อัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัว สำหรับระบบการจัดการสิทธิ์ดิจิตอล

A PRIVACY NEGOTIATION ALGORITHM FOR DIGITAL RIGHTS MANAGEMENT

จุไรรัตน์ พุทธรักษ์
JURAIRAT BHUDHARAK

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2547

ISBN 974-15-1255-4

อัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัว
สำหรับระบบการจัดการสิทธิ์ดิจิตอล

A PRIVACY NEGOTIATION ALGORITHM
FOR DIGITAL RIGHTS MANAGEMENT

จุไรรัตน์ พุทธรักษ์
JURAIRAT BHUDHARAK

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาเทคโนโลยีสารสนเทศ
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2547

ISBN 974-15-1255-4

A PRIVACY NEGOTIATION ALGORITHM FOR DIGITAL RIGHTS MANAGEMENT

JURAIRAT BHUDHARAK

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY
SCHOOL OF GRADUATE STUDIES
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2004

ISBN 974-15-1255-4

หัวข้อวิทยานิพนธ์	อัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล
นักศึกษา	นางสาวจุไรรัตน์ พุทธรักษ์
รหัสประจำตัว	44067018
ปริญญา	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
พ.ศ.	2547
อาจารย์ผู้ควบคุมวิทยานิพนธ์	ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์

บทคัดย่อ

ในการกระจายสินค้าหรือเนื้อหาดิจิตอลบนอินเทอร์เน็ตซึ่งเป็นช่องทางที่เหมาะสมสำหรับทั้งผู้ผลิต ผู้จำหน่ายสินค้า และผู้บริโภค แต่อาจถูกคุกคามความเป็นส่วนตัวของผู้ใช้งานได้ ระบบการจัดการสิทธิ์ดิจิตอล (**D**igital **R**ights **M**anagement System) ซึ่งเป็นเทคโนโลยีที่เกี่ยวกับการป้องกันสิทธิ์ของเจ้าของในเนื้อหาดิจิตอล แต่ระบบ DRM ที่เกิดขึ้นในปัจจุบันไม่ได้สนับสนุนการป้องกันข้อมูลส่วนบุคคลของผู้ใช้งานในระบบ งานวิจัยนี้ได้ทดสอบว่าระบบ DRM สามารถออกแบบและสร้างเพื่อป้องกันการสูญเสียความเป็นส่วนตัวของผู้ใช้งานได้ โดยได้ออกแบบนโยบายความเป็นส่วนตัวและการกำหนดความเป็นส่วนตัวของผู้ใช้ เพื่อป้องกันข้อมูลส่วนบุคคลของผู้ใช้จากการทำลายความเป็นส่วนตัวของระบบ DRM และ DRM privacy agent ทำหน้าที่ในการเจรจาต่อรองระหว่างนโยบายของระบบ DRM และการกำหนดความเป็นส่วนตัวของผู้ใช้ จากการดำเนินการวิจัยและทดลองได้พิสูจน์ว่า อัลกอริทึมการเจรจาต่อรองที่นำเสนอมีความเหมาะสมและสามารถเพิ่มประสิทธิภาพในการเจรจาต่อรองให้แก่ระบบ DRM และผู้ใช้ ในการเข้าใช้งานระบบ DRM

Thesis Title	A Privacy Negotiation Algorithm for Digital Rights Management
Student	Miss Jurairat Bhudharak
Student ID.	44067018
Degree	Master of Science
Programme	Information Technology
Year	2004
Thesis Advisor	Asst.Prof.Dr.Chanboon Sathitwiriyawong

ABSTRACT

Internet-based distribution of digital contents provides great opportunities for producers, distributors and consumers, but it may seriously threaten users' privacy. The **D**igital **R**ights **M**anagement (DRM) systems which are one of the current technologies, concern the protection of the ownership/copyright of digital content but the most recent DRM systems do not support the protection of the user's personal information. This paper examines the lack of privacy in DRM systems. A privacy policy and user's privacy preferences model that protect each user's personal information from privacy violation by DRM systems are described. DRM privacy agent is allowed to be the automatic negotiator between the DRM system policy and user's privacy preferences. An effective negotiation algorithm for the DRM system is proposed. The proposed privacy negotiation algorithm can be adapted appropriately to the existing DRM systems to solve the privacy problem effectively.

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้คงจะสำเร็จลุล่วงไปไม่ได้เลยหากไม่ได้รับคำปรึกษาแนะนำและความอนุเคราะห์จาก ผศ.ดร.จันทร์บูรณ์ สถิตวิริยวงศ์ ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ที่ท่านได้ให้ความสนใจห่วงใยและติดตามความก้าวหน้าของการทำวิทยานิพนธ์อย่างใกล้ชิดเสมอมา ตลอดจนให้คำปรึกษาและข้อเสนอแนะที่เป็นประโยชน์อย่างยิ่งในการทำวิทยานิพนธ์แก่ข้าพเจ้า ข้าพเจ้ารู้สึกซาบซึ้งและขอขอบพระคุณเป็นอย่างสูง

ขอบพระคุณครอบครัวอันเป็นที่รักของข้าพเจ้าประกอบไปด้วยคุณพ่อ คุณแม่ และพี่สาวที่เป็นกำลังใจอันดีให้แก่ข้าพเจ้าตลอดมา ข้าพเจ้าคงจะไม่สามารถผ่านพ้นอุปสรรคและความท้อแท้ใจไปได้เลยหากขาดกำลังใจและการสนับสนุนจากครอบครัว ขอบพระคุณญาติๆ ทุกคนที่เป็นกำลังใจให้ข้าพเจ้าด้วยเช่นกัน

นอกจากนี้แล้วข้าพเจ้าขอกราบขอบพระคุณครูอาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทความรู้ให้แก่ข้าพเจ้าตั้งแต่อดีตจนถึงปัจจุบัน

สุดท้ายนี้ข้าพเจ้าขอขอบคุณเพื่อนๆ โดยเฉพาะคุณสุเทพ มะลิวัลย์ และพี่ๆ นักศึกษาทุกคนที่เป็นกำลังใจ ช่วยเหลือ และเต็มใจให้คำปรึกษาในการทำวิทยานิพนธ์แก่ข้าพเจ้ามาโดยตลอด

จุไรรัตน์ พุทธรักษ์

สารบัญ

หน้า

บทคัดย่อภาษาไทย I

บทคัดย่อภาษาอังกฤษ II

กิตติกรรมประกาศ III

สารบัญ IV

สารบัญตาราง VII

สารบัญรูป VIII

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา 1

1.3 สมมติฐานของการศึกษา 2

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย 2

1.5 ขอบเขตของการวิจัย 3

1.6 ขั้นตอนของการศึกษา 3

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 4

2.1 การจัดการสิทธิ์ดิจิตอล 4

2.2 โครงสร้างระบบการจัดการสิทธิ์ดิจิตอล 6

2.2.1 Functional Architecture 6

2.2.2 Information Architecture 7

2.2.3 Reference Architecture 8

2.3 ความเป็นส่วนตัว 10

2.3.1 คำนิยาม 10

2.3.2 กฎหมายและข้อกำหนดความเป็นส่วนตัว 10

2.3.3 Fair Information Principles 11

2.3.4 ความเป็นส่วนตัวและระบบการจัดการสิทธิ์ดิจิตอล 12

2.3.5 เทคโนโลยีความเป็นส่วนตัว 13

2.4 การควบคุมความเป็นส่วนตัวด้วยเทคโนโลยี P3P 15

สารบัญ (ต่อ)

หน้า

2.4.1 P3P Policies 15
2.4.2 Privacy Preferences 16

บทที่ 3 การเพิ่มความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 18
3.1 บทนำ 18
3.2 โครงสร้างความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 18
3.3 องค์ประกอบนโยบายความเป็นส่วนตัว 21
3.3.1 จุดประสงค์ 21
3.3.2 ผู้รับ 22
3.3.3 ระยะเวลาในการเก็บข้อมูล 23
3.3.4 ข้อมูล 23
3.4 การร้องขอข้อมูลผู้ใช้ในระบบ DRM 24
3.5 การกำหนดความเป็นส่วนตัวของผู้ใช้ 26
3.6 อัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัว 27
3.6.1 กระบวนการ Rule Evaluation 28
3.6.2 กระบวนการ Negotiation Process 30
3.7 ขั้นตอนการทำงานของการเจรจาต่อรองความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 32
3.8 การกำหนดน้ำหนักในกระบวนการ Negotiation Process 38
3.9 กระบวนการทดสอบและวิเคราะห์เปรียบเทียบประสิทธิภาพ 44

บทที่ 4 การพัฒนาระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 45
4.1 โครงสร้างระบบ 45
4.2 ขอบเขตของการพัฒนาระบบ 46
4.3 แผนผังการทำงานของระบบ 47
4.4 การพัฒนาระบบ 48

บทที่ 5 การทดลองและผลการทดลอง 49

สารบัญ (ต่อ)

หน้า

5.1 หลักการทดลอง 49
5.2 การออกแบบการทดลองและการเตรียมเครื่องมือ 49
5.2.1 การออกแบบการทดลอง 50
5.2.2 การเตรียมเครื่องมือสำหรับการทดลอง 51
5.3 การวัดประสิทธิภาพ 54
5.4 วิเคราะห์ผลการทดลอง 64

บทที่ 6 สรุปผลการวิจัยและข้อเสนอแนะ 69
6.1 สรุปผลการวิจัย 69
6.2 ปัญหา 70
6.3 ข้อเสนอแนะ 70

เอกสารอ้างอิง 72

ภาคผนวก ก. ต้นแบบ (Prototype) ความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 74
ภาคผนวก ข. XML Schema ของ Policy และ Privacy User's Preferences 83
ภาคผนวก ค. ผลงานทางวิชาการที่ได้รับการตีพิมพ์ 90

ประวัติผู้เขียน 97

สารบัญตาราง

ตารางที่ หน้า

2.1 การเปรียบเทียบข้อดีและข้อเสีย ของวิธีการควบคุมความเป็นส่วนตัว 14

5.1 ตัวอย่างตารางตัวเลขสุ่มของสมาชิกใน Purpose 52

5.2 ตัวอย่างข้อมูลของผู้ใช้ 52

5.3 ตัวอย่างข้อมูลนโยบายของระบบ DRM 53

5.4 ชุดข้อมูลการทดลองชุดที่ 1 54

5.5 การเปรียบเทียบจำนวนความขัดแย้งระหว่าง Fact (Policy) และ Rule (User's privacy preferences) ใน Fact ที่ 1 56

5.6 การเปรียบเทียบจำนวนความขัดแย้งระหว่าง Fact (Policy) และ Rule (User's privacy preferences) ใน Fact ที่ 1-1 ถึง Fact ที่ 1-5 57

5.7 ชุดข้อมูลการทดลองชุดที่ 2 59

5.8 การเปรียบเทียบจำนวนความขัดแย้งระหว่าง Fact (Policy) และ Rule (User's privacy preferences) ใน Fact ที่ 2 61

5.9 การเปรียบเทียบจำนวนความขัดแย้งระหว่าง Fact (Policy) และ Rule (User's privacy preferences) ใน Fact ที่ 2-1 ถึง Fact ที่ 2-5 62

5.10 เปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process 66

สารบัญรูป

รูปที่ หน้า

2.1 Functional Architecture ของ DRM 6

2.2 DRM Core Entities Model ของ Information Architecture 7

2.3 DRM Rights Expression Model ของ Information Architecture 8

2.4 DRM Reference Architecture 8

2.5 บทบาท 3 ส่วนประกอบสำคัญที่กำหนดและป้องกันข้อมูลในการทำงานของการทำพาณิชย์อิเล็กทรอนิกส์ ที่อ้างอิงใน the Directive 11

2.6 ตัวอย่าง P3P Policy 16

2.7 ตัวอย่าง Privacy Preference ใน APPEL 17

3.1 องค์ประกอบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 19

3.2 โครงสร้างการทำงานของ DRM privacy agent 19

3.3 โครงสร้างการแบ่งประเภทของจุดประสงค์ในระบบ DRM 22

3.4 โครงสร้างการแบ่งประเภทของผู้รับในระบบ DRM 22

3.5 โครงสร้างการแบ่งประเภทของระยะเวลาในการเก็บข้อมูลในระบบ DRM 23

3.6 ตัวอย่างการกำหนดนโยบายความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 25

3.7 ตัวอย่างการกำหนดกฎทางเลือกโดยใช้ Conditional Statements 26

3.8 ตัวอย่างการกำหนดความเป็นส่วนตัวของผู้ใช้ 27

3.9 ขั้นตอนการทำงานความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 33

3.10 ขั้นตอนการทำงานของกระบวนการ Check User's privacy preferences 34

3.11 ขั้นตอนการทำงานของกระบวนการ Rule Evaluation 35

3.12 ขั้นตอนการทำงานของกระบวนการ Rule Evaluation กรณีที่ใช้ Conditional Statements 36

3.13 ขั้นตอนการทำงานของกระบวนการ Negotiation Process.....37

3.14 ตัวอย่างการกำหนด Privacy User's Preferences ในเงื่อนไข Free และ Limited 40

3.15 ตัวอย่างการกำหนดนโยบายในระบบ DRM 41

3.16 แผนภูมิต้นไม้การกำหนดความเป็นส่วนตัวของผู้ใช้ในเงื่อนไข Free และ Limited 42

4.1 โครงสร้างของระบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 45

4.2 แผนผังการทำงานความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 47

สารบัญรูป (ต่อ)

รูปที่ หน้า

5.1 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (User's Privacy Preferences) ใน Fact ที่ 1 58

5.2 การเปรียบเทียบเปอร์เซ็นต์การลดกระบวนการ Negotiation Process ของข้อมูลการทดลองชุดที่1 58

5.3 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (Privacy User's Preferences) ใน Fact ที่ 2 63

5.4 การเปรียบเทียบเปอร์เซ็นต์การลดกระบวนการ Negotiation Process ของข้อมูลการทดลองชุดที่ 2 63

5.5 ความสัมพันธ์ระหว่างจำนวน Conditional Statements กับ % เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process ในข้อมูลชุดที่ 1 67

5.6 ความสัมพันธ์ระหว่างจำนวน Conditional Statements กับ % เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process ในข้อมูลชุดที่ 2 67

ก.1 แผนผังการทำงานของระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล 75

ก.2 หน้าจอแรกเมื่อผู้ใช้เข้าสู่ระบบการจัดการสิทธิ์ดิจิตอล 76

ก.3 เมื่อผู้ใช้ต้องการลงทะเบียนเป็นสมาชิกในระบบ 77

ก.4 ข้อมูลชื่อของผู้ใช้และรหัสผ่านที่ผู้ใช้จำเป็นต้องติดต่อกับระบบ 77

ก.5 เนื้อหาและนโยบายของเนื้อหาทั้งหมดที่ระบบให้บริการเพื่อให้ผู้ใช้เลือกเพื่อทำข้อตกลงการใช้เนื้อหาต่อไป 78

ก.6 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM Policy และ User's Privacy Preferences และไม่เกิดความขัดแย้ง 79

ก.7 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM Policy และ User's Privacy Preferences และเกิดความขัดแย้งขึ้น 79

ก.8 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM Policy และ User's privacy preferences กรณีที่ระบบใช้ Conditional Statements ในการแก้ปัญหาความขัดแย้งในกระบวนการ Rule Evaluation 70

สารบัญรูป (ต่อ)

รูปที่ หน้า

ก.9 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM Policy และ User's privacy preferences กรณีที่ระบบใช้ Conditional Statements ในการแก้ปัญหาความขัดแย้งโดยเลือกกฎที่ดีที่สุดในกระบวนการ Negotiation Process 81

ก.10 การทำข้อตกลงระหว่างผู้ใช้กับเนื้อหาที่ระบบให้บริการ 81

ก.11 การเริ่มต้น Rendering Application ในเนื้อหาตามที่ผู้ใช้ได้ทำข้อตกลงกับระบบเอาไว้ 82

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันระบบพาณิชย์อิเล็กทรอนิกส์และอินเทอร์เน็ต เปรียบเสมือนคลังที่เก็บรวบรวมและใช้งานข้อมูลสารสนเทศของผู้บริโภค ซึ่งข้อมูลสารสนเทศของผู้บริโภคโดยเฉพาะข้อมูลส่วนบุคคล ที่นำไปใช้ในเชิงพาณิชย์อิเล็กทรอนิกส์ อาจถูกเก็บหรือขายโดยปราศจากการรับรู้และการยินยอมจากเจ้าของ ซึ่งความสามารถของระบบพาณิชย์อิเล็กทรอนิกส์นั้นทำให้เกิดปัญหาความเป็นส่วนตัวแก่ผู้บริโภคเป็นอย่างยิ่ง และด้วยความสามารถของระบบการจัดการสิทธิ์ดิจิตอล หรือ **D**igital **R**ights **M**anagement (DRM) ซึ่งให้สิทธิ์แก่เจ้าของ และตัวแทนจำหน่ายเนื้อหาดิจิตอลในการจัดการและกำหนดสิทธิ์การใช้งานเนื้อหาดิจิตอลแก่ผู้ใช้หรือผู้บริโภค โดยข้อมูลสารสนเทศและประวัติการใช้งานของผู้ใช้จะถูกเก็บและนำไปใช้ตามความต้องการของเจ้าของและตัวแทนจำหน่ายเนื้อหาดิจิตอล ซึ่งการนำข้อมูลเหล่านี้ไปใช้นำไปสู่การละเมิดหรือการคุกคามความเป็นส่วนตัวของผู้ใช้ได้ และในระบบ DRM ปัจจุบันได้ปกป้องสิทธิ์ในส่วนของผู้เป็นเจ้าของเท่านั้น ซึ่งจำเป็นอย่างยิ่งที่จะต้องมีการปกป้องสิทธิ์ในส่วนผู้บริโภคหรือผู้ใช้ด้วย เพื่อทำให้การทำงานของระบบ DRM มีความสมดุลทั้งเจ้าของสิทธิ์และผู้ใช้สิทธิ์ของระบบ ดังนั้นการเพิ่มความเป็นส่วนตัวให้แก่ระบบ DRM จึงเป็นสิ่งที่ควรพิจารณาเป็นอันดับแรกในการออกแบบระบบ DRM

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

1. เพื่อเพิ่มความเป็นส่วนตัวแก่ผู้ใช้ในระบบการจัดการสิทธิ์ดิจิตอล (DRM) โดยอาศัยหลักปฏิบัติพื้นฐานในการเก็บรวบรวมข้อมูลส่วนบุคคลของผู้ใช้ และออกแบบกฎความเป็นส่วนตัวแก่ระบบ DRM
2. เพื่อศึกษาการกำหนดนโยบาย และความเป็นส่วนตัวของผู้ใช้ โดยอ้างอิงเทคโนโลยี P3P และปรับให้เข้ากับระบบ DRM
3. เพื่อพัฒนาให้ระบบ DRM มีความยืดหยุ่นและการประนีประนอมในการกำหนดนโยบายและเจรจาต่อรองความเป็นส่วนตัวระหว่างผู้ใช้กับระบบ DRM
4. เพื่อพัฒนาอัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวเพื่อหากฎ (Best Matching Rule) ที่เหมาะสมระหว่างผู้ใช้และระบบ DRM
5. เพื่อรักษาสิทธิ์ความเป็นส่วนตัวของผู้ใช้ในระบบ DRM

1.3 สมมติฐานของการศึกษา

จากการศึกษาการทำงานของระบบ DRM ซึ่งเป็นการปกป้องสิทธิ์ในเนื้อหาดิจิตอลที่ผู้เป็นเจ้าของหรือผู้จำหน่าย ต้องการกำหนดสิทธิ์ในการกระจายเนื้อหาดิจิตอลนั้นๆ ไปยังผู้ใช้หรือผู้บริโภค เพื่อมิให้มีการละเมิดลิขสิทธิ์ความเป็นเจ้าของในเนื้อหาดิจิตอลนั้น จากการศึกษาจะเห็นได้ว่าระบบ DRM ในปัจจุบันปกป้องเพียงสิทธิ์ผู้เป็นเจ้าของและผู้จำหน่ายเนื้อหาดิจิตอลเท่านั้น แต่เมื่อผู้ใช้ระบบ DRM เข้ามาใช้งานในระบบแล้ว ข้อมูลส่วนตัวของผู้ใช้ที่ให้แก่ระบบและประวัติการใช้งาน จะถูกเก็บรวบรวมโดยระบบ DRM ซึ่งจะเป็นผู้จัดการข้อมูลเหล่านั้น ข้อมูลของผู้ใช้อาจถูกนำไปขาย หรือเพื่อผลประโยชน์ทางการค้าหรือทางการตลาดอื่นๆ โดยที่เจ้าของเนื้อหาและผู้จำหน่ายเนื้อหาดิจิตอลไม่ได้แจ้งนโยบายการนำข้อมูลของผู้ใช้ระบบให้ผู้ใช้ทราบ ซึ่งถือว่าเป็นการคุกคามความเป็นส่วนตัวของผู้ใช้หรือผู้บริโภคนั่นเอง ดังนั้นในการทำงานของระบบ DRM ถ้านำหลักการ นโยบาย และเทคนิคความเป็นส่วนตัวเพิ่มเข้าไปในระบบ DRM แล้ว ผู้ใช้จะได้รับการปกป้องสิทธิ์การนำข้อมูลส่วนบุคคลและประวัติการใช้งานในระบบ DRM เพิ่มขึ้น ทั้งยังทำให้ระบบ DRM สามารถกำหนดนโยบายความเป็นส่วนตัวที่มีความยืดหยุ่นและประนีประนอมในระบบแก่ผู้ใช้ได้

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

ในงานวิจัยนี้ได้นำเอาแนวคิดความเป็นส่วนตัวมาเป็นหลักการเบื้องต้นของแนวคิดในการพัฒนาการทำงานของระบบการจัดการสิทธิ์ดิจิตอล และพยายามแก้ปัญหาการละเมิดความเป็นส่วนตัวที่เกิดขึ้นในระบบ DRM ในปัจจุบัน โดยได้นำหลักการความเป็นส่วนตัว Fair Information Principles ซึ่งเป็นที่ยอมรับกันอย่างกว้างขวาง และง่ายในการทำความเข้าใจและปฏิบัติ ซึ่งใช้ในการแก้ปัญหาในการเก็บข้อมูลและการใช้งานของผู้ใช้อย่างเป็นธรรม ตามกฎหมายความเป็นส่วนตัวที่ได้ระบุเอาไว้ในแต่ละประเทศ และจากหลักการความเป็นส่วนตัวของสหภาพยุโรป (European Union Privacy principles) ซึ่งกล่าวถึงโครงสร้างของบทบาทหลัก คือ Data Subject, Data Controller และ Data Processor โดยนำมาออกแบบการจัดการความเป็นส่วนตัวสำหรับระบบ DRM และนอกจากนี้งานวิจัยนี้ได้อ้างอิงเทคโนโลยี P3P ซึ่งเป็นเทคนิคความเป็นส่วนตัว ในการกำหนดนโยบายของผู้ใช้และองค์กร ซึ่งเป็นที่ยอมรับและมีประสิทธิภาพในการกำหนดนโยบายความเป็นส่วนตัวของผู้ใช้และนโยบายของเจ้าของเว็บไซต์ ซึ่งงานวิจัยได้อ้างอิงหลักการและเทคนิคดังกล่าวเข้ามาปรับและแก้ปัญหาการคุกคามความเป็นส่วนที่เกิดขึ้นในระบบการจัดการสิทธิ์ดิจิตอล เพื่อสร้างให้ระบบประนีประนอม และป้องกันการสูญเสียความเป็นส่วนตัวของผู้ใช้ได้อย่างมีประสิทธิภาพ

1.5 ขอบเขตของการวิจัย

งานวิจัยนี้ได้นำเสนอการจัดการความเป็นส่วนตัวให้แก่ผู้ใช้ในระบบ DRM โดยเน้นกลไกการออกแบบนโยบาย (policies) ที่ยืดหยุ่น และการกำหนดความเป็นส่วนตัวของผู้ใช้ (Users' Privacy Preferences) ให้มีความเหมาะสมกับระบบ DRM และได้ออกแบบอัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวระหว่างผู้ใช้กับระบบ DRM เพื่อค้นหารูปแบบกฎที่เหมาะสมที่สุดให้แก่ระบบ DRM ในการที่ผู้ใช้สามารถเข้าใช้งานระบบ DRM ได้ ซึ่งในการออกแบบนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้เหล่านี้ได้นำหลักปฏิบัติ Fair Information Principles และหลักการความเป็นส่วนตัวของสหภาพยุโรป รวมทั้งอ้างอิงเทคโนโลยี P3P มาปรับให้เข้ากันได้กับระบบ เพื่อให้ผู้ใช้หรือผู้บริโภคเนื้อหาดิจิตอลได้รับความเป็นส่วนตัวเพิ่มขึ้น

1.6 ขั้นตอนของการศึกษา

1. ศึกษาการทำงานของระบบการจัดการสิทธิ์ดิจิตอลที่ใช้กันทั่วไปในระบบอินเทอร์เน็ต
2. ศึกษานโยบายความเป็นส่วนตัวและหลักการ Fair Information Principles และหลักการความเป็นส่วนตัวของสหภาพยุโรป (European Union Privacy Principles)
3. ศึกษาเทคโนโลยี P3P เพื่อปรับปรุงรูปแบบการกำหนดความเป็นส่วนตัวของผู้ใช้และนโยบายให้เข้ากันได้กับในระบบการจัดการสิทธิ์ดิจิตอล
4. ออกแบบอัลกอริทึมและโครงสร้างความเป็นส่วนตัวแก่ระบบการจัดการสิทธิ์ดิจิตอล โดยนำหลักการและเทคโนโลยีต่างๆ มาปรับใช้ร่วมด้วยกัน
5. วิเคราะห์เพื่อเลือกหาแนวทางในการออกแบบการเพิ่มความเป็นส่วนตัวในแก่ระบบการจัดการสิทธิ์ดิจิตอล
6. ทดลองและทดสอบความเป็นส่วนตัวของระบบการจัดการสิทธิ์ดิจิตอล และประเมินผลการทำงานของระบบ

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 การจัดการสิทธิ์ดิจิตอล

เนื้อหา (content) เช่น หนังสือ วิดีโอเทป เพลง ซึ่งเก็บในสื่อชนิดต่างๆ ได้ถูกเปลี่ยนมาอยู่ในรูปแบบของดิจิตอลมากขึ้นเพื่อความสะดวก และถูกกระจายอยู่ทั่วไปบนอินเทอร์เน็ต ซึ่งง่ายต่อการคัดลอก การขโมย และเกิดการละเมิดลิขสิทธิ์ความเป็นเจ้าของ ทำให้จำเป็นจะต้องพัฒนาวิธีการเพื่อป้องกันการกระทำเหล่านั้น การจัดการสิทธิ์ดิจิตอล หรือ **D**igital **R**ights **M**anagement (DRM) เป็นความพยายามที่จะแก้ปัญหาที่เกิดขึ้นเหล่านี้ โดยพิจารณาปัญหาเป็น 3 กลุ่มใหญ่ [1] นั่นคือ ทางเทคโนโลยี ทางเศรษฐศาสตร์ และทางกฎหมาย โดยการแก้ปัญหาดังกล่าวที่ดีที่สุดคือการประนีประนอมความเป็นไปได้ทั้งทางด้านเทคโนโลยี ต้นทุน ง่ายต่อการใช้งาน และทางด้านกฎหมายที่เกี่ยวกับความเป็นส่วนตัวและสิทธิของผู้ใช้

การจัดการสิทธิ์ดิจิตอลได้ถูกนิยามไว้มากมายดังนี้

นิยามที่ 1 "การจัดการสิทธิ์ดิจิตอลเกี่ยวข้องกับการป้องกันกรรมสิทธิ์หรือลิขสิทธิ์ในเนื้อหาดิจิตอลจากการใช้งานที่ผิดกฎหมาย โดยการจำกัดการกระทำของผู้บริโภคให้กระทำได้ตามที่อนุญาตในเนื้อหาดิจิตอลเท่านั้น" [17] จากนิยามข้างต้นจำกัดในความหมายของเนื้อหาดิจิตอลและผู้บริโภคเท่านั้น

นิยามที่ 2 "DRM เป็นเทคโนโลยีที่สามารถ กระจาย ส่งเสริม และขายเนื้อหาดิจิตอลอย่างปลอดภัยบนเครือข่ายอินเทอร์เน็ต" [17] จากนิยามเป็นมุมมองการกระจายเนื้อหาบนระบบอีคอมเมิร์ซ

นิยามที่ 3 "DRM เป็นรูปแบบทางธุรกิจและเทคโนโลยีที่ช่วยป้องกัน และเป็นประโยชน์สำหรับเนื้อหาที่เป็นหนังสือ รูปภาพ เพลง หรือ วิดีโอที่อยู่ในรูปแบบของดิจิตอล" [15]

นิยามที่ 4 "DRM เป็นการจัดการในเรื่องของสิทธิ์ โดยที่ DRM จะจัดการสิทธิ์ทั้งหมดไม่เฉพาะสิทธิ์ในเนื้อหาดิจิตอลเท่านั้น" [1] จากนิยามนี้ IPRSystems ซึ่งเป็นผู้พัฒนาภาษาในการแสดงสิทธิ์ (language for expressing rights) บนทรัพย์สินดิจิตอล

ในยุคเริ่มแรกของการพัฒนาระบบ DRM จะเน้นไปบนความปลอดภัยและการเข้ารหัสแก่เนื้อหาดิจิตอล ซึ่งเป็นการแก้ปัญหาจากการคัดลอกที่ไม่ได้รับอนุญาต และเป็นการป้องกัน จำกัดการกระจายเนื้อหาดิจิตอล โดยอนุญาตให้แก่ผู้ที่ชำระเงินแล้วเท่านั้น ซึ่งยังเป็นการทำงานที่จำกัด เมื่อกล่าวถึงความสามารถของ DRM ที่สมควรจะเป็น ทำให้ยุคถัดมาของระบบ DRM จะต้องครอบคลุมถึงการบรรยาย (rights description) การระบุ (identification) การทำการค้า (trading rules) การแลกเปลี่ยน (trading) การป้องกัน (protection) การเฝ้าสังเกต (monitoring) และการติดตาม

(tracking) การทำงานในรูปแบบทั้งหมดของการใช้งานสิทธิ์ โดยครอบคลุมทั้งทรัพย์สินที่จับต้องได้และทรัพย์สินที่จับต้องไม่ได้ รวมถึงการจัดการสิทธิ์ของผู้เป็นเจ้าของ [1]

เทคโนโลยี DRM จึงกลายเป็นความท้าทายที่เกิดขึ้นในยุคดิจิตอล เพื่อป้องกันการละเมิดในกรรมสิทธิ์และลิขสิทธิ์ของผู้สร้างเนื้อหาดิจิตอลจากการใช้งานของผู้บริโภคที่ไม่ได้รับอนุญาต หรือนำไปใช้ในทางที่ผิด เนื่องจากข้อมูลดิจิตอลเหล่านี้ง่ายต่อการได้มา การคัดลอก และหรือการแชร์ข้อมูลให้แก่ผู้อื่นอย่างผิดกฎหมาย ผู้สร้างและกระจายเนื้อหาดิจิตอลบนเครือข่ายอินเทอร์เน็ตจำเป็นอย่างยิ่งที่ต้องการเทคโนโลยีที่รองรับการควบคุมสิทธิ์การใช้งานเหล่านี้ แต่อย่างไรก็ตามเทคโนโลยีนี้อาจจะจำกัดผู้บริโภคในการใช้งานเนื้อหาดิจิตอล โดยปราศจากความยุติธรรมในการใช้งานเนื้อหาดิจิตอล ซึ่งผู้ใช้ควรจะได้รับสิทธิ์ในการใช้งานตามสิทธิ์ที่ผู้ใช้ควรจะได้รับโดยไม่ขัดต่อกฎหมาย ผู้ผลิต DRM หลายๆค่าย เช่น Microsoft [18], IBM [19], InterTrust [20] หรือ Real [21] ต่างได้ออกแบบระบบ DRM ให้เหมาะสมกับเทคโนโลยีของตน โดยมีมาตรฐานต่างกันไป ทำให้เทคโนโลยี DRM ได้พัฒนาไปอย่างรวดเร็ว และยากต่อการเลือกใช้ตามความเหมาะสมของระบบของผู้สร้างเนื้อหาดิจิตอล แม้ว่าผู้สร้างเนื้อหาดิจิตอลต้องการ การแก้ปัญหาพื้นฐานในการป้องกันการเข้าใช้งานที่ผิดกฎหมาย แต่ยังมีหลายๆ ปัจจัยรบกวนที่เกิดขึ้นในกระบวนการการรวมระบบเหล่านี้เข้าด้วยกัน

- มีความหลากหลายของเทคโนโลยี DRM ในการเสนอทางแก้ปัญหาที่เกิดขึ้น
- มีความยากในการสร้างมาตรฐาน ให้เป็นมาตรฐานทั่วไปสำหรับเทคโนโลยี DRM
- จำเป็นที่จะต้องออกแบบความปลอดภัยในระดับต่างๆ กัน ให้แก่ระบบ DRM
- ยากต่อการสร้างระบบ DRM ผนวกเข้าไปยังอุปกรณ์ชนิดต่างๆ เช่น ต่ออุปกรณ์สื่อสารเคลื่อนที่
- การขัดต่อกฎหมายและหลักจรรยาในการจำกัดการใช้งานของผู้บริโภคในระบบ DRM
- การสร้างระบบให้มีความจูงใจสำหรับผู้บริโภคในการเข้าใช้ระบบที่มีเทคโนโลยี DRM

จากนิยามและเทคโนโลยี DRM ที่กล่าวถึงข้างต้นนำไปสู่การออกแบบกระบวนการทำงานบนมาตรฐานต่างๆ เช่น W3C, IETF, MPEG, OASIS และอีกมากมาย ซึ่งในหัวข้อถัดไปจะกล่าวถึงโครงสร้างของระบบ DRM และ ภาษาที่ใช้ในการกำหนดสิทธิ์ในระบบการจัดการสิทธิ์ดิจิตอลต่อไป

2.2 โครงสร้างระบบการจัดการสิทธิ์ดิจิตอล

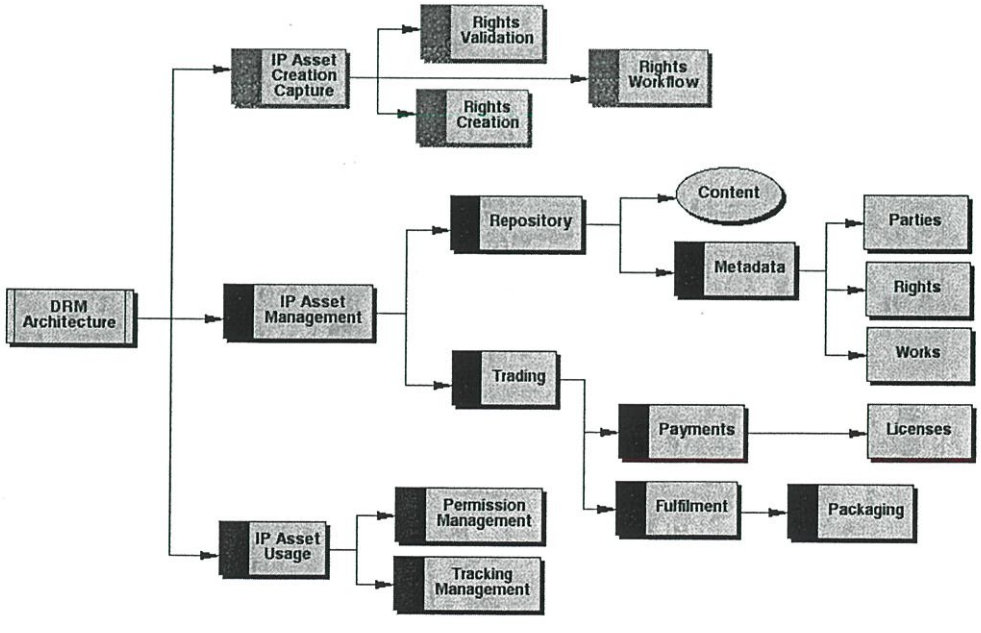
ในการออกแบบและการสร้างระบบ DRM มีโครงสร้างสำคัญที่ต้องพิจารณานั่น [1] คือ Functional Architecture ที่ครอบคลุมโมดูลระดับแนวคิดหรือองค์ประกอบของระบบ DRM ที่ใช้เพื่อการจัดการสิทธิ์ และโครงสร้างที่สำคัญถัดไปคือ Information Architecture ซึ่งจะครอบคลุมแบบจำลองความสัมพันธ์ของเอ็นติตี้ในระบบ DRM

2.2.1 Functional Architecture

ในการสร้างระบบ DRM ที่เหมาะสมนั้น สามารถแบ่งการทำงานเป็น 3 หน้าที่หลักคือ

- *Intellectual Property (IP) Asset Creation and Capture* - DRM จะจัดการการสร้างเนื้อหาให้ง่ายในการทำการค้า และรวมสิทธิ์ของเจ้าของเข้าไปในเนื้อหาที่ถูกสร้างเป็นครั้งแรกได้อย่างไร
- *IP Asset management* - DRM จะจัดการการค้าเนื้อหา และนำเนื้อหาจากผู้สร้างเข้าไปในระบบการจัดการทรัพย์สินได้อย่างไร ซึ่งในระบบการทำการค้าต้องการการอธิบายด้วย metadata และ สิทธิ์การใช้งาน
- *IP Asset Usage* - DRM จะจัดการการใช้เนื้อหาเมื่อมีการทำการค้า และการสนับสนุนข้อจำกัดที่อยู่นอกเหนือการทำการค้าหรือแลกเปลี่ยนเนื้อหาที่เจาะจงบนระบบหรือซอฟต์แวร์ได้อย่างไร

จากข้างต้นเป็นความต้องการที่ Functional Architecture ได้กำหนดกรอบความต้องการของ DRM ซึ่งแสดงไว้ดังรูปที่ 2.1



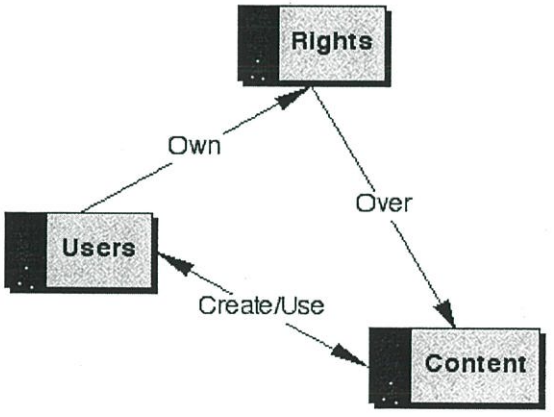
รูปที่ 2.1 Functional Architecture ของ DRM

2.2.2 Information Architecture

Information Architecture เกี่ยวข้องกับแบบจำลองความสัมพันธ์ของเอ็นติตี้ในระบบ DRM ประกอบด้วย

- *Modeling the entities*

พื้นฐานสำคัญของแบบจำลองระบบ DRM คือการแยกและการระบุอย่างชัดเจนถึงความสัมพันธ์ของเอ็นติตี้หลัก 3 ชนิด นั่นคือ ผู้ใช้ เนื้อหาดิจิตอล และ สิทธิ์ ดังแสดงในรูปที่ 2.2 โดยที่ผู้ใช้จะเป็นผู้ร้องขอการใช้งานใดๆ จากผู้เป็นเจ้าของเนื้อหาดิจิตอล รวมทั้งเจ้าของเนื้อหาดิจิตอลในการสร้างเนื้อหาเหล่านั้น ในส่วนสิทธิ์เป็นการแสดงถึงการยินยอม การบังคับ และข้อตกลง ระหว่างผู้ใช้และเนื้อหาดิจิตอล เหตุผลหลักของแบบจำลองนี้คือการจัดเตรียมให้มีความยืดหยุ่นเมื่อกำหนดสิทธิ์ให้แก่ผู้ใช้และเนื้อหาดิจิตอล



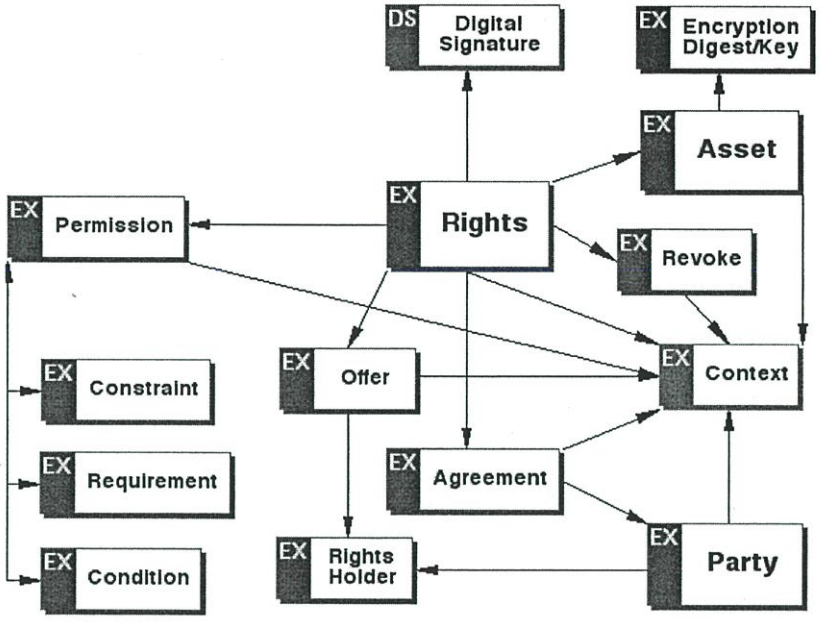
รูปที่ 2.2 DRM Core Entities Model ของ Information Architecture

- *Identifying and describing the entities*

เอ็นติตี้แต่ละชนิดต้องการการพิสูจน์และการบรรยาย โดยการพิสูจน์จะต้องเป็นกลไกที่เป็นมาตรฐาน เอ็นติตี้และ metadata จะต้องทำการพิสูจน์ได้ และมาตรฐานเช่น URI , DOI และ ISTC เป็นมาตรฐานที่ใช้พิสูจน์สิทธิ์

- *Expressing the rights statement*

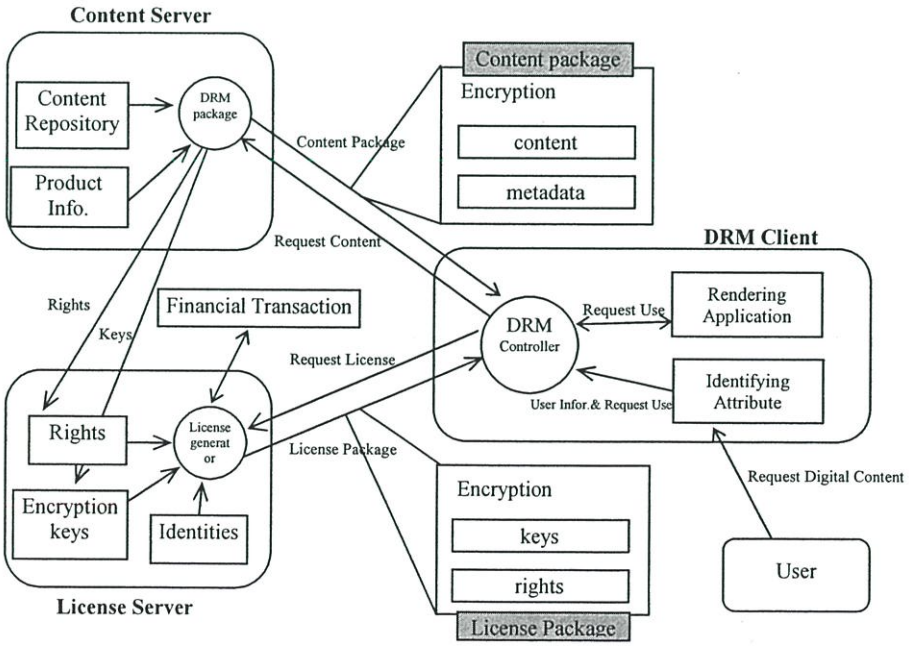
สิทธิ์เป็นการอนุญาตการแสดงถึงการยินยอม การบังคับ ข้อตกลง และความสัมพันธ์อื่นๆ ระหว่างผู้ใช้และเนื้อหาดิจิตอล การแสดงสิทธิ์จำเป็นต้องแสดงด้วยภาษาที่มีความหมาย เพื่อให้ผู้ใช้เข้าใจความสัมพันธ์เหล่านั้น โดยภาษาที่ใช้ในการแสดงสิทธิ์คือ Open Digital Rights Language (ODRL) แสดงดังรูปที่ 2.3



รูปที่ 2.3 DRM Rights Expression Model ของ Information Architecture

2.2.3 Reference Architecture

สำหรับโครงสร้างของ DRM [2,15] ที่นำมาอ้างอิงนี้ มีองค์ประกอบหลักที่สำคัญ 3 ส่วน แสดงในรูปที่ 2.4 ประกอบด้วย Content Server, License Server และ DRM Client กระบวนการทำงานของ DRM Reference Architecture เป็นดังนี้



รูปที่ 2.4 DRM Reference Architecture

1. เริ่มจากผู้ใช้จะรับเนื้อหาดิจิตอลจากเว็บไซต์ที่ให้บริการเนื้อหาดิจิตอลเหล่านั้น โดยที่เนื้อหาดิจิตอลจะบรรจุเป็นแพ็กเก็จที่ได้เข้ารหัสเอาไว้ (Content Package) ภายในประกอบด้วยเนื้อหาดิจิตอล (Digital Content) และ Metadata ซึ่งเป็นการอธิบายเนื้อหาดิจิตอล เช่น ISBN ราคา รูปแบบไฟล์ หรือ ชื่อของเจ้าของเนื้อหาดิจิตอลนั้น เป็นต้น โดยผู้ใช้จะร้องขอการใช้งานผ่าน DRM Controller

2. ในการร้องขอการใช้งานเนื้อหาดิจิตอลของผู้ใช้นั้นในส่วนของ DRM Client จะกระทำผ่านทาง DRM Controller ซึ่งมีหน้าที่ในติดต่อกับ License Server ในการขอใบอนุญาตสิทธิ์การใช้งานในเนื้อหาดิจิตอลนั้น และมีหน้าที่ในการควบคุมและปฏิบัติตามนโยบายในเนื้อหาดิจิตอลที่เจ้าของเนื้อหาดิจิตอลได้กำหนดไว้

3. หลังจากนั้น DRM Controller จะส่งคำร้องขอการใช้งานในเนื้อหาดิจิตอลของผู้ใช้มายัง License Server โดย DRM Controller จะรวบรวมข้อมูล ได้แก่ สิทธิ์ที่ผู้ใช้ทำการร้องขอการใช้งานในเนื้อหาดิจิตอลนั้น ข้อมูลระบุตัวตนของผู้ใช้ เช่น ชื่อผู้ใช้ ชื่ออุปกรณ์ และข้อมูลของเนื้อหาดิจิตอล เช่น Metadata เป็นต้น

4. เมื่อ License Server ได้รับข้อมูลการร้องขอจาก DRM Controller แล้ว จะทำการพิสูจน์ตัวตนของผู้ใช้ที่ทำงานร้องขอการใช้งานในเนื้อหาดิจิตอลจากฐานข้อมูลในระบบ และค้นหาสิทธิ์ที่เจ้าของเนื้อหาดิจิตอลได้ระบุการกระทำเอาไว้ และ License Server จะทำการประมวลผลสิทธิ์ที่ผู้ใช้ร้องขอการใช้งาน และข้อมูลสิทธิ์อื่นๆ แล้วส่งไปยังกระบวนการจัดการทางการเงิน (Financial Transaction) และหลังจากกระบวนการตรวจสอบของ License Server เสร็จสิ้น License Server ก็จะออกใบรับรองสิทธิ์การใช้งานในเนื้อหาดิจิตอลที่ผู้ใช้ได้ทำการร้องขอไว้ ซึ่งประกอบด้วย ข้อมูลสิทธิ์ (Rights) ข้อมูลการระบุตัวตน (Identity Information) และ กุญแจเพื่อถอดรหัส (Encryption key) แล้วรวมเข้าเป็นแพ็กเก็จที่ทำการเข้ารหัส แล้วส่งกลับไปยัง DRM Client ผ่านทาง DRM Controller

5. หลังจากที่ DRM Controller ได้รับ License Package แล้วจะทำการพิสูจน์การใช้งานกับโปรแกรมประยุกต์ เพื่อรับรองว่าสามารถแสดงเนื้อหาดิจิตอลได้ เมื่อการพิสูจน์สำเร็จ ใบรับรองสิทธิ์การใช้งานที่ได้รับจาก License Server จะรับรองการเปิดและส่งเนื้อหาดิจิตอลไปยังโปรแกรมประยุกต์เพื่อทำงานตามสิทธิ์ที่ผู้ใช้ร้องขอต่อไป

ระบบ DRM ข้างต้น DRM Controller จะเป็นตัวกลางในการติดต่อกับ Content Server และ License Server ผ่านทาง Content Package และ License Package ตามลำดับตามสิทธิ์ที่ได้ร้องขอและข้อมูลที่อยู่ในใน metadata

2.3 ความเป็นส่วนตัว

ความเป็นส่วนตัว (Privacy) ในหัวข้อนี้จะกล่าวถึงการนิยามความหมาย กฎหมายที่กล่าวถึงในเรื่องความเป็นส่วนตัว เทคโนโลยีความเป็นส่วนตัว และความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

2.3.1 คำนิยาม

ศตวรรษที่ 19 มีการนิยามเรื่องความเป็นส่วนตัวเป็นครั้งแรก โดย *Warren* และ *Brandeis* ได้ให้นิยามความเป็นส่วนตัวไว้ว่า "*the right to be let alone*" [5] ซึ่งเป็นจุดเริ่มต้นของการนำไปสู่การถกเถียงในเรื่องความเป็นส่วนตัวทางสังคมมากขึ้น *Warren* และ *Brandeis* ได้เชื่อมความสัมพันธ์ระหว่างความเป็นส่วนตัวกับสิทธิ์ในทรัพย์สิน ทั้งทรัพย์สินที่จับต้องได้และจับต้องไม่ได้ หลังจากนั้นได้มีผู้ให้คำนิยามเรื่องความเป็นส่วนตัวเพิ่มขึ้นมากมาย

หนึ่งในคำนิยามซึ่งครอบคลุมลักษณะของความเป็นส่วนตัวที่กำหนดโดย the British Committee on Privacy และ Related Matters คือ "*สิทธิ์ของความเป็นส่วนบุคคลที่ได้รับการป้องกันจากการคุกคามในชีวิตส่วนบุคคลหรือครอบครัวทั้งทางกายภาพหรือการเผยแพร่ข้อมูล*" [6]

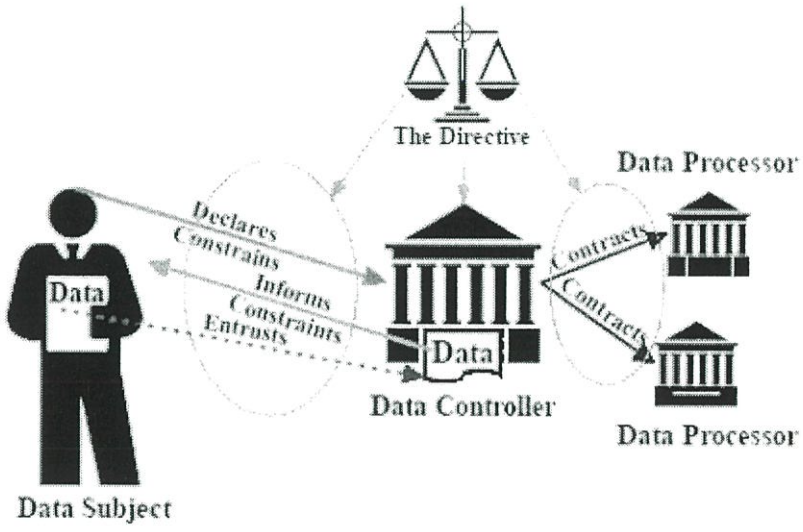
ในปัจจุบันมีการเก็บรวบรวมข้อมูลทางอิเลกทรอนิกส์เพิ่มขึ้น ซึ่งง่ายและเข้าถึงได้รวดเร็ว ทำให้เกิดปัญหาเกี่ยวข้องกับข้อมูลส่วนบุคคลที่ถูกเก็บไว้ในที่ต่างๆ อาจเข้าถึงโดยไม่ได้รับการอนุญาตจากเจ้าของ ซึ่งทำให้เกิดการทำลายความเป็นส่วนตัวขึ้น กระบวนการป้องกันข้อมูลจึงเป็นสิ่งสำคัญในการจัดการข้อมูลส่วนบุคคล ทำให้ Westin ได้ให้คำนิยามที่กระชับขึ้นคือ "*ความเป็นส่วนตัวคือการอ้างถึงบุคคล กลุ่ม และสถาบัน ที่กำหนดว่าข้อมูลสารสนเทศของเขาเหล่านั้นจะติดต่อกับผู้อื่นเมื่อไร อย่างไรและ เพื่ออะไร*" [9]

2.3.2 กฎหมายและข้อกำหนดความเป็นส่วนตัว

พระราชบัญญัติกฎหมายของหลายๆประเทศ ได้กล่าวถึงความเป็นส่วนตัวของบุคคล และได้ปรับปรุงบางส่วนในเรื่องสิทธิความเป็นส่วนตัว แต่ความเป็นส่วนตัวในข้อมูลสารสนเทศของบุคคล (Information privacy) ยังเป็นเรื่องที่ใหม่และต้องการกฎหมายที่รองรับการกระทำกับข้อมูลส่วนบุคคลเหล่านี้ ในหัวข้อนี้ได้กล่าวถึงกฎหมายที่เกี่ยวข้องกับสิทธิความเป็นส่วนตัวในสหภาพยุโรปและสหรัฐอเมริกา

ในปี 1995 สหภาพยุโรป (European Union) ได้ออก Directive 95/46/EC ในการปกป้องข้อมูล เป็นคำสั่งที่ต้องการเก็บข้อมูลที่ Data Subject ได้แจ้งเอาไว้ และ Data Subject จะต้องให้คำยินยอมที่ชัดเจนในการเก็บรวบรวมข้อมูล (อาจยกเว้นตามจุดประสงค์ของกฎหมายและภาวะฉุกเฉิน) โดยในการเก็บรวบรวมข้อมูลเพื่อจุดประสงค์ที่เปิดเผยและชัดเจน ในคำสั่งจะจำกัดการส่งข้อมูลไปยังประเทศนอกกฎหมาย EU โดยประเทศเหล่านั้นต้องมีการป้องกันความเป็นส่วนตัวที่ใน

ระดับที่เพียงพอในคำสั่งได้จัดเตรียมข้อมูลความเป็นส่วนตัวที่เป็นพื้นฐานทั่วไปและประยุกต์ใช้ความเป็นส่วนตัวบนอินเทอร์เน็ตและระบบเฉพาะจงอื่นๆ [7, 8]



รูปที่ 2.5 บทบาท 3 ส่วนประกอบสำคัญที่กำหนดและป้องกันข้อมูลในการทำงานของการทำพาณิชย์อิเล็กทรอนิกส์ ที่อ้างอิงใน the Directive

จากรูปที่ 2.6 the Directive จะประยุกต์ใช้กับการดำเนินชีวิตทั่วไป โดยระบุสิทธิ์การป้องกันข้อมูลที่สามารถกระทำได้กับ Data Subject และจะรวมเอาความต้องการและหน้าที่ที่ผูกพันกับกฎหมายของ Data Controller และมีความสัมพันธ์กับ Data Processor ซึ่งเป็นโครงสร้าง 3 ส่วนที่สมดุลกัน โดยกฎหมายได้วางข้อจำกัดในการติดต่อกันระหว่างบุคคลและองค์กรในการเก็บรวบรวม ซื้อขาย หรือ ใช้ข้อมูลส่วนตัว

ในสหรัฐอเมริกาไม่มีการกำหนดสิทธิ์ความเป็นส่วนตัวอย่างชัดเจน ข้อมูลความเป็นส่วนตัวจะได้รับการควบคุมจากการเจาะจงของกฎหมาย ไม่มีกฎหมายทั่วไปในการปกป้องข้อมูล การปกป้องข้อมูลได้รับการดูแลโดยองค์กรที่รวมตัวขึ้นในการเก็บข้อมูลทางการเงิน หมายเลขโทรศัพท์ อย่างไรก็ตามไม่มีการห้ามในการซื้อขายข้อมูลทางการแพทย์หรือข้อมูลส่วนตัวอื่นๆ มีการป้องกันการเก็บรักษาโดยตัวแทนรัฐบาลใน Privacy Act 1974 จะบรรจุด้วยหลักการการปฏิบัติกับข้อมูลอย่างเป็นธรรม การแจ้งว่าไม่เก็บข้อมูลความลับ ควรเข้าถึงได้ และมีจุดประสงค์ที่ชัดเจน

2.3.3 Fair Information Principles

เป็นหลักการพื้นฐานที่ยอมรับกันอย่างกว้างขวางในเรื่องความเป็นส่วนตัวในประเทศสหรัฐอเมริกา แคนนาดา ยุโรป และประเทศต่างๆ หลักการนี้ได้กำหนดขึ้นเป็นครั้งแรกที่ Department of Health Education and Welfare ประเทศสหรัฐอเมริกาในปี ค.ศ. 1973 และได้นำมา

อ้างอิงในคำแนะนำในการป้องกันความเป็นส่วนตัวและการนำเสนอข้อมูลส่วนบุคคลของ Organization for Economic Cooperation and Development (OECD) [3, 4] ดังนี้

- Openness
- Collection Limitation
- Purpose Specification
- Use Limitation
- Data Quality
- Individual Participation
- Security Safeguards
- Accountability

2.3.4 ความเป็นส่วนตัวและระบบการจัดการสิทธิ์ดิจิตอล

การที่ระบบการจัดการสิทธิ์ดิจิตอลเน้นไปที่ผู้ใช้หรือผู้บริโภคของระบบนั้น ในการออกแบบระบบการจัดการสิทธิ์ดิจิตอลจำเป็นต้องพิจารณาความต้องการของผู้ใช้ดังนี้ [22]

- การระบุตัวตนของผู้ใช้ควรตั้งอยู่บนสมมุติฐานที่ว่า ผู้ใช้หรือผู้บริโภคในระบบการจัดการสิทธิ์ดิจิตอลควรได้รับอนุญาตที่จะเลือกวิธีหรือระดับการปิดบังหรือซ่อนเร้นข้อมูลส่วนตัวที่ต่างระดับกันเพื่อความเหมาะสมในการใช้งานระบบ
- ในฐานข้อมูลสิทธิ์การใช้งานของผู้ใช้หรือผู้บริโภคควรตั้งอยู่บนสมมุติฐานที่ว่า ผู้ใช้หรือผู้บริโภคเนื้อหาดิจิตอลควรได้รับการอนุญาตที่จะมีส่วนร่วมในการกำหนดระดับการติดตามการทำงานหรือการเข้าใช้เนื้อหาดิจิตอลเหล่านั้น
- ในระบบการจัดการสิทธิ์ดิจิตอลควรถือว่าประวัติการใช้งานหรือกิจกรรมการทำงานต่างในระบบของผู้ใช้หรือผู้บริโภคเป็นทรัพย์สินที่ควรได้รับการดูแลรักษา

ระบบการจัดการสิทธิ์ดิจิตอลเกี่ยวข้องกับการกำหนดสิทธิ์และอนุญาตให้ใช้งานเนื้อหาดิจิตอลตามที่เจ้าของลิขสิทธิ์ได้กำหนดเอาไว้ ทำให้เกิดปัญหาตามมาภายหลังในเรื่องของการละเมิดความเป็นส่วนตัวของข้อมูลในกรณีที่ระบบนำข้อมูลส่วนบุคคลไปใช้หรือขายให้กับบุคคลที่สาม และยังมีปัญหาในเรื่องการใช้งานลักษณะ Fair Use ซึ่งเป็นการใช้งานที่จำเป็นต้องได้รับการยกเว้นจากระบบการจัดการสิทธิ์ดิจิตอล เป็นต้น สำหรับปัญหาในเรื่องการละเมิดความเป็นส่วนตัวนั้น จากการศึกษาเห็นว่าการควบคุมความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลสามารถทำได้ ซึ่งมีหลักการที่อ้างถึงความเป็นส่วนตัวมากมายโดยอธิบายดังนี้ [3]

- การแจ้งประกาศ (Notice) ด้วยเทคโนโลยีที่พัฒนาขึ้น การเก็บรวบรวมข้อมูลสามารถทำให้เป็นความลับ โดยที่ไม่สามารถตรวจจับได้ ดังนั้นการแจ้งประกาศจึงเป็นสิ่งจำเป็น

เพื่อเป็นการแสดงให้ผู้ใช้หรือผู้ให้ข้อมูลเหล่านั้นรับรู้ว่าระบบหรือใครเป็นผู้เก็บและเก็บข้อมูลเหล่านั้นเพื่อวัตถุประสงค์ใด

- ทางเลือกและการยินยอม (Choice and Consent) หลักการนี้ใกล้เคียงกับการแจ้งประกาศ ผู้ใช้ไม่เพียงรับทราบว่าข้อมูลส่วนตัวที่ระบบเก็บไปนั้นเพื่อจุดประสงค์ใด แต่ผู้ใช้ควรได้รับข้อเสนอที่เป็นทางเลือกที่ผู้ใช้สามารถเลือกได้ว่าจะยินยอมให้ระบบใช้ข้อมูลเหล่านั้นได้หรือไม่

- การเข้าถึง (Access) ในหลักการนี้ผู้ใช้สามารถควบคุมการใช้ข้อมูลส่วนตัวของตนเองได้ เช่น สามารถตรวจสอบ และแก้ไขข้อมูลเหล่านั้นได้

- การทำให้เป็นความลับ และ การใช้นามแฝง (Anonymity and Pseudonymity) กฎหมายความเป็นส่วนตัวที่กำหนดขึ้นไม่ได้จำกัดข้อมูลที่ทำการเก็บรวบรวม อย่างไรก็ตามบริการต่างๆ ไม่ควรที่จะเก็บรวบรวมข้อมูลที่มากเกินความจำเป็นที่บริการต้องการร้องขอ ดังนั้นข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผยที่ถูกรวบรวมก็จะไม่ถูกทำลายความเป็นส่วนตัว แต่โดยทั่วไปแล้วบริการต่างๆ ต้องการเก็บรวบรวมข้อมูลมากกว่าที่บริการต้องการร้องขอ การใช้นามแฝงจึงเป็นวิธีหนึ่งที่สามารถแก้ปัญหาการละเมิดความเป็นส่วนตัว โดยจะอนุญาตให้ผู้ใช้สามารถถูกติดตามได้โดยปราศจากเปิดเผยตัวตนที่แท้จริง อย่างไรก็ตามผู้ใช้ต้องการที่จะหยุดการบริการจากติดตามการทำงานได้ โดยเขาสามารถหยุดการใช้นามแฝงเพื่อระบุตัวจนจากบริการ

2.3.5 เทคโนโลยีความเป็นส่วนตัว

จากการศึกษาวิจัย และพัฒนาระบบการจัดการสิทธิ์ดิจิตอลนั้น ยังมีงานวิจัยน้อยมากที่นำเทคโนโลยีความเป็นส่วนตัวเข้าไปใช้ในระบบการจัดการสิทธิ์ดิจิตอล ในหัวข้อนี้ได้ทำการศึกษาวิธีการควบคุมความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล โดยทำศึกษาจากเทคโนโลยีความเป็นส่วนตัวที่แตกต่างกัน 3 เทคโนโลยีดังนี้ [22,23]

- Anonymization services เป็นวิธีการปกป้องข้อมูลส่วนบุคคลโดยการซ่อนข้อมูลส่วนตัวจากการสื่อสารระหว่างกัน ในผู้ใช้ที่แตกต่างกันหรือโปรแกรมประยุกต์ที่ต่างกันสามารถออกแบบให้มีระดับการซ่อนเร้นข้อมูลที่ต่างกันได้ เทคนิคที่ใช้กันทั่วไปได้แก่ Trusted Third Party, Personal/Nyms หรือ Public Key Infrastructure เป็นวิธีการปกป้องข้อมูลแบบ anonymity ที่แตกต่างกัน

- Privacy tagging เป็นอีกวิธีหนึ่งของการควบคุมความเป็นส่วนตัวที่สัมพันธ์กับข้อมูลในเอกสาร (documents) โดยจะเพิ่มส่วนของ Metadata ไปยังเอกสาร เพื่อใช้ในการอธิบายการทำงานที่เอกสารอนุญาตให้กระทำภายใต้เงื่อนไขที่กำหนดเอาไว้ ในรูปแบบการทำงานนี้ความเป็นส่วนตัวจำเป็นต้องบังคับจากซอฟต์แวร์ที่น่าเชื่อถือ

- Privacy policy description วิธีในการควบคุมความเป็นส่วนตัวที่ได้รับการเสนอขึ้นเพื่องานบริการสาธารณะ ซึ่งระบบจำเป็นจะต้องอธิบายให้ผู้ใช้ได้รับทราบว่าข้อมูลส่วนตัวที่ระบบจัดเก็บนั้น เพื่อวัตถุประสงค์ใด และใช้เมื่อไร เป็นต้น ผู้ใช้สามารถที่จะกำหนดการกระทำเหล่านั้นได้เอง และตัดสินว่าควรที่จะเข้าใช้บริการเหล่านั้นเหรอไม่ ตัวอย่างของระบบเหล่านั้นได้แก่ P3P ซึ่งได้พัฒนาโดย W3C เพื่องานบนอินเทอร์เน็ต โดยเว็บไซต์จะต้องระบุถึงจุดประสงค์การนำข้อมูลผู้ใช้ไปใช้ในลักษณะของภาษาที่เครื่องคอมพิวเตอร์เข้าใช้นั่นคือภาษา XML และในส่วนของผู้ใช้ระบบจำเป็นผู้กำหนดความเป็นส่วนตัวของตนเองในรูปของภาษา XML เช่นกัน โดยอาจใช้โปรแกรมประยุกต์อื่นๆ เพื่อเป็นตัวแทนในการเปรียบเทียบนโยบายของผู้ใช้และระบบในการที่จะตัดสินใจว่าควรเข้าใช้งานเว็บไซต์นั้นได้หรือไม่ ซึ่งจะอธิบายลักษณะการทำงานในหัวข้อที่ 2.4

ในตารางที่ 2.1 แสดงการเปรียบเทียบข้อดีและข้อเสียของวิธีการควบคุมความเป็นส่วนตัวที่ได้กล่าวถึงข้างต้น

ตารางที่ 2.1 การเปรียบเทียบข้อดีและข้อเสียของวิธีการควบคุมความเป็นส่วนตัว

เทคนิค	ข้อดี	ข้อเสีย	หลักการที่สนับสนุน
Anonymization/ Pseudonymization	- สามารถกำหนดความเป็นส่วนตัวได้อย่างมีประสิทธิภาพ - ผู้ใช้สามารถควบคุมการเปิดเผยข้อมูลส่วนบุคคลได้	- เป็นเทคนิควิธีที่มีความซับซ้อน - สนับสนุนการทำงานของในระดับเครือข่าย	- Anonymity - Notice - Consent - Access
Privacy tagging	- ควบคุมการใช้งานเอกสารจากการเพิ่ม Meta data ในเอกสาร	- ทำงานในระดับแอปพลิเคชั่นเลเยอร์	- Notice - Consent - Access
Privacy policy description	- ง่ายที่จะรวมเข้ากับสภาพแวดล้อมของเทคโนโลยีที่มีอยู่แล้ว	- การทำงานขึ้นอยู่กับความเชื่อมั่นของผู้ใช้กับบริการ	- Notice - Consent - Access

2.4 การควบคุมความเป็นส่วนตัวด้วยเทคโนโลยี P3P

P3P (Platform for Privacy Preferences) พัฒนาโดย World Wide Web Consortium (W3C) [10] โดยได้รับรองเป็นมาตรฐาน P3P รุ่นที่ 1.0 P3P เป็นวิธีการหนึ่งที่ช่วยให้ผู้ใช้สามารถควบคุมการใช้ข้อมูลส่วนตัวบนเว็บไซต์ ด้วยการแสดงนโยบายความเป็นในรูปแบบที่คอมพิวเตอร์เข้าใจด้วยภาษาเอ็กซ์เอ็มแอล และยังเป็นโปรโตคอลที่ทำให้เว็บบราวเซอร์สามารถอ่านนโยบายความเป็นส่วนตัวของเว็บไซต์กระทำการกับค่าที่ผู้ใช้กำหนดได้อย่างอัตโนมัติ [11]

2.4.1 P3P Policies

P3P ใช้ภาษา XML ในการอธิบายนโยบายความเป็นส่วนตัวของเว็บไซต์ นโยบายเหล่านี้จะอธิบายว่าใครเก็บข้อมูลอะไรและเพื่อจุดประสงค์ใด แสดงดังรูปที่ 2.7 นโยบาย P3P จะแสดงเป็นลำดับของ STATEMENT element โดยประกอบด้วย Subelements ดังนี้ [13]

- CONSEQUENCE อธิบายจุดประสงค์ในการเก็บข้อมูล ในรูปแบบข้อความที่สามารถอ่านเข้าใจได้
- PURPOSES อธิบายจุดประสงค์ในการเก็บข้อมูล สามารถกำหนดได้หลายจุดประสงค์ใน STATEMENT ถ้ามีค่าของ RECIPENT, RETENTION และ DATA-GROUPS เหมือนกัน สามารถกำหนดได้ 12 ชนิด ได้แก่ current, pseudo-analysis, individual-decision, contact เป็นต้น
- RECIPIENTS อธิบายถึงผู้รับข้อมูล สามารถกำหนดได้ 6 ชนิด ได้แก่ ours, same, unrelated เป็นต้น
- RETENTION อธิบายระยะเวลาที่ทำการเก็บข้อมูลไว้ ได้แก่ stated-purpose, business-practice, indefinitely เป็นต้น
- DATA GROUPS อธิบายชนิดของข้อมูลที่เก็บตามจุดประสงค์ โดยรูปแบบข้อมูลแบ่งเป็น 17 category ได้แก่ Unique Identifiers, Physical Contact Information, Online Contact Information เป็นต้น

ตัวอย่างนโยบาย [14] วอลก้าเป็นเจ้าของร้านขายหนังสือ ต้องการข้อมูลผู้ใช้เพียงเล็กน้อยเพื่อทำการซื้อขายให้สมบูรณ์ โดยต้องการ ชื่อ ที่อยู่ เพื่อส่งหนังสือและเลขบัตรเครดิตการ์ด และต้องการใช้ประวัติการซื้อหนังสือ ในการส่งแนะนำหนังสือให้แก่ลูกค้าผ่านทางอีเมล์

จากรูปที่ 2.6 STATEMENT แรก เป็นนโยบายที่บอกว่าต้องการชื่อ ที่อยู่ และข้อมูลการซื้ออื่นๆ เช่น ชื่อหนังสือ เลขบัตรเครดิตการ์ด เป็นต้น เพื่อให้การทำทรานแซกชั่นการซื้อขายได้สำเร็จ และ STATEMENT ถัดมา เจ้าของร้านต้องการใช้ข้อมูลการซื้อเพื่อส่งแนะนำหนังสือผ่านทางอีเมล์ โดย required attribute มีค่าเป็น opt-in เป็นความจำเป็นที่ต้องให้ผู้ใช้ยินยอมก่อนทำการเก็บข้อมูล

```
<POLICY>
 ... ....
  <STATEMENT>
     <PURPOSE> <current/> </PURPOSE>
     <RECIPIENT> <ours/><same/> </RECIPIENT>
     <RETENTION><stated-purpose/> </RETENTION>
     <DATA-GROUP>
          <DATA ref = "#user.name"/>
          <DATA ref = "#user.home-info.postal"/>
          <DATA ref = "#dynamic.miscdata">
            <CATEGORIES><purchase></CATEGORIES>
          </DATA>
     </DATA-GROUP>
  </STATEMENT>

  <STATEMENT>
     <PURPOSE>
          <individual-decision required = "opt-in"/>
          <contact required = "opt-in"/>
     </PURPOSE>
     <RECIPIENT><ours/></RECIPIENT>
     <RETENTION><business-practices/></RETENTION>
     <DATA-GROUP>
          <DATA ref = "#user.home-info.online.email"/>
          <DATA ref = "#dynamic.miscdata">
          </DATA>
              <CATEGORIES><purchase/></CATEGORIES>
     </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

รูปที่ 2.6 ตัวอย่าง P3P Policy

2.4.2 Privacy Preferences

ในการกำหนดความเป็นส่วนตัวนั้นแสดงด้วยภาษา APPEL 1.0 (A P3P Preferences Language) เป็นโครงการหนึ่งของ W3C [12] โดยแสดงเป็น RULEs กฎเหล่านี้กำหนดเพื่อเปรียบเทียบกับนโยบาย ประกอบด้วยสองส่วน [12, 14] ได้แก่

- Rule behavior เป็นการกำหนดการกระทำที่อยู่ใน Rule body แบ่ง behavior ได้เป็น request behavior นโยบายจะทำตามการกำหนดใน rule body ส่วน block behavior นโยบายจะไม่ปฏิบัติตามการกำหนดของผู้ใช้
- Rule body เป็นรูปแบบที่นำมาจับคู่กับนโยบาย มีลักษณะตามนโยบายข้างต้น

ตัวอย่าง Privacy Preference [14] เจนต้องการให้ข้อมูลแก่ร้านค้าเพื่อให้การทำทรานเซกชั่นสมบูรณ์เท่านั้น และเจนยินยอมที่จะให้อีเมล์และประวัติการใช้งานเพื่อจุดประสงค์ตามนโยบายเว็บไซต์ แต่อย่างไรก็ตามเจนไม่ต้องการให้ข้อมูลของเธอไปยังผู้ขายที่ไม่มีทางเลือกให้เธอตัดสินใจ

จากรูปที่ 2.7 ประกอบด้วย 3 กฎ ในกฎแรกเป็นการจำกัดจุดประสงค์อื่นๆทั้งหมดที่ไม่เกี่ยวกับจุดประสงค์ปัจจุบัน กฎข้อ 2 ผู้รับข้อมูลของเจนคือผู้จำหน่ายหรือตัวแทนที่ปฏิบัติตาม

เงื่อนไขความเป็นส่วนตัว กฎข้อสุดท้ายข้อมูลของเจนจะให้ไปถ้าเงื่อนไขไม่ตรงกับกฎสองข้อข้างต้น

```
<appel : RULESET>
  <appel : RULE behavior = "block">
    <POLICY>
      <STATEMENT>
        <PURPOSE appel : connective = "or">
          <admin/><develop/><tailoring/>
          <pseudo-analysis/><pseudo-decision/>
          <individual-analysis/>
          <individual-decision required = "always"/>
          <contact required = "always"/>
          <historical/><telemarketing/>
          <other-purpose/><extension/>
          </PURPOSE>
      </STATEMENT>
    </POLICY>
  </appel : RULE>

  <appel : RULE behavior = "block">
    <POLICY>
      <STATEMENT>
        <RECIPIENT appel : connective = "or">
          <delivery/><other-recipient/>
          <unrelated/><public/><extension/>
          </RECIPIENT>
      </STATEMENT>
    </POLICY>
  </appel : RULE>

  <appel : RULE behavior = "request">
    <appel : OTHERWISE>
  </appel : RULE>
</appel : RULESET>
```

รูปที่ 2.7 ตัวอย่าง Privacy Preference ใน APPEL

จากหลักการและทฤษฎีที่กล่าวถึงในข้างต้นนั้น ได้อธิบายความหมาย โครงสร้างและเทคโนโลยีที่เกิดขึ้นของระบบการจัดการสิทธิ์ดิจิตอล รวมทั้งได้อธิบายถึงหลักการและเทคโนโลยีความเป็นส่วนตัวที่ใช้อยู่ในปัจจุบัน ซึ่งนำไปสู่แนวความคิดที่ใช้ในงานวิจัยนี้ และในบทถัดไปจะได้กล่าวถึงโครงสร้างและวิธีการออกแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

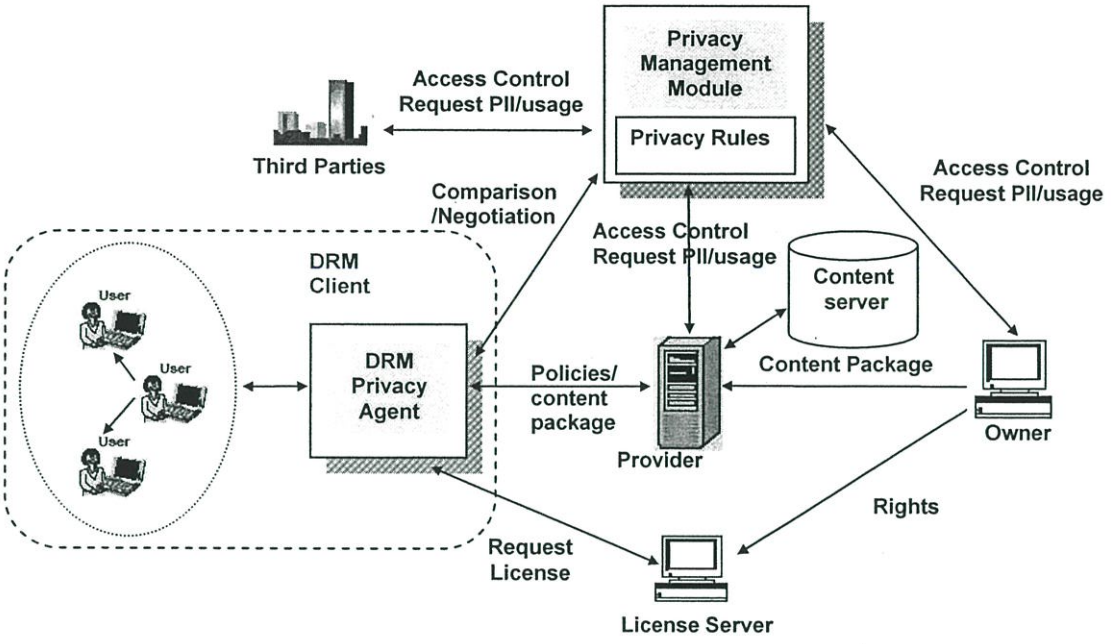
บทที่ 3
การเพิ่มความเป็นส่วนตัว
สำหรับระบบการจัดการสิทธิ์ดิจิตอล

3.1 บทนำ

จากการศึกษาถึงปัญหาที่เกิดขึ้นในระบบ DRM ส่วนของผู้ใช้ที่ใช้งานระบบจะถูกละเมิดความเป็นส่วนตัว โดยที่ระบบ DRM นำข้อมูลส่วนบุคคลของผู้ใช้ (personal data) หรือการติดตามพฤติกรรมการใช้งานของผู้ใช้ ซึ่งจะนำข้อมูลเหล่านั้นไปใช้งานโดยไม่ได้รับการอนุญาตจากผู้ใช้ในระบบ DRM นั้น ในบทนี้อธิบายการเพิ่มความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล โดยงานวิจัยนี้ได้ออกแบบนโยบายความเป็นส่วนตัว (DRM privacy policy) ที่มีความยืดหยุ่นสำหรับระบบ DRM และทำการออกแบบการกำหนดนโยบายความเป็นส่วนตัวในส่วนของผู้ใช้ (User's Privacy Preferences) โดยนำเอาแนวคิดของการกำหนดความเป็นส่วนตัวที่ใช้ทั่วไปบนเว็บไซต์นั่นคือ The Platform for Privacy Preferences หรือ P3P [10] ซึ่งเป็นมาตรฐานในการกำหนดนโยบายของเว็บไซต์ โดยมี User agent ทำหน้าที่ในการอ่านและแปลความนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้ในการเข้ามาใช้งานในเว็บไซต์ ว่าขัดแย้งกับการกำหนดความเป็นส่วนตัวที่ผู้ใช้ได้กำหนดขึ้นไว้หรือไม่ ในงานวิจัยได้ออกแบบการกำหนดนโยบายสำหรับระบบ DRM ที่มีความยืดหยุ่นทั้งระบบ DRM และผู้ใช้งานระบบ โดยที่ DRM privacy agent เป็นตัวแทนในการอ่านนโยบายของระบบ DRM อย่างอัตโนมัติ และทำการเปรียบเทียบระหว่างการกำหนดความเป็นส่วนตัวของผู้ใช้และนโยบายของระบบ DRM และ DRM privacy agent ยังทำหน้าที่เจรจาต่อรองในกรณีที่การกำหนดนโยบายความเป็นส่วนตัวของผู้ใช้เข้ากันไม่ได้กับนโยบายของระบบ DRM โดยงานวิจัยได้ออกแบบอัลกอริทึมในการเจรจาต่อรองความเป็นส่วนตัว โดยทำการเลือกกฎหรือข้อกำหนดที่ผู้ใช้ได้กำหนดความเป็นส่วนตัวเอาไว้ได้อย่างเหมาะสม และมีประสิทธิภาพ

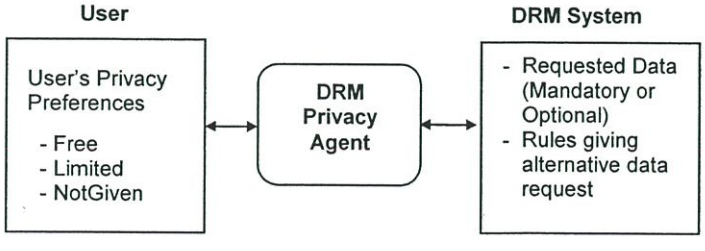
3.2 โครงสร้างความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

การเพิ่มความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล โดยสถาปัตยกรรมความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลแสดงดังรูปที่ 3.1 ในงานวิจัยนี้ได้อ้างอิงโครงสร้างของระบบ DRM ซึ่งประกอบด้วย ส่วนประกอบสำคัญ 3 ส่วน [15] คือ content server, license server และ DRM client โดยได้แสดงในรูปที่ 2.4 ซึ่งแต่ละส่วนประกอบจะมีความสัมพันธ์ในการทำงานและควบคุมสิทธิ์ของผู้ใช้ที่จะกระทำบนเนื้อหาดิจิตอลที่ร้องขอการใช้งาน โดยผู้ใช้จะมีสิทธิ์



รูปที่ 3.1 องค์ประกอบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

ตามที่เจ้าของได้กำหนดสิทธิ์เอาไว้เท่านั้น และจากในรูปที่ 3.1 ในงานวิจัยนี้ได้เพิ่มความเป็นส่วนตัวแก่ผู้ใช้ในฝั่งของ DRM client โดยการเพิ่ม DRM privacy agent ซึ่งจะทำหน้าที่ในการอ่านนโยบายและทำการเปรียบเทียบการกำหนดความเป็นส่วนตัวของผู้ใช้กับนโยบายของระบบ DRM ในเนื้อหาดิจิตอลที่ผู้ใช้ทำการร้องขอ และ DRM privacy agent ยังทำหน้าที่ในการเจรจาต่อรองในกรณีนี้ที่นโยบายของระบบ DRM กับการกำหนดความเป็นส่วนตัวของผู้ใช้เข้ากันไม่ได้ โดย DRM privacy agent จะส่งกฎที่เหมาะสมที่สุดหลังจากผ่านกระบวนการเจรจาต่อรองไปยังส่วนจัดการความเป็นส่วนตัว (privacy management module) เพื่อสร้างกฎความเป็นส่วนตัว (privacy rules) ที่เหมาะสมสำหรับผู้ใช้แต่ละบุคคลที่เข้าใช้เนื้อหาดิจิตอลในระบบ DRM เพื่อควบคุมการทำงานของระบบ DRM และเจ้าของเนื้อหาดิจิตอลในการเข้าใช้ข้อมูลส่วนบุคคล ตามที่ผู้ใช้ได้กำหนดเอาไว้



รูปที่ 3.2 โครงสร้างการทำงานของ DRM privacy agent

สำหรับ DRM privacy agent ซึ่งจะเก็บการกำหนดความเป็นส่วนตัวของผู้ใช้แต่ละบุคคล โดยจะทำหน้าที่เปรียบเทียบระหว่างนโยบายของเนื้อหาดิจิตอล (DRM policy) ที่กำหนดโดยเจ้าของเนื้อหาดิจิตอล และการกำหนดความเป็นส่วนตัวของผู้ใช้ (User's Privacy Preferences) โดยรูปที่ 3.2 แสดงหน้าที่การทำงานของ DRM privacy agent ซึ่งเป็นตัวแทนการติดต่อระหว่างผู้ใช้ (Users) และระบบ DRM (DRM System) โดยในส่วนผู้ใช้จะมีการกำหนดความเป็นส่วนตัวเป็น 3 ระดับ ได้แก่ Free, Limited และ NotGiven เพื่อระบุว่ามีเงื่อนไขในการให้ข้อมูลความเป็นส่วนตัวแก่ DRM System อย่างไรบ้าง และใน DRM System ได้กำหนดนโยบายความเป็นส่วนตัวในการร้องขอข้อมูลความเป็นส่วนตัวจากผู้ใช้ (Requested Data) ซึ่งมีลักษณะการร้องขอเป็น 2 ประเภท คือ Mandatory และ Optional และในนโยบายยังได้กำหนดทางเลือกของข้อมูลความเป็นส่วนตัวอื่นๆ (Rules giving alternative data request) ของผู้ใช้ ในกรณีที่ผู้ใช้ไม่สามารถให้ข้อมูลความเป็นส่วนตัวที่ระบบต้องการได้

จากสถาปัตยกรรมของความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลที่ได้กล่าวมาในข้างนั้น ในงานวิจัยนี้จะทำการอธิบายขั้นตอนและวิธีการความเป็นส่วนตัวสำหรับระบบ DRM ที่ได้ออกแบบตามลำดับหัวข้อดังต่อไปนี้

- องค์ประกอบของการกำหนดนโยบายความเป็นส่วนตัวสำหรับระบบ DRM *(Element of a privacy policy)* ในเนื้อหาดิจิตอล เช่น หนังสือ เพลง วิดีโอ เป็นต้น ซึ่งอยู่ในรูปไฟล์ดิจิตอล บนระบบ DRM จำเป็นต้องมีการกำหนดนโยบายในการใช้ข้อมูลของผู้ใช้ในระบบ เพื่อแสดงถึงจุดประสงค์ของการนำข้อมูลเหล่านั้นไปใช้งาน โดยได้อธิบายรายละเอียดองค์ประกอบของนโยบายความเป็นส่วนตัวที่จำเป็นสำหรับระบบ DRM ในหัวข้อถัดไป
- การร้องขอข้อมูลผู้ใช้ในระบบ DRM *(Requested data)* นโยบายของระบบจะทำการร้องขอข้อมูลของผู้ใช้ในระบบ DRM โดยในนโยบายประกอบด้วยสมาชิก Mandatory element และ Optional element ซึ่งภายในจะประกอบด้วยสเตทเมนท์ (policy statements) หลายๆสเตทเมนท์ และภายในสเตทเมนท์จะบอกถึงจุดประสงค์ผู้ใช้ข้อมูล ระยะเวลาที่ทำการเก็บข้อมูล และข้อมูลที่ทำการร้องขอ
- เงื่อนไขการร้องขอข้อมูลผู้ใช้ในระบบ DRM *(Condition statements)* ในการร้องขอข้อมูลของผู้ใช้ในนโยบายของระบบ DRM งานวิจัยได้ทำการออกแบบนโยบายให้มีความยืดหยุ่น โดยมีนโยบายที่กำหนดเงื่อนไขในลักษณะ If-then Rules เพื่อใช้ในกรณีที่ข้อมูลที่ทำการร้องขอไม่ถูกให้โดยผู้ใช้ในระบบ DRM

- การกำหนดความเป็นส่วนตัวของผู้ใช้ *(User's Privacy Preferences)* ในการออกแบบการกำหนดความเป็นส่วนตัวของผู้ใช้ในระบบ DRM นั้น ได้ออกแบบเป็นระดับการอนุญาตในการเข้าใช้ข้อมูลของผู้ใช้เป็น 3 ระบบ นั่นคือ Free, Limited และ NotGiven ซึ่งจะอธิบายในหัวข้อถัดไป
- กลไกการเจรจาต่อรอง *(Negotiation mechanism)* หลังจากที่ DRM privacy policy ได้ทำการอ่าน/แปลความนโยบาย และการกำหนดความเป็นส่วนตัวของผู้ใช้แล้ว กลไกการเจรจาต่อรอง ที่ทำการออกแบบจะประกอบด้วย 2 ขั้นตอนย่อย คือ
    - *Rule Evaluation* เป็นกระบวนการเปรียบเทียบระหว่างนโยบายของระบบกับการกำหนดความเป็นส่วนตัวของผู้ใช้ โดยใช้ DRM privacy agent ในการประเมินกฎ โดยใช้เงื่อนไข Conditional Statements ในการแก้ปัญหาเบื้องต้นก่อนที่จะส่งไปยังกระบวนการถัดไป ซึ่งจะอธิบายรายละเอียดต่อไปในหัวข้อ 3.6
    - *Negotiation Process* เมื่อผ่านกระบวนการ Rule Evaluation แล้วนโยบายของระบบ DRM ที่ขัดแย้งกับการกำหนดความเป็นส่วนตัวของผู้ใช้จะผ่านกระบวนการเจรจาต่อรองเพื่อให้ได้กฎที่เหมาะสมที่สุดสำหรับการร้องขอข้อมูลของผู้ใช้ในระบบ DRM ซึ่งจะอธิบายรายละเอียดต่อไปในหัวข้อ 3.6

3.3 องค์ประกอบนโยบายความเป็นส่วนตัวสำหรับระบบ DRM

ในการออกแบบนโยบายความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลนั้น ในงานวิจัยได้อ้างอิงองค์ประกอบที่สำคัญของมาตรฐาน P3P [10] ที่ใช้ทั่วไปในการกำหนดนโยบายความเป็นส่วนตัวบนเว็บ และได้นำหลักการของ FIPs [4] ซึ่งเป็นหลักปฏิบัติพื้นฐานที่ใช้ในการเก็บรวบรวมข้อมูลของผู้ใช้ เพื่อป้องกันความเป็นส่วนตัวและนำเสนอข้อมูลส่วนบุคคล โดยในงานวิจัยได้นำมาใช้และทำการปรับปรุงเปลี่ยนแปลงให้เหมาะสมกับระบบ DRM ดังนี้

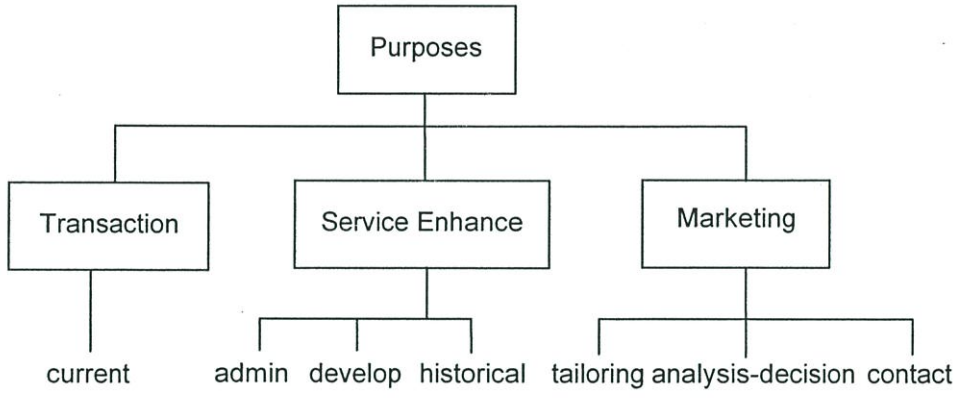
3.3.1 จุดประสงค์ *(Purposes)*

ในการกำหนดนโยบายของระบบจำเป็นต้องบอกจุดประสงค์ในการใช้ข้อมูลให้ผู้ใช้รับทราบว่าข้อมูลที่ร้องขอไปนั้นนำไปใช้งานเพื่อจุดประสงค์ใด สำหรับระบบ DRM จุดประสงค์ในการเก็บและรวบรวมข้อมูลของผู้ใช้นั้น มีความแตกต่างกันในแต่ละประเภทการใช้งานของระบบ DRM โดยพิจารณาจากการแบ่งประเภทดังนี้

- จุดประสงค์เพื่อใช้ในการขายสินค้า
- จุดประสงค์เพื่อการบริการระบบและเครือข่าย

- จุดประสงค์เพื่อการสำรองข้อมูล
- จุดประสงค์เพื่อการรวบรวมข้อมูลการใช้งานเพื่อประโยชน์ทางการตลาด
- จุดประสงค์เพื่อการเก็บประวัติของบุคคล
- จุดประสงค์เพื่อการให้บริการแก่ผู้ใช้งาน
- จุดประสงค์เพื่อการนำเสนอบริการให้แก่ผู้ใช้

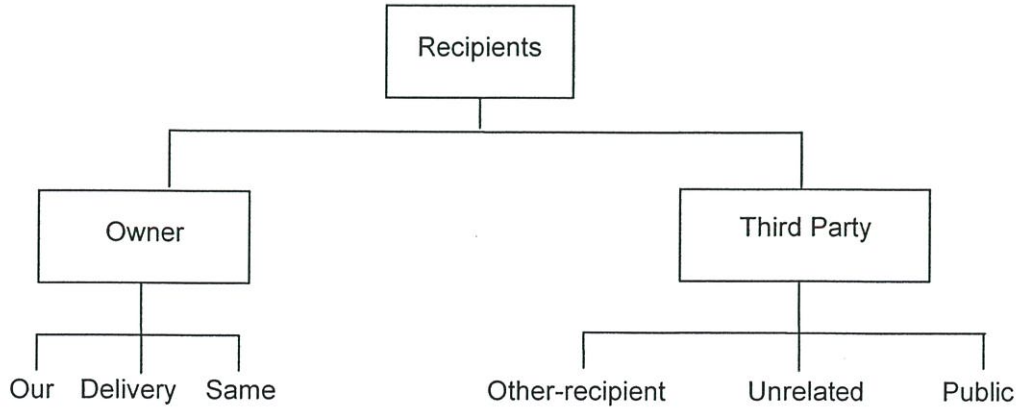
สำหรับจุดประสงค์ของการเก็บและรวบรวมข้อมูลของผู้ใช้งานในระบบ DRM ได้ปรับปรุงจากมาตรฐาน P3P โดยแบ่งได้ดังแสดงในรูปที่ 3.3 และงานวิจัยได้ออกแบบ XML Schema ของนโยบายความเป็นส่วนตัวสำหรับ DRM ไว้ในภาคผนวก ข.



รูปที่ 3.3 โครงสร้างการแบ่งประเภทของจุดประสงค์ในระบบ DRM

3.3.2 ผู้รับ *(Recipients)*

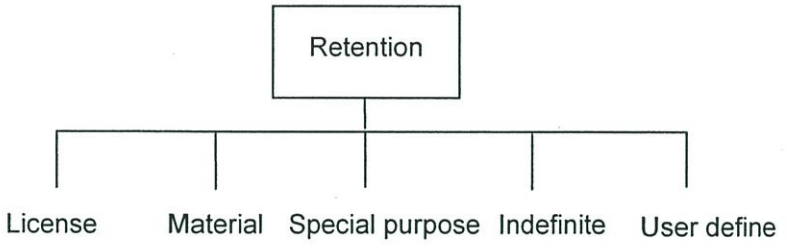
เมื่อระบบระบุจุดประสงค์สำหรับการเก็บรวบรวมข้อมูลของผู้ใช้งานแล้วระบบจำเป็นต้องระบุว่าใครเป็นผู้ขอใช้ข้อมูลเหล่านั้น โดยได้แบ่งประเภทของผู้รับเป็น 6 ชนิดตามที่มาตรฐาน P3P ได้กำหนดไว้ดังรูปที่ 3.4



รูปที่ 3.4 โครงสร้างการแบ่งประเภทของผู้รับข้อมูลในระบบ DRM

3.3.3 ระยะเวลาในการเก็บข้อมูล *(Retention)*

ในการกำหนดนโยบายของระบบ DRM ผู้เป็นเจ้าของเนื้อหาดิจิตอลหรือผู้ดูแลระบบ DRM จำเป็นต้องระบุเพื่อแจ้งให้ผู้ใช้ทราบว่าต้องการเก็บข้อมูลเหล่านั้นเป็นระยะเวลาเท่าใด โดยได้แบ่งประเภทระยะเวลาการเก็บข้อมูลให้เหมาะสมกับระบบ DRM แสดงดังรูปที่ 3.5



รูปที่ 3.5 โครงสร้างการแบ่งประเภทของระยะเวลาในการเก็บข้อมูลในระบบ DRM

- *License* : ข้อมูลของผู้ใช้จะถูกเก็บตามระยะเวลาของใบรับรองสิทธิ์ (license) ของผู้ใช้แต่ละบุคคล โดยที่เมื่อใบรับรองสิทธิ์การใช้งานเนื้อหาดิจิตอลหมดอายุ ข้อมูลส่วนบุคคลหรือข้อมูลการใช้งานอื่นๆ ของผู้ใช้จะถูกลบออกจากระบบ
- *Material* : ระยะเวลาการเก็บข้อมูลของผู้ใช้งานระบบจะเก็บตามอายุของเนื้อหาดิจิตอล
- *Special purpose* : ข้อมูลการใช้งานและข้อมูลส่วนบุคคลของผู้ใช้จะเก็บตามระยะเวลาที่เจ้าของเนื้อหาดิจิตอล หรือผู้บริหารระบบได้ระบุระยะเวลาตามจุดประสงค์การใช้งานเอาไว้
- *Indefinite* : ระบบจะทำการเก็บข้อมูลส่วนบุคคลและข้อมูลการใช้งานของผู้ใช้งานในระบบโดยไม่มีกำหนดระยะเวลา
- *User define* : ระบบจะเก็บข้อมูลของผู้ใช้ตามระยะเวลาที่ผู้ใช้กำหนด

3.3.4 ข้อมูล *(Data)*

ประเภทข้อมูลของผู้ใช้ที่ระบบ DRM ต้องการเก็บรวบรวม รวมถึงข้อมูลส่วนบุคคล (personally identifying information -- PII) ข้อมูลการใช้งานในเนื้อหาดิจิตอล เช่น จำนวนครั้งในการเข้าใช้งาน ระยะเวลาในการใช้งาน สิทธิ์ในเนื้อหาดิจิตอล ตำแหน่งหรือไอพีแอดเดรสที่ผู้ใช้เข้าถึง เป็นต้น โดยข้อมูลเหล่านี้จะถูกเก็บทั้งในฝั่งเซิร์ฟเวอร์ของผู้ให้บริการเนื้อหาดิจิตอลในระบบ DRM หรือฝั่ง DRM client ซึ่งจะเก็บข้อมูลการใช้งานของผู้ใช้และส่งไปยังเซิร์ฟเวอร์เพื่อการประมวลผลต่อไป ประเภทข้อมูลที่ระบบ DRM แบ่งประเภทจะอ้างอิงตามมาตรฐานของ P3P [10]

จากองค์ประกอบของนโยบายความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลที่กล่าวถึงทั้ง 4 องค์ประกอบนั้นเป็นองค์ประกอบเบื้องต้นที่ระบบ DRM จำเป็นจะต้องแจ้งให้ผู้ใช้ทราบว่าระบบต้องการร้องขอข้อมูลอะไร เพื่อวัตถุประสงค์ใด โดยใครเป็นผู้รับ และข้อมูลเหล่านั้นเก็บไว้ในระบบนานเท่าไร ทั้งนี้ผู้ใช้จะต้องบอกถึงเงื่อนไขเหล่านั้นว่าจะสามารถยินยอมหรือไม่ยินยอมให้ระบบนำข้อมูลอะไรไปใช้บ้าง ซึ่งองค์ประกอบเหล่านั้นเป็นสิ่งจำเป็นอย่างยิ่งที่นโยบายของระบบ DRM ต้องกำหนดเอาไว้

3.4 การร้องขอข้อมูลผู้ใช้ในระบบ DRM (Requested Data)

จากหลักปฏิบัติของ Fair Information Principles [4] ซึ่งเป็นมาตรฐานในการเก็บรวบรวมและใช้ข้อมูลส่วนบุคคลโดยอยู่บนพื้นฐานความเป็นส่วนตัวและความถูกต้อง ซึ่งมีหลักอยู่หลายประการตามที่ได้กล่าวมาแล้วในหัวข้อ 2.3.3 โดยได้นำหลักการดังกล่าวมาใช้ให้เหมาะสมกับระบบ DRM

สำหรับการออกแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลนั้น ในงานวิจัยได้ทำการออกแบบนโยบายในการร้องขอข้อมูลต่างจาก P3P [11] โดยได้แบ่งออกเป็นสองส่วน ในส่วนแรกประกอบด้วยสมาชิกในส่วน Mandatory element และ Optional element ในส่วนที่สองจะประกอบไปด้วยเงื่อนไขทางเลือกหรือ Alternative element ซึ่งทำหน้าที่เป็นทางเลือกกรณีที่ข้อมูลที่ระบบทำการร้องข้อไม่ถูกจัดเตรียมให้โดยผู้ใช้ โดยทำการอธิบายส่วนการร้องขอข้อมูลของระบบดังนี้

- *Essential of the data* -- เป็นส่วนการร้องขอข้อมูลที่ระบบ DRM ต้องการข้อมูลของผู้ใช้เพื่อจุดประสงค์ต่างๆ เช่น เพื่อทำทรานเซกชั่นให้สำเร็จ เป็นต้น โดยประกอบด้วย 2 elements ย่อย ดังนี้
    - *Mandatory element :* ข้อมูลที่ระบบร้องขอในแอลเลเมนท์นี้ เป็นข้อมูลของผู้ใช้ที่ระบบจำเป็นต้องเก็บข้อมูลเหล่านั้น เพื่อให้ระบบสามารถทำงานได้
    - *Optional element :* ข้อมูลที่ระบบร้องขอในแอลเลเมนท์นี้ เป็นข้อมูลของผู้ใช้ที่ระบบอาจต้องการข้อมูลสำหรับเงื่อนไขบางประการเท่านั้น
- *Alternative of the data* -- กำหนดกฎทางเลือกในลักษณะของ *Conditional Statements* โดยใช้ If-then rules เพื่อเป็นทางเลือกกรณีข้อมูลที่ระบบร้องขอแต่ผู้ใช้ไม่สามารถจัดเตรียมหรือยอมรับได้

โดยที่ Mandatory element และ Optional element จะประกอบด้วยหลายๆสเตทเมนท์ ภายในแต่ละสเตทเมนท์จะระบุจุดประสงค์ (Purposes) ผู้ที่ใช้ข้อมูล (Recipients) ระยะเวลาในการเก็บข้อมูล (Retention) และข้อมูล (Data) ผู้ใช้ที่ระบบต้องการ งานวิจัยได้ออกแบบ XML Schema

ในส่วนการร้องข้อมูลของระบบ DRM ไว้ในภาคผนวก ข. โดยแสดงตัวอย่างการกำหนดนโยบาย ดังรูปที่ 3.6

```
<?xml version="1.0"?>
  <policy Material_Name="The Lord Of The Ring" Material_Type="book">
     <mandatory>
        <statement>
         <purpose> <current/> <admin/> </purpose>
         <recipient> <ours/> <delivery/> </recipient>
         <retention defined-by="special-purpose" description="developement"/>
         <data-group>
             <data type="#user.name"/>
             <data type="#user.email.address"/>
         </data-group>
        </statement>
     </mandatory>
    <optional>
        <statement>
         <purpose> <historical> </purpose>
         <recipient> <our/> </recipient>
         <retention defined-by="material" description="marketing"/>
         <data-group>
             <data type="#uclick.stream"/>
         </data-group>
        </statement>
     </optional>
  </policy>
```

รูปที่ 3.6 ตัวอย่างการกำหนดนโยบายความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

ในรูปที่ 3.7 เป็นตัวอย่างแสดงการกำหนดกฎในลักษณะ Conditional Statements โดยใช้ If-then rules ในการแก้ปัญหากรณีที่ข้อมูลที่ระบบร้องขอแต่ผู้ใช้งานระบบไม่สามารถยอมรับได้ ซึ่งได้แสดง XML Schema ในส่วนกฎทางเลือกของข้อมูลในระบบ DRM ไว้ในภาคผนวก ข.

```
<rule>
    <IfRule>
        <IfNotGiven>
            <purpose><current/> </purpose>
        </IfNotGiven>
        <Then>
            <purpose> <admin/> </purpose>
        </Then>
    </IfRule>
    <IfRule>
        <IfNotGiven>
            <data-group> <data type="#user.name"/> </data-group>
        </IfNotGive>
        <Then>
            <data-group> <data type="#user.email.address"/> </data-group>
        </Then>
    </IfRule>
    <IfRule>
        <IfNotGiven>
            <data-group> <data type="#user.email.address"/> </data-group>
```

```
        </IfNotGiven>
        <Then>
            <data-group> <data type="#user.postal"/> </data-group>
        </Then>
    </IfRule>
    <IfRule>
        <IfNotGiven>
            <retention defined-by="special-purpose"/>
        </IfNotGiven>
        <Then>
            <retention defined-by="material"/>
        </Then>
    </IfRule>
</rule>
```

รูปที่ 3.7 ตัวอย่างการกำหนดกฎทางเลือกโดยใช้ Conditional Statements

3.5 การกำหนดความเป็นส่วนตัวของผู้ใช้

ในการกำหนดความเป็นส่วนตัวของผู้ใช้ (User's Privacy Preferences) สำหรับระบบ DRM นั้น ในงานวิจัยได้ทำการออกแบบการกำหนดความเป็นส่วนตัวเอาไว้ซึ่งแตกต่างจาก APPEL [12] โดยทำการแบ่งเป็นระดับการอนุญาตที่ต่างกัน 3 ระดับ ดังนี้

- Free : เงื่อนไขที่ผู้ใช้อนุญาตให้ระบบ DRM กระทำกับข้อมูลความเป็นส่วนตัวได้อย่างอิสระ
- Limited : เงื่อนไขที่ผู้ใช้ให้ระบบ DRM กระทำกับข้อมูลความเป็นส่วนตัวตามความจำเป็นเท่านั้น
- NotGiven : เงื่อนไขที่ผู้ใช้ไม่อนุญาตให้ระบบ DRM กระทำกับข้อมูลความเป็นส่วนตัวของผู้

ในการกำหนดความเป็นส่วนตัวของผู้ใช้สำหรับระบบการจัดการสิทธิ์ดิจิตอลนั้น ในบางครั้งการกำหนดเหล่านี้อาจเกิดการขัดแย้งกันระหว่างเงื่อนไข จำเป็นต้องแบ่งตามลำดับความสำคัญ (Priority) โดยที่กำหนดให้เงื่อนไขที่กำหนดใน NotGiven จะมีลำดับความสำคัญสูงสุด ถ้าเงื่อนไขที่กำหนดใน NotGiven ตรงกับเงื่อนไขอื่นๆแล้ว ระบบจะถือว่าผู้ใช้ไม่ให้ข้อมูลเหล่านั้นแก่ระบบ และเงื่อนไขที่กำหนดใน Free ระบบถือเป็นเงื่อนไขที่มีลำดับความสำคัญต่ำที่สุด โดยที่เงื่อนไข Limited จะมีลำดับความสำคัญรองจาก NotGiven โดยจะแสดงในตัวอย่างดังรูปที่ 3.8 และ XML Schema ของผู้ใช้ระบบ DRM จะถูกแสดงไว้ในภาคผนวก ข.

```
<?xml version="1.0"?>
  <preference>
    <free>
      <statement>
        <purpose> <current/> </purpose>
        <recipient> <ours/> </recipient>
        <retention defined-by="license"/>
        <data-group>
            <data type="#user.name"/>
            <data type="#user.gender"/>
        </data-group>
       </statement>
    </free>
    <limited>
      <statement>
        <purpose> <admin/> <develop/> </purpose>
        <recipient> <delivery/> <other-recipient/> </recipient>
        <retention defined-by="material"/>
        <data-group>
            <data type="#user.clickstream"/>
            <data type="#user.telephone"/>
        </data-group>
       </statement>
    </limited>
    <not-given>
      <statement>
        <purpose> <analysis-decision/> </purpose>
        <recipient> <public/> <unrelated/> </recipient>
        <retention defined-by="indefinite"/>
        <data-group>
            <data type="#user.email.address"/>
            <data type="#user.home.address"/>
            <data type="#user.creditcard"/>
        </data-group>
      </statement>
    </not-given>
  </preference>
```

รูปที่ 3.8 ตัวอย่างการกำหนดความเป็นส่วนตัวของผู้ใช้

3.6 อัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัว (Privacy Negotiation Algorithm)

จากการออกแบบนโยบายความเป็นส่วนตัวสำหรับผู้ใช้และระบบ DRM ในข้างต้นนั้น DRM privacy agent จะทำการอ่านนโยบายของระบบ DRM และทำการเปรียบเทียบการกำหนดความเป็นส่วนตัวของผู้ใช้กับนโยบายของระบบ DRM ซึ่งการทำงานดังกล่าวใช้อัลกอริทึมในการเปรียบเทียบ โดย DRM privacy agent มีขั้นตอนการทำงานแบ่งย่อยได้เป็น 2 ขั้นตอน คือ Rule Evaluation และ Negotiation Process ซึ่งแต่ละกระบวนการทำหน้าที่ได้อย่างมีประสิทธิภาพ เพื่อให้ได้กฎที่เหมาะสมที่สุด (Best matching rule) สำหรับการทำงานของผู้ใช้และระบบ DRM DRM privacy agent สามารถเป็นตัวแทนการเจรจาต่อรองการทำงานระหว่างผู้ใช้กับระบบ DRM เพื่อให้ได้ข้อตกลงที่เป็นที่พอใจของทั้ง 2 ฝ่ายและเพื่อเพิ่มความเป็นส่วนตัวให้แก่ผู้ใช้งานในระบบ DRM

การเจรจาต่อรองเป็นกระบวนการตัดสินใจที่กระทำระหว่างผู้มีส่วนร่วม 2 ฝ่าย เพื่อให้บรรลุจุดประสงค์เป็นที่พอใจของทั้งสองฝ่าย โดยในระบบเครือข่ายอินเทอร์เน็ตนั้นตัวแทนหรือ Agents จะทำหน้าที่เป็นผู้แทนในการเจรจาระหว่าง 2 ฝ่ายหรือหลายๆฝ่าย เพื่อให้ได้ข้อสรุปหรือข้อตกลงที่เป็นที่ยอมรับของแต่ละฝ่าย งานวิจัยและโครงการที่เกิดขึ้นได้แก่ AuctionBot [23] เป็นวิธีการประมูลราคาสินค้าทางอินเทอร์เน็ต โดยที่ผู้ขายจะทำการเสนอราคาสินค้าและให้ AuctionBot ทำหน้าที่ในการจัดการและกำหนดการประมูลสินค้าตามโปรโตคอลและพารามิเตอร์ให้แก่ผู้ที่ทำการประมูล ในงานวิจัยอื่นๆ Kasbah [24] เป็นระบบ Web-based multi-agent โดยที่ผู้ใช้จะทำการสร้างตัวแทนการซื้อและขายเพื่อช่วยในการติดต่อซื้อขายสินค้า การเจรจาต่อรองของ Kasbah นั้นเป็นวิธีพื้นฐาน นั่นคือหลังจากผู้ซื้อและผู้ขายจับคู่การซื้อขายได้แล้ว ตัวแทนการซื้อจะเสนอราคาให้แก่ตัวแทนการขาย และตัวแทนการขายตอบสนองข้อเสนอ(ตกลง/ไม่ตกลง)เหล่านั้น โดยในงานวิจัยนี้ได้ออกแบบ DRM privacy agent ที่แตกต่างจากวิธีการดังกล่าวเนื่องจากการเจรจาข้างต้นเป็นการเจรจาต่อรองในราคาสินค้าที่ทำการซื้อหรือขายกัน แต่ในการทำการเจรจาต่อรองในความเป็นส่วนตัวนี้ ได้กระทำกับประเภทข้อมูลส่วนบุคคลในการขอการใช้ข้อมูล ในกรณีต่างๆ ซึ่งเป็นการกระทำระหว่างระบบ DRM และผู้ใช้งานเนื้อหาดิจิตอล ซึ่งในวิธีการเจรจาต่อรองจะทำงานอัตโนมัติระหว่างผู้ใช้และระบบ DRM โดยจะกล่าวถึงในหัวข้อถัดไป

3.6.1 กระบวนการ Rule Evaluation

เป็นกระบวนการเปรียบเทียบการกำหนดความเป็นส่วนตัวของผู้ใช้กับนโยบายของระบบ DRM โดยใช้อัลกอริทึมความเป็นส่วนตัวในการเปรียบเทียบ ในกรณีที่เกิดความขัดแย้งระหว่าง User's Privacy Preferences และ DRM policy กระบวนการนี้จะใช้เงื่อนไข Conditional Statements ที่กำหนดใน DRM policy ในการแก้ปัญหาความขัดแย้งเบื้องต้นก่อนเข้าสู่กระบวนการถัดไป โดยได้กำหนดให้ความเป็นส่วนตัวของผู้ใช้เป็น Rules และ นโยบายของระบบ DRM เป็น Fact ซึ่งได้ให้คำนิยามดังนี้

นิยามที่ 1 กำหนดให้เซตของข้อมูลทั้งหมดของผู้ใช้แทนด้วยสัญลักษณ์ U

$$U = \{d_1, d_2, \ldots, d_n\} \qquad \text{โดยที่} \quad n \in I \tag{3.1}$$

นิยามที่ 2 กำหนดให้การกำหนดความเป็นส่วนตัวของผู้ใช้คือ Rules แทนด้วย R

$$R = \{r_1, r_2, \ldots, r_k\} \qquad \text{โดยที่} \quad k \in I \tag{3.2}$$

โดยที่ r_i แทนด้วยคู่ลำดับ

$$r_i = (D_{ri}, C_{ri}) \ , 1 \leq i \leq k \tag{3.3}$$

โดยที่ $D_{ri} \subseteq U$

$$C_{ri} = \{h_1, h_2, \ldots, h_l\} \ , l \in I$$

$$h_j = (X_j, V_j) \ , 1 \leq j \leq l$$

กำหนดให้ D_{ri} แทนข้อมูลของการกำหนดความเป็นส่วนตัวของผู้ใช้ (Data-group)

C_{ri} แทน Constraint ของการกำหนดความเป็นส่วนตัวของผู้ใช้ประกอบด้วย purpose, recipient, retention

X_j แทนด้วย Constraint ตัวที่ j

V_j แทนด้วยเซตของสมาชิกใน Constraint ตัวที่ j

นิยามที่ 3 กำหนดให้นโยบายของระบบ DRM คือ Facts แทนด้วย F

$$F = \{f_1, f_2, \ldots, f_m\} \qquad \text{โดยที่} \quad m \in I \tag{3.4}$$

โดยที่ f_o แทนด้วยคู่ลำดับ

$$f_o = (D_{fo}, C_{fo}) \ , 1 \leq o \leq m \tag{3.5}$$

โดยที่ $D_{fo} \subseteq U$

$$C_{fo} = \{g_1, g_2, \ldots, g_q\} \ , q \in I$$

$$g_j = (X_j, Z_j) \ , 1 \leq j \leq q$$

กำหนดให้ D_{fo} แทนข้อมูลของนโยบายความเป็นส่วนตัวของระบบ DRM (Data-group)

C_{fo} แทน Constraint ของนโยบายของระบบ DRM ประกอบด้วย purpose, recipient, retention

X_j แทนด้วย Constraint ตัวที่ j

Z_j แทนด้วยเซตของสมาชิกใน Constraint ตัวที่ j

เมื่อ DRM privacy agent ทำการเปรียบเทียบระหว่างการกำหนดความเป็นส่วนตัวของผู้ใช้ (Rules) กับนโยบายของระบบ DRM (Facts) แล้ว เมื่อ Rules ตรงกับ Facts ในเงื่อนไข Limited และ Free แล้ว ซึ่งผู้ใช้ได้ยินยอมในการเข้าใช้ข้อมูลสำหรับระบบ DRM โดยการยินยอมในเงื่อนไขนั้นจะต้องผ่านเงื่อนไข 2 เงื่อนไข คือ rule of constraint และ rule of data

กระบวนการ Rule Evaluation มีการกำหนดฟังก์ชั่นในการทำงาน ดังนี้

$$\beta(c,p) = \begin{cases} \text{true, if p satisfies c} \\ \text{false, otherwise} \end{cases} \tag{3.6}$$

ฟังก์ชั่น $\beta(c,p)$ เป็นฟังก์ชั่นที่ให้ค่าจริงหรือเท็จ เมื่อทำการเปรียบเทียบระหว่าง Facts กับ Rules โดยกำหนดให้ $p \in C_{fo}$ และ $c \in C_{ri}$

กำหนดให้ Facts f_o ยอมรับใน Rules r_i ถ้า :

A) $\forall (c \in C_{ri})$ and $\forall (p \in C_{fo})$ with $\beta(c,p) = \text{true}$ (3.7)

B1) Data-group for Free or Limited

$$D_{fo} \subseteq D_{ri} \leftrightarrow \forall (d_1 \in D_{fo}) \text{ and } \forall (d_1 \in D_{ri}) \tag{3.8.1}$$

B2) Data-group for NotGiven

$$D_{fo} \cap D_{ri} \neq \phi \tag{3.8.2}$$

ในกระบวนการ Rule Evaluation Facts ที่ผ่านอัลกอริทึมในการเปรียบเทียบความเป็นส่วนตัวกับ Rules แล้ว ในกรณีที่ Facts ตรงกับเงื่อนไข NotGiven ใน Rules อัลกอริทึมจะใช้เงื่อนไข If-then ในการแก้ปัญหากรณีเงื่อนไขตรงกัน แต่สำหรับกรณีที่ไม่สามารถแก้ปัญหาความเป็นส่วนตัวได้แล้ว ระบบจะผ่านไปยังกระบวนการเจรจาต่อรองต่อไปเพื่อค้นหา Rule ที่เหมาะสมที่สุดที่ระบบจะอนุญาตให้ผู้ใช้เข้าใช้เนื้อหาดิจิตอลได้

3.6.2 กระบวนการ Negotiation Process

หลังจากผ่านกระบวนการ Rule Evaluation แล้ว กรณีที่ Facts ไม่ตรงกับเงื่อนไข Free หรือ Limited หรือ ตรงกับเงื่อนไข NotGiven ใน Rule จะต้องผ่านกระบวนการเจรจาต่อรอง (Negotiation Process) เพื่อให้ได้ Rule ที่เหมาะสมสำหรับระบบ DRM ที่สุด เพื่อให้ระบบ DRM สามารถอนุญาตให้ผู้ใช้สามารถเข้าใช้เนื้อหาดิจิตอลได้ โดยในการหา Best Matching Rule นั้น DRM privacy agent จะทำหน้าที่ในการคำนวณโดยเอาน้ำหนัก (weight) ของเงื่อนไขต่างๆ คือ purpose, recipient, retention และ data ที่กำหนดโดยผู้ใช้ระบบหรือเป็นการกำหนดจากค่า

มาตรฐานของระบบ ที่อยู่ในเงื่อนไข Free และ Limited และนำมาหาผลรวมเพื่อให้ได้กฎที่เหมาะสมที่สุด (Best Matching Rule) ระหว่างผู้ใช้ และระบบ DRM ในการทำกระบวนการเจรจาต่อรองความเป็นส่วนตัว โดยได้กำหนดฟังก์ชั่นในการหา Best Matching Rule ดังนี้

กำหนดให้ฟังก์ชั่น σ_c เป็นค่าที่เกิดจากการคำนวณ โดยเปรียบเทียบระหว่าง constraint ของ Facts กับ Rules ที่มีสมาชิกตรงกันและ σ_d เป็นค่าที่เกิดจากการคำนวณ โดยเปรียบเทียบระหว่าง data-group ของ Facts กับ Rules ที่มีสมาชิกตรงกัน โดยกำหนดตัวแปรตามนิยามในหัวข้อ 3.6.1 และแสดงสมการดังนี้

$$\sigma_c(h_i,f_o) = \begin{cases} 0, & \text{if } (Z_i \cap V_i) = \phi \\ n, n > 0, & \text{if } (Z_i \cap V_i) \neq \phi \end{cases} \tag{3.9}$$

$$\sigma_d(D_{ri},f_o) = \begin{cases} 0, & \text{if } (D_{fo} \cap D_{ri}) = \phi \\ n, n > 0, & \text{if } (D_{fo} \cap D_{ri}) \neq \phi \end{cases} \tag{3.10}$$

ฟังก์ชั่น $\partial(r_i,f_o)$ เป็นฟังก์ชั่นที่คำนวณหาค่าผลรวมของจำนวน Rules ที่ตรงกับ Facts โดยนำ Weight ในเงื่อนไขของแต่ละ Rules มาคำนวณ แสดงดังนี้

$$\partial(r_i,f_o) = \left[\sum_{i=1}^{n} \sigma_c(h_i,f_o) \cdot w_i\right] + \sigma_d(D_{ri},D_{fo}) \cdot w_d \tag{3.11}$$

กำหนดให้ w_i และ w_d เป็นน้ำหนัก (Weights) ที่กำหนดใน Constraints และ Data-group ของ f_o ตามลำดับ ในการกำหนดค่าของน้ำหนักสามารถให้ค่าที่แสดงลำดับความสำคัญของเงื่อนไข purpose, recipient, retention และ data ใน Rule ได้ เพื่อให้ได้ Best matching rule ที่ถูกต้องและเหมาะสมที่สุด ได้อธิบายการกำหนดค่า Weights ในหัวข้อ 3.8 ต่อไป

หลังจากระบบ DRM ได้คำนวณหาจำนวนที่ Rules ตรงกับ Fact ในระบบตามสมการ (3.11) แล้ว DRM privacy agent จะทำหน้าที่เลือกกฎ (Rule) ที่เหมาะสมกับระบบ DRM (Fact) มากที่สุด (Best matching rule) เพื่อให้ทั้งระบบ DRM และผู้ใช้สามารถทำงานได้ โดยการคำนวณหา Best matching rule จะต้องผ่านฟังก์ชั่นเพื่อคำนวณหาค่าที่มากที่สุดที่ Fact ตรงกับ Rules โดยมีฟังก์ชั่นดังนี้

$$\max(\partial(r_i,f_o)) \qquad \text{โดยที่} \quad 1 \leq i \leq n \tag{3.12}$$

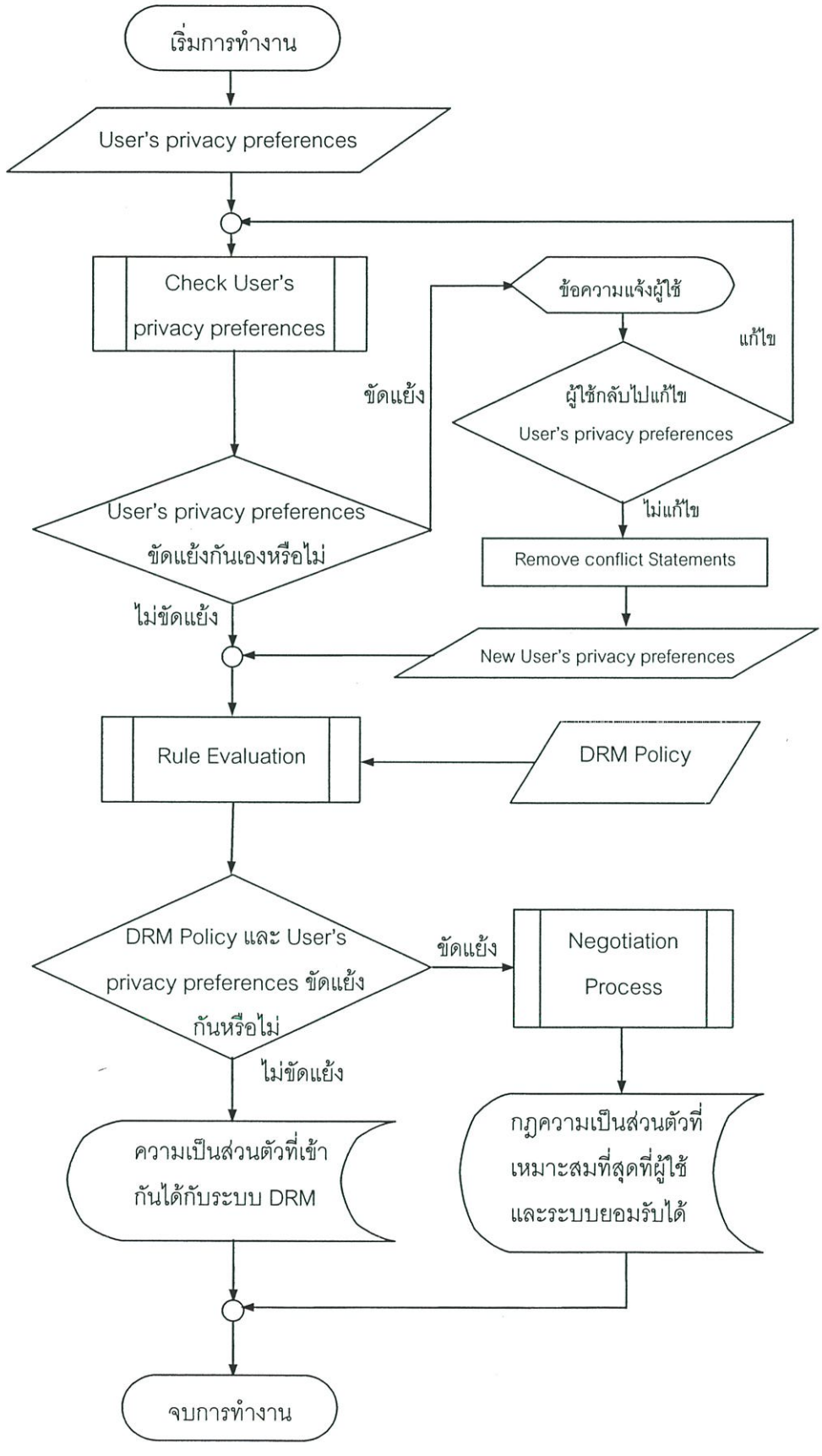
Best matching rule ที่คำนวณได้จากสมการ (3.12) นี้ คำนวณหาค่าสูงสุดที่เป็นไปได้ที่ Fact จะใกล้เคียง (matching) กับ Rule ของผู้ใช้มากที่สุด เพื่อระบบจะสามารถนำกฎ (Rule) ที่เหมาะสมที่สุดนี้ ไปปรับเปลี่ยนใน Fact เพื่อให้ผู้ใช้สามารถเข้าใช้งานเนื้อหาดิจิตอลได้ แต่ถ้าระบบ DRM ไม่สามารถแก้ไขตาม Rule ของผู้ใช้ได้แล้วระบบจำเป็นต้องแจ้งให้ผู้ใช้ทราบ

3.7 ขั้นตอนการทำงานของการเจรจาต่อรองความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

จากการออกแบบอัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล ซึ่งทำการนิยามและกล่าวถึงสมการในหัวข้อ 3.5 แล้วนั้น ในหัวข้อนี้จะได้อธิบายแผนผังการทำงานของอัลกอริทึม และกระบวนการที่เกี่ยวข้องในระบบ แสดงในหัวข้อถัดไป

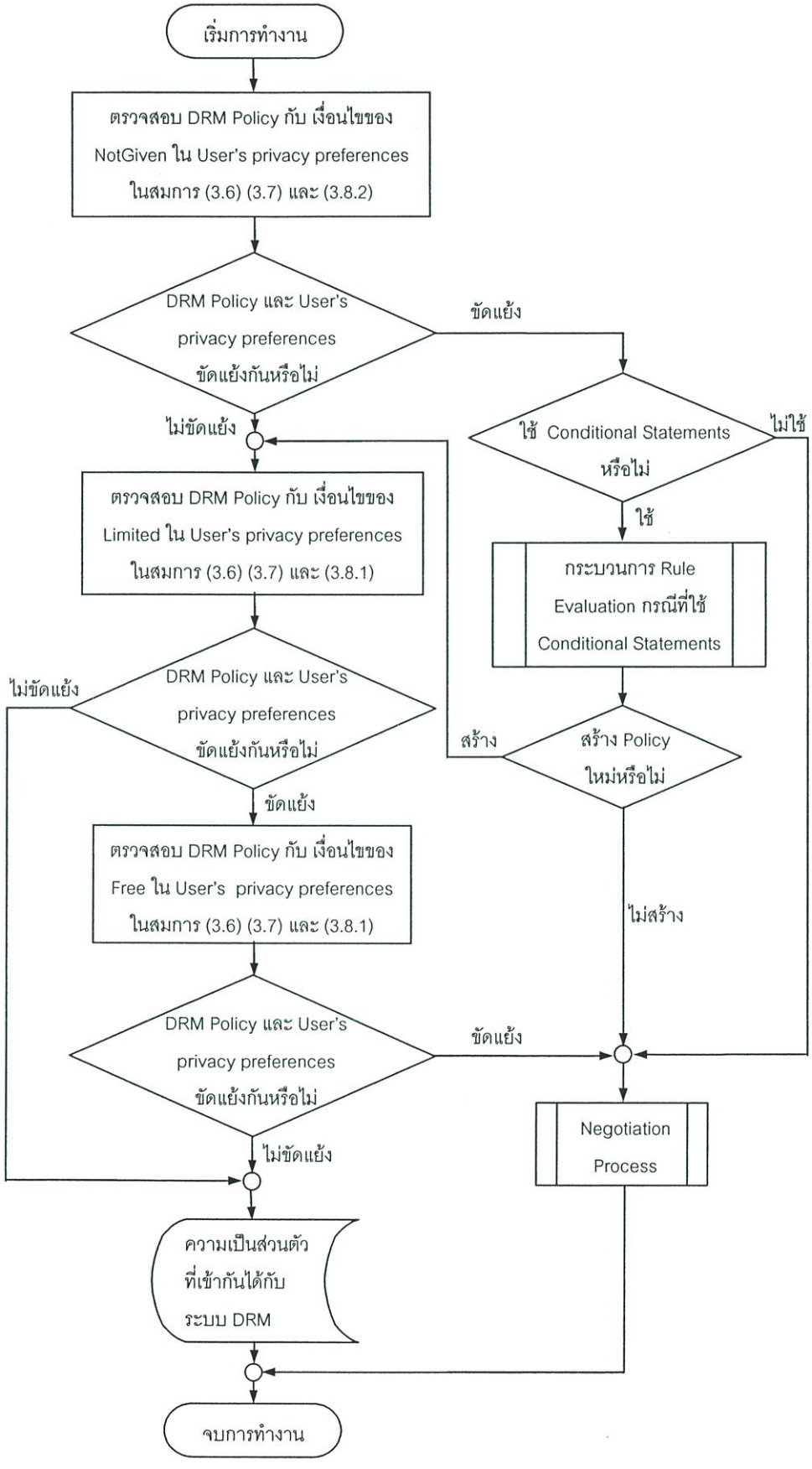
ขั้นตอนการทำงานความเป็นส่วนตัวสำหรับระบบ DRM จะแบ่งกระบวนการสำคัญเป็น 2 ขั้นตอน นั่นคือ Rule Evaluation และ Negotiation Process ซึ่งได้กล่าวในรายละเอียดในหัวข้อ 3.5 แล้วนั้น ขั้นตอนการทำงานเริ่มจากที่ DRM privacy agent ทำการอ่านนโยบายในเนื้อหาดิจิตอลที่ผู้เป็นเจ้าของได้กำหนดเอาไว้ และดึงเอาการกำหนดความเป็นส่วนตัวจากผู้ใช้มาเข้ากระบวนการ Rule Evaluation และเมื่อผ่านกระบวนการนี้แล้วจะตรวจสอบว่า DRM Policy และ User's Privacy Preference ขัดแย้งกันหรือไม่ ถ้าไม่ขัดแย้งกันผู้ใช้สามารถทำการถัดไปในการเข้าใช้งานเนื้อหาในระบบ DRM ได้ แต่ถ้าขัดแย้งกันระบบจำเป็นต้องผ่านกระบวนการ Negotiation Process เพื่อหากฎที่เหมาะสมที่สุดเพื่อผู้ใช้สามารถเข้าใช้ระบบได้ โดยแสดงแผนผังการทำงานของขั้นตอนความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลดังรูปที่ 3.9

จากแผนผังการทำงานในรูปที่ 3.9 เป็นขั้นตอนหลักในการทำงานการจัดการความเป็นส่วนตัวสำหรับระบบ DRM ซึ่งรูปที่ 3.10 และรูปที่ 3.12 จะแสดงขั้นตอนย่อยในการกระบวนการ Rule Evaluation และ Negotiation Process ซึ่งในแต่ละกระบวนการมีความสำคัญในการได้มาซึ่งการยอมรับ หรือกฎที่เข้ากันได้สำหรับระบบการจัดการสิทธิ์ดิจิตอล โดยในรูปที่ 3.11 แสดงขั้นตอนการทำงานย่อยในกระบวนการ Rule Evaluation ในกรณีที่ใช้เงื่อนไข Conditional Statements ในการแก้ปัญหาความขัดแย้งกันระหว่างนโยบายของระบบ DRM และการกำหนดความเป็นส่วนตัวของผู้ใช้

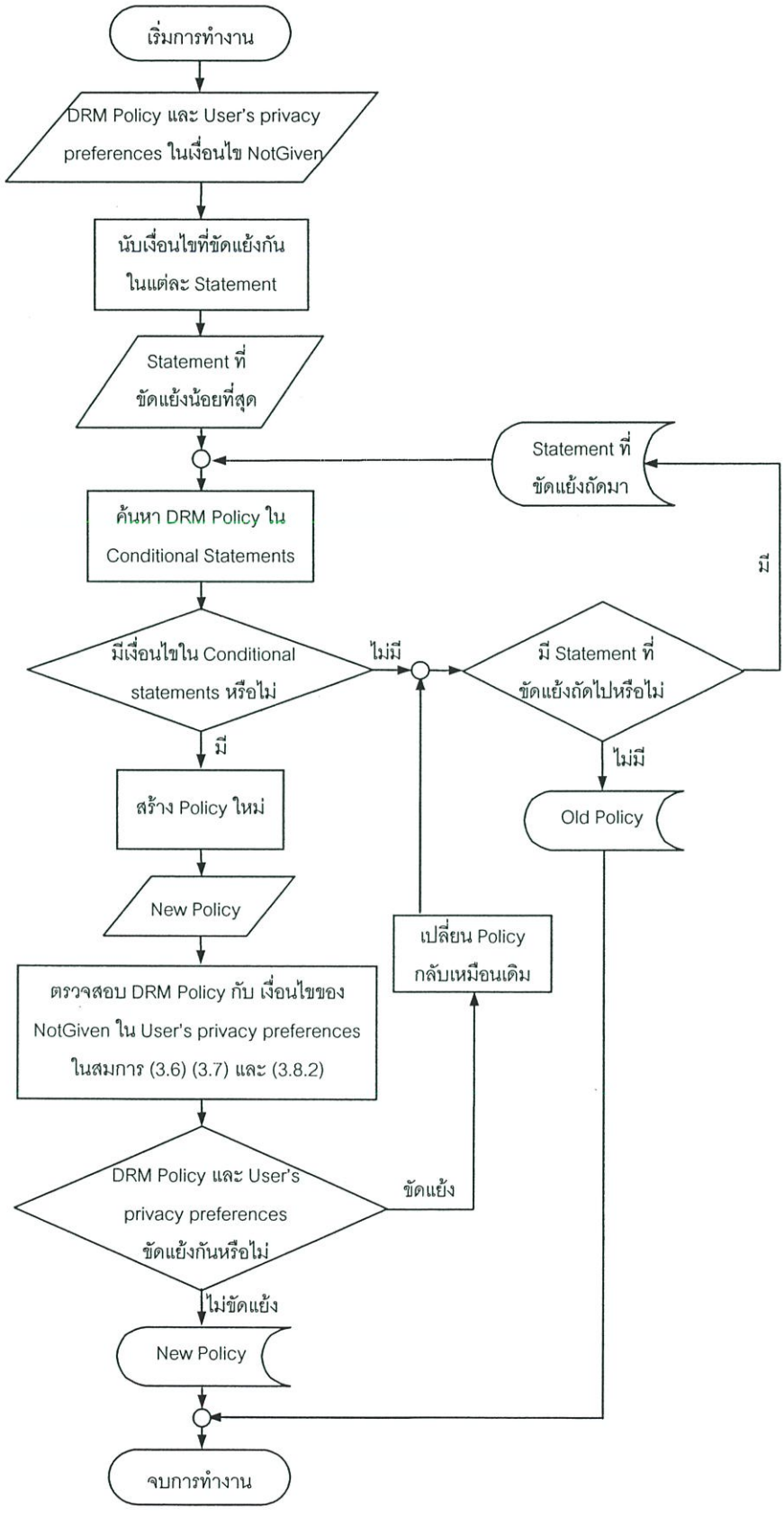


รูปที่ 3.9 ขั้นตอนการทำงานความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

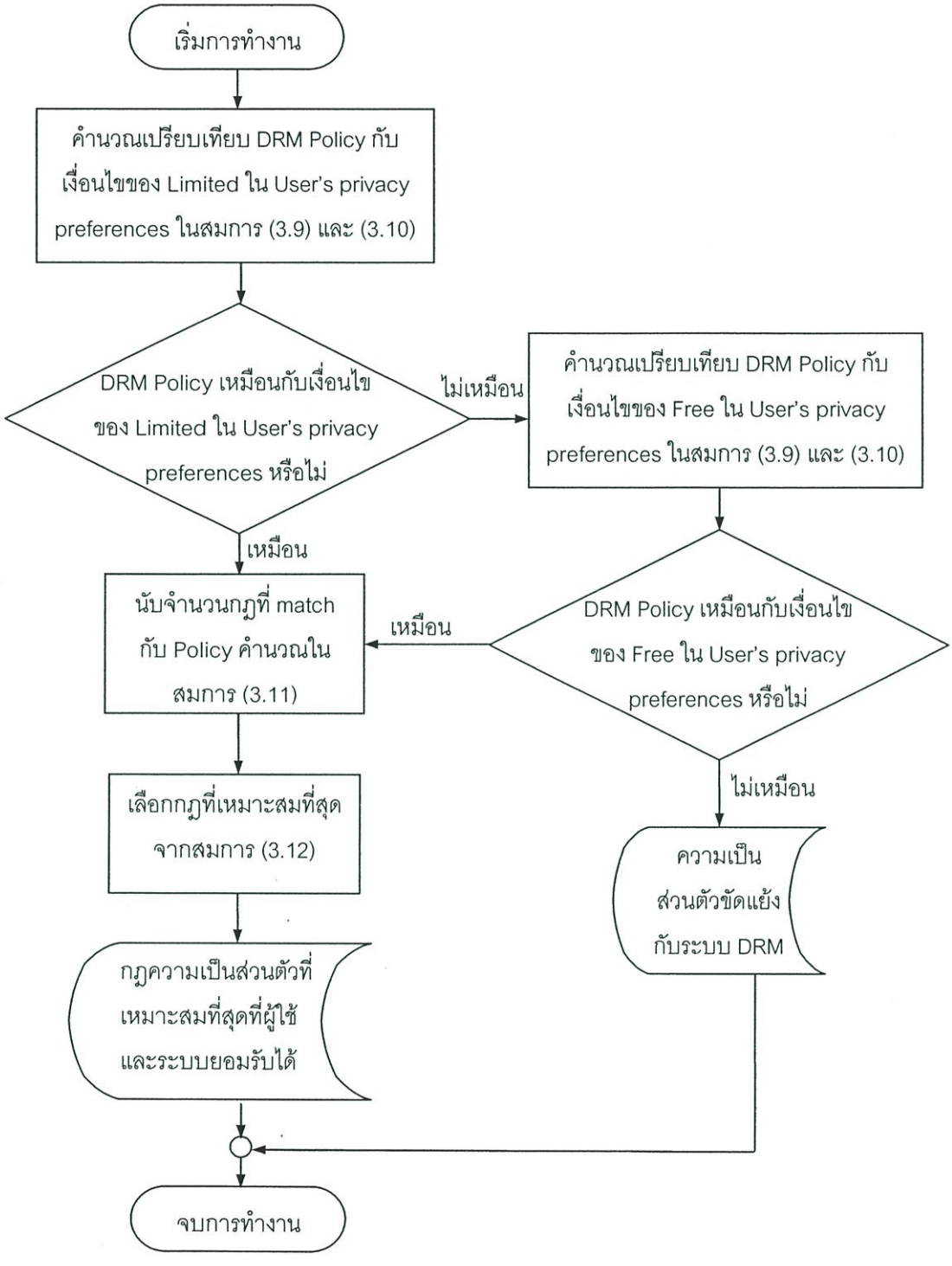
รูปที่ 3.10 ขั้นตอนการทำงานของกระบวนการ Check User's Privacy Preferences



รูปที่ 3.11 ขั้นตอนการทำงานของกระบวนการ Rule Evaluation



รูปที่ 3.12 ขั้นตอนการทำงานของกระบวนการ Rule Evaluation กรณีที่ใช้ Conditional Statements



รูปที่ 3.13 ขั้นตอนการทำงานของกระบวนในการ Negotiation Process

3.8 การกำหนดน้ำหนักในกระบวนการ Negotiation Process

หลังจากผ่านกระบวนการ Rule Evaluation มาแล้ว ในกระบวนการ Negotiation Process นี้เป็นกระบวนการค้นหากฎที่เหมาะสมที่สุด (Best Rule) ของผู้ใช้ เพื่อระบบจะยอมรับให้ผู้ใช้สามารถเข้าใช้เนื้อหาดิจิตอลในระบบ DRM ได้ ซึ่งได้กล่าวในรายละเอียดไปแล้วในหัวข้อ 3.6 นั้น ในกระบวนการนี้จำเป็นจะต้องกำหนดค่าน้ำหนัก (Weight) ให้แก่ Constraints ซึ่งประกอบด้วย Purpose, Recipient และ Retention และกำหนดค่าน้ำหนักให้แก่ Data-group (Data) เพื่อคำนวณหาค่าผลรวมตามสมการ (3.11) ในการหากฎของผู้ใช้ที่เหมาะสมที่สุดเพื่อเข้าใช้งานในระบบ DRM ได้ โดยค่า Weights นี้เป็นค่าที่ระบบ DRM ได้กำหนดขึ้น ซึ่งอาจจะกำหนดค่า Weights ให้แก่ Constraint และ Data-group ให้มีค่าเท่ากันหรือมีค่าแตกต่างกันก็ได้ โดยค่า Weights จะเป็นเลขจำนวนเต็ม โดยในงานวิจัยนี้ได้แบ่งเงื่อนไขเป็นการกำหนดค่า Weights เป็น 2 กรณี เพื่อคำนวณหา Best Rule ที่เหมาะสมที่สุดแก่ระบบ DRM และผู้ใช้ ดังนี้

กรณีที่ 1 กำหนดให้ Weights มีค่าเท่ากัน

การกำหนดค่า Weights ให้มีค่าเท่ากันในทุก Constraint และ Data-group นั้นหมายความว่าระบบต้องการให้ความสำคัญต่อ Constraints (Purpose, Recipient และ Retention) และ Data-group (Data) มีค่าเท่ากัน ดังนั้นการคำนวณเพื่อหา Best Rule จะขึ้นอยู่กับจำนวนของ Constraint และจำนวนของ Data-group ใน Rule ตรงกับ Fact มากที่สุด โดยมีเงื่อนไขในการกำหนดค่า Weights ดังนี้

1) $W_{purpose} = W_{recipient} = W_{retention} = W_{data}$

2) $W_{all} \geq 1$ และ $W_{all} \in I$

กรณีที่ 2 กำหนดให้ Weights มีค่าต่างกัน

การกำหนด Weights ใน Constraint และ Data-group ให้มีค่าต่างกัน นั่นหมายความว่าจะต้องกำหนดค่า Weights ใน Constraint (Purpose, Recipient และ Retention) และ Data-group (Data) ให้มีค่าแตกต่างกันไป โดยการกำหนดค่า Weight ให้มีค่าสูงใน Constraint หรือ Data-group แล้ว หมายความว่าในกระบวนการหา Best Rule ตามสมการ (3.11) และ สมการ (3.12) ระบบจะให้ความสำคัญใน Constraints หรือ Data-group นั้นมากกว่า Constraints หรือ Data-group อื่นๆ ซึ่งในการกำหนดค่า Weights ที่มีค่าต่างกันนั้น จำเป็นต้องเป็นค่าที่เหมาะสมเพื่อสามารถหา Best Rule ได้ตรงกับความต้องการของระบบ โดยในการกำหนดค่า Weights ที่ดีนั้น ในงานวิจัยนี้ได้มีการกำหนดค่าดังนี้

กำหนดให้

N_i เป็นจำนวนสมาชิกใน Constraint และ Data-group ใน Fact

W_i เป็นค่าน้ำหนักใน Constraint และ Data-group

โดย i แทนเลขจำนวนเต็มมีค่า 1-4 โดยตัวเลขที่มีค่าต่ำจะแทนลำดับความสำคัญน้อย และตัวเลขสูงขึ้นจะมีลำดับความสำคัญมากขึ้น

1) กำหนดลำดับความสำคัญให้แก่ Constraint (purpose, recipient, retention) และ Data-group (data)
2) กำหนดค่า Weight ให้กับเงื่อนไขที่มีลำดับความสำคัญน้อยที่สุด โดยที่

$$W_1 \geq 1 \text{ และ } W_1 \in I \tag{3.13}$$

3) หาค่า W_2 โดยที่ $W_2 \in I$ สามารถหาค่า W_2 ได้จากสมการ

$$W_1 < W_2 < (N_i \cdot W_1) \tag{3.14}$$

4) หาค่า W_3 โดยค่า $W_3 > W_2$ และ $W_3 \in I$ สามารถหาค่า W_3 ได้จากสมการ

$$W_2 < W_3 < ((N_1 \cdot W_1) + (N_2 \cdot W_2)) \tag{3.15}$$

5) หาค่า W_4 โดยค่า $W_4 > W_3$ และ $W_4 \in I$ สามารถหา W_4 ได้จากสมการ

$$W_3 < W_4 < ((N_1 \cdot W_1) + (N_2 \cdot W_2) + (N_3 \cdot W_3)) \tag{3.16}$$

ในการกำหนดค่า Weight ตามวิธีข้างต้นเป็นการหาค่า Weights ที่เหมาะสมตามลำดับความสำคัญแก่ Constraints และ Data-group ใน Fact โดยค่า Weights ที่คำนวณได้จะมีความสัมพันธ์กัน ซึ่งเป็นเลขจำนวนเต็มที่อยู่ในช่วงที่สัมพันธ์กันอย่างเหมาะสมเพื่อให้ได้ Best Rule ที่ตรงกับความต้องการกับระบบมากที่สุด โดยถ้ากำหนดค่า Weight ให้ใกล้เคียงกับค่าสูงสุดในช่วงที่เป็นไปได้ของ Weight แต่ละตัวแล้ว แสดงว่าระบบต้องการให้ความสำคัญกับ Constraints หรือ Data-group ใน Weight ตัวนั้นมากเป็นพิเศษ ทำให้การคำนวณค่าหา Best Rule ในระบบก็จะให้ความสำคัญในการเลือกกฎที่ตรงกับ Constraint หรือ Data-group ตัวนั้นมาก แต่ถ้ากำหนดค่า Weight ยิ่งใกล้เคียงกับค่าน้อยที่สุดในช่วงที่เป็นไปได้ของ Weight แต่ละตัวแล้ว แสดงว่าระบบต้องการให้ความสำคัญกับเงื่อนไขใน Weight ตัวนั้นน้อย ดังนั้นทำให้การคำนวณค่าหา Best Rule ระบบจะให้ความสำคัญในการเลือกกฎที่ตรงกับ Constraint หรือ Data-group ตัวนั้นน้อยลง แต่ถ้ากำหนดค่า Weights ให้กับ Constraints และ Data-group อยู่นอกเหนือช่วงที่กำหนดไว้ ในกรณีที่กำหนดค่า Weights มากกว่าช่วงที่กำหนดไว้ ระบบ DRM จะถือว่าให้ความสำคัญแก่ Constraints หรือ Data-group ตัวนั้นมาก โดยที่ไม่สนใจความสำคัญของ Constraints หรือ Data-group ที่มีความสำคัญรองลงมาเลย ซึ่งการกำหนดค่า Weights ในการคำนวณหา Best Rule นั้นควรกำหนดค่าให้ไม่ห่างจนเกินไปทั้งนี้ก็ขึ้นกับความต้องการของระบบ DRM

ต่อไปนี้จะแสดงตัวอย่างการกำหนดค่า Weight ในกรณีต่างๆ ที่ได้กล่าวถึงข้างต้นในกระบวนการ Negotiation Process โดยรูปที่ 3.14 แสดงตัวอย่างการกำหนด User's Privacy Preference (Rules) ในเงื่อนไข Free และ Limited และรูปที่ 3.15 แสดงตัวอย่างการกำหนดนโยบายในระบบ DRM

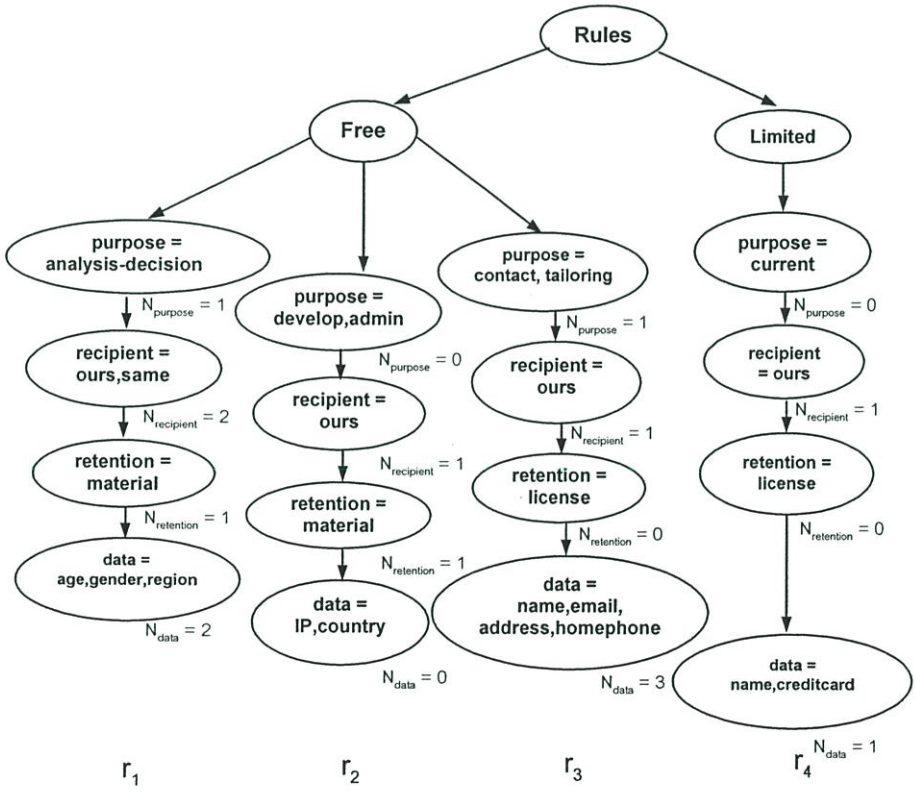
```
<free>
   <statement>
      <purpose> <analysis-decision/> </purpose>
      <recipient> <ours/> <same/> </recipient>
      <retention> <material/> </retention>
      <data-group>
        <data type="#age"/>
        <data type="#sex"/>
        <data type="#region"/>
        </data-group>
    </statement>
    <statement>
       <purpose> <develop/> <admin/> </purpose>
       <recipient> <ours/> </recipient>
       <retention> <material/> </retention>
       <data-group>
         <data type="#IP"/>
         <data type="#Country"/>
        </data-group>
     </statement>
     <statement>
         <purpose> <contact/> <tailoring/> </purpose>
         <recipient> <ours/> </recipient>
          <retention> <license/> </retention>
           <data-group>
              <data type="#name"/>
              <data type="#email.address"/>
              <data type="#address"/>
              <data type="#homephone"/>
         </data-group>
       </statement>
</free>
<limited>
       <statement>
         <purpose> <current/> </purpose>
         <recipient> <ours/> </recipient>
         <retention> <license/> </retention>
         <data-group>
              <data type="#name"/>
              <data type="#creditcard"/>
          </data-group>
        </statement>
</limited>
```

รูปที่ 3.14 ตัวอย่างการกำหนด User's Privacy Preference ในเงื่อนไข Free และ Limited

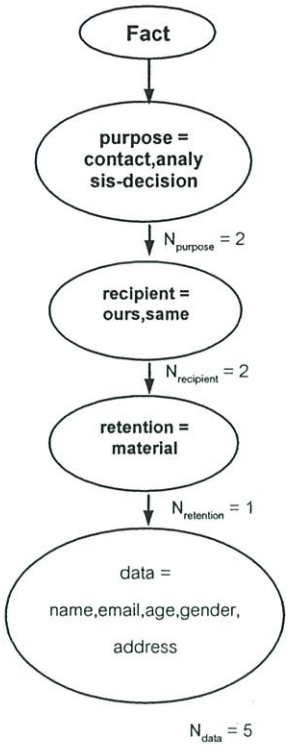
```
<mandatory>
    <statement>
        <purpose> <contact/> <analysis-decision/> </purpose>
        <recipient> <ours/> <same/> </recipient>
        <retention> <material/> </retention>
        <data-group>
            <data type="#name"/>
            <data type="#email"/>
            <data type="#age"/>
            <data type="#gender"/>
            <data type="#address"/>
        </data-group>
    </statement>
</mandatory>
```

รูปที่ 3.15 ตัวอย่างการกำหนดนโยบายในระบบ DRM

จากรูปที่ 3.14 และ รูปที่ 3.15 ทำการแปลงส่วน User's Privacy Preferences และ DRM policy ให้เป็นแผนภูมิต้นไม้ เพื่อสามารถทำความเข้าใจได้ดียิ่งขึ้นแสดงดังรูปที่ 3.16



รูปที่ 3.16 แผนภูมิต้นไม้ของ Rules (User's Privacy Preferences) ในเงื่อนไข Free และ Limited และ Fact (DRM policy)



รูปที่ 3.16 (ต่อ)

จากรูปที่ 3.16 เป็นตัวอย่างนโยบายของระบบ DRM ซึ่งเมื่อผ่านกระบวนการ Negotiation Process จะทำการ matching ระหว่าง Fact (Policy) กับ Rules (User's Privacy Preferences) เพื่อคำนวณหา Best Rule นั้น การคำนวณโดยการแทนค่าจำนวนการ matching เหล่านี้ในสมการ (3.9) แสดงดังนี้

<u>กรณีที่ 1</u> กำหนดให้ Weights มีค่าเท่ากัน

กำหนดให้ $W_{all} = 1$ สามารถหาค่าโดยแทนค่าในสมการ (3.11) แสดงดังนี้

$$\partial(r_1,f) = (1 \cdot w_{purpose} + 2 \cdot w_{recipient} + 1 \cdot w_{retention}) + 2 \cdot w_{data}$$

$$\partial(r_2,f) = (0 \cdot w_{purpose} + 1 \cdot w_{recipient} + 1 \cdot w_{recipient}) + 0 \cdot w_{data}$$

$$\partial(r_3,f) = (1 \cdot w_{purpose} + 1 \cdot w_{recipient} + 0 \cdot w_{recipient}) + 3 \cdot w_{data}$$

$$\partial(r_4,f) = (0 \cdot w_{purpose} + 1 \cdot w_{recipient} + 0 \cdot w_{recipient}) + 1 \cdot w_{data}$$

เมื่อแทนค่าแล้วจะได้ค่าดังนี้

$$\partial(r_1,f) = ((1x1) + (2x1) + (1x1)) + (2x1) = 6$$

$\partial(r_2,f) = ((0x1) + (1x1) + (1x1)) + (0x1) = 2$

$\partial(r_3,f) = ((1x1) + (1x1) + (0x1)) + (3x1) = 5$

$\partial(r_4,f) = ((0x1) + (1x1) + (0x1)) + (1x1) = 2$

ดังนั้นเมื่อแทนค่า $\partial(r_i,f)$ ในสมการ (3.12) เพื่อหาค่าสูงสุดแล้วจะได้ $\partial(r_1,f)$ ซึ่งมีค่าเท่ากับ 6 ดังนั้น Best Rule $= r_1$

<u>กรณีที่ 2</u> กำหนดให้ Weights มีค่าต่างกัน

จากกรณีที่ 2 การหาค่า Weight ที่เหมาะสมสามารถหาได้ตามวิธีข้างต้นดังนี้

1) กำหนดลำดับความสำคัญให้ Recipient < Retention < Purpose < Data
   จาก Fact ในรูปที่ 3.14 ทำให้กำหนดค่าตัวแปรได้ดังนี้
   $N_1 = 2, N_2 = 1, N_3 = 2, N_4 = 5$
2) กำหนดค่า Weight ให้กับเงื่อนไขที่มีลำดับความสำคัญน้อยที่สุดนั่นคือ Recipient
   จากสมการ (3.13) ดังนั้นกำหนดค่าให้ $W_1 = 2$
3) จากสมการ (3.14) ในการหาค่า W_2 นั่นคือ
   $W_1 < W_2 < (N_i \cdot W_1)$
   $2 < W_2 < 4$
   ดังนั้นกำหนดให้ค่า $W_2 = 3$
4) จากสมการ (3.15) จะได้ค่า W_3 มีค่าระหว่าง
   $W_2 < W_3 < (N_1 \cdot W_1) + (N_2 \cdot W_2)$
   $3 < W_3 < 7$
   ดังนี้กำหนดให้ $W_3 = 5$
5) จากสมการ (3.16) จะได้ค่า W_4 มีค่าระหว่าง
   $W_3 < W_4 < (N_1 \ W_1) + (N_2 \ W_2) + (N_3 \ W_3)$
   $5 < W_4 < 17$
   ดังนั้นกำหนดให้ $W_4 = 6$

ดังนั้น $W_{purpose} = 5$, $W_{recipient} = 2$, $W_{retention} = 3$, $W_{data} = 6$

สามารถหาค่าโดยแทนค่าในสมการ (3.11) ได้ค่าดังนี้

$\partial(r_1,f) = ((1x5) + (2x2) + (1x3)) + (2x6) = 24$

$\partial(r_1,f) = ((0x5) + (1x2) + (1x3)) + (0x6) = 5$

$\partial(r_1,f) = ((1x5) + (1x2) + (0x3)) + (3x6) = 25$

$\partial(r_1,f) = ((0x5) + (1x2) + (0x3)) + (1x6) = 8$

ดังนั้นเมื่อแทนค่า $\partial(r_i,f)$ ในสมการ (3.12) เพื่อหาค่าสูงสุดแล้ว จะได้ $\partial(r_3,f)$ เท่ากับ 25 ดังนั้น Best Rule $= r_3$

จากตัวอย่างที่แสดงข้างต้นนี้แสดงให้เห็นว่าการกำหนดค่า Weight ที่เหมือนหรือแตกต่างกันจะทำให้ผลลัพธ์ของการได้มาซึ่งกฎ (Best Rule) ที่เหมาะสมกับระบบ DRM และผู้ใช้มากที่สุดนั้นต่างกันด้วย ซึ่งการกำหนดค่า Weight มีความสำคัญในการกำหนดค่าให้แก่ Constraints (purpose, recipient และ retention) และ Data-group (data) ซึ่งทำให้บ่งบอกถึงการให้ลำดับความสำคัญของเงื่อนไขเหล่านี้ในระบบ DRM

3.9 กระบวนการทดสอบและวิเคราะห์เปรียบเทียบประสิทธิภาพ

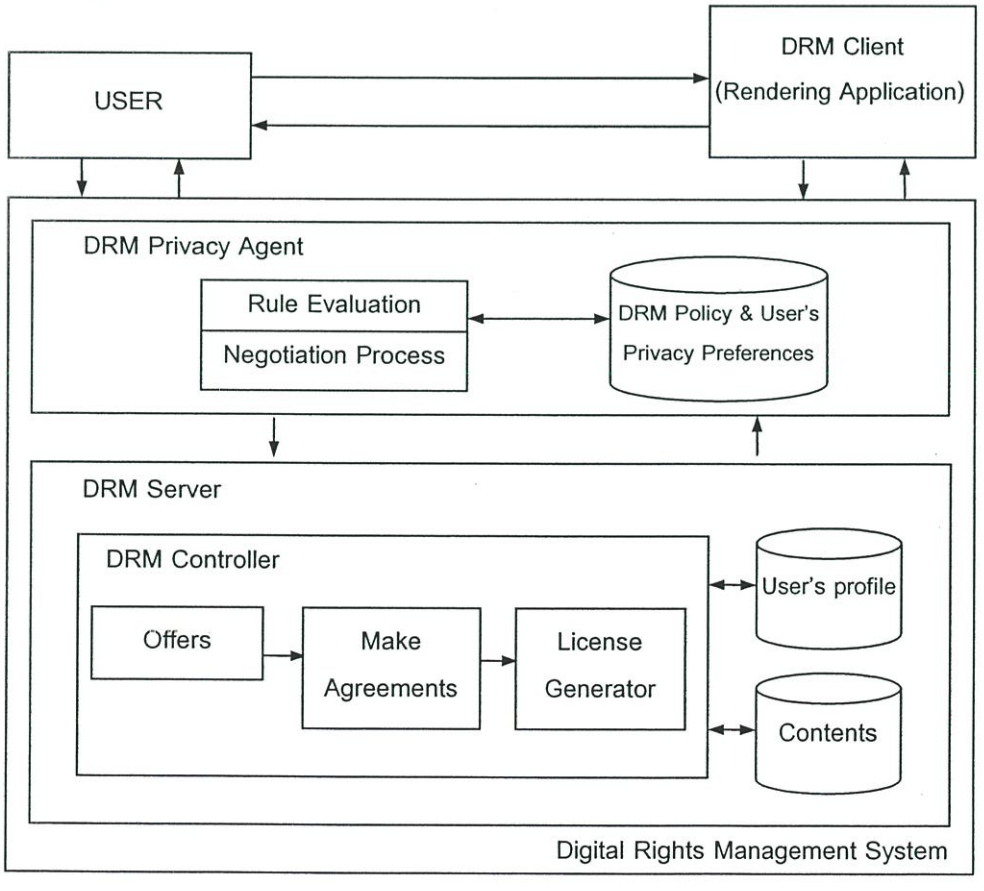
เมื่อออกแบบความเป็นส่วนตัวให้แก่ระบบ DRM แล้ว ในส่วนของการทดสอบจำเป็นต้องจำลองระบบ DRM ขึ้น และทำการตรวจสอบว่าระบบ DRM ที่เพิ่มความเป็นส่วนตัวเข้าไปในระบบแล้วนั้น สามารถให้ความเป็นส่วนตัวแก่ผู้ใช้เพิ่มขึ้นจริงหรือไม่ ในการหาคำตอบทำได้โดยการเปรียบเทียบประสิทธิภาพอัลกอริทึมการทำงานในขั้นตอน Rule Evaluation และ ขั้นตอน Negotiation Process โดยในขั้นตอน Rule Evaluation จากสมการ (3.6), (3.7), (3.8.1) และ (3.8.2) ในกรณีที่ระบบไม่มีการใช้เงื่อนไข Conditional Statement กับกรณีการใช้ Conditional Statements ในการแก้ปัญหา แล้วเปรียบเทียบเปอร์เซ็นต์ความสามารถในการลดขั้นตอนการ Negotiation Process และทำการทดลองปรับค่า Facts และ Rules ที่เข้ามาในระบบ เป็นค่าต่างๆ เพื่อให้ได้ที่มีความถูกต้องที่สุด

บทที่ 4
การพัฒนาระบบต้นแบบความเป็นส่วนตัว สำหรับระบบการจัดการสิทธิ์ดิจิตอล

ในบทที่ผ่านมาได้กล่าวถึง หลักการและวิธีการในการออกแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล ในบทต่อไปนี้จะอธิบายในรายละเอียดของการพัฒนาระบบต้นแบบในการเพิ่มความเป็นส่วนตัวเข้าไปยังระบบ DRM

4.1 โครงสร้างระบบ

ในการพัฒนาระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลที่ได้ทำการพัฒนาขึ้นนี้ ทำขึ้นเพื่อพิสูจน์แนวความคิดในการออกแบบนโยบายความเป็นส่วนตัวที่กล่าวถึงในบทที่ 3 สามารถเข้ากันได้กับระบบ DRM ที่มีอยู่ในปัจจุบันได้ โดยมีโครงสร้างการทำงานแสดงดังรูปที่ 4.1



รูปที่ 4.1 โครงสร้างของระบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

จากโครงสร้างการทำงานของความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลที่แสดงในรูปที่ 4.1 สามารถอธิบายการทำงานได้ดังนี้

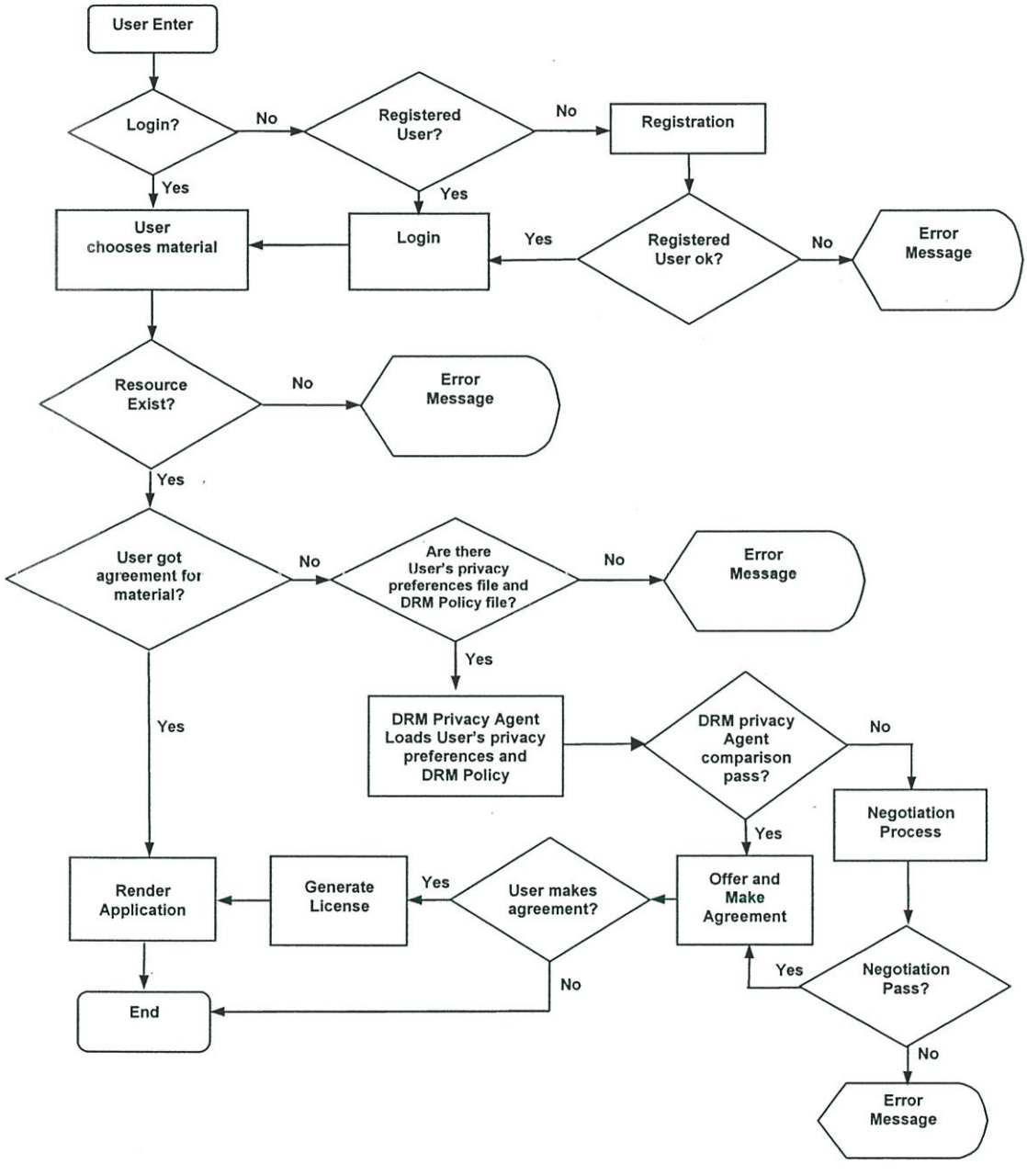
1) User เข้าใช้งานระบบ DRM โดยการเลือก Material ในระบบ
2) DRM privacy agent ทำหน้าที่อ่าน DRM policy จากระบบ และ User's Privacy Preferences จากผู้ใช้ และทำการเปรียบเทียบ DRM policy และ User's Privacy Preferences โดยมีกระบวนการ Rule Evaluation และ Negotiation Process ในการทำงานและแสดงผลการเปรียบเทียบให้ผู้ใช้
3) DRM Server จะจัดการเกี่ยวกับสิทธิ์ที่เจ้าของ material นำเสนอสิทธิ์ให้แก่ผู้ใช้ (Offer) และกระบวนการทำการตกลงระหว่างเจ้าของสิทธิ์และผู้ใช้ที่ต้องการใช้งาน material (Make agreement) และกระบวนการการสร้างใบรับรองสิทธิ์แก่ผู้ใช้ (License generator) ซึ่งติดต่อกับฐานข้อมูลผู้ใช้ (User's profile) และ ฐานข้อมูล material (Content server)
4) DRM Client ทำหน้าที่ Render Application โดยจะทำตามสิทธิ์ที่อยู่ใน License ที่ผู้ใช้ทำข้อตกลงไว้กับเจ้าของ material

4.2 ขอบเขตของการพัฒนาระบบ

ในการพัฒนาระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลนั้นจะพัฒนาตามการออกแบบความเป็นส่วนตัวที่ได้ทำการอธิบายในบทที่ 3 โดยจะเน้นการพัฒนาในส่วนความเป็นส่วนตัวที่เหมาะสมกับระบบ DRM เพื่อพิสูจน์แนวความคิดในการออกแบบนโยบายความเป็นส่วนตัว ให้สามารถเข้ากันได้กับระบบ DRM ที่มีอยู่ในปัจจุบัน โดยจะทำการเปรียบเทียบนโยบายการกำหนดความเป็นส่วนตัวของระบบกับการกำหนดความเป็นส่วนตัวของผู้ใช้ และในกรณีที่มีความขัดแย้งเกิดขึ้น ระบบจะทำการค้นหากฎความเป็นส่วนตัวของผู้ใช้ที่ใกล้เคียงกับระบบมากที่สุดเพื่อให้ผู้ใช้สามารถเข้าใช้งานระบบ DRM ได้โดยที่ไม่ละเมิดความเป็นส่วนตัวของผู้ใช้ และการทำงานในส่วนของ DRM นั้นระบบได้จำลองการทำงานจากโครงสร้างการทำงานของ DRM Reference Architecture [15] โดยแบ่งเป็นส่วนประกอบสำคัญ 2 ส่วน คือ DRM Server และ DRM Client โดย DRM Server มีกระบวนการทำงานภายใน 3 กระบวนการคือ Offers, Make Agreements และ License Generator โดย DRM Client ทำหน้าที่ Render Application ตามสิทธิ์ที่ผู้ใช้ทำข้อตกลงโดยอ่านจาก License ของผู้ใช้

4.3 แผนผังการทำงานของระบบ

ในการทำงานของระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลมีขั้นตอนการทำงานแสดงดังรูปที่ 4.2



รูปที่ 4.2 แผนผังการทำงานความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

4.4 การพัฒนาระบบ

ในการพัฒนาระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลนั้น ผู้วิจัยได้เลือกพัฒนาการทำงานของระบบ DRM ในรูปของ Web-based Application ซึ่งเป็นรูปแบบการทำงานขั้นพื้นฐานของระบบ DRM และเลือกใช้ภาษาจาวาในการพัฒนาระบบ โดยใช้เครื่องมือของ J2SDK (Java 2 Software Development Kit) ดาวน์โหลดได้จาก http://java.sun.com/j2se ซึ่งเป็นตัวแปลภาษาสำหรับแปลงไวยากรณ์ภาษาจาวาเป็นไบต์โค้ด โดยใช้สภาพแวดล้อมในรูปแบบการทำงานแบบไคลแอ็นต์/เซิร์ฟเวอร์ ซึ่งโปรแกรมภาษาจาวานี้จะทำงานบนเครื่องระดับเซิร์ฟเวอร์ มีรูปแบบการทำงานที่เรียกว่าจาวาเซิร์ฟเล็ต (Java Servlet) และใช้ Apache Tomcat เวอร์ชั่น 4.1 เป็นเว็บเซิร์ฟเวอร์ ดาวน์โหลดได้จาก http://jakarta.apache.org/tomcat/ เพื่อรองรับการทำงานของระบบและสนับสนุนฐานข้อมูลที่เป็นภาษา XML ซึ่งในการพัฒนาระบบต้นแบบความเป็นส่วนตัวสำหรับระบบ DRM นี้ได้ใช้โปรแกรมจัดการฐานข้อมูลที่เรียกว่า xindice เวอร์ชั่น 1.1 สามารถดาวน์โหลดได้จาก http://xml.apache.org/xindice/ ซึ่งเป็นโปรแกรมจัดการฐานข้อมูลของ XML การพัฒนาระบบต้นแบบทั้งหมดที่เลือกใช้เป็นฟรีซอร์ฟแวร์ที่สามารถดาวน์ได้ทั่วไปบนเว็บไซต์และมีประสิทธิภาพสูง

การพัฒนาระบบต้นแบบความเป็นส่วนตัวสำหรับระบบ DRM ซึ่งได้พัฒนาตามการออกแบบที่กล่าวถึงในบทที่ 3 โดยเน้นการทำงานในเรื่องความเป็นส่วนตัวในระบบการจัดการสิทธิ์ดิจิตอล ซึ่งเป็นการทดสอบว่าการเพิ่มความเป็นส่วนตัวเข้าไปยังระบบ DRM สามารถเข้ากันได้กับระบบที่เป็นรูปแบบทั่วไปที่พัฒนาขึ้น และเป็นการเพิ่มความเป็นส่วนตัวให้แก่ผู้ใช้และไม่ทำลายการละเมิดเงื่อนไขที่เจ้าของเนื้อหาดิจิตอลได้เป็นผู้กำหนดเอาไว้ โดยการออกแบบโครงสร้างและการใช้งานต้นแบบระบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลนั้นได้กล่าวไว้โดยละเอียดในภาคผนวก ก.

บทที่ 5
การทดลองและผลการทดลอง

ในบทที่ผ่านมาได้กล่าวถึง การพัฒนาระบบต้นแบบในการเพิ่มความเป็นส่วนตัวเข้าไปยังระบบ DRM ในบทนี้จะอธิบายในรายละเอียดของการทดลอง การวัดประสิทธิภาพจากระบบที่ได้พัฒนาขึ้น

5.1 หลักการทดลอง

เนื่องจากงานวิจัยนี้สร้างขึ้นมาจากแนวความคิดที่ต้องการแก้ปัญหาการละเมิดความเป็นส่วนของผู้ใช้งานที่เกิดขึ้นจากระบบการจัดการสิทธิ์ดิจิตอล โดยออกแบบนโยบายและอัลกอริทึมความเป็นส่วนตัวที่เหมาะสมกับระบบการจัดการสิทธิ์ดิจิตอล ซึ่งได้กล่าวถึงในบทที่ 3 โดยได้ออกแบบนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้ในรูปแบบที่เหมาะสมกับระบบ DRM ซึ่งได้ปรับปรุงให้มีความยืดหยุ่นและมีประสิทธิภาพเหมาะสำหรับระบบ DRM และสำหรับระบบต้นแบบที่ได้ทำการพัฒนาขึ้นนี้ ทำขึ้นเพื่อพิสูจน์แนวความคิดในการออกแบบนโยบายความเป็นส่วนตัว สามารถเข้ากันได้กับระบบ DRM ที่มีอยู่ในปัจจุบันได้หรือไม่ ซึ่งในการทำการทดลองจะทำการทดสอบจากแนวคิดที่ทำการออกแบบนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้ให้เหมาะสมสำหรับระบบ DRM และทดสอบอัลกอริทึม ว่ามีผลการทำงานอย่างไร และมีข้อบกพร่องที่ควรปรับปรุงแก้ไขประการใดบ้าง โดยมีสมมุติฐานที่ว่า "ถ้านโยบายความเป็นส่วนตัวของระบบการจัดการสิทธิ์ดิจิตอลมี Conditional Statement ในการแก้ปัญหาความเป็นส่วนตัวแล้ว จะทำให้ลดกระบวนการ Negotiation Process และเป็นการเพิ่มประสิทธิภาพของการเจรจาต่อรองความเป็นส่วนตัวแก่ระบบ DRM ด้วย"

5.2 การออกแบบการทดลองและการเตรียมเครื่องมือ

ในการทดสอบประสิทธิภาพการทำงานจากการออกแบบนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้ ว่ามีความเหมาะสม เพิ่มความยืดหยุ่นแก่ผู้ใช้ระบบและระบบ DRM หรือไม่นั้น ได้ทำการทดสอบตามสมมุติฐานที่ได้กล่าวในหัวข้อข้างต้น โดยในการทดลองได้กำหนดสภาพแวดล้อมของระบบ โดยทำการจำลองตัวอย่างข้อมูลการกำหนดความเป็นส่วนตัวของผู้ใช้ (User's Privacy Preferences) และนโยบายของระบบ (DRM policy) โดยแสดงข้อมูลเป็นเซตของตัวแปร เพื่อง่ายต่อการทดสอบและวัดประสิทธิภาพ ในหัวข้อนี้จะอธิบายการออกแบบการทดลอง เครื่องมือและสภาพแวดล้อมที่ใช้ในการทดลอง ดังนี้

5.2.1 การออกแบบการทดลอง

ในการออกแบบการทดลอง เพื่อวัดประสิทธิภาพของอัลกอริทึมตามสมมุติฐานข้างต้นนั้น ได้ทำการออกแบบการทดลองดังนี้

1. ทำการกำหนดความเป็นส่วนตัวของผู้ใช้ (User's Privacy Preferences) หรือ Rules จำนวนตั้งแต่ 50 – 1000 กฎ เพื่อใช้ในการเปรียบเทียบความเป็นส่วนตัวกับนโยบายของระบบ (DRM Policies) หรือ Facts โดยทำการโปรแกรมสุ่มตัวอย่างให้มีความหลากหลาย
2. ทำการกำหนดนโยบายของระบบ DRM หรือ Facts เพื่อเปรียบเทียบความเป็นส่วนตัวกับ Rules ที่ได้จากการสุ่มตัวอย่างในข้อ 1 โดยในการทดลองได้แบ่งชุดข้อมูลการทดลองเป็น 2 ชุดข้อมูล โดยข้อมูลทั้งสองชุดมีการกำหนดนโยบายความเป็นส่วนตัวที่แตกต่างกัน แต่มีวิธีการทดลองพิสูจน์ตามสมมุติฐานเหมือนกัน เพื่อใช้ในการเปรียบเทียบและสนับสนุนผลการทดลอง
3. ในการกำหนดชุดข้อมูลทดลอง 2 ชุดข้อมูลข้างต้น ในงานวิจัยนี้ได้ทำการทดลองตามเงื่อนไข 2 ประการ เพื่อนำไปสู่การพิสูจน์ตามสมมุติฐานการทดลอง โดยมีเงื่อนไขดังนี้
    ก) มีการใช้เงื่อนไข Conditional Statements ในนโยบายความเป็นส่วนตัวสำหรับระบบ DRM เพื่อแก้ปัญหากรณีที่ผู้ใช้ไม่ต้องการให้ข้อมูลเหล่านั้นแก่ระบบ ใน Fact ที่ 1 และ Fact ที่ 2
    ข) ทำการเพิ่มจำนวนเงื่อนไข Conditional Statements ไปทีละเงื่อนไข ในชุดข้อมูลที่ 1 ได้แก่ Fact ที่ 1-1, 1-2, 1-3, 1-4, 1-5 และในชุดข้อมูลที่ 2 ได้แก่ Fact ที่ 2-1, 2-2, 2-3, 2-4, 2-5
4. หลังจากเตรียมข้อมูล Rules และ Facts แล้ว นำ Rules และ Facts มาทำการเปรียบเทียบโดยใช้อัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวที่ได้ออกแบบไว้ในบทที่ 3 จำลองการทำงานโดยใช้โปรแกรม MATLAB ในการทำวัดประสิทธิภาพ ซึ่งในการวัดประสิทธิภาพอัลกอริทึมนั้น ได้ทำการเปรียบเทียบระหว่างการกำหนดนโยบายความเป็นส่วนตัวระบบ DRM ที่งานวิจัยได้ออกแบบขึ้นกรณีที่มีการใช้ Conditional Statements ในการแก้ปัญหาความขัดแย้งระหว่าง DRM policy และ User's Privacy Preferences กับ กรณีที่การกำหนดนโยบายความเป็นส่วนตัวโดยทั่วไปที่ไม่มีการแก้ปัญหาความขัดแย้งโดยใช้ Conditional Statements ใน P3P [11]

5. การทดลองได้หาค่าจำนวนการขัดแย้งเมื่อไม่ใช้ Conditional Statements กับกรณีที่ใช้ Conditional Statements และคำนวณหาเปอร์เซ็นต์ความสามารถในการลดกระบวนการ Negotiation Process ซึ่งสามารถนำมาวิเคราะห์ประสิทธิภาพการทำงานของอัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวและประสิทธิภาพการทำงานของระบบ DRM ได้ โดยได้อธิบายการวิเคราะห์ผลการทดลองในหัวข้อที่ 5.4

5.2.2 การเตรียมเครื่องมือสำหรับการทดลอง

ในส่วนของการทดสอบประสิทธิภาพนี้ ได้ทำการทดลองโดยใช้เครื่องมือและคุณสมบัติของเครื่องมือดังนี้

ในส่วนของฮาร์ดแวร์ประกอบด้วย

- Dell PC Compatible ใช้ CPU Pentium 4 1.6 GHz
- หน่วยความจำขนาด 256 MB
- ฮาร์ดดิสก์ขนาด 20 GB

ในส่วนของซอฟต์แวร์ประกอบด้วย

- ระบบปฏิบัติการ Windows XP Professional
- โปรแกรม MATLAB เวอร์ชั่น 6.1

สำหรับข้อมูลที่ใช้ในการทดลองเป็นการกำหนดนโยบายความเป็นส่วนตัวของระบบ DRM (DRM Policy) และทำการสุ่มตัวอย่าง (Random Sampling) การกำหนดความเป็นส่วนตัวของผู้ใช้ (User's privacy preferences) โดยใช้โปรแกรม MATLAB ในการสร้างและสุ่มข้อมูลในการทดลอง และเก็บไว้ในรูปของฐานข้อมูล

ในการสร้างชุดข้อมูลโดยการสุ่มนั้นเป็นการสุ่มตัวอย่างแบบวิธีความน่าจะเป็น (Probability Sampling Methods) โดยใช้วิธีการสุ่มตัวอย่างแบบง่าย (Simple Random Sampling Method) เป็นวิธีการสุ่มตัวอย่างซึ่งประชากรทั้งหมดมีโอกาสที่จะได้รับการคัดเลือกอย่างเท่าเทียมกัน ทั้งนี้เนื่องจากในทางปฏิบัติจะเป็นการคัดเลือกโดยการสุ่มจากสมาชิกของ Purpose, Recipient, Retention และ Data จากกรอบของจำนวนสมาชิกที่มีอยู่ กระบวนการในการคัดเลือกไม่มีความซับซ้อนยุ่งยาก สามารถทำได้โดยการตารางตัวเลขสุ่ม (Table of Random Numbers) ตารางนี้สร้างโดยโปรแกรม MATLAB ประกอบด้วยกลุ่มตัวเลขหลายหลัก ตัวอย่างของตารางนี้แสดงในตารางที่ 5.1 เป็นตัวอย่างการสุ่มสมาชิกใน Purpose ประกอบด้วยกลุ่มตัวเลข 1 – 7 หลัก เนื่องจากมีสมาชิกที่ใช้ในงานวิจัยนี้ 7 ประเภท โดยกำหนดให้แทนด้วยตัวเลข 1-7 เรียงตามลำดับของชนิด Purpose เพื่อให้การสุ่มตัวอย่างทำได้ง่ายขึ้นแสดงดังนี้

ตารางที่ 5.1 ตัวอย่างตารางตัวเลขสุ่มของสมาชิกใน Purposes

123456	123	1356	457	14567	3467
356	2 12367	347	1357	12346	23567
2567	37	256	24567	23467	257
234	12357	1	26	47	1347
.....					

หลังจากได้สร้างตารางตัวเลขสุ่มที่ทำการสุ่มสมาชิกใน Purpose, Recipient, Retention และ Data แล้ว จะทำการสุ่มค่าในตารางตัวเลขสุ่มของสมาชิกทั้ง 4 เหล่านี้ออกมาอีกครั้ง เพื่อสร้างชุดข้อมูลการกำหนดความเป็นส่วนตัวของผู้ใช้ (User's privacy preferences) โดยประกอบไปด้วย Purpose, Recipient, Retention และ Data ดังแสดงในตารางที่ 5.2 โดยการสุ่มนี้ทำเพื่อให้ได้ชุดข้อมูลที่มีความหลากหลาย และเป็นประโยชน์ในการทดสอบวิธีการต่างๆ ต่อไป และเพื่อให้ง่ายในการทำความเข้าใจและไม่สับสน งานวิจัยนี้ได้แสดงกำหนดตัวเลขสุ่มโดยแทนด้วยตัวแปร เช่น Purpose มีค่าเป็น $\{P_1, P_2, P_3,..., P_7\}$ โดยค่า P_1 แทนด้วยตัวเลข 1 P_2 แทนด้วยตัวเลข 2 เป็นต้น Recipient มีค่าเป็น $\{R_1, R_2,..., R_6\}$ Retention มีค่าเป็น $\{T_1, T_2,..., T_4\}$ และ Data มีค่าเป็น $\{D_1, D_2,..., D_{15}\}$ ได้กำหนดเช่นเดียวกับการกำหนดใน Purpose

ตารางที่ 5.2 ตัวอย่างข้อมูลของผู้ใช้

User's Privacy Preferences	Purpose $\{P_1,P_2,...,P_7\}$	Recipient $\{R_1,R_2,...,R_6\}$	Retention $\{T_1,T_2,...,T_4\}$	Data $\{D_1,D_2,...,D_{15}\}$
Free	$\{P_2,P_3\}$	$\{R_2,R_4,R_7\}$	$\{T_1\}$	$\{D_1,D_3,D_4,D_7\}$
Limited	$\{P_2\}$	$\{R_1\}$	$\{T_3\}$	$\{D_{12},D_{13}\}$
NotGiven	$\{P_1\}$	$\{R_3,R_5\}$	$\{T_4\}$	$\{D_5,D_6,D_8\}$

จากตารางที่ 5.2 ได้แสดงตัวอย่างข้อมูลในส่วนผู้ใช้ โดยทำการสุ่มจากโปรแกรม MATLAB และเก็บไว้เป็นเซตในฐานข้อมูล เพื่อสำหรับการทดสอบวัดประสิทธิภาพการทำงานตามสมมุติฐานที่ได้ตั้งเอาไว้ ในการกำหนดข้อมูลในส่วนของผู้ใช้ซึ่งได้แบ่งเป็น 3 เงื่อนไขคือ Free, Limited และ NotGiven โดยแต่ละลำดับเงื่อนไขอาจจะประกอบด้วยหลายๆ Statement ซึ่งภายในแต่ละ Statement ประกอบด้วยเงื่อนไขย่อยที่ผู้ใช้ได้แจ้งบอกให้แก่ระบบ DRM ประกอบด้วย Purpose, Recipient, Retention และ Data โดยเงื่อนไขย่อยเหล่านี้โปรแกรมได้กำหนดค่าสูงสุดที่

เป็นไปได้ในแต่ละเงื่อนไขเอาไว้ เช่น Purpose จะกำหนดค่าที่เป็นไปได้ตามองค์ประกอบของการกำหนดนโยบายความเป็นส่วนตัวสำหรับระบบ DRM ที่กล่าวถึงในหัวข้อ 3.3 ไว้ทั้งหมด 7 วัตถุประสงค์ ซึ่งค่าที่กำหนดในเงื่อนไข Purpose โปรแกรม MATLAB จะทำการสุ่มค่าตัวแปรในรูปของเซตที่เป็นไปได้ตั้งแต่ P_1 ถึง P_7 เป็นต้น หลังจากนั้นโปรแกรมจะทำการสุ่มค่าที่เหมาะสมและเก็บไว้ในฐานข้อมูลของผู้ใช้เพื่อการทดสอบต่อไป

ตารางที่ 5.3 ตัวอย่างข้อมูลนโยบายของระบบ DRM

DRM policy	Purpose $\{P_1,P_2,\ldots,P_7\}$	Recipient $\{R_1,R_2,\ldots,R_6\}$	Retention $\{T_1,T_2,\ldots,T_4\}$	Data $\{D_1,D_2,\ldots,D_{15}\}$	Conditional Statements
Mandatory	$\{P_1,P_3,P_4,P_5,P_6\}$	$\{R_1,R_2\}$	$\{T_3\}$	$\{D_1,D_6,D_7\}$	$\{(P_6,P_7)\}$ $\{(R_1,R_4)\}$ $\{(D_1,D_2),(D_6,D_8),(D_7,D_{14})\}$
Optional	$\{P_2,P_4\}$	$\{R_5\}$	$\{T_4\}$	$\{D_1,D_2,D_4,D_5\}$	-

จากตารางที่ 5.3 ได้แสดงตัวอย่างข้อมูลในส่วนของนโยบายของระบบ DRM ซึ่งประกอบไปด้วย Mandatory และ Optional ซึ่งได้กล่าวในรายละเอียดในบทที่ 3 แล้วนั้น ข้อมูลที่ทำการเก็บจะมีส่วนประกอบเช่นเดียวกับส่วนของผู้ใช้ดังแสดงในตารางที่ 5.2 แต่มีส่วน Conditional Statements ที่เพิ่มขึ้น โดยจะทำการเก็บเงื่อนไว้สำหรับกรณีที่ผู้ใช้ไม่อนุญาตให้ใช้ข้อมูลเหล่านั้น ข้อมูลในส่วนนี้ Conditional Statement อาจมีหรือไม่มีก็ได้ขึ้นอยู่กับนโยบายของระบบที่ได้กำหนดไว้ จากตัวอย่างข้อมูลในตารางที่ 5.3 สามารถอธิบายได้ว่า ข้อมูลที่ระบบ DRM ต้องการ (Mandatory) ประกอบด้วย Purpose คือ $\{P_1,P_3,P_4,P_5,P_6\}$ Recipient คือ $\{R_1,R_2\}$ Retention คือ $\{T_3\}$ และ Data คือ $\{D_1,D_6,D_7\}$ และใน Conditional Statement ได้กำหนดเป็นเซตของคู่ลำดับ โดยตัวแรกของคู่ลำดับแทนสมาชิกในเงื่อนไขกรณีที่ผู้ใช้ไม่อนุญาตให้ใช้สมาชิกในเงื่อนไขนั้น และคู่ลำดับตัวที่สองเป็นสมาชิกในเงื่อนไขที่ใช้แทนสมาชิกในเงื่อนไขแรก จากตารางสามารถอธิบายได้ว่า ถ้ากรณีที่ผู้ใช้ไม่ให้วัตถุประสงค์ P_6 แล้ว ระบบได้กำหนดให้นำวัตถุประสงค์ P_7 แทนลงไปในเซต ดังนั้นเซตที่แทนค่าแล้วจะมีค่าเป็น $\{P_1,P_3,P_4,P_5,\mathbf{P_7}\}$ สำหรับเงื่อนไขใน Recipient มีการอธิบายเช่นเดียวกับเงื่อนไขย่อยใน Purpose สำหรับเงื่อนไข Data นั่นข้อมูลที่ระบบ DRM ต้องการคือเซต $\{D_1,D_6,D_7\}$ และใน Conditional Statement ได้กำหนดไว้ว่า ถ้ากรณีที่ผู้ใช้ไม่ให้ข้อมูล D_1 แล้วระบบได้ให้นำข้อมูล D_2 แทนได้ ถ้ากรณีที่ผู้ใช้ไม่ให้ข้อมูล D_6 แล้วระบบได้ให้นำข้อมูล D_8 แทนได้ และสุดท้ายถ้าผู้ใช้ไม่ให้ข้อมูล D_7 แล้ว ระบบได้ให้นำข้อมูล D_{14} แทนได้ และในเงื่อนไข Retention ในที่นี้ระบบ DRM ไม่ได้กำหนด Conditional Statement เนื่องจากระบบถือว่าข้อมูลนี้จำเป็นมากสำหรับระบบ ไม่มีข้อมูลใดๆ ที่สามารถแทนกันได้

5.3 การวัดประสิทธิภาพ

จากการอธิบายการออกแบบการทดลอง และเตรียมเครื่องมือสำหรับการทดลองซึ่งได้กล่าวถึงไปแล้วนั้น ในส่วนของการทดลองวัดประสิทธิภาพของอัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวตามสมมุติฐานนั้น ได้ทำการทดลองทีละชุดข้อมูล โดยเริ่มจากชุดข้อมูลแรก คือ Fact ที่ 1, 1-1, 1-2, 1-3, 1-4, 1-5 และชุดข้อมูลที่สองคือ Fact ที่ 2, 2-1, 2-2, 2-3, 2-4, 2-5 และทำการเปรียบเทียบกับ Rules ที่ทำการสุ่มขึ้นมาโดยทำการเพิ่มค่า Rules ทีละ 50 จนกระทั่ง 1,000 Rules ได้แสดงการทดลอง และผลการทดลองดังนี้

ข้อมูลชุดที่ 1 ประกอบด้วย Fact ที่ 1, Fact ที่ 1-1, Fact ที่ 1-2, Fact ที่ 1-3, Fact ที่ 1-4 และ Fact ที่ 1-5 โดยที่ Fact ที่ 1-1 ถึง Fact ที่ 1-5 จะมีเซตข้อมูลใน Purpose, Recipient, Retention และ Data เหมือนกับ Fact ที่ 1 แต่แตกต่างกันที่เงื่อนไขใน Conditional Statement โดยที่ Fact ที่ 1-1 ถึง Fact ที่ 1-5 จะทำการเพิ่มเงื่อนไข Conditional Statement ไปทีละ 1 เงื่อนไข ซึ่งแสดงข้อมูลดังตารางที่ 5.4

ตารางที่ 5.4 ชุดข้อมูลการทดลองชุดที่ 1

DRM policy	Purpose $\{P_1,P_2,\ldots,P_7\}$	Recipient $\{R_1,R_2,\ldots,R_6\}$	Retention $\{T_1,T_2,\ldots,T_4\}$	Data $\{D_1,D_2,\ldots,D_{15}\}$	Conditional Statements
Fact ที่ 1	$\{P_3,P_5,P_6\}$	$\{R_2,R_6\}$	$\{T_1\}$	$\{D_4,D_5,D_7\}$	$\{(P_3,P_4),(P_5,P_7)\}$
Fact ที่ 1-1	$\{P_3,P_5,P_6\}$	$\{R_2,R_6\}$	$\{T_1\}$	$\{D_4,D_5,D_7\}$	$\{(P_3,P_4),(P_5,P_7)\}$ **$\{(R_2,R_1)\}$**
Fact ที่ 1-2	$\{P_3,P_5,P_6\}$	$\{R_2,R_6\}$	$\{T_1\}$	$\{D_4,D_5,D_7\}$	$\{(P_3,P_4),(P_5,P_7)\}$ $\{(R_2,R_1),$**(R_6,R_4)**$\}$
Fact ที่ 1-3	$\{P_3,P_5,P_6\}$	$\{R_2,R_6\}$	$\{T_1\}$	$\{D_4,D_5,D_7\}$	$\{(P_3,P_4),(P_5,P_7)\}$ $\{(R_2,R_1),(R_6,R_4)\}$ **$\{(D_4,D_8)\}$**

ตารางที่ 5.4 (ต่อ)

DRM policy	Purpose $\{P_1,P_2,\ldots,P_7\}$	Recipient $\{R_1,R_2,\ldots,R_6\}$	Retention $\{T_1,T_2,\ldots,T_4\}$	Data $\{D_1,D_2,\ldots,D_{15}\}$	Conditional Statements
Fact ที่ 1-4	$\{P_3,P_5,P_6\}$	$\{R_2,R_6\}$	$\{T_1\}$	$\{D_4,D_5,D_7\}$	$\{(P_3,P_4),(P_5,P_7)\}$ $\{(R_2,R_1),(R_6,R_4)\}$ $\{(D_4,D_8),\ \mathbf{(D_5,D_{10})}\}$
Fact ที่ 1-5	$\{P_3,P_5,P_6\}$	$\{R_2,R_6\}$	$\{T_1\}$	$\{D_4,D_5,D_7\}$	$\{(P_3,P_4),(P_5,P_7)\}$ $\{(R_2,R_1),(R_6,R_4)\}$ $\{(D_4,D_8),\ (D_5,D_{10}),$ $\mathbf{(D_7,D_{14})}\}$

จากการกำหนดชุดข้อมูลการทดลองชุดที่ 1 ดังแสดงในตารางที่ 5.4 โดยกำหนดให้ Fact ที่ 1 ประกอบด้วย 1 statement ในสมาชิกของ Mandatory โดยใน statement นี้ประกอบด้วยเซตของ Purpose $\{P_3,P_5,P_6\}$, Recipient $\{R_2,R_6\}$, Retention $\{T_1\}$ และ Data $\{D_4,D_5,D_7\}$ และมี Conditional Statements $\{(P_3,P_4),(P_5,P_7)\}$ สำหรับ Fact ที่ 1-1, 1-2, 1-3, 1-4 และ 1-5 มีการกำหนด statement เช่นเดียวกับ Fact ที่ 1 แต่ทำการเพิ่มเงื่อนไขใน Conditional Statements ทีละเงื่อนไข

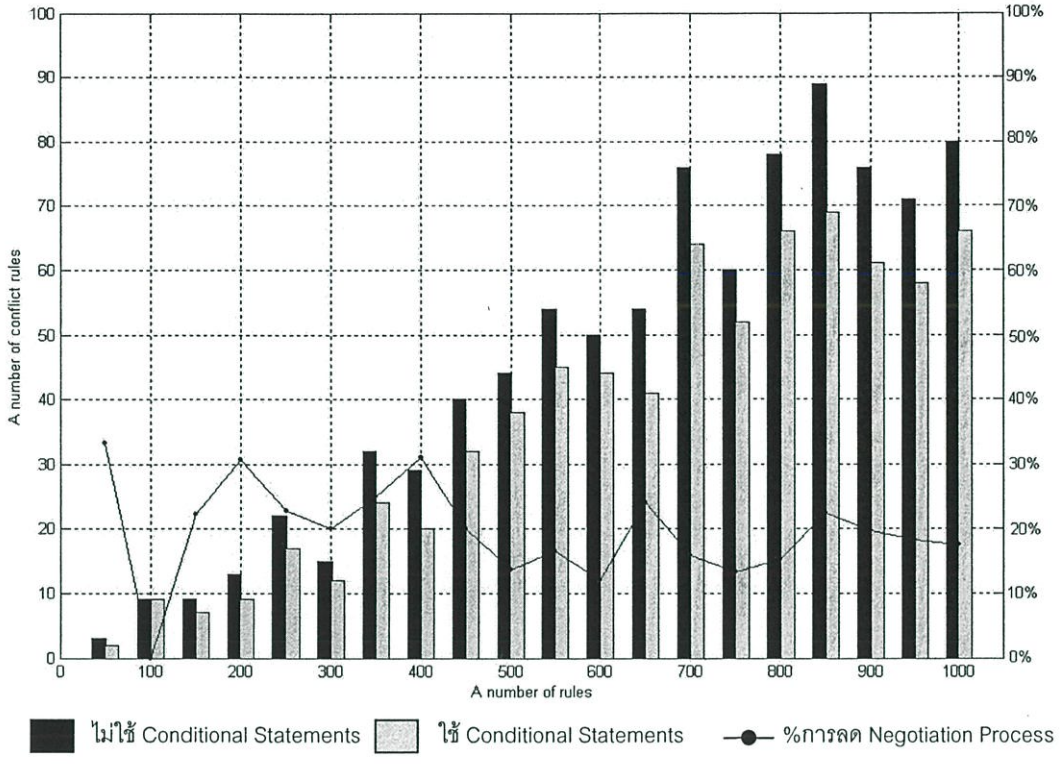
ในการทดลอง เมื่อนำชุดข้อมูลการทดลองชุดที่ 1 โดยทำการทดลองทีละ Fact เปรียบเทียบกับ Rule ที่เกิดจากการสุ่มแล้ว ถ้า Rule ใดมีการกำหนด statements ในเงื่อนไข NotGiven เหมือนกับ Fact แล้ว ระบบจะแก้ปัญหาความขัดแย้งกันระหว่าง Fact และ Rule ในเงื่อนไข NotGiven โดยนำเงื่อนไขที่กำหนดใน Conditional Statement มาแทนค่าเพื่อช่วยในการแก้ปัญหาความขัดแย้งนี้ ซึ่งกระบวนการในการเปรียบเทียบและการแทนค่าได้อธิบายในหัวข้อ 3.6 และหัวข้อ 3.7 แล้ว และผลของการทดลองโดยทำการเปรียบเทียบจำนวนความขัดแย้งที่ระหว่าง Fact และ Rule กรณีที่ใช้เงื่อนไขใน Conditional Statement ในนโยบายความเป็นส่วนตัวของระบบ DRM และกรณีที่ไม่ใช้เงื่อนไขใน Conditional Statement ของระบบ P3P [11] แสดงดังตารางที่ 5.5 และตารางที่ 5.6

ตารางที่ 5.5 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (User's Privacy Preferences) ใน Fact ที่ 1

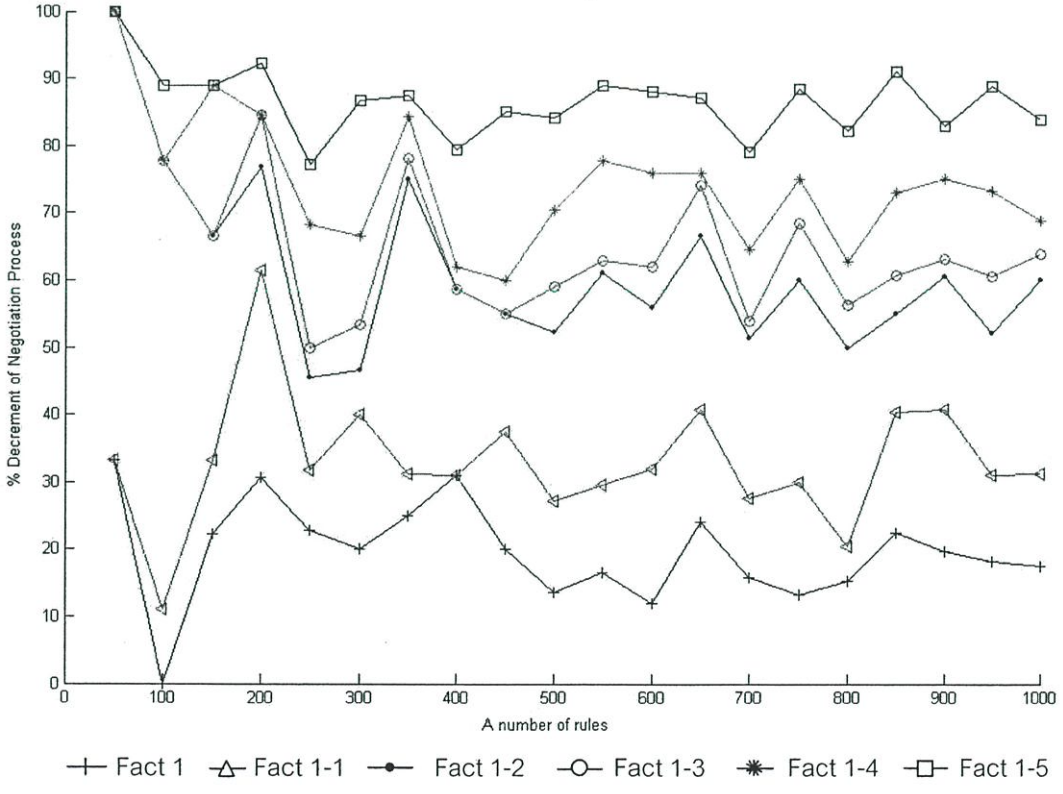
จำนวนกฎ (กฎ)	จำนวนการขัดแย้งเมื่อไม่ใช้ Conditional Statements (เงื่อนไข)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)
50	3	2	33.33%
100	9	9	0%
150	9	7	22.22%
200	13	9	30.77%
250	22	17	22.73%
300	15	12	20.00%
350	32	24	25.00%
400	29	20	31.03%
450	40	32	20.00%
500	44	38	13.64%
550	54	45	16.67%
600	50	44	12.00%
650	54	41	24.07%
700	76	64	15.79%
750	60	52	13.33%
800	78	66	15.38%
850	89	69	22.47%
900	76	61	19.74%
950	71	58	18.31%
1000	80	66	17.50%

ตารางที่ 5.6 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rules (User's Privacy Preferences) ใน Fact ที่ 1-1 ถึง Fact ที่ 1-5

จำนวน กฎ (กฎ)	Fact 1-1		Fact 1-2		Fact 1-3		Fact 1-4		Fact 1-5	
	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)
50	2	33.33	0	100.00	0	100.00	0	100.00	0	100.00
100	8	11.11	2	77.78	2	77.78	2	77.78	1	88.89
150	6	33.33	3	66.67	3	66.67	1	88.89	1	88.89
200	5	61.54	3	76.92	2	84.62	2	84.62	1	92.31
250	15	31.82	12	45.45	11	50.00	7	68.18	5	77.27
300	9	40.00	8	46.67	7	53.33	5	66.67	2	86.67
350	22	31.25	8	75.00	7	78.13	5	84.38	4	87.50
400	20	31.03	12	58.62	12	58.62	11	62.07	6	79.31
450	25	37.50	18	55.00	18	55.00	16	60.00	6	85.00
500	32	27.27	21	52.27	18	59.09	13	70.45	7	84.09
550	38	29.63	21	61.11	20	62.96	12	77.78	6	88.89
600	34	32.00	22	56.00	19	62.00	12	76.00	6	88.00
650	32	40.74	18	66.67	14	74.07	13	75.93	7	87.04
700	55	27.63	37	51.32	35	53.95	27	64.47	16	78.95
750	42	30.00	24	60.00	19	68.33	15	75.00	7	88.33
800	62	20.51	39	50.00	34	56.41	29	62.82	14	82.05
850	53	40.45	40	55.06	35	60.67	24	73.03	8	91.01
900	45	40.79	30	60.53	28	63.16	19	75.00	13	82.89
950	49	30.99	34	52.11	28	60.56	19	73.24	8	88.73
1000	55	31.25	32	60.00	29	63.75	25	68.75	13	83.75



รูปที่ 5.1 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (User's Privacy Preferences) ใน Fact ที่ 1



รูปที่ 5.2 กราฟเปรียบเทียบเปอร์เซ็นต์การลด Negotiation process ของข้อมูลการทดลองชุดที่1

การทดลองและผลการทดลองของข้อมูลชุดที่ 2 ซึ่งประกอบด้วย Fact ที่ 2, Fact ที่ 2-1, Fact ที่ 2-2, Fact ที่ 2-3, Fact ที่ 2-4 และ Fact ที่ 2-5 โดยที่ Fact ที่ 2-1 ถึง Fact ที่ 2-5 จะมีเซตข้อมูลใน Purpose, Recipient, Retention และ Data เหมือนกับ Fact ที่ 2 แต่แตกต่างกันที่เงื่อนไขใน Conditional Statements โดยที่ Fact ที่ 2-1 ถึง Fact ที่ 2-5 จะทำการเพิ่มเงื่อนไข Conditional Statement ไปทีละ 1 เงื่อนไข ซึ่งแสดงข้อมูลดังตารางที่ 5.7

ตารางที่ 5.7 ชุดข้อมูลการทดลองชุดที่ 2

DRM policy	Purpose $\{P_1,P_2,\ldots,P_7\}$	Recipient $\{R_1,R_2,\ldots,R_6\}$	Retention $\{T_1,T_2,\ldots,T_4\}$	Data $\{D_1,D_2,\ldots,D_{15}\}$	Conditional Statements
Fact ที่ 2	$\{P_1,P_2\}$	$\{R_3,R_5\}$	$\{T_3\}$	$\{D_1,D_5,D_9,$ $D_{12},D_{14}\}$	$\{(P_1,P_5)\}$ $\{(D_5,D_{10}),(D_9,D_{11}),$ $(D_{12},D_{14})\}$
Fact ที่ 2-1	$\{P_1,P_2\}$	$\{R_3,R_5\}$	$\{T_3\}$	$\{D_1,D_5,D_9,$ $D_{12},D_{14}\}$	$\{(P_1,P_5),\mathbf{(P_2,P_3)}\}$ $\{(D_5,D_{10}),(D_9,D_{11}),$ $(D_{12},D_{14})\}$
Fact ที่ 2-2	$\{P_1,P_2\}$	$\{R_3,R_5\}$	$\{T_3\}$	$\{D_1,D_5,D_9,$ $D_{12},D_{14}\}$	$\{(P_1,P_5),(P_2,P_3)\}$ $\mathbf{\{(R_3,R_1)\}}$ $\{(D_5,D_{10}),(D_9,D_{11}),$ $(D_{12},D_{14})\}$
Fact ที่ 2-3	$\{P_1,P_2\}$	$\{R_3,R_5\}$	$\{T_3\}$	$\{D_1,D_5,D_9,$ $D_{12},D_{14}\}$	$\{(P_1,P_5),(P_2,P_3)\}$ $\{(R_3,R_1),\mathbf{(R_5,R_4)}\}$ $\{(D_5,D_{10}),(D_9,D_{11}),$ $(D_{12},D_{14})\}$
Fact ที่ 2-4	$\{P_1,P_2\}$	$\{R_3,R_5\}$	$\{T_3\}$	$\{D_1,D_5,D_9,$ $D_{12},D_{14}\}$	$\{(P_1,P_5),(P_2,P_3)\}$ $\{(R_3,R_1),(R_5,R_4)\}$ $\mathbf{\{(D_1,D_4)},(D_5,D_{10}),$ $(D_9,D_{11}),(D_{12},D_{14})\}$

ตารางที่ 5.7 (ต่อ)

DRM policy	Purpose $\{P_1,P_2,\ldots,P_7\}$	Recipient $\{R_1,R_2,\ldots,R_6\}$	Retention $\{T_1,T_2,\ldots,T_4\}$	Data $\{D_1,D_2,\ldots,D_{15}\}$	Conditional Statements
Fact ที่ 2-5	$\{P_1,P_2\}$	$\{R_3,R_5\}$	$\{T_3\}$	$\{D_1,D_5,D_9,$ $D_{12},D_{14}\}$	$\{(P_1,P_5), (P_2,P_3)\}$ $\{(R_3,R_1),(R_5,R_4)\}$ $\{(D_1,D_4),(D_5,D_{10}),$ $(D_9,D_{11}), (D_{12},D_{14}),$ $\mathbf{(D_{14},D_6)}\}$

จากการกำหนดชุดข้อมูลการทดลองชุดที่ 2 ดังแสดงในตารางที่ 5.7 โดยกำหนดให้ Fact ที่ 2 ประกอบด้วย 1 statement ในสมาชิกของ Mandatory โดยใน statement นี้ประกอบด้วยเซตของ Purpose $\{P_1,P_2\}$, Recipient $\{R_3,R_5\}$, Retention $\{T_3\}$ และ Data $\{D_1,D_5,D_9,D_{12},D_{14}\}$ และมี Conditional Statements $\{(P_1,P_5)\},\{(D_5,D_{10}), (D_9,D_{11}), (D_{12},D_{14})\}$ สำหรับ Fact ที่ 2-1, 2-2, 2-3, 2-4 และ 2-5 มีการกำหนด statement เช่นเดียวกับ Fact ที่ 2 แต่ทำการเพิ่มเงื่อนไขใน Conditional Statements ทีละเงื่อนไข

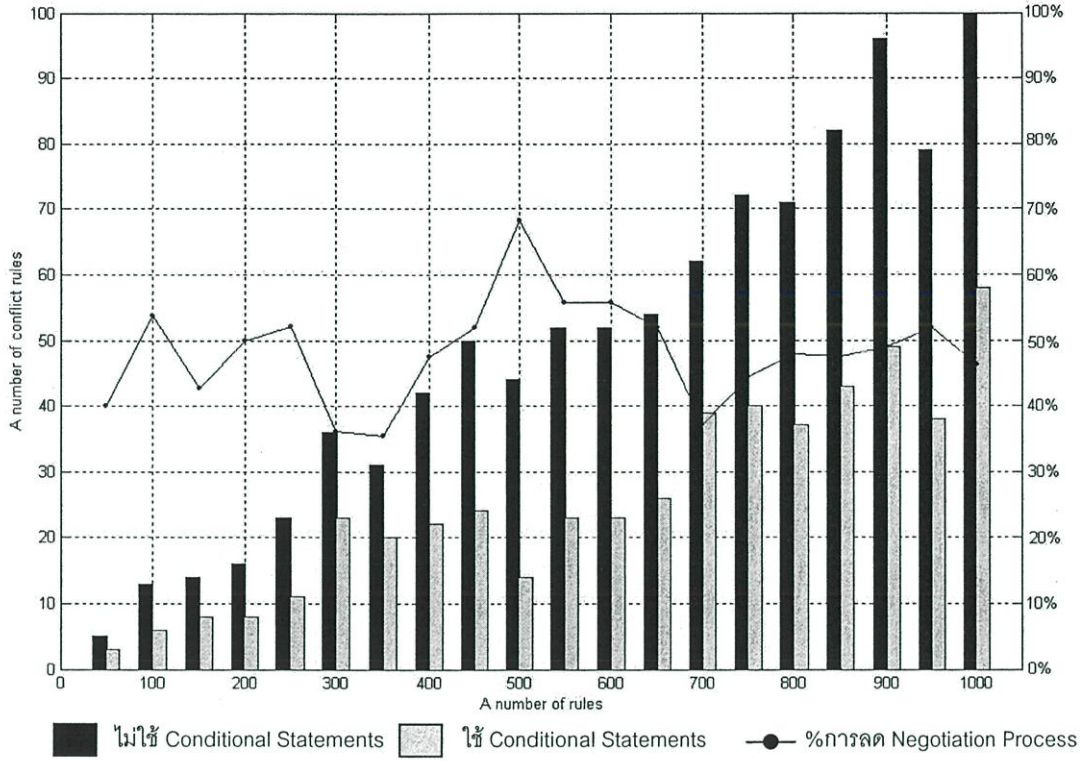
ในการทดลอง เมื่อนำชุดข้อมูลการทดลองชุดที่ 2 ซึ่งทำการทดลองเช่นเดียวกับชุดข้อมูลการทดลองชุดที่ 1 โดยทำการทดลองทีละ Fact เปรียบเทียบกับ Rule ที่เกิดจากการสุ่มแล้ว ถ้า Rule ใดมีการกำหนด statements ในเงื่อนไข NotGiven เหมือนกับ Fact แล้ว ระบบจะแก้ปัญหาความขัดแย้งกันระหว่าง Fact และ Rule ในเงื่อนไข NotGiven โดยนำเงื่อนไขที่กำหนดใน Conditional Statement มาแทนค่าเพื่อช่วยในการแก้ปัญหาความขัดแย้งนี้ ผลของการทดลองโดยทำการเปรียบเทียบจำนวนความขัดแย้งที่ระหว่าง Fact และ Rule กรณีที่ใช้เงื่อนไขใน Conditional Statement ในนโยบายความเป็นส่วนตัวของระบบ DRM และกรณีที่ไม่ใช้เงื่อนไขใน Conditional Statement ของระบบ P3P [11] แสดงดังตารางที่ 5.8 และตารางที่ 5.9

ตารางที่ 5.8 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (User's Privacy Preferences) ใน Fact ที่ 2

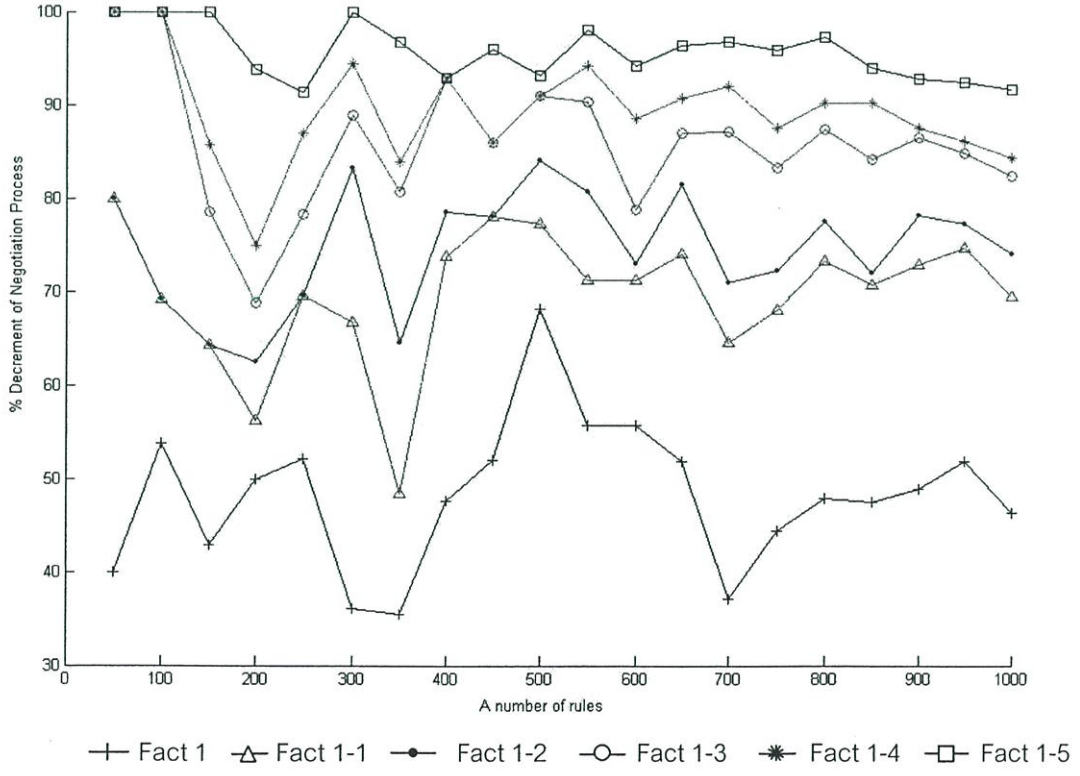
จำนวนกฎ (กฎ)	จำนวนการขัดแย้งเมื่อไม่ใช้ Conditional Statements (เงื่อนไข)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)
50	5	3	40.00
100	13	6	53.85
150	14	8	42.86
200	16	8	50.00
250	23	11	52.17
300	36	23	36.11
350	31	20	35.48
400	42	22	47.62
450	50	24	52.00
500	44	14	68.18
550	52	23	55.77
600	52	23	55.77
650	54	26	51.85
700	62	39	37.10
750	72	40	44.44
800	71	37	47.89
850	82	43	47.56
900	96	49	48.96
950	79	38	51.90
1000	108	58	46.30

ตารางที่ 5.9 การเปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (User's Privacy Preferences) ใน Fact ที่ 2-1 ถึง Fact ที่ 2-5

จำนวนกฎ (กฎ)	Fact 2-1		Fact 2-2		Fact 2-3		Fact 2-4		Fact 2-5	
	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)	จำนวนการขัดแย้งเมื่อใช้ Conditional Statements (เงื่อนไข)	ลด Negotiation Process ได้ (%)
50	1	80.00	1	80.00	0	100.00	0	100.00	0	100.00
100	4	69.23	4	69.23	0	100.00	0	100.00	0	100.00
150	5	64.29	5	64.29	3	78.57	2	85.71	0	100.00
200	7	56.25	6	62.50	5	68.75	4	75.00	1	93.75
250	7	69.57	7	69.57	5	78.26	3	86.96	2	91.30
300	12	66.67	6	83.33	4	88.89	2	94.44	0	100.00
350	16	48.39	11	64.52	6	80.65	5	83.87	1	96.77
400	11	73.81	9	78.57	3	92.86	3	92.86	3	92.86
450	11	78.00	11	78.00	7	86.00	7	86.00	2	96.00
500	10	77.27	7	84.09	4	90.91	4	90.91	3	93.18
550	15	71.15	10	80.77	5	90.38	3	94.23	1	98.08
600	15	71.15	14	73.08	11	78.85	6	88.46	3	94.23
650	14	74.07	10	81.48	7	87.04	5	90.74	2	96.30
700	22	64.51	18	70.97	8	87.10	5	91.94	2	96.77
750	23	68.06	20	72.22	12	83.33	9	87.50	3	95.83
800	19	73.24	16	77.46	9	87.32	7	90.14	2	97.18
850	24	70.73	23	71.95	13	84.15	8	90.24	5	93.90
900	26	72.92	21	78.13	13	86.46	12	87.50	7	92.70
950	20	74.68	18	77.22	12	84.81	11	86.08	6	92.40
1000	33	69.44	28	74.07	19	82.41	17	84.26	9	91.67



รูปที่ 5.3 เปรียบเทียบจำนวนการขัดแย้งระหว่าง Fact (Policy) และ Rule (User's Privacy Preferences) ใน Fact ที่ 2



รูปที่ 5.4 เปรียบเทียบเปอร์เซ็นต์การลด Negotiation process ของข้อมูลการทดลองชุดที่ 2

5.4 วิเคราะห์ผลการทดลอง

จากหัวข้อที่ผ่านมาเป็นผลของการทดลองการวัดประสิทธิภาพของระบบ DRM ที่เพิ่มความเป็นส่วนตัวเข้าไปในระบบ การทดลองได้กำหนด Policies (Facts) และสุ่มตัวอย่าง User's Privacy Preferences (Rules) และทำการวัดประสิทธิภาพการทำงานของอัลกอริทึมการเจรจาต่อรองความเป็นส่วนตัวที่ได้กล่าวถึงไปในหัวข้อ 3.6 ตามสมมุติฐานที่ว่า "ถ้านโยบายความเป็นส่วนตัวของระบบการจัดการสิทธิ์ดิจิตอลมี Conditional Statements ในการแก้ปัญหาความเป็นส่วนตัวแล้วจะทำให้ลดกระบวนการ Negotiation Process และเป็นการเพิ่มประสิทธิภาพของการเจรจาต่อรองความเป็นส่วนตัวแก่ระบบ DRM ด้วย" ที่ได้กล่าวถึงในหัวข้อ 5.1 นั่น ในหัวข้อนี้จะทำการวิเคราะห์ผลการทดลองที่ได้แสดงผลไปในหัวข้อข้างต้น โดยทำแบ่งการวิเคราะห์เป็นหัวข้อต่อไปนี้

1. จากชุดข้อมูลการทดลองที่ได้ทำการทดลองทั้ง 2 ชุด เมื่อทำการทดลองตามเงื่อนไข (ก) ในหัวข้อ 5.2.1 แสดงผลการทดลองในตารางที่ 5.5 และตารางที่ 5.8 สามารถนำมาเปรียบเทียบโดยแสดงในรูปของกราฟแท่ง ดังรูปที่ 5.1 และ 5.3 ซึ่งแสดงให้เห็นถึงการเปรียบเทียบจำนวนการขัดแย้งกันของ User's Privacy Preferences (Rules) จำนวนตั้งแต่ 50 ถึง 1000 ของการสุ่มตัวอย่างและ Policies (Facts) ใน Fact ที่ 1 และ Fact ที่ 2 ระหว่างกรณีที่ Fact มีการใช้เงื่อนไข Conditional Statements กับกรณีที่ Fact ไม่ได้ใช้เงื่อนไข Conditional Statements ใน สามารถวิเคราะห์ผลการทดลองจากกราฟจะสังเกตได้ว่า กราฟแท่งแทนกรณีที่ไม่ใช้ Conditional Statements นั้นมีค่าสูงกว่ากราฟแท่งแทนกรณีที่ใช้ Conditional Statements นั่นหมายความว่าจำนวนความขัดแย้งระหว่างนโยบายของระบบ กับการกำหนดความเป็นส่วนตัวของผู้ใช้ เกิดความขัดแย้งมากกว่ากรณีการกำหนดนโยบายโดยให้มีการใช้การกำหนดเงื่อนไข Conditional Statements หรือการใช้ If-then ในการแก้ปัญหาความขัดแย้งระหว่าง Policy และ User's Privacy Preferences นั่นเอง ดังนั้นจึงสามารถสรุปได้ว่า การใช้นโยบายความเป็นส่วนตัวที่ใช้เงื่อนไข Conditional Statements นั้นสามารถแก้ปัญหาความขัดแย้งกันระหว่าง Policy และ User's Privacy Preferences ได้ดีกว่าถ้านโยบายของระบบไม่มีการใช้ Conditional Statements

นอกจากนี้ในรูปที่ 5.1 และ รูปที่ 5.3 ได้แสดงกราฟเส้นแทนค่าเปอร์เซ็นต์การลดลงก่อนเข้าสู่กระบวนการ Negotiation Process โดยค่าเปอร์เซ็นต์ที่ได้นี้ มาจากการทำการเปรียบเทียบจากจำนวนเงื่อนไขที่ขัดแย้งในกรณีที่ไม่ใช้ Conditional Statements กับจำนวนเงื่อนไขที่ขัดแย้งในกรณีที่ใช้ Conditional Statements ตามสมการ (5.1) ดังนี้

$$\%D_N = \frac{Cf_n - Cf_u}{Cf_n} \times 100 \qquad (5.1)$$

กำหนดให้

$\%D_N$ คือค่าเปอร์เซ็นต์การลดลงก่อนเข้าสู่กระบวนการ Negotiation Process

Cf_n คือจำนวนเงื่อนไขที่เกิดความขัดแย้งกันระหว่าง Policies และ User's Privacy Preferences ในกรณีที่ไม่ใช้ Conditional Statements

Cf_u คือจำนวนเงื่อนไขที่เกิดความขัดแย้งกันระหว่าง Policies และ User's Privacy Preferences ในกรณีที่ใช้ Conditional Statements

จากสมการ (5.1) สามารถหาเปอร์เซ็นต์การลดลงก่อนผ่านเข้าสู่กระบวนการ Negotiation Process ซึ่งในกระบวนการ Rule Evaluation ที่ใช้เงื่อนไข Conditional Statements ในแก้ปัญหากรณีที่นโยบายของระบบและการกำหนดความเป็นส่วนตัวของผู้ใช้ขัดแย้งกันนั้น ทำให้สามารถลดกระบวนการ Negotiation Process โดยสามารถคำนวณประสิทธิภาพได้ตามสมการ (5.1) การนำเสนอข้อมูลทั้งในรูปตารางและกราฟทั้งนี้เพื่อให้ง่ายในการพิจารณาเปรียบเทียบความแตกต่างของนโยบายของระบบที่ไม่ใช้เงื่อนไข Conditional Statements และเงื่อนไขที่ไม่ใช้ Conditional Statements ซึ่งจะพบว่าปริมาณ Rules ที่เพิ่มขึ้นเมื่อผ่านกระบวนการ Rule Evaluation กรณีที่ไม่ใช้ Conditional Statements ก็ยิ่งทำให้เกิดความขัดแย้งของนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้เพิ่มขึ้น ทำให้ต้องผ่านเข้าสู่กระบวนการ Negotiation Process เพิ่มขึ้น ซึ่งนั่นหมายถึงว่าระบบจำเป็นที่จะต้องแก้ปัญหาและเลือก Rules ที่เหมาะสมที่สุดที่ยินยอมให้ผู้ใช้สามารถเข้าใช้เนื้อหา (contents) ในระบบการจัดการสิทธิ์ดิจิตอล ดังนั้นการที่ระบบใช้เงื่อนไข Conditional Statements ในนโยบายของระบบแล้วนั้นจะทำให้ประสิทธิภาพของการเจรจาต่อรองความเป็นส่วนตัวของระบบ DRM ดีขึ้นนั่นเอง

2. จากชุดข้อมูลการทดลองทั้ง 2 ชุด เมื่อทำการทดลองตามเงื่อนไข (ข) ในหัวข้อ 5.2.1 เมื่อทำการเพิ่มจำนวนเงื่อนไข Conditional Statements ไปทีละเงื่อนไขในชุดข้อมูลการทดลองทั้ง 1 และ 2 ผลการทดลองแสดงในตารางที่ 5.6 และตารางที่ 5.9 จากตารางจะเห็นว่าจำนวนความขัดแย้งของ User's Privacy Preferences (Rules) จำนวนตั้งแต่ 50 ถึง 1000 ของการสุ่มตัวอย่าง และ Policies (Facts) ใน Fact ที่ 1-1, 1-2, 1-3, 1-4, 1-5 ในชุดข้อมูลชุดที่ 1 และ Fact ที่ 2-1, 2-2, 2-3, 2-4, 2-5 ในชุดที่ 2 มีค่าลดลงแปรผันตามจำนวน Conditional Statements ที่ทำการเพิ่มขึ้น และผลการทดลองในส่วนของการหาค่าเปอร์เซ็นต์การลดลงก่อนเข้าสู่กระบวนการ Negotiation Process ในตารางที่ 5.6 และ ตารางที่ 5.9 นั้น สามารถแสดงผลในรูปของกราฟเส้นดังรูปที่ 5.2 และรูปที่ 5.4 ตามลำดับ และทำการวิเคราะห์ผลการทดลองโดยทำการหาค่าเปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process แสดงในตารางที่ 510

ตารางที่ 5.10 เปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process

ชุดข้อมูลการทดลอง	Fact ที่	% เฉลี่ย
1	1	19.70%
	1-1	33.11%
	1-2	61.36%
	1-3	65.46%
	1-4	74.25%
	1-5	86.48%
2	2	48.29%
	2-1	69.67%
	2-2	74.57%
	2-3	85.84%
	2-4	89.34%
	2-5	95.65%

จากตารางที่ 5.10 ในการหาค่าเปอร์เซ็นต์เฉลี่ยของการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process นั้นสามารถหาค่าได้จากสมการ (5.2)

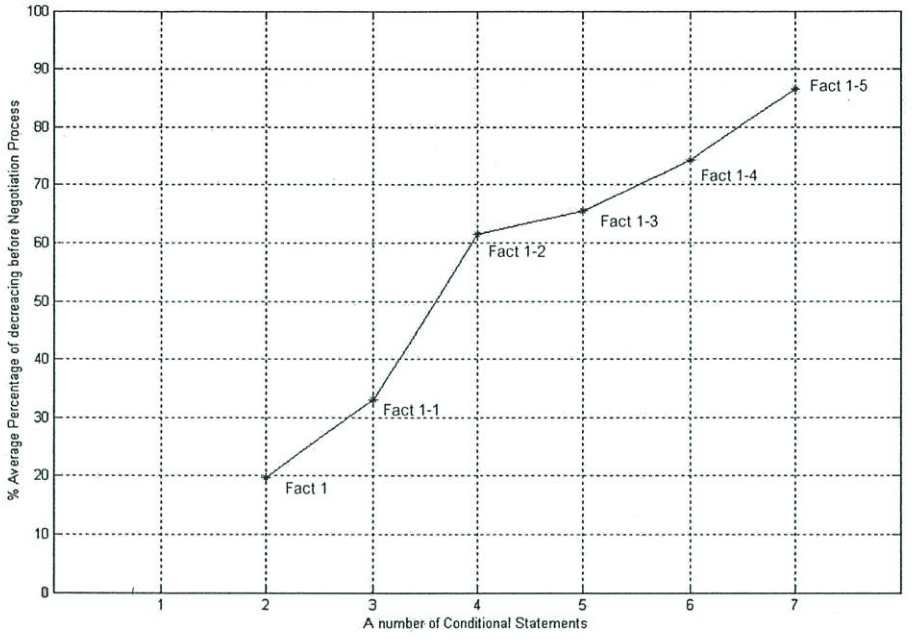
$$\text{ค่าเฉลี่ย } \%D_N = \frac{\sum_{i=1}^{n} \%D_N}{n} \quad (5.2)$$

กำหนดให้

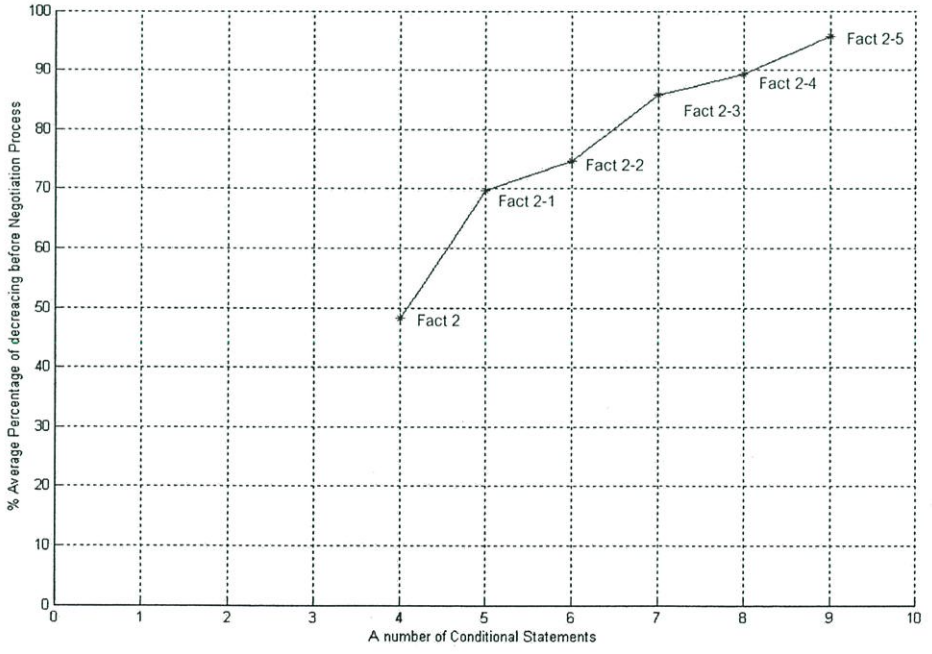
$\%D_N$ คือค่าเปอร์เซ็นต์การลดลงก่อนเข้าสู่กระบวนการ Negotiation Process

n คือจำนวนครั้งของกฎที่ใช้ในการทดลองมีค่าเท่ากับ 20

จากสมการ (5.2) นี้สามารถอธิบายความสัมพันธ์ระหว่างการกำหนด Facts ในชุดข้อมูลการทดลองทั้ง 2 ชุด กับผลลัพธ์ค่าเปอร์เซ็นต์เฉลี่ยที่คำนวณได้ นั่นคือเมื่อพิจารณาจากตารางที่ 5.10 สามารถแสดงความสัมพันธ์ระหว่างจำนวน Conditional Statements ในชุดข้อมูลที่ 1 และ ชุดข้อมูลชุดที่ 2 กับเปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process ได้ในรูปแบบของกราฟเส้นได้ดังรูปที่ 5.5 และ รูปที่ 5.6 ตามลำดับ



รูปที่ 5.5 ความสัมพันธ์ระหว่างจำนวน Conditional Statements กับเปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process ในชุดข้อมูลที่ 1



รูปที่ 5.6 ความสัมพันธ์ระหว่างจำนวน Conditional Statements กับเปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่ กระบวนการ Negotiation Process ในชุดข้อมูลที่ 2

จากรูปที่ 5.5 และ รูปที่ 5.6 นั้น แสดงกราฟความสัมพันธ์ระหว่างจำนวน Conditional Statement ที่ได้ทำการทดลองการเพิ่มทีละ 1 Conditional Statement ในเงื่อนไขการทดลอง (ข) กับเปอร์เซ็นต์เฉลี่ยของการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process โดยจะสังเกตได้ว่าเปอร์เซ็นต์เฉลี่ยการลดลงก่อนเข้าสู่กระบวนการ Negotiation Process มีค่าเพิ่มขึ้นแบบแปรผันตรงใน Fact ที่ทำการเพิ่ม Conditional Statements ไปทีละเงื่อนไข ซึ่งมีค่าเพิ่มขึ้นเช่นเดียวกันในชุดข้อมูลการทดลองทั้ง 2 ชุด ทำให้วิเคราะห์ได้ว่ายิ่งเพิ่มเงื่อนไข Conditional Statements ให้มากขึ้นจะเป็นการเพิ่มประสิทธิภาพในการแก้ปัญหาการขัดแย้งกันระหว่าง DRM privacy policy และ User's Privacy Preferences ของระบบมากขึ้นด้วยเช่นกัน

สำหรับการทดสอบประสิทธิภาพของอัลกอริทึมตามสมมุติฐานนั้น จากที่ทำการทดสอบไปแล้วนั้น เป็นการทดสอบเพื่อเปรียบเทียบการกำหนดนโยบายความเป็นส่วนตัวกรณีที่ใช้ Conditional Statements ในการแก้ปัญหาความขัดแย้งระหว่างนโยบายของระบบและการกำหนดความเป็นส่วนตัวของผู้ใช้ กับกรณีที่นโยบายของระบบไม่ได้ใช้เงื่อนไข Conditional Statements สามารถกล่าวได้ว่าการกำหนดนโยบายของระบบโดยใช้เงื่อนไข Conditional Statements นั้นทำให้ระบบ DRM สามารถแก้ปัญหาความขัดแย้งที่เกิดขึ้นระหว่างผู้ใช้และนโยบายของระบบได้ และทำให้ระบบมีประสิทธิภาพในการทำงานเพิ่มขึ้น เนื่องจากลดขั้นตอนในกระบวนการ Negotiation Process และยังสังเกตได้ว่ายิ่งเพิ่มเงื่อนไข Conditional Statements ให้มากขึ้นจะเป็นการเพิ่มประสิทธิภาพในการแก้ปัญหาของระบบมากขึ้นด้วยเช่นกัน พิจารณาได้จากการทดลองตามเงื่อนไขทั้ง 2 เงื่อนไข ที่ได้ทำการทดลองไปแล้วในขั้นต้น ซึ่งจะกล่าวสรุปในบทที่ 6 ต่อไป

บทที่ 6
สรุปผลการวิจัยและข้อเสนอแนะ

ในบทนี้จะกล่าวถึงผลสรุปที่ได้จากการทำวิทยานิพนธ์ และปัญหาที่เกิดขึ้นระหว่างการทำวิทยานิพนธ์ครั้งนี้ รวมทั้งข้อเสนอแนะสำหรับผู้ที่สนใจศึกษาในการทำวิทยานิพนธ์เรื่องนี้ เพื่อใช้เป็นแนวทางในการพัฒนาหรือศึกษาต่อไป

6.1 สรุปผลการวิจัย

งานวิจัยนี้เป็นการเพิ่มความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล โดยอาศัยแนวคิดในการออกแบบนโยบายของระบบ (DRM Policy) และออกแบบการกำหนดความเป็นส่วนตัวของผู้ใช้ (User's privacy preferences) ให้มีความเหมาะสมและยืดหยุ่นสำหรับระบบการจัดการสิทธิ์ดิจิตอล (DRM) โดยในงานวิจัยแบ่งออกเป็น 3 ส่วน ส่วนแรกเป็นการออกแบบความเป็นส่วนตัวของผู้ใช้ ซึ่งผู้ใช้สามารถกำหนดความเป็นส่วนตัวของตัวเอง โดยมีโครงสร้างของการกำหนดความเป็นส่วนตัวแบ่งออกเป็น 3 ระดับ คือ Free Limited และ NotGiven ซึ่งในแต่ละระดับมีความสำคัญที่แตกต่างกัน ขึ้นอยู่กับผู้ใช้จะเป็นผู้กำหนดลำดับความสำคัญของข้อมูลลงในแต่ละเงื่อนไข ซึ่งจะใช้ไวยากรณ์ที่ทำความเข้าใจได้ง่าย และง่ายในการเขียน การที่ผู้ใช้สามารถกำหนดความเป็นส่วนตัวของตัวเอง ทำให้ผู้ใช้สามารถป้องกันมิให้ระบบขอข้อมูลที่ผู้ใช้ไม่ยินยอมได้ ในส่วนที่สองเป็นการกำหนดนโยบาย (policy) ของระบบ DRM โดยได้ทำการออกแบบให้อยู่ในรูปแบบแบบมาตรฐาน ซึ่งแบ่งการออกแบบเป็นสองส่วน คือ Mandatory และ Optional ในส่วนของ Mandatory จะเป็นส่วนที่ระบบทำการระบุข้อมูลที่ระบบจำเป็นจะต้องร้องขอการใช้ข้อมูลของผู้ใช้ และในส่วนของ Optional เป็นข้อมูลส่วนเพิ่มเติมที่ระบบทำการร้องขอซึ่งอาจจะเป็นข้อมูลที่สำคัญรองลงมา โดยการกำหนดความเป็นส่วนตัวของผู้ใช้จะถูกประมวลผลเปรียบเทียบกับนโยบายของระบบ DRM โดยผ่านทาง agent และในส่วนสุดท้ายที่ได้กล่าวถึงในงานวิจัยนี้เป็นการสร้าง DRM privacy agent และทำการออกแบบกระบวนการ Negotiation Mechanism โดย DRM privacy agent จะทำหน้าที่ในการนำนโยบายของระบบและการกำหนดความเป็นส่วนตัวของผู้ใช้ทำการเปรียบเทียบกัน โดยในขั้นตอน Negotiation Mechanism จะเป็นกระบวนการที่ช่วยให้ระบบที่ทำการร้องขอข้อมูลของผู้ใช้ สามารถผ่านเงื่อนไขของผู้ใช้ โดยใช้กระบวนการ Rule Evaluation เพื่อหาตัวแทนของข้อมูล ซึ่งได้กำหนดอยู่ในเงื่อนไข Mandatory ในนโยบายของระบบ DRM เพื่อให้ได้ข้อมูลที่เข้ากันได้กับการกำหนดความเป็นส่วนตัวของผู้ใช้ แต่ในกรณีที่เงื่อนไขของผู้ใช้และระบบเกิดความขัดแย้งขึ้นระบบก็จะใช้กระบวนการ Negotiation Process เพื่อที่หากฎของผู้ใช้ที่เหมาะสมกับระบบดีที่สุด เพื่อระบบจะใช้กฎนี้ในการตัดสินใจปรับนโยบายของตนเอง โดยระบบ

สามารถกำหนดน้ำหนัก (weight) เพื่อเป็นตัวช่วยในหาการหากฎที่เหมาะสมที่สุด จากการทดลองและทดสอบประสิทธิภาพนั้นทำให้สามารถสรุปได้ว่าการกำหนดนโยบายและการกำหนดความเป็นส่วนตัวของผู้ใช้ในระบบ DRM อย่างเหมาะสมจะทำให้ประสิทธิภาพของการทำงานในระบบ DRM เพิ่มขึ้น

6.2 ปัญหา

ปัญหาที่พบในงานวิจัยคือ

- กระบวนการทำงานที่ซับซ้อนขึ้น อาจทำให้ระยะเวลาในการประมวลผลการทำงานของ DRM privacy agent เพิ่มขึ้น จึงต้องออกแบบ agent ให้รองรับกระบวนการทำงานที่ซับซ้อนเหล่านี้
- การกำหนด Weight ของระบบในกระบวนการ Negotiation process ไม่ควรให้ระยะห่างของค่า Weight แต่ละค่ามากเกินไป เพราะผลลัพธ์ที่ได้จะไม่ดีเท่าที่ควร
- การกำหนดความเป็นส่วนตัวของผู้ใช้ที่จำกัดจนเกินไป เมื่อทำการประมวลผลจะทำให้เกิดความขัดแย้งกับระบบ ซึ่งทำให้ระบบ และผู้ใช้เองสูญเสียโอกาส ดังนั้นควรมีการวิจัยการเพิ่มความเป็นส่วนตัวของผู้ใช้ว่าควรอยู่ในระดับไหน โดยทั้งผู้ใช้และระบบมีความพึงพอใจทั้ง 2 ฝ่าย
- การกำหนดประเภทของข้อมูลควรใช้เป็นมาตรฐานเดียวกันเพื่อในการประมวลผลของ DRM privacy agent จะได้ทำงานอย่างถูกต้อง

6.3 ข้อเสนอแนะ

ในการทำงานวิจัยความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลต่อไปในอนาคต ผู้วิจัยได้เสนอแนวความคิดเห็นต่างๆ เพื่อเป็นประโยชนต่อการทำงานวิจัยด้านนี้ต่อไปในอนาคต

1. ควรมีการเพิ่มความสามรถของ DRM privacy agent โดยเพิ่มความสามารถซึ่งอาจจะใช้ความรู้ทางด้านปัญญาประดิษฐ์ หรือการใช้ฐานข้อมูลมาประกอบการตัดสินใจให้กับผู้ใช้
2. ควรมีการเพิ่มความปลอดภัยเข้าไปในตัว DRM privacy agent และให้ agent สามารถทำงานได้โดยไม่ยึดติดกับระบบและรูปแบบของภาษา
3. ตัว DRM privacy agent ที่ดีควรมีความฉลาดสามารถนำเสนอเงื่อนไขที่ทั้งระบบและผู้ใช้ยอมรับ โดยสามารถนำเอาทั้งการกำหนดความเป็นส่วนตัวของผู้ใช้และนโยบายของระบบมาประมวลผล และหาทางเลือกที่ดีที่สุดให้กับระบบ DRM และผู้ใช้

4. การเพิ่ม Privacy Rule ลงไปเพื่อเป็นข้อผูกพันที่ผู้ใช้ได้ทำกับระบบ เมื่อการเปรียบเทียบระหว่าง นโยบายของผู้ใช้กับนโยบายของระบบไม่มีข้อขัดแย้งกัน การสร้าง Privacy Rule จะเป็นการสร้างสัญญาระหว่างระบบกับผู้ใช้ ในการนำข้อมูลไปใช้
5. การวิจัยครั้งนี้เป็นการวิจัยในขั้นตอนที่ให้ผู้ใช้ตัดสินใจว่าจะให้ข้อมูลอะไรแก่ระบบ แต่ยังขาดกระบวนการตรวจสอบระบบว่าระบบได้นำข้อมูลไปใช้ตามเงื่อนไขที่กำหนดหรือไม่

เอกสารอ้างอิง

[1] Iannella, R. **"Digital Rights Management (DRM) Architectures."** [Online]. Available : http://www.dlib.org/dlib/june01/iannella/06iannella.html. 2001.

[2] Agrawal, S. **"Investigation of Third Party Rights Service and Shibboleth Modification to Introduce the Service."** pp. 3-6. [Online]. Available : http://www.cs.dartmouth.edu/~sws/theses/sanket.pdf. 2003.

[3] Feigenbaum, J.,Freedman, M., Sander, T., Shostack, A. "Privacy Engineering for Digital Rights Management Systems." **the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management**. 2002. pp. 76-105.

[4] **"Office of Privacy Protection."** [Online]. Available : http://www.privacy.ca.gov /code/fairinfo.htm. 2002.

[5] Warren, S. and Brandeis L. **The Right to Privacy.** Harvard Law Review. pp. 1980. 193-220.

[6] British House of Commons, Committee on Privacy and Related Matters. **Report of the Committee on Privacy and Related Matters**. Cm1102. 1990.

[7] Korba L. "Privacy in Distributed Electronic Commerce." **Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS)**. 7-10 January 2002. pp. 4017 – 4026.

[8] Korba, L. and Kenny, S. "Towards Meeting the Privacy Challenge: Adapting DRM". **ACM Workshop on Digital Rights Management.** 18 November 2002.

[9] Zuidweg, M. **"P3P-based Privacy architecture for a context-aware service platform."** [Online]. Available : http://arch.cs.utwente.nl/assignments/thesis/ARCH-2003-07.pdf. 2003.

[10] W3C. **"Platform for Privacy Preferences."** [Online]. Available : http://www.w3c.org /p3p. 2002.

[11] W3C. **"The Platform for Privacy Preferences 1.0 (P3P1.0) Specification."** [Online]. Available : http://www.w3.org/TR/P3P/. 2002.

[12] W3C. **"A P3P Preference Exchange Language (APPEL)."** [Online]. Available : http://www.w3.org/TR/P3P-preferences.html. 2002.

[13] Lategan, F.A. and Olivier. "A Chinese Wall Approach to Privacy Policies for the

Web." **Proceeding of the 26th International Annual Conference on Computer Software and Applications Conference (COMPSAC 2002).** 26-29 Aug. 2002. pp. 940 – 944.

[14] Agrawal, R., Kiernan, J., Ramakrishnan and Srikant Yirong Xu. 2003. "Implementing P3P using database technology." **Proceeding of the 19th International Conference on Data Engineering.** 5-8 March 2003. pp. 595 – 606.

[15] Rosenblatt, **Digital Rights Management Business and Technology**. First Edition. New York : Hungry Minds Inc. 2002.

[16] Park, J. and Sandhu, R. "Towards Usage Control Models: Beyond Traditional Access Control." **In ACM symposium on Access Control Models and Technologies.** June 2002. pp. 57-64.

[17] Schmalz, D., Lenoir, P. and Jonker, W. **"Description of Current DRM Techniques and Solutions."** [Online]. Available : http://www.rge.brabantbreedband.nl /docs / RGE_D5_1.pdf. 2002.

[18] Microsoft. **"Architecture Microsoft Media Rights Manager."** [Online]. Available : http:// www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx. 2002.

[19] EMMS. **"Electronic Media Management System."** [Online]. Available : http://www.ibm.com/software/emms. 2001.

[20] InterTrust. [Online]. Available : http://www.intertrust.com. 2000.

[21] RMCS. **"Real Systems Media Commerce Suite."** [Online]. Available : http://docs.real.com/docs/drm/DRM_ WP1.pdf. 2001.

[22] Vora, P., Reynolds, D., Dickinson, I., Erickson, J., Banks and D.P. Vora, D. **"Privacy and Digital Rights Management."** the W3C Workshop on Digital Rights Management for the Web. [Online]. Available : http://www.w3.org/2000/12/ drm-ws/pp/hp-poorvi.html. 2001.

[23] AuctionBot. [Online]. Available : http://auction.eecs.umich.edu/

[24] Kasbah. [Online]. Available : http://ecommerce.media.mit.edu/Kasbah/

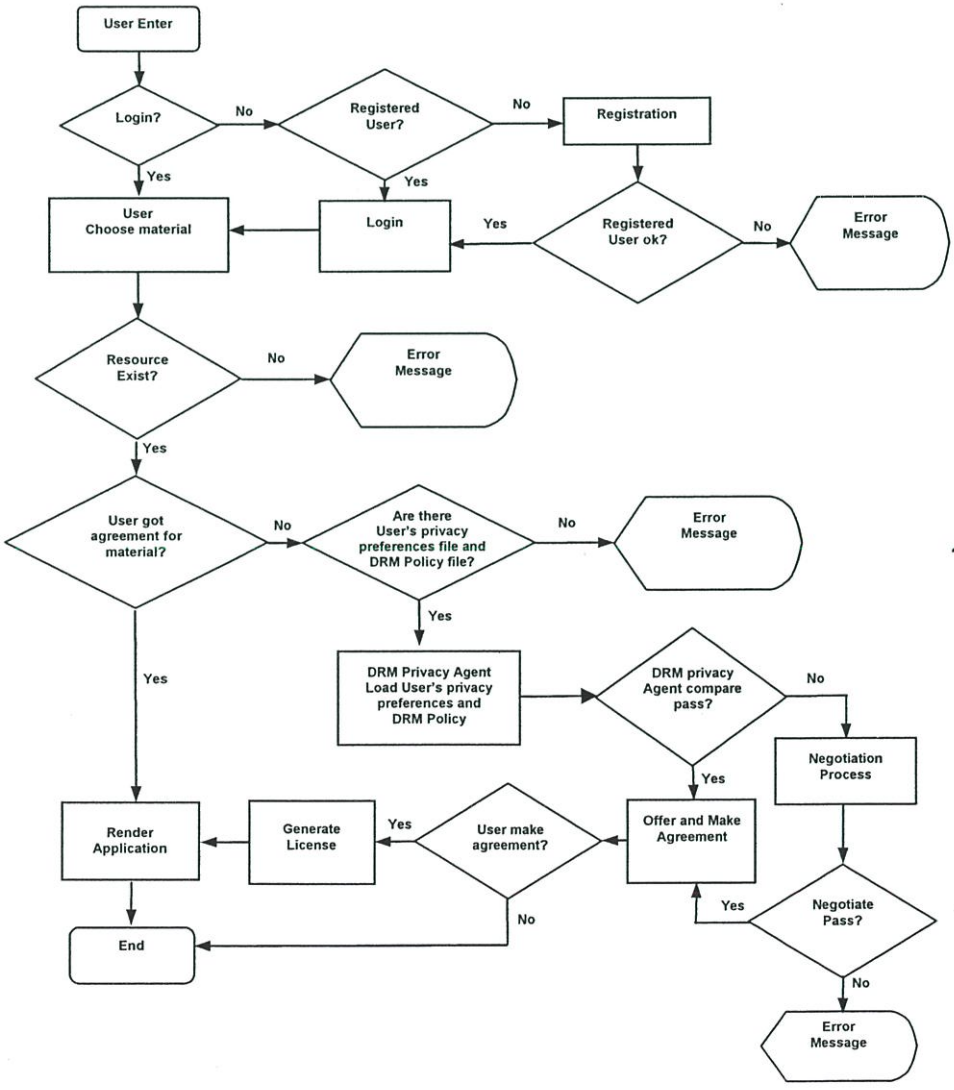
ภาคผนวก ก.

ระบบต้นแบบความเป็นส่วนตัว
สำหรับระบบการจัดการสิทธิ์ดิจิตอล

ภาคผนวก ก.

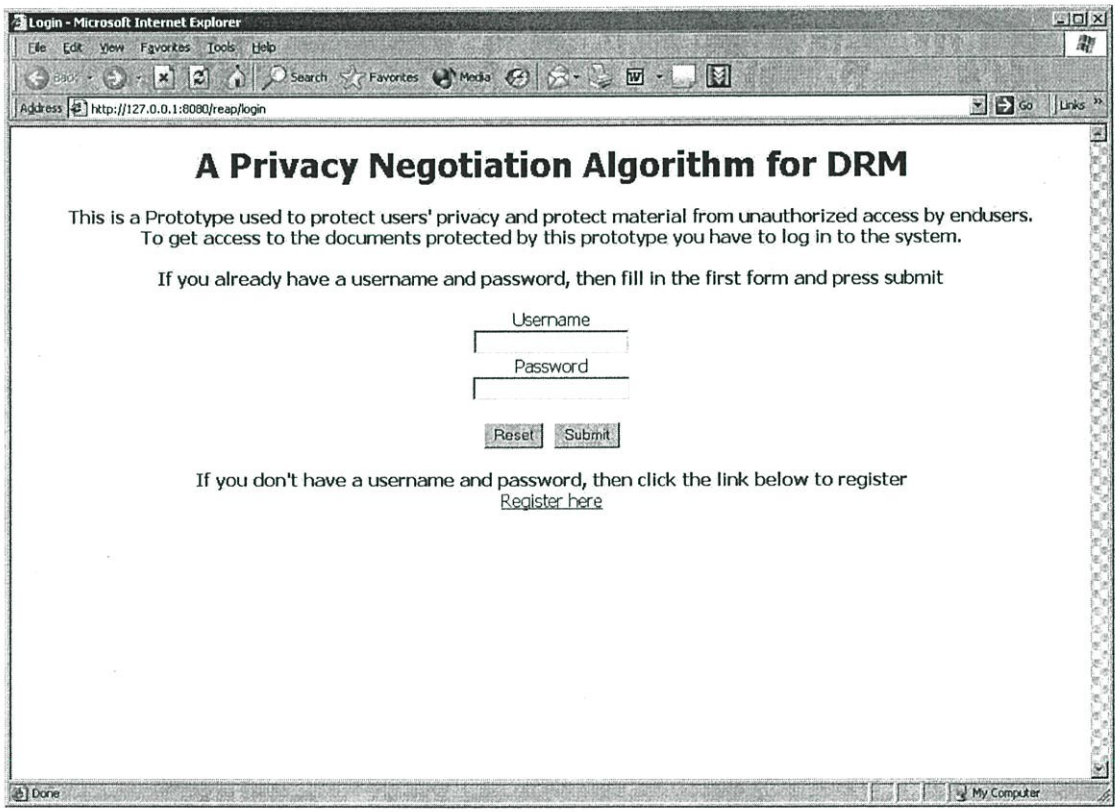
ระบบต้นแบบความเป็นส่วนตัว สำหรับระบบการจัดการสิทธิ์ดิจิตอล

สำหรับระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอลที่ทำการพัฒนาขึ้นมานั้น พัฒนาตามโครงสร้างที่ทำการศึกษาและการออกแบบซึ่งได้กล่าวถึงในบทที่ 3 อย่างละเอียด ในภาคผนวก ก.จะทำการอธิบายโครงสร้างการทำงานของระบบต้นแบบ และการใช้งานระบบต้นแบบที่ได้ทำการพัฒนาขึ้น โดยระบบต้นแบบที่พัฒนาขึ้นนี้ เพื่อให้ผู้ที่สนใจและต้องการนำงานวิจัยนี้ไปพัฒนาต่อสามารถทำความเข้าใจและเรียนรู้การทำงานได้อย่างสะดวกรวดเร็ว



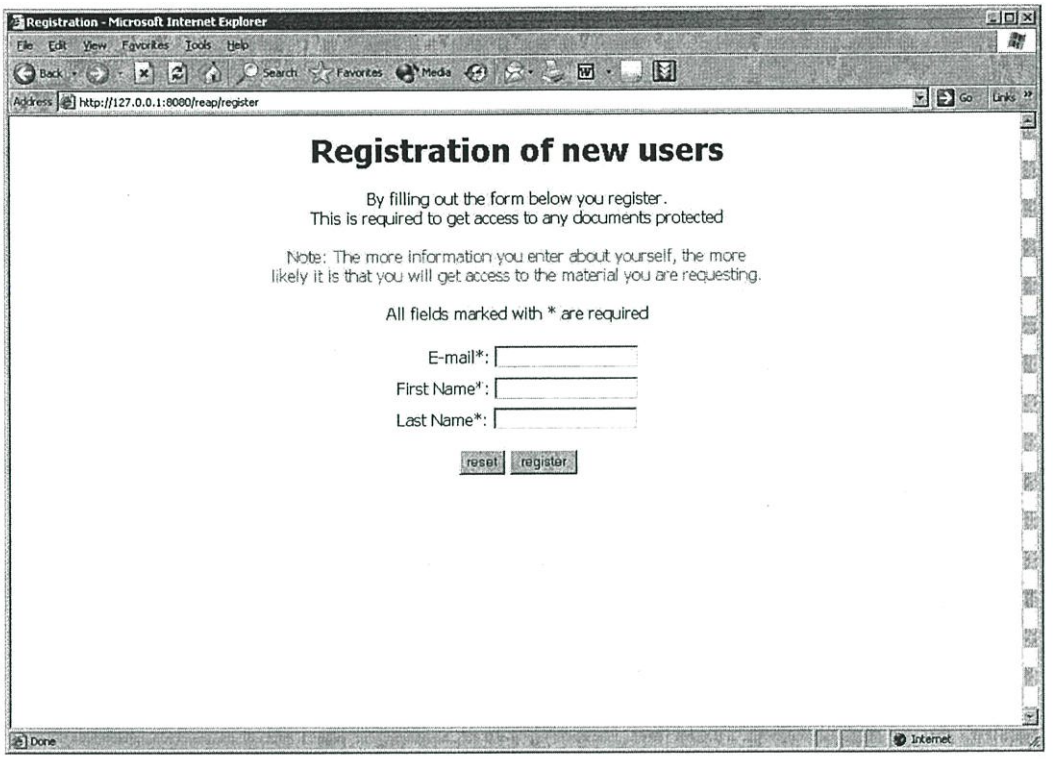
รูปที่ ก.1 แผนผังการทำงานของระบบต้นแบบความเป็นส่วนตัวสำหรับระบบการจัดการสิทธิ์ดิจิตอล

สำหรับระบบต้นแบบที่ได้พัฒนาขึ้นจะมีโครงสร้างตามระบบ DRM ใน DRM Reference Architecture [15] โดยการจำลองระบบเพื่อใช้งานในเนื้อหาดิจิตอล ในระบบต้นแบบนี้ทำการเพิ่มความเป็นส่วนตัวเข้าไปในระบบการจัดการสิทธิ์ดิจิตอล โดยผู้ใช้จำเป็นต้องมีการกำหนดความเป็นส่วนตัวของตนเองตามรูปแบบโครงสร้างภาษา XML หรือ XML Schema และเนื้อหาดิจิตอลในระบบ DRM จำเป็นจะต้องมีการกำหนดนโยบายของตนเองตามรูปแบบโครงสร้างภาษา XML เช่นกัน ซึ่งได้อธิบายรูปแบบภาษาไว้ในภาคผนวก ข. การใช้งานระบบต้นแบบที่พัฒนาขึ้นนี้ แสดงดังรูปต่อไปนี้

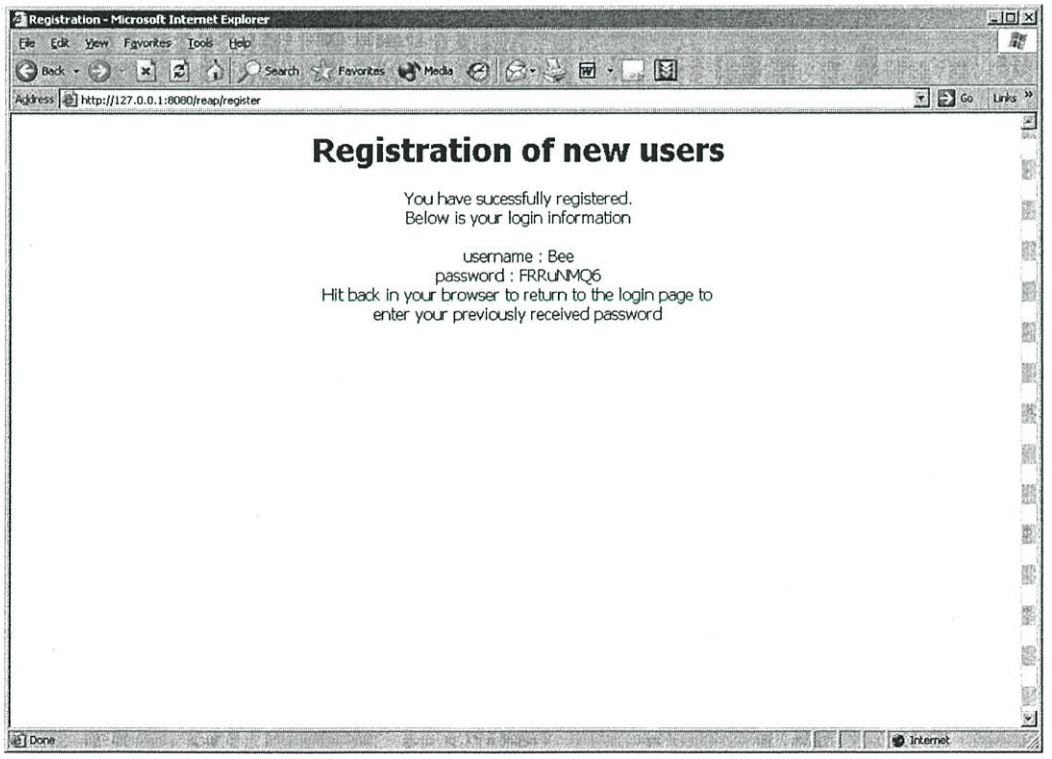


รูปที่ ก.2 หน้าจอแรกเมื่อผู้ใช้เข้าสู่ระบบการจัดการสิทธิ์ดิจิตอล

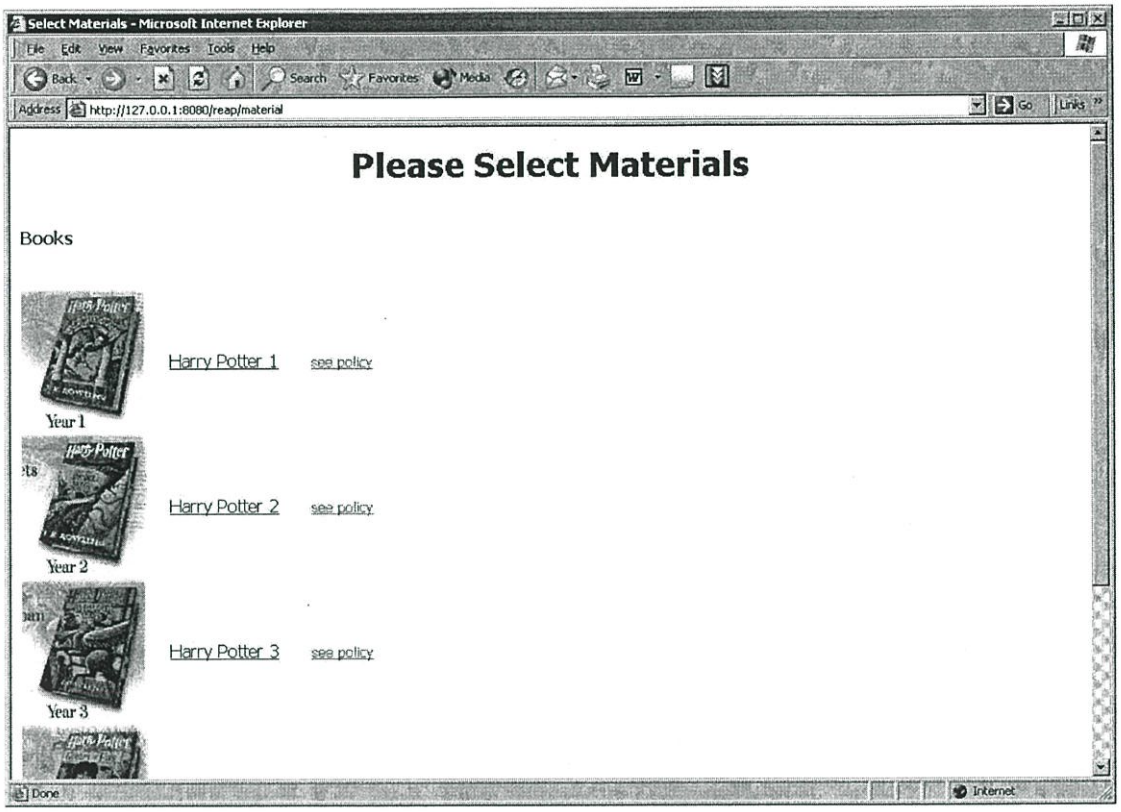
จากรูปที่ ก.2 เมื่อผู้ใช้เข้าสู่ระบบการจัดการสิทธิ์ดิจิตอลเริ่มต้น ผู้ใช้จำเป็นต้องใส่ Username และ Password เพื่อเข้าสู่ระบบ หากผู้ใช้มี Username และ Password อยู่แล้วผู้ใช้สามารถ login เข้าสู่ระบบเพื่อไปยังขั้นตอนต่อไปได้ แต่ถ้าเป็นผู้ใช้ใหม่จำเป็นจะต้องทำการ register ก่อน แสดงดังรูปที่ ก.3 โดยให้ผู้ใช้กรอก E-mail, ชื่อ, นามสกุล เพื่อระบบจะสร้าง Username และ Password ให้แก่ผู้ใช้ในการ Login เข้าสู่ระบบ หลังจากที่ผู้ใช้ใหม่ทำการ register แล้ว ระบบจะทำการสร้าง Username และ Password และแจ้งให้ผู้ใช้ได้ทราบ แสดงดังรูปที่ ก.4



รูปที่ ก.3 เมื่อผู้ใช้ต้องการลงทะเบียนเป็นสมาชิกในระบบ

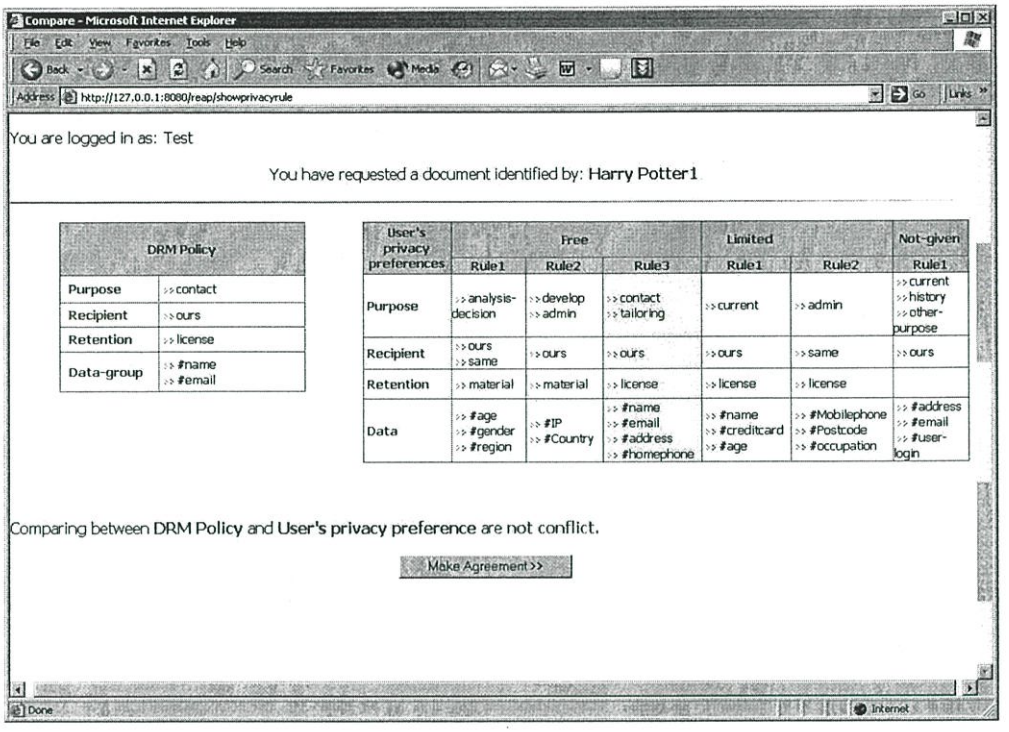


รูปที่ ก.4 ข้อมูลชื่อของผู้ใช้และรหัสผ่านที่ผู้ใช้จำเป็นต้องติดต่อกับระบบ

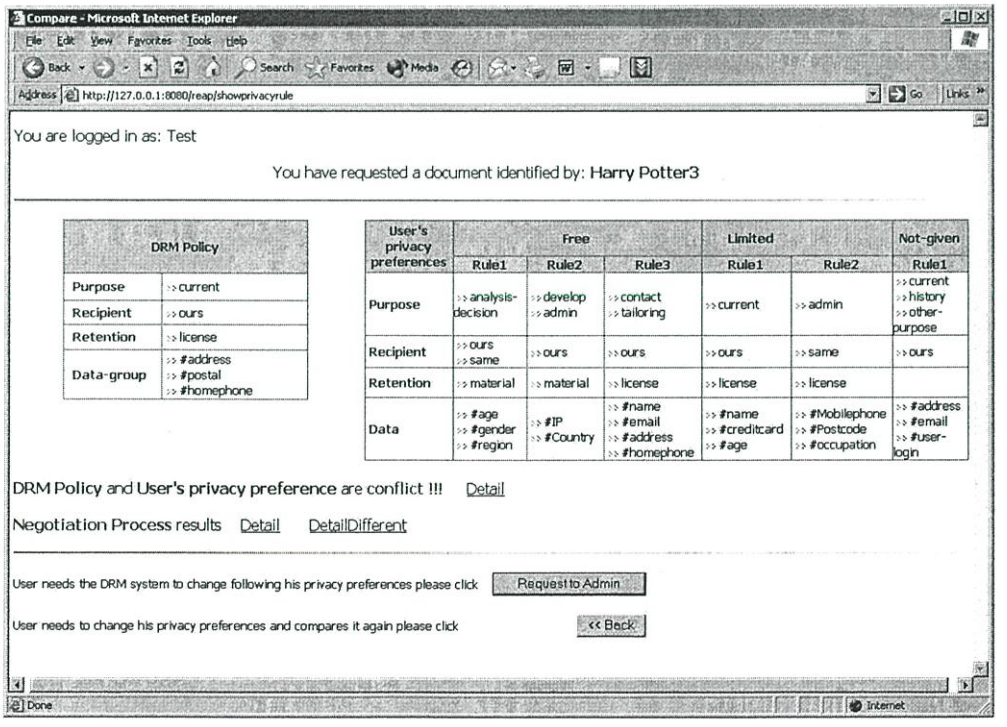


รูปที่ ก.5 เนื้อหาและนโยบายของเนื้อหาทั้งหมดที่ระบบให้บริการเพื่อให้ผู้ใช้เลือกเพื่อทำข้อตกลงการใช้เนื้อหาต่อไป

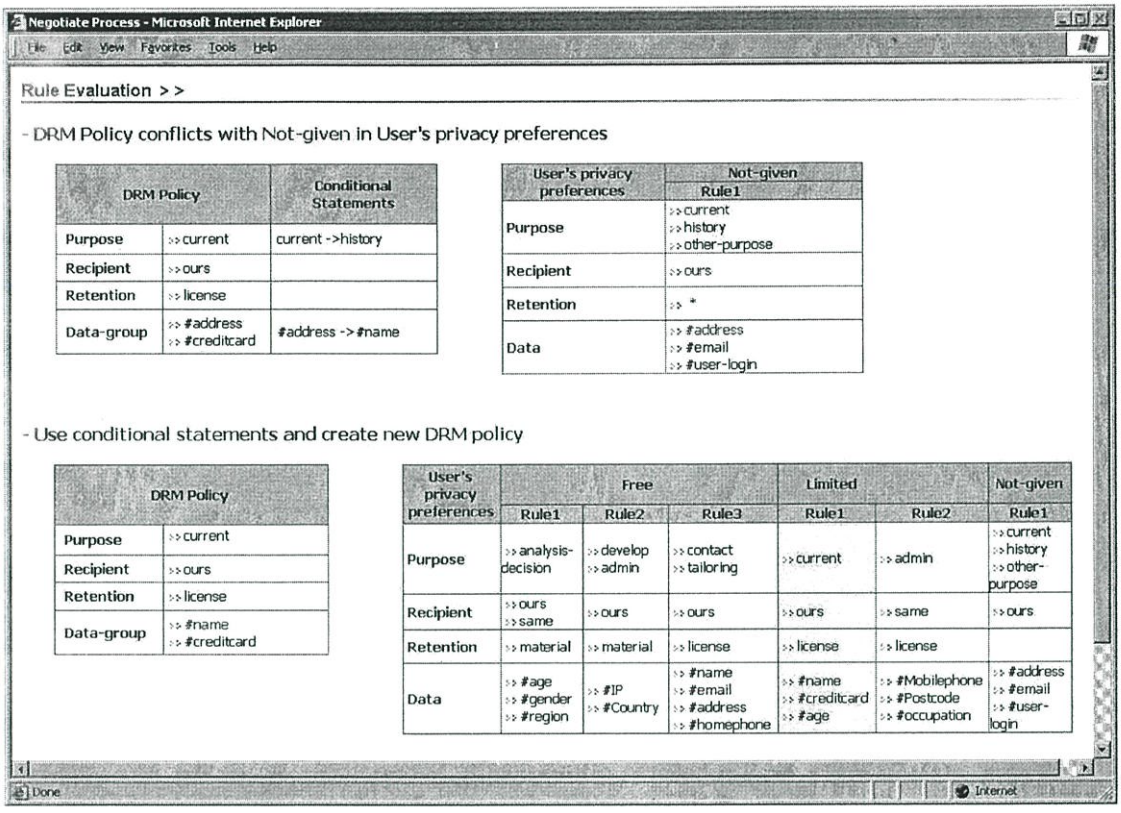
จากรูปที่ ก.5 หลังจากที่ผู้ใช้ Login เข้าสู่ระบบการจัดการสิทธิ์ดิจิตอลได้เรียบร้อยแล้ว ระบบจะแสดงเนื้อหาดิจิตอลที่ระบบจัดเตรียมไว้ให้ผู้ใช้ โดยผู้ใช้จะทำการเลือกเนื้อหาดิจิตอลเหล่านั้นตามที่ผู้ใช้ต้องการ เมื่อผู้ใช้เลือกเนื้อหาดิจิตอลแล้ว ระบบจะนำเอานโยบายความเป็นส่วนตัวของผู้ใช้และนโยบายของเนื้อหาดิจิตอลตามที่เจ้าของเนื้อหาได้กำหนดไว้นั้น มาทำการเปรียบเทียบกัน ซึ่งหากนโยบายของผู้ใช้และนโยบายของเนื้อหาดิจิตอล ไม่ขัดแย้งกันระบบแสดงข้อความให้ผู้ใช้รับทราบ ดังรูปที่ ก.6 แต่หากนโยบายของผู้ใช้และนโยบายของเนื้อหาดิจิตอลขัดแย้งกันระบบจะต้องผ่านกระบวน Negotiate mechanism โดยแจ้งบอกให้ผู้ใช้ทราบแสดงดังรูปที่ ก.7 โดยระบบจะแสดงนโยบายของระบบและกฎทางเลือกที่เป็นไปได้ที่ระบบสามารถปรับให้ผู้ใช้สามารถเข้ามาใช้งานเนื้อหาดิจิตอลในระบบได้



รูปที่ ก.6 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM policy และ User's Privacy Preferences และไม่เกิดความขัดแย้ง

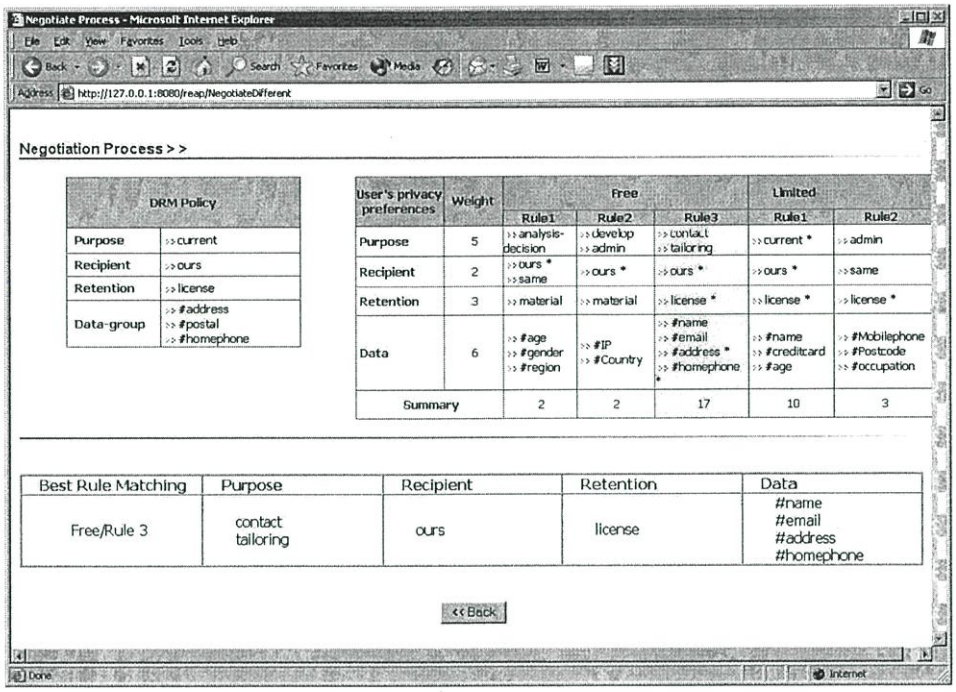


รูปที่ ก.7 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM policy และ User's Privacy Preferences และเกิดความขัดแย้งขึ้น

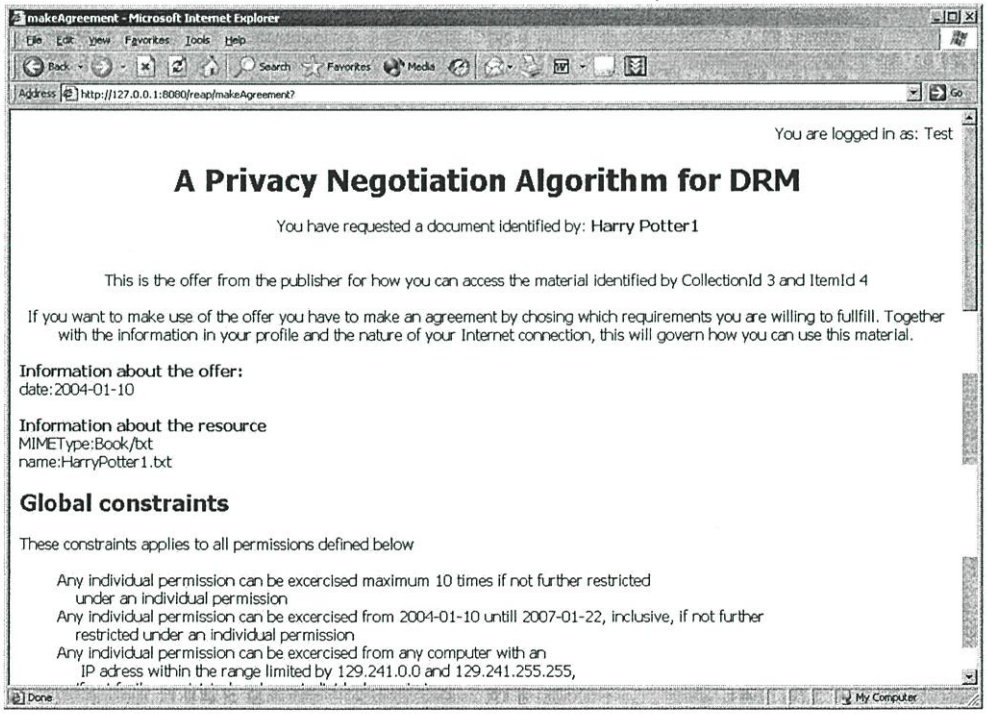


รูปที่ ก.8 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM policy และ User's Privacy Preferences กรณีที่ระบบใช้ Conditional Statements ในการแก้ปัญหาความขัดแย้งในกระบวนการ Rule Evaluation

จากรูปที่ ก.8 ระบบจะทำการเปรียบเทียบนโยบายความเป็นส่วนตัวของผู้ใช้และนโยบายของระบบ ซึ่งจากรูปจะเห็นได้ว่าระบบจะต้องปรับเปลี่ยนนโยบายของระบบเพื่อให้สอดคล้องกับการกำหนดความเป็นส่วนตัวของผู้ใช้ เห็นได้จากตารางแสดง New Policy ซึ่งระบบทำการปรับนโยบายและนำนโยบายใหม่ไปเปรียบเทียบอีกครั้งหนึ่ง และระบบสามารถแก้ปัญหาความขัดแย้งได้ สำหรับในรูปที่ ก.9 ระบบจะทำการหากฎที่เหมาะสมที่สุดก็ต่อเมื่อระบบได้ทำการปรับนโยบายของเนื้อหาดิจิตอลในระบบแล้ว และนำนโยบายที่ปรับแล้ว ไปเปรียบเทียบอีกครั้งหากยังมีการขัดแย้งเกิดขึ้นอีก ระบบก็จะทำการหากฎที่เหมาะสมที่สุด โดยการกำหนดค่า Weights ให้กับเงื่อนไข และคำนวณหาค่าที่มากที่สุด ในการสรรหากฎที่เหมาะสมที่สุดให้แก่ผู้ใช้งานในระบบ

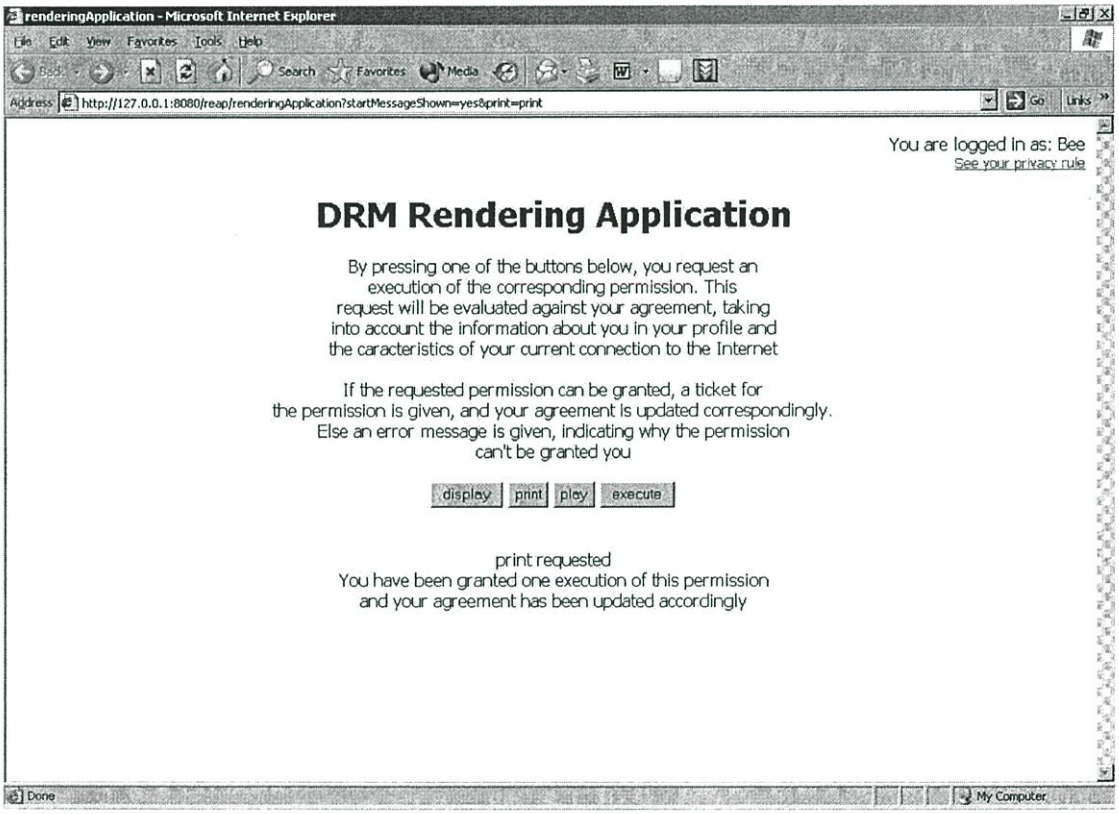


รูปที่ ก.9 ผลการเปรียบเทียบความเป็นส่วนตัวระหว่าง DRM policy และ User's Privacy Preferences กรณีที่ระบบแก้ปัญหาความขัดแย้งโดยเลือกกฎที่ดีที่สุดในกระบวนการ Negotiation Process



รูปที่ ก.10 การทำข้อตกลงระหว่างผู้ใช้กับเนื้อหาที่ระบบให้บริการ

จากรูปที่ ก.10 เมื่อระบบได้ทำการเปรียบเทียบการกำหนดความเป็นส่วนตัวของผู้ใช้และนโยบายความเป็นส่วนตัวของระบบ DRM ซึ่งอาจผ่านกระบวนการเจรจาต่อรองเพื่อให้ได้ข้อตกลงในการใช้ข้อมูลความเป็นส่วนตัวที่เหมาะสมและพอใจแก่ผู้ใช้และเจ้าของเนื้อหาดิจิตอลในระบบ DRM แล้ว จากนั้นระบบจะนำเสนอข้อตกลงและเงื่อนไขในเนื้อหาดิจิตอลที่เจ้าของได้ทำการกำหนดเอาไว้ เพื่อนำเสนอให้ผู้ใช้ได้เลือกและทำข้อตกลงกับระบบ DRM



รูปที่ ก.11 การเริ่มต้น Rendering Application ในเนื้อหาตามที่ผู้ใช้ได้ทำข้อตกลงกับระบบเอาไว้

จากรูปที่ ก.11 เมื่อผู้ใช้ทำข้อตกลงในเนื้อหาดิจิตอลในระบบ DRM แล้ว ระบบจะออกใบรับรองสิทธิ์ (License) ให้แก่ผู้ใช้ เพื่อกำหนดสิทธิ์การใช้งานเนื้อหาดิจิตอลตามข้อตกลงที่ผู้ใช้ได้เลือกไว้ และระบบ DRM จะทำการ Render Application ตามสิทธิ์ใน License ที่ผู้ใช้ได้ทำข้อตกลงไว้แก่เนื้อหาดิจิตอลในระบบ DRM

ภาคผนวก ข.

XML Schema ของ Policy และ User's Privacy Preferences

XML Schema ของ Policy ในระบบ DRM

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.Drm.org/Policy"
xmlns="http://www.w3.org/2001/XMLSchema" xmlns:po="http://www.Drm.org/Policy"
elementFormDefault="qualified">
  <element name="policy">
    <complexType>
      <sequence>
        <element ref="po:mandatory" />
        <element ref="po:optional" minOccurs="0" />
      </sequence>
      <attribute name="Material_Name" type="string" use="required" />
      <attribute name="Material_Type" type="string" use="required" />
      <attribute name="date" type="string" use="optional" />
    </complexType>
  </element>

<!-- ************* Mandatory ************* -->
  <element name="mandatory">
    <complexType>
      <sequence>
        <element ref="po:statement" maxOccurs="unbounded" />
      </sequence>
    </complexType>
  </element>
  <element name="statement">
    <complexType>
      <choice maxOccurs="unbounded">
        <element ref="po:purpose" />
        <element ref="po:recipient" />
        <element ref="po:retention" />
        <element name="data-group" type="po:data-group-type" />
        <element ref="po:rule" />
      </choice>

      <attribute name="description" type="string" use="optional" />
    </complexType>
  </element>

<!-- ************* Optional ************* -->
  <element name="optional">
    <complexType>
      <sequence>
        <element ref="po:statement" maxOccurs="unbounded" />
      </sequence>
    </complexType>
  </element>

  <element name="statement">
    <complexType>
      <choice maxOccurs="unbounded">
        <element ref="po:purpose" />
        <element ref="po:recipient" />
        <element ref="po:retention" />
        <element name="data-group" type="po:data-group-type" />
        <element ref="po:rule" />
      </choice>
      <attribute name="description" type="string" use="optional" />
```

```
    </complexType>
  </element>

<!-- ************ data ************ -->
  <complexType name="data-group-type">
    <sequence>
      <element name="data" type="po:data-type" maxOccurs="unbounded" />
    </sequence>
    <attribute name="base" type="anyURI" use="optional" default="http://www.Drm.org/Policy/base"
/>
  </complexType>
  <complexType name="data-type" mixed="true">
    <attribute name="type" type="anyURI" use="required" />
  </complexType>

<!-- ************ mandatory-rule ************ -->
  <complexType name="mandatory-rule">
    <choice>
      <element ref="po:purpose" />
      <element ref="po:recipient" />
      <element name="data-group" type="po:data-group-type" />
    </choice>
  </complexType>

<!-- ************ Rule************ -->
  <element name="rule">
    <complexType>
      <sequence>
        <element ref="po:IfRule" maxOccurs="unbounded" />
      </sequence>
    </complexType>
  </element>
  <element name="IfRule">
    <complexType>
      <sequence>
        <element name="IfNotGive" type="po:mandatory-rule" />
        <element name="Then" type="po:mandatory-rule" />
      </sequence>
    </complexType>
  </element>

<!-- ************ Purpose************ -->
  <element name="purpose">
    <complexType>
      <sequence>
        <choice maxOccurs="unbounded">
          <element name="current" type="po:purpose-value" />
          <element name="admin" type="po:purpose-value" />
          <element name="develop" type="po:purpose-value" />
          <element name="analysis-decision" type="po:purpose-value" />
          <element name="history" type="po:purpose-value" />
          <element name="other-purpose" type="po:purpose-value" />
        </choice>
      </sequence>
    </complexType>
  </element>
  <complexType name="purpose-value" />

<!-- ************Recipient ************ -->
  <element name="recipient">
```

```
    <complexType>
      <sequence>
        <choice maxOccurs="unbounded">
          <element name="ours" type="po:recipient-value" />
          <element name="other-recipient" type="po:recipient-value" />
          <element name="delivery" type="po:recipient-value" />
          <element name="public" type="po:recipient-value" />
          <element name="unrelated" type="po:recipient-value" />
        </choice>
      </sequence>
    </complexType>
  </element>
  <complexType name="recipient-value" />

<!--**********Retention**********-->
  <element name="retention">
    <complexType>
      <sequence>
        <choice>
          <element name="license" type="po:retention-type" />
          <element name="material" type="po:retention-type" />
          <element name="special-purpose" type="po:retention-type" />
          <element name="indefinite" type="po:retention-type" />
          <element name="user" type="po:retention-type" />
        </choice>
      </sequence>
    </complexType>
  </element>
  <complexType name="retention-value" />
</schema>
```

XML Schema ของ User's Privacy Preferences ในระบบ DRM

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.Drm.org/Preference" elementFormDefault="qualified"
xmlns:pre="http://www.Drm.org/Preference" xmlns="http://www.w3.org/2001/XMLSchema">
<element name="preference">
        <complexType>
                <sequence>
                        <element ref="pre:free"/>
                        <element ref="pre:limited"/>
                        <element ref="pre:not-given"/>
                </sequence>
                <attribute name="name" type="string" use="optional"/>
                <attribute name="date" type="string" use="optional"/>
        </complexType>
</element>
<!--********************Free*************** -->
<element name="free">
        <complexType>
                <sequence>
                        <element ref="pre:statement" maxOccurs="unbounded"/>
                </sequence>
        </complexType>
</element>
<!--********************Limited*************** -->
<element name="limited">
        <complexType>
                <sequence>
                        <element ref="pre:statement" maxOccurs="unbounded"/>
                </sequence>
        </complexType>
</element>
<!--********************NotGiven*************** -->
<element name="not-given">
        <complexType>
                <sequence>
                        <element ref="pre:statement" maxOccurs="unbounded"/>
                </sequence>
        </complexType>
</element>
<element name="statement">
        <complexType>
                <choice maxOccurs="unbounded">
                        <element ref="pre:purpose"/>
                        <element ref="pre:recipient"/>
                        <element ref="pre:retention"/>
                        <element name="data-group" type="pre:data-group-type"/>
                </choice>
        </complexType>
</element>
<!--******************** purpose*************** -->
<element name="purpose">
        <complexType>
                <sequence>
                        <choice maxOccurs="unbounded">
                                <element name="current" type="pre:purpose-value"/>
                                <element name="admin" type="pre:purpose-value"/>
                                <element name="develop" type="pre:purpose-value"/>
                        <element name="analysis-decision" type="pre:purpose-value"/>
```

```
                        <element name="history" type="pre:purpose-value"/>
                        <element name="other-purpose" type="pre:purpose-value"/>
                    </choice>
                </sequence>
            </complexType>
        </element>
        <complexType name="purpose-value"/>
        <!--********************recipient*************** -->
        <element name="recipient">
            <complexType>
                <sequence>
                    <choice maxOccurs="unbounded">
                        <element name="ours" type="pre:recipient-value"/>
                        <element name="other-recipient" type="pre:recipient-value"/>
                        <element name="delivery" type="pre:recipient-value"/>
                        <element name="public" type="pre:recipient-value"/>
                        <element name="unrelated" type="pre:recipient-value"/>
                    </choice>
                </sequence>
            </complexType>
        </element>
        <complexType name="recipient-value"/>
        <!-- ************ data ************ -->
        <complexType name="data-group-type">
            <sequence>
                <element name="data" type="pre:data-type" maxOccurs="unbounded"/>
            </sequence>
            <attribute name="base" type="anyURI" use="optional"
            default="http://www.Drm.org/Policy/base"/>
        </complexType>
        <complexType name="data-type" mixed="true">
            <attribute name="type" type="anyURI" use="required"/>
        </complexType>
        <!--*****************Retention****************-->
        <element name="retention">
            <complexType>
                <sequence>
                    <choice>
                        <element name="license" type="pre:retention-value"/>
                        <element name="material" type="pre:retention-value"/>
                        <element name="special-purpose" type="pre:retention-value"/>
                        <element name="indefinite" type="pre:retention-value"/>
                        <element name="policy" type="pre:retention-value"/>
                    </choice>
                </sequence>
            </complexType>
        </element>
        <complexType name="retention-value"/>
</schema>
```

ภาคผนวก ค.

ผลงานทางวิชาการที่ได้รับการตีพิมพ์

2004 INTERNATIONAL CONFERENCE ON CONTROL, AUTOMATION, AND SYSTEMS (ICCAS2004)

August 25 - 27, 2004

The Shangri-La Hotel, Bangkok, Thailand

A Privacy Negotiation Algorithm for Digital Rights Management

Jurairat Phuttharak, and Chanboon Sathitwiriyawong

Faculty of Information Technology, and
Research Center for Communications and Information Technology (ReCCIT)
King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand
Email: s4067018@kmitl.ac.th, chanboon@it.kmitl.ac.th

Abstract: Internet-based distribution of digital contents provides great opportunities for producers, distributors and consumers, but it may seriously threaten users' privacy. The Digital Rights Management (DRM) systems which are one of the current technologies, concern the protection of the ownership/copyright of digital content but the most recent DRM systems do not support the protection of the user's personal information. This paper examines the lack of privacy in DRM systems. A privacy policy and user's privacy preferences model that protect each user's personal information from privacy violation by DRM systems are described. DRM privacy agent is allowed to be the automatic negotiator between the DRM system policy and user's privacy preferences. An effective negotiation algorithm for the DRM system is proposed. Privacy rules are created following the negotiation process to control access of the user's personal information in the DRM system. The proposed privacy negotiation algorithm can be adapted appropriately to the existing DRM systems to solve the privacy problem effectively.

Keywords: Digital Rights Management, Privacy Policy, User's privacy preferences, Privacy Negotiation

1. INTRODUCTION

Contents are increasingly in digital forms and are widely distributed via the Internet. The ease of making copies has created the need to develop a means to protect them. Digital rights management (DRM) technology is a solution for controlling the usage of the digital contents. The DRM protects the owner of the digital contents by restricting what actions an authorized recipient may take in regard to those contents [1].

The functional DRM architecture can be divided into three areas: content creation, content management, and content usage. Content creation includes the creation of the digital content and the definition of rights. Content management is about content distribution and trading of the rights. Finally, content usage is used to enforce the rights and to track the usage of contents.

Current DRM has been developed by several companies: InterTrust's Rights|System [11], Microsoft's Windows Media Rights Manager (WMRM) [12], IBM's Electronic Media Management System (EMMS) [13], RealNetworks' Real Systems Media Commerce Suite (RMCS) [14], and so on. DRM systems focus on the rights of the content provider or owner. User information can be easily revealed and tracked the usage. However, DRM systems and framework have not assumed any user privacy. Privacy protection scheme would enable the protection of consumer rights as well as content provider rights [3]. Rights enforcement may be facilitated by user's tracking or by network control of users' computers. However, both techniques are potentially destructive of user privacy [2].

This paper addresses a new protection scheme for users' privacy for digital rights management. Privacy protection can be compromised through the collection of data by owners or distributors. The DRM policy and the users' privacy preferences are designed for digital rights management and using input parameters as mandatory and optional.

The DRM system policy can declare alternative elements in case that a user does not want to provide some mandatory input parameters. Users can declare how much their personal information can be made available to the DRM system to compromise their privacy preferences with the DRM system. A negotiation algorithm that provides flexibility and helpful assistant to automatically negotiate the term and conditions when a user is connected to the DRM system is proposed. The DRM privacy agent would apply the user's privacy preferences and try to negotiate an agreement to the DRM system. Finally, the privacy rules are created for accessing control on the use of the personal information in the DRM system.

The rest of this paper is organized as follows: In Section 2, we discuss the related works. The basis element of a privacy policy and user's privacy preferences for the DRM system are described in Section 3. In Section 4, we propose a privacy negotiation algorithm for the DRM system. An example scenario is given to illustrate the concepts in Section 5. Finally, in Section 6, we conclude the paper.

2. RELATED WORKS

InterTrust [11] offers a solution for content packaging, distribution and rights management based on a packager program and rights server technology. This system supports the varieties requirement of electronic commerce such as pay-per-use, rentals, sales, and try-before-buy business model. WMRM [12] is an end-to-end DRM system for the secure distribution of multimedia files over the Internet. The solution is based on Windows Media Player and Server. It provides a flexible platform to content providers for secure distribution of digital media file. The user must acquire a license key to unlock the media file. The supported business model can be subscription, sales, counted operations and secure transfer of protected digital media files to devices or PC. IBM EMMS [13] was developed for the preparation and secure distribution of all forms of digital contents. This system supports pay-per-use, pay-per-time, subscription, controlled printing, and protected transfer to portable devices. RMCS [14] offer a package server, streaming server, license server and a secure file format plug-in for RealPlayer and supports subscription, video on demand and other business model. PrecePt [15] is a protocol that affirms user's anonymity using temporary ID (TID) and token to guarantee anonymity. This protocol protects user privacy when it authenticates a user in issuing a license. The information can be protected from danger which may be flowed out by cryptography.

According to the privacy engineering for digital rights management system, privacy concerns two essential ways [2]. The first way is that the DRM model requires the user to provide an ID number that links the user's personal information (name, address, transaction history, etc.) with the device or service a person intends to use. The paper said that tracking for the purpose of tying content to a set of devices obviously put at risk some previous private information about the user. The second way is that the DRM model requires the users to reconfirm that they will not copy a product for resale or sharing. The model not only catalogues the user under a user-specific ID, but also catalogues the customer's usage history of a product that has been downloaded from the system that is subscribed to and streamed whenever requested [6].

They suggested an alternative to privacy engineering that avoids the problem of the DRM system. The fair information practice allows the provision of personal information for a specific purpose without the fear that it may later be used for an unrelated purpose without the owner's knowledge or consent. Privacy enhancement should also be built directly into the DRM technology [2].

Among several approaches for privacy management using service policies and privacy preferences, the most mature one is the Platform for Privacy Preferences Project (P3P) [7] developed by the World Wide Web Consortium (W3C). P3P enables web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents like web browsers. The P3P Specification 1.0 [7] includes the definition of the syntax and semantics of a vocabulary to describe data uses, data recipients, data retention policy and other privacy disclosures in P3P privacy policy files. APPEL (A P3P Preference Exchange Language) [8] provides a standard way of defining the user privacy preferences in a set of preference rules, while can be used by the user agent to make automated or semi-automated decisions regarding the acceptance of privacy policies from P3P enabled web sites.

It should be noted that P3P is for web sites and does not intend to exploit DRM. In fact only a few recent works address DRM issues for privacy management.

3. A PRIVACY FRAMEWORK COMPONENTS FOR DIGITAL RIGHTS MANAGEMENT

3.1 Overview of the proposed system

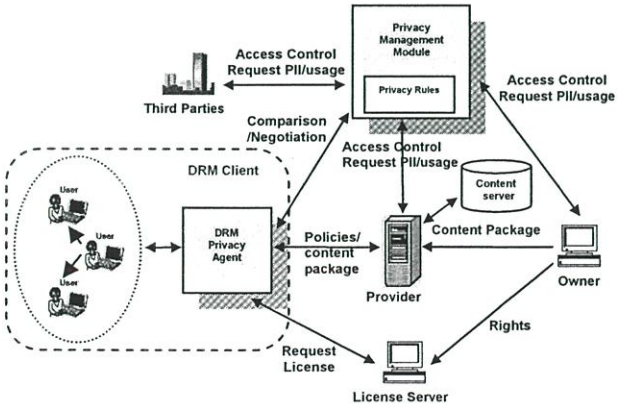


Fig. 1 Privacy framework components for DRM

The DRM system model with the proposed privacy negotiation algorithm is shown in Fig. 1. The basic elements for privacy DRM system model are proposed. A DRM privacy agent is allowed to compare and automatically negotiate between user's privacy preferences and DRM policy, and then the appropriate privacy rules for each user are generated. The privacy management module is one of the components that collect the privacy rules and access control the user's personal information to the parties. The basic elements comprise the following:

- *Element of Privacy Policy:* A material such as music, movie, documents etc. on DRM systems describes the use of personal user information in policy statements.
- *Requested Data:* The policy statements request the data set from the user as mandatory and optional element of DRM systems.
- *Privacy Preferences:* The user is responsible for declaring his privacy preferences regarding the policy statements of DRM systems. The declaration of privacy preferences are based on three permission levels as NotGiven, Limited, and Free.
- *Rule Evaluation:* This process determines the user's privacy rules regarding the DRM system, to be utilized during the negotiation phase between user's privacy preference and the DRM policy.
- *Negotiation mechanism:* This process is based on the policy declaring the material on DRM system's request and rules describing the privacy preferences of the user. The negotiation mechanism tries to find an agreement between the user and the DRM system. Comparing between the policy statements and user permission levels and the alternative rules, this process generates a privacy rules set that describes the access control of the user personal information that is sufficient for the DRM system and allowed by the user.

The DRM privacy agent stores the privacy preferences of a user. Material on the DRM system describes the requested data and alternative rules. The DRM privacy agent compares the user's privacy preferences with the requested data and alternative rules on the DRM system as shown in Fig. 2.

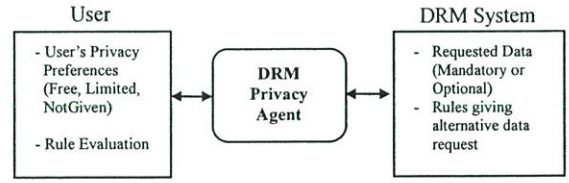


Fig. 2 DRM privacy agent architecture

3.2 Elements of a privacy policy

We introduce the elements of our privacy policy statements that provide a way to describe the data use practices on DRM systems. For each material on the DRM system should also declare their policies regarding such as their purpose to request the data, with whom that they may share the data and when they will retain the data.

3.2.1 Purpose

The purposes declare the basis objective for collecting user's data on the DRM system. This paper intends to collect data into categories for the DRM system. Those purposes for collecting data in the DRM system include the following:

- Personalized use for direct marketing
- Quality of service enhancement
- Backup and archives

- Aggregate usage of information for marketing
- Profiling (de)personalized records
- Customer service and retention
- Recommendation service

Those purposes adapted the P3P [7] policy mechanism to DRM systems as shown in Fig. 3.

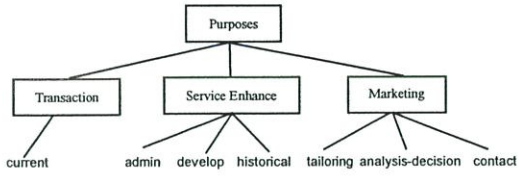


Fig. 3 Hierarchy of purposes for DRM system

3.2.2 Recipient

The recipients describe the parties with whom the data will be shared. The P3P [7] defined six types of recipient policies. The recipient type is adapted appropriately for the DRM system as shown in Fig. 4.

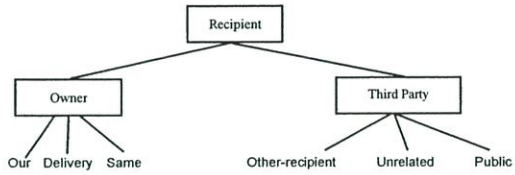


Fig. 4 Hierarchy of recipient for DRM system

3.2.3 Retention

The retentions define the duration for which the collected information will be kept. The retention type is adapted for DRM systems as following:

- *License:* Information is retained to meet in period of time by license.
- *Material:* Information is retained to meet in period of time by material.
- *Special-purpose:* Information is retained to meet the special purpose and determined by administrator or provider's business practices.
- *Indefinite:* Information is retained for an indeterminate period of time.
- *User define:* Information is retained by user definition.

3.2.4 Data

Information collected in a DRM system may include data about personally identifying information (PII), content retrieval, rights retrieval, content accessing, frequency, times, access location, etc. This information can be obtained by logging server-side or by having client-side DRM software to store relevant usage data. We define data reference by the P3P [7] policy.

3.3 Requested data of the DRM system

The fair information practice is a general term for a set of standards governing the collection and use of personal data and addressing issues of privacy and accuracy. The OECD [10] has written "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" which have been widely accepted to describe their desirable privacy goal. This is particularly well suited for relatively complex systems like the DRM systems, in which there are a number of legitimate purposes for collecting and using information [2].

This paper defines two parts of requested data on the DRM system. The first part comprises a mandatory element and an optional element. The second part provides rules that are used to request alternative elements if the required information is not provided by the user.

Mandatory is essential for DRM to collect and execute the information. Optional is requested for some other purposes. Both mandatory and optional elements consist of a set of purposes, a set of recipients, a set of retention periods, and a set of data, to form a major part of the entire DRM policy. Alternative elements are also defined using "if-then" rules to get some required elements if the required mandatory elements are not given by the user. Fig. 5 and Fig. 6 show the examples for DRM policy.

```
<?xml version="1.0"?>
<policy Material_Name="The Lord Of The Ring" Material_Type="book">

    <mandatory>
        <statement>
          <purpose> <current/> <admin/> </purpose>
          <recipient> <ours/> <delivery/> </recipient>
          <retention defined-by="special-purpose" description="developement"/>
          <data-group>
                <data type="#user.name"/>
                <data type="#user.email.address"/>
          </data-group>
        </statement>
    </mandatory>

    <optional>
        <statement>
          <purpose> <historical> </purpose>
          <recipient> <our/> </recipient>
          <retention defined-by="material" description="marketing"/>
          <data-group>
                <data type="#uclick.stream"/>
          </data-group>
        </statement>
    </optional>

</policy>
```

Fig. 5 Privacy policies in DRM system

```
<rule>

  <IfRule>
        <IfNotGiven>
              <purpose> <current/> </purpose>
        </IfNotGiven>
        <Then>
              <purpose> <admin/> </purpose>
        </Then>
  </IfRule>

  <IfRule>
        <IfNotGiven>
              <data-group> <data type="#user.name"/> </data-group>
        </IfNotGiven>
        <Then>
              <data-group> <data type="#user.email.address"/> </data-group>
        </Then>
  </IfRule>

  <IfRule>
        <IfNotGiven>
              <data-group> <data type="#user.email.address"/> </data-group>
        </IfNotGiven>
        <Then>
              <data-group> <data type="#user.postal"/> </data-group>
        </Then>
  </IfRule>

  <IfRule>
        <IfNotGiven>
              <retention defined-by="special-purpose"/>
        </IfNotGiven>
        <Then>
              <retention defined-by="material"/>
        </Then>
   </IfRule>

</rule>
```

Fig. 6 An example of conditional statements

3.4 Description of user's privacy preferences

The users define their privacy preferences for the DRM

system through a rule-based mechanism. There are three permission level rules that can be imposed on the elements.

- *Free:* the elements are given freely by the user.
- *Limited:* the elements are provided by the user only if it is mandatory for the DRM system.
- *NotGiven:* the elements are not provided by the user.

Sometimes user's privacy preference rules may impose conflicting on the elements. It is considered that NotGiven rule is over other rules. Free rule has the least priority and Limit rule's priority is between these two. Fig. 7 shows an example of user's privacy preferences.

```
<?xml version="1.0"?>
<preference>
    <free>
        <statement>
            <purpose> <current/> </purpose>
            <recipient> <ours/> </recipient>
            <retention defined-by="license"/>
            <data-group>
                <data type="#user.name"/>
                <data type="#user.gender"/>
            </data-group>
        </statement>
    </free>
    <limited>
        <statement>
            <purpose> <admin/> <develop/> </purpose>
            <recipient> <delivery/> <other-recipient/> </recipient>
            <retention defined-by="material"/>
            <data-group>
                <data type="#user.clickstream"/>
                <data type="#user.telephone"/>
            </data-group>
        </statement>
    </limited>
    <not-given>
        <statement>
            <purpose> <analysis-decision/> </purpose>
            <recipient> <public/> <unrelated/> </recipient>
            <retention defined-by="indefinite"/>
            <data-group>
                <data type="#user.email.address"/>
                <data type="#user.home.address"/>
                <data type="#user.creditcard"/>
            </data-group>
        </statement>
    </not-given>
</preference>
```

Fig. 7 User's privacy preferences rules

4. NEGOTIATION MECHANISM

Negotiation mechanism comprises a set of activities that the user's privacy preferences are compared with DRM policy in order to reach an agreement. If an agreement cannot be reached, the alternative rules are requested through conditional statements provided by the DRM system.

4.1 Rule evaluation

Rule evaluation is the process of comparing user's privacy preferences rules against the DRM policy. We introduce the relevant terms that will be used for rule evaluation. Rules are privacy preferences for each statement, and facts are DRM policy. The following definitions will introduce the term rules and facts.

- U is set of data, where $U = \{d_1, d_2, \ldots, d_n\}$ $d_i, 1 \leq i \leq n$
- A rule denotes r that is defined by a pair (D_r, C_r), $D_r \subseteq U$, $C_r = \{c_1, c_2, \ldots, c_m\}$ c_j, $1 \leq j \leq m$ and $c_j = (x_j, v_j)$, $1 \leq j \leq m$, x_j denotes the name and v_j denotes the set of values.
- The facts denotes f that are defined by a pair (D_f, G_f) $D_f \subseteq U$, $G_f = \{g_1, g_2, \ldots, g_k\}$ g_j, $1 \leq j \leq k$ and $g_j = (x_j, v_j)$, $1 \leq j \leq m$, x_j denotes the name and v_j denotes the set of values.

When a rule was found that is matched by the facts, access to the requested data can be granted. In order to match a rule, the facts need to meet two requirements. Firstly, the facts must satisfy all of the rule's constraints. Secondly, the requested data as specified in the facts must be a subset to the data specified in the rule.

The constraint-matching function (β) is a Boolean function that show whether a name-value pair $p \in G_f$ of the facts matches constraint $c \in C_r$ of a rule.

$$\beta(c,p) = \begin{cases} \text{true, if p satisfies c} \\ \text{false, otherwise} \end{cases} \quad (1)$$

We give facts $f = (D_f, G_f)$ match rule $r = (D_r, C_r)$, if: (2)

(a) $\forall (c \in C_r)$ and $\forall (p \in G_f)$ with $\beta(c, p) = \text{true}$

(b) $D_f \subseteq D_r \leftrightarrow \forall (d_l \in D_f)$ and $\forall (d_l \in D_r)$

4.2 Negotiation algorithm

According to above we use user's privacy preference as rule sets in order to support the automated negotiation. When the data provided by the user does not match with the data requested by the DRM system, the alternative rules are provided by the DRM system. After the rule evaluation component rejects a request for data, we need to find out how the best rule matches the facts. This rule specifies acceptable conditions for the release of a set of data. In order to offer a reasonable alternative to a user's rejected request, it is goal now to find the rule that best matches the facts.

Our approach to find the best rule matching is to compute the weight between the individual rules in the rule sets and the facts. And we also use the alternative conditions as if-then rule to find the best rule matching. The rule with the maximum weight is considered the closest rule and is used to produce privacy rule for user. Based on this weights compute, the rule with the maximum weight, it is needed to determine how well the fact satisfies the constraints of the rule. Firstly, we define a function that computes to what degree the facts satisfy a rule constraint.

The function σ_c is a number of matching between the constraint of the rule $r = (D_r, \{c_1, \ldots, c_n\})$, $c_i = \{x_i, v_i\}$, $v_i = \{a_1, \ldots, a_n\}$ and the facts $f = (Df, \{g_1, \ldots, g_n\})$, $g_j = \{y_j, z_j\}$, $z_j = \{b_1, \ldots, b_n\}$, $v_{then} = \{k_1, \ldots, k_n\}$. It is defined such that:

$$\sigma_c(c_i, f) = \begin{cases} 0, & \text{if } ((z_i \cup v_{then}) \cap v_i) = \phi \\ > 0, & \text{otherwise} \end{cases} \quad (3)$$

Secondly, we define the function σ_d that is a number of matching between a set of data of a rule r and facts f, D_{then} is a set of data in if-then rules. It is defines such that:

$$\sigma_d(D_r, f) = \begin{cases} 0, & \text{if } ((D_f \cup D_{then}) \cap D_r) = \phi \\ > 0, & \text{otherwise} \end{cases} \quad (4)$$

The function $\partial(r_i, f)$ is a number of matching between a rule and facts on the set of positive integers. $\partial(r_i, f)$ is defined as follows:

$$\partial(r_i, f) = \left[\sum_{i=1}^{n} \sigma_c(ci, f) \cdot w_i \right] + \sigma_d(D_r, f) \cdot w_d \quad (5)$$

The terms w_i and w_d are weights which are related to the n constraints c_i and the data set D_f of a rule. Weights can be used to set the importance of constraint and allow specifying some parts of the rule that are more important than others, while searching for the closest rule.

$$\partial(f) = \sum_{i=1}^{k} L_c \,.\, w_i + n \,.\, w_d \qquad (6)$$

where L_c is a number of value for each constraints.
n is a number of data in the facts.

The function $\partial(f)$ computes the sum between weight of constraints and weight of data in the facts. This result is compared with the function $\partial(r_i, f)$ so that matching rules can be checked.

The function grant(r_i, f) is a Boolean function that shows the matching of the rules.

$$\text{grant}(r_i, f) = \begin{cases} \text{true}, & \partial(ri, f) = \partial(f) \\ \text{false}, & \text{otherwise} \end{cases} \qquad (7)$$

The best matching rule is computed from the function as the following.

$$\max(\partial(r_j, f)), \quad (1 \le j \le n) \qquad (8)$$

5. PROOF OF AN EXAMPLE SCENARIO

In this section, we provide a scenario to better illustrate the concept presented for the negotiation algorithm in DRM systems. We assume the DRM policies as Facts and user's privacy preferences as Rules, as shown in Fig. 8 and Fig. 9.

```
<mandatory>
  <statement>
    <purpose> <develop/> </purpose>
    <recipient> <ours/> </recipient>
    <retention defined-by="material" description="developement"/>
    <data-group>
        <data type="#user.name"/>
        <data type="#user.age"/>
        <data type="#user.clickstream"/>
    </data-group>
    <rule>
      <IfRule>
        <IfNotGiven>
          <purpose><develop/> </purpose>
        </IfNotGiven>
        <Then>
          <purpose> <admin/> </purpose>
        </Then>
      </IfRule>
      <IfRule>
        <IfNotGiven>
          <data-group> <data type="#user.age"/> </data-group>
        </IfNotGiven>
        <Then>
          <data-group><data type="#user.gender"/> </data-group>
        </Then>
      </IfRule>
    </rule>
  </statement>
</mandatory>
```

Fig. 8 An example of the DRM system requested data (Facts)

```
<?xml version="1.0"?>
<preference>
  <free>
    <statement>
      <purpose> <current/> </purpose>
      <recipient> <ours/> </recipient>
      <retention defined-by="license"/>
      <data-group>
          <data type="#user.name"/>
          <data type="#user.creditcard"/>
          <data type="#user.age"/>
          <data type="#user.mobilephone"/>
      </data-group>
    </statement>
  </free>
  <limited>
    <statement>
      <purpose> <admin/> </purpose>
      <recipient> <our/> </recipient>
      <retention defined-by="material"/>
      <data-group>
          <data type="#user.name"/>
          <data type="#user.homephone"/>
          <data type="#user.clickstream"/>
      </data-group>
    </statement>
  </limited>
  <not-given>
    <statement>
      <purpose> <historical/> <develop/> </purpose>
      <recipient> <public/> <unrelated/> </recipient>
      <retention defined-by="indefinite"/>
      <data-group>
          <data type="#user.email.address"/>
          <data type="#user.clickstream"/>
          <data type="#user.mobilephone"/>
      </data-group>
    </statement>
  </not-given>
</preference>
```

Fig.9 An example of user' privacy preferences (Rules)

5.1 Rule evaluation

The facts f in Fig. 8 do not match any of the three rules R in Fig. 9 because some constraints are not satisfied and the data set do not match completely from functions (1), (2). In the Free rule statement which has purpose, retention, and some data elements, does not match with the facts f. The Limited rule statement which comprises purpose, retention, and some data elements, does not match with the facts f. Finally, the NotGiven rule statement that comprises recipient, retention, and some data elements, does not match with the facts f. As a result, this process must be passed to the negotiation process.

5.2 Negotiation algorithm

Following the rule evaluation, the facts f do not match any rules R. Negotiation process is provided, the firstly to compute the sum between weight of constraints and weight of data in the facts as following (6). Then the facts are compared with the rules as following the functions (3), (4), (5). Alternative conditions of rules are also provided in the functions (3), (4). Fig. 10 shows the tree of Limited rules and Free rules

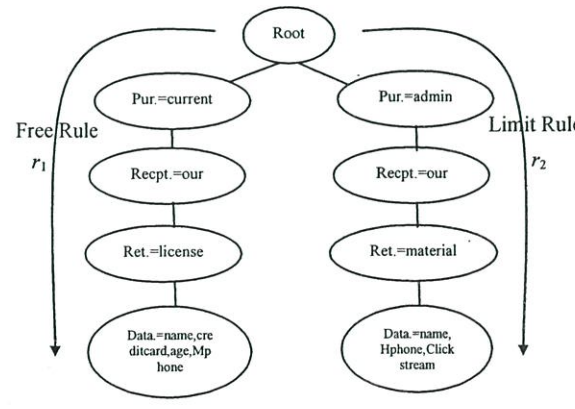


Fig. 10 An example tree of Limited and Free rules set

The user's privacy preferences result in the facts f:

Purpose = *develop* Recipient = *our* Retention = *material* Data = *name, age, clickstream*	Mandatory Statement
If *develop* then *admin* If *age* then *gender*	Conditional Statements

The facts f do not match any of the two rules in Fig. 10. The user sets the weights w_i and w_d as equal to 1. Using the function (6), the result is as follows.

$$\partial(f) = (1 \cdot 1) + (1 \cdot 1) + (1 \cdot 1) + (3 \cdot 1) = 6$$

However, the rules could be used to find the best matching rules. We get the weights both rules.

$$\partial(r_1, f) = (0 \cdot 1) + (1 \cdot 1) + (0 \cdot 1) + (2 \cdot 1) = 3$$
$$\partial(r_2, f) = (1 \cdot 1) + (1 \cdot 1) + (1 \cdot 1) + (2 \cdot 1) = 5$$

The weights of rules r_1 and r_2 do not equal the weight of the facts such that the best matching rule can be found. The function (8) is provided to find the best matching rule with facts.

$$\max(\partial(r_1, f),\ \partial(r_2, f)) = 5$$

So rule r_2 should be chosen in order to produce the matching. This best matching rule will be offered to the DRM system. The DRM system will use the offered rule for adapting appropriate rule and offer it to the user again.

6. CONCLUSION

The goal of the DRM technology is the distribution of digital contents in a manner that protects the rights of all parties involved, including copyright owners, distributors, and users. The problem of the present DRM system is seriously threatening users' privacy.

In this paper presented an appropriate privacy policy and user's privacy preferences for the DRM system. The user's privacy preferences define the rules that control the read accessing for personal information. Furthermore the privacy policy model allows DRM systems to declare alternative requested data if a mandatory element is not given by the users. In this way it becomes possible to automate negotiation mechanism with the DRM system to reach an agreement. An effective negotiation algorithm is proposed. The negotiation processes comprise rule evaluation and negotiation mechanism. The rule evaluation determines the user's privacy rules regarding the DRM system, to be utilized during the negotiation between user's privacy preference and the privacy policy of the DRM system. The negotiation mechanism tries to find an agreement between the user and the DRM system, and compare among policy statements, user permission levels, and alternative rules. We believe that this framework can be used to enhance the negotiation capabilities of existing DRM systems, which are currently limited to negotiate the user's personal information.

ACKNOWLEDGMENTS

The authors gratefully acknowledge the contribution of the Research Center for Communications and Information Technology (ReCCIT), King Mongkut's Institute of Technology Ladkrabang (KMITL).

REFERENCES

[1] A. Russ, "Digital Rights Management Overview," SysAdmin, Audit, Networking and Security (SANS) Information Security Reading Room, July 26, 2001.

[2] J. Feigenbaum, M. Freedman, T. Sander, and A. Shostack, "Privacy Engineering for Digital Rights Management Systems," the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, pp. 76-105, 2001.

[3] P. Vora, D. Reynolds, I. Dickinson, J. Erickson, and D. Banks, "Privacy and Digital Rights Management," the W3C Workshop on Digital Rights Management for the Web, [Online]. Available: http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi.html, January 2001.

[4] L. Korba, "Privacy in Distributed Electronic Commerce," Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS), pp. 4017-4026, January 2002.

[5] L. Korba, and S. Kenny, "Towards Meeting the Privacy Challenge: Adapting DRM," ACM Workshop on Digital Rights Management, pp. 118-136, November 18, 2002.

[6] A. Cavukian, "Privacy and Digital Rights Management (DRM): An Oxymoron," Information and Privacy Commissioner/Ontario, October 2002, [Online]. Available: http://home.inter.net/gt/grabbag/Ontario.drm.pdf.

[7] W3C, "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification", [Online]. Available: http://www.w3.org /TR/P3P/, April 2002.

[8] W3C, "A P3P Preference Exchange Language (APPEL)," [Online]. Available: http://www.w3.org/TR/P3Ppreferences.html

[9] B. Rosenblatt, Digital Rights Management Business and Technology, New York, Hungry Minds Inc., 2002.

[10] Organization for Economic Co-operation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," [Online]. Available:http://www.oecd.org/dsti/sti/it/secure/prod/PRIV-EN.HTM, September 1980.

[11] InterTrust, [Online]. Available:http://www.intertrust.com.

[12] Microsoft, "Architecture Microsoft Media Rights Manager,"[Online].Available:http://www.microsoft.com/windows/windowsmedia/wm7/drm/architecture.aspx.

[13] EMMS, "Electronic Media Management System," [Online]. Available:http://www.ibm.com/software/emms.

[14] RMCS, "Real Systems Media Commerce Suite," [Online]. Available:http://docs.real.com/docs/drm/DRM_WP1.pdf.

[15] P. Bok-Nyong, K. Jae-Won, and L. Wonjun, "PrecePt: A Privacy-Enhancing License Management Protocol for Digital Rights Management," Proceedings of the 18th International Conference on Advanced Information Networking and Applications (AINA), Volume 1, pp. 574-579, March 2004.

ประวัติผู้เขียน

ชื่อ-นามสกุล	นางสาวจุไรรัตน์ พุทธรักษ์
วัน เดือน ปีเกิด	1 พฤษภาคม 2522
ที่อยู่	44/16 ซอย 4 ถนน สังขวิทย์ ตำบลทับเที่ยง อำเภอเมือง จังหวัดตรัง 92000
	โทร. 0-7521-4376
ประวัติการศึกษา	วิทยาศาสตรบัณฑิต (วิทยาการคอมพิวเตอร์)
	มหาวิทยาลัยสงขลานครินทร์ 2544