

ระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส

นายณัฐสุกฤตย์ สงวนดีกุล

ศูนย์วิทยพัชการ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์


คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ปีการศึกษา 2546

ISBN 974-17-3658-4

ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

ROLE-BASED MDS INFORMATION ACCESS CONTROL SYSTEM



Mr. Natthakrit Sanguandikul

A Thesis Submitted in Partial Fulfillment of the Requirements
for the Degree of Master of Engineering in Computer Engineering

Department of Computer Engineering

Faculty of Engineering

Chulalongkorn University

Academic Year 2003

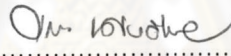
ISBN 974-17-3658-4

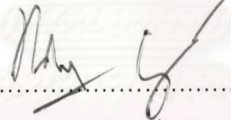
หัวข้อวิทยานิพนธ์ ระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส
โดย นายณัฐฤกษ์กุล สงวนดีกุล
สาขาวิชา วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา อาจารย์ ดร.ณัฐฤกษ์กุล หนูไพโรจน์

คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้บัณฑิตวิทยาลัย
เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาโทบัณฑิต

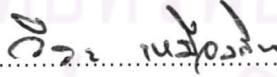

..... คณบดี คณะวิศวกรรมศาสตร์
(ศาสตราจารย์ ดร.สมศักดิ์ ปัญญาแก้ว)

คณะกรรมการสอบวิทยานิพนธ์


..... ประธานกรรมการสอบ
(อาจารย์ ดร.ยรรยง เต็งอำนาจ)


..... อาจารย์ที่ปรึกษา
(อาจารย์ ดร.ณัฐฤกษ์กุล หนูไพโรจน์)


..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.รุ่งรงค์ อุตโยภาส)


..... กรรมการ
(อาจารย์ ดร.วีระ เหมือนสิน)

ศูนย์วิทยุโทรพัสดุ
จุฬาลงกรณ์มหาวิทยาลัย

ณัฐกรฤกษ์ สงวนดีกุล : ระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส. (ROLE-BASED MDS INFORMATION ACCESS CONTROL SYSTEM) อ. ที่ปรึกษา : อ.ดร. ณัฐวุฒิ หนูไพโรจน์, 82 หน้า, ISBN 974-17-3658-4.

เทคโนโลยีกริดได้ถูกพัฒนาขึ้นเพื่อควบคุมการขอใช้ทรัพยากรระหว่างองค์กรตามนโยบายที่ได้กำหนดขึ้นร่วมกัน ทำให้เทคโนโลยีกริดกำลังได้รับความสนใจจากทั้งนักวิจัยและนักพัฒนาระบบแบบกระจาย แต่ระบบโกลบัสซึ่งเป็นกริดซอร์ฟแวร์ ยังขาดความสามารถในการควบคุมการเรียกดูข้อมูลซึ่งถูกคัดลอกและส่งต่อกันระหว่างเซิร์ฟเวอร์ภายในระบบโกลบัส ซึ่งจะเป็นปัญหาสำคัญเมื่อนำเทคโนโลยีกริดไปใช้ภายในโลกธุรกิจเพราะในโลกธุรกิจจะถือว่าข้อมูลต่างๆเป็นทรัพยากรประเภทหนึ่งที่ต้องมีการควบคุมที่เหมาะสม

วิทยานิพนธ์นี้จึงได้เสนอการออกแบบ และพัฒนาต้นแบบระบบการควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส ที่เป็นหน่วยควบคุมการแลกเปลี่ยนข้อมูลระหว่างเซิร์ฟเวอร์ภายในระบบโกลบัส เพื่อเปิดโอกาสให้เจ้าของทรัพยากรสามารถควบคุมการเรียกดูข้อมูลของตนที่ถูกคัดลอกและส่งต่อกันระหว่างเซิร์ฟเวอร์ ซึ่งหัวใจหลักของระบบคือการแนบข้อมูลควบคุมสิทธิการเรียกดูข้อมูลเข้ากับข้อมูลจริงที่มีอยู่เดิม โดยจะยังอาศัยลักษณะโครงสร้างของการแลกเปลี่ยนข้อมูลเดิมของระบบโกลบัสรุ่น 2.0 ซึ่งอยู่ในรูปของมาตรฐานแอลแคปเป็นพื้นฐานสำคัญ นอกจากนี้ ยังมีการนำแนวความคิดของการควบคุมสิทธิเชิงบทบาทมาใช้ เพื่อให้เกิดความสะดวกในการจัดการสิทธิการเข้าถึงสำหรับองค์กรขนาดใหญ่ ถึงแม้ว่างานวิจัยนี้จะใช้เอ็มดีเอสเป็นระบบต้นแบบ แนวความคิดในงานวิจัยนี้สามารถนำไปประยุกต์ใช้กับระบบอื่นได้เช่น ระบบกริดเพื่อการเก็บรวบรวมข้อมูล (Datagrid) เป็นต้น

ศูนย์วิทยทรัพยากร จุฬาลงกรณ์มหาวิทยาลัย

ภาควิชา วิศวกรรมคอมพิวเตอร์
สาขาวิชา วิศวกรรมคอมพิวเตอร์
ปีการศึกษา 2546

ลายมือชื่อนิสิต
ลายมือชื่ออาจารย์ที่ปรึกษา
ลายมือชื่ออาจารย์ที่ปรึกษาร่วม

4570304921 : MAJOR COMPUTER ENGINEERING

KEY WORD: DISTRIBUTED SYSTEM / GRID / ACCESS CONTROL

NATTHAKRIT SANGUANDIKUL: ROLE-BASED MDS INFORMATION ACCESS
CONTROL SYSTEM. THESIS ADVISOR : NATAWUT NUPAIROJ, Ph.D, 82 pp.
ISBN 974-17-3658-4.

Grid technology has been developed to control the access to resources being shared between organizations with mutual cooperated agreement. This makes Grid technology become more attractive to both researchers and distributed system software developers. However, Globus toolkit, which is the open-sourced grid software, still lacks the functionalities to control the information accessing among servers. This will become an important problem, when considering the possibility of using Grid technology in business since businesses consider information as resources, which require proper control mechanisms.

This thesis focuses on the design and implementation of role-based MDS information access control system to provide information owners with access control of information transferred between servers in grid system. This can be done by adding access control information while utilizing the primitive information exchange mechanism in Globus toolkit version 2.0 as a foundation. In addition, the role-based management concept is introduced to simplify the access control management in large organization. Although our prototype is based on MDS, our concept is applicable to other systems, such as Datagrid, as well.

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

DepartmentComputer Engineering.....

Field of studyComputer Engineering.....

Academic year2003.....

Student's signature

Advisor's signature

Co-advisor's signature

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ได้สำเร็จลุล่วงไปได้ด้วยความช่วยเหลืออย่างดียิ่งของ อ.ดร.ณัฐวุฒิ หนูไพโรจน์ อาจารย์ที่ปรึกษา และขอขอบคุณ อ.ดร.ยรรยง เต็งอำนาจ ผศ.ดร.ภูงศ์ อุทโยภาศ อ.ดร.วีระ เหมือนสิน กรรมการวิทยานิพนธ์ที่กรุณาเสียสละเวลาให้คำแนะนำ ตรวจสอบและแก้ไขต้นฉบับวิทยานิพนธ์

ขอขอบคุณพี่ๆ เพื่อนๆ และน้องๆ ในห้องปฏิบัติการวิศวกรรมระบบสารสนเทศที่เสียสละเวลาในการให้คำปรึกษา ช่วยตรวจสอบผลการวิจัย และคำแนะนำต่างๆ ในการเขียนโปรแกรม

สุดท้ายนี้ ผู้วิจัยใคร่ขอกราบขอบพระคุณ มารดา และครอบครัวที่สนับสนุนในด้านต่างๆ และให้กำลังใจแก่ผู้วิจัยเสมอมา

ณัฐกฤตย์ สงวนดีกุล

ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญ

	หน้า
บทคัดย่อภาษาไทย	ง
บทคัดย่อภาษาอังกฤษ	จ
กิตติกรรมประกาศ.....	ฉ
สารบัญ	ช
สารบัญตาราง.....	ฌ
สารบัญภาพ.....	ญ
บทที่ 1 บทนำ.....	1
1.1 ความเป็นมาและความสำคัญของปัญหา	1
1.2 วัตถุประสงค์	5
1.3 ขอบเขตการวิจัย.....	5
1.4 ขั้นตอนในการดำเนินงาน	6
1.5 ประโยชน์ที่จะได้รับ	6
1.6 โครงสร้างวิทยานิพนธ์.....	7
บทที่ 2 งานวิจัยและทฤษฎีที่เกี่ยวข้อง.....	8
2.1 งานวิจัยที่เกี่ยวข้อง	8
2.1.1 การควบคุมการเรียกใช้ข้อมูลของฐานข้อมูลแอลเด็ป	8
2.2 ทฤษฎีที่เกี่ยวข้อง.....	10
2.2.1 กริดเทคโนโลยี (Grid Technology).....	10
2.2.2 ระบบโกลบัล	12
2.2.3 แนวคิดการควบคุมตามบทบาท (RBAC: Role-Based Access Control)	13
บทที่ 3 การออกแบบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส	19
3.1 โครงสร้างและขั้นตอนการทำงานของระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาท	22
3.2 รายละเอียดภายในแต่ละส่วนของระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาท	24
3.2.1 ส่วนควบคุมชนิดและการแลกเปลี่ยนของข้อมูลระหว่างแต่ละเซิร์ฟเวอร์	24
3.2.2 ส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลาง.....	25
3.2.3 ส่วนควบคุมบทบาทส่วนกลาง	27

สารบัญ (ต่อ)

	หน้า
3.2.4 ส่วนติดต่อกับผู้ใช้	28
3.3 การออกแบบข้อมูลควบคุมสิทธิและการกระจายอำนาจการควบคุม	29
3.3.1 ข้อมูลอธิบายสิทธิการเรียกดูข้อมูล	30
3.3.2 ข้อมูลควบคุมบทบาทของผู้ใช้ในองค์กรเสมือน	31
3.3.3 การกระจายอำนาจการควบคุมขององค์ประกอบแต่ละส่วน	31
3.4 การพิจารณาในแง่ของความปลอดภัยของระบบควบคุม.....	33
บทที่ 4 ต้นแบบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส	35
4.1 ส่วนควบคุมชนิดและการแลกเปลี่ยนของข้อมูล	37
4.2 ส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลาง	46
4.3 ส่วนควบคุมบทบาทส่วนกลาง	55
4.4 ส่วนติดต่อกับผู้ใช้	56
บทที่ 5 การทดสอบการใช้งานต้นแบบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาท.....	58
5.1 สภาวะที่ใช้ในการทดสอบ	58
5.2 โครงสร้างของระบบโกลบัลตัวอย่างที่ติดตั้งระบบควบคุมการเข้าถึงข้อมูล	58
5.3 การทดสอบระบบควบคุมการเข้าถึงข้อมูลเชิงบทบาทของเอ็มดีเอส	61
5.3.1 การทดสอบหน่วยควบคุมบทบาทกลาง	62
5.3.2 การทดสอบการทำงานโดยการเรียกดูข้อมูลของผู้ใช้งาน	63
บทที่ 6 การสรุปผลการวิจัยและข้อเสนอแนะ	65
6.1 สรุปผลการวิจัย	65
6.2 ปัญหาและข้อจำกัดที่ได้พบจากการวิจัย	66
6.3 ข้อเสนอแนะ	66
รายการอ้างอิง.....	68
ภาคผนวก.....	69
ภาคผนวก ก.....	70
ประวัติผู้เขียนวิทยานิพนธ์.....	82

สารบัญตาราง

หน้า

ตารางที่ 4.1 แสดงรายละเอียดในการพัฒนาแต่ละองค์ประกอบภายในระบบควบคุม.....	36
ตารางที่ 4.2 แสดงรายละเอียดในการพัฒนาแต่ละองค์ประกอบภายในส่วนเปรียบเทียบสถิติ.....	47
ตารางที่ 5.1 แสดงรายละเอียดของการทดสอบระบบควบคุมการเข้าถึงข้อมูล.....	61



ศูนย์วิทยทรัพยากร
จุฬาลงกรณ์มหาวิทยาลัย

สารบัญภาพ

	หน้า
รูปที่ 1.1 แสดงการแบ่งแยกการควบคุมระหว่างไฟล์ควบคุมและตัวข้อมูล	2
รูปที่ 1.2 แสดงลักษณะการส่งข้อมูลควบคุมไปพร้อมกับข้อมูลจริง.....	3
รูปที่ 1.3 แสดงรูปแบบการรวบรวมข้อมูลภายในระบบกริด.....	4
รูปที่ 2.1 แสดงตัวอย่างของข้อมูลควบคุมสถิติ.....	9
รูปที่ 2.2 แสดงโครงสร้างการแลกเปลี่ยนข้อมูลเทียบกับการกำหนดข้อมูลควบคุม	9
รูปที่ 2.3 แสดงโครงสร้างลำดับชั้นของระบบกริด	11
รูปที่ 2.4 แสดงการทำงานของจีอาร์ไอเอสและจีไอไอเอสของบริการเอ็มดีเอส	13
รูปที่ 2.5 แสดงโครงสร้างของระบบควบคุมสถิติเชิงบทบาท	14
รูปที่ 2.6 แสดงความสัมพันธ์ระหว่างแต่ละบทบาท	14
รูปที่ 2.7 แสดงโครงสร้างการกำหนดข้อมูลบทบาทของระบบปฏิบัติการลินุกซ์.....	16
รูปที่ 2.8 แสดงโครงสร้างของการกำหนดข้อมูลบทบาทในระบบปฏิบัติการโซลาริส.....	17
รูปที่ 3.1 แสดงปัญหาที่เกิดขึ้นภายในหน่วยควบคุมการเปลี่ยนข้อมูลของระบบโกลบัล	19
รูปที่ 3.2 แสดงโครงสร้างทางสถาปัตยกรรมของระบบควบคุมการเข้าถึงข้อมูล.....	20
รูปที่ 3.3 แสดงการทำงานของระบบควบคุมการเรียกดูข้อมูลเชิงบทบาท	21
รูปที่ 3.4 แสดงโครงสร้างภายในระบบควบคุมการเข้าถึงข้อมูลของเอ็มดีเอส	22
รูปที่ 3.5 แสดงลำดับการทำงานของระบบควบคุมการเข้าถึงข้อมูล	23
รูปที่ 3.6 แสดงการแนบข้อมูลควบคุมไปพร้อมกับข้อมูลจริง	24
รูปที่ 3.7 แสดงชนิดของข้อมูลจากส่วนต่างๆที่ถูกพิจารณาโดยหน่วยประมวลผล	25
รูปที่ 3.8 แสดงโครงสร้างภายในส่วนเปรียบเทียบสิทธิการเรียกดูข้อมูลส่วนกลาง.....	25
รูปที่ 3.9 แสดงโครงสร้างของระบบคัดลอกของส่วนควบคุมบทบาท	28
รูปที่ 3.10 แสดงโครงสร้างของแนวความคิดควบคุมสถิติขั้นพื้นฐาน	29
รูปที่ 3.11 แสดงโครงสร้างของข้อมูลควบคุมบทบาทภายในระบบควบคุม	30
รูปที่ 3.12 แสดงขอบเขตการควบคุมสำหรับผู้ดูแลแต่ละชนิด	32
รูปที่ 3.13 แสดงการป้องกันการแก้ไขข้อมูลควบคุมโดยผู้ที่ไม่ประสงค์ดี	33
รูปที่ 4.1 แสดงโครงสร้างความสัมพันธ์ระหว่างข้อมูลแต่ละชนิด.....	35
รูปที่ 4.2 โครงสร้างของต้นแบบระบบควบคุมการเข้าถึงข้อมูล.....	36
รูปที่ 4.3 แสดงโครงสร้างของข้อมูลภายหลังจากที่เพิ่มข้อมูลควบคุม	37

รูปที่ 4.4 แสดงรูปแบบการถูกเรียกโดยบริการเอ็มดีเอสของโปรแกรมเพิ่มเติม ข้อมูลควบคุมสิทธิ.....	41
รูปที่ 4.5 แสดงการเปิดปิดเอ็มดีเอส	45
รูปที่ 4.6 แสดงผลลัพธ์หลังจากทำการเรียกดูข้อมูล	46
รูปที่ 4.7 แสดงข้อมูลที่ส่งต่อระหว่างแต่ละองค์ประกอบย่อยภายในส่วนเปรียบเทียบสิทธิ	47
รูปที่ 4.8 แสดงการแลกเปลี่ยนข้อมูลกับองค์ประกอบอื่นๆของส่วนรับข้อมูลจากผู้ใช้งาน.....	48
รูปที่ 4.9 แสดงผลลัพธ์ที่ได้จากการเรียกใช้ฟังก์ชันของหน่วยสืบค้นข้อมูล	51
รูปที่ 4.10 แสดงลักษณะการวางไฟล์อธิบายของบทบาทภายในขอบเขตขององค์กรจริง.....	53
รูปที่ 4.11 แสดงการทำงานของหน่วยประมวลผล	54
รูปที่ 4.12 แสดงโครงสร้างการกระจายข้อมูลจากเซิร์ฟเวอร์หลัก.....	55
รูปที่ 4.13 แสดงลักษณะการเรียกใช้งานส่วนติดต่อกับผู้ใช้งาน.....	56
รูปที่ 4.14 แสดงผลลัพธ์เมื่อทำการเรียกชุดคำสั่งใหม่ของระบบควบคุม.....	57
รูปที่ 5.1 แสดงการติดตั้งระบบควบคุมการเข้าถึงข้อมูล.....	58
รูปที่ 5.2 แสดงโครงสร้างของต้นไม้ข้อมูลภายในเครื่องเซิร์ฟเวอร์ Apollo 10	60
รูปที่ 5.3 แสดงปัญหาที่เกิดขึ้นเนื่องมาจากความผิดพลาดทางด้านเครือข่าย	62
รูปที่ 5.4 แสดงการระบุระยะเวลาการเก็บข้อมูลบทบาท.....	62
รูปที่ 5.5 แสดงลักษณะการเรียกใช้งาน.....	63
รูปที่ 5.6 แสดงการเปรียบเทียบของผลลัพธ์หลังจากสืบค้นข้อมูลผ่านระบบควบคุม.....	64
รูปที่ 6.1 แสดงปัญหาอันเนื่องมาจากการจัดหมวดหมู่ข้อมูล	66