บทที่ 2

การทบทวนวรรณกรรม

ภายในบทนี้จะกล่าวถึงรายละเอียดของทฤษฎีและเทคนิควิธีการต่างๆ ที่นำมาประยุกต์ใช้ในงานวิจัย รวมถึงผลของงานวิจัยอื่นๆ ที่เกี่ยวข้อง ซึ่งประกอบไปด้วยสองส่วนใหญ่ๆ คือ ทฤษฎีบทที่เกี่ยวข้องและงานวิจัยที่เกี่ยวข้องโดยมีรายละเอียดดังนี้

2.1 ทฤษฎีบทที่เกี่ยวข้อง

ทฤษฎีที่เกี่ยวข้องกับงานวิจัยฉบับนี้ประกอบด้วย โครงสร้างกุญแจสาธารณะ, รูปแบบการกำหนดสิทธิเข้าใช้งานแบบแบ่งตามบทบาทหน้าที่ (Role Base Access Control - RBAC) และ เทคนิคการทำงานของ XACML ซึ่งได้ถูกรวบรวมไว้ในส่วนนี้

2.1.1. โครงสร้างกุญแจสาธารณะ (Public Key Infrastructure)

โครงสร้างกุญแจสาธารณะ หรือ Public Key Infrastructure (PKI) เป็นสิ่งที่ช่วยให้ผู้ใช้ที่อยู่ในเครือข่ายที่ไม่มีความปลอดภัยอย่างเช่นอินเตอร์เน็ต ให้สามารถสร้างความปลอดภัยในการใช้งานเครือข่ายที่อาจจะมีการส่งข้อมูลหรือแลกเปลี่ยนข้อมูลทางด้านการเงินขึ้นมาได้ โดยผ่านการใช้การเข้ารหัสแบบที่มีการใช้คู่กุญแจแบบสาธารณะ และแบบส่วนตัว ที่ได้รับมาจากผู้มีอำนาจที่ไว้วางใจ (Trusted Authority) โครงสร้างกุญแจสาธารณะสามารถนำมาใช้ในการสร้างลายเซ็นต์อิเล็กทรอนิกส์ (Digital Signature) ที่สามารถใช้เพื่อระบุตัวตนของบุคคลหรือองค์กรได้ โดยโครงสร้างกุญแจสาธารณะมีคุณสมบัติที่ใช้ในการสร้างความปลอดภัยดังนี้

1. การยืนยันตัวบุคคล (Authentication)
2. การรักษาความลับของข้อมูล (Confidential)
3. การรักษาความครบถ้วนถูกต้องของข้อมูล (Integrity)
4. การไม่สามารถปฏิเสธความรับผิดชอบได้ (Non-Repudiation)

โครงสร้างกุญแจสาธารณะจะประกอบด้วนส่วนต่างๆ ดังต่อไปนี้

1. Certification Authority (CA) ทำหน้าที่ในการออกใบรับรองอิเล็กทรอนิกส์ และตรวจสอบใบรับรองอิเล็กทรอนิกส์ โดยใบรับรองอิเล็กทรอนิกส์จะมีข้อมูลในส่วนของกุญแจสาธารณะและข้อมูลเกี่ยวกับกุญแจสาธารณะ
2. Registration Authority (RA) ทำหน้าที่เป็นผู้ตรวจสอบคำขอใบรับรองอิเล็กทรอนิกส์ ก่อนที่จะให้ CA ทำการออกใบรับรองอิเล็กทรอนิกส์
3. บริการไดเร็กทรอรี่ ทำหน้าที่ในการเก็บใบรับรองอิเล็กทรอนิกส์และรายชื่อใบรับรองอิเล็กทรอนิกส์ที่ถูกยกเลิก
4. ระบบบริหารจัดการใบรับรองอิเล็กทรอนิกส์

ส่วนหลักการทำงานของการเข้ารหัส/ถอดรหัสโดยใช้กุญแจสาธารณะและกุญแจส่วนตัวคือ การสร้างคู่กุญแจสาธารณะและกุญแจส่วนตัวโดยใช้อัลกอริทึมอย่างเช่น RSA, DSA หรือ Elipstic Curve เป็นต้น โดยถ้าใช้กุญแจดอกใดดอกหนึ่งเข้ารหัสไว้ ก็จำเป็นจะต้องใช้กุญแจที่เป็นคู่กันอีกดอกหนึ่งถอดรหัสเท่านั้น ซึ่งโดยปกติแล้วกุญแจสาธารณะนั้นจะเปิดเผยให้กับผู้อื่นได้ทราบอยู่แล้วซึ่งจะอยู่ในรูปของใบรับรองอิเล็กทรอนิกส์ ที่จะเก็บอยู่ในบริการไดเร็กทรอรี่ แต่กุญแจส่วนตัวจะอยู่ที่เจ้าของเพียงผู้เดียวเท่านั้น ซึ่งสามารถดูความสัมพันธ์ได้จากตารางที่ 2.1 นี้ได้ว่าเหตุการณ์ใด ควรจะใช้กุญแจของใคร และประเภทใดในการเข้ารหัสหรือถอดรหัส

ตารางที่ 2.1 แสดงความสัมพันธ์ของเหตุการณ์และประเภทกุญแจที่ใช้ในการเข้ารหัสหรือถอดรหัส

เหตุการณ์	**ต้องใช้กุญแจของ**	**ประเภทของกุญแจ**
เมื่อต้องการจะส่งข้อความที่เข้ารหัสไว้	ผู้รับ	กุญแจสาธารณะ
เมื่อต้องการจะส่งข้อความที่มีลายเซ็นต์	ผู้ส่ง	กุญแจส่วนตัว
เมื่อต้องการจะถอดรหัสของข้อความที่เข้ารหัสไว้	ผู้รับ	กุญแจส่วนตัว
เมื่อต้องการจะถอดรหัสของข้อความที่มีลายเซ็นต์ (ใช้ในการยืนยันตัวบุคคลของผู้ส่งได้)	ผู้ส่ง	กุญแจสาธารณะ

2.1.2. การกำหนดสิทธิเข้าใช้งาน (Authorization)

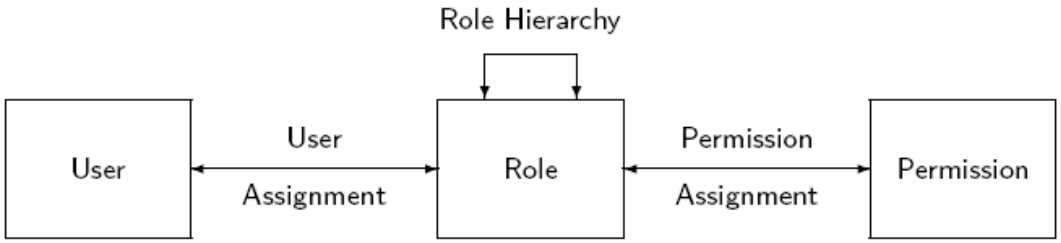
การกำหนดสิทธิเข้าใช้งานคือกระบวนการในการกำหนดสิทธิเข้าใช้งานทรัพยากรที่อาจจะอยู่ในรูปแบบไฟล์ แฟ้มข้อมูล หรือแอพพลิเคชั่น เป็นต้น ซึ่งสามารถแบ่งได้เป็น 3 ประเภทหลักๆ ได้แก่

1. ประเภทแบ่งตามการตัดสินใจ หรือ Discretionary Access Control (DAC) คือการควบคุมการเข้าถึงโดยเจ้าของทรัพยากรสามารถกำหนดสิทธิให้ผู้อื่นหรือกลุ่มต่างๆได้เอง ตัวอย่างเช่นระบบไฟล์ของ UNIX ที่ทุกๆ ไฟล์ในระบบจะมีเจ้าของ และเจ้าของจะสามารถกำหนดสิทธิให้กับผู้ใช้คนอื่นๆได้ นอกจากนี้ผู้ใช้ใน DAC ยังสามารถมอบหมายการควบคุมของไฟล์ให้ผู้ใช้คนอื่นได้อีกด้วย และ DAC ยังมีการใช้กันอย่างกว้างขวางในการบังคับนโยบายการเข้าถึงในระบบปฏิบัติการต่างๆ

2. ประเภทแบ่งตามการรับมอบอำนาจ หรือ Mandatory Access Control (MAC) คือการกำหนดสิทธิในลักษณะของการติดป้ายบอกระดับความปลอดภัยของทรัพยากรไว้ โดยผู้ใช้จะสามารถอ่านข้อมูลของทรัพยากรได้ก็ต่อเมื่อผู้ใช้มีระดับความปลอดภัยมากกว่าหรือเท่ากับระดับความปลอดภัยของทรัพยากร และผู้ใช้จะสามารถเขียนข้อมูลของทรัพยากรได้ก็ต่อเมื่อผู้ใช้มีระดับความปลอดภัยน้อยกว่าหรือเท่ากับระดับความปลอดภัยของทรัพยากร ซึ่ง MAC จะมีการใช้ในระบบที่เกี่ยวข้องกับข้อมูลที่มีความสำคัญเป็นอย่างมาก เช่นในวงการทหาร เป็นต้น

3. ประเภทแบ่งตามบทบาทหน้าที่ หรือ Role Based Access Control (RBAC) จะมีส่วนประกอบ 3 ส่วนคือ ผู้ใช้(User) บทบาท(Role) และสิทธิ(Permission) ซึ่ง RBAC จะไม่ได้กำหนดสิทธิให้กับผู้ใช้โดยตรง แต่จะกำหนดสิทธิให้กับบทบาทว่าสามารถมีสิทธิใดบ้าง โดยผู้ใช้จะถูกกำหนดบทบาทให้อย่างน้อย 1 บทบาท หรือมากกว่า โดยบทบาทสามารถสืบทอดได้ (inherited) และให้ส่วนของการกำหนดสิทธิสามารถทำการเปลี่ยนแปลงได้ง่าย โดยจะส่งผลให้กับผู้ใช้ทุกคนภายใต้บทบาทที่ได้ทำการเปลี่ยนแปลง ซึ่งในภาพที่ 2.1 นี้จะแสดงถึงลักษณะการทำงานของ Role Based Access Control

ภาพที่ 2.1 ลักษณะการทำงานของ Role Based Access Control (Axel Kern and Claudia Walhorn, 2005, p. 131)



ซึ่งเมื่อผู้วิจัยได้พิจารณาถึงความเหมาะสมของประเภทการกำหนดสิทธิเข้าใช้งาน ผู้วิจัยเห็นควรว่างานวิจัยนี้ มีความเหมาะสมกับการกำหนดสิทธิเข้าใช้งานประเภทแบ่งตามบทบาทหน้าที่ เนื่องจากสามารถบริหารจัดการในเรื่องของการกำหนดสิทธิให้ผู้ใช้ได้ง่ายกว่าประเภทอื่น จึงเหมาะกับระบบที่สนับสนุนผู้ใช้จำนวนมากเช่นระบบที่ต้องใช้งานแอพพลิเคชั่นข้ามองค์กร เป็นต้น

2.1.3. เทคนิคการทำงานของ XACML

XACML(Extensible Access Control Markup Language) คือภาษามาตรฐานของ OASIS (OASIS, 2005) เพื่อใช้ในการกำหนดสิทธิในการเข้าใช้งานหรือนโยบายในการกำหนดการเข้าถึง โดย XACML เป็นภาษาที่มีความยืดหยุ่น โดยภาษาสนับสนุนรูปแบบข้อมูล(data types), ฟังก์ชั่น (functions) และวิธีในการรวมกฎแบบเรียบง่ายหรือซับซ้อน นอกจากนี้ XACML ยังมีภาษาสำหรับตัดสินใจการเข้าถึง โดยใช้เพื่อแทนการร้องขอทรัพยากรขณะทำงาน นโยบายจะถูกติดตั้งเพื่อปกป้องทรัพยากร และฟังก์ชั่นก็จะทำการเปรียบเทียบแอตทริบิวต์ของคำร้องขอกับกฎเพื่อทำการตัดสินใจว่าจะอนุญาตหรือไม่อนุญาตให้ใช้ทรัพยากร

ในการกำหนดนโยบายของการเข้าถึงทรัพยากรของ XACML จะประกอบไปด้วย 4 ส่วนหลักได้แก่

Attributes และ Functions โดย Attributes คือคุณสมบัติของ subjects, resources, actions, หรือ environments ที่จะใช้ในการกำหนดเงื่อนไขโดยมีรูปแบบของข้อมูลเช่น String, Time, Boolean, Double, and AnyURI เป็นต้น ในลักษณะเดียวกัน Functions คือตัวปฏิบัติการ

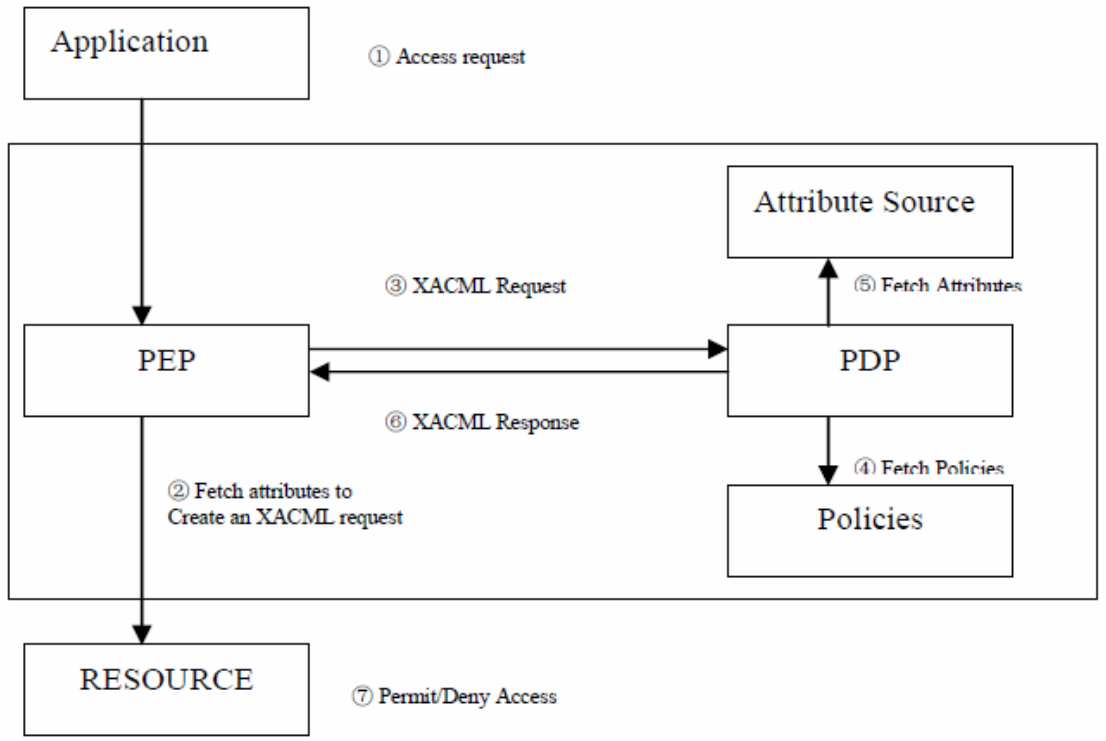
ที่เป็นไปได้เพื่อใช้ในการกำหนดเงื่อนไขเช่น String-Equal, Greater-Then, Date-Equal, String-Is-In, and AnyURI-One-And-Only เป็นต้น

Rule คือองค์ประกอบ (element) พื้นฐานของนโยบาย จะใช้เพื่อระบุเงื่อนไขของการเข้าใช้งานของนโยบายที่ได้สร้างขึ้น โดย rule จะประกอบด้วย Target เพื่อระบุกฎของคำร้องขอที่ต้องการจำกัดสิทธิว่าจะอนุญาต (Permit) หรือ ไม่อนุญาต (Deny) และเงื่อนไข (Condition) ที่ต้องการเมื่อนำกฎมาใช้กับคำร้องขอ

Policies คือนโยบายที่มีการรวมกับ Rule ที่มีจำนวนเท่ากับหนึ่งหรือมากกว่าหนึ่ง โดยนโยบายจะประกอบไปด้วย Target (ทำหน้าที่เหมือนกันกับ Target ที่ระบุไว้ใน Rule) กลุ่มของกฎ และ วิธีการในการรวมกฎ (Rule Combination Algorithm)

Policy Set คือกลุ่มของนโยบายที่มีการรวมกับนโยบายที่มีจำนวนมากกว่าหนึ่ง โดยจะใช้เมื่อต้องการควบคุมการเข้าถึงจากผู้ที่เกี่ยวข้องที่หลากหลาย โดยจะประกอบด้วย Target, กลุ่มของนโยบาย และ วิธีการในการรวมนโยบาย (Policy Combination Algorithm)

ภาพที่ 2.2 แสดงภาพรวมการทำงานของ XACML (Han Tao, 2005, p. 1141)



โดยในภาพที่ 2.2 แสดงภาพรวมการทำงานของ XACML และ XACML ไม่ได้มีเพียงแค่ภาษาสำหรับกำหนดนโยบาย แต่ว่ายังรวมถึงวิธีการในการประเมินนโยบายบนพื้นฐานของค่าที่เกี่ยวข้องกับแอตทริบิวต์ของนโยบายกับคำร้องขอด้วย กระบวนการในการประเมินและบังคับใช้นโยบายในการควมคุมการเข้าถึงมีพื้นฐานอยู่บน 3 องค์ประกอบต่อไปนี้

1. Policy Decision Point (PDP) คือองค์ประกอบที่ทำหน้าที่ในการคำนวนนโยบายที่เหมาะสมและส่งผลลัพท์ของการตัดสินใจในการอนุญาตเข้าใช้งาน
2. Policy Enforcement Point (PEP) คือองค์ประกอบที่บังคับใช้การอนุญาตเข้าใช้งาน
3. Context Handler คือองค์ประกอบที่ทำหน้าที่ในการเปลี่ยนคำร้องขอจากรูปแบบเดิมมายังในรูปแบบของ XACML และเปลี่ยนจาก XACML มาเป็นรูปแบบเดิมที่ PEP สนับสนุน

2.2 งานวิจัยที่เกี่ยวข้อง

ในส่วนของงานวิจัยและบทความที่เกี่ยวข้องกับวิทยานิพนธ์ฉบับนี้ แบ่งออกเป็น 4 ส่วนด้วยกัน ประกอบไปด้วยงานวิจัยที่เกี่ยวกับการยืนยันตัวบุคคล, งานวิจัยที่เกี่ยวกับการประยุกต์ใช้ระบบหลายตัวแทน, งานวิจัยที่เกี่ยวกับการประยุกต์ใช้ XACML และงานวิจัยที่เกี่ยวกับการใช้งานแอพพลิเคชั่นข้ามองค์กร

2.2.1. งานวิจัยที่เกี่ยวกับการยืนยันตัวบุคคล

งานวิจัยที่เกี่ยวข้องกับการยืนยันตัวบุคคลในระบบเครือข่ายและอินเตอร์เน็ตบนพื้นฐานการประยุกต์ใช้ ได้มีการทำโดยเทคนิคจำนวนมากมาย (Federal Information Processing Standards Publication 190, 1994; Federal Information Processing Standards Publication 112, 1985; Martha E. Haykin and Robert B.J. Warna, 1988; Dray, Smid and Warnar, 1989) เช่น การยืนยันตัวบุคคลโดยใช้รหัสผ่าน การยืนยันตัวบุคคลโดยใช้โทเคน การยืนยันตัวบุคคลโดยใช้ข้อมูลทางชีวภาพ และการผสมผสานวิธีการดังกล่างข้างต้น

จากการสำรวจพบว่ามีงานวิจัยอยู่เพียงจำนวนน้อยที่ออกแบบมาสำหรับการยืนยันตัวบุคคลสำหรับหลายแอพพลิเคชั่น และการจัดการความปลอดภัยสำหรับหลายแอพพลิเคชั่น

ใน (Markantonakis and Mayes, 2004) เป็นการใช้โปรโตคอลการเข้ารหัสถอดรหัสบนพื้นฐานของกุญแจสาธารณะ โดยใช้การผสมผสานของกุญแจสาธารณะร่วมกับ กุญแจลับ และกุญแจ Diffie-Hellman ในการสร้างความปลอดภัยของโปรโตคอล มีจุดประสงค์เพื่อรองรับสมาร์ทการ์ดแบบหลายแอพพลิเคชั่น โดยงานวิจัยนี้เน้นที่การสร้างโปรโตคอลความปลอดภัยบนพื้นฐานของโครงสร้างกุญแจสาธารณะ การใช้สมาร์ทการ์ดแบบหลายแอพพลิเคชั่นมีประโยชน์เพื่อสนับสนุนการใช้สมาร์ทการ์ดที่บรรจุกุญแจ สำหรับแอพพลิเคชั่นใดๆ ที่ต้องการความปลอดภัย อย่างไรก็ตามในงานวิจัยนี้ยังไม่ได้กล่าวถึงวิธีการสำหรับการประยุกต์ใช้กับสภาพแวดล้อมที่หลากหลาย

จุดมุ่งหมายของงานของ (Dae-Hee Seo, Im-Yeong Lee, Soo-Young Chae and Choon-Soo Kim, 2003) เป็นแรงบันดาลใจต่องานวิจัยชิ้นนี้ โดยจุดมุ่งหมายของผู้แต่งต้องการนำเสนอการยืนยันตัวบุคคลโดยใช้โบรกเกอร์ (Broker Authentication) ซึ่งรวมการใช้ ระบบการเข้าใช้งานเพียงครั้งเดียวและระบบหลายตัวแทน เพื่อตอบสนองความต้องการที่จำเป็นต่อความปลอดภัย รวมไปถึงการรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล

(Integrity) และการไม่สามารถปฏิเสธความรับผิดชอบ (Non-Repudiation) ปัจจัยระบบและโปรโตคอลของการสร้างตัวแทนได้นำเสนอเกี่ยวกับการอนุญาตตามระดับอำนาจของบริการที่สัมพันธ์กัน อย่างไรก็ตามหน้าที่ที่ชัดเจนของการใช้ตัวแทนในการกำหนดสิทธิเข้าใช้งานยังไม่ได้กล่าวไว้ และรูปแบบการยืนยันตัวบุคคลแบบตัวแทนยังมีปัญหาอยู่มาก เช่นการบริหารจัดการผู้ใช้จำนวนมากที่ไม่ได้มีการระบุตัวตน ช่องโหว่เกี่ยวกับการไม่สามารถปฏิเสธความรับผิดชอบและการเปิดเผยชื่อผู้ใช้และรหัสผ่าน

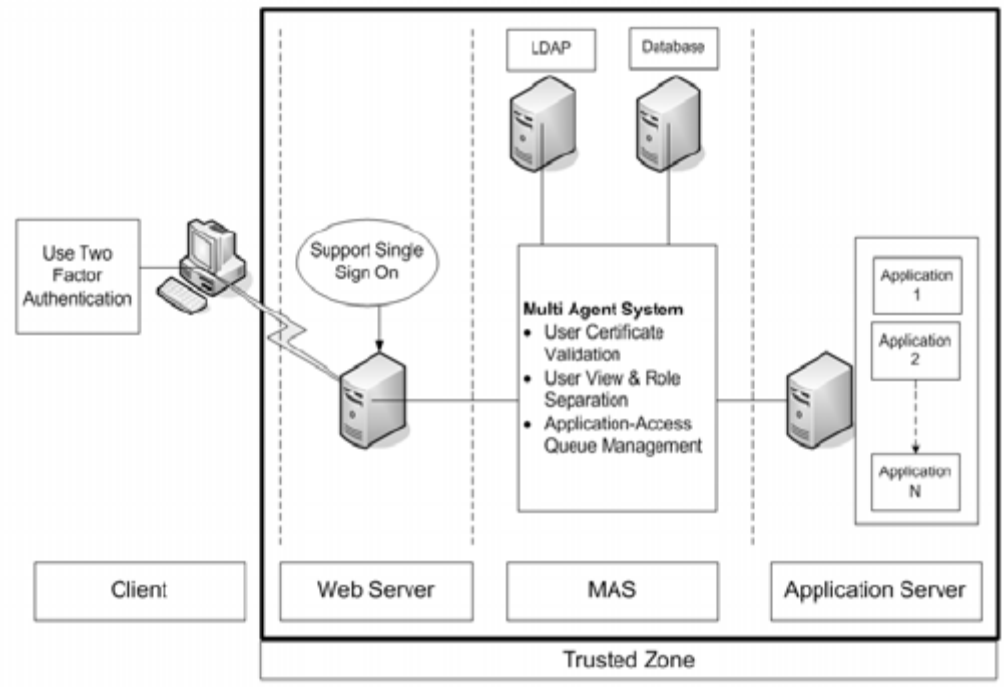
แต่ในงานวิจัยของผู้วิจัยนี้จะเน้นการใช้โครงสร้างกุญแจสาธารณะแบบเต็มรูปแบบโดยใช้การยืนยันตัวบุคคลด้วยสององค์ประกอบ (Two-Factor Authentication) และการเข้าใช้งานเพียงครั้งเดียว (Single Sign On) ผู้วิจัยมีจุดประสงค์เพื่อนำเสนอเทคโนโลยีโครงสร้างกุญแจสาธารณะ ซึ่งผู้บริการออกใบรับรองอิเล็กทรอนิกส์ (Certification Authority หรือ CA) ถือเป็นส่วนสำคัญในการสร้างกุญแจคู่และใบรับรองอิเล็กทรอนิกส์สำหรับผู้ใช้ เพื่อที่จะสนับสนุนการให้บริการทางด้านความปลอดภัยพร้อมกับการยืนยันตัวบุคคล โดยผู้ใช้ในสภาพแวดล้อมที่ผู้วิจัยทดสอบนั้นจำเป็นต้องมีการระบุตัวตนโดย CA และต้องมีกุญแจคู่พร้อมด้วยใบรับรองอิเล็กทรอนิกส์ที่บรรจุไว้อย่างปลอดภัยในรูปแบบของสมาร์ทการ์ด หรือ โทเคน และอีกส่วนที่ผู้วิจัยต้องการเน้นคือการประยุกต์ใช้ระบบหลายตัวแทนเพื่อควบคุมการยืนยันตัวบุคคลที่ปลอดภัยและสามารถใช้งานโดยผู้ใช้จำนวนมากกับหลายแอพพลิเคชั่นได้อย่างยืดหยุ่น

2.2.2. งานวิจัยที่เกี่ยวกับการประยุกต์ใช้ระบบหลายตัวแทนเพื่อสนับสนุนการใช้งานหลายแอพพลิเคชั่น

ระบบหลายตัวแทนคือการที่มีตัวแทนหลายตัวทำงานอย่างอัตโนมัติและอย่างอิสระโดยใช้ข้อมูลภายใน หรือเป็นไปได้ที่อาจจะมีการสื่อสารกับสิ่งอื่น โดยใน (Fugkeaw, Manpanpanich and Juntapremjitt, 2007a) ได้มีการนำระบบหลายตัวแทนมาประยุกต์ใช้ในการทำการยืนยันตัวบุคคล ร่วมกับโครงสร้างกุญแจสาธารณะ โดยใช้ระบบหลายตัวแทนเป็นตัวจัดการงานในหลายๆ ส่วน โดยแบ่งตัวแทน (Agent) ออกตามประเภทต่างๆ ดังต่อไปนี้

1. UA ทำหน้าที่เสมือนเป็นผู้ใช้งานและทำหน้าที่ตรวจสอบตัวบุคคลของผู้ใช้
2. AA ทำหน้าที่เสมือนเป็นแอพพลิเคชั่นและช่วยบริหารจัดการลำดับคำร้องขอเพื่อการเข้าใช้งานแอพพลิเคชั่น

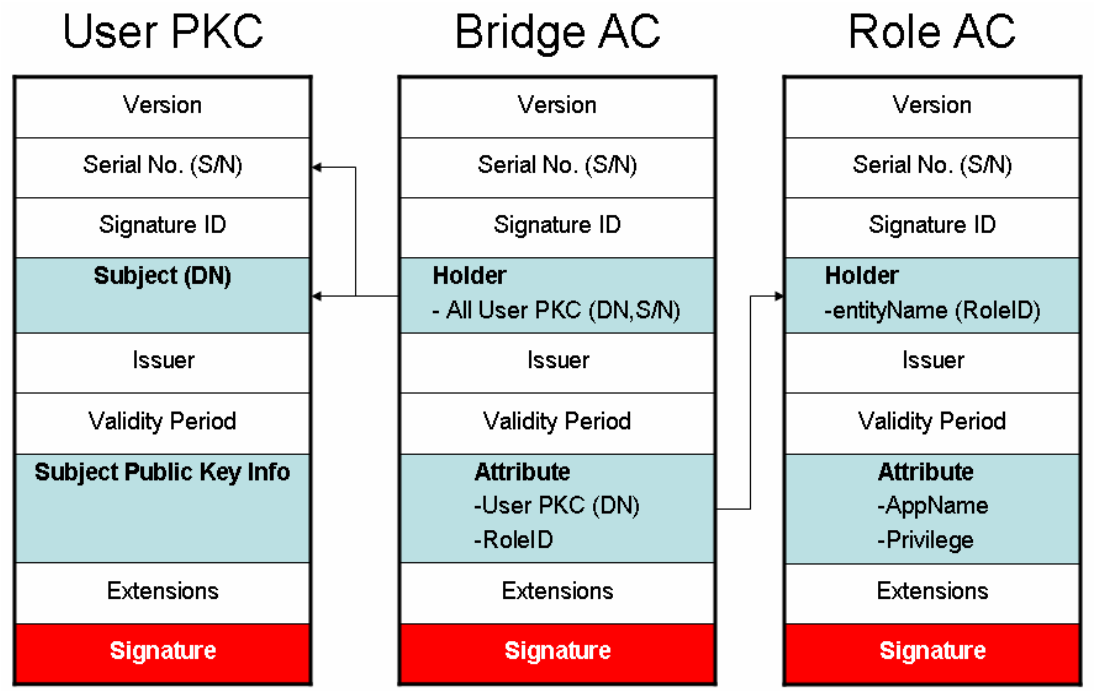
ภาพที่ 2.3 แสดงโครงร่างการประยุกต์ใช้ระบบหลายตัวแทนเพื่อใช้ในการยืนยันตัวบุคคล (Fugkeaw, Manpanpanich and Juntapremjitt, 2007a)



โดยในภาพที่ 2.3 จะแสดงโครงสร้างของระบบหลายตัวแทนที่ผู้แต่งได้นำเสนอไว้ ซึ่งจะมีการแบ่งออกเป็น 4 ส่วนได้แก่ส่วนของผู้ใช้ (Client), ส่วนของเว็บเซริฟเวอร์ (Web Server), ส่วนของระบบหลายตัวแทน (MAS) และส่วนของแอพพลิเคชั่นเซริฟเวอร์ (Application Server)

อีกหนึ่งงานวิจัยที่มีการประยุกต์ใช้ระบบหลายตัวแทนคือ (Fugkeaw, Manpanpanich and Juntapremjitt, 2007b) โดยมีแนวคิดที่ว่าจะนำการยืนยันตัวบุคคล การกำหนดสิทธิเข้าใช้งาน การตรวจสอบบันทึกเหตุการณ์ สำหรับหลายแอพพลิเคชั่น และหลายผู้ใช้ โดยใช้เทคนิคของโครงสร้างกุญแจสาธารณะและระบบหลายตัวแทนเป็นสิ่งที่ช่วยสนับสนุนงานวิจัยนี้ โดยในการยืนยันตัวบุคคลจะใช้ใบรับรองของผู้ใช้ในการยืนยันตัวบุคคลของผู้ใช้ (User Certificate) และในส่วนของการกำหนดสิทธิการเข้าใช้งานจะใช้ใบรับรองแอตทริบิวต์ประเภทที่แบ่งตามบทบาท (Role Attribute Certificate) และยังใช้ใบรับรองแอตทริบิวต์แบบสะพาน (Bridge Attribute Certificate) เพื่อเป็นกลไกในการจัดการจับคู่ระหว่างผู้ใช้กับบทบาทที่กำหนดไว้ ดังที่ได้แสดงไว้ในภาพที่ 2.4 ซึ่งจะเป็นการสร้างความยืดหยุ่นเมื่อมีการเปลี่ยนแปลงใบรับรองของผู้ใช้ ใบรับรองแอตทริบิวต์ประเภทที่แบ่งตามบทบาทมากยิ่งขึ้น

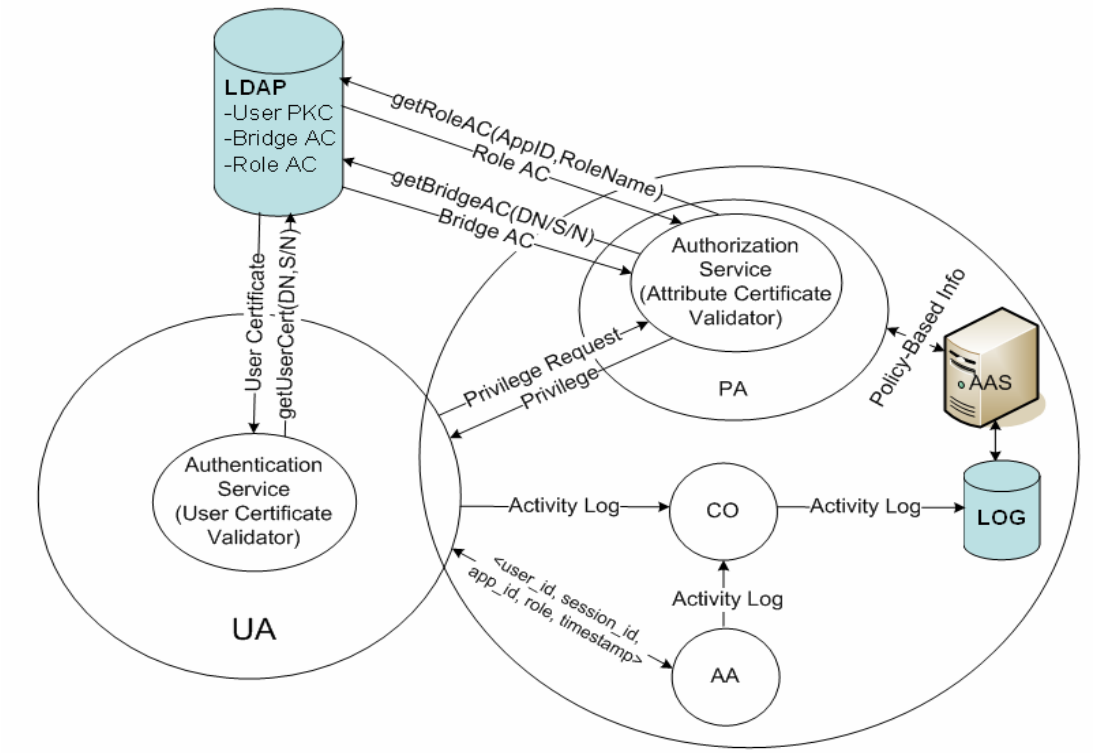
ภาพที่ 2.4 แสดงการจับคู่ของ User Certificate, Bridge AC และ Role AC (Fugkeaw, Manpanpanich and Juntapremjitt, 2007b, p. 736)



นอกจากนี้ยังมีการแบ่งประเภทของ Agent ออกตามประเภทต่างๆ ดังต่อไปนี้

1. User Agent (UA) ทำหน้าที่เสมือนเป็นผู้ใช้งานและทำหน้าที่ตรวจสอบตัวบุคคลของผู้ใช้
2. Application Agent (AA) ทำหน้าที่เสมือนเป็นแอพพลิเคชั่นและช่วยบริหารจัดการลำดับคำร้องขอเพื่อการเข้าใช้งานแอพพลิเคชั่น
3. Policy Agent (PA) ทำหน้าที่ในการตรวจสอบสิทธิการใช้งานของแอพพลิเคชั่น โดยคำนวนจากสิทธิของบทบาทที่ได้กำหนดไว้แล้ว คู่กับพฤติกรรมการใช้งานของผู้ใช้
4. Collector Agent (CO) ทำหน้าที่เป็นตัวกลางระหว่าง Agent ต่างๆ กับ Log Server ในการเก็บบันทึกข้อมูลการทำงานของ Agent ทุกตัว

ภาพที่ 2.5 แสดงการทำงานของระบบหลายตัวแทน (Fugkeaw, Manpanpanich and Juntapremjitt, 2007b, p. 735)



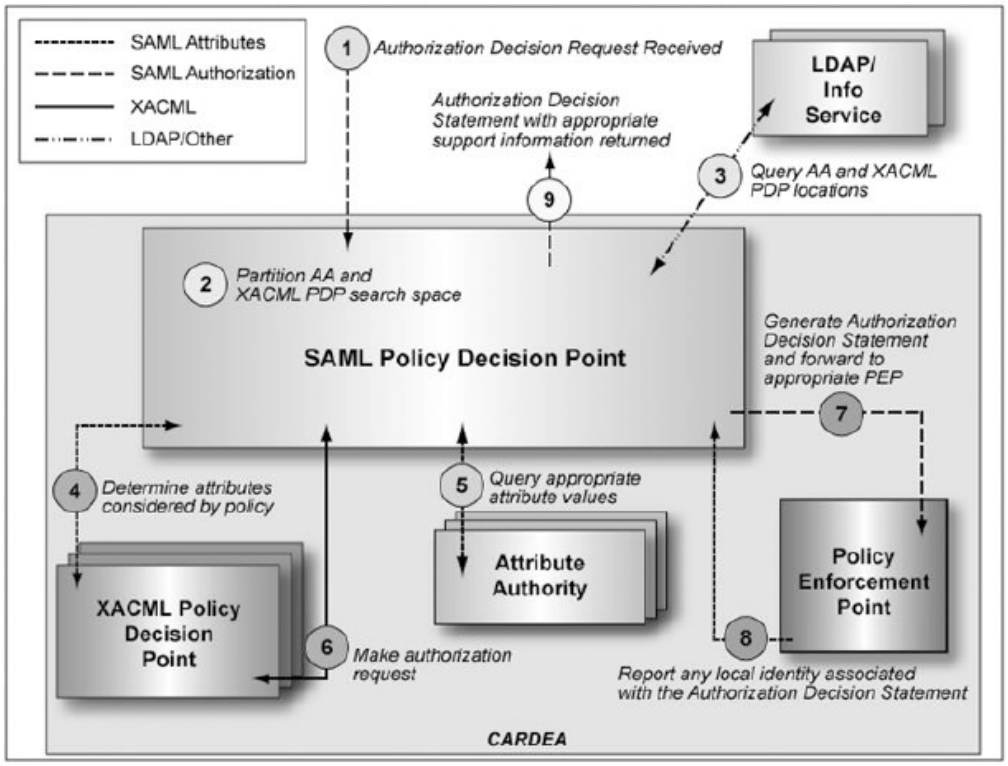
โดยในภาพที่ 2.5 จะแสดงการทำงานของระบบหลายตัวแทนที่ผู้แต่งได้นำเสนอไว้ ซึ่งแสดงให้เห็นถึงการติดต่อสื่อสารกันภายในของ Agent แต่ละแบบ

ซึ่งจะเห็นได้ว่าในระบบดังกล่าวข้างต้นยังไม่ได้กล่าวถึงการรองรับการทำงานจากหลายองค์กรหรือจากระบบแบบกระจายไว้ อีกทั้งระบบที่นำเสนอยังคงสนับสนุนการกำหนดสิทธิของผู้ใช้ในรูปแบบของ attribute certificate เท่านั้น จากจุดนี้จึงทำให้ผู้วิจัยต้องการให้ระบบหลายตัวแทนที่จะนำเสนอนี้สามารถสนับสนุนการทำงานแบบระบบกระจาย (Distributed Systems) รวมทั้งสนับสนุนและจัดการนโยบายการควบคุมการเข้าถึงที่มีความหลากหลายขององค์กรได้ เพื่อให้สามารถทำงานข้ามองค์กรได้และเพื่อให้สอดคล้องกับความต้องการทางธุรกิจในปัจจุบัน

2.2.3. งานวิจัยที่เกี่ยวกับการประยุกต์ใช้ XACML

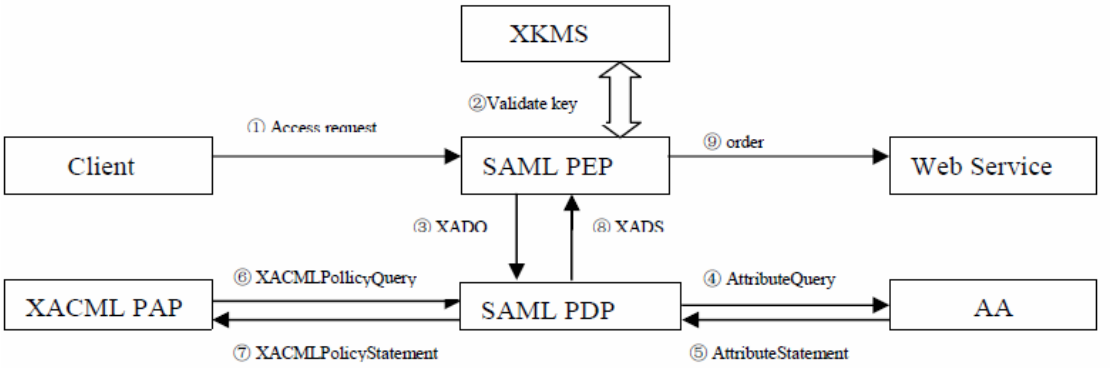
งานวิจัยของ (Rebekah Lepro, 2003) ได้มีการนำเสนอระบบกำหนดการเข้าถึงแบบกระจาย (Distributed Authorization System) โดยใช้ชื่อโครงการนี้ว่า Cardea ซึ่งเป็นส่วนหนึ่งของ NASA Information Power Grid ที่ซึ่งได้มีการนำ SAML และ XACML มาใช้ในการควมคุมการเข้าถึงการทำงานของระบบแบบกระจาย เพื่อต้องการสร้างความปลอดภัยและตรวจสอบการทำงานของสิ่งแวดล้อมแบบกระจายสำหรับการเข้าใช้งานทรัพยากรข้ามโดเมนอย่างยืดหยุ่น Cardea ถูกพัฒนาด้วยภาษา Java และส่วนประกอบของระบบประกอบด้วย SAML Policy Decision Point, Attribute Authorities, Policy Enforcement Points, Information Service/LDAP, XACML context handler, XACML Policy Administration Points, XACML Policy Decision Point ดังแสดงในภาพที่ 2.6 แต่ในงานวิจัยนี้ได้มีการกำหนดสิทธิเข้าใช้งานด้วย XACML เพียงรูปแบบเดียว ซึ่งจะทำให้ระบบที่มีการกำหนดสิทธิในรูปแบบอื่นๆ ที่ไม่ได้อยู่ในรูปแบบ XACML ก็จะทำให้ไม่สามารถใช้งานกับระบบนี้ได้

ภาพที่ 2.6 โครงสร้างการทำงานของ Cardea (Rebekah Lepro, 2003, p.10)



และในงานวิจัยของ (Han Tao, 2005) โดยในงานวิจัยนี้มีการนำ XACML มาใช้ในการควมคุมการเข้าถึงของ Web Service โดยเป็นการใช้ Security Assertion Markup Language หรือ SAML สำหรับป้องกันการส่งข้อมูลในรูปแบบของคำร้องและผลตอบของ XACML ซึ่งในภาพที่ 2.7 ได้แสดงรูปแบบการควบคุมการเข้าถึงสำหรับ Web Service ด้วย XACML แต่ในงานวิจัยนี้ได้มีการกำหนดสิทธิเข้าใช้งานด้วย XACML เพียงรูปแบบเดียว ซึ่งจะทำให้ระบบที่มีการกำหนดสิทธิในรูปแบบอื่นๆ ที่ไม่ได้อยู่ในรูปแบบ XACML ก็จะทำให้ไม่สามารถใช้งานกับระบบนี้ได้ด้วยเช่นกัน

ภาพที่ 2.7 แสดงรูปแบบการควบคุมการเข้าถึงสำหรับ Web Service ด้วย XACML (Han Tao, 2005, p. 1142)



2.2.4. งานวิจัยที่เกี่ยวกับการสนับสนุนการใช้งานแอพพลิเคชั่นข้ามองค์กร

ในสภาพแวดล้อมที่มีการใช้งานแอพพลิเคชั่นข้ามองค์กร กลไกที่มีประสิทธิภาพสำหรับการสนับสนุนการระบุกลุ่มคนหลายๆ กลุ่มที่เกี่ยวข้องและการจัดสรรหลายๆ แอพพลิเคชั่นเป็นสิ่งจำเป็น การควบคุมการเข้าถึง เป็นตัวที่ทำหน้าที่ตัดสินใจและใช้บริหารจัดการทรัพยากรให้อย่างเหมาะสม เช่น การประยุกต์ใช้ระบบขององค์กร โดยทั่วไปแล้วแนวทางในการอนุญาตให้ใช้งานจะมีการรวมการยืนยันตัวบุคคลด้วยเพื่อป้องกันการการเข้าถึงทรัพยากรจากผู้ที่ไม่ได้รับอนุญาต ซึ่งสิ่งนี้เป็นสิ่งที่ง่ายและมีความเป็นไปได้สำหรับควบคุมการตัดสินใจอย่างรวดเร็ว อย่างไรก็ตามเมื่อมีจำนวนผู้ใช้จำนวนมากขึ้น วิธีการนี้ก็จะมีการบริหารจัดการที่ซับซ้อนขึ้น ดังนั้นจึงได้มีการนำเสนอวิธีการในการควบคุมการเข้าถึงโดยแบ่งตามบทบาท หรือ Role Based Access Control (RBAC) ซึ่งมีการจัดการควบคุมการเข้าถึงได้อย่างมีประสิทธิภาพสำหรับผู้ใช้

จำนวนมากเพราะสามารถอนุญาตให้ใช้งานได้ตามบทบาทหน้าที่ มากกว่าที่จะให้ใช้งานได้ตามแต่ละบุคคล ซึ่งโดยปกติแล้วจำนวนบทบาทมักจะมีจำนวนน้อยกว่าผู้ใช้อยู่แล้ว จึงทำให้สามารถบริหารจัดการบทบาทได้อย่างสะดวกมากกว่าด้วย

สำหรับงานวิจัยที่เกี่ยวกับการนำใบรับรองแอตทริบิวต์มาประยุกต์ใช้เพื่อสนับสนุนการใช้งานแอพพลิเคชั่นข้ามองค์กร ก็ได้มีการนำเสนออยู่หลายงานวิจัยด้วยกัน เช่น (Thompson, Johnston, Mudumbai, Hoo, Jackson, and Essiari, 1999; Chadwick, Otenko, and Ball, 2003; Otenko and Chadwick, 2002). โดยในงานวิจัยของ (Thompson and others, 1999) ได้มีการออกใบรับรองอิเล็กทรอนิกส์ให้กับผู้ใช้เพื่อใช้ในการยืนยันตัวบุคคล และได้มีการนำเสนอกลไกที่ชื่อว่า Akenti ในการกำหนดสิทธิเข้าใช้งานทรัพยากรแบบกระจาย (Distributed Resource) โดยใช้ใบรับรองแอตทริบิวต์ และในงานวิจัยของ (Chadwick, Otenko, and Ball, 2003; Otenko and Chadwick, 2002) ผู้แต่งได้พัฒนาระบบที่เรียกว่า โครงการ PERMIS ที่สามารถควบคุมการเข้าถึงโดยแบ่งตามบทบาทโดยมีพื้นฐานมาจากใบรับรองแอตทริบิวต์ X.509 ซึ่งโครงการ PERMIS ได้มีการประยุกต์ X.509 Privilege Management Infrastructure (PMI) เพื่อทำให้ระบบบริหารจัดการความน่าเชื่อถือของบทบาทและการจัดสรรบทบาทให้ผู้ใช้มีประสิทธิภาพมากขึ้น อย่างไรก็ตามในงานวิจัยเหล่านี้ไม่ได้กล่าวถึงการยืนยันตัวบุคคลเพื่อการเข้าใช้งานเพียงครั้งเดียว (Single Sign On - SSO) และการบริหารจัดการรูปแบบการกำหนดสิทธิเข้าใช้งานในหลายๆ รูปแบบ