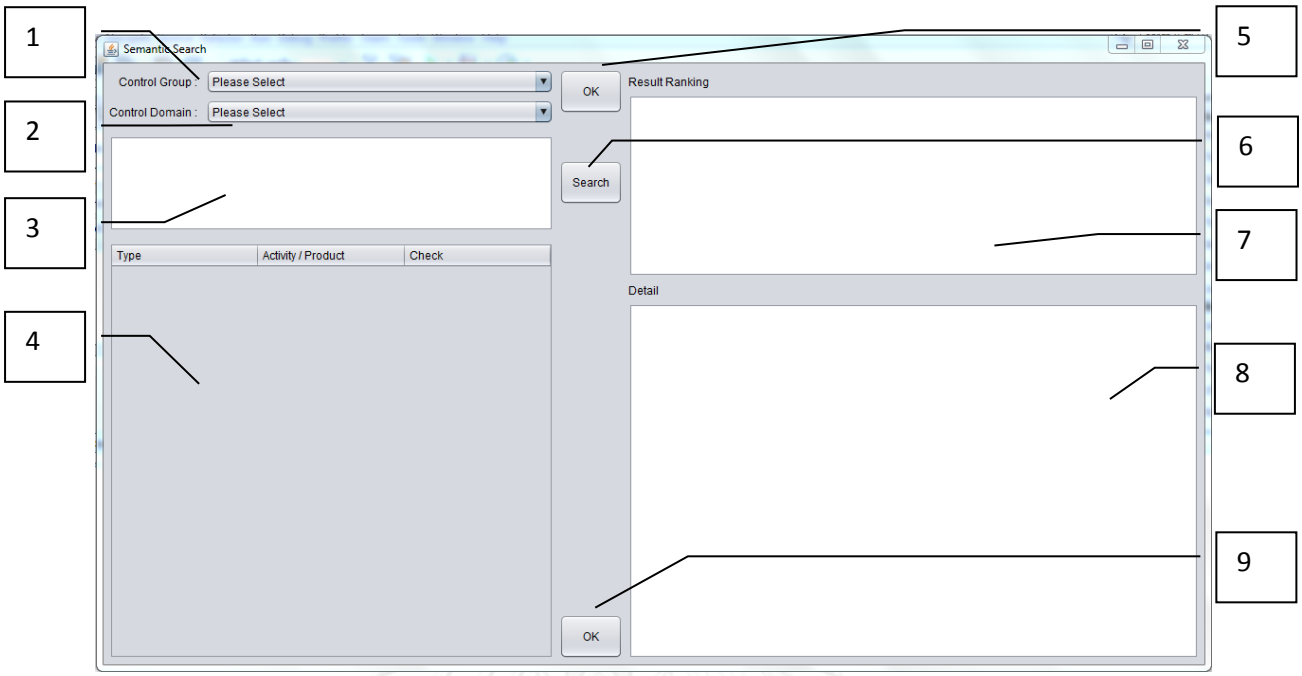
3. ขั้นตอนในการพัฒนาโปรแกรมเพื่อช่วยในการค้นหาผู้ให้บริการคลาวด์เชิงความหมาย (Semantic Search) เมื่อผู้ใช้บริการทำการค้นหาด้วยเงื่อนไขที่ต้องการ เช่น ต้องการค้นหาตาม Control Group หรือ Control Domain ว่ามีผู้ให้บริการรายใดบ้างที่ได้ปฏิบัติตาม ต้องการค้นหาว่าผู้ให้บริการรายใดบ้างที่ดำเนินการตาม Activity หรือมี Product ที่สนใจ เป็นต้น ระบบจะทำการสร้างโปรไฟล์ข้อคำถามขึ้นมาโดยอิงออนโทโลจีที่สร้างขึ้น เพื่อใช้ในการจับคู่ในขั้นตอนถัดไป แผนภาพ Class Diagram ของโปรแกรม Semantic Search เป็นดังภาพที่ 3.15 คำอธิบายแผนภาพ Class Diagram ของโปรแกรม Semantic Search ดังตาราง 3.6 ส่วนต่อประสานผู้ใช้ของโปรแกรม Semantic Search แสดงดังภาพที่ 3.16 และคำอธิบายส่วนต่อประสานผู้ใช้ ดังตารางที่ 3.7



ภาพที่ 3.15 แผนภาพ Class Diagram ของโปรแกรม Semantic Search

ตารางที่ 3.6 คำอธิบายแผนภาพ Class Diagram ของโปรแกรม Semantic Search

หัวข้อ	คำอธิบาย
Semantic Search	ทำหน้าที่ด้านการจัดการหลักในการค้นหาเชิงความหมาย
Evidence	ทำหน้าที่ในการจัดเก็บคำศัพท์ตามออนโทโลจีความมั่นคง ซึ่งผู้ใช้บริการระบุว่าต้องการค้นหา
OntologyWord	ทำหน้าที่ในการค้นหาคำศัพท์ในออนโทโลจีมาแสดง
Provider Profile	ทำหน้าที่ด้านการจัดการหลักเกี่ยวกับโปรไฟล์ของผู้ให้บริการ



ภาพที่ 3.16 ส่วนต่อประสานผู้ใช้ของโปรแกรม Semantic Search

ตารางที่ 3.7 คำอธิบายส่วนต่อประสานผู้ใช้ของโปรแกรม Semantic Search

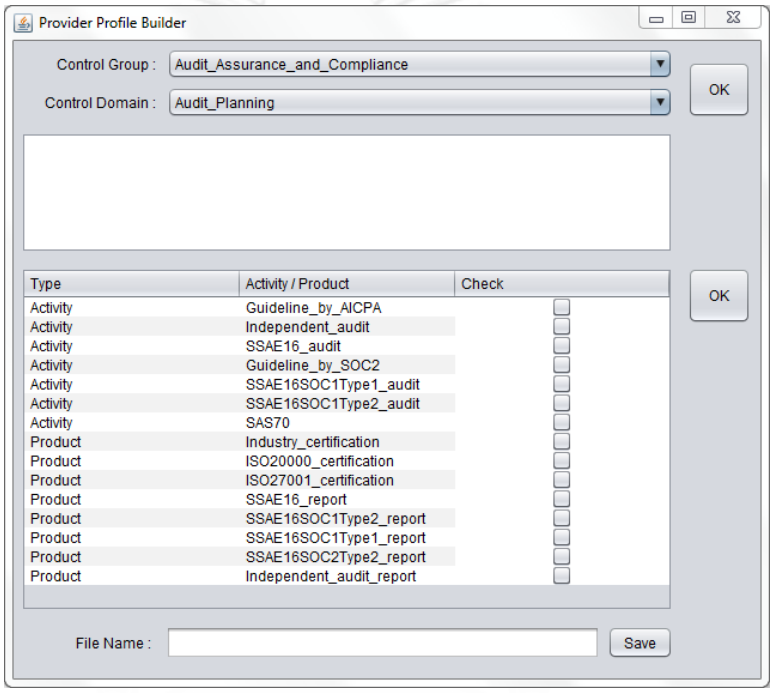
หมายเลขที่	ความหมาย
1	คำศัพท์ของ Control Group
2	คำศัพท์ของ Control Domain
3	ส่วนแสดงข้อมูล Activity หรือ Product ที่ได้เลือก
4	ส่วนแสดงข้อมูล Activity หรือ Product ภายใต้ Control Group และ Control Domain สำหรับให้เลือก
5	ยืนยันการเลือก Control Group และ Control Domain เพื่อคัดกรอง เฉพาะ Activity และ Product ที่เกี่ยวข้อง
6	ทำการค้นหา
7	แสดงผู้ให้บริการคลาวด์ทั้งหมดที่ได้จัดลำดับแล้ว
8	แสดงรายละเอียดคะแนนของผู้ให้บริการคลาวด์ที่เลือก
9	ยืนยันการเลือก Activity หรือ Product ตามที่ระบุไว้สำหรับโปรไฟล์

3.7 ขั้นตอนการทดสอบ

ขั้นตอนการทดสอบแบ่งเป็น 2 ส่วนคือ การทดสอบโปรแกรม Provider Profile Builder และโปรแกรม Semantic Search ซึ่งผลการทดสอบเป็นไปอย่างถูกต้อง รายละเอียดดังนี้

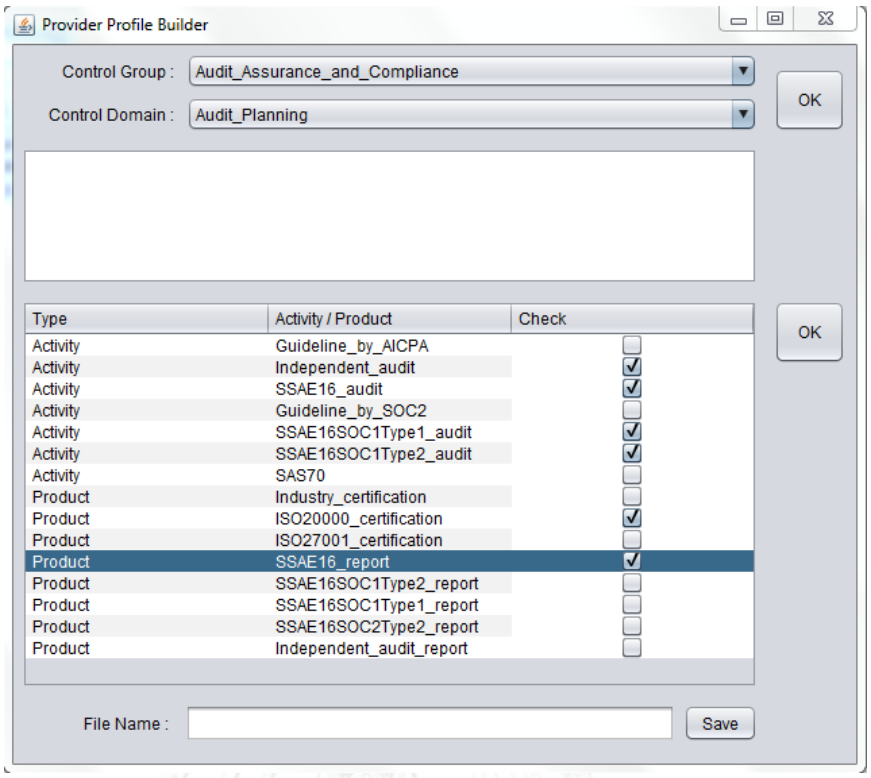
3.7.1 Provider Profile Builder

ในส่วนนี้จะเป็นการทดสอบว่าโปรแกรมสามารถสร้างโปรไฟล์ตามที่เลือกได้หรือไม่ โดยภาพที่ 3.15 แสดงให้เห็นว่าเมื่อทำการเลือก Control Group และ Control Domain แล้วทำการกดปุ่ม OK จะแสดง Activity และ Product ทั้งหมดใน Control Group และ Control Domain ที่เลือก

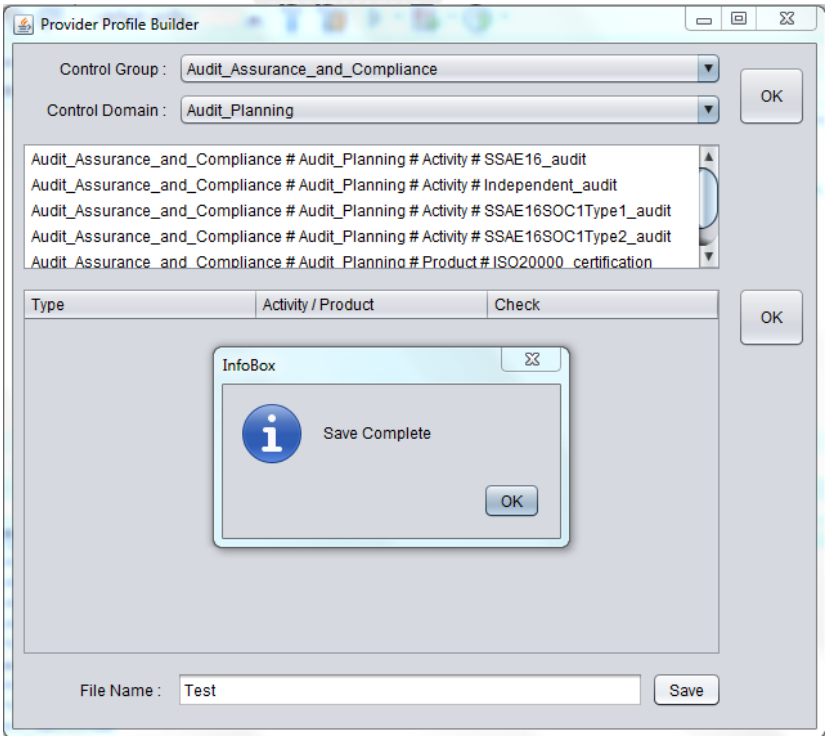


ภาพที่ 3.17 ขั้นตอนการเลือก Control Group และ Control Domain

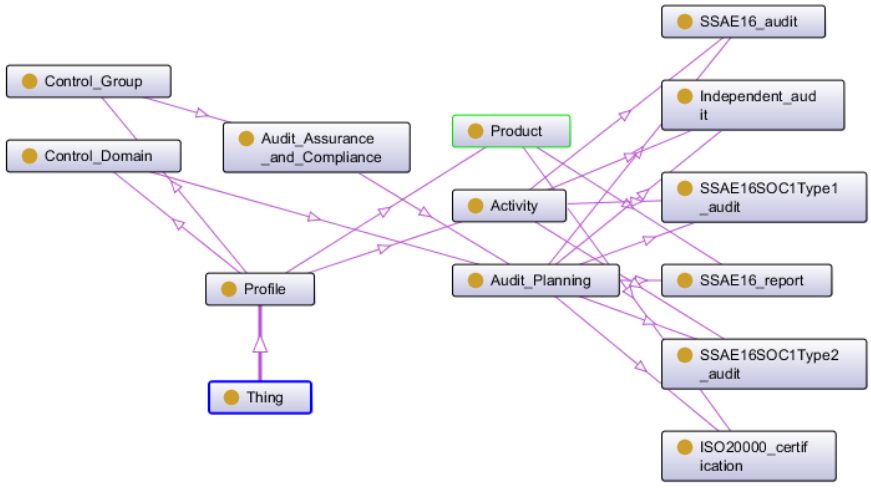
จากภาพที่ 3.18 และ 3.19 นั้น เมื่อทำการเลือก Activity และ Product ที่ผู้ให้บริการเจ้านั้นได้ทำหรือได้ปฏิบัติตามแล้วทำการบันทึก เพื่อทำการสร้างโปรไฟล์ของผู้ให้บริการ ผลลัพธ์ที่ได้คือโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ ที่มีโครงสร้าง Control Group, Control Domain, Activity, Product ตามที่ได้เลือกเอาไว้ ดังภาพที่ 3.20



ภาพที่ 3.18 ขั้นตอนการเลือก Activity และ Product



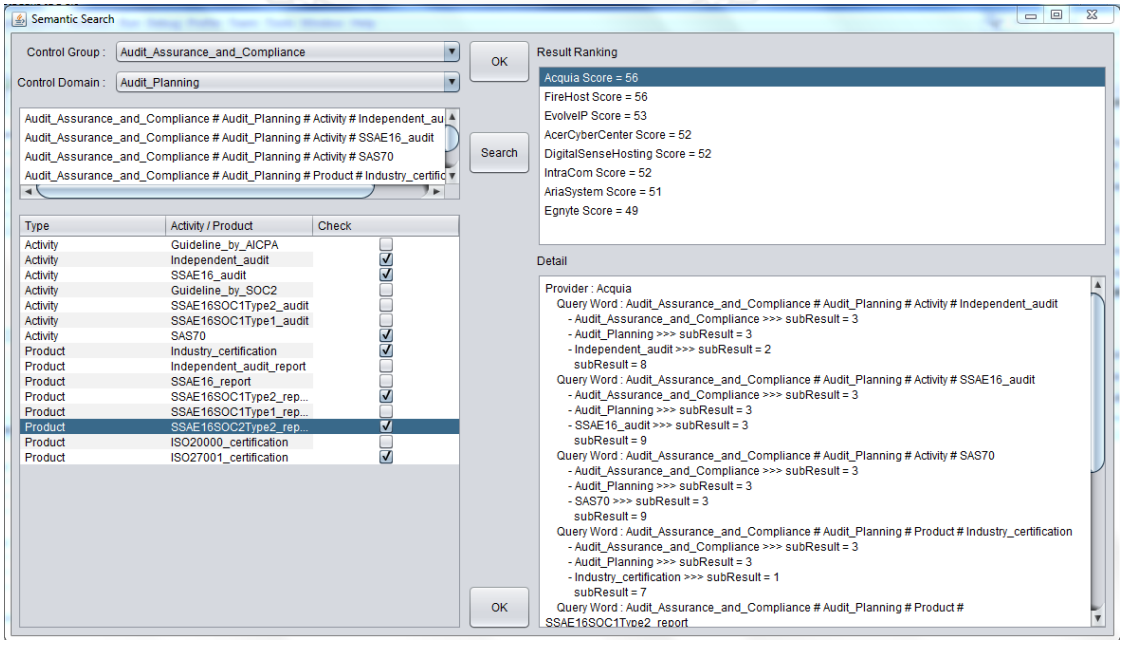
ภาพที่ 3.19 ขั้นตอนในการบันทึกเพื่อสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์



ภาพที่ 3.20 โปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ ที่สร้างจากโปรแกรม

3.7.2 Semantic Search

ในส่วนนี้เป็นการค้นหาข้อมูลตามที่ได้เลือกเอาไว้ จากภาพที่ 3.21 จะเห็นว่าเป็นการค้นหาผู้ให้บริการคลาวด์ ที่มีการปฏิบัติตาม Control Group ที่ชื่อว่า Audit Assurance and Compliance ในหมวดย่อย Control Domain ที่ชื่อว่า Audit Planning โดยค้นหาตาม Activity และ Product ที่ระบุในภาพที่ 3.21 เมื่อทำการกดปุ่ม Search จะทำการค้นหาข้อมูลตามที่เลือกแล้วนำมาแสดงในส่วนของ Result Ranking และเมื่อทำการคลิกในส่วน Result Ranking จะแสดงรายละเอียดของการจับคู่นิพจน์ความสัมพันธ์ของผู้ให้บริการรายนั้น



ภาพที่ 3.21 ตัวอย่างการค้นหาโดยใช้โปรแกรม Semantic Search

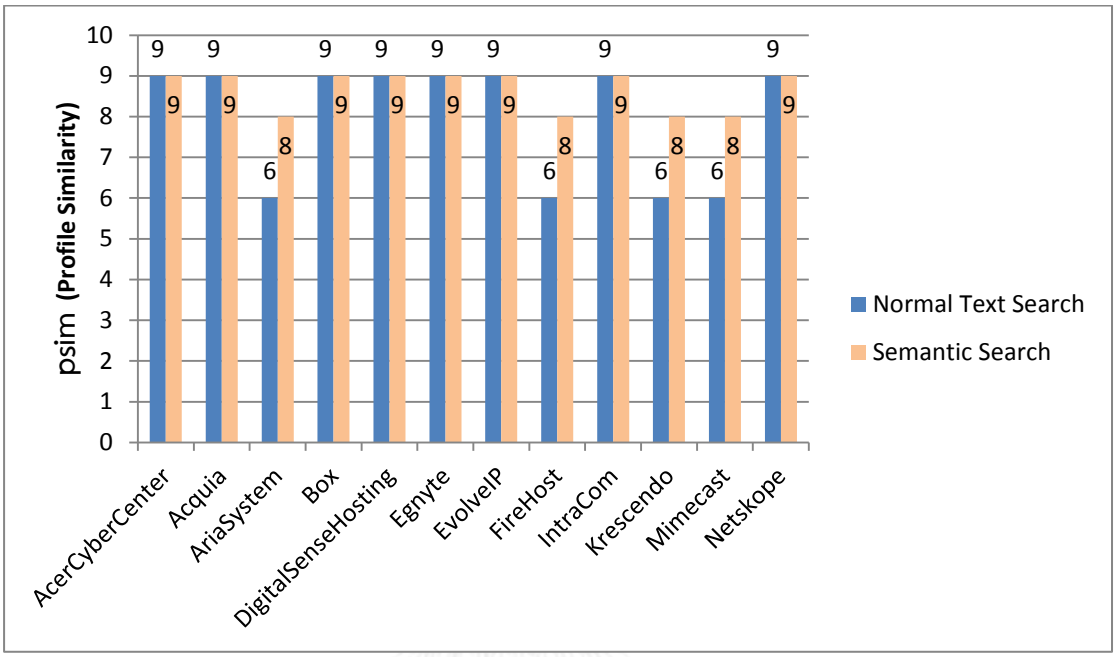
บทที่ 4
การประเมินผลการวิจัย

ในการประเมินผลการวิจัย จะทำการทดสอบการค้นหาผู้ให้บริการคลาวด์โดยแบ่งเป็น 2 แบบ คือ การค้นหาข้อความแบบปกติ (Normal Text Search) และ การค้นหาเชิงความหมาย (Semantic Search) ในการค้นหาข้อความแบบปกติ โปรไฟล์ของผู้ให้บริการจะเปรียบเหมือนข้อความปกติ ไม่ใช่ออนโทโลจี ดังนั้นทุกนิพจน์ความสัมพันธ์ (q_i) ในโปรไฟล์ข้อคำถาม จะถูกนำไปสืบค้นกับข้อความในโปรไฟล์ของผู้ให้บริการ โดยที่โปรไฟล์ของผู้ให้บริการ ที่มีคำศัพท์ที่จับคู่ได้อย่างถูกต้อง (Exact Match) กับอย่างน้อย 1 นิพจน์ความสัมพันธ์ q_i ในโปรไฟล์ข้อคำถาม จะถือว่าเป็นผู้ให้บริการที่สามารถจับคู่กับข้อคำถามได้ และมีการคำนวณคะแนนความคล้ายคลึงของการจับคู่ psim (Profile Similarity) ให้ ในกรณีที่โปรไฟล์ของผู้ให้บริการไม่สามารถจับคู่อย่างถูกต้องได้กับ q_i ใดๆ เลย จะถือว่าคะแนน psim (Profile Similarity) ของผู้ให้บริการรายนั้นเป็น 0 ในการค้นหาเชิงความหมาย นิพจน์ความสัมพันธ์ p_j จะเป็นคอนเซปต์ในออนโทโลจีที่ถูกจับคู่เชิงความหมายกับนิพจน์ความสัมพันธ์ q_i ของโปรไฟล์ข้อคำถาม โดยการจับคู่จะเป็นทั้งแบบจับคู่อย่างถูกต้อง จับคู่อย่างเจาะจง และจับคู่ทั่วไป และมีการคำนวณคะแนน psim (Profile Similarity) ให้ในทำนองเดียวกัน

ผู้วิจัยได้รวบรวมข้อมูลผู้ให้บริการคลาวด์ 12 ราย เพื่อนำมาทดสอบและประเมินผลได้แก่ AcerCyberCenter, Acquia, ArialSystem, Box, DigitalSenseHosting, Egnyte, EvoveIP, FireHost, IntraCom, Krescendo, Mimecast และ Netskope การทดสอบทำโดยใช้ข้อคำถาม 10 แบบ รายละเอียดของข้อคำถามและผลการค้นหามีดังนี้

4.1 ข้อคำถามเฉพาะ Control Group

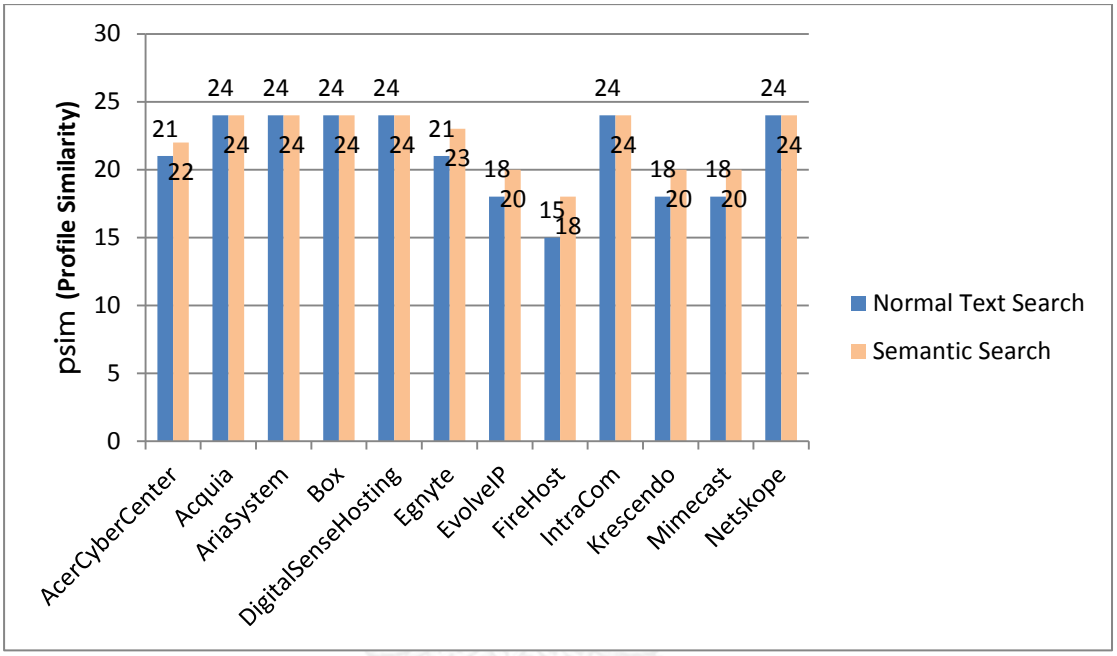
ข้อคำถามเฉพาะ Control Group เป็นการค้นหาเพียง Control Group ที่สนใจเท่านั้น ซึ่งทดสอบโดยค้นหาผู้ให้บริการที่ได้ทำตาม Control Group Audit Assurance and Compliance, Datacenter Security และ Encryption and Key Management ผลการค้นหาข้อความแบบปกติและผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.1



ภาพที่ 4.1 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามเฉพาะ Control Group

4.2 ข้อคำถามเฉพาะ Control Domain

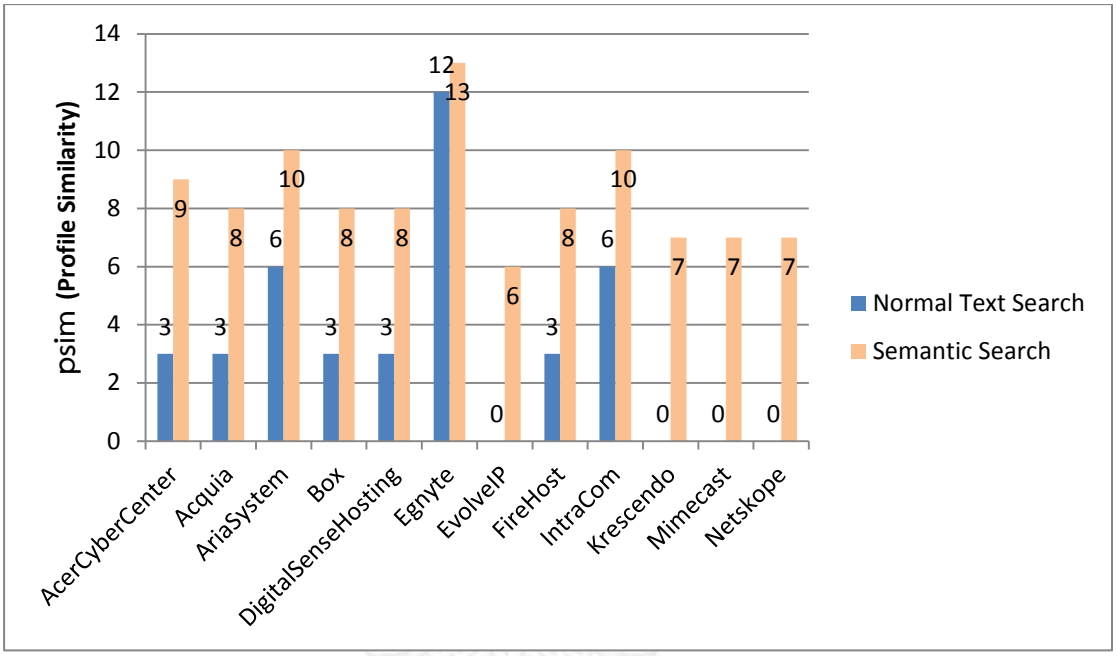
ข้อคำถามเฉพาะ Control Domain เป็นการค้นหาเพียง Control Domain ที่สนใจเท่านั้น ซึ่งทดสอบโดยค้นหาผู้ให้บริการที่ได้ทำตาม Control Domain Audit Planning, Audit Tools Access, Clock Synchronization และ Incident Management ผลการค้นหาข้อความแบบปกติและผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.2



ภาพที่ 4.2 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามเฉพาะ Control Domain

4.3 ข้อคำถามเฉพาะ Activity

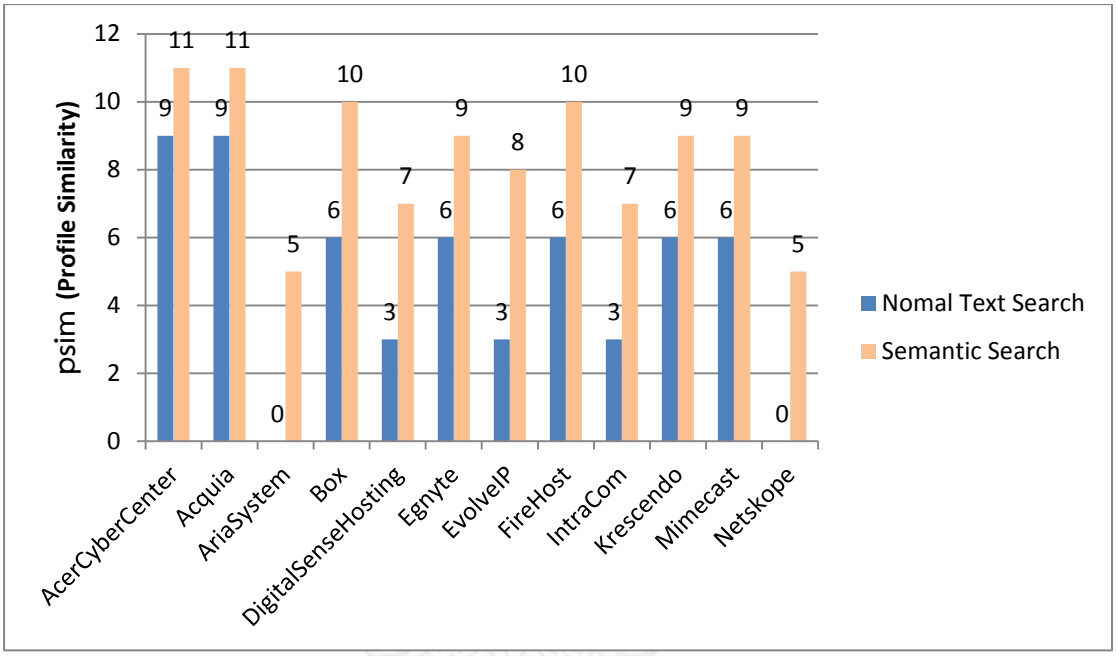
ข้อคำถามเฉพาะ Activity เป็นการค้นหาเพียงแค่ Activity ที่สนใจเท่านั้น ซึ่งทดสอบโดยค้นหาผู้ให้บริการที่ได้ทำ Activity Physical Separation, Vulnerability Scan, Physical Security Control, Temper Audit และ Recovery Data ผลการค้นหาข้อความแบบปกติและผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.3



ภาพที่ 4.3 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามเฉพาะ Activity

4.4 ข้อคำถามเฉพาะ Product

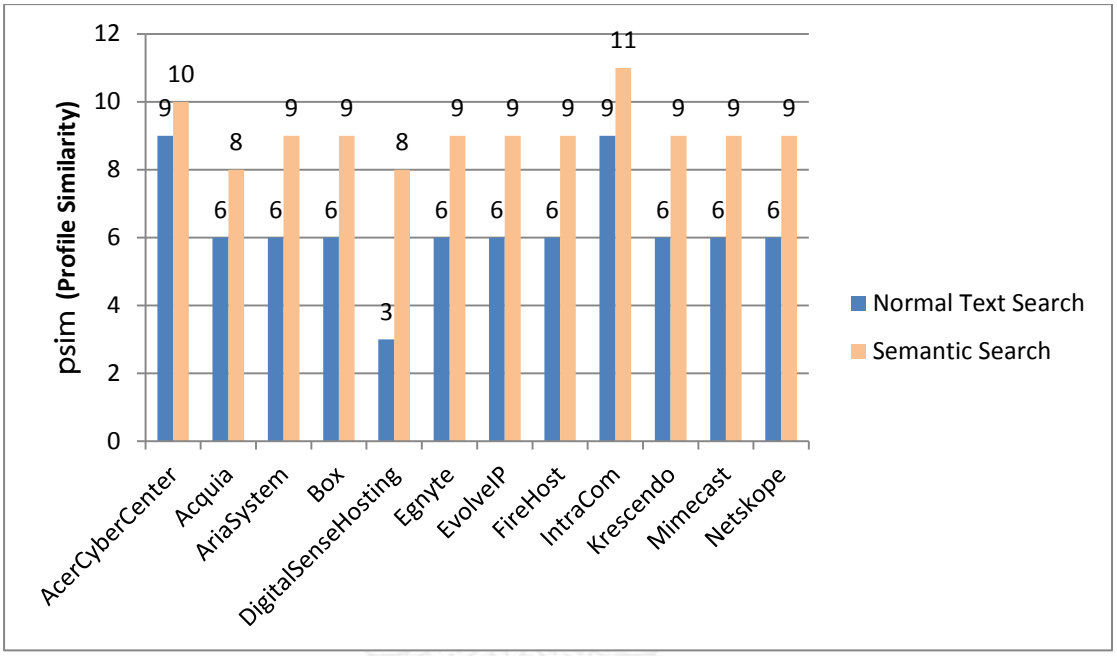
ข้อคำถามเฉพาะ Product เป็นการค้นหาเพียงแค่ Product ที่สนใจเท่านั้น ซึ่งทดสอบโดยค้นหาผู้ให้บริการที่ได้ทำ Product Document describes ISMP, Business continuity plan, SSAE16 Report, ISO27001 Certification และ ISO20000 Certification ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.4



ภาพที่ 4.4 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามเฉพาะ Product

4.5 ข้อคำถามแบบผสม Activity และ Product

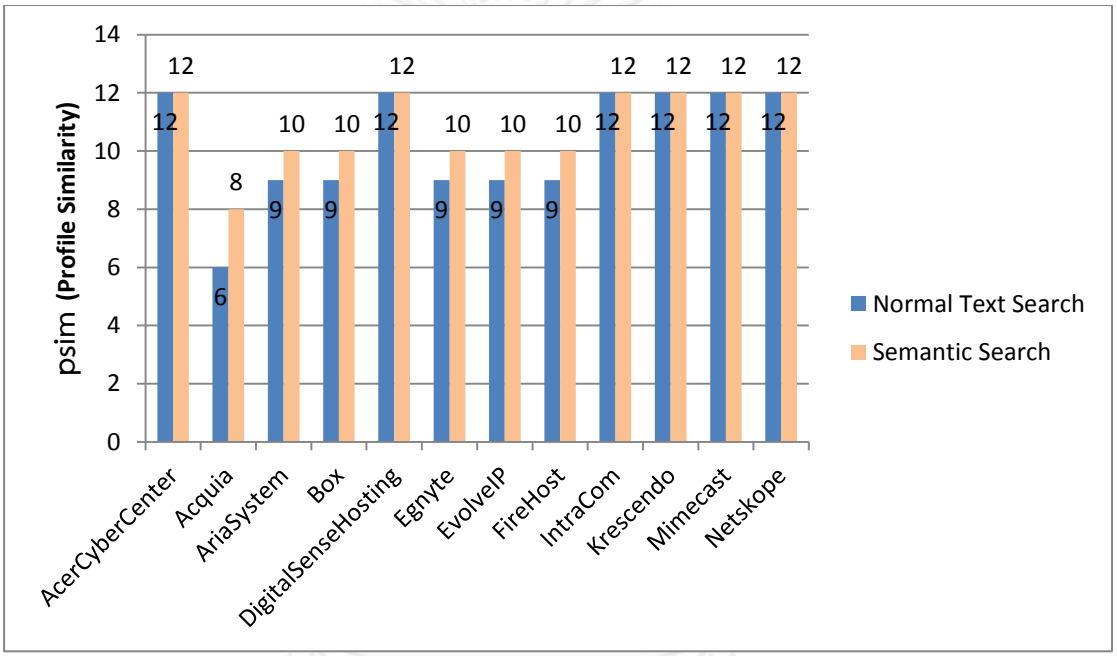
ข้อคำถามแบบผสมนี้ เป็นการค้นหาซึ่งเลือกข้อมูลจากหลาย Activity และ Product มาทำการค้นหา การทดสอบทำโดยค้นหาผู้ให้บริการที่ได้ทำ Activity ได้แก่ Logical Separation, Security Awareness Training และAccess Control และ Product ได้แก่ ISO27001 Requirement ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.5



ภาพที่ 4.5 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามแบบผสม Activity และ Product

4.6 ข้อคำถามแบบผสม Control Domain ภายใต้ Control Group

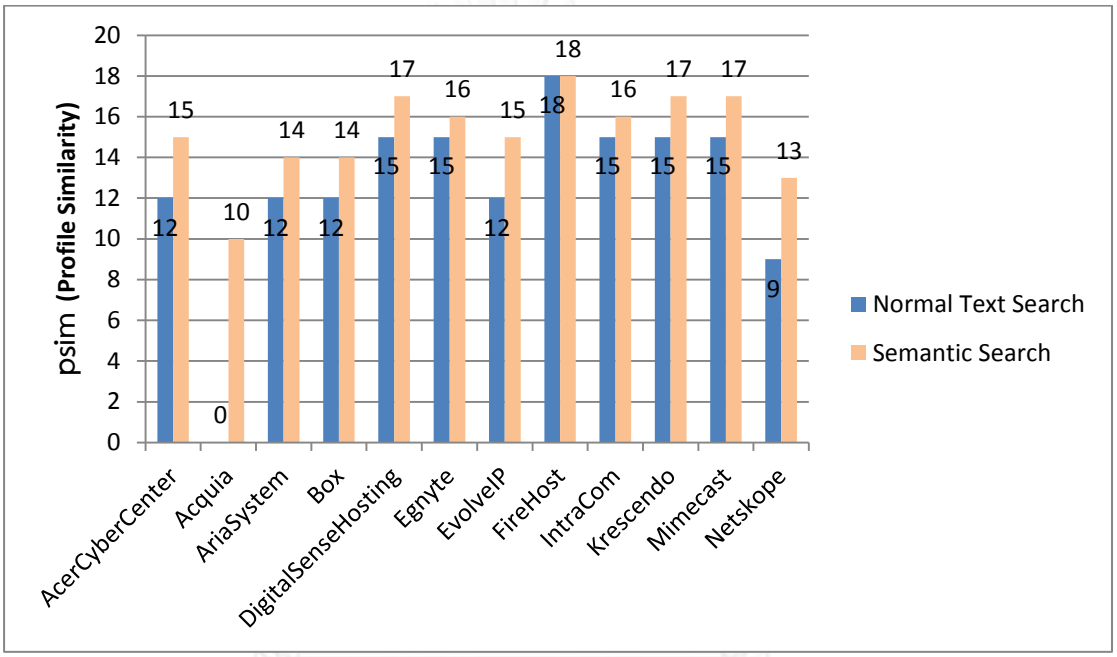
ข้อคำถามแบบผสมนี้ เป็นการค้นหาซึ่งเลือกข้อมูลจาก Control Domain ภายใต้ Control Group หนึ่ง ๆ มาทำการค้นหา การทดสอบทำโดยค้นหาผู้ให้บริการที่ได้ทำ Control Domain : Quality Testing ภายใต้ Control Group : Change Control and Configuration Management และ Control Domain : Vulnerability and Patch Management ภายใต้ Control Group : Threat and Vulnerability Management ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.6



ภาพที่ 4.6 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามแบบผสม Control Domain ภายใต้ Control Group

4.7 ข้อคำถามแบบผสม Activity จาก Control Domain

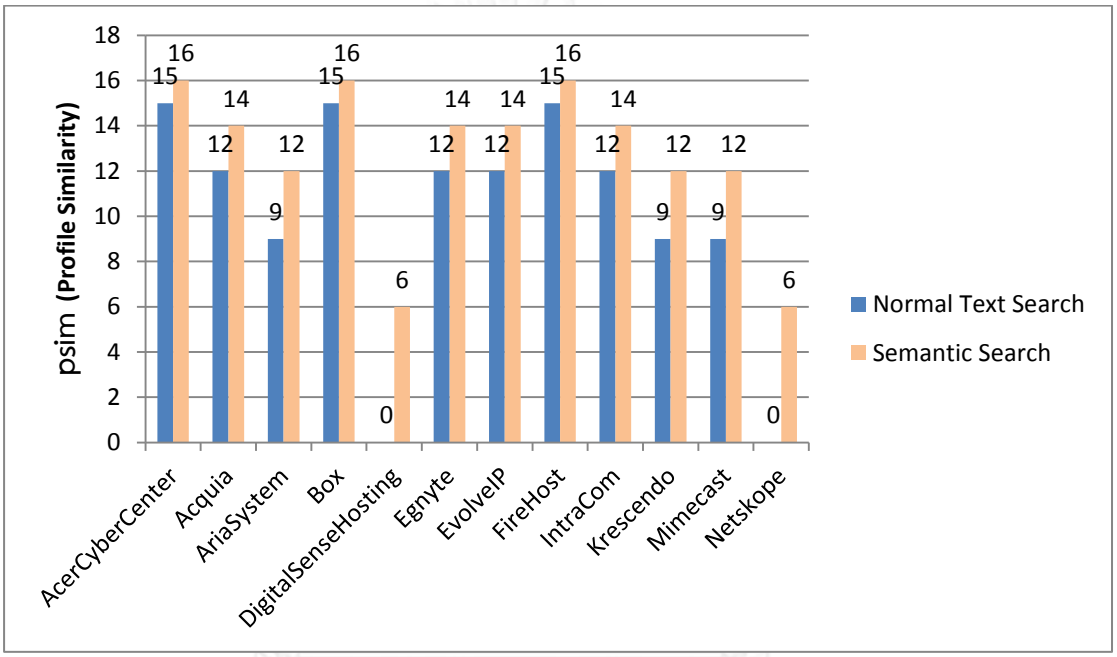
ข้อคำถามแบบผสมนี้ เป็นการค้นหาซึ่งเลือกข้อมูล Activity จาก Control Domain หนึ่ง ๆ มาทำการค้นหา การทดสอบทำโดยค้นหาผู้ให้บริการที่ได้ทำ Activity จาก Control Domain Controlled Access Points ได้แก่ Physical Security Control, Monitor Access Control และ Electronic Access Card ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.7



ภาพที่ 4.7 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามแบบผสม Activity จาก Control Domain

4.8 ข้อคำถามแบบผสม Product จาก Control Domain

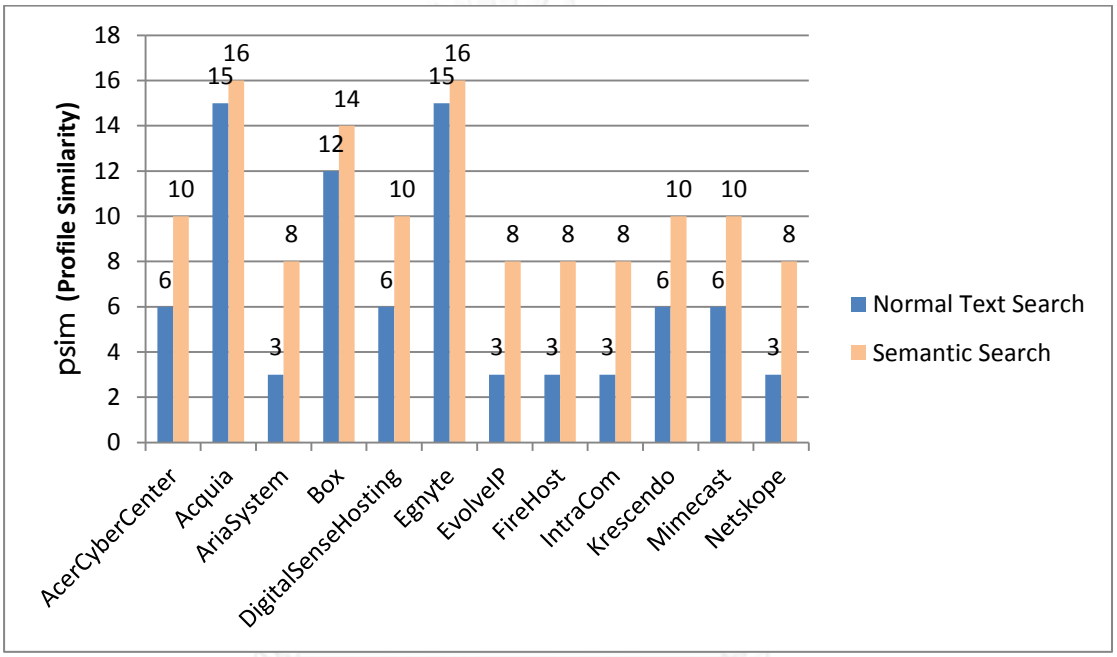
ข้อคำถามแบบผสมนี้ เป็นการค้นหาซึ่งเลือกข้อมูล Product จาก Control Domain หนึ่ง ๆ มาทำการค้นหา การทดสอบทำโดยค้นหาผู้ให้บริการที่ได้ทำ Product จาก Control Domain Business Continuity Testing ได้แก่ Business Continuity Plan, Regular recovery drill, ISO27001 certified ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.8



ภาพที่ 4.8 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามแบบผสม Product จาก Control Domain

4.9 ข้อคำถามแบบผสม Activity และ Product จาก Control Domain

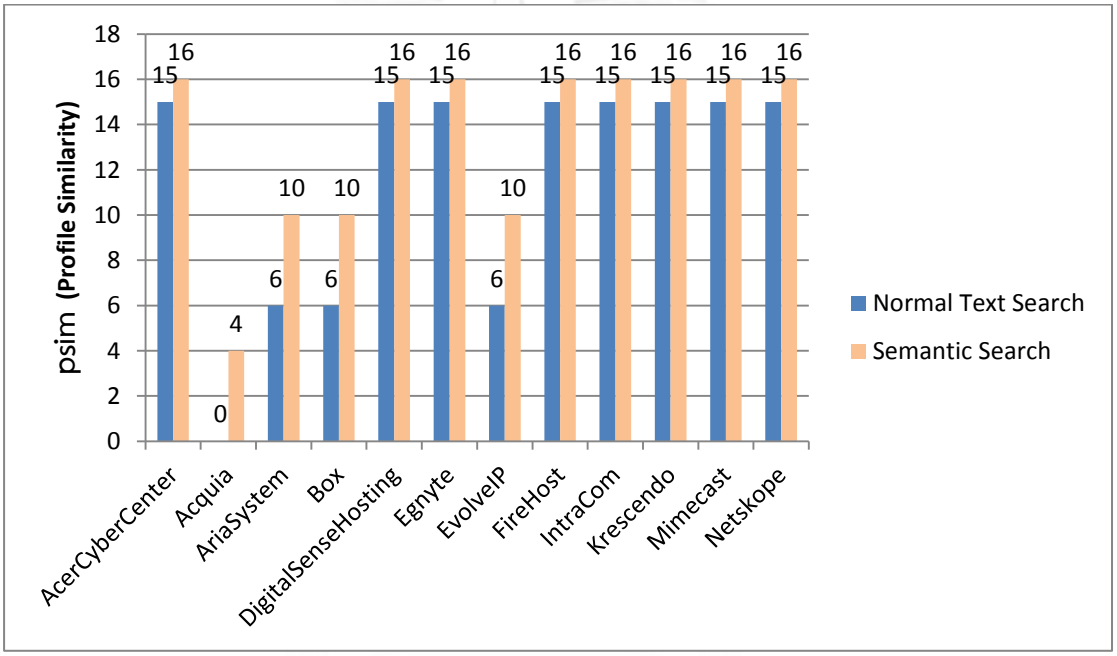
ข้อคำถามแบบผสมนี้ เป็นการค้นหาซึ่งเลือกข้อมูล Product และ Activity จาก Control Domain ต่าง ๆ มาทำการค้นหา การทดสอบทำโดยค้นหาผู้ให้บริการที่ได้ทำ Product จาก Control Domain Anti Virus and Malicious ได้แก่ Antivirus Software และ Activity จาก Control Domain Mobile Code ได้แก่ Mobile Code Authorized และ Code Configuration Check ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.9



ภาพที่ 4.9 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามแบบผสม Activity และ Product จาก Control Domain

4.10 ข้อคำถามแบบผสม Activity และ Product จาก Control Domain ภายใต้ Control Group

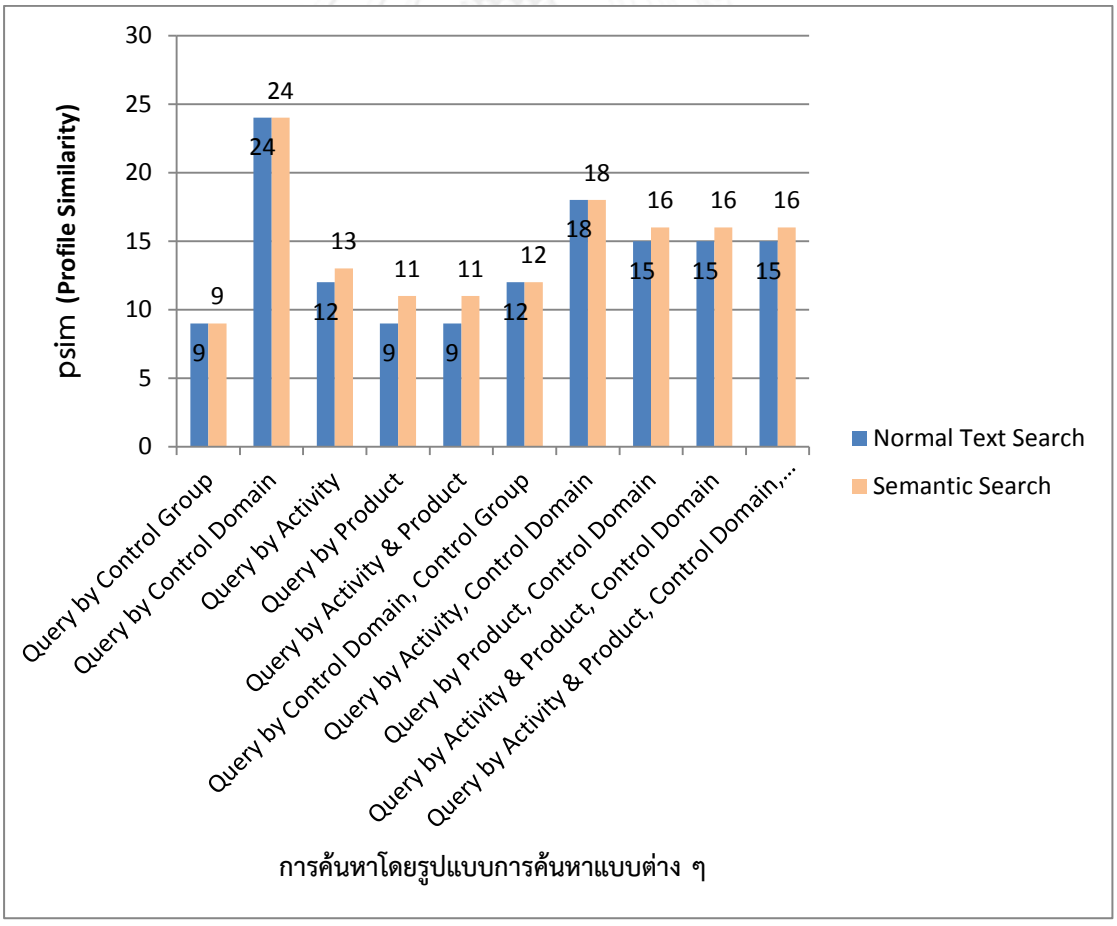
ข้อคำถามแบบผสมนี้ เป็นการค้นหาซึ่งเลือกข้อมูล Product และ Activity จาก Control Domain ภายใต้ Control Group หนึ่ง ๆ มาทำการค้นหา การทดสอบทำโดยค้นหาผู้ให้บริการที่ได้ทำ Activity และ Product จาก Control Domain Product Changes ภายใต้ Control Group Change Control and Configuration Management ได้แก่ Activity Notify Customer และ Product Document of Production Change ผลการค้นหาข้อความแบบปกติ และผลการค้นหาเชิงความหมาย แสดงดังภาพที่ 4.10



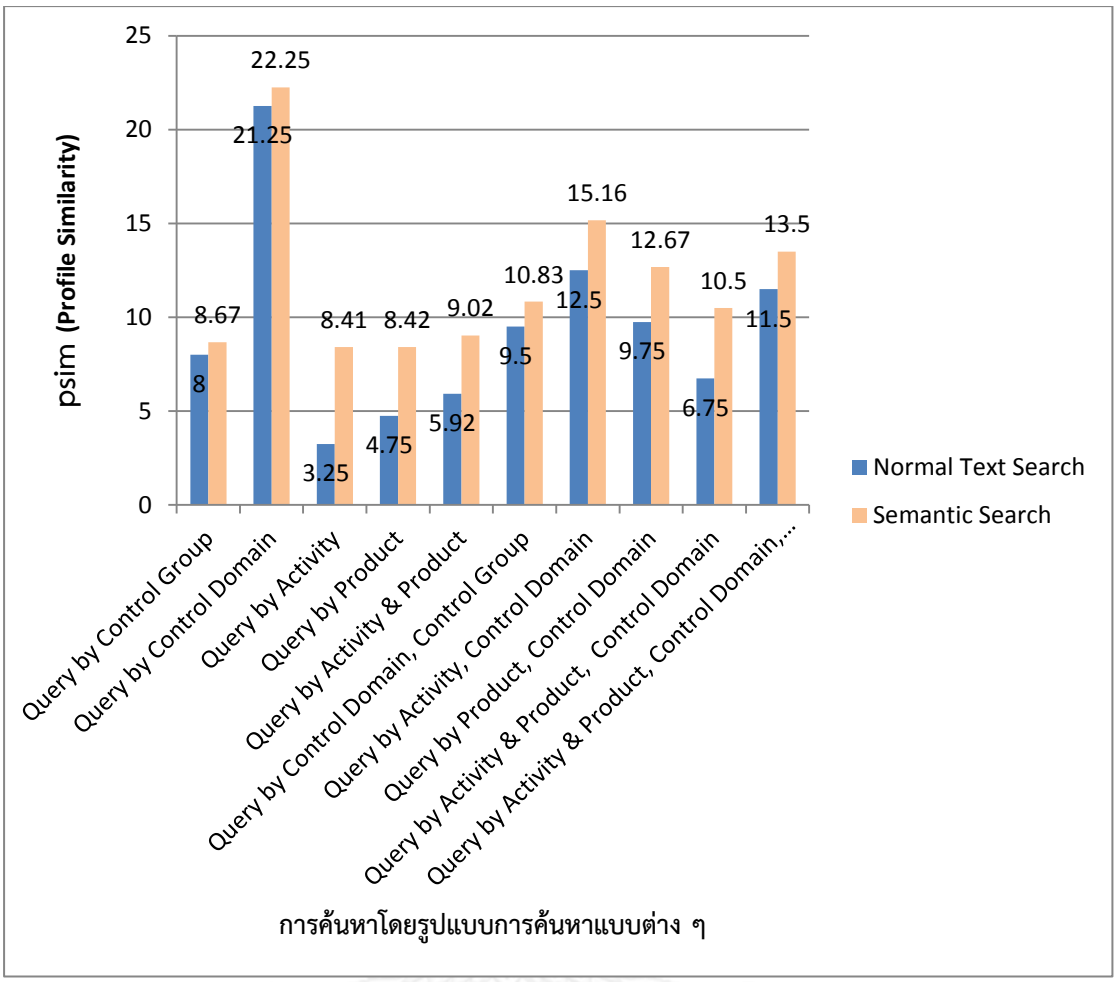
ภาพที่ 4.10 การเปรียบเทียบผลการค้นหาด้วยข้อคำถามแบบผสม Activity และ Product จาก Control Domain ภายใต้ Control Group

4.11 ผลการประเมิน

การทดลองประกอบด้วย 10 รูปแบบการค้นหา จากโปรไฟล์ของผู้ให้บริการ 12 ราย คะแนนของผู้ให้บริการที่เป็นคำตอบ ซึ่งมีค่า psim (Profile Similarity) สูงสุดจากการค้นหา แสดงดังภาพที่ 4.11 และคะแนน psim (Profile Similarity) เฉลี่ยของผู้ให้บริการที่เป็นคำตอบ แสดงดังภาพที่ 4.12 เห็นได้ว่าในการค้นหาข้อความแบบปกติ คะแนน psim (Profile Similarity) ต่ำกว่าการค้นหาเชิงความหมาย เพราะเมื่อโปรไฟล์ของผู้ให้บริการคลาวด์ ไม่มีนิพจน์ความสัมพันธ์ที่ตรงกับนิพจน์ความสัมพันธ์ที่ต้องการ จะไม่ได้คะแนน ในขณะที่การค้นหาเชิงความหมายอาจได้คะแนนบ้าง เช่น สมมติว่าโปรไฟล์ข้อคำถามมีนิพจน์ความสัมพันธ์ เป็น “Information System Regulatory Mapping” และโปรไฟล์ของผู้ให้บริการประกอบด้วยนิพจน์ “Audit Assurance and Compliance” ซึ่งการค้นหาข้อความแบบปกติจะได้รับคะแนนเป็น 0 เพราะผู้ให้บริการไม่มีนิพจน์ “Information System Regulatory Mapping” แต่ในการค้นหาเชิงความหมายจะได้รับคะแนนเป็น 1 (การจับคู่ทั่วไป) เพราะ Control Domain “Information System Regulatory Mapping” อยู่ภายใต้ Control Group “Audit Assurance and Compliance”



ภาพที่ 4.11 คะแนน psim (Profile Similarity) สูงสุดในแต่ละรูปแบบการค้นหา



ภาพที่ 4.12 คะแนน psim (Profile Similarity) เฉลี่ยในแต่ละรูปแบบการค้นหา

ค่า psim (Profile Similarity) สูงสุดในภาพที่ 4.11 และค่า psim (Profile Similarity) เฉลี่ยในภาพที่ 4.12 สะท้อนถึงประสิทธิภาพของการค้นหาข้อมูลแบบเชิงความหมายว่ามีประสิทธิภาพดีกว่าการค้นหาข้อความแบบปกติ ประสิทธิภาพนี้สามารถอธิบายได้ในเชิงของมาตรวัดค่าความแม่นยำ (Precision) และค่าระลึก (Recall) ซึ่งเป็นมาตรวัดที่ใช้ทั่วไปในการค้นคืนสารสนเทศ (Information Retrieval) โดยมาตรวัดทั้งสองมีนิยาม คือ

$$\text{Precision} = \frac{\text{Number of relevant data retrieved}}{\text{Number of data retrieved}}$$

$$= \frac{\text{Number of retrieved provider profiles that match query profile}}{\text{Number of retrieved provider profiles}}$$

$$\text{Recall} = \frac{\text{Number of relevant data retrieved}}{\text{Number of relevant data}}$$

$$= \frac{\text{Number of retrieved provider profiles that match query profile}}{\text{Number of provider profiles that match query profile}}$$

ค่าความแม่นยำและค่าระลึกจะอยู่ในช่วง [0,1] ค่าความแม่นยำถือเป็นมาตรวัดความถูกต้องหรือคุณภาพ (Correctness or Quality) ของผลการสืบค้น ในการทดลองนี้ทั้งการค้นหาข้อความแบบปกติและการค้นหาเชิงความหมาย จะถือว่ามีความแม่นยำเป็น 1 ทั้งคู่ เพราะคำตอบที่ได้จะสอดคล้องกับข้อคำถามเสมอ โดยอาจสอดคล้องแบบถูกต้อง แบบเจาะจง หรือแบบทั่วไป ก็ได้แล้วแต่กรณี ส่วนค่าระลึกถือเป็นมาตรวัดความสมบูรณ์หรือปริมาณ (Completeness or Quantity) ของผลการสืบค้น ซึ่งการค้นหาแบบเชิงความหมายจะถือว่ามีค่าระลึกเป็น 1 เพราะคำตอบที่ค้นคืนมาจะสอดคล้องกับข้อคำถามเสมอ กล่าวคือ ไม่ว่าจะเป็นการจับคู่แบบถูกต้อง แบบเจาะจง หรือแบบทั่วไป จะถือว่าทุกแบบสอดคล้องกับข้อคำถาม ในขณะที่การค้นหาข้อความแบบปกติ จะมีค่าระลึกที่ต่ำกว่า เพราะสามารถค้นคืนได้เฉพาะคำตอบที่จับคู่แบบถูกต้องเท่านั้น

บทที่ 5
สรุปผลการวิจัย

5.1 สรุปผลการวิจัย

ต้นแบบเครื่องมือการค้นหาผู้ให้บริการคลาวด์ที่สอดคล้องกับเมตริกซ์ควบคุมคลาวด์แบบเชิงความหมายที่นำเสนอนี้ ทำหน้าที่เป็นตัวกลางสำหรับผู้ใช้งานบริการคลาวด์ที่ต้องการค้นหาผู้ให้บริการคลาวด์ที่มีบริการที่มีความมั่นคง โดยได้ทำตามข้อปฏิบัติของเอกสารเมตริกซ์ควบคุมคลาวด์ ซึ่งมีอยู่ 16 ด้าน ผู้วิจัยได้สร้างออนโทโลจีความมั่นคงที่ได้จากการพิจารณาเอกสารเมตริกซ์ควบคุมคลาวด์เป็นหลัก และใช้แบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันเป็นส่วนเสริม เพื่อนำมาสร้างคำศัพท์ให้แก่ออนโทโลจีความมั่นคง แล้วจึงนำออนโทโลจีความมั่นคงที่พัฒนาขึ้นมา พัฒนาโปรแกรม 2 ตัว ได้แก่ โปรแกรมเพื่อสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการคลาวด์ และโปรแกรมเพื่อช่วยในการค้นหาผู้ให้บริการคลาวด์เชิงความหมาย โดยได้โปรไฟล์ของผู้ให้บริการคลาวด์ และโปรไฟล์ข้อคำถาม เพื่อนำมาใช้ในการจับคู่ความสัมพันธ์ระหว่างนิพจน์ความสัมพันธ์ ซึ่งมี 4 แบบ ได้แก่ การจับคู่อย่างถูกต้อง การจับคู่อย่างเจาะจง การจับคู่ทั่วไป และไม่จับคู่ จากการทดลองโดยใช้เครื่องมือการค้นหาเชิงความหมายที่พัฒนาขึ้นมานั้น สามารถค้นพบผู้ให้บริการที่ตรงกับความต้องการของผู้ใช้งานบริการคลาวด์ โดยถือว่ามีค่าระลึกที่ดีกว่าการค้นหาข้อความแบบปกติ เพราะการจับคู่ระหว่างนิพจน์ความสัมพันธ์ของโปรไฟล์ผู้ให้บริการ และโปรไฟล์ข้อคำถามนั้น ในการจับคู่เชิงความหมายทั้งจับคู่อย่างถูกต้อง จับคู่อย่างเจาะจง และจับคู่ทั่วไป จะถือว่าสอดคล้องกับข้อคำถามทั้งหมด และยังสะท้อนไปถึงคะแนนความคล้ายคลึงกันของการจับคู่ที่มีค่าสูงกว่ากรณีของการค้นหาข้อความแบบปกติ ผู้วิจัยเห็นว่าการค้นหาแบบเชิงความหมายจะเป็นประโยชน์กับผู้ใช้บริการคลาวด์ เพราะช่วยให้ค้นพบผู้ให้บริการคลาวด์ที่มีโปรไฟล์ด้านความมั่นคงใกล้เคียงกับที่ต้องการได้

5.2 ปัญหาและข้อจำกัด

ปัญหาและข้อจำกัดของงานวิจัยนี้มีดังนี้

1. แม้จะมีประโยชน์ในการช่วยผู้ใช้งานบริการคลาวด์ในการเลือกผู้ให้บริการคลาวด์ที่มีคุณภาพ แต่เครื่องมือที่นำเสนอยังต้องให้ผู้ให้บริการคลาวด์ทำการสร้างโปรไฟล์ความมั่นคงผ่านส่วนต่อประสานผู้ใช้ของระบบ อีกทั้งการระบุข้อมูลลงในโปรไฟล์ยังต้องให้สอดคล้องกับข้อมูลในแบบการประเมินตนเองในสตาร์ และในหน้าเว็บของผู้ให้บริการ การสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการจึงยาก เนื่องจากต้องประเมินตนเองและหน้าเว็บเพื่อให้เกิดความสอดคล้อง และต้องทำความเข้าใจหลักการหรือคำศัพท์ต่าง ๆ ในออนโทโลจีความมั่นคงซึ่งมีจำนวนมาก

2. งานวิจัยนี้เน้นที่การสร้างออนโทโลจีโดยยึดเอกสารเมตริกซ์ควบคุมคลาวด์ และแบบสอบถามที่เป็นที่เห็นพ้องต้องกันเท่านั้น ในปัจจุบันมีออนโทโลจีด้านความมั่นคงที่มีอยู่แล้วแต่ไม่ได้นำมาพิจารณา เนื่องจากต้องทำความเข้าใจเนื้อหาทางเทคนิคเชิงลึก ซึ่งมีศัพท์เฉพาะทางเป็นจำนวนมาก ออนโทโลจีที่ได้จึงยังไม่ใช่ออนโทโลจีที่แสดงองค์ความรู้ด้านความมั่นคงที่สมบูรณ์
3. การวิเคราะห์คำศัพท์เพื่อนำมาสร้างออนโทโลจีความมั่นคงทำได้ค่อนข้างยาก เนื่องจากเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกันเป็นเอกสารที่มีเนื้อหาทางเทคนิคเชิงลึก และเชื่อมโยงไปยังเอกสารมาตรฐานอื่นอีกเป็นจำนวนมาก การแยกประเภทว่าคำศัพท์ใดควรเป็นกิจกรรมหรือผลผลิตจากการกระทำก็ทำได้ยาก ออนโทโลจีความมั่นคงที่ผู้วิจัยเสนอจึงยังเป็นเพียงกลุ่มของคำศัพท์เบื้องต้นที่นำมาจากเนื้อหาในเอกสารเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

5.3 แนวทางการวิจัยต่อไป

แนวทางในการพัฒนางานวิจัยนี้ต่อมีดังนี้

1. เนื่องจากตอนนี้งานวิจัยได้วิเคราะห์ความหมายของคำศัพท์ เฉพาะตามลำดับชั้นในออนโทโลจี โดยไม่ได้วิเคราะห์รูปคำที่ใกล้เคียงกันหรือคำศัพท์ที่มีความหมายเหมือนกัน ดังนั้นแนวทางการพัฒนาต่อก็คือการวิเคราะห์ความหมายของคำศัพท์ในออนโทโลจีเพิ่มเติม เพื่อทำให้เป็นการวิเคราะห์เชิงความหมายมากขึ้น
2. เนื่องจากการสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการยังทำได้ยาก เนื่องจากต้องประเมินตนเองและหน้าเว็บเพื่อให้เกิดความสอดคล้อง และต้องทำความเข้าใจคอนเซปต์หรือคำศัพท์ต่าง ๆ ในออนโทโลจีความมั่นคงซึ่งมีจำนวนมาก ดังนั้นแนวทางการพัฒนาต่อคือ ทำการสร้างโปรไฟล์ความมั่นคงของผู้ให้บริการอย่างอัตโนมัติ โดยทำการสกัดคำศัพท์จากหน้าเว็บของผู้ให้บริการหรือข้อมูลการประเมินตนเองในสตาร์อย่างอัตโนมัติ
3. เนื่องจากในปัจจุบันมีออนโทโลจีด้านความมั่นคงที่มีอยู่แล้วแต่ไม่ได้นำมาพิจารณาในการสร้างออนโทโลจี เช่นงานวิจัยของ Bill Tsoumas และ Dimitris Gritzalis [12] ได้พูดถึงออนโทโลจีด้านความมั่นคง ซึ่งสามารถนำมาเป็นส่วนเสริมในการเพิ่มประสิทธิภาพของออนโทโลจีได้ รวมถึงออนโทโลจีด้านความมั่นคงของงานวิจัยของ Carlos Blanco [13] ดังนั้นแนวทางการพัฒนาต่อคือ การนำออนโทโลจีความมั่นคงเหล่านั้นมาทำการเพิ่มคอนเซปต์ให้กับออนโทโลจีความมั่นคงของคลาวด์เพื่อให้มีความสมบูรณ์ขึ้น

เนื่องจากการจับคู่เชิงความหมาย มีเพียง 4 แบบได้แก่ การจับคู่อย่างถูกต้อง การจับคู่อย่างเจาะจง การจับคู่ทั่วไป และไม่จับคู่ ดังนั้นแนวทางการพัฒนาต่อคือ การเพิ่มความสามารถให้กับการจับคู่เชิงความหมายเช่นการพิจารณาการจับคู่แบบบางส่วน (Partial Match) ซึ่งเป็นการจับคู่นิพจน์ความสัมพันธ์ที่มีบรรพบุรุษร่วมกัน แต่ไม่ใช่พ่อ-ลูกกันโดยตรง

รายการอ้างอิง

1. *Cloud Hosting Directory. Cloud Directory.* 2013 [cited 2013 August]; Available from: http://www.clouddir.com.
2. *Cloud Security Alliance. Cloud Controls Matrix.* 2013 [cited 2013 August]; Available from: https://cloudsecurityalliance.org/research/ccm.
3. *Cloud Security Alliance. Consensus Assessments Initiative Questionnaire.* 2013 [cited 2013 August]; Available from: https://cloudsecurityalliance.org/research/cai.
4. *Cloud Security Alliance. Trust & Assurance Registry (STAR).* 2013 [cited 2013 August]; Available from: https://cloudsecurityalliance.org/star/.
5. Chandrasekaran, B., and J.R. Josephson, *What are ontologies, and why do we need them?*, in *IEEE Intelligent systems 14.1 (1999)*. p. 20-26.
6. Han, T. and K.M. Sim, *An ontology-enhanced cloud service discovery system*, in *Proc. Int. MultiConf. Engineers and Computer Scientists, Hong Kong*. 17-19 March 2010. p. 483-490.
7. Kang, J. and K.M. Sim, *Towards agents and ontology for cloud service discovery*, in *Proc. Int. Conf. Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2011), Beijing, China*. 10-12 October 2011. p. 483-490.
8. Zhang, M., et al., *An Ontology-based System for Cloud Infrastructure Services' Discovery*, in *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2012 8th International Conference*. p. 524-530.
9. Modica, G.D. and O. Tomarchio, *Semantic security policy matching in service oriented architectures*, in *Proc. 2011 IEEE World Congress on Services (SERVICES 2011), Washington, DC*. 4-9 July 2011. p. 399-405.
10. Bhensook, N. and T. Senivongse, *An assessment of security requirements compliance of cloud providers*, in *Proc. 2012 IEEE 4th Int. Conf. Cloud Computing Technology and Science (CloudCom 2012), Taipei, Taiwan*. 3-6 December 2012. p. 520-525.
11. Sriharee, N. and T. Senivongse, *Matchmaking and ranking of semantic Web services using integrated service profile*, in *Int. J. Metadata, Semantics, and Ontologies, vol. 1, no. 2*. October 2006. p. 100-118.
12. TSOUMAS, B., and GRITZALIS, *Towards an Ontology-based Security Management*, in *in the 20th International Conference on Advanced Information Networking and Applications (AINA'06)*. 2006. p. 985-992.

13. Blanco1, C., et al, *A Systematic Review and Comparison of Security Ontologies*, in *Third International Conference on Availability, Reliability and Security (ARES 2008)*. Barcelona, Spain, 4-7 March 2008. p. 813-820.

ภาคผนวก

ภาคผนวก ก. คำศัพท์ในออนโทโลจี

ตารางที่ ก.1 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Application & Interface Security

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Application_Security	Utilize_industry_standard Automated_sourceCode_analysis Detect_code_defect Design_review Code_review Detect_vulnerability Vulnerability_scan	
Customer_Access_Requirements	Granting_customers_access	Regulatory_requirement
Data_Integrity		
Data_Security_and_Integrity	Designed_using_industry_standard	FedRAMP_requirement

ตารางที่ ก.2 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Audit Assurance & Compliance

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Audit_Planning	SSAE16_audit SSAE16SOC1Type1_audit SSAE16SOC1Type2_audit Independent_audit SAS70 Guideline_by_AICPA Guideline_by_SOC2	Industry_certification ISO20000_certification ISO27001_certification Independent_audit_report SSAE16_report SSAE16SOC1Type1_report SSAE16SOC1Type2_report SSAE16SOC2Type2_report
Independent_Audits	Vulnerability_scan WebApplication_vulnerability_scan AdHoc_scan Internal_audit External_audit SSAE16SOC1Type1_audit Penetration_test Network_penetration_test Application_penetration_test	SSAE16_report Internal_audit_plan External_audit_plan Result_of_penetration_test Result_of_network_penetration_test Result_of_application_penetration_test ISO27001_audit_report Third_party_audit_report Audit_report
Information_System_Regulatory_Mapping	Logical_separation Granular_recovery Recovery_data Recovery_image Data_encryption Fully_encrypted Physical_separation	

ตารางที่ ก.3 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Business Continuity Management & Operational Resilience

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Business_Continuity_Planning		Geographically_resilient MultiSite_operation_plan Infrastructure_service_failaver
Business_Continuity_Testing	Disaster_recovery_test	Business_continuity_plan Regular_recovery_drill ISO27001_certified
Datacenter_Utilities_and_Environmental_Contitions	Legal_jurisdiction	
Documentation		
Environmental_Risks	Physical_protection_against_damage	
Equipment_Location	High_impact_environmental_risk Designed_resist_earthquakes Physical_and_environmental_security	
Equipment_Maintenance		
Equipment_Power_Failures	Protect_equipment Separate_power_substation Datacenter_location	
Impact_Analysis		SLA_data_report Security_metric Visibility_and_reporting
Management_Program	Defining_business_continuity Disaster_recovery	Disaster_recovery_plan ISO27001_certified
Policy		Policies_and_Procedure
Retention_Policy		Data_rentation_policy Response to requir_for_data

ตารางที่ ก.4 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Change Control & Configuration Management

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
New_Development_and _Acquisition	Management_authorization Extensive_testing	ISO27001_requirement
Outsourced_Developme nt	Detect_source_code_security_defects Source_code_review Vulnerability_scan	Test_plan
Quality_Testing	QA_process	Document_of_quality_assurance ISO20000_certified ISO9001_certified
Unauthorized_Software_ Installations	Restrict_and_monitor_installation	ISO20000_certified ISO27001_certified
Production_Changes	Notiify_customer	Document_of_production_change

ตารางที่ ก.5 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Data Security & Information Lifecycle Management

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Classification		Tag Metadata Geographic_location Built_on_Amazon_AWS
Data_Inventory_and_Flows		
eCommerce_Transactions	Open_encryption_methodology	
Handling_and_Labeling_and_Security_Policy		Labeling Handing Security_policy
Information_Leakage	DLD Prevent_data_leakage	
Non-Production_Data	Data_replication Follow_ISO27001	
Ownership_and_Stewardship	Follow_ISO15489 Follow_Oasis_XML Follow_CSA Follow_ISO27001 Follow_data_label_standard Data_classification	
Secure_Disposal	Degauss_HardDisk Cryptographic_wiping Multiple_pass_data_wiping	

ตารางที่ ก.6 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Datacenter Security

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Asset_Management	Maintain_inventory_of_critical_asset Maintain_inventory_of_critical_supplier	
Controlled_Access_Points	Physical_security_control Biometric_scan Electronic_access_card	
Equipment_Identification	Connection_authentication Automation_network_analysis	
Off-Site_Authorization		Snapshots_of_storage Document_describes_scenarios Document_for_application_service SSAE16SOC1Type2_report
Off-Site_Equipment		Document_describes_policy_and_procedures
Policy	OHSAS18001 SA8000	Maintaining_a_secure_work_outline ISO27001_certification Human_safety_and_security
Secure_Area_Authorization		Geographic_location Legal_jurisdiction
Unauthorized_Persons_Entry	Physical_security_control Biometric_scan Electronic_access_card 7x24guards CCTV_cameras Unauthorized_personel Two_factor_authentication 24x7x365 Monitor_access_control	
User_Access	Background_verification	

ตารางที่ ก.7 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Encryption & Key Management

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Entitlement		
Key_Generation	Manage_encryption_keys Leverage_encryption Maintain_key_management	Public keys Private keys revocation
Sensitive_Data_Protection	Generated_encryption_keys Creation_unique_encryption_keys Data_encryption Manage_encryption	Public keys Private keys revocation
Storage_and_Access		

ตารางที่ ก.8 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Governance and Risk Management

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Baseline_Requirements	Vulnerability_scan Continuous_monitor_and_report Virtual_machine_image	Document_of_information_security_baseline
Data_Focus_Risk_Assessments	Internal_monitoring Nagios_monitoring Continuous_monitoring Infrastructure_monitoring Amazon_monitoring Healt_monitoring	SIM_and_SEM_service
Management_Oversight	Maintain_awareness_security_policy	
Management_Program		Document_describes_ISMP
Management_SupportandInvolvement	Verification_of_assignment Action_to_support_information_security Review_security_management_status Streeing_committee Management_commitment	
Policy	Continuously_update_control_mapping_document	Security_policy NIST ISO27001 CoBit ISO20000
Policy_Enforcement	Review_violation Disciplinary_action_for_violation	
Policy_Impact_on_Risk_Assessments	Review_policies_and_procedures Change_policies_and_procedures	
Policy_Reviews	Notify_material_change	
Risk_Assessments	Formal_risk_assessment Likelihood_and_impact	
Risk_Management_Framework	Remumerateted_SLA	Professional_liability_policy
Risk_Mitigation_and_Acceptance	Risk_mitigated Risk_review Risk_identified Risk_categorized	

ตารางที่ ก.9 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Human Resources

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Asset_Returns		
Background_Screening	Background_verification	
Employment_Agreements	Tracked_and_audited_training Information_security_training	
Employment_Termination	Employee_termination Audited_employee_exit	
Industry_Knowledge_and_Benchmarking	Benchmark_security_control Participate_in_industrygroup	
Mobile_Device_Management		
Non-Disclosure_Agreements		Non_disclosure_agreement
Roles_and_Responsibilities		Responsibility_role
Technology_Acceptable_Use	No_access_customer_data	Inspection_technologies Acceptable_policy
Training_and_Awareness	Security_awareness_training Staff_receive_training Third_party_training	
User_Responsibility	Maintain_awareness_security_policy	
Workspace	Follow_SLA_Standard Temper_audit Track_log_for_audit Unauthorize_access_data	

ตารางที่ ก.10 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Identity & Access Management

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Audit_Tools_Access	Restrict_log_and_monitor_access	
Credential_Lifecycle_and_Provision_Management	Tracked_employee_exit Audited_employee_exit Timely_removal_of_user_access	
Diagnostic_and_Configuration_Ports_Access	Dedicated_network	
Policies_and_Procedures		
Segregation_of_Duties		Segregation_of_duty_documentation
Source_Code_Access_Restriction	Prevent_unauthorize_access	
Third_Party_Access	Multi_failure_disaster_recovery Disaster_recovery Monitor_service_continuity Access_operational_redundancy Share_business_continuity	
Trusted_Sources	Approve_access_data Data_classification Access_control Benchmark_security_control Participate_in_industrygroup	
User_Access_Authorization	Approve_access_data Data_classification Access_control	
User_Access_Reviews	Access_right_check Review_of_certification Remediction_action_record Certification_action_record	Certification_report SSAE16SOC1Type1_report SSAE16SOC1Type2_report
User_Access_Revocation	Modification_of_user_access Revocation_of_user_access Termination_of_employment	
User_ID_Credentials	Single_sign_on Delegate_authentication Support_SAML Support_identity_federation	Policy_enforment_point_capability Identity_management_system
Utility_Programs_Access	Prevent_unauthorize_access Detect_attack Virtualization_management	

ตารางที่ ก.11 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Infrastructure & Virtualization Security

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Audit_Logging_and_Intrusion_Detection	Physical_and_logical_useraccess Audit_log_restrict	Network_infrusion_detection Mapping_of_regulation
Change_Detection		
Clock_Synchronization		Synchrozization_time_service
Information_System_Documentation	Restrict_use_memory Capacity_management Capacity_planning	
Management_Vulnerability_Management		
Network_Security		Guildline_to_create_layer_security_architecture
OS_Hardening_and_Base_Conrols		
Production_and_Non-Production_Environments	Logical_separation	
Segmentation	Logical_separation	
VM_Security_vMotion_Data_Protection		
VMM_Security_Hypervisor_Hardening		
Wireless_Security		

ตารางที่ ก.12 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Interoperability & Portability

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
APIs		
Data_Request		
Policy_and_Legal		
Standardized_Network_ Protocols		
Virtualization		

ตารางที่ ก.13 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Mobile Security

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Anti-Malware		
Application_Stores		
Approved_Applications		
Approved_Software_for_BYOD		
Awareness_and_Training		
Cloud_Based_Services		
Compatibility		
Device_Eligibility		
Device_Inventory		
Device_Management		
Encryption		
Jailbreaking_and_Rooting		
Legal		
Lockout_Screen		
Operating_Systems		
Passwords		
Policy		
Remote_Wipe		
Security_Patches		
Users		

ตารางที่ ก.14 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Security Incident Management, E-Discovery & Cloud Forensics

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Contact_and_Authority_Maintenance		
Incident_Management		Incident_management_plan Incident_response_plan
Incident_Reporting	Logging_and_monitoring Event_management	
Incident_Response_Legal_Preparation	Support_legal_hold	Incident_response_plan
Incident_Response_Metrics	Statical_informaton_incident_data Quantify_and_monitoring	

ตารางที่ ก.15 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Supply Chain Management, Transparency and Accountability

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Data_Quality_and_Integrity		
Incident_Reporting		
Network_and_Infrastructure_Services		Capacity_plan Utilization_report
Provider_Internal_Assessments		
Supply_Chain_Agreements	Review_third_party_agreement	
Supply_Chain_Governance_Reviews		
Supply_Chain_Metrics		
Third_Party_Assessment		
Third_Party_Audits		

ตารางที่ ก.16 คำศัพท์ในออนโทโลจีของความมั่นคงด้าน Threat and Vulnerability Management

คำศัพท์ในออนโทโลจี		
Control Domain	Activity	Product
Anti-Virus_and_Malicious_Software		Security_treat_detection_system AntiVirus_software AntiMalware_software
Vulnerability_and_Patch_Management	Network_vulnerability_scan Application_vulnerability_scan System_vulnerability_scan	Result_of_vulnerability_scan Patch_timeframe
Mobile_Code	Mobile_code_authorized Code_configuration_check	

ภาคผนวก ข. คำศัพท์ในคลาส Activity และ Product

ตารางที่ ข.1 คำศัพท์ในคลาส Activity โดยแบ่งเป็นคลาสย่อย

คำศัพท์ในออนโทโลจี คลาส Activity		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Independent_audit	SSAE16SOC1Type1_audit SSAE16SOC1Type2_audit	
Independent_audit	SAS70	
Guideline_by_AICPA		
Guideline_by_SOC2		
Vulnerability_scan	WebApplication_vulnerability_scan Network_vulnerability_scan Application_vulnerability_scan System_vulnerability_scan	
AdHoc_scan		
Internal_audit		
External_audit		
Penetration_test	Network_penetration_test Application_penetration_test	
Logical_separation		
Physical_separation		
Granular_recovery		
Recovery_data	Recovery_image	
Data_encryption	Fully_encrypted Manage_encryption Generated_encryption_keys Manage_encryption_keys Leverage_encryption Maintain_key_management Creation_unique_encryption_keys Open_encryption_methodology	
Data_classification		
Follow_standard	Follow_ISO15489 Follow_Oasis_XML Follow_CSA Follow_ISO27001 Follow_data_label_standard Follow_SLA_Standard	
Degauss_HardDisk		
Cryptographic_wiping		
Multiple_pass_data_wiping		

ตารางที่ ข.1 คำศัพท์ในคลาส Activity โดยแบ่งเป็นคลาสย่อย (ต่อ)

คำศัพท์ในออนโทโลจี คลาส Activity		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Data_replication		
DLD		
Prevent_data_leakage		
Internal_monitoring	Nagios_monitoring Continuous_monitoring	
Infrastructure_monitoring	Amazon_monitoring	
Healt_monitoring		
OHSAS18001		
SA8000		
Background_verification		
Physical_security_control	Biometric_scan Electronic_access_card 7x24guards CCTV_cameras Unauthorized_personel Two_factor_authentication 24x7x365 Monitor_access_control	
Maintain_inventory_of_critical_asset		
Maintain_inventory_of_critical_supplier		
Information_security_training	Tracked_and_audited_training	
Employee_termination	Tracked_employee_exit Audited_employee_exit	
Verification_of_assignment		
Action_to_support_information_security		
Review_security_management_status		
Streeing_committee		
Management_commitment		
Continuously_update_control_mapping_document		
Information_security_baseline		
Continuous_monitor_and_report		
Virtual_machine_image		
Notify_material_change		
Review_violation		
Disciplinary_action_for_violation		

ตารางที่ ข.1 คำศัพท์ในคลาส Activity โดยแบ่งเป็นคลาสย่อย (ต่อ)

คำศัพท์ในออนโทโลจี คลาส Activity		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Access_control	Timely_removal_of_user_access Approve_access_data Termination_of_employment Modification_of_user_access Revocation_of_user_access Unauthorize_access_data	
Certification_action_record		
Access_right_check		
Review_of_certification		
Remediction_action_record		
Security_awareness_training	Staff_receive_training Third_party_training	
Benchmark_security_control		
Participate_in_industrygroup		
Maintain_awareness_security_policy		
Temper_audit		
Regulatory_compliance		
Logging_and_monitoring	Track_log_for_audit	
Quantify_and_monitoring		
Event_management		
Support_legal_hold		
No_access_customer_data		
Statical_informaton_incident_data		
Restrict_log_and_monitor_access		
Dedicated_network		
Prevent_unauthorize_access	Detect_attack	
Virtualization_management		
Review_third_party_agreement		
Restrict_use_memory		
Capacity_management		
Capacity_planning		
Remumerateted_SLA		
Formal_risk_assessment		
Likelihood_and_impact		
Risk_mitigated		
Risk_review		
Risk_identified		

ตารางที่ ข.1 คำศัพท์ในคลาส Activity โดยแบ่งเป็นคลาสย่อย (ต่อ)

คำศัพท์ในออนโทโลจี คลาส Activity		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Risk_categorized		
Review_policies_and_procedures		
Change_policies_and_procedures		
Monitor_service_continuity		
Access_operational_redundancy		
Share_business_continuity		
Disaster_recovery	Multi_failure_disaster_recovery Disaster_recovery_test	
Management_authorization		
Extensive_testing		
Notiify_customer		
QA_process		
Detect_source_code_security_defects		
Source_code_review		
Restrict_and_monitor_installation		
Defining_business_continuity		
Physical_protection_against_damage	High_impact_environmental_risk Designed_resist_earthquakes	
Physical_and_environmental_security		
Protect_equipment	Separate_power_substation	
Datacenter_location		
Legal_jurisdiction		
Granting_customers_access		
Single_sign_on		
Delegate_authentication		
Support_SAML		
Support_identity_federation		
Designed_using_industry_standard		
Utilize_industry_standard		
Automated_sourceCode_analysis		
Detect_code_defect		
Design_review		
Code_review		
Detect_vulnerability		
Connection_authentication		
Automation_network_analysis		

ตารางที่ ข.1 คำศัพท์ในคลาส Activity โดยแบ่งเป็นคลาสย่อย (ต่อ)

คำศัพท์ในออนโทโลจี คลาส Activity		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Physical_and_logical_useraccess		
Audit_log_restrict		
Mobile_code_authorized		
Code_configuration_check		

ตารางที่ ข.2 คำศัพท์ในคลาส Product โดยแบ่งเป็นคลาสย่อย

คำศัพท์ในออนโทโลจี คลาส Product		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Industry_certification	ISO20000_certification ISO27001_certification	
Audit_report	Independent_audit_report ISO27001_audit_report Third_party_audit_report	
	SSAE16_report	SSAE16SOC1Type1_report SSAE16SOC1Type2_report SSAE16SOC2Type2_report
Audit_plan	Internal_audit_plan External_audit_plan	
Result_of_penetration_test	Result_of_network_penetration_test Result_of_application_penetration_test	
Tag		
Metadata		
Geographic_location		
Built_on_Amazon_AWS		
Labeling		
Handing		
SIM_and_SEM_service		
Legal_jurisdiction		
Policies_and_Procedure	Security_policy	Data_rentation_policy NIST ISO27001 CoBit ISO20000
	Maintaining_a_secure_work_outline Response to requir_for_data Acceptable_policy Professional_liability_policy Policy_enforment_point_capability Human_safety_and_security	
Snapshots_of_storage		
Document_describes_ISMP		
Document_describes_policy_and_procedures		
Document_describes_scenarios		
Document_for_application_service		
Document_of_information_security_baseline		

ตารางที่ ข.2 คำศัพท์ในคลาส Product โดยแบ่งเป็นคลาสย่อย (ต่อ)

คำศัพท์ในออนโทโลจี คลาส Product		
Main Class	Sub Class Lv.1	Sub Class Lv.2
Certification_report		
Responsibility_role		
Segregation_of_duty_documentation		
Result_of_vulnerability_scan		
Patch_timeframe		
Security_treat_detection_system	AntiVirus_software AntiMalware_software	
Incident_management_plan	Incident_response_plan	
Inspection_technologies		
Capacity_plan		
Utilization_report		
Non_disclosure_agreement		
Document_of_production_change		
Document_of_quality_assurance		
Industry_certified	ISO20000_certified ISO9001_certified ISO27001_certified	
ISO27001_requirement		
Test_plan		
Disaster_recovery_plan		
SLA_data_report		
Security_metric		
Visibility_and_reporting		
Business_continuity_plan		
MultiSite_operation_plan		
Geographically_resilient		
Regular_recovery_drill		
Infrastructure_service_failaver		
Regulatory_requirement		
Identity_management_system		
FedRAMP_requirment		
Guildline_to_create_layer_security_architecture		
Synchrozization_time_service		
Network_infrusion_detection		
Mapping_of_regulation		

ภาคผนวก ค. ตัวอย่างของเมตริกซ์ควบคุมคลาวด์และแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

ตารางที่ ค.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์

Control Domain	Control ID	Control Specification
Audit Assurance & Compliance *Audit Planning*	AAC-01	Audit plans, activities, and operational action items focusing on data duplication, access, and data boundary limitations shall be designed to minimize the risk of business process disruption. Audit activities must be planned and agreed upon in advance by stakeholders.
Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following:
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.

ตารางที่ ค.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain	Control ID	Control Specification
Data Security &Information Lifecycle Management *Classification*	DSI-01	Data and objects containing data shall be assigned a classification based on data type, jurisdiction of origin, jurisdiction domiciled, context, legal constraints, contractual constraints, value, sensitivity, criticality to the organization, third-party obligation for retention, and prevention of unauthorized disclosure or misuse.
Datacenter Security *Asset Management*	DCS-01	Assets must be classified in terms of business criticality in support of dynamic and distributed physical and virtual computing environments, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly (or in real-time), and assigned ownership supported by defined roles and responsibilities, including those assets used, owned, or managed by customers (tenants).
Encryption & Key Management *Entitlement*	EKM-01	All entitlement decisions shall be derived from the identities of the entities involved. These shall be managed in a corporate identity management system. Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.

ตารางที่ ค.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain	Control ID	Control Specification
Governance and Risk Management *Baseline Requirements*	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and established and authorized based on business need.
Human Resources *Asset Returns*	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally-owned assets shall be returned within an established period.
Identity & Access Management *Audit Tools Access*	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.

ตารางที่ ค.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain	Control ID	Control Specification
Infrastructure & Virtualization Security *Audit Logging / Intrusion Detection*	IVS-01	Higher levels of assurance are required for protection, retention, and lifecyle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.
Interoperability & Portability *APIs*	IPY-01	The provider shall use open and published APIs to ensure the broadest support for interoperability between components and to facilitate migrating applications.
Security Incident Management, E-Discovery & Cloud Forensics *Contact / Authority Maintenance*	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.

ตารางที่ ค.1 ตัวอย่างของเมตริกซ์ควบคุมคลาวด์ (ต่อ)

Control Domain	Control ID	Control Specification
Mobile Security *Anti-Malware*	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.
Threat and Vulnerability Management *Anti-Virus / Malicious Software*	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components..
Supply Chain Management, Transparency and Accountability *Data Quality and Integrity*	STA-01	Providers shall inspect, account for, and correct data quality errors and risks inherited from partners within their cloud supply-chain. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.

ตารางที่ ค.2 ตัวอย่างของแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน

Control Domain	CGID	CID	Consensus Assessment Question
Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?
Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?
		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?
		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?
		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?

ตารางที่ ค.2 ตัวอย่างของแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน (ต่อ)

Control Domain	CGID	CID	Consensus Assessment Question
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?
		CO-02.7	Are the results of internal and external audits available to tenants at their request?
Background Screening	HR-01	HR-01.1	Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background verification?
	HR-02	HR-02.1	Do you specifically train your employees regarding their role vs. the tenant's role in providing information security controls?
		HR-02.2	Do you document employee acknowledgment of training they have completed?
Employment Termination	HR-03	HR-03.1	Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?

ตารางที่ ค.2 ตัวอย่างของแบบสอบถามการประเมินที่เป็นที่เห็นพ้องต้องกัน (ต่อ)

Control Domain	CGID	CID	Consensus Assessment Question
Management Program	IS-01	IS-01.1	Do you provide tenants with documentation describing your Information Security Management Program (ISMP)?
Management Support / Involvement	IS-02	IS-02.1	Are policies in place to ensure executive and line management take formal action to support information security through clear documented direction, commitment, explicit assignment and verification of assignment execution?
Policy	IS-03	IS-03.1	Do your information security and privacy policies align with particular industry standards (ISO-27001, ISO-22307, CoBIT, etc.)?

ประวัติผู้เขียนวิทยานิพนธ์

นายจักรินทร์ ทวีจินดา เกิดเมื่อวันที่ 30 ธันวาคม พ.ศ. 2531 ที่จังหวัดมหาสารคาม สำเร็จการศึกษาระดับปริญญาตรีหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ปีการศึกษา 2554 และเข้าศึกษาต่อในหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิศวกรรมซอฟต์แวร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ในปีการศึกษา 2555