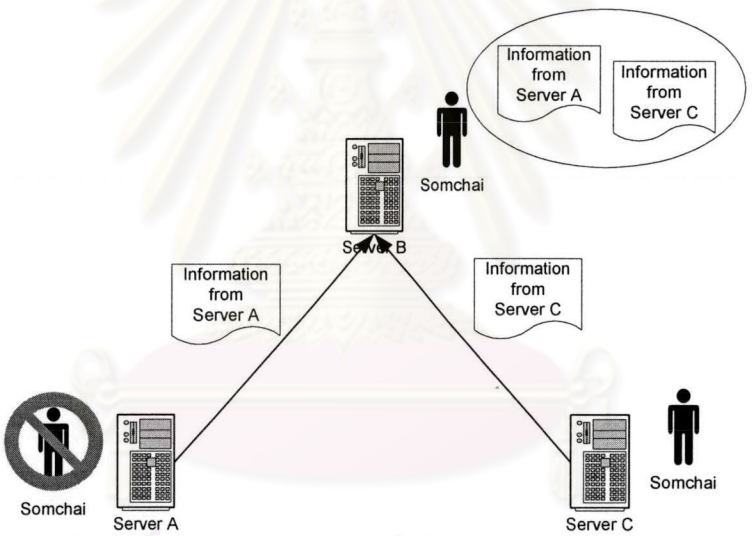
บทที่ 3

การออกแบบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส

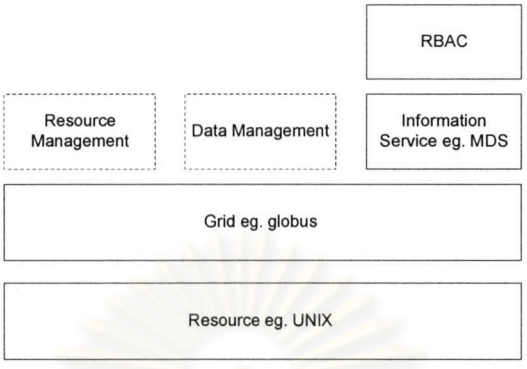
พื้นฐานของการควบคุมทรัพยากรของระบบโกลบัสจะเป็นการควบคุมการเข้าถึงทรัพยากร ณ จุดที่ผู้ใช้ทำการติดต่อเรียกใช้งาน จุดให้บริการจึงเป็นจุดที่ควบคุมการเข้าถึงอย่างแท้จริง ดังนั้น สำหรับข้อมูลซึ่งเป็นทรัพยากรที่สามารถคัดลอกไปยังจุดให้บริการต่างๆได้ จะมีลักษณะการควบคุมการเข้าถึงที่ต่างจากทรัพยากรทั่วไป โดยแทนที่จะถูกควบคุมโดยเครื่องที่เป็นต้นตอของข้อมูล จะกลายเป็นถูกควบคุมโดยเครื่องที่ติดตั้งหน่วยให้บริการจีไอไอเอสที่ทำหน้าที่เก็บรวบรวมสารบัญข้อมูล ซึ่งจะทำให้เจ้าของเครื่องเซิร์ฟเวอร์ที่เป็นต้นตอของข้อมูลไม่สามารถควบคุมการเข้าถึงข้อมูลได้ ดังที่แสดงให้เห็นในรูปที่ 3.1



รูปที่ 3.1 แสดงปัญหาที่เกิดขึ้นภายในหน่วยควบคุมการแลกเปลี่ยนข้อมูลของระบบโกลบัส

รูปที่ 3.1 แสดงให้เห็นถึงปัญหาที่เกิดขึ้นภายในระบบโกลบัสทูลคิตรุ่น 2.0 ซึ่งจะเห็นได้ว่านายสมชายถึงแม้จะไม่ได้เป็นสมาชิกภายในเซิร์ฟเวอร์เอ (ไม่มีชื่อเอกเทศอยู่ภายในไฟล์ควบคุม) จะสามารถดูข้อมูลของเซิร์ฟเวอร์เอ ได้จากการติดต่อไปที่จีไอไอเอสของเครื่องเซิร์ฟเวอร์บีที่นายสมชายเป็นสมาชิกอยู่ ซึ่งเซิร์ฟเวอร์เอ ได้ส่งข้อมูลของตนไปเก็บรวบรวมไว้

งานวิจัยนี้จึงได้ออกแบบโครงสร้างทางสถาปัตยกรรมของระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทการควบคุมการเรียกดูข้อมูลซึ่งจะมีลักษณะดังรูปที่ 3.2

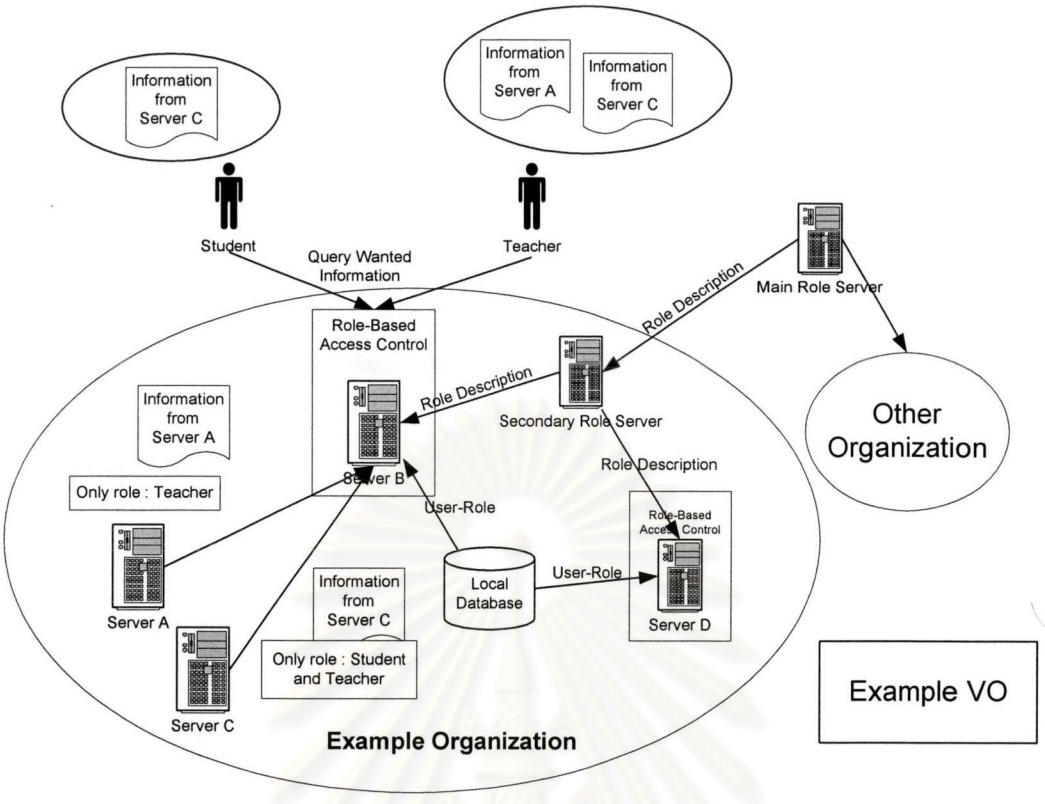


รูปที่ 3.2 แสดงโครงสร้างทางสถาปัตยกรรมของระบบควบคุมการเข้าถึงข้อมูล

รูปที่ 3.2 แสดงโครงสร้างของการควบคุมสิทธิเชิงบทบาทให้กับบริการทางด้านข้อมูลหรือบริการเอ็มดีเอสของระบบโกลบัส เพื่อให้สามารถควบคุมการเรียกดูข้อมูลของผู้ใช้ในกรณีที่ข้อมูลนั้นถูกคัดลอกส่งต่อกันระหว่างแต่ละเซิร์ฟเวอร์ภายในระบบกริด โดยการออกแบบระบบควบคุมการเข้าถึงเชิงบทบาทจำเป็นจะต้องคำนึงถึงรายละเอียดของส่วนต่างๆดังต่อไปนี้

- โครงสร้างการแลกเปลี่ยนข้อมูลที่มีอยู่เดิม
- การรองรับปัญหาการเพิ่มจำนวนของผู้ใช้งานและเซิร์ฟเวอร์ที่ถูกควบคุมในอนาคต (Scalability Problem)
- รูปแบบของข้อมูลควบคุมสิทธิ
- ชนิดของผู้ดูแลระบบที่จะถูกแบ่งตามสิทธิในการแก้ไขข้อมูลควบคุม

โดยแต่ละหัวข้อจะถูกอธิบายภายในรายละเอียดของการออกแบบในส่วนต่อไป



รูปที่ 3.3 แสดงการทำงานของระบบควบคุมการเรียกดูข้อมูลเชิงบทบาท

จากรูปที่ 3.3 แสดงให้เห็นถึงโครงสร้างของระบบควบคุมการเข้าถึงข้อมูลในงานวิจัยนี้ ที่ถูกพัฒนาเพื่อจะลดปัญหาการขาดความสามารถในการควบคุมผู้ที่มีสิทธิในการเข้าถึงข้อมูลของระบบโกลบัสรุ่น 2.0 โดยจากรูปจะเห็นว่า

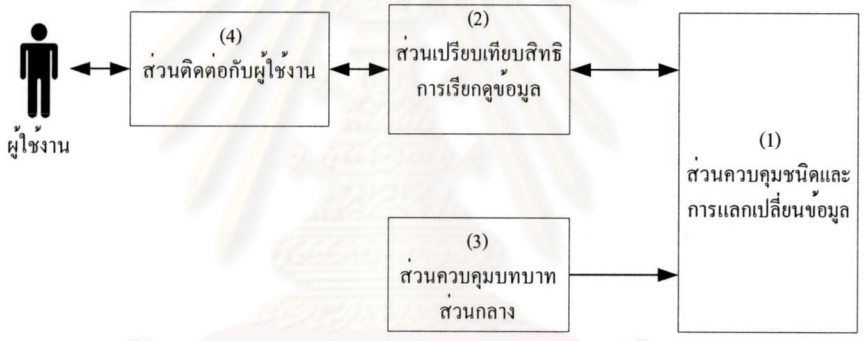
- สามารถควบคุมการเข้าถึงข้อมูลที่จุดให้บริการ โดยเซิร์ฟเวอร์ที่เป็นต้นตอจะส่งข้อมูลควบคุมสิทธิมาพร้อมกับข้อมูลจริงเพื่อให้แน่ใจว่าข้อมูลของตนจะถูกควบคุมสิทธิการเข้าถึงอย่างถูกต้องโดยจุดบริการใดๆ
- มีการควบคุมสิทธิของผู้ใช้แต่ละคนให้เป็นไปตามบทบาทส่วนกลาง โดยจะมีการส่งข้อมูลควบคุมบทบาทมาจากเซิร์ฟเวอร์หลักที่จะคอยดูแลบทบาททั้งหมดภายในองค์กรเสมือน
- ผู้ใช้แต่ละคนจะมองเห็นข้อมูลของแต่ละจุดให้บริการแตกต่างกันตามชนิดของบทบาทที่ผู้ใช้คนนั้นๆรับผิดชอบอยู่

3.1 โครงสร้างและขั้นตอนการทำงานของระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส

การออกแบบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส จะสามารถแบ่งระบบควบคุมออกเป็น 4 ส่วนหลักๆได้แก่

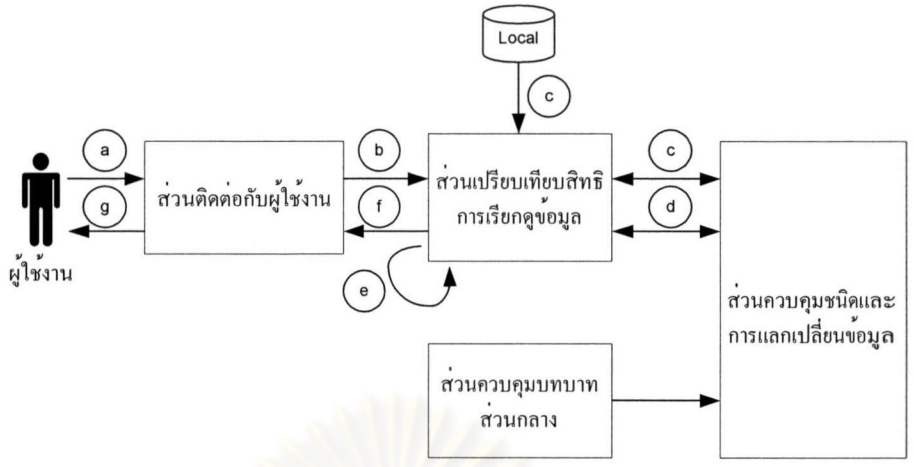
- ส่วนควบคุมการแลกเปลี่ยนของข้อมูลระหว่างแต่ละเซิร์ฟเวอร์
- ส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลาง
- ส่วนควบคุมบทบาทส่วนกลาง
- ส่วนติดต่อกับผู้ใช้งาน

ซึ่งได้แสดงโครงสร้างของระบบควบคุมการดังรูปที่ 3.4



รูปที่3.4 แสดงโครงสร้างภายในระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส

รูปที่ 3.4 แสดงองค์ประกอบหลักๆ ภายในระบบควบคุมการเข้าถึงข้อมูล ซึ่งการที่ระบบถูกออกแบบให้แยกออกเป็นแต่ละส่วนย่อยๆก็เพื่อให้แต่ละส่วนสามารถทำงานได้โดยไม่ขึ้นกับลักษณะการทำงานภายในแต่ละส่วนหลังจากนำไปพัฒนาเป็นระบบควบคุมเช่นส่วนติดต่อกับผู้ใช้งานสามารถที่จะถูกนำไปพัฒนาได้หลายรูปแบบไม่ว่าจะอยู่ในรูปของชุดคำสั่งหรืออยู่ในรูปแบบเว็ปเพจเป็นต้น



รูปที่ 3.5 แสดงลำดับการทำงานของระบบควบคุมการเข้าถึงข้อมูล

รูปที่ 3.5 แสดงลำดับการทำงานเริ่มตั้งแต่ผู้ใช้แสดงความต้องการของตน จนผู้ใช้ได้รับข้อมูลที่ผู้ใช้ต้องการตามบทบาทของผู้ใช้คนนั้นภายในองค์กรเสมือน ซึ่งลำดับการทำงานจะถูกเรียงตามตัวอักษรภาษาอังกฤษตั้งแต่ a ถึง g ภายในรูปที่ 3.5

a. ผู้ใช้งานประกาศชนิดของข้อมูลที่ผู้ใช้ต้องการไปยังส่วนติดต่อกับผู้ใช้งาน

b. ส่วนติดต่อกับผู้ใช้งานจะเรียกข้อมูลรายละเอียดส่วนตัวของผู้ใช้ก่อนที่จะส่งข้อมูลดังกล่าวไปพร้อมกับความต้องการของผู้ใช้

c. ส่วนประมวลผลเรียกข้อมูลบทบาทส่วนกลางมาเปรียบเทียบกับรายละเอียดส่วนตัวของผู้ใช้เพื่อเปรียบเทียบหาบทบาทที่แท้จริงของผู้ใช้

d. ส่วนประมวลผลติดต่อไปยังส่วนควบคุมการแลกเปลี่ยนข้อมูลเพื่อนำความต้องการของผู้ใช้ไปเรียกข้อมูลจริง พร้อมกับข้อมูลควบคุมที่ถูกเก็บไว้ภายในเซิร์ฟเวอร์นั้นๆ ในกรณีที่ข้อมูลจริงที่ผู้ใช้ต้องการนั้นถูกควบคุมโดยเจ้าของข้อมูล

e. ส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลจะเปรียบเทียบข้อมูลควบคุมสิทธิกับข้อมูลบทบาทของผู้ใช้เพื่อพิจารณาว่าข้อมูลใดที่ผู้ใช้คนนั้นสามารถเรียกดูได้

f. ส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลจะส่งข้อมูลที่อยู่ในขอบเขตความต้องการและบทบาทของผู้ใช้คนนั้นไปยังส่วนติดต่อกับผู้ใช้

g. ส่วนติดต่อกับผู้ใช้แสดงข้อมูลที่ได้รับจากส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลในรูปแบบที่ผู้ใช้ต้องการ

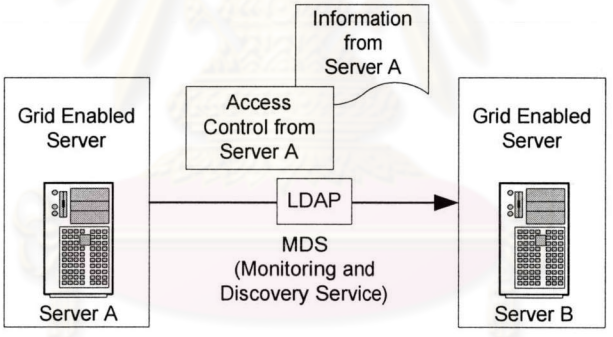
นอกจากนี้ส่วนควบคุมบทบาทส่วนกลางจะแก้ไขข้อมูลบทบาทภายในเซิร์ฟเวอร์ที่ทำหน้าที่เก็บรวบรวมรายละเอียดของบทบาทในแต่ละองค์กร โดยติดต่อไปที่ส่วนควบคุมชนิดและการแลกเปลี่ยนข้อมูล ซึ่งการทำงานดังกล่าวนี้จะทำทุกๆช่วงเวลาหนึ่งซึ่งจะไม่ขึ้นกับการเรียกดูข้อมูลของผู้ใช้แต่อย่างไร

3.2 รายละเอียดภายในแต่ละส่วนของระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาท

ในหัวข้อนี้จะกล่าวถึงรายละเอียดขององค์ประกอบต่างๆภายในระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส

3.2.1 ส่วนควบคุมชนิดและการแลกเปลี่ยนของข้อมูลระหว่างแต่ละเซิร์ฟเวอร์

เป็นส่วนที่รับผิดชอบเกี่ยวกับการเพิ่มข้อมูลควบคุมสิทธิ ก่อนที่จะถูกนำไปแลกเปลี่ยนข้อมูลระหว่างแต่ละเซิร์ฟเวอร์พร้อมกับข้อมูลจริงภายในระบบโกลบัส โดยใช้โครงสร้างการแลกเปลี่ยนข้อมูลที่มีอยู่เดิมของระบบโกลบัสที่ส่งข้อมูลระหว่างแต่ละเซิร์ฟเวอร์โดยใช้มาตรฐานแอลแดป ดังรูปที่ 3.6



รูปที่3.6 แสดงการแนบข้อมูลควบคุมไปพร้อมกับข้อมูลจริง

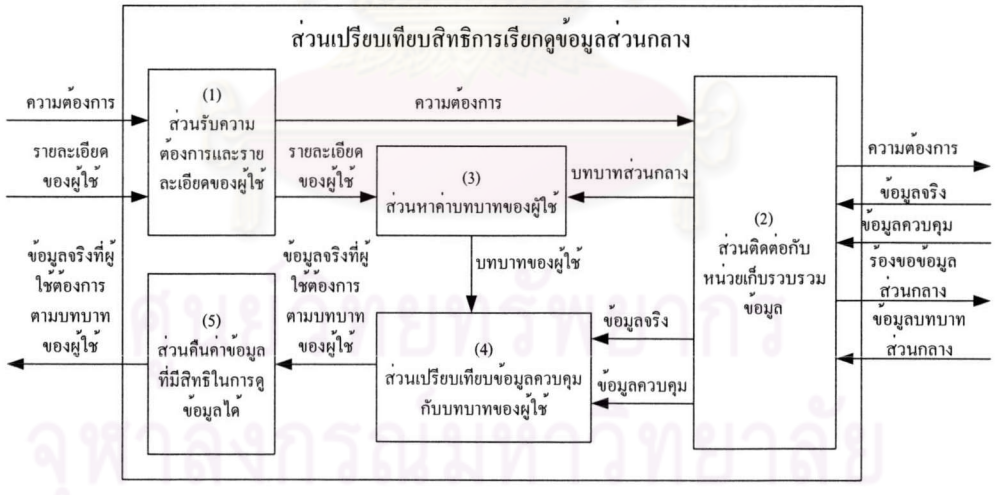
จากรูปที่ 3.6 แสดงให้เห็นถึงการเพิ่มข้อมูลควบคุมสิทธิการเข้าถึงข้อมูลโดยเซิร์ฟเวอร์ที่เป็นต้นตอ โดยเพิ่มข้อมูลควบคุมดังกล่าวเข้าไปในต้นไม้ข้อมูลก่อนที่จะส่งไปเก็บไว้ยังส่วนเก็บรวบรวมสารบัญข้อมูลบนเซิร์ฟเวอร์อื่นพร้อมกับข้อมูลจริงที่ถูกควบคุม

3.2.2 ส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลาง

ส่วนนี้จะมีหน้าที่ในการเปรียบเทียบสิทธิตามบทบาทของผู้ใช้กับข้อมูลควบคุมสิทธิที่ถูกส่งมาพร้อมกับข้อมูลจริง ว่าจากข้อมูลทั้งหมดที่ผู้ใช้ต้องการนั้นมีข้อมูลใดบ้างที่ผู้ใช้นั้นๆมีสิทธิตามบทบาทในการเข้าถึงข้อมูลได้ ข้อมูลที่เกี่ยวข้องกับการทำงานของส่วนเปรียบเทียบการเรียกดูข้อมูลส่วนกลางจะแสดงไว้ในรูปที่ 3.7

รูปที่3.7 แสดงชนิดของข้อมูลจากส่วนต่างๆที่ถูกพิจารณาโดยหน่วยประมวลผล

ภายในส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลางจะถูกแบ่งออกเป็นส่วนย่อยๆ ซึ่งมีรูปแบบการแลกเปลี่ยนข้อมูลระหว่างแต่ละองค์ประกอบดังรูปที่ 3.8



รูปที่3.8 แสดงโครงสร้างภายในส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลาง

จากรูปที่3.8 แสดงให้เห็นว่าภายในส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลางได้ถูกแบ่งออกเป็นองค์กรประกอบย่อยๆ ซึ่งแต่ละส่วนจะมีรายละเอียดดังต่อไปนี้

1. ส่วนรับความต้องการและรายละเอียดของผู้ใช้จากส่วนติดต่อกับผู้ใช้

เป็นส่วนที่จะรับเอาความต้องการและรายละเอียดจากส่วนติดต่อกับผู้ใช้ มาเปลี่ยนแปลงข้อมูลให้อยู่ในรูปแบบที่เหมาะสม ก่อนที่จะส่งข้อมูลดังกล่าวไปยังส่วนติดต่อกับหน่วยเก็บรวบรวมข้อมูลเพื่อดึงข้อมูลจริงและข้อมูลควบคุมที่เกี่ยวข้องไปพิจารณาต่อไป

2. ส่วนติดต่อกับหน่วยเก็บรวบรวมข้อมูล

เป็นส่วนที่จะนำข้อมูลความต้องการของผู้ใช้มาใช้ในการดึงข้อมูลจริงและข้อมูลควบคุมที่เกี่ยวข้องตามความต้องการของผู้ใช้ที่ได้รับมาจากส่วนที่หนึ่ง โดยการติดต่อกับบริการเอ็มดีเอสเดิม ซึ่งผลลัพท์ที่ได้ในขั้นนี้จะได้ทั้งข้อมูลจริงและข้อมูลควบคุมสิทธิที่เกี่ยวข้องทั้งหมดตามความต้องการของผู้ใช้ภายในต้นไม้ข้อมูลของเครื่องเซิร์ฟเวอร์ที่ติดตั้งระบบควบคุมการเข้าถึงข้อมูล

นอกจากทำหน้าที่ในการสืบค้นข้อมูลตามความต้องการของผู้ใช้แล้ว ส่วนติดต่อกับหน่วยเก็บรวบรวมข้อมูลยังมีหน้าที่เรียกดูข้อมูลบทบาทส่วนกลางเพื่อส่งไปให้ส่วนหาค่าบทบาทของผู้ใช้ต่อไป

3. ส่วนหาค่าบทบาทของผู้ใช้

เป็นส่วนที่จะนำเอารายละเอียดของผู้ใช้มาเปลี่ยนเป็นบทบาทที่ได้ถูกกำหนดร่วมกันระหว่างแต่ละองค์กรจริงภายในองค์กรเสมือน ซึ่งการเปรียบเทียบจะอาศัยการพิจารณาจากข้อมูลที่เก็บบทบาทของผู้ใช้ที่ถูกเก็บอยู่ภายในแต่ละองค์กรจริง และข้อมูลบทบาทส่วนกลาง เพื่อป้องกันการคลาดเคลื่อนของการกำหนดบทบาทของผู้ใช้แต่ละคน

4.ส่วนเปรียบเทียบข้อมูลควบคุมกับบทบาทของผู้ใช้

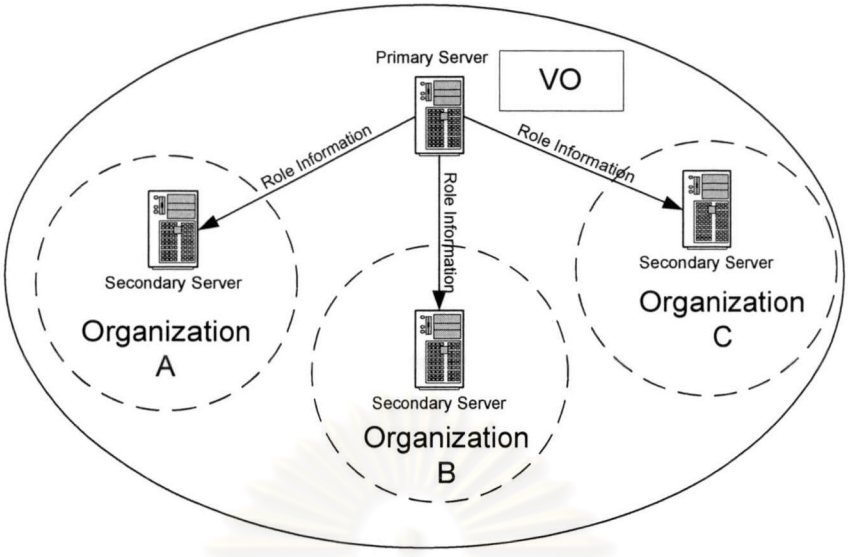
ส่วนนี้จะเปรียบเทียบสิทธิการเรียกดูข้อมูลโดยการดึงเอาข้อมูลควบคุมที่มีอยู่ในกรณีที่ข้อมูลจริงนั้นถูกควบคุมมาเปรียบเทียบกับบทบาทของผู้ใช้ที่ได้รับมาจากส่วนหาค่าบทบาทของผู้ใช้ ถ้าบทบาทของผู้เรียกดูข้อมูลนั้นตรงกับเงื่อนไขที่ถูกระบุไว้ภายในข้อมูลควบคุมของข้อมูลจริงที่ผู้ใช้ต้องการ ส่วนเปรียบเทียบข้อมูลก็จะส่งข้อมูลจริงนั้นไปยังส่วนคืนค่าต่อไป

5. ส่วนคืนค่าข้อมูลที่มีสิทธิในการดูข้อมูลได้

จะคืนค่าข้อมูลจริงที่ผู้ใช้สามารถเรียกดูได้กลับไป โดยอาจจะต้องเปลี่ยนรูปแบบของข้อมูลจริงที่ได้รับจากส่วนเปรียบเทียบข้อมูลให้อยู่ในรูปแบบที่เหมาะสมก่อนจะส่งข้อมูลดังกล่าวกลับไปยังส่วนติดต่อกับผู้ใช้

3.2.3 **ส่วนควบคุมบทบาทส่วนกลาง**

ส่วนควบคุมบทบาทส่วนกลางมีหน้าที่ควบคุมบทบาททั้งหมดภายในองค์กรเสมือน เพื่อให้ทุกเซิร์ฟเวอร์ที่ติดตั้งระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทสามารถมองเห็นรายละเอียดของแต่ละบทบาทเหมือนกัน โดยส่วนควบคุมบทบาทจะส่งข้อมูลบทบาทส่วนกลางที่ตนรับผิดชอบอยู่ไปยังเซิร์ฟเวอร์ที่ติดตั้งระบบควบคุมการเข้าถึงข้อมูลภายในแต่ละองค์กรเพื่อให้แต่ละองค์กรสามารถกำหนดบทบาทของผู้ใช้ภายในองค์กรของตน อย่างไรก็ตามจำนวนของเซิร์ฟเวอร์ที่ติดตั้งระบบควบคุมอาจจะมีจำนวนมากและกระจัดกระจายอยู่ตามองค์จริงภายในองค์กรเสมือน ดังนั้นเพื่อให้การเข้าถึงข้อมูลของบทบาทกลางเป็นไปอย่างมีประสิทธิภาพสามารถรองรับจำนวนเซิร์ฟเวอร์ที่มีจำนวนมากได้ อีกทั้งเพื่อเพิ่มความสามารถในการรองรับปัญหาที่อาจเกิดขึ้นจากความผิดปรกติในเครือข่าย งานวิจัยนี้จึงได้นำเอาแนวความคิดของการคัดลอกข้อมูล (Replica Server) ในลักษณะของการคัดลอกข้อมูลอ่านได้เพียงอย่างเดียวเข้ามาใช้ในระบบ โดยมีโครงสร้างดังรูปที่ 3.9



รูปที่3.9 แสดงโครงสร้างของระบบคัดลอกของส่วนควบคุมบทบาท

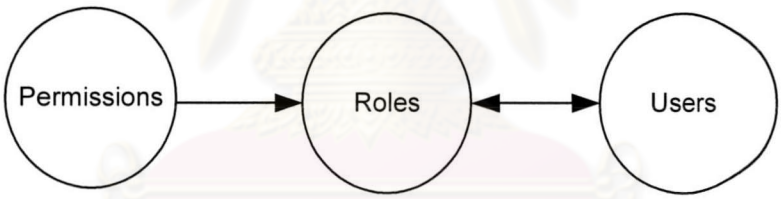
จากรูป 3.9 แสดงให้เห็นว่ามีการคัดลอกข้อมูลบทบาทจากเซิร์ฟเวอร์ส่วนกลาง (Primary Server) ไปยังเซิร์ฟเวอร์สำรอง (Secondary Server) ที่อยู่ภายในเครือข่ายของแต่ละองค์กรจริง โดยการแก้ไขข้อมูลส่วนกลางจำเป็นที่จะต้องแก้ไขที่ต้นตอของข้อมูลหรือเซิร์ฟเวอร์ส่วนกลางเท่านั้น ดังนั้นถึงแม้ว่าเครือข่ายข้ามระหว่างแต่ละองค์กรจริงเกิดปัญหาขึ้น ระบบควบคุมยังสามารถเข้าถึงข้อมูลบทบาทกลางผ่านทางเซิร์ฟเวอร์ย่อยที่ติดตั้งอยู่ภายในองค์กรจริง และเนื่องจากข้อมูลของบทบาทส่วนกลางจะเป็นข้อมูลที่มีการเปลี่ยนแปลงไม่บ่อยนั้น งานวิจัยนี้จึงอนุญาตให้ข้อมูลบทบาทกลางมีความคลาดเคลื่อนขึ้นระหว่างเซิร์ฟเวอร์ของส่วนกลางและเซิร์ฟเวอร์สำรองภายในแต่ละองค์กรจริงได้

3.2.4 **ส่วนติดต่อกับผู้ใช้**

เป็นส่วนที่จัดการเกี่ยวกับการเรียกดูข้อมูลของผู้ใช้และยังจัดการเกี่ยวกับรายละเอียดของผู้ใช้แต่ละคนโดยจะส่งไปให้หน่วยประมวลผลพร้อมกับชนิดของข้อมูลที่ผู้ใช้คนนั้นๆต้องการ ข้อมูลรายละเอียดของผู้ใช้ที่ถูกเรียกโดยส่วนนี้ จะถูกเก็บแยกอยู่ภายในแต่ละองค์กรจริง โดยจะไม่มีส่งข้อมูลดังกล่าวนี้ออกไปเก็บไว้ยังองค์กรจริงอื่น โดยจะถือว่าทุกๆเซิร์ฟเวอร์ที่ติดตั้งหน่วยติดต่อกับผู้ใช้ของระบบควบคุมการเข้าถึงข้อมูล จะต้องสามารถเรียกดูข้อมูลดังกล่าวได้

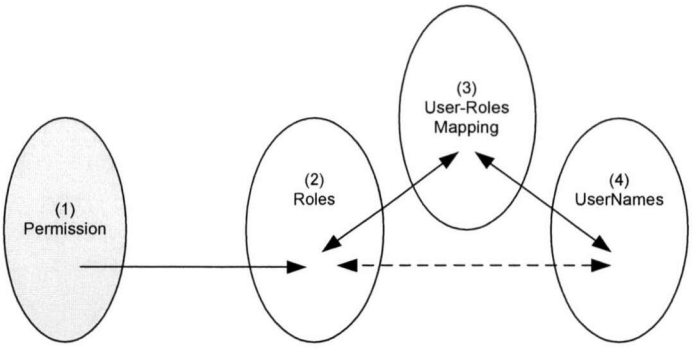
3.3 การออกแบบข้อมูลควบคุมสิทธิและการกระจายอำนาจการควบคุมของแต่ละองค์ประกอบภายในระบบควบคุมการเข้าถึงข้อมูล

การออกแบบข้อมูลควบคุมสิทธิในส่วนนี้จะนำเอาแนวความคิดการควบคุมสิทธิเชิงบทบาทขั้นพื้นฐานมาเป็นต้นแบบเพื่อให้สามารถควบคุมสิทธิการเรียกดูข้อมูลของผู้ใช้แต่ละคนให้เป็นไปตามบทบาทภายในองค์กร และเนื่องจากการทำงานของระบบกริดซึ่งเป็นเทคโนโลยีระบบแบบกระจายที่มีการเชื่อมต่อกันระหว่างแต่ละเซิร์ฟเวอร์ที่ผู้ใช้ได้ทำการติดต่อเข้าไปขอใช้บริการซึ่งจะถือได้ว่ามีหลายจุดควบคุมภายในระบบจึงทำให้ผู้กำหนดสิทธิของแต่ละบทบาทไม่อาจจะทราบถึงชนิดของทรัพยากรทั้งหมดภายในระบบกริด ภายในงานวิจัยนี้จึงได้เลือกใช้วิธีการกำหนดสิทธิการเรียกดูข้อมูลเข้ากับชื่อของบทบาทโดยเจ้าของข้อมูล (Discretionary Mechanism) แทน ซึ่งไม่ถือเป็นการออกแบบที่ขัดกับแนวความคิดการควบคุมสิทธิตามบทบาทของผู้ใช้แต่อย่างใดเพราะแนวความคิดการควบคุมสิทธิตามบทบาทจะไม่ขึ้นกับรูปแบบการกำหนดนโยบายจึงสามารถที่จะกำหนดรายละเอียดของแต่ละบทบาทว่ามีสิทธิอะไรโดยผู้ดูแลส่วนกลาง (Mandatory Mechanism) หรือจะกำหนดสิทธิเข้ากับชื่อบทบาทโดยเจ้าของข้อมูล (Discretionary Mechanism) ซึ่งลักษณะของข้อมูลควบคุมที่ถูกใช้ภายในระบบควบคุมการเข้าถึงข้อมูลจะมีลักษณะดังรูปที่ 3.10



รูปที่3.10 แสดงโครงสร้างของแนวความคิดควบคุมสิทธิขั้นพื้นฐาน

จากรูปที่ 3.10 เราได้นำมาออกแบบเป็นข้อมูลควบคุมสิทธิโดยจะแบ่งออกเป็นสองส่วนได้แก่ข้อมูลอธิบายสิทธิการใช้ข้อมูล และข้อมูลควบคุมที่ถูกเพิ่มเติมขึ้นมาเพื่อให้สามารถทำงานในลักษณะการควบคุมเชิงบทบาทและสอดคล้องกับลักษณะการทำงานภายในระบบโกลบัสที่มีผู้ดูแลระบบอยู่หลายระดับดังรูปที่ 3.11



รูปที่ 3.11 แสดงโครงสร้างของข้อมูลควบคุมบทบาทภายในระบบควบคุม

จากรูปที่ 3.11 จะสังเกตได้ว่ามีการเพิ่มองค์ประกอบเพื่อให้สอดคล้องกับรูปแบบการทำงานภายในระบบกริดที่มีผู้ดูแลระบบหลายคน โดยข้อมูลควบคุมทั้งหมดจะถูกแบ่งเป็น 2 ประเภทประกอบด้วยข้อมูลอธิบายสิทธิการเรียกดูข้อมูล (ส่วนที่ 1) และข้อมูลที่เกี่ยวข้องกับการควบคุมบทบาทของผู้ใช้ภายในองค์กรเสมือน (ส่วนที่ 2 ถึง ส่วนที่ 4) ซึ่งแต่ละส่วนจะมีรายละเอียดดังต่อไปนี้

3.3.1 ข้อมูลอธิบายสิทธิการเรียกดูข้อมูล

ส่วนควบคุมสิทธิการเรียกดูข้อมูล (Permission) หรือส่วนที่ 1 ภายในรูป 3.10 จะถูกระบุโดยเจ้าของข้อมูลในกรณีที่เจ้าของข้อมูลเป็นเจ้าของเซิร์ฟเวอร์ หรือถูกระบุโดยผู้ดูแลระบบของแต่ละเซิร์ฟเวอร์ในกรณีที่เจ้าของข้อมูลไม่ใช่เจ้าของเซิร์ฟเวอร์ โดยข้อมูลในส่วนนี้จะอธิบายว่าผู้ใช้หรือเซิร์ฟเวอร์ที่เรียกดูข้อมูลดังกล่าวต้องมีรายละเอียดอย่างไรจึงจะมีสิทธิในการเรียกดูข้อมูลดังกล่าว

รายละเอียดในส่วนนี้เราสามารถจะกำหนดเป็นชื่อเอกเทศของผู้ใช้แต่ละคนภายในองค์กรเสมือนเพื่อให้สามารถควบคุมการเข้าถึงข้อมูลของผู้ใช้แต่ละคนได้ แต่ในงานวิจัยนี้เราได้เพิ่มความสามารถในการควบคุมการเข้าถึงเชิงบทบาท เราจึงได้เก็บข้อมูลรายละเอียดเฉพาะชื่อบทบาทและชื่อเซิร์ฟเวอร์ที่สามารถแสดงข้อมูลจริงที่ถูกข้อมูลควบคุมสิทธินี้กำกับอยู่

ข้อมูลบทบาทภายในส่วนควบคุมสิทธิการเรียกดูข้อมูลนี้ จะถูกนำไปเปรียบเทียบกับข้อมูลควบคุมบทบาทของผู้ใช้ต่ออีกทีหนึ่ง เพื่อหาว่าผู้ที่ทำการเรียกดูข้อมูลมีบทบาทอะไรและสามารถเรียกดูข้อมูลนี้ได้หรือไม่

3.3.2 ข้อมูลควบคุมบทบาทของผู้ใช้ภายในองค์กรเสมือน

ข้อมูลที่เกี่ยวข้องกับการควบคุมบทบาทของผู้ใช้ภายในองค์กรเสมือนจะมีอยู่ 3 ประเภทใหญ่ๆได้แก่

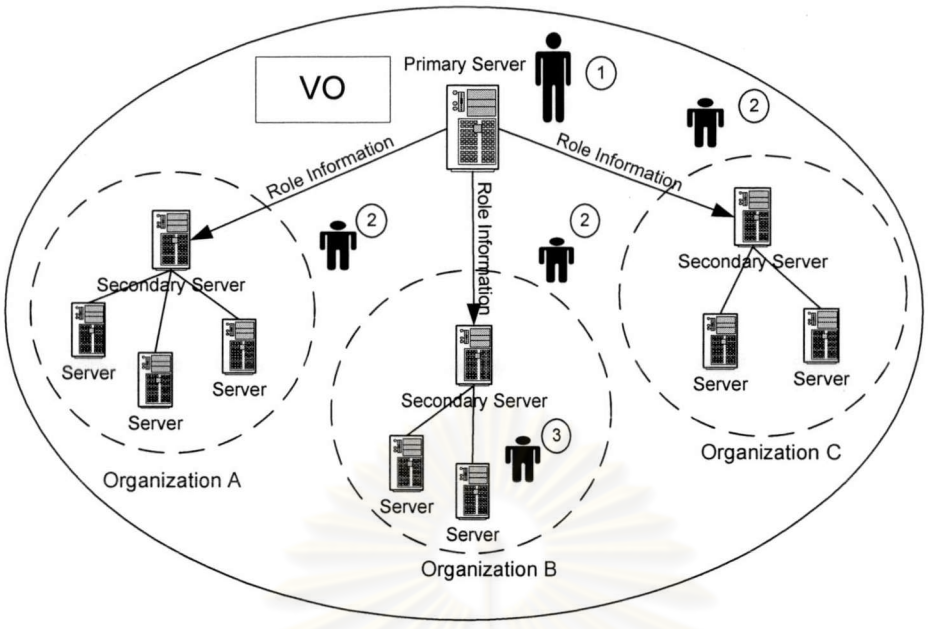
1. ส่วนควบคุมบทบาท (Role) หรือส่วนที่ 2 ในรูป 3.10 เป็นส่วนควบคุมบทบาทส่วนกลาง เพื่อให้บทบาทของผู้ใช้ระบบทุกคนเป็นไปตามข้อตกลงร่วมกันภายในองค์กรเสมือน โดยข้อมูลในส่วนนี้จะถูกดูแลโดย ผู้ดูแลบทบาทส่วนกลาง

2. ส่วนเชื่อมต่อระหว่างชื่อและบทบาทของผู้ใช้ (User-Role Mapping) หรือส่วนที่ 3 ในรูป 3.10 เป็นส่วนที่จะเก็บรวบรวมข้อมูลว่าขณะนี้ผู้ใช้ที่มีชื่อเอกเทศดังกล่าวถูกกำหนดให้เป็นบทบาทอะไรภายในองค์กร โดยข้อมูลส่วนนี้จะถูกดูแลแก้ไขโดย ผู้ดูแลข้อมูลบทบาทของผู้ใช้แต่ละคนขององค์กรจริงแต่ละแห่ง

3. ส่วนควบคุมรายชื่อผู้ใช้ (User Name) หรือส่วนที่ 4 ในรูป 3.10 ซึ่งจะเป็นส่วนที่รวบรวมราบชื่อของผู้ใช้ทั้งหมดให้อยู่ในรูปของชื่อเอกเทศ (Distinguished Name) ที่ผู้ใช้แต่ละคนจะมีเพียงชื่อเดียวภายในระบบโกลบัส ที่แตกต่างจากชื่อผู้ใช้งานทั่วไป (Local name) ที่ผู้ใช้แต่ละคนจะมีชื่อแตกต่างกันตามเครื่องเซิร์ฟเวอร์ที่ผู้ใช้ติดต่อเข้าไป

3.3.3 การกระจายอำนาจการควบคุมขององค์ประกอบแต่ละส่วนภายในระบบควบคุมการเข้าถึงข้อมูล

เนื่องจากภายในระบบโกลบัสซึ่งเป็นการทำงานในลักษณะของระบบกริดที่ภายในองค์กรเสมือนอาจจะประกอบไปด้วยหลายๆองค์กรจริงเข้าด้วยกัน เพราะฉะนั้นจึงไม่ใช่เรื่องแปลกอะไรนัก ในการที่ภายในองค์กรเสมือนจะประกอบไปด้วยผู้ดูแลระบบมากกว่าหนึ่งคน ซึ่งเมื่อพิจารณาบทบาทและหน้าที่ของผู้ดูแลระบบที่เกี่ยวข้องกับระบบควบคุมการเข้าถึงข้อมูลและทรัพยากรต่างๆภายในระบบโกลบัส จะสามารถแบ่งออกได้เป็นหลายระดับดังรูปที่ 3.12



รูปที่ 3.12 แสดงขอบเขตการควบคุมสำหรับผู้ดูแลแต่ละชนิด

จากรูปที่ 3.12 แสดงให้เห็นว่ามีผู้ดูแลหลายระดับที่เกี่ยวข้องกับการทำงานของระบบควบคุมการเข้าถึงข้อมูลและระบบโกลบัส ซึ่งแต่ละคนก็จะมีภาระความรับผิดชอบแตกต่างออกไป เพื่อลดปัญหาการจัดการโดยผู้ดูแลระบบเพียงผู้เดียว จึงทำให้เหมาะสมสำหรับการทำงานในลักษณะกริดที่สามารถรองรับจำนวนเซิร์ฟเวอร์ที่มาทำงานร่วมกันได้เป็นจำนวนมาก ซึ่งผู้ดูแลแต่ละระดับจะมีรายละเอียดดังต่อไปนี้

1. ผู้ดูแลบทบาทส่วนกลาง

เป็นผู้ที่มีหน้าที่กำหนดบทบาทของผู้ใช้งานทั้งหมดภายในองค์กรเสมือนให้เป็นไปตามข้อตกลงร่วมกันระหว่างแต่ละองค์กรที่ได้ตกลงกันในตอนแรก ซึ่งผู้ดูแลส่วนนี้ จริงๆแล้วอาจจะตั้งอยู่ภายในองค์กรจริงองค์กรใดองค์กรหนึ่งภายในองค์กรเสมือน ที่ทำหน้าที่เสมือนเป็นศูนย์กลางการดูแลการใช้งานทรัพยากรภายในองค์กรเสมือนนี้

2. ผู้ดูแลข้อมูลบทบาทของผู้ใช้แต่ละคน

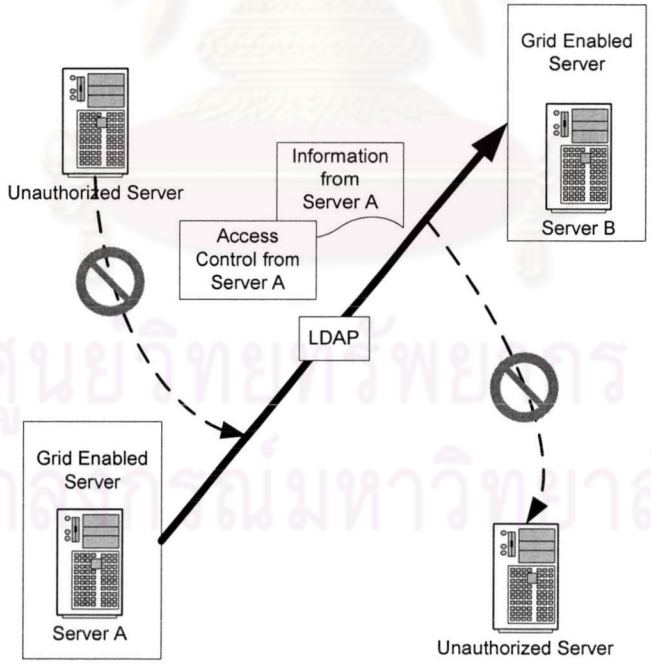
เป็นผู้ควบคุมบทบาทของผู้ใช้งานแต่ละคน ซึ่งจะมีขอบเขตอยู่เฉพาะภายในแต่ละองค์กรจริงเท่านั้น โดยจะมีหน้าที่กำหนดบทบาทของผู้ใช้ภายในแต่ละองค์กรจริงที่อาจจะมีชื่อที่ใช้ในการติดต่อกับแต่ละทรัพยากร (Local Account) แตกต่างกัน แต่หน้าที่เกี่ยวข้องกับการทำงานภายในองค์กรเสมือนนั้นเหมือนกัน เป็นบทบาทกลางที่ถูกกำหนดโดยผู้ดูแลบทบาทส่วนกลาง

3. ผู้ดูแลระบบของแต่ละเซิร์ฟเวอร์

เนื่องจากการเพิ่มข้อมูลควบคุมเข้าไปภายในระบบควบคุมการเข้าถึงข้อมูลจำเป็นจะต้องมีสิทธิในระดับรูท (root) ซึ่งถ้าในกรณีที่เจ้าของข้อมูลดังกล่าวไม่ใช่เจ้าของทรัพยากรซึ่งก็คือเซิร์ฟเวอร์แต่เพียงผู้เดียว ก็อาจจะจำเป็นที่จะต้องมีผู้ดูแลระบบที่คอยดูแลการทำงานของเซิร์ฟเวอร์ภายในแต่ละองค์กรจริง

3.4 การพิจารณาในแง่ของความปลอดภัยของระบบควบคุม

ภายในงานวิจัยนี้ ได้ใช้โครงสร้างการแลกเปลี่ยนข้อมูลของบริการเอ็มดีเอสซึ่งจะอยู่ในรูปของมาตรฐานแอลแด็ป ซึ่งจะมีผลต่อความปลอดภัยของระบบควบคุมการเข้าถึงข้อมูลดังที่แสดงไว้ในรูปที่ 3.13



รูปที่ 3.13 แสดงการป้องกันการแก้ไขข้อมูลควบคุมโดยผู้ที่ไม่ประสงค์ดี

จากรูปที่ 3.13 ได้แสดงให้เห็นว่าระบบควบคุมการเข้าถึงข้อมูลที่ใช้โครงสร้างการแลกเปลี่ยนข้อมูลของระบบโกลบัสทูลคิตรุ่น 2.0 จะสามารถป้องกันปัญหาการแก้ไขข้อมูลควบคุมโดยผู้ที่ไม่ประสงค์ดีได้ เนื่องจากผู้ที่มีสิทธิในการเพิ่มเติมข้อมูลควบคุมสิทธิจะมีเพียงเจ้าของทรัพยากรที่เป็นต้นตอของข้อมูลจริงที่ถูกควบคุมเท่านั้น เพราะก่อนการส่งข้อมูลในแต่ละครั้งจำเป็นจะต้องมีการพิสูจน์ฐานะระหว่างเซิร์ฟเวอร์ที่ส่งข้อมูลและเซิร์ฟเวอร์ที่รับข้อมูล (Mutual Authentication) จึงให้เซิร์ฟเวอร์ของคนนอกที่ไม่มีสิ่งยืนยันฐานะ (Server Credential) ก็จะไม่สามารถส่งหรือรับข้อมูลจากเซิร์ฟเวอร์ภายในระบบกริดได้ นอกจากนั้นข้อมูลที่ถูกส่งผ่านระหว่างแต่ละเซิร์ฟเวอร์จะถูกเข้ารหัสกุญแจสาธารณะ (PKI: Public Key Infrastructure) ซึ่งถึงแม้ผู้ประสงค์ร้ายจะสามารถดักเอาข้อมูลที่ถูกส่งภายในเครือข่ายไปได้ ก็จะไม่สามารถเปิดดูข้อมูลภายในได้แต่อย่างใด และปัญหาที่เกิดจากผู้ใช้ทำการเรียกดูข้อมูลที่ถูกเก็บอยู่ภายในฐานข้อมูลแอลแดปโดยตรงก็สามารถป้องกันได้โดยการแก้ไขซอร์สโค้ดของระบบโกลบัสเพื่อบังคับให้ผู้ใช้จำเป็นจะต้องสืบค้นข้อมูลที่ตนต้องการผ่านทางชุดคำสั่งของระบบควบคุมการเข้าถึงข้อมูลเท่านั้น

จากที่ได้อธิบายมาแล้วข้างต้นแสดงให้เห็นว่าระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของบริการเอ็มดีเอสสอดคล้องทั้งในแง่ของการนำไปใช้ในระบบกริด, ความเหมาะสมกับการทำงานภายในแต่ละองค์กรที่พิจารณาบทบาทของผู้ใช้เป็นสิ่งสำคัญ และยังมีโครงสร้างการรักษาความปลอดภัยของข้อมูลที่เหมาะสมอีกด้วย