บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

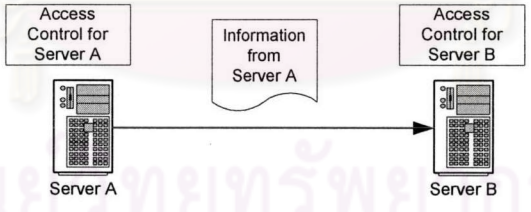
เทคโนโลยีกริด (Grid Technology) [2] เป็นเทคโนโลยีในสาขาระบบแบบกระจาย (Distributed System Technology) ซึ่งกำลังได้รับความนิยมในปัจจุบันอันเนื่องมาจากความสามารถในการควบคุมการใช้ทรัพยากรร่วมกันระหว่างหลายองค์กรที่ได้ตกลงถึงความต้องการในการใช้ทรัพยากรของแต่ละฝ่ายเพื่อให้บรรลุวัตถุประสงค์อย่างใดอย่างหนึ่งร่วมกัน โดยกลุ่มขององค์กรที่ตกลงจะใช้ทรัพยากรร่วมกันจะเรียกอีกอย่างหนึ่งได้ว่าเป็นองค์กรเสมือน (VO: Virtual Organization)

ลักษณะการควบคุมการขอเข้าใช้ทรัพยากรของสมาชิกภายในองค์กรเสมือนของระบบกริด จะเน้นให้เจ้าของทรัพยากรสามารถควบคุมการใช้ทรัพยากรของตนเองได้ กล่าวคือในการเข้าใช้ ผู้ขอใช้จะต้องติดต่อกับระบบรักษาความปลอดภัยที่มีอยู่เดิมภายในแต่ละทรัพยากรย่อยๆ ซึ่งระบบรักษาความปลอดภัยอาจจะอยู่ในรูปของระบบปฏิบัติการยูนิกซ์ (Unix) หรือระบบรักษาความปลอดภัยเคอเบรอส (Kerberos) จะเห็นได้ว่าระบบกริดจะไม่ไปแทนที่ระบบรักษาความปลอดภัยที่มีอยู่เดิม ดังนั้น หัวใจสำคัญของการควบคุมการขอเข้าใช้ทรัพยากรภายในระบบกริด จึงจะอยู่ในรูปของการเปรียบเทียบระหว่างชื่อของผู้ใช้ทั่วไปภายในองค์กรเสมือนกับชื่อสมาชิกที่ระบบรักษาความปลอดภัยของทรัพยากรย่อยเป็นผู้กำหนด ตัวอย่างเช่น ระบบโกลบัส [2] จะควบคุมการขอใช้ทรัพยากรโดยอาศัยการกำหนดชื่อเอกเทศ (Distinguished Name) ของผู้ใช้แต่ละคน ก่อนที่จะนำไปเปรียบเทียบกับชื่อของผู้ใช้งานภายในแต่ละทรัพยากร (Local Name) ที่อยู่ภายในไฟล์ควบคุม (Gridmapfile) อีกทีหนึ่ง

ลักษณะการเก็บรวบรวมข้อมูลภายในระบบกริดจะถูกแบ่งออกเป็นสองส่วนหลักๆได้แก่ หน่วยเก็บข้อมูลภายในแต่ละทรัพยากรย่อยๆ และ หน่วยบริการสารบัญข้อมูล (Directory Service) ซึ่งหน่วยบริการสารบัญข้อมูลจะทำหน้าที่เก็บรวบรวมสารบัญข้อมูลจากแต่ละหน่วยย่อยๆเพื่อให้สมาชิกภายในองค์กรเสมือนสามารถสืบค้นข้อมูลที่ตนต้องการได้อย่างสะดวก ตัวอย่างเช่น ระบบโกลบัสจะมีบริการเอ็มดีเอส (MDS: Monitoring and Discovering Service)

[9] ซึ่งถูกพัฒนามาจากมาตรฐานแอลแด็ป (LDAP : Lightweight Directory Access Protocol) [7] โดยภายในบริการเอ็มดีเอสจะถูกแบ่งออกเป็นสองส่วนย่อยๆได้แก่จีอาร์ไอเอส (GRIS : Grid Resource Information Service) ซึ่งจะทำหน้าที่เก็บข้อมูลของแต่ละทรัพยากรย่อย และจีไอไอเอส (Grid Information Index Service) ที่ทำหน้าที่เก็บรวบรวมสารบัญข้อมูล ตามที่ได้ถูกกำหนดไว้ในระบบโกลบัสตามลำดับ

ระบบข้อมูลภายในของระบบกริดได้ถูกออกแบบบนพื้นฐานของการนำไปใช้ในงานวิจัยทางวิทยาศาสตร์ที่มองว่าข้อมูลต่างๆสามารถใช้งานร่วมกันโดยไม่จำเป็นต้องมีมาตรการควบคุมแต่อย่างใด จึงทำให้ระบบโกลบัสในปัจจุบันไม่สามารถควบคุมทรัพยากรประเภทสามารถทำซ้ำได้ (Replicatable Resource) ตัวอย่างเช่น ข้อมูลที่แสดงสภาพการทำงานปัจจุบันของทรัพยากรภายในระบบโกลบัส หรือ ข้อมูลทั่วไปที่เกี่ยวข้องกับงานที่กำลังถูกประมวลผลอยู่ จะมีเฉพาะตัวข้อมูลเท่านั้นที่ถูกคัดลอกและถูกส่งต่อกันระหว่างแต่ละเซิร์ฟเวอร์ดังที่แสดงในรูปที่ 1.1 การคัดลอกและส่งต่อนั้นจะทำได้โดยเซิร์ฟเวอร์ที่มีข้อมูลเครื่องใดก็ได้ซึ่งจะอยู่นอกเหนือการควบคุมของเจ้าของข้อมูล นอกจากนี้ถ้าผู้ใช้มีชื่ออยู่ภายในไฟล์ (Gridmapfile) ของเซิร์ฟเวอร์ที่มีข้อมูลที่ผู้ใช้ต้องการ ก็จะสามารถเรียกดูข้อมูลทั้งหมดที่ถูกเก็บอยู่ทั้งภายในหน่วยเก็บข้อมูลย่อย (จีอาร์ไอเอส) และหน่วยรวบรวมสารบัญข้อมูล (จีไอไอเอส) ภายในบริการเอ็มดีเอสของเครื่องนั้นๆได้ โดยที่ผู้ใช้อาจจะไม่มีสิทธิในการดูข้อมูลที่เซิร์ฟเวอร์เจ้าของข้อมูลเลย จากแนวโน้มของการนำกริดไปใช้ในภาคธุรกิจ ทำให้การควบคุมการเข้าถึงข้อมูลกลายเป็นประเด็นสำคัญเพราะในโลกธุรกิจจะถือว่าข้อมูลเป็นทรัพยากรประเภทหนึ่งที่จำเป็นจะต้องมีการควบคุมที่เหมาะสม

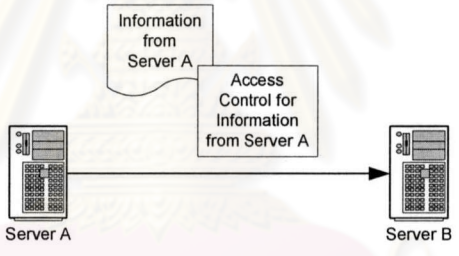


รูปที่ 1.1 แสดงการแบ่งแยกการควบคุมระหว่างไฟล์ควบคุมและตัวข้อมูล

ถึงแม้ในปัจจุบันจะมีงานวิจัยที่เกี่ยวข้องกับการควบคุมการเรียกดูข้อมูลที่ถูกเก็บภายในฐานข้อมูลของมาตรฐานแอลแด็ป [5] ซึ่งเป็นมาตรฐานที่ระบบโกลบัสรุ่น 2.0 ใช้ในการเก็บและแลกเปลี่ยนข้อมูลระหว่างเซิร์ฟเวอร์แต่ละเครื่อง แต่เนื่องจากงานวิจัยดังกล่าวจำเป็นที่จะต้องกำหนดไฟล์ควบคุมสิทธิการเรียกข้อมูลไว้เป็นส่วนหนึ่งของสตาร์ทอัพไฟล์ (Start-up file) ของแต่

ละเครื่อง จึงจำเป็นที่จะต้องไปกำหนดไฟล์ควบคุมสิทธิของแต่ละเครื่องด้วยตนเองซึ่งไม่เหมาะสมกับลักษณะการทำงานของระบบกริดที่มีจำนวนเซิร์ฟเวอร์จำนวนมาก นอกจากนี้ งานวิจัยอื่นๆเช่น งานวิจัยกริดเพื่อการเก็บรวบรวมข้อมูล (Datagrid) [3] ที่ถูกพัฒนาให้สามารถรองรับการเรียกใช้ไฟล์ต่างๆภายในระบบกริด โดยเพิ่มความสามารถที่จำเป็นดังเช่นการคัดลอกไฟล์ (Replica management service) และการเก็บรวบรวมรายละเอียดของข้อมูล (Metadata Catalog) แต่รูปแบบการควบคุมการเข้าถึงข้อมูลของงานวิจัยดังกล่าวยังไม่ครอบคลุมการควบคุมการเรียกดูข้อมูลที่ถูกคัดลอกและส่งต่อระหว่างแต่ละเซิร์ฟเวอร์

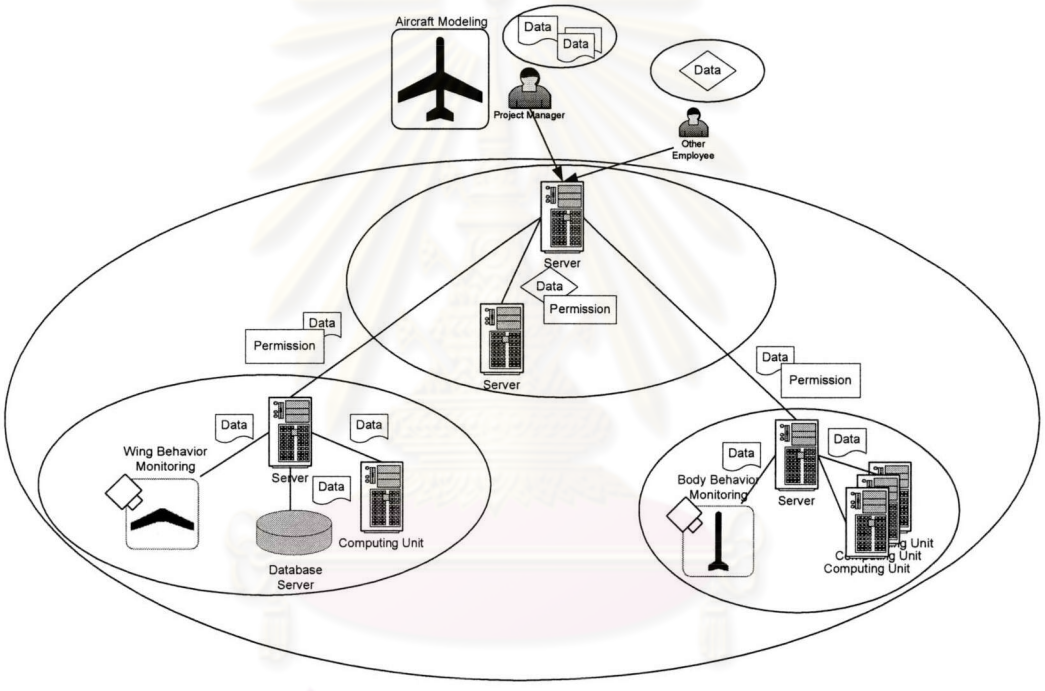
งานวิจัยนี้ได้มุ่งเน้นความสนใจในกระบวนการควบคุมการเรียกดูข้อมูลที่ถูกคัดลอกส่งต่อระหว่างแต่ละเซิร์ฟเวอร์ภายในระบบโกลบัส ซึ่งจะต้องเปิดโอกาสให้เจ้าของทรัพยากรที่เป็นต้นตอของข้อมูลสามารถควบคุมการเรียกดูข้อมูลของตน โดยจะอาศัยโครงสร้างการแลกเปลี่ยนข้อมูลเดิมของระบบโกลบัส ในการส่งข้อมูลควบคุมสิทธิในการเรียกดูข้อมูลไปพร้อมกับข้อมูลจริง เพื่อทำให้แน่ใจว่าเจ้าของข้อมูลสามารถควบคุมการเรียกดูข้อมูลของตนได้ไม่ว่าข้อมูลดังกล่าวจะถูกส่งต่อกันไปกี่ทอดภายในระบบโกลบัสก็ตาม ดังที่แสดงในรูปที่ 1.2



รูปที่ 1.2 แสดงลักษณะการส่งข้อมูลควบคุมไปพร้อมกับข้อมูลจริงโดยใช้โครงสร้างส่งข้อมูลเดิมของบริการเอ็มดีเอส

ในปัจจุบันมาตรฐานที่ใช้ในการแลกเปลี่ยนข้อมูลของระบบโกลบัสมีอยู่หลายรูปแบบ ได้แก่ บริการเอ็มดีเอสและบริการกริดเอฟทีพี (GridFTP) ซึ่งสามารถแลกเปลี่ยนข้อมูลระหว่างแต่ละเซิร์ฟเวอร์เพียงทอดเดียว (Peer-to-Peer) รวมไปถึงรูปแบบการกระจายข้อมูลของงานวิจัยกริดเพื่อการเก็บข้อมูล (Datagrid) จากการศึกษาพบว่าการกระจายข้อมูลทุกรูปแบบต่างก็ยังไม่มีโครงสร้างการควบคุมการเรียกดูข้อมูลของข้อมูลที่ถูกคัดลอกและส่งต่อให้แตกต่างตามสิทธิของผู้ใช้ จากข้อจำกัดดังกล่าว พบว่า การกระจายข้อมูลในกริดมีความจำเป็นที่จะต้องถูกควบคุมการเรียกดูให้ตรงกับสิทธิของผู้ใช้แต่ละคนเมื่อนำเอาระบบกริดไปใช้ภายในองค์กร เช่นนำไปใช้ในการ

ออกแบบโครงสร้างเครื่องบินที่จำเป็นต้องจำลองสภาวะการทำงานของแต่ละองค์ประกอบพร้อมๆ กัน เช่นการพิจารณาผลกระทบของระดับความสูงกับแต่ละส่วนของเครื่องบินเมื่อทำการแก้ไขโครงสร้างของเครื่องบินต้นแบบเป็นต้น ซึ่งการทดสอบในลักษณะดังกล่าวจำเป็นต้องใช้ทรัพยากรหลายประเภทไม่ว่าจะเป็นหน่วยประมวลผล, หน่วยเก็บรวบรวมข้อมูลหรือแม้กระทั่งอุปกรณ์อิเลคโทรนิคส์ประเภทเซนเซอร์ที่สามารถติดตั้งระบบกริดเพื่อควบคุมการใช้งานร่วมกัน โดยข้อมูลที่เกี่ยวข้องกับการทดสอบที่ได้จะถูกเก็บรวบรวมจากแต่ละทรัพยากรที่ติดตั้งระบบโกลบัสโดยบริการเอ็มดีเอสซึ่งจำเป็นจะต้องถูกควบคุมการเรียกดูข้อมูลของผู้ใช้เพื่อให้แน่ใจได้ว่าเฉพาะผู้ที่มีหน้าที่รับผิดชอบเกี่ยวกับการออกแบบเครื่องบินต้นแบบเท่านั้นจึงจะสามารถเรียกดูข้อมูลภายในบริการเอ็มดีเอสได้ ซึ่งจะมีลักษณะการทำงานดังรูปที่ 1.3



รูปที่ 1.3 แสดงรูปแบบการรวบรวมข้อมูลภายในระบบกริดเพื่อการออกแบบเครื่องบินต้นแบบ

จากรูปที่ 1.3 จะเห็นได้ว่าจะมีเฉพาะผู้ที่รับผิดชอบด้านการออกแบบเครื่องบินต้นแบบรุ่นใหม่เท่านั้น จึงจะสามารถเรียกดูข้อมูลที่เกี่ยวข้องกับการทดสอบเครื่องต้นแบบ ซึ่งจะป้องกันข้อมูลทางธุรกิจรั่วไหลไปยังผู้ที่ไม่มีส่วนเกี่ยวข้องภายในบริษัท

เนื่องจากบริการเอ็มดีเอสเป็นมาตรฐานกลางในการแลกเปลี่ยนข้อมูลที่มีโครงสร้างรองรับการเก็บข้อมูลจากแต่ละทรัพยากรภายในองค์กรเสมือนของระบบโกลบัส ดังนั้นงานวิจัยนี้จะใช้บริการเอ็มดีเอสเป็นบริการแลกเปลี่ยนข้อมูลตัวอย่างของระบบกริดในการพัฒนาเพิ่มความสามารถในการควบคุมการเข้าถึงข้อมูล อย่างไรก็ตามเราสามารถนำแนวความคิดนี้ไปประยุกต์ใช้กับการแลกเปลี่ยนข้อมูลผ่านบริการอื่นๆได้ นอกจากนี้ เพื่อให้งานวิจัยนี้มีรูปแบบการกำหนดข้อมูลควบคุมการเข้าถึงข้อมูลที่เหมาะสมกับการนำไปใช้ภายในองค์กรขนาดใหญ่ที่การดูแลสิทธิของผู้ใช้แต่ละคนทำได้ยาก ขอบเขตของงานยังได้รวมไปถึงการออกแบบลักษณะการควบคุมการเรียกข้อมูลให้ผู้ใช้แต่ละคนมองเห็นข้อมูลเพียงบางส่วนแตกต่างกันตามบทบาทของผู้ใช้แต่ละคนภายในองค์กร โดยใช้ลักษณะการควบคุมตามบทบาทขั้นพื้นฐาน ($RBAC_0$) ซึ่งเป็นส่วนหนึ่งของแนวความคิดการควบคุมตามบทบาท (RBAC: Role-Based Access Control) [6]

1.2 วัตถุประสงค์

ทำการพัฒนาระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส เพื่อพิสูจน์แนวความคิดที่ว่าด้วยการนำเอารูปแบบการควบคุมสิทธิตามบทบาทมาควบคุมการเรียกดูข้อมูลของผู้ใช้บนโครงสร้างของการแลกเปลี่ยนข้อมูลที่มีอยู่เดิมของระบบโกลบัส

1.3 ขอบเขตการวิจัย

1. สร้างระบบควบคุมการเข้าถึงข้อมูลบนกริดซอร์ฟแวร์ โกลบัสทูลคิดรุ่น 2.0 (Globus Toolkit 2.0) เพื่อให้สามารถควบคุมการเรียกดูข้อมูลทั้งหมดภายในองค์กรเสมือน
2. ภายในระบบควบคุมการเข้าถึงข้อมูลนี้จะอาศัยวิธีการแลกเปลี่ยนข้อมูลเดิมของเอ็มดีเอสในการแลกเปลี่ยนข้อมูลระหว่างแต่ละเซิร์ฟเวอร์ภายในองค์กรเสมือน ซึ่งจะเป็นการแลกเปลี่ยนข้อมูลผ่านทางมาตรฐานแอลแดป (LDAP : Lightweight Directory Access Protocol) [7]
3. นำเอาแนวความคิดการควบคุมสิทธิตามบทบาทของผู้ใช้ขั้นพื้นฐานซึ่งเป็นส่วนหนึ่งของแนวคิดการควบคุมสิทธิตามบทบาท (RBAC: Role-Base Access Control) [6] เข้ามาใช้ในระบบ
4. ภาษาที่ใช้ในการพัฒนาระบบการให้บริการสารสนเทศร่วมบนกริดนี้จะใช้ภาษาจาวาและชุดคำสั่งของยูนิกต์ (UNIX Script)

1.4 ขั้นตอนในการดำเนินงาน

1. ศึกษาเทคโนโลยีกริด และงานวิจัยอื่นๆที่เกี่ยวข้องกับเทคโนโลยีกริดที่เกิดขึ้นในปัจจุบัน เพื่อดูแนวโน้มของเทคโนโลยีกริดในอนาคต
2. ติดตั้งกริดซอร์ฟแวร์ลงบนเซิร์ฟเวอร์ที่ได้เตรียมไว้เพื่อศึกษาลักษณะการทำงาน โดยในงานวิทยานิพนธ์นี้ได้ตัดสินใจเลือกใช้โกลบัสทูลคิดรุ่น 2.0 (Globus Toolkits 2.0) ซึ่งเป็นกริดซอร์ฟแวร์ที่ทางผู้พัฒนาอนุญาตให้นักวิจัยที่สนใจทางด้านเทคโนโลยีกริดสามารถนำไปติดตั้งได้โดยไม่คิดค่าใช้จ่ายแต่ประการใด
3. ศึกษาเอ็มดีเอ็สซึ่งเป็นหน่วยให้บริการข้อมูลภายในระบบโกลบัสเพื่อดูลักษณะการทำงานและข้อจำกัดในการเรียกดูข้อมูลต่างๆที่เกิดขึ้นภายในระบบโกลบัสรุ่น 2.0
4. ศึกษางานวิจัยอื่นๆในสาขาเทคโนโลยีสารสนเทศเพื่อศึกษาว่างานวิจัยใดบ้างที่เราสามารถนำเอาแนวความคิดมาประยุกต์ใช้ในวิทยานิพนธ์นี้ได้
5. ศึกษางานวิจัยที่เกี่ยวข้องกับเทคโนโลยีการรักษาความปลอดภัยเพื่อหาวิธีที่จะนำมาใช้ควบคุมการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนภายในระบบโกลบัส
6. ออกแบบระบบควบคุมการเข้าถึงข้อมูลโดยจะใช้รูปแบบการแลกเปลี่ยนข้อมูลของเอ็มดีเอส ภายในระบบโกลบัสมาใช้ประโยชน์ให้มากที่สุด
7. พัฒนาระบบควบคุมการเข้าถึงข้อมูล ตามที่ได้ออกแบบไว้เพื่อศึกษาผลกระทบต่อระบบเดิมและดูผลลัพธ์ว่าเป็นไปตามที่คาดไว้หรือไม่
8. ศึกษาหน่วยให้บริการข้อมูลรูปแบบอื่นซึ่งประกอบไปด้วยเอ็ททีฟไดเร็คทอรี่ (ADS : Active Directory Service) [8] และฐานข้อมูลแอลแด็ป (LDAP Database) [7] เพื่อศึกษาความเป็นไปได้ในการพัฒนาระบบควบคุมการเข้าถึงข้อมูลสามารถทำงานข้ามเทคโนโลยีได้โดยที่ยังคงรักษาความสามารถในการควบคุมการแลกเปลี่ยนข้อมูลให้เป็นไปตามนโยบายของแต่ละองค์กร

1.5 ประโยชน์ที่จะได้รับ

1. ได้ระบบควบคุมการเข้าถึงข้อมูลที่เปิดโอกาสให้เจ้าของทรัพยากรภายในแต่ละองค์กรสามารถควบคุมการเรียกดูข้อมูลให้เป็นไปตามนโยบายที่ถูกกำหนดร่วมกันขององค์กรเสมือน
2. ผู้ใช้งานทั่วไปจะได้รับข้อมูลที่ตนต้องการตามสิทธิในการเรียกใช้ข้อมูลของผู้ใช้ดังกล่าว

3. เนื่องจากการนำเอาแนวความคิดทางด้านการควบคุมสิทธิตามบทบาท มาประยุกต์ใช้จึงทำให้ง่ายต่อการควบคุมการมองเห็นข้อมูลของผู้ใช้แต่ละคน

1.6 โครงสร้างวิทยานิพนธ์

ในบทต่อไปของวิทยานิพนธ์นี้จะกล่าวถึงทฤษฎีที่นำมาประยุกต์ใช้ และงานวิจัยที่เกี่ยวข้อง ส่วนในบทที่ 3 และบทที่ 4 จะกล่าวถึงการออกแบบโครงสร้างการทำงาน และการพัฒนาต้นแบบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส ในบทที่ 5 จะกล่าวถึงการทดสอบการทำงานของต้นแบบระบบควบคุมการเข้าถึงข้อมูล และในบทสุดท้ายจะเป็นการสรุปผลของงานวิทยานิพนธ์และข้อเสนอแนะในการพัฒนาต่อไป