บทที่ 2

งานวิจัยและทฤษฎีที่เกี่ยวข้อง

2.1 งานวิจัยที่เกี่ยวข้อง

2.1.1 การควบคุมการเรียกใช้ข้อมูลของฐานข้อมูลแอลแด็ป [5]

เป็นงานวิจัยที่ว่าด้วยการเพิ่มเติมข้อมูลควบคุมสิทธิในการเรียกดูข้อมูล (ACL:Access Control List) สำหรับฐานข้อมูลแอลแด็ปเพื่อให้เจ้าของฐานข้อมูลสามารถควบคุมการเรียกข้อมูลของผู้ใช้แต่ละคนได้ โดยในปัจจุบันได้มีงานวิจัยเกี่ยวกับหัวข้อนี้ถูกพัฒนาลงบนฐานข้อมูลหลายรูปแบบ (Netscape Directory Server, UMich LDAP-3.3 และ OpenLDAP) ซึ่งต่างก็ควบคุมการเรียกดูข้อมูลโดยการระบุแอททริบิวท์ของรายละเอียดภายในฐานข้อมูล เช่นชื่อหัวข้อของข้อมูลหรือแอททริบิวท์ของข้อมูลภายนอกดังเช่นแผนกที่ผู้เรียกดูข้อมูลสังกัดอยู่ โดยถึงแม้ว่าเน็ตสเคปจะเปลี่ยนชื่อจาก เอซีแอล (ACL) เป็น เอซีไอ (ACI) แต่ลักษณะการทำงานก็คล้ายคลึงกัน สิ่งที่แตกต่างกันระหว่างระบบควบคุมการเรียกใช้ข้อมูลบนเน็ตสเคปไดเร็คทอรีเซิร์ฟเวอร์และบนฐานข้อมูลแอลแดปชนิดอื่นๆ คือ ข้อมูลควบคุมการเรียกใช้ข้อมูลของเน็ตเคปจะถูกเก็บอยู่ภายในไดเร็คทอรีเซิร์ฟเวอร์ซึ่งจะอยู่ในรูปของฐานข้อมูลแอลแด็ป แต่ฐานข้อมูลแอลแดปชนิดอื่น (UMich และ OpenLDAP) ข้อมูลควบคุมการเรียกใช้ข้อมูลจะถูกเก็บอยู่ภายนอกฐานข้อมูลซึ่งมักจะอยู่ในรูปของไฟล์สตาร์อัพ (Startup File)

โครงสร้างของข้อมูลควบคุมสิทธิบนฐานข้อมูลแอลแดปจะมีรายละเอียดดังต่อไปนี้

```
<access directive> ::= access to <what>
[by <who> <access>] +

<what> ::= * | [dn=<regex>]
[filter=<ldapfilter>]
[attrs=<attrlist>]

<who>  ::= * | self | dn=<regex> |
addr=<regex> |
domain=<regex> |
dnattr=<dn attribute>

<access> ::= [self]none   | [self]compare |
[self]search | [self]read |
[self]write
```

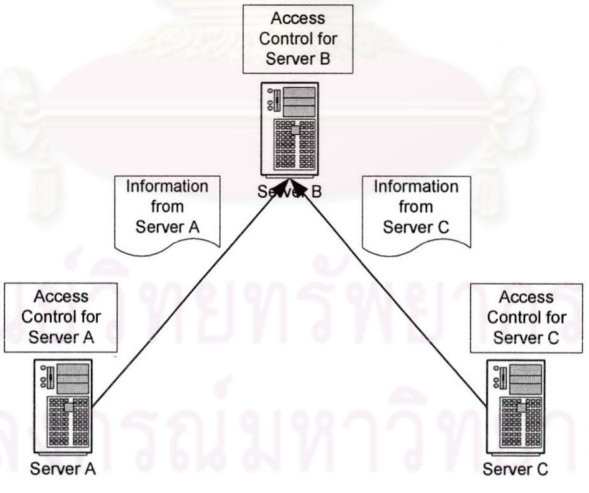
ตัวอย่างของข้อมูลควบคุมสิทธิบนฐานข้อมูลแอลแดปจะมีรายละเอียดดังรูปที่ 2.1

```
access to filter="cn=<newsgroup name>"
     attr=certifiedHost,certifiedAuthor
  by self write
  by dnattr=owner write
  by dn="cn=Manager,ou=People,
     o=<our domain>,c=US" write
  by dn="cn=<News Server IP hostname>,
     ou=Network Hosts,o=<our domain>,
     c=US" read
  by addr=<News Server IP address> read
  by * none

access to attr=MVSpasswd
  by self write
  by dn="cn=Manager,ou=People,
     o=<our domain>,c=US" write
  by addr=<Samba server IP address> read
  by * none
```

รูปที่ 2.1 แสดงตัวอย่างของข้อมูลควบคุมสิทธิ

ภายในระบบการควบคุมการเรียกดูข้อมูลบนมาตรฐานแอลแด็ปจะมีโครงสร้างการแลกเปลี่ยนข้อมูลระหว่างแต่ละเซิร์ฟเวอร์และการกำหนดข้อมูลควบคุมการเรียกดูข้อมูลดังรูปที่ 2.2



รูปที่ 2.2 แสดงโครงสร้างการแลกเปลี่ยนข้อมูลเทียบกับลักษณะการกำหนดข้อมูลควบคุมการเรียกดูข้อมูล

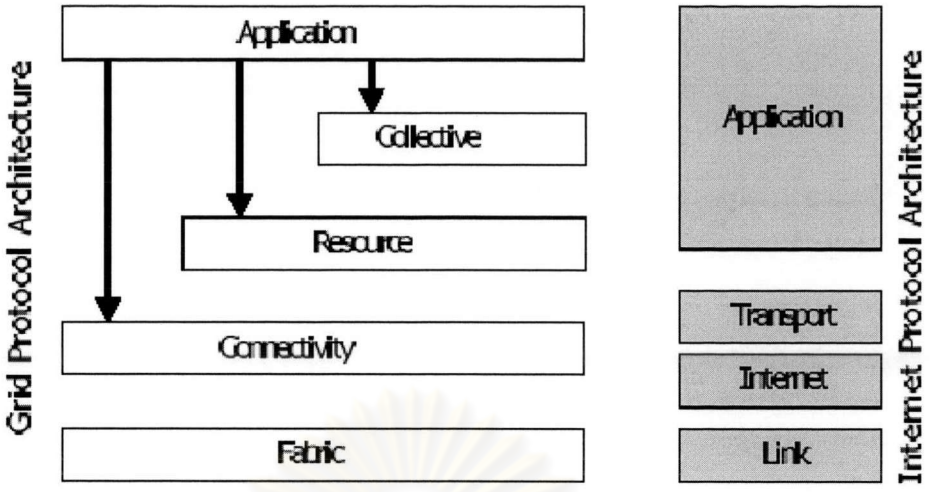
จากรูปที่ 2.2 จะสังเกตได้ว่าถึงแม้ว่าภายในงานวิจัยการควบคุมการเรียกดูข้อมูลภายในฐานข้อมูลแอลแดป จะกำหนดโครงสร้างข้อมูลควบคุมการเรียกดูข้อมูล ซึ่งจะถูกนำไปติดตั้งภายในแต่ละเซิร์ฟเวอร์เพื่อควบคุมการเรียกดูของผู้ใช้ระบบให้เป็นไปตามสิทธิของผู้ใช้แต่ละคน แต่เนื่องจากเซิร์ฟเวอร์จะส่งเฉพาะข้อมูลจริงเท่านั้นโดยจะปล่อยให้ข้อมูลควบคุมสิทธิของเครื่องเซิร์ฟเวอร์ที่รับข้อมูลดังกล่าวเป็นผู้ควบคุมการเรียกดูข้อมูลแทนข้อมูลควบคุมของเครื่องเซิร์ฟเวอร์ที่เป็นเจ้าของข้อมูล จะทำให้เจ้าของข้อมูลไม่สามารถมั่นใจได้ว่าเซิร์ฟเวอร์ที่รับข้อมูลของตนไปจะยังกำหนดสิทธิการเรียกดูข้อมูลตรงกับข้อมูลควบคุมสิทธิของตน และการแก้ไขข้อมูลควบคุมสิทธิในกรณีที่มีการเพิ่มเติมข้อมูลชนิดใหม่ๆก็ทำได้ยากเพราะจำเป็นจะต้องไปแก้ไขข้อมูลสิทธิของแต่ละเซิร์ฟเวอร์ให้สอดคล้องกับข้อมูลที่ถูกเพิ่มเติมเข้ามา ซึ่งจะทำให้ไม่เหมาะสมกับการนำไปใช้ภายในระบบกริดเนื่องจากภายในระบบกริดอาจจะประกอบไปด้วยเซิร์ฟเวอร์จำนวนมาก

2.2 ทฤษฎีที่เกี่ยวข้อง

2.2.1 กริดเทคโนโลยี (Grid Technology) [2]

กริดเป็นระบบแบบกระจายที่กำลังได้รับความสนใจจากนักวิจัยต่างๆทั่วโลก อันเนื่องมาจากกริดมีความสามารถที่จะกำหนดองค์กรเสมือนใดๆ (VO : Virtual Organization) ซึ่งเป็นกลุ่มของทรัพยากรจากแต่ละองค์กรที่ตกลงที่จะมาทำงานร่วมกันเพื่อบรรลุวัตถุประสงค์หนึ่งๆ โดยไม่ขึ้นกับโครงสร้างการเชื่อมต่อจริงของแต่ละองค์กร กริดจะรองรับลักษณะการใช้ทรัพยากรร่วมกันภายในองค์กรเสมือนได้หลายรูปแบบไม่ว่าจะเป็นงานที่จำเป็นต้องการความสามารถในการประมวลผล หรืองานที่จำเป็นต้องมีการติดต่อเปลี่ยนแปลงข้อมูลตลอดเวลา ตลอดจนรองรับชนิดของทรัพยากรที่จะเข้ามารวมอยู่ภายในองค์กรเสมือนได้หลายชนิด โดยจะยังอนุญาตให้เจ้าของทรัพยากรสามารถควบคุมการเรียกใช้งานทรัพยากรของตนโดยผู้ใช้คนอื่นที่อยู่ภายในองค์กรเสมือนเดียวกันได้

โครงสร้างภายในของกริดนั้นได้ถูกแบ่งออกเป็น 5 ชั้น (Layered Architecture) ซึ่งจะอยู่ในรูปของนาฬิกาทราย เพื่อให้ผู้ที่จะพัฒนาซอร์ฟแวร์ที่จะมาติดต่อกับกริดสามารถออกแบบโดยยึดกับมาตรฐานกลางที่ใช้ในการติดต่อแต่ละทรัพยากรภายในกริด โดยมาตรฐานกลางดังกล่าวจะถูกจำกัดให้แคบที่สุดเพื่อให้แน่ใจว่าส่วนต่างๆที่ถูกพัฒนาขึ้นภายในกริดจะสามารถติดต่อกันผ่านทางมาตรฐานกลางโดยไม่เกิดปัญหาอันเนื่องจากการใช้คนละมาตรฐานในการติดต่อดังที่จะแสดงในรูปที่ 2.3



รูปที่ 2.3 แสดงโครงสร้างลำดับชั้นของระบบกริด

รายละเอียดของแต่ละชั้นภายในโครงสร้างของกริดจะมีรายละเอียดดังต่อไปนี้

1. ชั้นฟาบริก (Fabric Layer) เป็นชั้นที่ทำหน้าที่เสมือนตัวเชื่อมต่อระหว่างระบบกริดกับทรัพยากรภายในระบบกริด เพื่อให้ระบบกริดสามารถติดต่อหรือสั่งให้แต่ละทรัพยากรย่อยทำงานตามที่ต้องการได้ ตัวอย่างของชั้นนี้ได้แก่ส่วนต่อเชื่อมกับทรัพยากรฐานข้อมูลเป็นต้น

2. ชั้นคอนเน็ตทิวิตี (Connectivity Layer) เป็นชั้นที่รับผิดชอบเกี่ยวกับมาตรฐานในการติดต่อภายในระบบกริด โดยจะรวมไปถึงมาตรฐานในด้านการควบคุมความปลอดภัยด้วย ตัวอย่างมาตรฐานภายในชั้นนี้ได้แก่ TCP (Transport Control Protocol) หรือ TLS (Transport Layer Security) เป็นต้น

3. ชั้นรีซอร์ส (Resource Layer) เป็นชั้นที่รับผิดชอบบริการต่างๆที่เกี่ยวข้องกับแต่ละทรัพยากรย่อยเพียงอันใดอันหนึ่งเท่านั้น ตัวอย่างของบริการภายในชั้นนี้ได้แก่ การติดต่อขอเรียกดูข้อมูล หรือ การขอใช้ทรัพยากรภายในระบบกริด

4. ชั้นคอลเล็คทีฟ (Collective Layer) เป็นชั้นที่รับผิดชอบบริการต่างๆที่เกี่ยวข้องกับกลุ่มของทรัพยากรภายในระบบกริด ตัวอย่างของบริการภายในชั้นนี้ได้แก่ บริการหาทรัพยากร เป็นต้น

5. ชั้นแอปพลิเคชั่น (Application Layer) เป็นส่วนที่จะอธิบายถึงโปรแกรมใช้งานต่างๆที่จะเข้ามาใช้งานทรัพยากรและบริการต่างๆภายในระบบกริด โดยตัวอย่างของโปรแกรมใช้งานในชั้นนี้ได้แก่ โปรแกรมออกแบบวัตถุดิบที่ต้องการหน่วยประมวลผลจำนวนมาก

2.2.2 ระบบโกลบัส

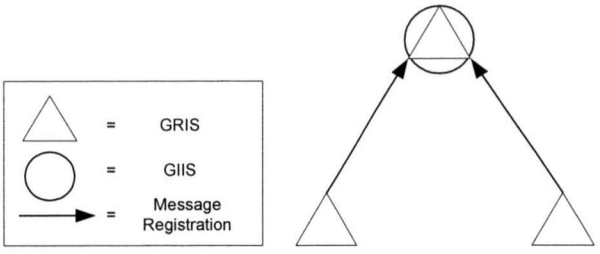
ระบบโกลบัสเป็นกริดซอร์ฟแวร์ที่ทางผู้พัฒนาได้อนุญาตให้นักวิจัยที่มีความสนใจสามารถนำไปทดลองใช้ได้โดยไม่คิดค่าใช้จ่ายแต่อย่างใด โดยในปัจจุบันระบบโกลบัสได้ถูกพัฒนาถึงรุ่น 2.4 ซึ่งเป็นระบบโกลบัสที่ทำงานโดยใช้มาตรฐานของทีซีพีทั่วไป และรุ่น 3.0 ที่จะนำเอามาตรฐานเว็ปเซอร์วิสเข้ามาใช้แทนมาตรฐานเดิม

2.2.2.1 ลักษณะการควบคุมการใช้ทรัพยากรทั่วไปในระบบโกลบัส [1]

ระบบโกลบัสได้พัฒนาฟังก์ชั่นต่างๆที่จำเป็นต้องมีในการทำงานในการใช้ทรัพยากรร่วมกันไม่ว่าจะเป็น การลงทะเบียนเข้าระบบเพียงครั้งเดียว (Single Sign-on) หรือการยืนยันฐานะของผู้ใช้แต่ละคนโดยใช้โครงสร้างการเข้ารหัสสาธารณะ (PKI : Public-Key Infrastructure) ที่จำเป็นต้องมีการกำหนดหน่วยดูแลส่วนกลาง (CA :Central Authorization) เพื่อรับผิดชอบในการสร้างใบรับรองสิทธิของผู้ใช้แต่ละคนในการขอเข้าไปใช้ทรัพยากรต่างๆในองค์กรเสมือน โดยลักษณะการควบคุมทรัพยากรจะเป็นการเปรียบเทียบชื่อเอกเทศของผู้ใช้ (DN: Dintinguished Name) กับชื่อทั่วไปภายในแต่ละเซิร์ฟเวอร์ (Local Account) ที่เจ้าของทรัพยากรสามารถกำหนดสิทธิการใช้งานได้

2.2.2.2 ลักษณะการแลกเปลี่ยนข้อมูลของบริการเอ็มดีเอส [9]

โครงสร้างการแลกเปลี่ยนข้อมูลหรือเอ็มดีเอส (MDS:Monitoring and Discovering Service) จะเป็นส่วนที่รับผิดชอบเกี่ยวกับการแลกเปลี่ยนข้อมูลที่แสดงสภาวะการทำงานและรายละเอียดต่างๆของแต่ละเซิร์ฟเวอร์ภายในระบบโกลบัส ซึ่งเอ็มดีเอสของโกลบัสทูลคิต 2.0 จะพัฒนามาจากมาตรฐานแอลแด็ป (LDAP: Lightweight Directory Access Protocol) โดยภายในเอ็มดีเอสจะประกอบไปด้วยส่วนประกอบย่อยๆได้แก่ จีอาร์ไอเอส (GRIS: Grid Resource Information Service) และ จีไอไอเอส (GIIS: Grid Institution Index Service) โดยจีอาร์ไอเอสจะเป็นผู้รวบรวมเอาข้อมูลเฉพาะเครื่องเซิร์ฟเวอร์ที่หน่วยให้บริการจีอาร์ไอเอสนั้นติดตั้งอยู่ ก่อนที่จะส่งข้อมูลดังกล่าวไปเก็บรวบรวมยังเซิร์ฟเวอร์ที่ติดตั้งหน่วยให้บริการจีไอไอเอส ซึ่งทำหน้าที่เก็บรวบรวมข้อมูลจากแต่ละทรัพยากรย่อยๆ ดังรูปที่ 2.4

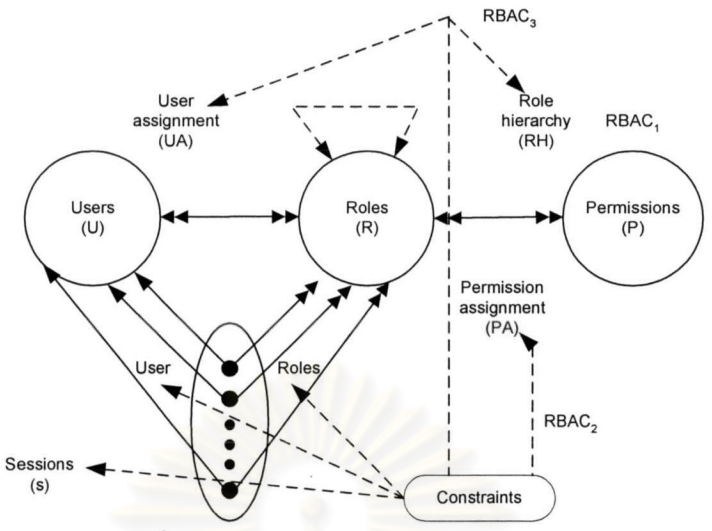


รูปที่ 2.4 แสดงการทำงานของจีอาร์ไอเอสและจีไอไอเอสของบริการเอ็มดีเอส

จากรูปที่ 2.4 แสดงหน่วยบริการเก็บข้อมูลภายในแต่ละทรัพยากรหรือจีอาร์ไอเอสที่ถูกติดตั้งลงบนเซิร์ฟเวอร์ทั้งสาม โดยจีอาร์ไอเอสทั้งสามนี้จะส่งข้อมูลของตนไปเก็บไว้ยังหน่วยเก็บรวบรวมสารบัญข้อมูลหรือจีไอไอเอสของเครื่องเซิร์ฟเวอร์ที่สอง

2.2.3 **แนวคิดการควบคุมตามบทบาท** (RBAC: Role-Based Access Control) [6]

การควบคุมสิทธิของผู้ใช้ในระบบผ่านทางบทบาทของแต่ละคนเป็นแนวความคิดเกี่ยวกับการรักษาความปลอดภัยรูปแบบใหม่ ที่จะอาศัยการกำหนดบทบาทต่างๆขึ้นมาเพื่อมาเป็นตัวคั่นระหว่างผู้ใช้งานและสิทธิของการใช้งานทรัพยากรต่างๆภายในระบบ ทำให้สามารถควบคุมภาพรวมของผู้ใช้งานภายในระบบได้อย่างง่ายดาย เนื่องจากผู้ดูแลระบบย่อยๆทุกคนจะมองเห็นภาพของผู้ใช้งานเป็นภาพเดียวกัน นั่นคือเห็นเป็นบทบาทต่างๆ นอกจากนั้นการควบคุมสิทธิของผู้ใช้ในระบบผ่านทางบทบาทของแต่ละคนยังรองรับการทำงานในลักษณะควบคุมผ่านจุดศูนย์กลางเพราะจะเปิดโอกาสให้จุดศูนย์กลางการควบคุมภายในแต่ละองค์กรสามารถกำหนดสิทธิของแต่ละบทบาทโดยจะเปิดโอกาสให้ผู้ดูแลระบบย่อยๆภายในองค์กรสามารถทำได้แค่กำหนดบทบาทให้แก่ผู้ใช้งานเท่านั้น โดยมีโครงสร้างดังรูปที่ 2.5



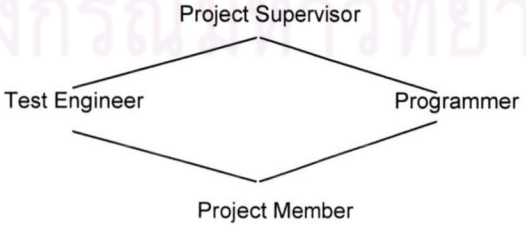
รูปที่ 2.5 แสดงโครงสร้างของระบบควบคุมสิทธิเชิงบทบาท

2.2.3.1 โครงสร้างของแนวความคิดควบคุมสิทธิเชิงบทบาท

ภายในโครงสร้างของแนวความคิดการควบคุมสิทธิตามบทบาทจะมีรายละเอียดในแต่ละขั้นดังต่อไปนี้

1. อาร์แบ็คศูนย์ ($RBAC_0$) เป็นรูปแบบการควบคุมสิทธิตามบทบาทขั้นพื้นฐานคือจะอาศัยการกำหนดบทบาทขึ้นมาคั่นระหว่างผู้ใช้งานและสิทธิการใช้ข้อมูลเพื่อให้ง่ายต่อการดูแลและควบคุมสิทธิการใช้งานของผู้ใช้ระบบแต่ละคน

2. อาร์แบ็คหนึ่ง ($RBAC_1$) นอกจากจะมีโครงสร้างการทำงานของอาร์แบ็คศูนย์แล้วยังจะมีการเพิ่มความสามารถในการกำหนดความสัมพันธ์ระหว่างแต่ละบทบาทให้บทบาทที่มีระดับสูงกว่ามีสิทธิทุกอย่างที่บทบาทที่อยู่ในระดับต่ำกว่าถือครองอยู่ (Role Hierarchy) ดังรูปที่ 2.6



รูปที่ 2.6 แสดงความสัมพันธ์ระหว่างแต่ละบทบาท

จากรูปที่ 2.6 แสดงให้เห็นว่าบทบาท "ผู้พัฒนาระบบ" และ "ผู้ทดสอบระบบ" จะมีสิทธิทั้งหมดเท่าที่บทบาท "สมาชิกโครงการ" มีอยู่ โดยบทบาท "ผู้ทดสอบระบบ" อาจจะถูกเพิ่มเติมสิทธิเท่าที่จำเป็นสำหรับภาระหน้าที่ที่รับผิดชอบอยู่ ซึ่งสิทธิที่ถูกเพิ่มขึ้นมานี้จะไม่ถูกรวมอยู่ในบทบาท "ผู้พัฒนาระบบ" นอกจากนั้น บทบาทในชั้นสูงสุดหรือบทบาท "ผู้ดูแลโครงการ" จะมีสิทธิทั้งหมดเท่าที่บทบาท "สมาชิกโครงการ", "ผู้พัฒนาระบบ" และ "ผู้ทดสอบระบบ" มีอยู่ตามลำดับ

3. อาร์แบ็คสอง ($RBAC_2$) นอกจากจะมีโครงสร้างขั้นพื้นฐานตามที่ได้ถูกระบุไว้ภายในอาร์แบ็คศูนย์แล้ว อาร์แบ็คสองยังมีความสามารถในการระบุเงื่อนไขต่างๆ (Constraints) ซึ่งเกี่ยวข้องกับการระบุบทบาท ดังเช่น ผู้ใช้จะไม่สามารถมีบทบาททั้งสองบทบาทที่ได้ถูกกำหนดไว้พร้อมกันได้ หรือผู้ใช้จำเป็นต้องมีบทบาทหนึ่งๆก่อนที่จะมีบทบาทที่ถูกระบุไว้ได้

4. อาร์แบ็คสาม ($RBAC_3$) จะรวมเอาความสามารถทั้งการกำหนดโครงสร้างของบทบาท (Role Hierarchy) ของอาร์แบ็คหนึ่ง และการกำหนดเงื่อนไข (Constraints) ของอาร์แบ็คสอง ซึ่งอาจจะอยู่ในรูปของการกำหนดเงื่อนไขภายในโครงสร้างของบทบาท ดังเช่นบางบทบาทจะไม่อนุญาตให้มีการสร้างบทบาทที่อยู่สูงกว่าซึ่งจะได้รับสิทธิทั้งหมดของบทบาทที่ถูกระบุไว้

2.2.3.2 **ความแตกต่างระหว่างการกำหนดสิทธิการใช้งานเชิงบทบาทกับการกำหนดกลุ่มของผู้ใช้** (RBAC Vs User Group)

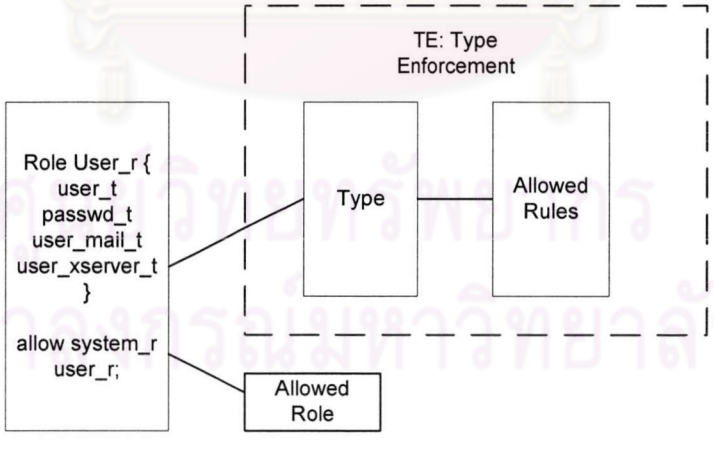
ถึงแม้ในปัจจุบันระบบควบคุมการใช้ทรัพยากรได้มีการกำหนดกลุ่มของผู้ใช้ขึ้นเพื่อให้ง่ายต่อการควบคุมและการกำหนดสิทธิการใช้งาน แต่สิ่งที่แตกต่างระหว่างการกำหนดกลุ่มและการกำหนดบทบาทของผู้ใช้จะอยู่ที่การกำหนดชื่อกลุ่มจะเป็นเพียงแค่การรวบรวมชื่อของผู้ใช้แล้วค่อยนำมากำหนดสิทธิการใช้งานของกลุ่มที่ถูกสร้างขึ้นเพื่อให้เหมาะสมกับสมาชิกภายในกลุ่มซึ่งแตกต่างจากการกำหนดบทบาทที่เสมือนเป็นการรวบรวมสิทธิการใช้งาน (Permission) เข้าไว้ร่วมกัน ก่อนที่จะนำไปกำหนดบทบาทให้กับผู้ใช้แต่ละคนต่อไป

จากความแตกต่างดังกล่าวจะทำให้เห็นได้ว่าการกำหนดสิทธิการใช้งานของแต่ละทรัพยากรโดยการกำหนดชื่อของกลุ่มผู้ใช้ในบางครั้งจำเป็นจะต้องไปพิจารณาสมาชิกทั้งหมดภายในกลุ่มว่าสิทธิที่กำหนดให้แก่กลุ่มนั้นเหมาะสมหรือไม่ในกรณีที่ชื่อกลุ่มไม่แสดงให้เห็นถึงหน้าที่ๆรับผิดชอบของสมาชิกภายในกลุ่มดังเช่น ชื่อกลุ่มที่ถูกกำหนดตามปีที่ผู้ใช้งานได้จดทะเบียนเพื่อขอเข้าใช้ระบบ ซึ่งจะทำให้ยุ่งยากกว่าการกำหนดสิทธิโดยการพิจารณาจากบทบาทที่ถูกกำหนดโดยพิจารณาจากโครงสร้างของบทบาทภายในองค์กรจริง ซึ่งจะทำให้การกำหนดสิทธิของผู้ใช้แต่ละคนจะทำได้อย่างถูกต้อง

2.2.3.3 ตัวอย่างการนำเอาแนวความคิดการควบคุมเชิงบทบาท (RBAC) มาใช้ในปัจจุบัน

- **การนำไปใช้ในระบบปฏิบัติการลินุกซ์ที่ถูกเพิ่มโครงสร้างรักษาความปลอดภัย (Security-Enhanced Linux) [10]**

เนื่องจากแต่เดิมภายในระบบปฏิบัติการลินุกซ์ที่ถูกเพิ่มโครงสร้างการรักษาความปลอดภัย (Security-Enhanced Linux) จะใช้ลักษณะการกำหนดสิทธิการใช้งานตามชนิดของทรัพยากร (Type Enforcement) เป็นหลัก การนำเอาแนวความคิดการควบคุมสิทธิการใช้งานเชิงบทบาทจะเป็นเพียงแค่การกำหนดชื่อของบทบาทเพื่อเก็บรวบรวมสิทธิการใช้งานของทรัพยากรแต่ละชนิดอีกทีหนึ่งซึ่งจะมีลักษณะดังรูปที่ 2.7

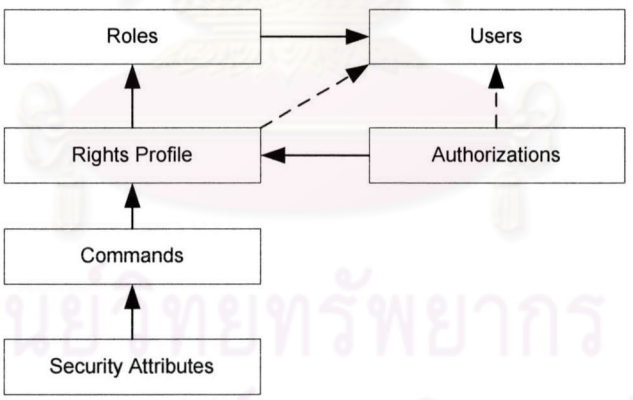


รูปที่ 2.7 แสดงโครงสร้างการกำหนดข้อมูลบทบาทของระบบปฏิบัติการลินุกซ์ที่ถูกเพิ่มโครงสร้างการรักษาความปลอดภัย

จากรูปที่ 2.7 จะแสดงให้เห็นว่าข้อมูลควบคุมบทบาทจะทำหน้าที่เก็บรวบรวมสิทธิว่าผู้ใช้ที่มีบทบาทดังกล่าวจะสามารถติดต่อกับทรัพยากรประเภทอะไรด้วยวิธีใดได้บ้างเท่านั้น ซึ่งแต่ละบทบาทที่ได้ถูกกำหนดขึ้นจะไม่มีความสัมพันธ์ต่อกัน และการเปลี่ยนแปลงบทบาทจำเป็นที่จะต้องให้ผู้ใช้ทำการยืนยันตัวเองอีกครั้งเพื่อป้องกันการเปลี่ยนแปลงบทบาทโดยที่ผู้ใช้ไม่ทราบถึงบทบาทของตัวในปัจจุบัน

- **การนำไปใช้ในระบบปฏิบัติการโซลาริส** (Solaris) [11]

เหตุผลที่ระบบปฏิบัติการโซลาริสได้นำเอาแนวความคิดการควบคุมสิทธิเชิงบทบาทเข้ามาเป็นส่วนหนึ่งของระบบควบคุมการใช้ทรัพยากรของผู้ใช้เพื่อแก้ไขปัญหาการควบคุมทรัพยากรทั้งหมดโดยผู้ที่มีฐานะรูท (Root) เพียงผู้เดียว ซึ่งเป็นลักษณะการรักษาความปลอดภัยของระบบปฏิบัติการทั่วไป การนำเอาแนวความคิดการควบคุมการใช้งานเชิงบทบาทมาใช้จะทำให้สามารถแบ่งความรับผิดชอบออกเป็นแต่ละบทบาทเช่นผู้ดูแลพื้นที่ใช้งานหรือผู้ดูแลโครงสร้างของการเชื่อมต่อเป็นต้น เพื่อป้องกันปัญหาที่เกิดจากการทำงานในลักษณะของรูทซึ่งถ้ามีผู้ที่ไม่ประสงค์ดีได้พาสเวิร์ดไปจะสามารถสร้างความเสียหายได้ทั้งระบบ โดยรูปแบบการกำหนดข้อมูลบทบาทภายในระบบปฏิบัติการโซลาริสจะมีลักษณะดังรูปที่ 2.8



รูปที่ 2.8 แสดงโครงสร้างของการกำหนดข้อมูลบทบาทในระบบปฏิบัติการโซลาริส

จากรูปที่ 2.8 จะเห็นได้ว่าข้อมูลบทบาทจะเกิดจากการรวบรวมข้อมูลกำหนดสิทธิการใช้งานที่มีการระบุว่าสามารถทำอะไรกับทรัพยากรประเภทอะไรได้บ้าง โดยเส้นประจะแทนรูปแบบการกำหนดสิทธิที่เป็นไปได้แต่จะไม่ปลอดภัยและจะสร้างความยุ่งยากให้กับรูปแบบการกำหนดสิทธิของผู้ใช้ภายในระบบ

จากตัวอย่างของการนำเอาแนวความคิดการควบคุมสิทธิการใช้งานผ่านทางบทบาทของผู้ใช้ ไปพัฒนาลงบนระบบปฏิบัติการลินุกซ์ที่ถูกเพิ่มโครงสร้างการรักษาความปลอดภัยและระบบปฏิบัติการโซลาริสจะแสดงให้เห็นถึงการกำหนดสิทธิของการใช้ทรัพยากรประเภทต่างๆที่ตัวบทบาท (Mandatory Mechanism) เพราะทรัพยากรทั้งหมดจะถูกเก็บอยู่ภายในเซิร์ฟเวอร์ที่ติดตั้งระบบปฏิบัติการซึ่งจะหมายถึงจะมีจุดควบคุมเพียงจุดเดียว แต่เนื่องจากแนวความคิดว่าด้วยการควบคุมสิทธิตามบทบาทของผู้ใช้เป็นรูปแบบการกำหนดสิทธิโดยไม่ขึ้นกับนโยบายใดๆ (Policy Neutral) จึงทำให้สามารถกำหนดสิทธิการใช้งานเข้ากับแต่ละบทบาทโดยเจ้าของทรัพยากร (Discretionary Mechanism) ซึ่งเหมาะสมกับการทำงานภายในระบบกริดที่มีจุดควบคุมหลายจุด โดยรายละเอียดของการนำเอาแนวความคิดการควบคุมสิทธิเชิงบทบาทภายในระบบกริดจะกล่าวถึงในส่วนของการออกแบบต่อไป