การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพื่อความมั่นคงปลอดภัยในเว็บเซอร์วิส

นางสาวศิริรัตนา นิลน้อย

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
พ.ศ. 2556

การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพื่อความมั่นคงปลอดภัยในเว็บเซอร์วิส

นางสาวศิริรัตนา นิลน้อย วท.บ. (วิทยาการคอมพิวเตอร์)

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
ปีการศึกษา 2556

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการสอบวิทยานิพนธ์
(ผศ. ดร.พรชัย มงคลนาม)

..... กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์
(ผศ. ดร.เกรียงไกร ปอแก้ว)

..... กรรมการ
(ผศ. ดร.ชลเมธ อาปณิกานนท์)

..... กรรมการ
(รศ. ดร.พีระพนธ์ โสพัศสถิตย์)

หัวข้อวิทยานิพนธ์	การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพื่อความมั่นคงปลอดภัยในเว็บเซอร์วิส
หน่วยกิต	12
ผู้เขียน	นางสาวศิริรัตนา นิลน้อย
อาจารย์ที่ปรึกษา	ผศ. ดร.เกรียงไกร ปอแก้ว
หลักสูตร	วิทยาศาสตรมหาบัณฑิต
สาขาวิชา	เทคโนโลยีสารสนเทศ
คณะ	เทคโนโลยีสารสนเทศ
พ.ศ.	2556

บทคัดย่อ

เนื่องจากในปัจจุบันเว็บเซอร์วิสมีบทบาทมากในเรื่องการแลกเปลี่ยนข้อมูลกันระหว่างเครื่องคอมพิวเตอร์ผ่านระบบเครือข่าย การรักษาความปลอดภัยในการเข้าถึงข้อมูลที่รับส่งผ่านเว็บเซอร์วิสนั้นจึงเป็นเรื่องที่สำคัญ ดังนั้นจึงมีการศึกษาวิจัยเรื่องการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสในด้านการเข้าถึงข้อมูล โดยงานวิจัยนี้ให้ความสนใจในขั้นตอนกระบวนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่มีกระบวนการในการป้องกันการโจมตีแบบ Replay Attack โดยมีกระบวนการนำค่า Nonce เข้ามาใช้ประกอบในการพิสูจน์ตัวตน

โดยภาพรวมงานวิจัยนี้จะมุ่งเน้นศึกษาในด้านการเพิ่มประสิทธิภาพของขั้นตอนการพิสูจน์ตัวตนเว็บเซอร์วิสด้วยยูสเซอร์เนมเคน งานวิจัยนี้ได้เสนอแนวคิดการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่มีการเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลโดยเก็บข้อมูลเพิ่มขึ้นเรื่อยๆในช่วงเวลาที่กำหนด และเสนอการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่หลีกเลี่ยงการเก็บค่า Nonce ทุกค่าที่ได้รับไว้ในฐานข้อมูล อีกทั้งได้ดำเนินการทดสอบเปรียบเทียบค่าเวลาที่ใช้ในการประมวลผลการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนของเว็บเซอร์วิสทั้งสองรูปแบบ วัดค่าและเปรียบเทียบเวลาที่ใช้ประมวลผลการทำรายการการเรียกใช้บริการเว็บเซอร์วิสตามจำนวนการทำรายการและเวลาที่กำหนด

คำสำคัญ : การพิสูจน์ตัวตน / ความมั่นคงปลอดภัย / เว็บเซอร์วิส / โซพเมสเซจ / ยูสเซอร์เนมโทเคน

Thesis Title	Secure Web Services Authentication with UsernameToken
Thesis Credits	12
Candidate	Miss Sirirattana Nilnoi
Thesis Advisor	Asst. Prof. Dr. Kriengkrai Porkaew
Program	Master of Science
Field of Study	Information Technology
Faculty	School of Information Technology
Academic Year	2013

Abstract

Web services are currently very active in the exchange of information between computers over a network. Security of data access transmitted over the web services is an important issue. Therefore, the thesis focuses on the identification process with UsernameToken that has a process to prevent the replay attack from malicious users. The Nonce value is also applied in the identification process.

Overall, this thesis focuses on the optimization of web services authentication with UsernameToken. It proposes the authentication with UsernameToken that all of the Nonce value is collected and evaluated in the database by increasing the storage within the allocated time as well as the authentication with UsernameToken that avoids storing all of the Nonce value in the database. In so doing, the researcher measured and compared the time it took to process the identification with UsernameToken of both web services transactions based on the number of transaction and time limit.

Keywords : Authentication / Security / SOAP Message / UsernameToken / Web Services

กิตติกรรมประกาศ

ข้าพเจ้าในฐานะผู้วิจัยขอกราบขอบพระคุณ ผศ.ดร.เกรียงไกร ปอแก้ว อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งท่านได้สละเวลาให้ความรู้ คำปรึกษาพร้อมทั้งข้อเสนอแนะต่างๆที่เกี่ยวข้องกับงานวิจัย ซึ่งส่งผลให้งานวิจัยนี้สำเร็จลุล่วงไปได้ด้วยดี ผู้วิจัยขอกราบขอบพระคุณ ผศ.ดร. ชลเมธ อาปณิกานนท์, ผศ. ดร. พรชัย มงคลนาม และ รศ.ดร. พีรพนธ์ โสพัศสถิตย์ ที่ท่านได้กรุณาเป็นคณะกรรมการในการสอบหัวข้อวิทยานิพนธ์และสอบวิทยานิพนธ์ขั้นสุดท้าย ผู้วิจัยขอขอบคุณ คุณนิรุทธ์ รวยรื่น คุณธีรเดช โอทกานนท์ และ คุณกำพล ฟ้าภิญโญ ที่ช่วยให้ความรู้ คำแนะนำและสนับสนุนในการการวิจัยครั้งนี้

สุดท้ายผู้วิจัยขอกราบขอบพระคุณอย่างสูงต่อคุณบิดา มารดา ที่ได้มอบชีวิต และอบรมเลี้ยงดู สนับสนุน ช่วยเหลือผู้วิจัยในทุกๆด้านโดยตลอด สุดท้ายขอขอบคุณครูบาอาจารย์ทุกท่านที่ให้วิชาความรู้ ญาติมิตรเพื่อนทุกท่านที่ให้การสนับสนุนช่วยเหลือ ความดีอันใดที่ได้เกิดจากงานวิจัยในครั้งนี้ ผู้วิจัยขออุทิศให้แก่บุคคลผู้มีพระคุณดังกล่าวทุกท่าน

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

รายการตาราง

ตาราง **หน้า**

รายการรูปประกอบ

รูป **หน้า**

รายการรูปประกอบ(ต่อ)

รูป **หน้า**

บทที่ 1
บทนำ

งานวิจัยฉบับนี้จัดทำขึ้นเพื่อศึกษาการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสในด้านการเข้าถึงข้อมูลโดยวิธีการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน โดยงานวิจัยให้ความสนใจในขั้นตอนกระบวนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่มีกระบวนการในการป้องกันการโจมตีแบบ Replay Attack โดยใช้ค่า Nonce เข้ามาใช้ในการพิสูจน์ตัวตน แต่การนำค่าทั้งสองนี้มาใช้ในการพิสูจน์ตัวตนจะมีกระบวนการจัดเก็บค่าและตรวจสอบค่าทั้งสองนั้นซึ่งเป็นการเพิ่มต้นทุนในการทำงานของเว็บเซอร์วิส โดยรวมงานวิจัยจะมุ่งเน้นศึกษาในด้านการเพิ่มประสิทธิภาพของขั้นตอนการพิสูจน์ตัวตนเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคน เพื่อให้ต้นทุนในการทำงานดังกล่าวเกิดขึ้นน้อยที่สุด โดยงานวิจัยจะศึกษาเปรียบเทียบประสิทธิภาพของเว็บเซอร์วิสที่มีขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบเดิมตามมาตรฐานกับเว็บเซอร์วิสที่มีขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่มีการนำเสนอเทคนิควิธีการขั้นตอนพิสูจน์ตัวตนเพิ่มเติม

1.1 ความสำคัญและที่มาของงานวิจัย

ในยุคปัจจุบันเทคโนโลยีเว็บเซอร์วิสเข้ามามีบทบาทต่อองค์กรภาครัฐและภาคเอกชนแม้กระทั่งประชาชนทั่วไปเป็นอย่างมาก องค์กรจะใช้เทคโนโลยีเว็บเซอร์วิสในการแลกเปลี่ยนข้อมูลกันระหว่างเครื่องคอมพิวเตอร์โดยผ่านระบบเครือข่าย การนำเทคโนโลยีเว็บเซอร์วิสเข้ามาใช้ในการขับเคลื่อนธุรกิจ ใช้ด้านการให้บริการ หรือใช้เพื่อบรรลุวัตถุประสงค์ขององค์กรนั้น มีตั้งแต่การนำเว็บเซอร์วิสเข้ามาใช้ในงานตั้งแต่ระดับง่ายไม่ซับซ้อน เช่น การดึงข้อมูลเพื่อนำข้อมูลที่ต้องการนำไปประมวลผล จนไปถึงการนำเว็บเซอร์วิสเข้ามาใช้ในกระบวนการทางธุรกิจระดับใหญ่ที่มีกระบวนการซับซ้อน เป็นต้น

ในปัจจุบันมีการพัฒนาสถาปัตยกรรมเชิงบริการ SOA (Service Oriented Architecture) ใช้ภายในองค์กรมากขึ้นซึ่งเป็นสถาปัตยกรรมที่ออกแบบมาเพื่อใช้ในการรวมระบบภายในองค์กร ให้เชื่อมโยงกัน เทคโนโลยีหลักที่ใช้ในการพัฒนาสถาปัตยกรรมเชิงบริการคือ เทคโนโลยีเว็บเซอร์วิสเพราะเว็บเซอร์วิสมีลักษณะเป็นเว็บให้บริการที่มีโมดูลการทำงานแบบสมบูรณ์ในตัวเอง เว็บเซอร์วิสไม่ใช่เทคโนโลยีที่ใหม่แต่เป็นเทคโนโลยีที่องค์กรส่วนใหญ่ให้ความสำคัญในการนำมาใช้พัฒนาเป็นเว็บเซอร์วิสประยุกต์ใช้งานจริงในการขับเคลื่อนธุรกิจและบรรลุเป้าหมายขององค์กร เมื่อมีการนำเว็บเซอร์วิสเข้ามาใช้ในการติดต่อสื่อสารแลกเปลี่ยนข้อมูลเรื่องที่สำคัญที่ตามมาคือความมั่นคงปลอดภัยในการเข้าถึงข้อมูล หากข้อมูลที่มีความสำคัญเหล่านี้ถูกเข้าถึงโดยความตั้งใจหรือไม่ตั้งใจของผู้ที่

ไม่ได้รับสิทธิ์ในการเข้าถึงข้อมูลนั้นอาจทำให้องค์กรเกิดความเสียหายที่ร้ายแรงได้ ดังนั้นการพัฒนาเว็บเซอร์วิสไม่ว่าจะเป็นองค์กรใดควรคำนึงถึงความมั่นคงปลอดภัยในการเข้าถึงข้อมูลการใช้งานรับส่งข้อมูล

การสร้างเว็บเซอร์วิสให้มีความมั่นคงความปลอดภัยนั้นมีหลักในด้านต่างๆนี้คือ การพิสูจน์ตัวตน (Authentication) การแสดงตัวตน (Identification) การกำหนดสิทธิ์ใช้งาน (Authorization) การรักษาความลับ (Confidentiality) และความสมบูรณ์ของข้อมูล (Integrity) ในงานวิจัยนี้จะวิจัยด้านการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสในการพิสูจน์ตัวตนในการเข้าใช้บริการและเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิส องค์กรเพื่อความก้าวหน้าของมาตรฐานโครงสร้างสารสนเทศ OASIS (Organization for the Advancement of Structured Information Standards) [4] ได้ประกาศมาตรฐานเปิดการรักษาความมั่นคงปลอดภัยเว็บเซอร์วิสยูสเซอร์เนมโทเคน (Web Services Security UsernameToken) ในมาตรฐานได้อธิบายวิธีการที่ผู้ขอใช้บริการเว็บเซอร์วิสนำยูสเซอร์เนมโทเคนไปใช้ในการพิสูจน์ตัวตนเพื่อขอเข้าใช้บริการและเข้าถึงข้อมูลเว็บเซอร์วิสของผู้ให้บริการ โดยมาตรฐานแสดงวิธีการรักษาความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสในส่วน SOAP Message มีการประกาศตัวแปรยูสเซอร์เนมโทเคน (UsernameToken) ตามมาตรฐานที่ใช้ในการพิสูจน์ตัวตนใน SOAP Message Header ซึ่งประกอบไปด้วยตัวแปรชื่อ Username, Password, Nonce, และ Createdtime

ใน [5,6,7,8] มีการกล่าวถึงการนำยูสเซอร์เนมโทเคนเข้ามาใช้ในการพิสูจน์ตัวตนของเว็บเซอร์วิสและมีการเพิ่มความมั่นคงปลอดภัยในการพิสูจน์ตัวตนให้ดียิ่งขึ้นโดย [5,6] มีการนำเสนอกระบวนการขั้นตอนการพิสูจน์ตัวตนแบบสองขั้นตอนที่มีการเพิ่มการพิสูจน์ค่า Security Token ที่ใช้ร่วมกับการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน เป็นการเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสให้ดียิ่งขึ้น

ในงานวิจัยนี้มีการศึกษาการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนและมีการนำเสนอเทคนิคกระบวนการนำค่า Nonce มาใช้ในการป้องกันการรักษาความมั่นคงปลอดภัยด้านการโจมตีแบบ Replay Attack โดยมีการปรับปรุงจากวิธีการเดิมตามมาตรฐานที่มีการนำค่า Nonce มาใช้ป้องกันการโจมตีแบบ Replay Attack โดยทางฝั่งผู้ให้บริการเว็บเซอร์วิสจะต้องมีการเก็บค่า Nonce โดยต้องทำการสร้างฐานข้อมูลในการเก็บและต้องมีการกำหนดช่วงเวลาในการเก็บค่า Nonce ในฐานข้อมูลเหล่านั้น ซึ่งวิธีเดิมทำให้เกิดปัญหาในด้านการใช้ทรัพยากรพื้นที่ในการเก็บค่า Nonce ในฐานข้อมูลจำนวนมากและต้องมีการกำหนดช่วงเวลาที่เก็บค่า Nonce เมื่อครบกำหนดถึงช่วงเวลานั้นแล้วต้องมีการลบค่า Nonce ในฐานข้อมูล ถ้ามีการกำหนดช่วงเวลาที่น้อยเกินไป การโจมตีโดยการทำ Replay

Attack ก็สามารถทำได้ง่ายแต่ถ้ากำหนดช่วงเวลาไว้นานจำนวนค่า Nonce ที่เก็บไว้ในฐานข้อมูลก็จะมีปริมาณมากทำให้ฐานข้อมูล ต้องเพิ่มขนาดพื้นที่ในการเก็บค่า Nonce จำนวนมากทำให้สิ้นเปลืองทรัพยากรพื้นที่ในการเก็บค่า Nonce มาก และการตรวจสอบค่า Nonce ที่ได้รับมาจากผู้ขอใช้บริการว่าเป็นผู้ขอใช้บริการจริงหรือมาจากผู้ไม่ประสงค์ดีนั้นก็ต้องใช้เวลานานมากขึ้นในการค้นหาว่าค่า Nonce ที่เก็บในฐานข้อมูล กับค่า Nonce ที่รับมาว่าค่าตรงกันหรือไม่

งานวิจัยจึงได้นำเสนอเทคนิคที่ได้พัฒนาการนำค่า Nonce มาใช้ในการพิสูจน์ตัวตนและป้องกันการโจมตีแบบ Replay Attack ในรูปแบบการพิสูจน์ตัวตนของเว็บเซอร์วิสแบบสองขั้นตอนโดยแก้ปัญหาดังที่กล่าวมาข้างต้น เทคนิคที่ได้เสนอในงานวิจัยเป็นขั้นตอนการพิสูจน์ตัวตนที่หลีกเลี่ยงการเก็บค่า Nonce ทุกค่าที่ได้รับในฐานข้อมูลในฝั่งเซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิสและหลีกเลี่ยงการกำหนดค่าช่วงเวลาในการเก็บและลบค่า Nonce ไว้ในฐานข้อมูล โดยใช้กระบวนการนำค่าที่บ่งบอกตัวตนจริงของผู้ใช้บริการและของผู้ให้บริการมาทำการตรวจสอบและใช้การอัพเดทค่าข้อมูลที่ใช้พิสูจน์ตัวตนในฐานข้อมูลแทนวิธีการเดิม ในการทดลองนั้นจะมีการจำลองการติดต่อสื่อสารกันระหว่างผู้ขอใช้บริการเว็บเซอร์วิสกับผู้ให้บริการเว็บเซอร์วิส สร้างเว็บเซอร์วิสที่มีขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบเดิมตามมาตรฐาน กับเว็บเซอร์วิสที่มีขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่มีการนำเสนอเทคนิควิธีการขั้นตอนพิสูจน์ตัวตนเพิ่มเติมและทำการตรวจวัดค่าเวลาที่ใช้ในการทำงานของทั้งสองรูปแบบ นำค่าที่ได้จากการทดลองนำมาเปรียบเทียบพร้อมทั้งอธิบายวิเคราะห์คุณภาพของการประมวลผลที่ได้จากการทดลองในงานวิจัยนี้

1.2 วัตถุประสงค์ของงานวิจัย

ในงานวิจัยนี้มีวัตถุประสงค์ในการดำเนินการวิจัยดังต่อไปนี้

1) เพื่อศึกษาวิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กรเพื่อความก้าวหน้าของมาตรฐานโครงสร้างสารสนเทศ OASIS (Organization for the Advancement of Structured Information Standards)

2) เพื่อศึกษาอัลกอริทึมและวิธีการพิสูจน์ตัวตนโดยการส่งค่า Nonce ซึ่งเป็นค่าของพารามิเตอร์ของวิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคน

3) เพื่อพัฒนาเทคนิควิธีการในการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคน โดยการหลีกเลี่ยงการเก็บและตรวจสอบค่า Nonce ทุกค่าไว้ในฐานข้อมูลในฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิส

4) เพื่อศึกษาและเปรียบเทียบผลลัพธ์ที่ได้จากการพัฒนาเทคนิควิธีการในการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนที่นำเสนอกับผลลัพธ์ที่ได้จากการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนที่ใช้วิธีการเก็บและตรวจสอบค่า Nonce ทุกค่าไว้ในฐานข้อมูลที่ฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิส

1.3 ประโยชน์ที่ได้รับจากงานวิจัย

ในงานวิจัยนี้มีประโยชน์ที่ได้รับจากงานวิจัยดังต่อไปนี้

1) งานวิจัยนี้ได้เสนอวิธีการรักษาความมั่นคงปลอดภัยในการเข้าใช้บริการและเข้าถึงข้อมูลของเว็บเซอร์วิส ซึ่งเป็นประโยชน์ในด้านการรักษาความมั่นคงปลอดภัยให้กับข้อมูล ป้องกันการโจรกรรมข้อมูลที่อาจเกิดขึ้นได้จากผู้ไม่ประสงค์ดีที่เข้ามาโจรกรรมข้อมูลเว็บเซอร์วิสของผู้ให้บริการ

2) งานวิจัยนี้ได้เสนอการพัฒนาเทคนิคเพื่อเป็นแนวทางในการใช้วิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กร OASIS ให้มีประสิทธิภาพมากขึ้น

3) งานวิจัยนี้ได้เสนอการพัฒนาเทคนิคในการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนในการเข้าถึงบริการข้อมูลของเว็บเซอร์วิสและการใช้ค่า Nonce ให้มีประสิทธิภาพมากขึ้นในการป้องกันการโจมตีแบบ Replay Attack โดยการหลีกเลี่ยงการเก็บค่า Nonce ทุกค่าในฐานข้อมูลที่เซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิส และหลีกเลี่ยงการกำหนดช่วงเวลาในการเก็บและลบค่า Nonce ในฐานข้อมูลที่เซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิส

1.4 ขอบเขตงานวิจัย

ในงานวิจัยนี้มีขอบเขตการวิจัยดังต่อไปนี้

1) งานวิจัยนี้ได้นำเสนอการพัฒนาเทคนิควิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กร OASIS ที่มีการสร้างและนำค่า Nonce มาใช้ในการพิสูจน์ตัวตนโดยการหลีกเลี่ยงการเก็บค่า Nonce ทุกค่าไว้ในฐานข้อมูลในฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิส

2) งานวิจัยนี้ได้นำเสนอการเปรียบเทียบผลลัพธ์ที่ได้จากการทดลองโดยการจำลองสร้างโปรแกรมเว็บเซอร์วิสในการติดต่อสื่อสาร เพื่อขอใช้บริการเว็บเซอร์วิสจากผู้ขอใช้บริการเว็บเซอร์วิสไปยังผู้ให้บริการเว็บเซอร์วิสที่มีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กร OASIS ที่มีการสร้างและนำค่า Nonce มาใช้ในการพิสูจน์ตัวตนในแบบวิธีเก็บค่า Nonce ทุกค่าไว้ในฐานข้อมูลในฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิส กับวิธีที่นำเสนอ คือ การหลีกเลี่ยงการเก็บค่า Nonce ทุกค่าไว้ในฐานข้อมูลของฝั่งเครื่องผู้ให้บริการเว็บ

เซอร์วิส ในการทดลองจะมีการวัดค่าเวลาที่ใช้ในการประมวลผลโดยมีตัวแปรที่นำมาใช้ในการคำนวนคุณภาพของการทำรายการเว็บเซอร์วิส คือ จำนวนการทำรายการ และ เวลาที่ใช้ในการทำรายการ

1.5 ขั้นตอนการดำเนินงาน

งานวิจัยนี้ได้แสดงการดำเนินงานวิจัยและอธิบายโดยการแบ่งเนื้อหาทั้งหมดออกเป็น 5 บทด้วยกัน โดยแต่ละบทมีการนำเสนอเนื้อหาดังรายละเอียดต่อไปนี้

บทที่ 1 บรรยายความสำคัญและที่มาของการทำวิจัย ปัญหาที่ทำให้เกิดงานวิจัยนี้ วัตถุประสงค์ของงานวิจัย ประโยชน์และผลที่คาดว่าจะได้รับจากการทำงานวิจัย และขอบเขตในการทำงานวิจัยนี้

บทที่ 2 อธิบายทฤษฎีพื้นฐานที่เกี่ยวข้อง ซึ่งประกอบด้วยหัวข้อเกี่ยวข้องกับ เว็บเซอร์วิส การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและเว็บเซอร์วิส การพิสูจน์ตัวตนการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กร OASIS ตลอดจนกล่าวถึงวรรณกรรมที่เกี่ยวข้องกับงานวิจัยนี้

บทที่ 3 อธิบายหลักการพัฒนาเทคนิควิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กร OASIS โดยการหลีกเลี่ยงการเก็บและตรวจสอบค่า Nonce ไว้ในที่เก็บค่าของข้อมูลที่มีขนาดใหญ่ในฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิส โดยกล่าวถึงขั้นตอนการทำงานอย่างละเอียด รวมถึงแสดงอัลกอริทึมที่จำเป็นต้องใช้ในงานวิจัยนี้

บทที่ 4 แสดงวิธีการทดลองที่ใช้เพื่อทดสอบวัดคุณภาพของเวลาที่ใช้ในการประมวลผลของการใช้เทคนิคหลักการวิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนโดยการหลีกเลี่ยงการเก็บและตรวจสอบค่า Nonce ทุกค่าไว้ในฐานข้อมูลในฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิสที่นำเสนอในงานวิจัยนี้โดยเปรียบเทียบกับ วิธีการพิสูจน์ตัวตนในการเข้าถึงบริการและข้อมูลของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคน โดยการเก็บและตรวจสอบค่า Nonce ทุกค่าไว้ในฐานข้อมูลในฝั่งเครื่องผู้ให้บริการเว็บเซอร์วิส แสดงผลที่ได้จากการทดลอง พร้อมทั้งอธิบายการวิเคราะห์คุณภาพของการประมวลผลซึ่งวิเคราะห์จากค่าเวลาที่ใช้ในการประมวลผลที่ได้จากการทดลอง

บทที่ 5 สรุปผลที่ได้รับจากการทำวิจัยนี้ และกล่าวถึงการนำงานวิจัยนี้ไปเป็นแนวทางพัฒนางานสืบต่อไปในอนาคต

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

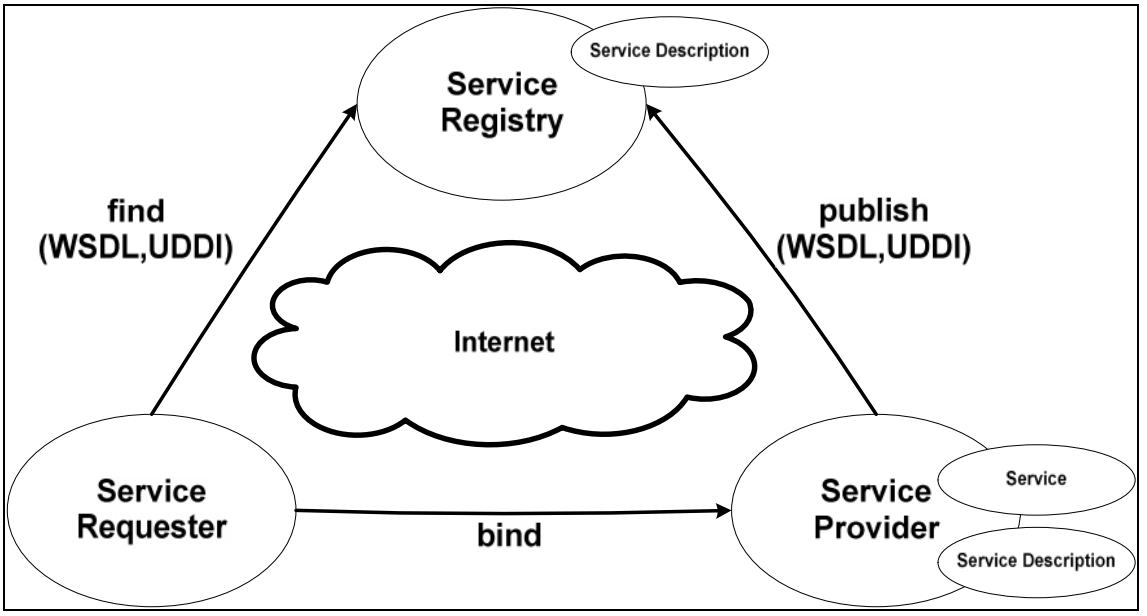
ในบทนี้กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้องกับงานวิจัยนี้ ซึ่งหัวข้อสำคัญที่กล่าวถึงคือ ความหมายและความสำคัญของเว็บเซอร์วิส ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) ความมั่นคงปลอดภัยของเว็บเซอร์วิส (WS-Security) การพิสูจน์ตัวตน (Authentication) มาตรฐานเปิดการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน (WS-Security UsernameToken) และหัวข้องานวิจัยที่เกี่ยวข้อง โดยอธิบายถึงความรู้ทฤษฎีและงานวิจัยที่เกี่ยวข้องดังเนื้อหาต่อไปนี้

2.1 เว็บเซอร์วิส

เว็บเซอร์วิสไม่ใช่เทคโนโลยีที่ใหม่แต่เป็นเทคโนโลยีที่องค์กรส่วนใหญ่ให้ความสำคัญ ในเนื้อหาส่วนนี้จะอธิบายถึง ความหมายเว็บเซอร์วิสและองค์ประกอบของเว็บเซอร์วิสดังเนื้อหาต่อไปนี้

2.1.1 ความหมายเว็บเซอร์วิส

คำนิยามเว็บเซอร์วิสโดย Booth และ Haas [1] กล่าวว่า World Wide Web Consortium (W3C) ให้ความหมายเว็บเซอร์วิส คือ โปรแกรมหรือแอพพลิเคชันที่ถูกกำหนดด้วย URI ซึ่งเป็นโปรแกรมที่ทำหน้าที่ประสานงานและเชื่อมโยงเพื่อแลกเปลี่ยนข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่สามารถทำได้โดยมีการประกาศ อธิบาย และทำให้รับรู้ ด้วยภาษา XML เว็บเซอร์วิสสนับสนุนการแลกเปลี่ยนข้อมูลแบบโดยตรงกับโปรแกรมอื่นๆ การแลกเปลี่ยนข้อมูลนั้นอยู่บนพื้นฐานการแลกเปลี่ยนข้อความด้วยภาษา XML และใช้ช่องทางแลกเปลี่ยนข้อมูลผ่านโพรโตคอลอินเทอเน็ต การทำงานของเว็บเซอร์วิสมีลักษณะเป็นเว็บให้บริการให้กับแอพพลิเคชันอื่นเรียกใช้งาน มีรูปแบบการทำงานแบบ RPC (Remote Procedure Call) ซึ่งการให้บริการของเว็บเซอร์วิสจะมีเอกสารกำกับอธิบายการให้บริการของเว็บเซอร์วิสนั้น เว็บเซอร์วิสเป็นโปรแกรมแบบ loosely couple มีความสมบูรณ์การทำงานในตัวเองและเป็นอิสระ รูปที่ 2.1 เป็นการแสดงกระบวนการทำงานของเว็บเซอร์วิส โดยผู้ให้บริการเว็บเซอร์วิสจะประกาศชื่อบริการและวิธีการติดต่อเรียกใช้บริการของตนไปยังหน่วยงานกลางทำหน้าที่จัดเก็บบริการของผู้ให้บริการเว็บเซอร์วิส เมื่อผู้ที่ต้องการเรียกใช้บริการเว็บเซอร์วิสก็จะไปทำการค้นหาบริการจากหน่วยงานกลาง เมื่อได้ชื่อบริการและวิธีการติดต่อเว็บเซอร์วิสจากนั้นผู้เรียกใช้บริการเว็บเซอร์วิสก็จะดำเนินการส่งคำร้องขอใช้บริการเว็บเซอร์วิสไปยังผู้ให้บริการเว็บเซอร์วิสนั้น



รูปที่ 2.1 กระบวนการทำงานเว็บเซอร์วิส [1]

2.1.2 องค์ประกอบของเว็บเซอร์วิส

เว็บเซอร์วิสมีองค์ประกอบหลัก 4 อย่างดังต่อไปนี้

- XML (Extensible Markup Language) คือ ภาษามาตรฐานที่ W3C ประกาศใช้ ภาษา XML เป็นภาษาที่นำมาใช้ในกำหนดโครงสร้างของข้อมูล กำหนดรูปแบบของข้อมูล สามารถอธิบายค่าของข้อมูล จึงเป็นภาษามาตรฐานที่นำมาใช้ในการแลกเปลี่ยนข้อมูลกันของเว็บเซอร์วิส
- SOAP (Simple Object Access Protocol) คือ มาตรฐานข้อความการรับส่งแลกเปลี่ยนข้อมูลระหว่างเว็บเวอร์วิสกับแอพพลิเคชันที่ขอใช้บริการ SOAP เปรียบเสมือนจดหมายใช้ในการสื่อสารโดยติดต่อสื่อสารส่งผ่านโพรโตคอล HTTP มาตรฐาน SOAP สามารถนำไปใช้แลกเปลี่ยนข้อมูลข้ามแพลตฟอร์มได้ แลกเปลี่ยนข้อมูลข้ามระบบที่พัฒนาจากภาษาที่แตกต่างกันได้ การส่งข้อความตามมาตรฐาน SOAP มีรูปแบบการส่งในรูป SOAP Message มีการแลกเปลี่ยนข้อมูลข่าวสารที่เป็นภาษา XML ระหว่างผู้ให้บริการเว็บเซอร์วิสและผู้ขอใช้งานเว็บเซอร์วิส
- WSDL (Web Services Description Language) คือ มาตรฐานที่ใช้อธิบายการนำเว็บเซอร์วิสไปใช้งาน เปรียบได้กับคู่มือการใช้งานเว็บเซอร์วิส WSDL เป็นเอกสารจัดทำโดยใช้ภาษา XML อธิบายเว็บเซอร์วิสรูปแบบการรับพารามิเตอร์ อธิบายรูปแบบการส่งผลลัพธ์พารามิเตอร์ และอธิบายโพรโตคอลการติดต่อตำแหน่งในการติดต่อกับเว็บเซอร์วิสผู้ให้บริการ

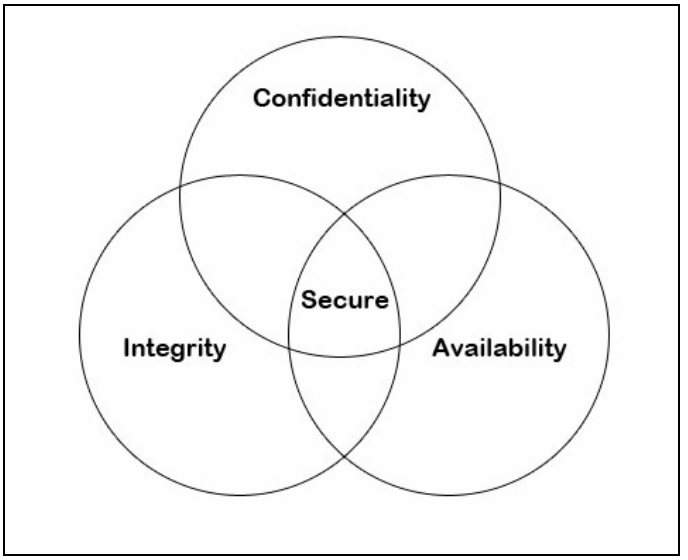
- UDDI (Universal Description Discovery and Integration) คือ มาตรฐานในการเก็บรายละเอียดในการอธิบายและค้นหาเว็บเซอร์วิส UDDI ทำหน้าที่เป็นตัวกลางในการจัดเก็บเว็บเซอร์วิสของผู้ให้บริการ ทางด้านผู้ให้บริการเว็บเซอร์วิสสามารถนำเอกสาร WSDL และแจ้งข้อมูลผู้ให้บริการ ข้อมูลการให้บริการเว็บเซอร์วิส ผู้ขอใช้บริการสามารถค้นหาเว็บเซอร์วิสเพื่อขอเข้าใช้บริการได้จากทาง UDDI

2.2 ความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์มีความสำคัญอย่างมากต่อข้อมูลที่จัดเก็บในคอมพิวเตอร์นั้น ในส่วนนี้จะกล่าวถึง ความหมายของความมั่นคงปลอดภัยระบบคอมพิวเตอร์ การโจมตีความมั่นคงปลอดภัยข้อมูล และ การควบคุมความมั่นคงปลอดภัยซอฟต์แวร์ ดังรายละเอียดต่อไปนี้

2.2.1 ความหมายของความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ความมั่นคงปลอดภัยระบบคอมพิวเตอร์คือ การที่ข้อมูลถูกป้องกัน ควบคุม ให้พ้นจากการถูกเปิดเผยข้อมูลของผู้ที่ไม่ได้รับอนุญาต [2] ได้อธิบายถึงความหมายของความมั่นคงปลอดภัยระบบสารสนเทศว่า จุดประสงค์หลักของความมั่นคงปลอดภัยระบบสารสนเทศคือ การป้องกันจุดอ่อนของระบบสารสนเทศให้พ้นจากการถูกเอาเปรียบจากผู้อื่น เมื่อกล่าวถึงความมั่นคงปลอดภัยระบบสารสนเทศ วัตถุประสงค์หลักที่สำคัญที่ต้องคำนึงถึงมีอยู่ 3 ประการคือ ความลับของข้อมูล (Confidentiality), ความถูกต้องของข้อมูล (Integrity) และ การพร้อมเข้าถึงข้อมูล (Availability) รูปที่ 2.2 แสดงความสัมพันธ์ระหว่าง ความลับของข้อมูล, ความถูกต้องของข้อมูล, การพร้อมเข้าถึงข้อมูล



รูปที่ 2.2 ความสัมพันธ์ระหว่าง ความลับ, ความถูกต้อง, การพร้อมเข้าถึงของข้อมูล [2]

ความลับของข้อมูล (Confidentiality) ข้อมูลสารสนเทศจะเป็นความลับต้องสามารถมั่นใจได้ว่าความสามารถเข้าถึงข้อมูลนั้นทำได้เฉพาะผู้ที่ได้รับสิทธิ์ให้สามารถเข้าถึงข้อมูลเท่านั้น โดยผู้ที่ได้รับอนุญาตให้สามารถเข้าถึงข้อมูลได้นั้น คำว่าสามารถเข้าถึงข้อมูลได้ไม่ได้หมายความว่าสามารถอ่านข้อมูลนั้นได้เท่านั้นแต่ยังสามารถเข้าถึงดูรายละเอียด สามารถนำข้อมูลออกมาใช้งานได้เช่น การพิมพ์ข้อมูล และยังสามารถทำในสิ่งต่างที่เป็นสิทธิ์ที่ผู้ได้รับอนุญาตการเข้าถึงข้อมูลนั้นได้เป็นต้น

ความถูกต้องของข้อมูล (Integrity) ความถูกต้องของข้อมูลหมายถึง ข้อมูลนั้นสามารถแก้ไขโดยผู้ที่ได้รับอนุญาตการเข้าถึงข้อมูลเท่านั้น การแก้ไขข้อมูลนั้นประกอบด้วย การเขียนข้อมูล การเปลี่ยนแปลงข้อมูล การเปลี่ยนแปลงสถานะของข้อมูล การลบและการสร้างข้อมูลเป็นต้น

การพร้อมเข้าถึงข้อมูล (Availability) การพร้อมเข้าถึงข้อมูลหมายถึง ข้อมูลสารสนเทศสามารถถูกเข้าถึงข้อมูลพร้อมนำข้อมูลไปใช้งานโดยผู้ที่ได้รับอนุญาตการเข้าถึงข้อมูลเท่านั้นในช่วงเวลาที่ได้จัดสรรไว้สำหรับการเข้าถึงข้อมูล ผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลจะไม่สามารถเข้าถึงและไม่สามารถกระทำใดๆต่อข้อมูลนั้นได้

2.2.2 การโจมตีความมั่นคงปลอดภัยข้อมูล

การที่ข้อมูลสารสนเทศอยู่ในสภาวะไม่มั่นคงปลอดภัยนั้นสืบเนื่องมาจากข้อมูลถูกกลุ่มหรือผู้ไม่ประสงค์ดีทำการโจมตีความมั่นคงปลอดภัยเพื่อเข้าถึงและโจรกรรมข้อมูล [2] ได้กล่าวว่าการโจมตีความมั่นคงปลอดภัยของข้อมูลสามารถแบ่งได้ 4 ชนิด ดังต่อไปนี้คือ

- การสกัดกั้น (Interception) ไม่ให้ผู้มีสิทธิ์เข้าถึงข้อมูลนั้นสามารถเข้าถึงข้อมูลได้

- การขัดจังหวะ (Interruption) ทำให้ข้อมูลไม่สามารถพร้อมใช้งานจากผู้มีสิทธิ์เข้าถึงข้อมูลนั้นได้
- การดัดแปลง (Modification) ผู้ไม่มีสิทธิ์สามารถเข้าถึงข้อมูลแก้ไขดัดแปลงข้อมูลให้ผิดไปจากข้อมูลเดิม
- การบิดเบือนความจริง (Fabrication) ผู้ไม่มีสิทธิ์สามารถเข้าถึงข้อมูลและบิดเบือนความเป็นจริงของการเข้าถึงข้อมูล เช่นการโจมตีแบบ Replay Attack โดยทำการคัดลอกวิธีการเข้าถึงข้อมูลของผ้มีสิทธิ์เข้าถึงข้อมูลแล้วดำเนินการทำรายการนั้นซ้ำ และ Rewriting Attack ดำเนินการคัดลอกวิธีการเข้าถึงข้อมูลและเปลี่ยนแปลงการทำรายการเพื่อสามารถเข้าถึงข้อมูลได้

2.2.3 การควบคุมความมั่นคงปลอดภัยซอฟต์แวร์

การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศให้พ้นจากภัยคุกคามจากการโจมตีของผู้ไม่มีสิทธิ์เข้าถึงข้อมูลนั้น สิ่งสำคัญคือการควบคุมการเข้าถึงข้อมูลให้มั่นคงปลอดภัยในด้านซอฟต์แวร์ก็เป็นด้านที่สำคัญในการจัดการการควบคุมความมั่นคงปลอดภัยในการเข้าถึงข้อมูลให้เป็นไปตามหลักการของการรักษาความมั่นคงปลอดภัยข้อมูล [2] ได้กล่าวว่าการควบคุมความมั่นคงปลอดภัยซอฟต์แวร์ประกอบด้วยดังต่อไปนี้

- การควบคุมโปรแกรมภายใน (Internal Program Controls) เช่น การจำกัดจำนวนการเข้าถึงข้อมูลภายใน
- การควบคุมระบบหน่วยปฏิบัติการและระบบเครือข่าย (Operating System and Network System Controls) เช่น จำกัดระบบหน่วยปฏิบัติการและระบบเครือข่ายของผู้ที่ต้องการเข้าถึงข้อมูล ป้องกันการเข้าถึงข้อมูลเฉพาะระบบหน่วยปฏิบัติการและระบบเครือข่ายที่ระบุเท่านั้น
- การควบคุมของโปรแกรมที่ไม่ขึ้นกับซอฟต์แวร์ (Independent Control Programs) เช่น แอพพลิเคชันที่ประกอบด้วย การตรวจสอบรหัสผ่าน การตรวจจับการโจมตีของผู้ไม่ประสงค์ดี การตรวจสอบไวรัส
- การควบคุมการพัฒนา (Development Controls) เป็นการควบคุมความมั่นคงปลอดภัยทุกขั้นตอนกระบวนการพัฒนาระบบ ตั้งแต่การออกแบบ สร้างโปรแกรม ทดสอบ ไปจนถึงบำรุงรักษาระบบ ปกป้องทุกขั้นตอนให้พ้นจากภัยคุกคาม

2.3 ความมั่นคงปลอดภัยเว็บเซอร์วิส

ความมั่นคงปลอดภัยของเว็บเซอร์วิส Singhal และคณะ[3] ให้คำอธิบายเกี่ยวกับมิติความมั่นคงปลอดภัยเว็บเซอร์วิสสามารถแบ่งได้ 5 ด้านดังนี้คือ การรักษาความมั่นคงปลอดภัยในด้านการรับส่งข้อความ (Secure Messaging), การปกป้องทรัพยากร (Protecting Resources), สัญญาข้อตกลงในการกระทำเพื่อเข้าถึงข้อมูล (Negotiation of Contracts), ความน่าเชื่อถือในการติดต่อเชื่อมโยง (Trust Relationship), ความต้องการความมั่นคงปลอดภัยของการพัฒนาซอฟต์แวร์ (Requirement for Secure Software)การรักษาความมั่นคงปลอดภัยในด้านการรับส่งข้อความ (Secure Messaging) ในการติดต่อสื่อสารรับส่ง SOAP Message บนช่องทางผ่านเครือข่ายอินเตอร์เน็ตนั้น SOAP Message อาจถูกดักจับเพื่อดูและแก้ไขโดยผู้ไม่ประสงค์ดีเพื่อทำการปลอมแปลงเป็นผู้ขอใช้บริการเว็บเซอร์วิสในการเข้าถึงข้อมูล ดังนั้นการรักษาความมั่นคงปลอดภัยของการรับส่งข้อความสามารถป้องกันความมั่นคงปลอดภัยให้กับข้อความได้ดังนี้

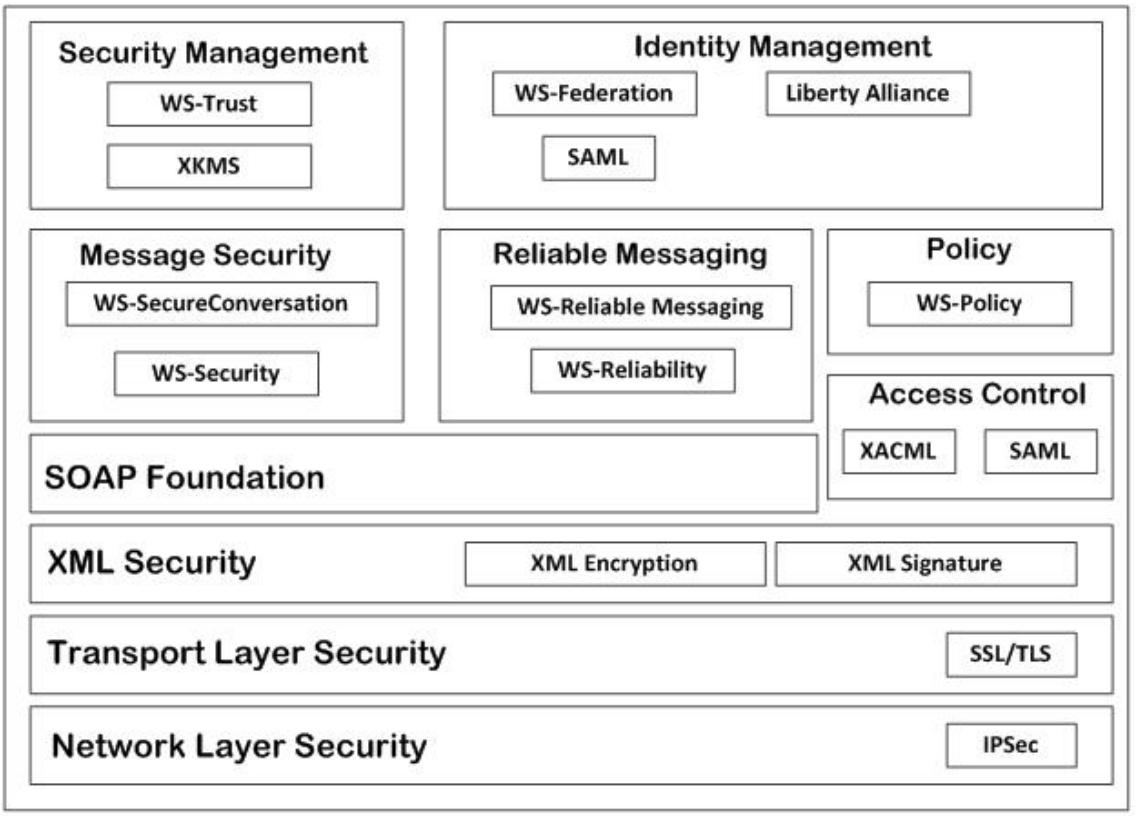
- HTTP over SSL/TLS (HTTPS) เว็บเซอร์วิสรับส่งข้อความผ่านเครือข่ายอินเตอร์เน็ตโดยใช้โพรโตคอล HTTP ดังนั้นจึงสามารถทำเว็บเซอร์วิสให้รองรับโพรโตคอล HTTPS (Hypertext Transfer Protocol Over Secure Socket Layer) เป็นการเพิ่มความมั่นคงปลอดภัยให้กับการรับส่งข้อความ
- XML Encryption and XML Signature เป็นมาตรฐานการพัฒนาความมั่นคงปลอดภัยให้กับ XML ขององค์กร W3C ใน SOAP Message เป็นข้อความรูปแบบ XML ผู้พัฒนาเว็บเซอร์วิสสามารถใช้มาตรฐานนี้ในการลงนาม (Sign) และ เข้ารหัส (Encrypt) ให้กับ SOAP Message เพื่อเพิ่มความมั่นคงปลอดภัยให้กับการรับส่งข้อความของเว็บเซอร์วิส
- WS-Security เป็นมาตรฐานการพัฒนาความมั่นคงปลอดภัยให้กับ XML ขององค์กร W3C ใน SOAP Message เป็นส่วนเพิ่มเติมของ XML Encryption and XML Signature ในการรักษาความมั่นคงปลอดภัยให้กับ SOAP Message โดยเฉพาะการปกป้องทรัพยากร (Protecting Resources) เมื่อผู้ให้บริการเว็บเซอร์วิสเปิดให้บริการข้อมูลสู่สาธารณะ

เว็บเซอร์วิสเป็นเว็บให้บริการแลกเปลี่ยนข้อมูล ดังนั้นเว็บเซอร์วิสจึงต้องให้ความสำคัญในด้านความสามารถในการเข้าถึงข้อมูล โดยอนุญาตให้ผู้ที่มีสิทธิ์ที่จะสามารถเข้าถึงข้อมูลได้เท่านั้น ต้องมีกลไกข้อตกลงกันในการเข้าถึงข้อมูล ความมั่นคงปลอดภัยในการเข้าถึงข้อมูลเว็บเซอร์วิสจึงต้องการให้ผู้ต้องการเข้าถึงข้อมูลระบุตัวตน และต้องการพิสูจน์ตัวตนผู้ที่ต้องการเข้าใช้งานเว็บเซอร์วิสว่ามีสิทธิ์ในการเข้าถึงข้อมูลหรือไม่ การพิสูจน์ตัวตนมีหลากหลายวิธีเช่น การพิสูจน์ตัวตนในส่วน

Transport Layer การพิสูจน์ตัวตนโดยใช้โทเคนตามมาตรฐาน WS-Security เช่น SAML Assertions ยูสเซอร์เนมโทเคนซึ่งเป็นการพิสูจน์ตัวตนในส่วน SOAP Message Header เป็นต้น

สัญญาข้อตกลงในการกระทำเพื่อเข้าถึงข้อมูล (Negotiation of Contracts) การติดต่อสื่อสารเว็บเซอร์วิสระหว่างองค์กรนั้นจะแน่ใจได้อย่างไรว่าการติดต่อกันนั้นกระทำกันระหว่างองค์กรสององค์กรนั้นจริง โดยเฉพาะเว็บเซอร์วิสที่ให้บริการข้อมูลที่สำคัญ เช่น ข้อมูลการเงิน ดังนั้นจึงมีข้อตกลงกันในการระบุขั้นตอนฟังก์ชันในการติดต่อสื่อสารรับส่งข้อมูลก่อนการพัฒนาระบบเว็บเซอร์วิส เพื่อให้ทราบถึงขั้นตอนการติดต่อเฉพาะองค์กรสององค์กรเท่านั้น ข้อตกลงในการติดต่อสื่อสารไม่ได้เป็นมาตรฐานของทั่วไปเพราะข้อตกลงจะทราบเฉพาะระหว่างองค์กรที่ติดต่อสื่อสารกันเท่านั้นจึงเป็นการสร้างความมั่นคงปลอดภัยในด้านการติดต่อระหว่างเว็บเซอร์วิสผู้ให้บริการและผู้ขอใช้บริการ

ความน่าเชื่อถือในการติดต่อเชื่อมโยง (Trust Relationship) เว็บเซอร์วิสอนุญาตให้สามารถสร้างรูปแบบตรวจสอบความน่าเชื่อถือได้หลากหลายรูปแบบในการระบุตัวตนเว็บเซอร์วิสของผู้ให้บริการในด้านทางผู้ขอใช้บริการเว็บเซอร์วิสจะไม่สามารถทราบได้ว่าสิ่งที่ตนร้องขอไปนั้นและได้รับข้อมูลที่ตอบกลับมาข้อมูลที่ได้รับนั้นเป็นของผู้ให้บริการหรือเป็นข้อมูลของผู้ไม่ประสงค์ดีดังนั้นการตรวจสอบความน่าเชื่อถือการระบุตัวตนและการพิสูจน์ตัวตนเป็นสิ่งที่จำเป็นและสำคัญอย่างมากในการพัฒนาเว็บเซอร์วิสให้มีความมั่นคงปลอดภัยในการรับส่งข้อมูลความต้องการออกแบบด้านความมั่นคงปลอดภัยของการพัฒนาซอฟต์แวร์ (Requirement for Secure Software) การออกแบบพัฒนาเว็บเซอร์วิสให้มีความมั่นคงปลอดภัยนั้นควรนำมาตรฐานเปิดและเทคนิคขององค์กรที่ประกาศมาตรฐานความมั่นคงปลอดภัยเว็บเซอร์วิส เช่น OASIS, W3C นำมาใช้ในการออกแบบพัฒนาเว็บเซอร์วิสตามมาตรฐานนั้น

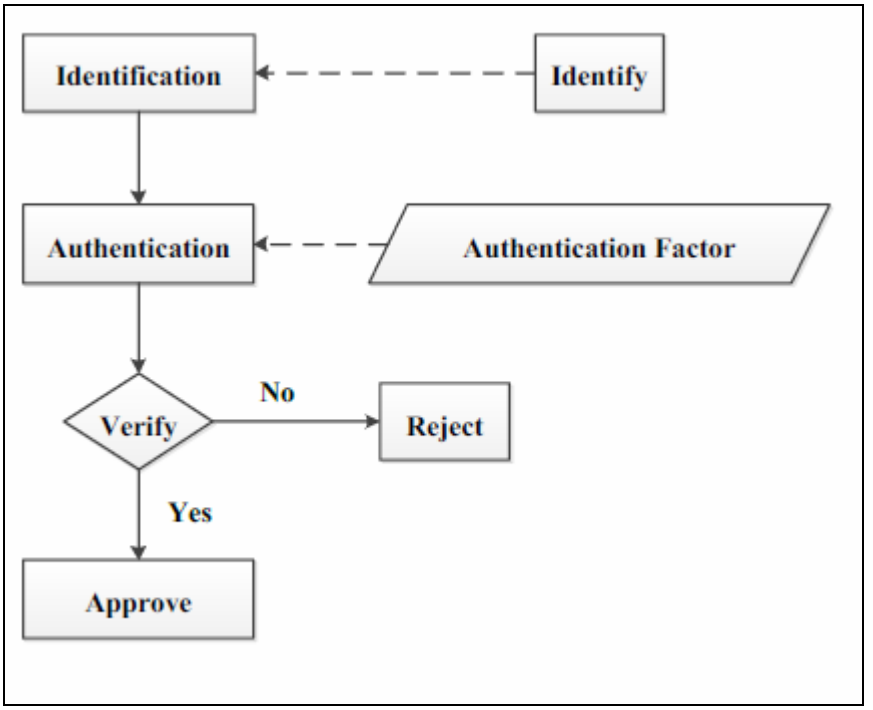


รูปที่ 2.3 มาตรฐานเปิดที่ประกาศใช้ด้านความมั่นคงปลอดภัยเว็บเซอร์วิส [3]

อธิบายรูปที่ 2.3 ได้ว่ารูปแบบของมาตรฐานเปิดได้ประกาศใช้ในด้านความมั่นคงปลอดภัยของการพัฒนาเว็บเซอร์วิส เป็นรูปแบบการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสในแต่ละชั้นตั้งแต่ Network Layer, Transport Layer, XML Security Layer การรักษาความมั่นคงปลอดภัยจะเป็นรักษาความมั่นคงปลอดภัยด้านการรับส่งข้อมูล มาตรฐานที่ใช้คือ IPSec, SSL/TLS และXML Encryption and XML Signature ในส่วนที่อยู่เหนือชั้น XML Security Layer จะเป็นมาตรฐานที่เพิ่มเติมบน SOAP มาตรฐานด้านความมั่นคงปลอดภัยของข้อความได้แก่ WS-Security และ WS-SecureConversation มาตรฐานทั้งสองนี้ประกาศวิธีการใช้งาน XML Signature , XML Encryption และอธิบายการรับรอง SOAP Message ในส่วนมาตรฐานในการเข้าถึงข้อมูลได้แก่ XACML อธิบายนโยบายการเข้าถึงเว็บเซอร์วิส และ SAML อธิบายความสามารถที่ใช้ยืนยันตัวตน ในส่วนของชั้น Policy Layer มาตรฐาน WS-Policy อธิบายหลักการติดต่อของความต้องการนโยบายของเว็บเซอร์วิส ในส่วนชั้น Security Management จะมีมาตรฐาน อธิบายการรับรองตัวตนเช่น ใบรับรอง PKI (PKI Certificates) ในส่วนของชั้น Identity Management ในส่วนนี้จะมีมาตรฐาน WS-Trust ที่ช่วยเสริมในเรื่องการเข้าถึงข้อมูลนโยบายมาตรฐาน SOAP ของผู้ให้บริการเว็บเซอร์วิสในการจัดการระบุตัวตนและรับรองผู้ขอใช้บริการเว็บเซอร์วิส เช่น การใช้ยูสเซอร์เนมโทเคนในการระบุข้อมูลที่ใช้ในการพิสูจน์ตัวตนของผู้ที่ต้องการเข้าใช้บริการเว็บเซอร์วิส เป็นต้น

2.4 การพิสูจน์ตัวตน

การพิสูจน์ตัวตนและการตรวจสอบหลักฐานเป็นการยืนยันตัวตนจริงว่าเป็นผู้มีสิทธิ์สามารถเข้าถึงข้อมูลได้จริง ซึ่งเป็นสิ่งที่สำคัญมากในด้านการป้องกันความมั่นคงปลอดภัยให้กับข้อมูล การที่ผู้ที่จะสามารถเข้าถึงข้อมูลได้นั้นต้องเป็นผู้ที่ได้รับอนุญาตสามารถเข้าถึงและนำข้อมูลนั้นไปใช้งานได้ ในรูปที่ 2.4 แสดงหลักการผู้ที่ต้องการเข้าถึงข้อมูลเข้าใช้งานระบบจะต้องแจ้งความจำนงค์หรือลงทะเบียนกับผู้ให้บริการ จากนั้นผู้ให้บริการจะกำหนดระบุชื่อผู้เข้าใช้งานระบบและรหัสผ่านที่เป็นเฉพาะเจาะจงของผู้ขอเข้าใช้งานแต่ละคนนั้น เมื่อผู้ต้องการขอเข้าถึงข้อมูลจะต้องส่งชื่อผู้เข้าใช้งานระบบและรหัสผ่านมาให้ทางผู้ให้บริการข้อมูล การทำเช่นนี้ผู้ให้บริการข้อมูลสามารถตรวจสอบพิสูจน์ตัวตนผู้ที่ต้องการจะเข้าใช้บริการข้อมูลเป็นการป้องกันผู้ที่ไม่ประสงค์ดีเข้าถึงข้อมูลและโจรกรรมข้อมูลหรือกระทำการอันไม่พึงประสงค์ได้



รูปที่ 2.4 ขั้นตอนการพิสูจน์ตัวตน

การพิสูจน์ตัวตนแบบสองขั้นตอน ในบางครั้งการพิสูจน์ตัวตนโดยการใช้ชื่อผู้ใช้งานและรหัสผ่านเพื่อพิสูจน์ตัวตนนั้นอาจไม่เพียงพอ เนื่องจากการอนุญาตให้เข้าถึงข้อมูลบางประเภทนั้นนั้นเป็นข้อมูลที่มีความสำคัญมาก เช่น ข้อมูลทางด้านการเงิน ข้อมูลส่วนตัวของแต่ละบุคคล เป็นต้น ดังนั้นจึงต้องมีการเพิ่มเติมขั้นตอนในการพิสูจน์ตัวตน โดยมีขั้นตอนในการผู้ที่ต้องการเข้าถึงข้อมูลต้องร้องขอ Security Token จากผู้ที่ให้บริการข้อมูลก่อน แล้วผู้ต้องการเข้าถึงข้อมูลต้องนำ Security Token ที่ได้

รับมานำไปประกอบเป็นข้อมูลในการพิสูจน์ตัวตนเพื่อขอเข้าถึงข้อมูลของผู้ให้บริการนั้น ผู้ให้บริการก็จะดำเนินการตรวจสอบว่าเป็นผู้ที่มีสิทธิ์สามารถเข้าถึงข้อมูลได้หรือไม่ Security Token เป็นการสร้างรหัสเพิ่มเติมที่นอกเหนือจากชื่อผู้ขอเข้าใช้งานระบบ และรหัสผ่าน การพิสูจน์ตัวตนแบบสองขั้นตอนจะมีการนำ Security Token ไปใช้งานร่วมกับ ชื่อผู้ขอใช้งานระบบและรหัสผ่าน เป็นการสร้างความมั่นคงปลอดภัยในด้านการเข้าถึงข้อมูลให้มีความมั่นคงปลอดภัยเพิ่มมากขึ้นโดยเฉพาะการเข้าถึงข้อมูลที่มีความสำคัญมาก

2.5 WS-Security UsernameToken

การที่จะทำให้เว็บเซอร์วิสมีความมั่นคงปลอดภัยนั้นต้องมีกระบวนการเพื่อสร้างความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสตามมาตรฐาน WS-Security ซึ่งมาตรฐานการรักษาความมั่นคงปลอดภัยตามมาตรฐาน WS-Security มีหลายส่วน หนึ่งในนั้นคือ ยูสเซอร์เนมโทเคนตามมาตรฐานเปิดขององค์กร OASIS [4] ยูสเซอร์เนมโทเคนเป็นเทคโนโลยีการรักษาความมั่นคงปลอดภัยใน WS-Security เป็นการรักษาความมั่นคงปลอดภัยในด้านการเข้าถึงข้อมูล เป็นรูปแบบข้อมูลแทรกอยู่ใน SOAP Message Header ใช้เพื่อการพิสูจน์ตัวตนเพื่อเข้าถึงบริการข้อมูลของผู้ให้บริการเว็บเซอร์วิส ในมาตรฐานได้อธิบายวิธีการที่ผู้ขอใช้บริการเว็บเซอร์วิสนำยูสเซอร์เนมโทเคนไปใช้ในการพิสูจน์ตัวตนเพื่อขอเข้าใช้บริการและเข้าถึงข้อมูลเว็บเซอร์วิสของผู้ให้บริการโดยมาตรฐานแสดงวีธีการรักษาความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสในส่วน SOAP Message มีการประกาศตัวแปรยูสเซอร์เนมโทเคน (UsernameToken) ตามมาตรฐานที่ใช้ในการพิสูจน์ตัวตนใน SOAP Message Header ซึ่งประกอบไปด้วยตัวแปรชื่อผู้ใช้งานระบบ (Username), ตัวแปรรหัสผ่าน (Password), ตัวแปร Nonce เป็นค่าตัวอักษรสุ่ม (Random String) ของทางฝั่งผู้ขอใช้งานเว็บเซอร์วิสจะสร้างใหม่ทุกครั้งเมื่อต้องการติดต่อขอใช้งานเว็บเซอร์วิส, และ ค่าเวลาการทำรายการ (Createdtime) ของทางฝั่งผู้ขอใช้งานเว็บเซอร์วิส ดังรูปที่ 2.5 และตัวอย่างการใส่ค่าตัวแปรของยูสเซอร์เนมโทเคนดังรูปที่ 2.6 ค่าตัวแปร Nonce และค่าของตัวแปร Createdtime เป็นค่าที่องค์กร OASIS [4] ได้ประกาศใช้เพื่อการป้องกันการโจมตีจากผู้ไม่ประสงค์ดีแบบ Replay Attack

```
<wsse:UsernameToken wsu:Id="Example-1">
        <wsse:Username> ... </wsse:Username>
        <wsse:Password Type="..."> ... </wsse:Password>
        <wsse:Nonce EncodingType="..."> ... </wsse:Nonce>
        <wsu:Created> ... </wsu:Created>
</wsse:UsernameToken>
```

รูปที่ 2.5 การประกาศตัวแปรของยูสเซอร์เนมโทเคน [4]

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu= "...">
    <S11:Header>
        ...
        <wsse:Security>
            <wsse:UsernameToken>
                <wsse:Username>USRSIT</wsse:Username>
                <wsse:Password Type="...#PasswordDigest">
                seYI3nYd8LjMNVksCPFV8t3rgHh3Aw==
                </wsse:Password>
                <wsse:Nonce>PScqanjCEAA4mKoBE07sAQ==</wsse:Nonce>
                <wsu:Created>2012-07-16T01:29:38Z</wsu:Created>
            </wsse:UsernameToken>
        </wsse:Security>
        ...
    </S11:Header>
```

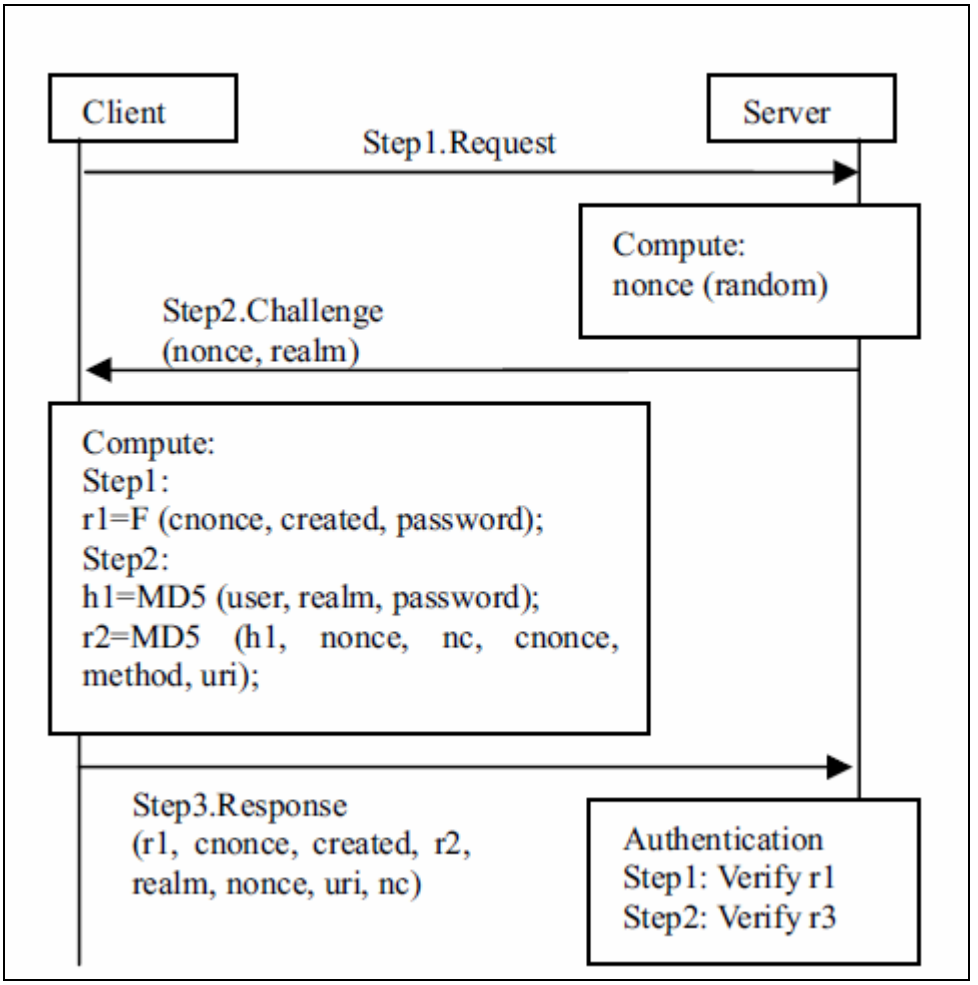
รูปที่ 2.6 ตัวอย่างการใส่ค่าตัวแปรของยูสเซอร์เนมโทเคน [4]

2.6 งานวิจัยที่เกี่ยวข้อง

ในการศึกษางานวิจัยที่เกี่ยวข้องนั้น จะเน้นศึกษางานวิจัยที่มีการวิจัยในเรื่องการพิสูจน์ตัวตนของเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนที่มีการเพิ่มประสิทธิภาพขั้นตอนการพิสูจน์ตัวตนให้มีประสิทธิภาพมากขึ้น ดังอธิบายในหัวข้อในส่วนความมั่นคงปลอดภัยเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนดังเนื้อหาต่อไปนี้

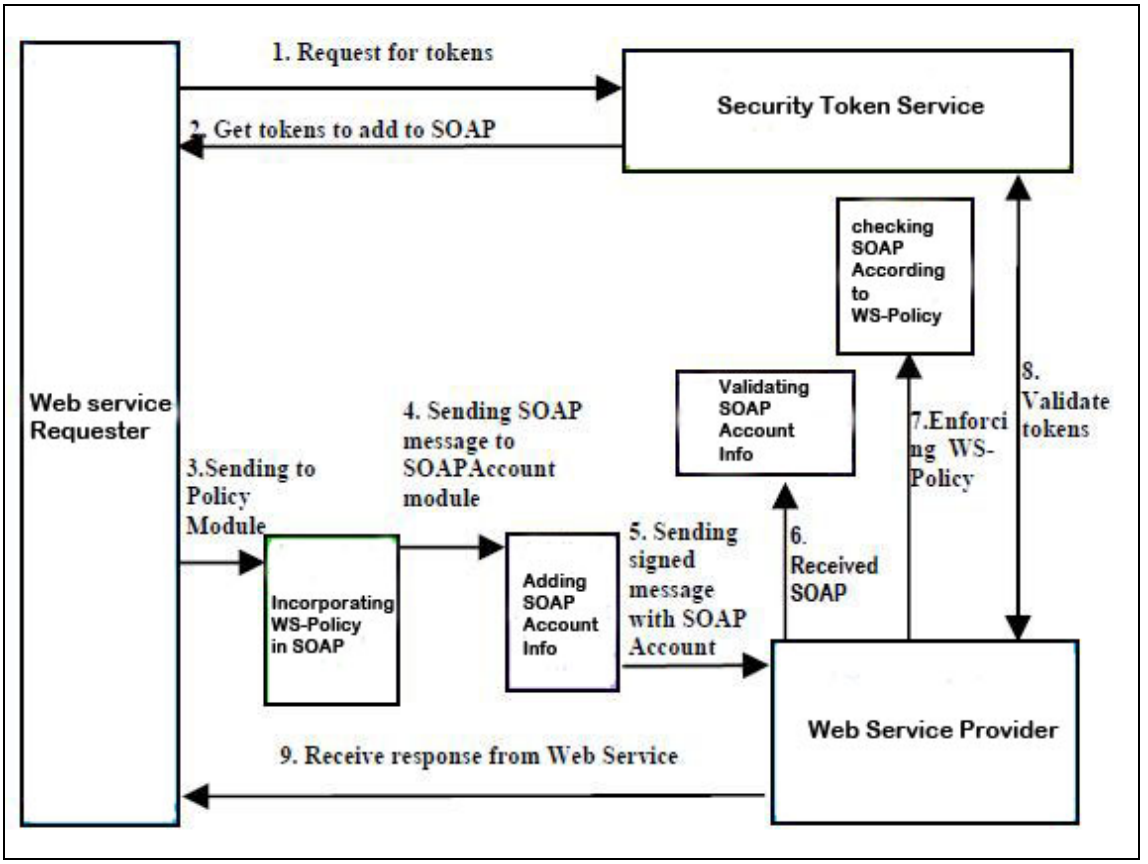
มาตรฐานของยูสเซอร์เนมโทเคนจะเป็นการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสแบบ SOAP Message ในงานวิจัยของ Peng และคณะ [5] ได้นำหลักการยูสเซอร์เนมโทเคนมาประยุกต์ใช้ในการพิสูจน์ตัวตนในการขอเข้าใช้บริการเว็บเซอร์วิสแบบ Rest-Style โดยการพิสูจน์ตัวตนผู้ที่ต้องการขอเข้าใช้บริการเว็บเซอร์วิสเป็นการรักษาความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสของผู้ให้บริการ และได้เสนอแนวคิด Secondary Password เข้ามาช่วยเพิ่มความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสในด้านการถูกโจมตีแบบ Replay Attack และ การถูกโจมตีแบบ Off-line Password Guessing Attack ได้เสนอกระบวนการพิสูจน์ตัวตนดังนี้คือ นำเสนอการพิสูจน์ตัวตนแบบ 2 ขั้นตอนของเว็บเซอร์วิสแบบ Rest-Style โดยการนำหลักการของยูสเซอร์เนมโทเคนและเสนอหลักการ Secondary Password นำหลักทั้งสองมาใช้ร่วมกันในการพิสูจน์ตัวตน การที่นำยูสเซอร์เนมโทเคนมาใช้ในการพิสูจน์ตัวตนเพียงอย่างเดียวนั้นมีจุดเสี่ยงคือเซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิสต้องทำการเก็บรหัสผ่านไว้ในเครื่องเซิร์ฟเวอร์ ถ้าเครื่องเซิร์ฟเวอร์ถูกโจรกรรมข้อมูล ผู้ไม่ประสงค์ดีสามารถนำรหัสผ่านมาใช้ตามหลักยูสเซอร์เนมโทเคนเพื่อสามารถผ่านการพิสูจน์ตัวตนในการเข้าถึงการใช้งานเว็บเซอร์วิสได้

ในงานวิจัยของ Peng และคณะ [5] จึงนำเสนอหลักการ Secondary Password ดังแสดงในรูปที่ 2.7 เข้ามาใช้ร่วมกับยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนเพื่อเป็นการตรวจสอบแบบ 2 ขั้นตอน ซึ่งการเข้าใช้งานเว็บเซอร์วิสของงานวิจัยนี้มีรูปแบบการติดต่อกันระหว่างผู้ให้บริการเว็บเซอร์วิสกับผู้ขอใช้บริการเว็บเซอร์วิสหรือ Message Flow จะมี 2 ขั้นตอน โดยขั้นตอนแรกทางผู้ขอใช้บริการเว็บเซอร์วิสต้องส่งคำร้องไปยังผู้ให้บริการเว็บเซอร์วิสเพื่อขอข้อมูลระบุตัวตนการขอเข้าใช้งาน ขั้นตอนที่สองเมื่อผู้ขอใช้บริการเว็บเซอร์วิสได้รับข้อมูลระบุตัวตนก็จะต้องนำข้อมูลนั้นมาเป็นข้อมูลส่วนหนึ่งในส่วนยูสเซอร์เนมโทเคนเพื่อใช้ในการพิสูจน์ตัวตนในการส่งคำร้องไปยังผู้ให้บริการเว็บเซอร์วิส ซึ่งเป็นการเพิ่มประสิทธิภาพในการรักษาความมั่นคงปลอดภัยให้กับเว็บเซอร์วิส



รูปที่ 2.7 ขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน [5]

ในงานวิจัยของ Rahaman และคณะ [6] มีการใช้ยูสเซอร์เนมโทเคนร่วมกับ SOAP Account ดังแสดงในรูปที่ 2.8 ซึ่งเป็นแนวคิดการเก็บโครงสร้างของ SOAP Message เป็นการช่วยให้สามารถตรวจสอบการโจมตีแบบ Replay Attack และ Rewriting Attack ได้ง่ายขึ้นและได้นำเสนอ Message Flow ในการติดต่อระหว่างเว็บเซอร์วิสที่มีการรักษาความมั่นคงปลอดภัยตามมาตรฐาน WS-Security และนำหลักการ SOAP Account ที่มีโมดูลช่วยตรวจสอบการโจมตีแบบ Rewriting Attack เพิ่มเติม



รูปที่ 2.8 ขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพิ่มแนวคิด SOAP Account [6]

จากงานวิจัย [5,6] จะเห็นได้ว่าทั้งสองงานวิจัยได้นำเสนอการรักษาความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสโดยใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตน รูปแบบการติดต่อกันระหว่างผู้ให้บริการเว็บเซอร์วิสกับผู้ขอใช้บริการเว็บเซอร์วิสจะเป็นการติดต่อแบบ 2 ขั้นตอน และยังได้เสนอแนวคิดวิธีการป้องกันการโจมตีดักจับ SOAP Message เพื่อนำ SOAP Message ที่ดักจับได้มาใช้ในการเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิส แต่งานวิจัยทั้งสองนั้นไม่ได้เน้นการใช้ยูสเซอร์เนมโทเคนให้มีประสิทธิภาพมากที่สุด เนื่องจากการพิสูจน์ตัวตนโดยใช้หลักการยูสเซอร์เนมโทเคนและป้องกันการโจมตีแบบ Replay Attack และการโจมตีแบบ Rewriting Attack ในหลักการของยูสเซอร์เนมโทเคนจะมีการนำค่า Nonce และ ค่า Createdtime ซึ่งเป็นค่าที่ผู้ขอใช้บริการเว็บเซอร์วิสสร้างขึ้นมาใหม่ทุกครั้งเมื่อต้องการขอเข้าใช้บริการเว็บเซอร์วิส ในส่วนของผู้ให้บริการเว็บเซอร์วิสจะดำเนินการตรวจสอบค่า Nonce ว่าทางผู้ขอเข้าใช้งานเว็บเซอร์วิสมีการนำค่า Nonce มาใช้ซ้ำหรือไม่ในเวลาที่ได้กำหนด เป็นการป้องกันการโจมตีแบบ Replay Attack และ Rewriting Attack ข้อเสียของการนำค่า Nonce มาใช้ป้องกันการโจมตีแบบดังกล่าวคือ ถ้ามีการทำรายการเพื่อขอเข้าใช้งานเว็บเซอร์วิสจำนวนมากทางฝั่งผู้ให้บริการเว็บเซอร์วิสจำเป็นต้องเก็บค่า Nonce ที่ได้รับมาจากผู้ขอใช้งานทุกค่าเพื่อใช้ตรวจสอบว่ามีการส่งค่าซ้ำหรือไม่มาจัดเก็บต่อกันเรื่อยๆในฐานข้อมูล ในการขอเข้าใช้บริการเว็บ

เซอร์วิสจำนวนมาก ผู้ให้บริการเว็บเซอร์วิสก็ต้องใช้ทรัพยากรหน่วยความจำในการเก็บค่า Nonce จำนวนมาก และในการตรวจสอบค่า Nonce ว่าซ้ำหรือไม่ก็ต้องใช้เวลาที่มากขึ้นในการค้นหาเพื่อเปรียบเทียบค่า Nonce ด้วย อีกนัยถ้าในด้านผู้ให้บริการเว็บเซอร์วิสกำหนดช่วงเวลาในการลบค่า Nonce ที่เก็บในหน่วยความจำนั้นกำหนดช่วงเวลาน้อยเกินไปก็ทำให้เสี่ยงต่อการถูกโจมตีแบบ Replay Attack และ Rewriting Attack ได้เพราะค่า Nonce ที่เก็บไว้ถูกลบไปแล้วเมื่อมีการตรวจสอบก็พบว่าค่า Nonce ที่ได้จากการดักจับ SOAP Message ที่ส่งมาจากผู้ไม่ประสงค์ดีนั้นไม่ซ้ำแล้วทำให้สามารถเข้าใช้งานเว็บเซอร์วิสได้ ในบทถัดไปนั้นจะเป็นการเสนอแนวทางการรักษาความมั่นคงปลอดภัยของเว็บเซอร์วิสโดยใช้ยูสเซอร์เนมโทเคนและป้องการโจมตีแบบ Replay Attack และ Rewriting Attack โดยการหลีกเหลี่ยงการเก็บค่า Nonce ทุกค่าในฐานข้อมูลที่ใช้พื้นที่ในการเก็บขนาดใหญ่มากเมื่อมีการทำรายการการใช้งานเว็บเซอร์วิสจำนวนมาก

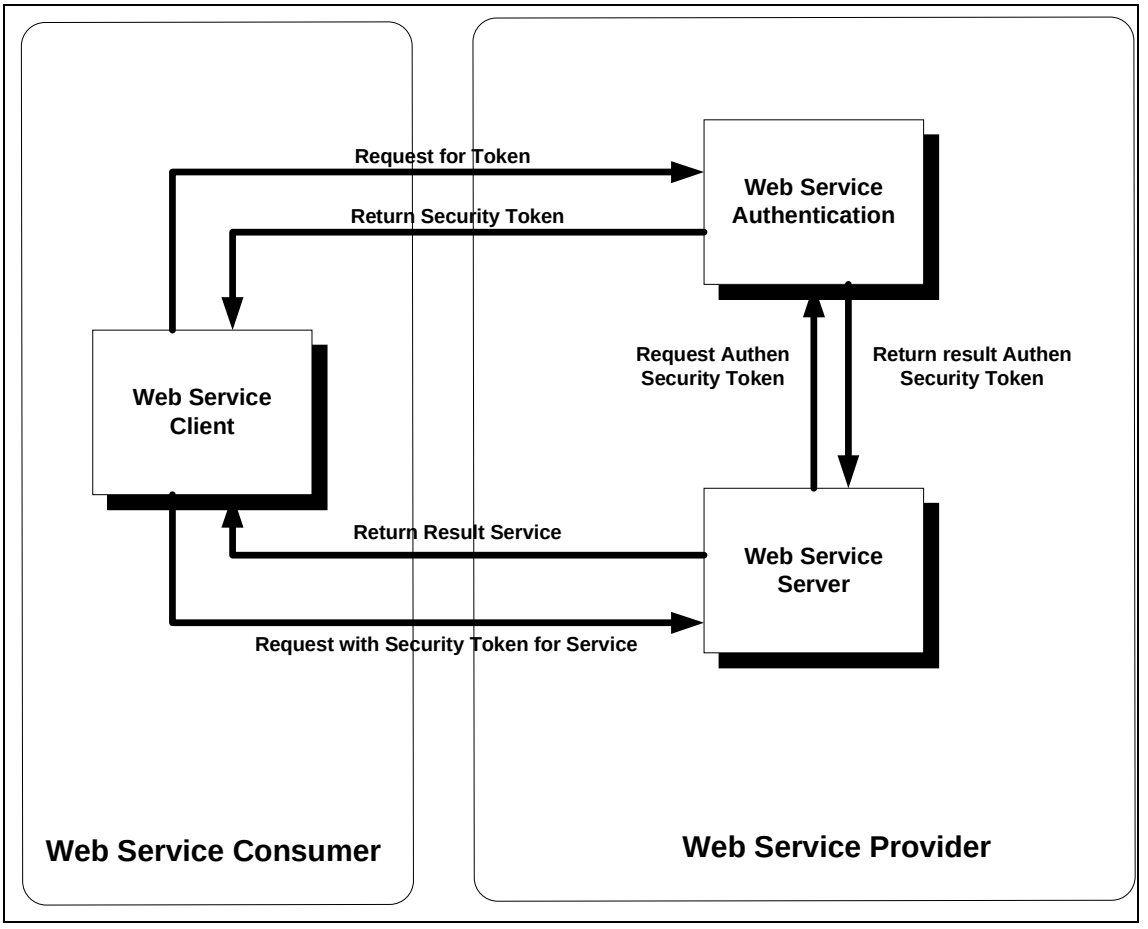
บทที่ 3
การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพื่อความมั่นคงปลอดภัยในเว็บเซอร์วิส

ในงานวิจัยฉบับนี้ได้ทำการศึกษาและเปรียบเทียบการดำเนินการพิสูจน์ตัวตนของเว็บเซอร์วิสผู้ขอใช้บริการและเว็บเซอร์วิสผู้ให้บริการด้วยยูสเซอร์เนมโทเคนในรูปแบบการพิสูจน์ตัวตนบนพื้นฐานแบบสองขั้นตอน การเปรียบเทียบนั้นจะทำการเปรียบเทียบประสิทธิภาพการทำงานระหว่างการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS มีการเก็บค่า Nonce ไว้ในฐานข้อมูลของเซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิส กับ การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS ที่มีการเสนอเทคนิคเพิ่มเติมในการจัดการการเก็บค่า Nonce ในเซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิส โดยลดการจัดเก็บค่า Nonce ทุกค่าไว้ในฐานข้อมูล เมื่อมีการทำรายการใช้บริการเว็บเซอร์วิสจำนวนมากการจัดเก็บค่า Nonce ของการพิสูจน์ตัวตนทั้งสองรูปแบบจะถูกนำมาศึกษาเปรียบเทียบประสิทธิภาพในการทำงาน

ซึ่งการทำการเปรียบเทียบ จะดำเนินการเปรียบเทียบในแง่ของเวลาที่ใช้ในกระบวนการทำงานของเว็บเซอร์วิส (Processing Time) ที่มีการพิสูจน์ตัวตนแบบสองขั้นตอน และการเสนอเทคนิคเพิ่มเติมนั้นได้มีการเพิ่มเติมในส่วน SPassword เพื่อช่วยเสริมความมั่นคงปลอดภัยให้กับเว็บเซอร์วิสในด้านการเข้าถึงข้อมูลในระดับ SOAP Message ของผู้ให้บริการเว็บเซอร์วิส เป็นการเพิ่มความมั่นคงปลอดภัยเสริมการป้องกันการโจมตีการเข้าถึงข้อมูลแบบ Replay Attack และ การโจมตีการเข้าถึงข้อมูลแบบ Rewriting และงานวิจัยนี้ได้มีการวิเคราะห์ถึงด้านความมั่นคงปลอดภัยของเว็บเซอร์วิสระหว่างการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS กับ การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS ที่มีการเสนอเทคนิคเพิ่มเติมโดยการพิสูจน์ตัวตนทั้งสองรูปแบบมีการทำงานภายใต้สภาพแวดล้อมเดียวกัน

3.1 รูปแบบการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน

ส่วนนี้เป็นการสำรวจศึกษาการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนบนพื้นฐานการพิสูจน์ตัวตนแบบสองขั้นตอน ดังรูป 3.1



รูปที่ 3.1 รูปแบบการพิสูจน์ตัวตนแบบสองขั้นตอน

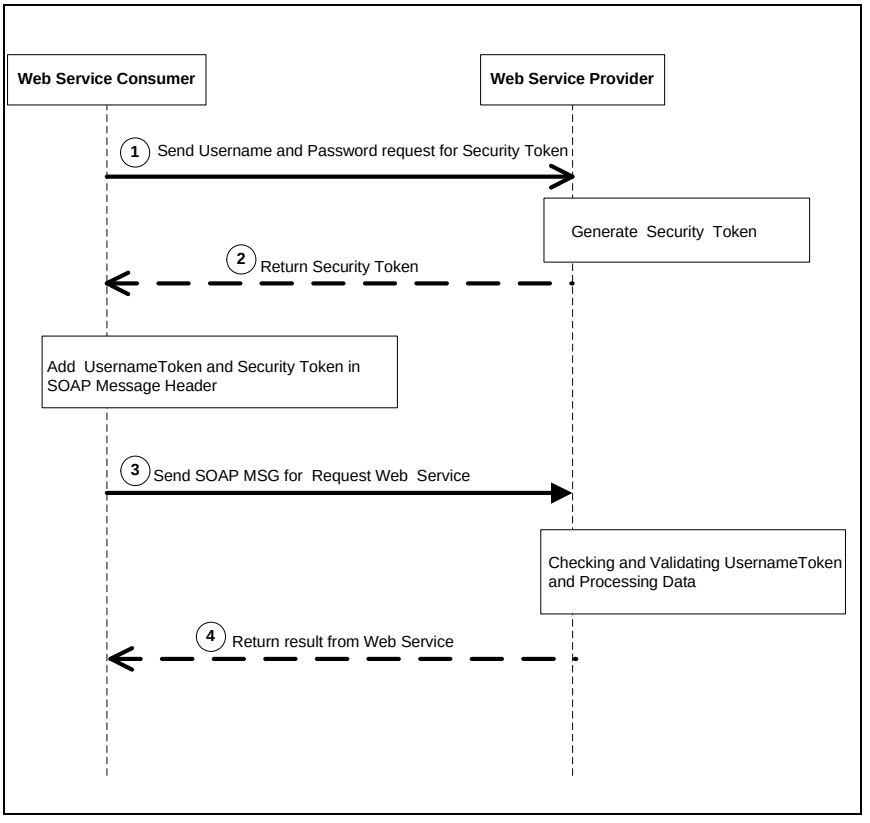
จากรูป 3.1 แสดงการพิสูจน์ตัวตนแบบสองขั้นตอน เริ่มจากผู้ขอใช้บริการเว็บเซอร์วิสต้องดำเนินการส่งคำร้องขอไปยังผู้ให้บริการเว็บเซอร์วิสเพื่อขอ Security Token ผู้ให้บริการเว็บเซอร์วิสทำการสร้าง Security Token แล้วส่งไปยังผู้ขอใช้บริการเว็บเซอร์วิส ทางผู้ขอใช้บริการเว็บเซอร์วิสจะนำ Security Token ที่ได้รับไปประมวลผลในการใส่เพิ่มเข้าไปใน SOAP Message Header และทำการส่ง SOAP Message ที่มี Security Token ส่งไปยังผู้ให้บริการเว็บเซอร์วิส เมื่อผู้ให้บริการเว็บเซอร์วิสได้รับ SOAP Message ก็จะนำ Security Token ที่อยู่ใน SOAP Message Header ของผู้ใช้บริการนั้นจะนำไปเข้ากระบวนการตรวจสอบพิสูจน์ตัวตนว่าเป็นผู้สามารถเข้าถึงข้อมูลได้จริงหรือไม่ ถ้าเป็นผู้ไม่สามารถเข้าถึงข้อมูลได้ก็จะทำการตอบกลับผู้ขอใช้บริการเว็บเซอร์วิสว่าไม่สามารถเข้าถึงข้อมูลได้แต่ถ้าตรวจสอบแล้วพบว่าเป็นผู้สามารถเข้าถึงข้อมูลได้ผู้ให้บริการเว็บเซอร์วิสก็จะอนุญาตให้เข้าถึงข้อมูลประมวลผลส่งผลลัพธ์กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส ในงานวิจัยนี้จะดำเนินการศึกษาการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนบนพื้นฐานการพิสูจน์ตัวตนแบบสองขั้นตอน และเปรียบเทียบประสิทธิภาพการทำงานของการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน

การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่ศึกษาในงานวิจัยนี้มีการศึกษาสองรูปแบบดังนี้คือ

- การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS
- การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS ที่มีการเสนอเทคนิคเพิ่มเติมหลีกเลี่ยงการตรวจสอบและจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูล

3.2 การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS

การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS มีขั้นตอนการพิสูจน์ตัวตนดังนี้คือ จากรูปที่ 3.2 แสดงขั้นตอนผู้ขอใช้บริการเว็บเซอร์วิสต้องการขอใช้บริการจากผู้ให้บริการเว็บเซอร์วิส



รูปที่ 3.2 ขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐาน

ขั้นตอนที่ 1 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้อง Username และ Password เพื่อร้องขอ Security Token กับทางผู้ให้บริการเว็บเซอร์วิสผู้ขอใช้บริการเว็บเซอร์วิสต้องดำเนินการส่งคำร้องขอไปยังเว็บเซอร์วิสผู้ให้บริการเพื่อขอ Security Token จากผู้ให้บริการเว็บเซอร์วิส

ขั้นตอนที่ 2 ผู้ให้บริการเว็บเซอร์วิสส่ง Security Token ให้ทางผู้ขอใช้บริการเว็บเซอร์วิส ผู้ให้บริการเว็บเซอร์วิสทำการสร้าง Security Token แล้วส่งไปยังผู้ขอใช้บริการเว็บเซอร์วิส

ขั้นตอนที่ 3 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอเพื่อขอเข้าใช้บริการเว็บเซอร์วิส ทางผู้ขอใช้บริการเว็บเซอร์วิสจะนำ Security Token ที่ได้รับไปประมวลผลในการใส่เพิ่มเข้าไปใน SOAP Message Header และทำการส่ง SOAP Message ที่มียูสเซอร์เนมโทเคนที่ประกอบด้วยพารามิเตอร์ Username, Password, Nonce และ Created ส่งไปยังผู้ให้บริการเว็บเซอร์วิส เริ่มต้นผู้ให้บริการเว็บเซอร์วิสทำการตรวจสอบค่าของ Security Token ที่แนบมาใน SOAP Message Header ว่าผู้ขอใช้บริการมีการส่ง Security Token ที่ได้รับจากผู้ให้บริการเป็นของจริงหรือใหม่ ถ้าเป็นค่าจริงแล้วจากนั้นก็จะดำเนินการพิสูจน์ตัวตนในส่วนของยูสเซอร์เนมโทเคน ในรูปที่ 3.3 แสดงตัวอย่าง SOAP Message Header ที่มียูสเซอร์เนมโทเคนแนบไปกับ SOAP Message เพื่อส่งคำขอร้องไปยังผู้ให้บริการเว็บเซอร์วิส ซึ่งยูสเซอร์เนมโทเคนจะมีค่าของพารามิเตอร์ดังนี้

- พารามิเตอร์ Username มีค่าคือ KMUTTUSR
- พารามิเตอร์ Password มีรูปแบบเป็น Password Digest
  Base64(SHA1[Nonce + Created + Password]) มีค่าคือ
  707e14667b409777db1d45a7505f2eb4c81fc023
- พารามิเตอร์ Nonce เป็นข้อความแบบสุ่มสร้างโดยผู้ขอใช้บริการเว็บเซอร์วิส มีค่าคือ
  U2FsdGVkX1+wcxGElzktLhB3fvrrCmxVyc+9Fm4ofhs=
- พารามิเตอร์ Created เป็นค่าเวลาที่ทำรายการของขอใช้บริการเว็บเซอร์วิสมีค่าคือ
  2013-02-16T17:30:32Z

```
<S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu= "...">
        <S11:Header>
        ...
                <wsse:Security>
                        <wsse:UsernameToken>
                                <wsse:Username>KMUTTUSR</wsse:Username>
                                <wsse:Password Type="...#PasswordDigest">
                                707e14667b409777db1d45a7505f2eb4c81fc023
                                </wsse:Password>
                                <wsse:Nonce>
                                U2FsdGVkX1+wcxGElzktLhB3fvrrCmxVyc+9Fm4ofhs=
                                </wsse:Nonce>
                                <wsu:Created>2013-02-16T17:30:32Z</wsu:Created>
                        </wsse:UsernameToken>
                </wsse:Security>
        ...
        </S11:Header>
        ...
</S11:Envelope>
```

รูปที่ 3.3 รายละเอียดค่าของยูสเซอร์เนมโทเคนใน SOAP Message Header

ค่า Nonce และค่า Created เป็นค่าที่ใช้ในการป้องกันการโจมตีแบบ Replay Attack เมื่อผู้ให้บริการเว็บเซอร์วิสได้รับ SOAP Message ก็จะนำยูสเซอร์เนมโทเคนที่อยู่ใน SOAP Message Header นั้นจะนำไปตรวจสอบพิสูจน์ตัวตนว่าเป็นผู้สามารถเข้าถึงข้อมูลได้จริงหรือไม่ โดยมีวิธีการตรวจสอบดังต่อไปนี้คือ

- ตรวจสอบค่า Nonce

  ค่าของพารามิเตอร์ Nonce เป็นค่าข้อความแบบสุ่มที่ทางผู้ขอใช้บริการเว็บเซอร์วิสส่งมาให้ผู้ให้บริการเว็บเซอร์วิสเมื่อมีการร้องขอใช้บริการ ทางผู้ให้บริการเว็บเซอร์วิสจะนำค่า Nonce ไปทำการตรวจสอบกับค่า Nonce เดิมที่เคยมีการทำรายการเข้ามานั้นที่เก็บไว้ในพื้นที่ที่ใช้เก็บข้อมูล เช่น ฐานข้อมูล ในงานวิจัยนี้จะใช้ฐานข้อมูลเป็นที่เก็บค่า Nonce โดยตรวจสอบค่า Nonce ที่รับมาว่าเคยมีค่า Nonce ที่เก็บไว้ซ้ำกันหรือไม่ถ้าซ้ำก็จะไม่

อนุญาตให้ผู้ร้องขอเข้าถึงข้อมูลได้ ซึ่งในการทำรายการร้องขอใช้บริการเว็บเซอร์วิสของนั้น ผู้ให้บริการจะมีการเก็บค่า Nonce ที่ได้รับมาในฐานข้อมูลเสมอและจะดำเนินการลบค่า Nonce ก็ต่อเมื่อถึงระยะเวลาที่ได้ตั้งไว้ในการลบค่า Nonce นั้น ถ้าในกรณีมีการทำรายการขอใช้บริการเว็บเซอร์วิสของผู้ให้บริการจำนวนมากก็จะทำให้ต้องเก็บค่า Nonce ที่ได้รับมาไว้ในฐานข้อมูลใช้พื้นที่ในการจัดเก็บจำนวนมากเช่นกัน และถ้าทางผู้ให้บริการเว็บเซอร์วิสกำหนดเวลาที่จะลบค่า Nonce ที่เก็บไว้ในฐานข้อมูลนั้นกำหนดช่วงเวลาลบน้อยไปก็เป็นจุดเสี่ยงที่ผู้ไม่ประสงค์ดีทำการโจมตีแบบ Replay Attack โดยทำการดักจับ SOAP Message และนำ SOAP Message ที่ดักจับนั้นทำรายการเข้ามาใหม่และสามารถเข้าถึงข้อมูลได้เช่นกัน เพราะเป็น SOAP Message ชุดเดียวกันที่สามารถทำรายการขอใช้บริการเว็บเซอร์วิสได้ และทางผู้ให้บริการเว็บเซอร์วิสตรวจสอบค่า Nonce ที่ได้รับมากับค่า Nonce ที่เก็บไว้ในฐานข้อมูลแล้วไม่พบค่าที่ซ้ำกัน ซึ่งจุดนี้เป็นที่ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลผู้ให้บริการเว็บเซอร์วิสได้ และข้อเสียในการเก็บค่า Nonce จำนวนมากในฐานข้อมูลอีกประการหนึ่งนั้นคือ เมื่อผู้ให้บริการเว็บเซอร์วิสได้รับค่า Nonce จากทางผู้ขอใช้บริการเว็บเซอร์วิสแล้วต้องนำค่า Nonce ที่ได้รับมาเปรียบเทียบกับค่า Nonce เดิมที่เคยใช้ทำรายการที่เก็บไว้ในฐานข้อมูล เวลาที่ใช้ในการตรวจสอบค่า Nonce ว่ามีค่าที่ซ้ำกันหรือไม่ก็จะใช้เวลามากขึ้นเพราะต้องทำการเปรียบเทียบค่า Nonce ทั้งหมดที่เก็บไว้ในฐานข้อมูล ซึ่งมีจำนวนมากทำให้ส่งผลต่อประสิทธิภาพในการทำงานของโปรแกรมเว็บเซอร์วิสนั้นมีประสิทธิภาพในการทำงานลดลง

- ตรวจสอบค่า Created

ค่าพารามิเตอร์ Created เป็นค่าวันที่และเวลาที่ทางผู้ขอใช้บริการเว็บเซอร์วิสส่งไปยังผู้ให้บริการเว็บเซอร์วิสเมื่อมีการร้องขอใช้บริการเว็บเซอร์วิส ผู้ให้บริการเว็บเซอร์วิสจะนำค่าของ Created ไปทำการตรวจสอบกับช่วงเวลาที่กำหนดไว้หรือเรียกช่วงเวลานี้ว่า Freshness Time เป็นช่วงเวลากำหนดไว้เพื่อระบุว่ารายการที่ทำเข้ามาขอใช้บริการเว็บเซอร์วิสนั้นต้องเป็นรายการที่ร้องขออยู่ภายในช่วงเวลานี้เท่านั้น ถ้าค่าของ Created เป็นค่าที่นอกเหนือจากค่า Freshness Time ที่กำหนด ตัวอย่างเช่น กำหนด Freshness Time ไว้ 5 นาที ค่า Created ที่ได้รับมาจากผู้ขอใช้บริการเว็บเซอร์วิสจะต้องเป็นวันที่และเวลาที่ไม่ล่าช้ากว่าเวลา ของทางผู้ให้บริการเว็บเซอร์วิสอยู่ 5 นาทีทางผู้ให้บริการเว็บเซอร์วิสก็จะไม่อนุญาตให้ทำรายการขอใช้บริการเว็บเซอร์วิสเป็นต้น ค่า Created เป็นอีกค่าหนึ่งในยูเซอร์เนมโทเคนที่ใช้ในการป้องการการโจมตีแบบ Replay Attack

- ตรวจสอบค่า Username และ Password

เมื่อทางผู้ให้บริการเว็บเซอร์วิสได้รับค่า Username และ Password ก็ทำการนำ ค่า Username ไปตรวจสอบกับฐานข้อมูลว่าตรงกับค่าที่ได้เก็บไว้หรือไม่ โดยปกติจะมีการเก็บข้อมูลของผู้ต้องการใช้บริการเว็บเซอร์วิส เช่น ข้อมูลผู้ขอใช้บริการ ข้อมูล Username และข้อมูลรหัสผ่านไว้ในฐานข้อมูลของผู้ให้บริการเว็บเซอร์วิสเพื่อใช้เป็นข้อมูลในการตรวจสอบพิสูจน์ตัวตนการขอเข้าใช้งานเว็บเซอร์วิส ถ้าตรวจสอบแล้วพบว่าตรงกัน ผู้ให้บริการเว็บเซอร์วิสก็จะทำการนำค่ารหัสผ่านข้อมูล Password นั้นมารวมกับค่า Nonce และค่า Created ที่ได้รับมาทำการเข้ารหัสแบบ SHA1 เพื่อตรวจสอบกับค่า Password ที่ได้รับมาซึ่งค่า Password ที่ได้รับมานั้นเกิดจากผู้ขอใช้บริการเว็บเซอร์วิสทำการเข้ารหัสแบบเดียวกันคือ SHA1[Nonce + Created + Password] ผู้ให้บริการเว็บเซอร์วิสตรวจการเข้ารหัสของค่าทั้งสองนี้ว่ามีค่าตรงกันหรือไม่ ถ้าตรงกันผู้ให้บริการเว็บเซอร์วิสก็จะอนุญาตให้ผู้ขอใช้บริการสามารถเข้าถึงข้อมูลได้แต่ถ้าไม่ตรงก็จะไม่อนุญาตให้เข้าถึงข้อมูล

ขั้นตอนที่ 4 ผู้ให้บริการเว็บเซอร์วิสดำเนินการตรวจสอบการพิสูจน์ตัวตนและส่งค่ากลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส เมื่อผู้ให้บริการเว็บเซอร์วิสดำเนินการตรวจสอบการพิสูจน์ตัวตนในขั้นตอนที่ 3 เรียบร้อยแล้ว ถ้าการตรวจสอบพบว่าเป็นผู้ไม่สามารถเข้าถึงข้อมูลได้ก็จะทำการตอบกลับผู้ขอใช้บริการเว็บเซอร์วิสว่าไม่สามารถเข้าถึงข้อมูลได้ แต่ถ้าตรวจสอบแล้วพบว่าเป็นผู้สามารถเข้าถึงข้อมูลได้ผู้ให้บริการเว็บเซอร์วิสก็จะอนุญาตให้เข้าถึงข้อมูลประมวลผลส่งผลลัพธ์กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส

3.3 การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS มีการเสนอเทคนิคเพิ่มเติม

งานวิจัยนี้ได้มีการนำเสนอเทคนิคเพิ่มเติมในการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนบนพื้นฐานรูปแบบการพิสูจน์ตัวตนแบบสองขั้นตอน มีการเสนอเทคนิคขั้นตอนการพิสูจน์ตัวตนเพิ่มเติมดังต่อไปนี้

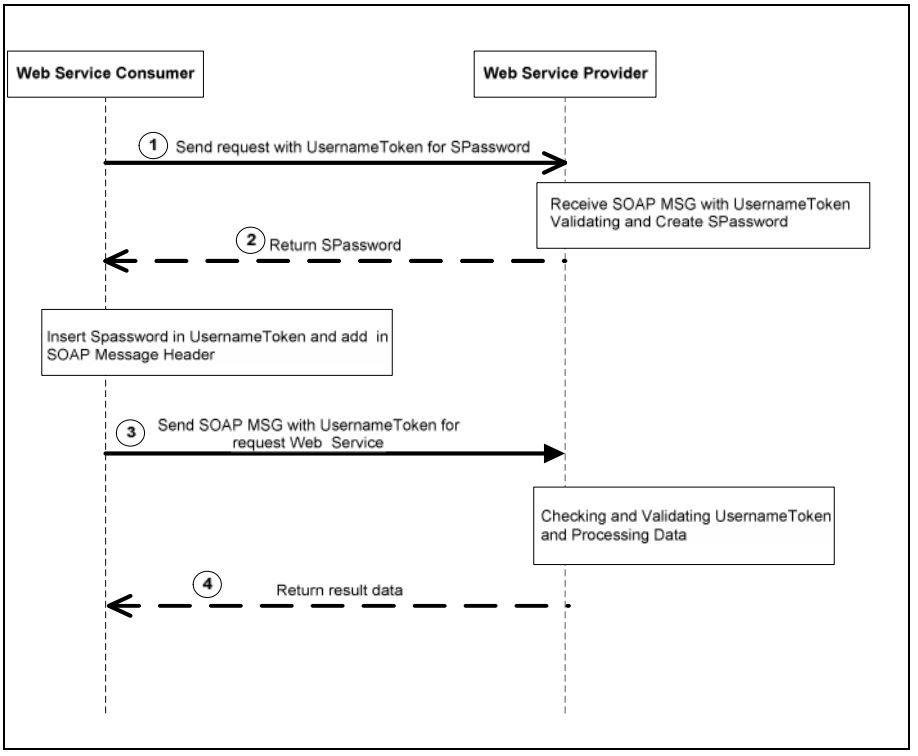
- นำเสนอโดยเพิ่มการพิสูจน์ตัวตนด้วยยูสเซอร์เซอร์เนมโทเคนแบบสองขั้นตอนที่ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องเพื่อร้องขอ Security Token กับทางผู้ให้บริการเว็บเซอร์วิสใช้หลักการตรวจสอบและอัพเดทค่า Nonce แทนการเก็บค่า Nonce ทุกค่าในฐานข้อมูล

- นำเสนอ SPassword ซึ่งเป็น Security Token ที่เกิดจากการสร้างจากทางผู้ให้บริการเว็บเซอร์วิส

การนำเสนอเทคนิคเพิ่มเติมที่ใช้ในการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนบนพื้นฐานรูปแบบการพิสูจน์ตัวตนแบบสองขั้นตอนนั้น เป็นวิธีการที่ช่วยในด้านการจัดการการเก็บค่า Nonce ของทางด้านผู้ให้บริการเว็บเซอร์วิสให้มีประสิทธิภาพเพิ่มขึ้น โดยหลีกเลี่ยงการจัดเก็บค่า Nonce ทุกค่าไว้ในฐานข้อมูลเพื่อแก้ไขปัญหาในด้านที่ต้องมีพื้นที่ในเครื่องเซิร์ฟเวอร์จำนวนมากเพื่อรองรับการจัดเก็บค่า Nonce ลดปัญหาการที่ต้องใช้เวลามากในการค้นหาค่า Nonce จำนวนมากในฐานข้อมูลเพื่อตรวจสอบว่าค่า Nonce เป็นค่าที่เคยมีการส่งเข้ามาทำรายการหรือไม่และเป็นการเพิ่มการรักษาความมั่นคงปลอดภัยในการขอเข้าถึงการใช้บริการเว็บเซอร์วิส

3.3.1 เทคนิคขั้นตอนการพิสูจน์ตัวตนที่นำเสนอ

ในงานวิจัยนำเสนอการเพิ่มการพิสูจน์ตัวตนด้วยยูสเซอร์เซอร์เนมโทเคนในขั้นตอนที่ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องเพื่อร้องขอ Security Token กับทางผู้ให้บริการเว็บเซอร์วิส และนำเสนอ SPassword ซึ่งเป็น Security Token ที่เกิดจากการสร้างจากทางผู้ให้บริการเว็บเซอร์วิส เทคนิคขั้นตอนที่นำเสนอสามารถอธิบายตามขั้นตอนได้ดังนี้ จากรูปที่ 3.4 เป็นการแสดงขั้นตอนที่มีการเสนอเทคนิคเพิ่มเติมและสามารถอธิบายได้ดังนี้



รูปที่ 3.4 ขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนแบบที่นำเสนอ

ขั้นตอนที่ 1 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องที่มียูสเซอร์เนมโทเคนใน SOAP Message Header เพื่อร้องขอ SPassword กับทางผู้ให้บริการเว็บเซอร์วิส ในขั้นตอนนี้มีการให้ทางผู้ขอใช้บริการเว็บเซอร์วิสจะต้องส่งคำขอใช้บริการหรือ SOAP Message ที่มีการแนบยูสเซอร์เนมโทเคนมาเพื่อขอ SPassword ซึ่งเป็น Security Token ที่ทางผู้ให้บริการเว็บเซอร์วิสเป็นผู้สร้างขึ้น ที่ทางผู้ขอใช้บริการเว็บเซอร์วิสจะต้องส่งยูสเซอร์เนมโทเคนเพื่อมาขอ SPassword นั้นเพื่อเป็นการสร้างความมั่นคงปลอดภัยให้กับการร้องขอ SPassword หรือ Security Token เพื่อนำไปใช้ในการพิสูจน์ตัวตนในการขอเข้าใช้งานผู้ให้บริการเว็บเซอร์วิส

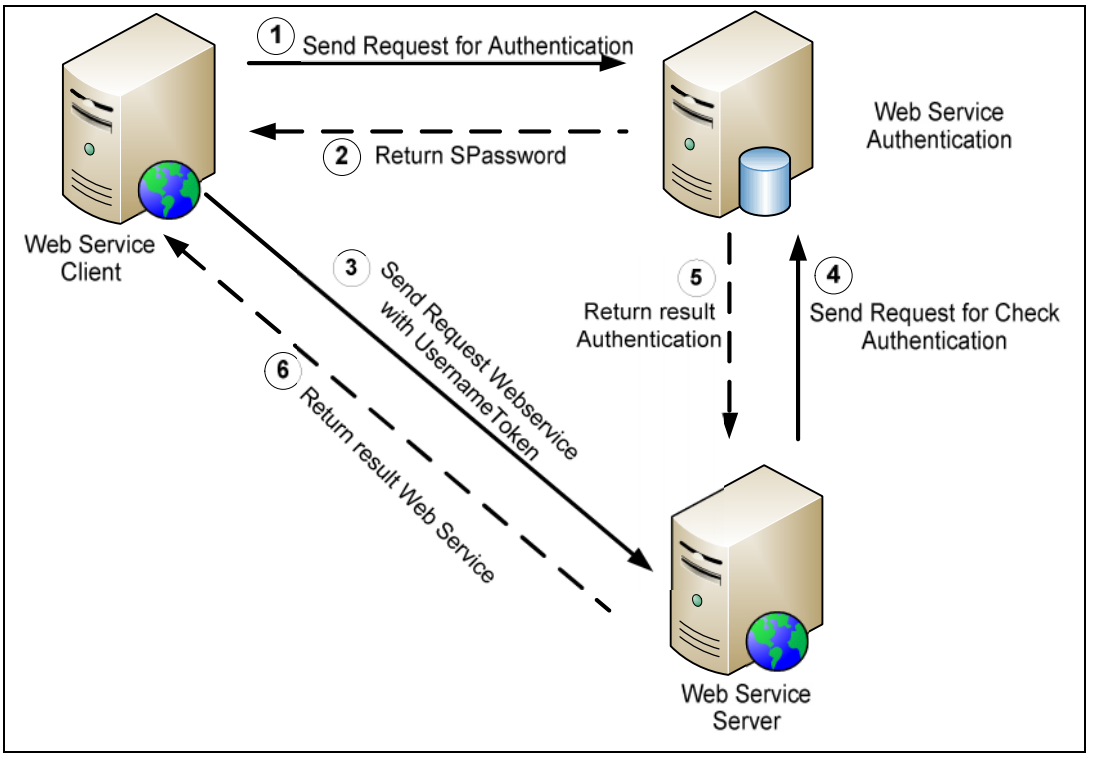
ขั้นตอนที่ 2 ผู้ให้บริการเว็บเซอร์วิสส่ง SPassword ให้ทางผู้ขอใช้บริการเว็บเซอร์วิส โดยผู้ให้บริการเว็บเซอร์วิสทำการสร้าง SPassword ซึ่งเป็น Security Token แล้วส่งไปยังผู้ขอใช้บริการเว็บเซอร์วิส ซึ่งกระบวนการนี้จะมีกระบวนการสร้าง SPassword เป็นหลักการหนึ่งที่จะช่วยในเรื่องการหลีกเลี่ยงการจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูลและเป็นส่วนที่ช่วยเพิ่มความมั่นคงปลอดภัยให้กับการเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิสเพราะการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนนั้นจะมีจุดเสี่ยงในเรื่องที่จะต้องเก็บชื่อผู้เข้าใช้งานระบบและรหัสผ่านไว้ที่ฐานข้อมูลของผู้ให้บริการเว็บเซอร์วิส ซึ่งกระบวนการสร้าง SPassword จะกล่าวในส่วนของแนวทางที่นำเสนอเนื้อหาถัดไป

ขั้นตอนที่ 3 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอเพื่อเข้าใช้บริการเว็บเซอร์วิสทางผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอที่มีการนำ SPassword ที่ได้รับมา นำมาทำเป็นค่าของพารามิเตอร์ Password ที่มีรูปแบบ Password Digest ซึ่งเป็นพารามิเตอร์หนึ่งในยูสเซอร์เนมโทเคน ซึ่งค่า Password ในยูสเซอร์เนมโทเคนมีรูปแบบการสร้างค่าโดยนำค่า Nonce, ค่า Created, ค่า Password (ค่ารหัสผ่านที่ได้รับเมื่อลงทะเบียนขอใช้งานเว็บเซอร์วิส)รวมกับ ค่า Spassword และนำค่าทั้งหมดที่ได้รับมาเข้ารหัสแบบ SHA1 ดังนี้คือ Base64(SHA1[Nonce + Created + Password+SPassword]) ซึ่งผู้ขอใช้บริการเว็บเซอร์วิสจะส่ง SOAP Message ไปยังผู้ให้บริการเว็บเซอร์วิสเพื่อร้องขอการเข้าใช้บริการเว็บเซอร์วิส

ขั้นตอนที่ 4 ผู้ให้บริการเว็บเซอร์วิสดำเนินการตรวจสอบการพิสูจน์ตัวตนและส่งค่ากลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส เมื่อทางผู้ให้บริการเว็บเซอร์วิสได้รับคำร้องขอเข้าใช้บริการเว็บเซอร์วิสที่มียูสเซอร์เนมโทเคนจากผู้ขอใช้บริการเว็บเซอร์วิส ก็จะนำค่าในยูสเซอร์เนมโทเคนนั้นนำมาเข้ากระบวนการตรวจสอบพิสูจน์ตัวตนผู้ขอเข้าใช้บริการเว็บเซอร์วิสว่าเป็นตัวตนจริงหรือหรือไม่ ซึ่งกระบวนการตรวจสอบจะเป็นกระบวนการที่เสนอในส่วนของแนวทางซึ่งเป็นกระบวนการการตรวจสอบพิสูจน์ตัวตนในการหลีกเลี่ยงการเก็บค่า Nonce จำนวนมากไว้ในฐานข้อมูลซึ่งจะนำเสนอเนื้อหาถัดไป และผลการตรวจสอบพบว่าเป็นผู้ไม่สามารถเข้าถึงข้อมูลได้ก็จะทำการตอบกลับผู้ขอใช้บริการเว็บเซอร์วิสว่าไม่สามารถเข้าถึงข้อมูลได้ แต่ถ้าตรวจสอบแล้วพบว่าเป็นผู้สามารถเข้าถึงข้อมูล

ได้ผู้ให้บริการเว็บเซอร์วิสก็จะอนุญาตให้เข้าถึงข้อมูลประมวลผลส่งผลลัพธ์กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส

งานวิจัยนี้จะนำเสนอกระบวนการการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนบนพื้นฐานรูปแบบการพิสูจน์ตัวตนแบบสองขั้นตอน โดยหลีกเลี่ยงการจัดเก็บค่า Nonce จำนวนมากไว้ใน ฐานข้อมูลพื้นที่ขนาดใหญ่ ในแนวทางที่นำเสนอนั้น และงานวิจัยนี้ยังได้เสนอการเพิ่มความมั่นคงปลอดภัยให้กับการร้องขอเข้าใช้บริการเว็บเซอร์วิสด้วยเสนอแนวคิด SPassword เพื่อเป็นเพิ่มการป้องกันการโจมตีแบบ Replay Attack และการโจมตีแบบ Rewriting Attack โดยมีการนำเสนอแนวคิดขั้นตอนการติดต่อสื่อสารของเว็บเซอร์วิสที่มีพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนดังต่อไปนี้



รูปที่ 3.5 การติดต่อสื่อสารของเว็บเซอร์วิสที่มีพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน

จากรูป 3.5 สามารถอธิบายได้ว่าการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่นำเสนอแบ่งได้สองส่วนคือ

- ส่วนที่ 1 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำขอไปยังเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน
- ส่วนที่ 2 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำขอไปยังผู้ให้บริการเว็บเซอร์วิส

ในการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนนั้นมีการนำเสนอโพรซีเดอร์ที่ใช้ในการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนของการขอเข้าใช้บริการเว็บเซอร์วิส มีสามโพรซีเดอร์ดังนี้คือ

- โพรซีเดอร์ 1 WSClientAuthen

- โพรซีเดอร์ 2 WSServerCheckAuthen
- โพรซีเดอร์ 3 Password_Digest

โดยโพรซีเดอร์ทั้งสามนี้จะอยู่ในส่วนของเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน ในรูปแสดงการติดต่อกันระหว่างผู้ขอใช้บริการเว็บเซอร์วิส (Web Services Client) กับ ผู้ให้บริการเว็บเซอร์วิส (Web Services Server) และการขอเข้าใช้บริการนั้นต้องมีการพิสูจน์ตัวตนโดยผ่านเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน (Web Services Authentication) มีการจัดเก็บค่าที่ใช้ในการพิสูจน์ตัวตนลงในฐานข้อมูล

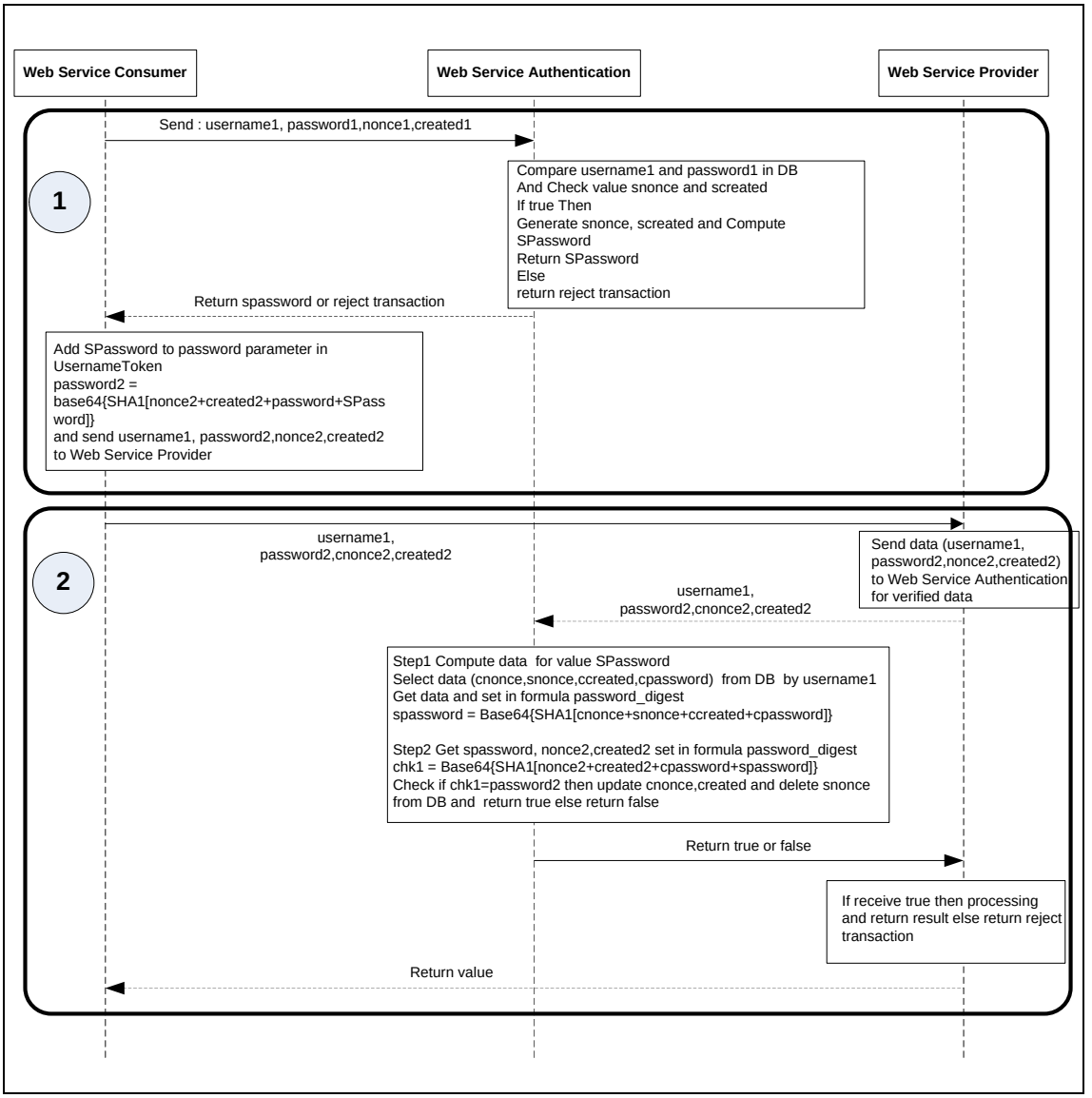
ตารางที่ 3.1 ค่าในฐานข้อมูลที่ใช้ในการพิสูจน์ตัวตน

CUsername	CPassword	CNonce	SNonce	CCreated	SCreated
KMSIT001	U2FsdGVkX1/kJHjKUMfCFPqX9YeMD8xqjhjzXMHtQiQ=	WScqanjCEAC4mQoBE07sAQ==	weYI3nXd8LjMNVksCKiJ=	2013-02-16T01:24:32Z	2013-02-16T01:24:42Z
KMSIT002	U2FsdGVkX1+wcxGElzktLhB3fvrrCmxVyc+9Fm4ofhs=	RSctanjmEU6mQoCE07sJQ==	jeYI3nyd8LjMOlksCKiJ=	2013-02-16T09:45:21Z	2013-02-16T09:45:32Z

จากตาราง 3.1 แสดงในส่วนตารางของฐานข้อมูลที่ใช้ในการจัดเก็บค่า Nonce นั้นโดยการวิจัยนั้นจะแสดงการจัดการในการเก็บค่า Nonce ที่ได้รับมาจากผู้ขอใช้บริการเว็บเซอร์วิสมีการเสนอขั้นตอนในการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนที่หลีกเลี่ยงการจัดเก็บค่า Nonce จำนวนมากที่ได้รับมาจากผู้ขอใช้งานเว็บเซอร์วิสเมื่อมีความต้องการเข้าขอใช้บริการเว็บเซอร์วิส

3.3.2 ขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนตามแนวคิดที่นำเสนอ

ในรูปที่ 3.6 แสดงขั้นตอนเริ่มต้นผู้ที่ต้องการใช้งานผู้ให้บริการเว็บเซอร์วิสต้องทำการลงทะเบียนก่อน โดยผู้ที่ต้องการขอใช้บริการเว็บเซอร์วิสจะได้รับ Username และ Password ซึ่งข้อมูลเหล่านี้ถูกเก็บไว้ในฐานข้อมูล ของ เซิร์ฟเวอร์เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนทางผู้ที่ต้องการขอใช้บริการเว็บเซอร์วิสจะต้องส่งข้อมูลเหล่านี้ในรูปแบบยูสเซอร์เนมโทเคน มาเพื่อใช้ในการพิสูจน์ตัวตนก่อนเข้าใช้บริการของผู้ให้บริการเว็บเซอร์วิส โดยมีการแบ่งขั้นตอนในการติดต่อสื่อสารเพื่อร้องขอใช้บริการข้อมูลเว็บเซอร์วิสเป็นสองส่วนใหญ่โดยสามารถอธิบายจากรูป 3.6 ดังนี้



รูปที่ 3.6 ขั้นตอนการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนตามแนวคิดที่นำเสนอ

ขั้นตอนในส่วนที่ 1 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำขอไปยังเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน ผู้ขอใช้บริการเว็บเซอร์วิสทำการสร้างค่า Nonce, Created และสร้างค่าของตัวแปร Password โดยค่าของตัวแปร Password ต้องอยู่ในรูปแบบ Password_Digest นำค่า Nonce,Created,Password เข้าโพรซีเดอร์ Password_Digest และนำค่าที่ได้มากำหนดค่าให้กับตัวแปรของยูสเซอร์เนมโทเคนแต่ละตัวแปรดังนี้ Username, Password, Nonce, Created จากนั้นผู้ขอใช้บริการเว็บเซอร์วิสทำการส่งคำร้องในรูปแบบ SOAP Message ไปยังทางเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน โดยส่งค่าของตัวแปรยูสเซอร์เนมโทเคนแนบไปกับ SOAP Message ซึ่งอยู่ในส่วนของ SOAP Message Header

เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนได้รับค่าของตัวแปรยูสเซอร์เนมโทเคนที่ผู้ขอใช้บริการเว็บเซอร์วิสส่งมาทาง เว็บเซอร์วิสพิสูจน์ตัวตนจะนำค่าที่ได้รับมาเข้าประมวลผลในโพรซีเดอร์ WSClientAuthen โดยจะโพรซีเดอร์มีกระบวนการเช็คการพิสูจน์ตัวตนจากค่าที่ได้รับมากับ ค่าที่เก็บไว้ในฐานข้อมูล ที่เก็บข้อมูลที่ใช้ในการพิสูจน์ตัวตน การประมวลผลตามขั้นตอนใน โพรซีเดอร์ WSClientAuthen กรณีได้ผลลัพธ์ว่าการพิสูจน์ตัวตนไม่ผ่านก็จะส่งค่า Authen Fail กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส แต่ถ้ากรณีได้ผลลัพธ์ว่าการพิสูจน์ตัวตนผ่านก็จะสร้างค่า Snonce, Screated และทำการเก็บค่า Snonce, ค่า Screated, ค่า Nonce (เก็บในชื่อ Cnonce) และค่า Created (เก็บในชื่อ Ccreated) ที่ได้รับมาบันทึกลงในฐานข้อมูล เมื่อบันทึกข้อมูลเรียบร้อยจะนำ ค่า Snonce, Cnonce, Ccreated เข้า โพรซีเดอร์ Password_Digest เพื่อสร้าง Spassword แล้วจึงส่งค่า Spassword กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส ขั้นตอนในส่วนที่ 2 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำขอไปยังผู้ให้บริการเว็บเซอร์วิส

ผู้ขอใช้บริการเว็บเซอร์วิสนำค่าที่ได้รับจากขั้นตอนในส่วนที่ 1 ซึ่งเป็นผลลัพธ์จากการส่งคำขอเพื่อไปพิสูจน์ตัวตนในกรณีได้ผลลัพธ์ว่าการพิสูจน์ตัวตนผ่านก็จะได้รับค่า Spassword กลับมา ทางผู้ขอใช้บริการเว็บเซอร์วิสทำการสร้างค่า Nonce, ค่า Created ใหม่อีกครั้งและนำค่า Nonce, Created, Password + Spassword นำไปเข้าโพรซีเดอร์ Password_Digest และนำค่าที่ได้มากำหนดค่าให้กับตัวแปรของยูสเซอร์เนมโทเคนแต่ละตัวแปรดังนี้ Username, Password, Nonce, Created

ผู้ขอใช้บริการเว็บเซอร์วิสทำการส่งคำร้องในรูปแบบ SOAP Message ไปยังผู้ให้บริการเว็บเซอร์วิสทาง ผู้ขอใช้บริการเว็บเซอร์วิสส่งค่าของตัวแปรยูสเซอร์เนมโทเคนแนบไปกับ SOAP Message ซึ่งอยู่ในส่วนของ SOAP Message Header ผู้ให้บริการเว็บเซอร์วิสได้รับค่าของตัวแปรยูสเซอร์เนมโทเคนที่ผู้ขอใช้บริการเว็บเซอร์วิสส่งมา ทางผู้ให้บริการเว็บเซอร์วิสจะนำค่าที่ได้รับมาเข้าส่งไปเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนและนำค่าที่ได้รับไปประมวลผลในโพรซีเดอร์ WSServerCheckAuthen

ในส่วนของโพรซีเดอร์ WSServerCheckAuthen จะนำค่าที่ได้รับไปตรวจสอบกับฐานข้อมูลที่เก็บข้อมูลการพิสูจน์ตัวตนประมวลตามขั้นตอนใน โพรซีเดอร์ WSServerCheckAuthen ผลกรณีได้ผลลัพธ์ว่าการพิสูจน์ตัวตนไม่ผ่านก็จะส่งค่า false กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส แต่ถ้ากรณีได้ผลลัพธ์ว่าการพิสูจน์ตัวตนผ่านก็จะทำการอัพเดทฐานข้อมูลที่ฟิลด์ Cnonce เป็นค่า Nonce ที่ได้รับมาใหม่ และฟิลด์ Ccreated เป็นค่า Created ที่ได้รับมาใหม่ แล้วส่งค่า True กลับไปยังผู้ให้บริการเว็บเซอร์วิส ทางผู้ให้บริการเว็บเซอร์วิสเมื่อได้รับค่าที่ตอบกลับมาจากเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนก็จะตรวจสอบค่าที่ได้จากเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนกรณีได้รับค่าเป็น True จะดำเนินการอนุญาตให้สามารถเข้าถึงการประมวลผลและส่งผลลัพธ์ที่ได้จากการประมวลผลกลับไปยังผู้ขอใช้บริการเว็บ

เซอร์วิส ถ้ากรณีได้รับค่าเป็น False ทางผู้ให้บริการเว็บเซอร์วิสจะส่งค่า Authen Fail กลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส

3.3.3 โพรซีเดอร์ที่ใช้ในการพิสูจน์ตัวตนด้วยยูเซอร์เนมโทเคน

โพรซีเดอร์ที่ใช้ในงานวิจัยดังต่อไปนี้

1) โพรซีเดอร์ WSClientAuthen เป็นโพรซีเดอร์ใช้ในการพิสูจน์ตัวตนในส่วนที่ 1 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำขอไปยังเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนมีรายละเอียดดังนี้

```
Procedure 1
Function  WSClientAuthen(wcUsername,wcPassword,wcNonce,wcCreated)
BEGIN
        Query data in Table tb_Authen  search  by   wcusername
                If  not  found data
                Then
                        Return Authen Fail
                Else
                        Get data at Table tb_Authen  Field CPassword
                        chkCPassword = Password_Digest(wcNonce, wcCreated,
                        CPassword)
                        Check Value chkCPassword and wcPassword
                        If  chkCPassword not equal with wcPassword
                        Then
                                Return Authen Fail
                        Else
                                Check Field SNonce and SCreated in DB
                                If SNonce value not null and SCreated value not equal Expired
                                Then
                                        Return Authen Fail
                                Else
                                        Generate SNonce and SCreated
                                        Update data wcNonce, wcCreated,
                                        SNonce,SCreated in table  tb_Authen

                                        Create   SPassword
                                        acNonce = wcNonce + SNonce
                                        SPassword = Password_Digest(acNonce,
                                        wcCreated, CPassword)

                                        Return  SPassword
END
```

รูปที่ 3.7 รายละเอียดโพรซีเดอร์ WSClientAuthen

จากรูป 3.7 ภายในโพรซีเดอร์ WSClientAuthen จะมีการรับค่าตัวแปร 4 ตัวที่ได้รับจากผู้ขอใช้บริการเว็บเซอร์วิสโดยการส่งค่าในรูปแบบยูสเซอร์เนมโทเคนผ่าน SOAP Message Header มีดังนี้คือ ตัวที่หนึ่ง wcUsername เป็นค่าชื่อผู้เข้าใช้งานระบบ ตัวที่สอง wcPassword เป็นค่ารหัสผ่านที่ได้เข้ารหัสตามมาตรฐานของยูสเซอร์เนมโทเคน ตัวที่สาม wcNonce เป็นค่าตัวอักษรแบบสุ่มที่สร้างโดยผู้ขอใช้บริการเว็บเซอร์วิส ตัวที่สี่ wcCreated เป็นค่าวันที่เวลาที่ทำรายการของผู้ขอใช้บริการเว็บเซอร์วิส โดยการทำงานของฟังก์ชันนี้เริ่มต้นฟังก์ชันจะนำค่า wcUsername นำไปค้นหาในฐานข้อมูลว่ามีผู้ใช้งานระบบในฐานข้อมูลหรือไม่ ถ้าไม่มีฟังก์ชันจะส่งค่ากลับผู้ขอใช้บริการเว็บเซอร์วิสเป็นค่า Authen Fail ถ้ามีชื่อผู้ใช้งานระบบก็จะดำเนินการตรวจสอบค่ารหัสผ่านโดยการดึงข้อมูลของฟิวล์ CPassword ที่อยู่ในฐานข้อมูลแถวเดียวกับค่าชื่อผู้ใช้งานระบบนั้น นำค่า wcNonce ค่า wcCreated และค่า CPassword นำไปเข้าโพรซีเดอร์ Password_Digest เพื่อนำค่าที่ได้รับจากการเข้าโพรซีเดอร์ Password_Digest มาสร้างเป็นค่า chkCPassword เมื่อได้ค่า chkCPassword แล้วให้นำค่า wcPassword มาเปรียบเทียบกับค่า chkCPassword ว่ามีค่าตรงกันหรือไม่ ถ้าผลลัพธ์มีค่าไม่ตรงกันให้ดำเนินการส่งค่ากลับผู้ขอใช้บริการเว็บเซอร์วิสเป็นค่า Authen Fail ถ้าผลลัพธ์ค่าทั้งสองตรงกันให้ดำเนินการตรวจสอบค่าข้อมูลของฟิวล์ SNonce และ SCreated ที่อยู่ในฐานข้อมูลแถวเดียวกับค่าชื่อผู้ใช้งานระบบ ตรวจสอบค่าของ SNonce ว่าเป็นค่าว่างหรือไม่ และถ้าค่า SNonce ไม่ใช่ค่าว่างก็จะตรวจสอบค่า SCreated เทียบกับวันที่และเวลาของเซิร์ฟเวอร์ของเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนผลที่ได้ต้องไม่เกินช่วงเวลาที่กำหนดไว้ถ้าเกินจะถือว่าค่า SNonce จะเป็นค่าที่ยังไม่หมดอายุแล้ว ระบบจะไม่อนุญาตให้สามารถทำรายการได้ให้ดำเนินการส่งค่ากลับผู้ขอใช้บริการเว็บเซอร์วิสเป็นค่า Authen Fail แต่ถ้าตรวจสอบแล้วค่า SNonce หมดอายุให้ดำเนินการสร้างค่า SNonce ขึ้นโดยการสร้างตัวอักษรแบบสุ่มและดำเนินการสร้าง SCreated โดยการนำวันที่และเวลานำมาสร้างเป็นค่า SCreated และดำเนินการบันทึกในฐานข้อมูลดังนี้ ค่า wcNonce บันทึกลงในฟิวด์ CNonce บันทึกค่า wcCreated ลงในฟิวด์ CCreated บันทึกค่า SNonce ลงในฟิวด์ SNonce และ บันทึกค่า SCreated ลงในฟิวด์ SCreated เมื่อบันทึกข้อมูลเสร็จให้ดำเนินการสร้างค่า SPassword โดยการ สร้างค่าตัวแปร acNonce โดยค่า acNonce เกิดจากการนำค่า wcNonce นำมารวมตัวอักษรต่อกันกับค่า SNonce แล้วให้นำค่า acNonce ค่า wcCreated และค่า CPassword นำไปเข้าโพรซีเดอร์ Password_Digest ผลลัพธ์ที่ได้รับจากโพรซีเดอร์ Password_Digest จะเป็นค่าของ SPassword เมื่อดำเนินการสร้าง SPassword เสร็จเรียบร้อยแล้วก็จะส่งค่า SPassword เป็นผลลัพธ์ส่งกลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส

2) โพรซีเดอร์ WSServerCheckAuthen เป็นโพรซีเดอร์ใช้ในการพิสูจน์ตัวตนในส่วนที่ 2 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำขอไปยังผู้ให้บริการเว็บเซอร์วิสมีรายละเอียดดังต่อไปนี้

```
Procedure 2
Function WSServerCheckAuthen(wsUsername,wsPassword,wsNonce,wsCreated)
BEGIN
        Query data in Table tb_Authen search by wsUsername
                If not found data
                Then
                        Return False
                Else
                        Check value SNonce in tb_Authen
                        If SNonce equal null
                        Then
                                Return False
                        Else
                                Get data at Table tb_Authen Field
                                (CPassword,CNonce,SNonce,CCreated)
                                SPassword = Password_Digest(CNonce+SNonce, CCreated,
                                CPassword)
                                chkWSPassword = Password_Digest(wsNonce, wsCreated,
                                                        Cpassword+SPassword)
                                Check wsPassword equal to chkWSPassword
                                If wsPassword not equal with chkWSPassword
                                Then
                                        Return False
                                Else
                                        Update data CNonce= wsNonce,CCreated= wsCreated
                                        in tb_Authen

                                        Delete data SNonce and SCreated in tb_Authen

                                        Return True
END
```

รูปที่ 3.8 รายละเอียดโพรซีเดอร์ WSServerCheckAuthen

จากรูป 3.8 ภายในโพรซีเดอร์ WSServerCheckAuthen จะมีการรับค่าตัวแปร 4 ตัวที่ได้รับจากผู้ให้บริการเว็บเซอร์วิสมีดังนี้คือ ตัวที่หนึ่ง wsUsername เป็นค่าชื่อผู้เข้าใช้งานระบบ ตัวที่สอง wsPassword เป็นค่ารหัสผ่านผู้ขอใช้บริการเว็บเซอร์วิสสร้างจากรหัสผ่านที่ได้จากการลงทะเบียนและรวมกับค่า SPassword ที่ได้รับจากเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนในส่วนแรกได้เข้ารหัสตามมาตรฐานของยูสเซอร์เนมโทเคนที่ทางผู้ให้บริการเว็บเซอร์วิสได้รับมาจากผู้ขอใช้บริการเว็บเซอร์วิส ตัวที่สาม wsNonce เป็นค่าตัวอักษรแบบสุ่มที่สร้างโดยผู้ขอใช้บริการเว็บเซอร์วิสและส่งไปให้กับผู้ให้บริการเว็บเซอร์วิส ตัวที่สี่ wsCreated เป็นค่าวันที่เวลาที่ทำรายการของผู้ขอใช้บริการเว็บเซอร์วิสและส่งไปให้กับผู้ให้บริการเว็บเซอร์วิส โดยการทำงานของฟังก์ชันนี้เริ่มต้นฟังก์ชันจะนำค่า wsUsername นำไปค้นหาในฐานข้อมูลว่ามีผู้ใช้งานระบบในฐานข้อมูลหรือไม่ ถ้าไม่มีฟังก์ชันจะส่งค่ากลับเว็บเซอร์วิสผู้ให้บริการเป็นค่า False ถ้ามีชื่อผู้ใช้งานระบบก็จะดำเนินการตรวจสอบค่า SNonce ที่อยู่ในฐานข้อมูลว่ามีค่าหรือไม่ ถ้าตรวจสอบแล้วไม่มีค่าฟังก์ชันจะส่งค่า False กลับไปยังเว็บเซอร์วิสผู้

ให้บริการแต่ถ้าตรวจสอบแล้วว่าค่า SNonce มีค่าก็จะดำเนินการตรวจสอบค่ารหัสผ่านโดยการดึงค่าข้อมูลของฟิวล์ CPassword, CNonce, SNonce และ CCreated ที่อยู่ในฐานข้อมูลแถวเดียวกับค่าชื่อผู้ใช้งานระบบนั้น และดำเนินการหาค่า SPassword โดยการนำค่า CNonce รวมกับค่า SNonce นำค่า wsCreated และค่า CPassword นำไปเข้าโพรซีเดอร์ Password_Digest เพื่อนำค่าที่ได้รับจากการเข้าโพรซีเดอร์ Password_Digest มาสร้างเป็นค่า SPassword

เมื่อได้ค่า SPassword แล้วให้ดำเนินการหาค่า chkWSPassword โดยการนำค่า wsNonce, ค่า wsCreated และนำค่าจากฐานข้อมูล CPassword มารวมกับค่า SPassword ซึ่งหาค่าได้จากขั้นตอนที่กล่าวมาแล้ว ให้นำค่าทั้งหมดนั้นนำไปเข้าโพรซีเดอร์ Password_Digest อีกครั้งเพื่อนำค่าที่ได้รับจากการเข้าฟังก์ชัน Password_Digest มาสร้างเป็นค่า chkWSPassword

เมื่อได้ค่า chkWSPassword แล้วให้นำค่า chkWSPassword มาเปรียบเทียบกับค่า wsPassword ว่ามีค่าตรงกันหรือไม่ ถ้าค่าเปรียบเทียบกันแล้วไม่ตรงกันฟังก์ชันจะส่งค่ากลับให้ผู้ให้บริการเว็บเซอร์วิสเป็น False ถ้าค่าเปรียบเทียบกันแล้วตรงกันฟังก์ชันจะดำเนินการบันทึกข้อมูลในฐานข้อมูลโดยบันทึกค่า wsNonce ลงในฟิวด์ CNonce บันทึกค่า wsCreated ลงในฟิวด์ CCreated และทำการลบค่า SNonce และค่า SCreated โดยการอัพเดทค่า SNonce และค่า SCreated เป็นค่าว่างในฐานข้อมูล เมื่อดำเนินการบันทึกค่าและลบค่าดังกล่าวในฐานข้อมูลเรียบร้อยแล้ว ฟังก์ชันจะดำเนินการส่งค่ากลับให้ผู้ให้บริการเว็บเซอร์วิสเป็นค่า True

ในส่วนโพรซีเดอร์ Password_Digest เป็นโพรซีเดอร์ใช้ในการสร้างรหัสผ่านของค่าพารามิเตอร์ Password ในยูสเซอร์เนมโทเคน ซึ่งเป็นโพรซีเดอร์ในการสร้างรหัสผ่านโดยการนำค่า ParamNonce ค่า ParamCreated และค่า ParamPassword นำมาเข้ารหัสด้วยอัลกอลิทึม SHA1 และ Base64 ให้รหัสผ่านอยู่ในรูปแบบตามมาตรฐานยูสเซอร์เนมโทเคนแบบตามมาตรฐานเปิด Web Service Security UsernameToken ที่ประกาศโดยองค์กร OASIS มีรายละเอียดดังต่อไปนี้

```
Procedure 3
Function Password_Digest(paramNonce,paramCreated,paramPassword)
BEGIN
        Return Base64{SHA1[paramNonce + paramCreated + paramPassword]}
END
```

รูปที่ 3.9 รายละเอียดโพรซีเดอร์ Password_Digest

จากรูป 3.9 ภายในโพรซีเดอร์ Password_Digest จะมีการรับค่าตัวแปร 3 ตัวที่ได้รับจากการส่งค่าของ Procedure 1 และ Procedure 2 ค่าที่ได้รับมีดังนี้ ค่า ParamNonce เป็นค่าตัวอักษรแบบสุ่มที่ได้รับเข้ามา ค่า ParamCreated เป็นค่าวันที่เวลาในการทำรายการที่ได้รับเข้ามา และค่า ParamPassword เป็นค่ารหัสผ่านที่ได้รับเข้ามา ฟังก์ชันจะดำเนินการนำค่า ParamNonce มารวมต่อกันกับค่า ParamCreated และมารวมต่อกันกับค่า ParamPassword เมื่อนำค่านำทั้งหมดมารวมต่อกันแล้วก็จะนำค่าที่ได้เข้ารหัสแบบ SHA1 และดำเนินการเข้ารหัสแบบ Base64 อีกครั้งและนำค่าที่ได้ส่งค่ากลับไปยังโพรซีเดอร์ที่เรียกใช้ฟังก์ชันนี้

บทที่ 4
ระเบียบวิธีการวิจัย

ผู้วิจัยได้ดำเนินการตรวจสอบวัดประสิทธิภาพการทำงานของเว็บเซอร์วิส โดยดำเนินการพัฒนาโปรแกรมเว็บเซอร์วิสซึ่งประกอบด้วย โปรแกรมเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล โปรแกรมเว็บเซอร์วิสของผู้ให้บริการข้อมูล โปรแกรมเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และจำลองสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และ เว็บเซอร์วิสของผู้ให้บริการข้อมูล ผู้วิจัยได้แบ่งรูปแบบสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสออกเป็นสองรูปแบบดังนี้ รูปแบบที่หนึ่ง การติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.2 และ รูปแบบที่สอง การติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการเรียกใช้โพรซีเดอร์ในการจัดการหลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.3

4.1 วิธีการทดลองและการประเมินผล

ในการทดลองนั้น ผู้วิจัยได้ดำเนินการใช้เครื่องมือในสร้างเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และ เว็บเซอร์วิสของผู้ให้บริการข้อมูล ดังนี้คือ ใช้โปรแกรม Visual Studio 2005 โดยใช้ภาษา C# ในการพัฒนาเว็บเซอร์วิสดังกล่าว ใช้ฐานข้อมูล Microsoft SQL Server 2005 ในการจัดเก็บค่าที่ใช้ในการพิสูจน์ตัวตน ใช้โปรแกรม WAPT 3.0 ในการจำลองสถานการณ์ทำรายการทดสอบ และมีการสร้างสภาพแวดล้อมด้วยเครื่องคอมพิวเตอร์ CPU : Intel Dual Core 1.8 GHz, RAM 2 GB, OS : Windows XP และ Network Speed : 512 kbps ผู้วิจัยได้จำลองสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และ เว็บเซอร์วิสของผู้ให้บริการข้อมูลเป็นสองรูปแบบดังนี้คือ

รูปแบบที่หนึ่ง WS Storing All Nonce เป็นการติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.2

รูปแบบที่สอง WS Not Storing All Nonce เป็นการติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการเรียกใช้โพรซีเดอร์ในการจัดการหลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.3

สามารถอธิบายวิธีการทดสอบในสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสแต่ละรูปแบบได้ดังนี้

1.การจำลองสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสตามรูปแบบที่หนึ่ง WS Storing All Nonce ประกอบไปด้วยเว็บเซอร์วิสดังต่อไปนี้

1.1.เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล

URL :

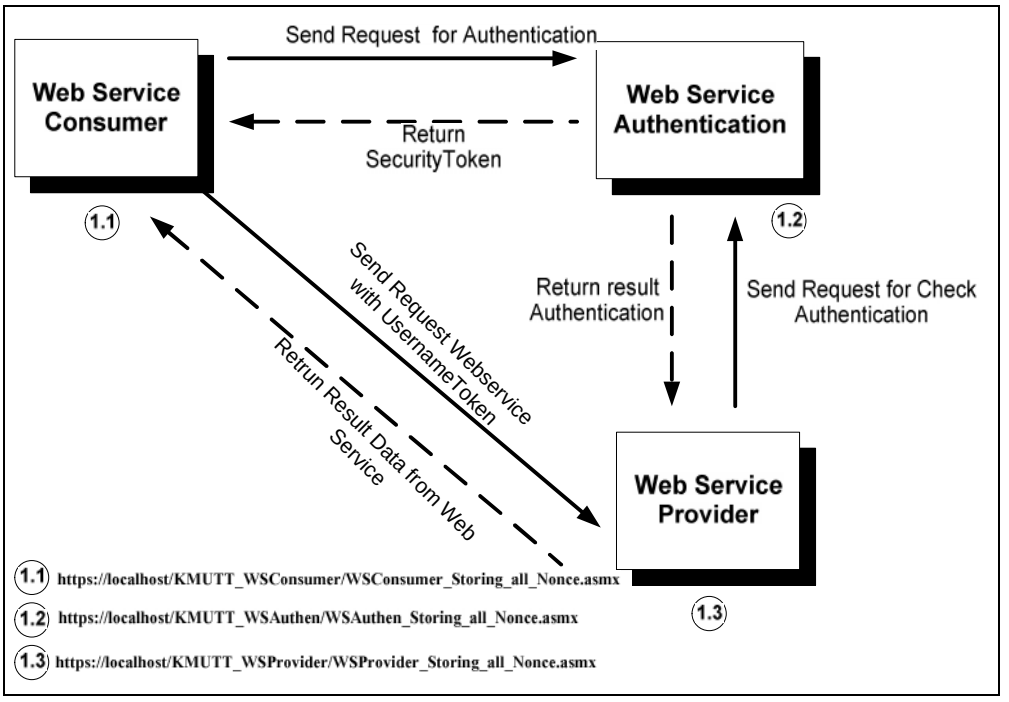
https://localhost/KMUTT_WSConsumer/WSConsumer_Storing_all_Nonce.asmx

1.2.เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน

URL : https://localhost/KMUTT_WSAuthen/WSAuthen_Storing_all_Nonce.asmx

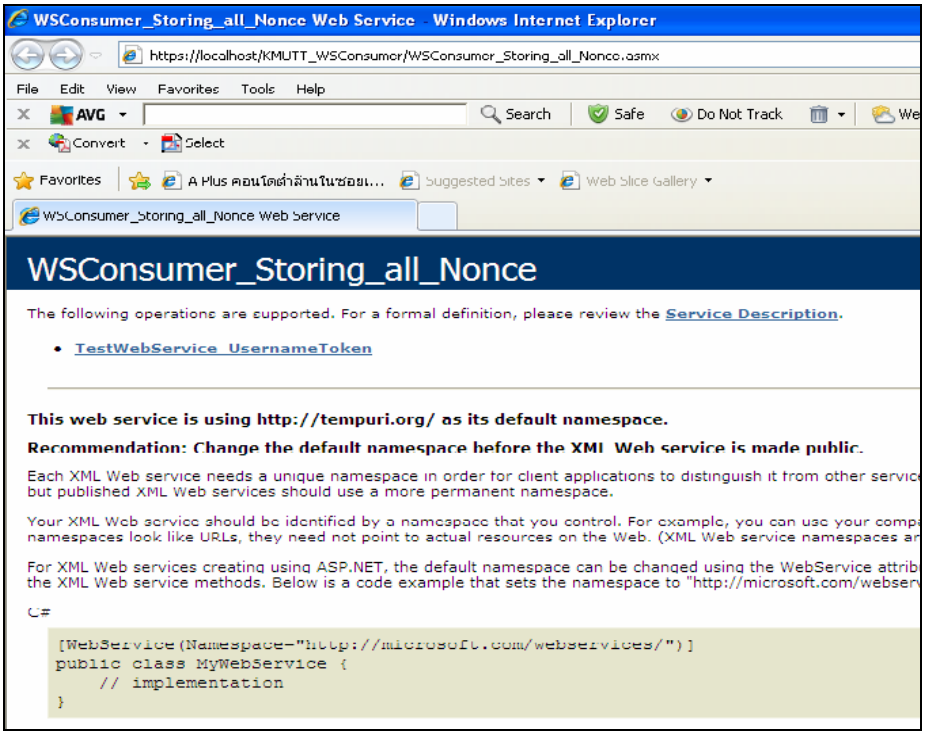
1.3.เว็บเซอร์วิสของผู้ให้บริการข้อมูล

URL : https://localhost/KMUTT_WSProvider/WSProvider_Storing_all_Nonce.asmx



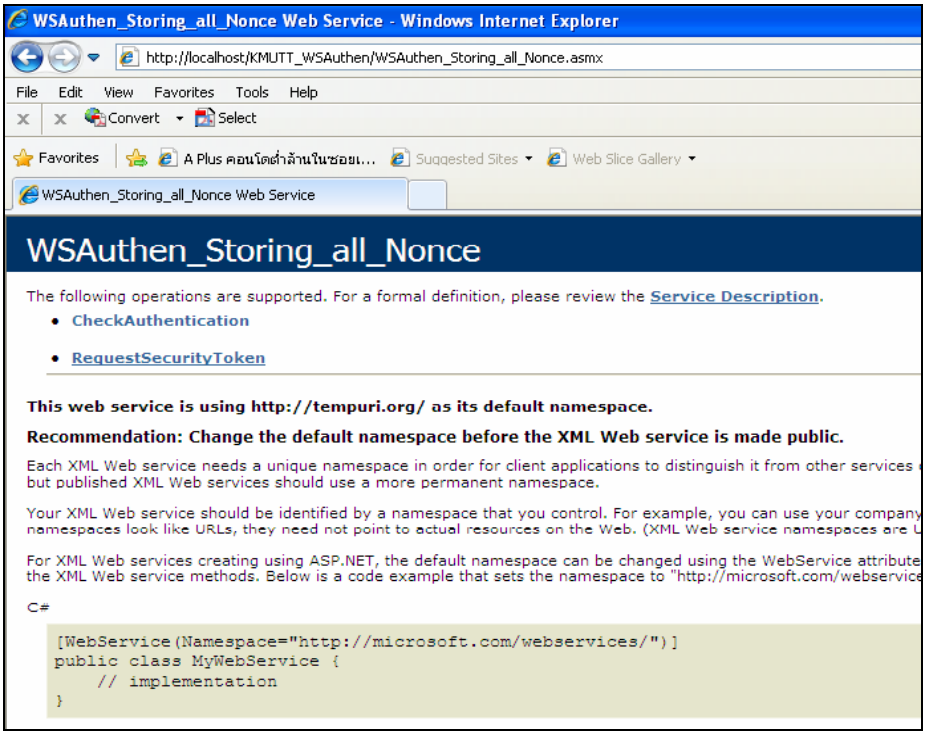
รูปที่ 4.1 รายละเอียดการจำลองสถานการณ์การติดต่อสื่อสารเว็บเซอร์วิสตามรูปแบบที่หนึ่ง

ในรูปที่ 4.1 แสดงรายละเอียดของการจำลองสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และ เว็บเซอร์วิสของผู้ให้บริการข้อมูลตามรูปแบบที่หนึ่ง การติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.2



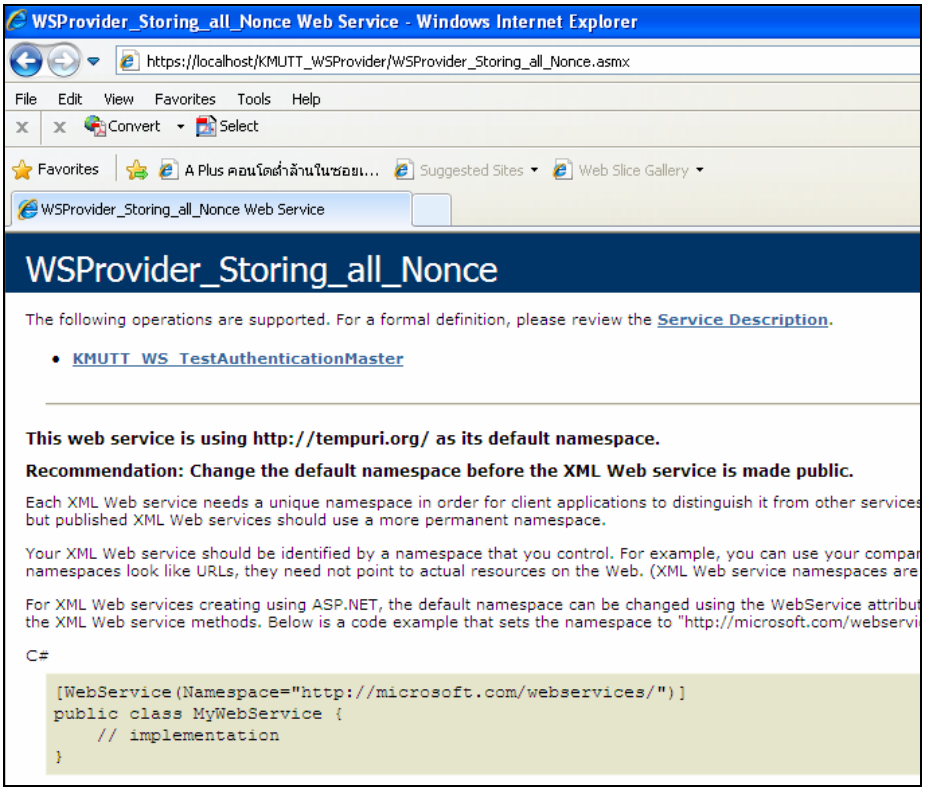
รูปที่ 4.2 เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลในการติดต่อสื่อสารตามรูปแบบที่หนึ่ง

ในรูปที่ 4.2 แสดงเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล โดยมีฟังก์ชันที่ชื่อว่า TestService_UsernameToken ภายในการทำงานของฟังก์ชันนี้ก็จะไปเรียกเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนเพื่อขอ SecurityToken และการทำงานของฟังก์ชันนี้ยังมีการส่งคำร้องขอที่มียูสเซอร์เนมโทเคนไปเรียกเว็บเซอร์วิสของผู้ให้บริการเพื่อขอข้อมูล



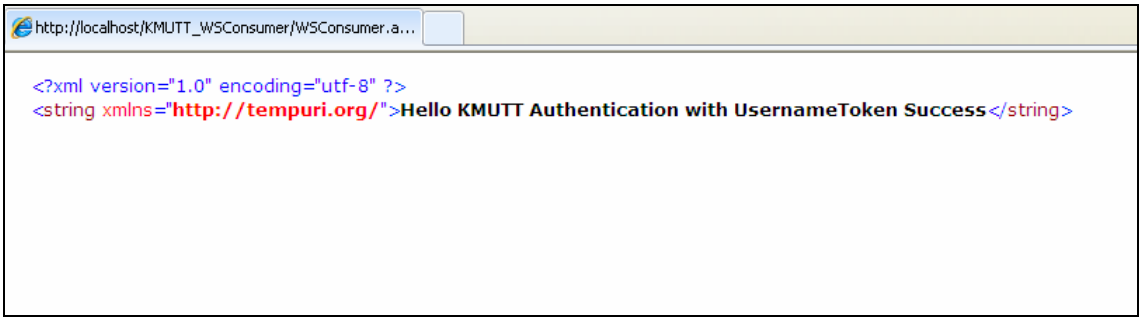
รูปที่ 4.3 เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนในการติดต่อสื่อสารตามรูปแบบที่หนึ่ง

ในรูปที่ 4.3 แสดงเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน โดยมีฟังก์ชันที่ชื่อว่า RequestSecurityToken ภายในการทำงานของฟังก์ชันนี้มีรองรับการร้องขอ SecurityToken จากทางเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลเป็นฟังก์ชันสร้าง SecurityToken ส่งเป็นข้อมูลกลับไปยังเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล และยังมีฟังก์ชันที่ชื่อว่า CheckAuthentication ฟังก์ชันนี้เป็นฟังก์ชันรองรับการร้องขอตรวจสอบสิทธิ์การเข้าถึงข้อมูลจากเว็บเซอร์วิสผู้ให้บริการ โดยมีกระบวนการตรวจสอบพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน เว็บเซอร์วิสผู้ให้บริการข้อมูลจะเรียกใช้ฟังก์ชันนี้ในการตรวจสอบค่าของยูสเซอร์เนมโทเคนที่ได้รับมาจากเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลว่าเป็นผู้มีสิทธิ์ในการเข้าถึงข้อมูลหรือไม่ จะมีกระบวนการตรวจสอบและจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.2



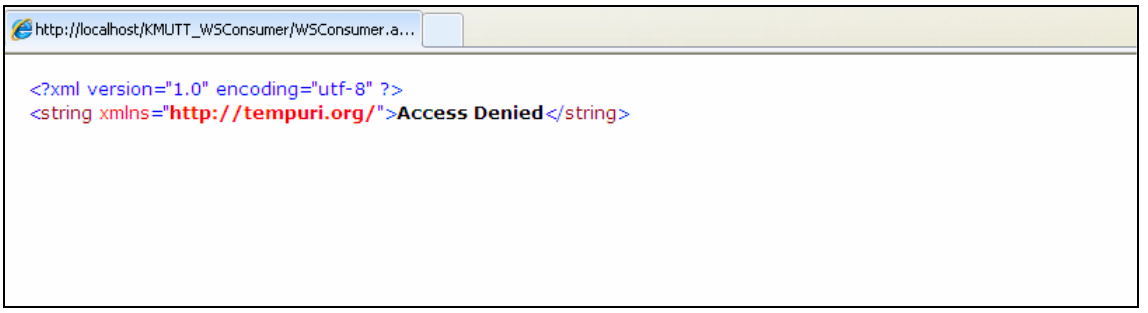
รูปที่ 4.4 เว็บเซอร์วิสของผู้ให้บริการข้อมูลในการติดต่อสื่อสารตามรูปแบบที่หนึ่ง

ในรูปที่ 4.4 แสดงเว็บเซอร์วิสของผู้ให้บริการข้อมูล โดยมีฟังก์ชันที่ชื่อว่า KMUTT_WS_TestAuthentication การทำงานของฟังก์ชันนี้จะมีหน้าที่รับการร้องขอจากเว็บเซอร์วิสของผู้ขอใช้ข้อมูลที่มีการส่งยูสเซอร์เนมโทเคนและ SecurityToken มาด้วยโดยฟังก์ชันนี้จะมีการส่งค่าทั้งสองไปยังเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนเพื่อขอทำการตรวจสอบว่ามีสิทธิ์ในการเข้าถึงข้อมูลหรือไม่ ถ้ามีสิทธิ์ก็ส่งส่งค่าข้อมูลที่สามารถเข้าถึงได้กลับไปยังเว็บเซอร์วิสของผู้ขอใช้ข้อมูล ถ้าไม่มีสิทธิ์ก็จะส่งค่าแจ้งกลับไปว่าไม่สามารถเข้าถึงข้อมูลที่ต้องการได้



รูปที่ 4.5 ผลลัพธ์ของเว็บเซอร์วิสเมื่อมีสิทธิ์เข้าถึงข้อมูลในการติดต่อสื่อสารตามรูปแบบที่หนึ่ง

ในรูปที่ 4.5 เป็นค่าที่เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลได้รับจากทางเว็บเซอร์วิสของผู้ให้บริการข้อมูล เมื่อมีการตรวจสอบแล้วว่าเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลเป็นผู้สามารถเข้าถึงข้อมูลได้



รูปที่ 4.6 ผลลัพธ์ของเว็บเซอร์วิสเมื่อไม่มีสิทธิ์เข้าถึงข้อมูลในการติดต่อสื่อสารตามรูปแบบที่หนึ่ง

ในรูปที่ 4.6 เป็นค่าที่เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลได้รับจากทางเว็บเซอร์วิสของผู้ให้บริการข้อมูล เมื่อมีการตรวจสอบแล้วว่าเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลเป็นผู้ไม่มีสิทธิ์เข้าถึงข้อมูลได้

2.การจำลองสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสตามรูปแบบที่สอง WS Not Storing All Nonce ประกอบไปด้วยเว็บเซอร์วิสดังต่อไปนี้

2.1.เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล

URL :

https://localhost/KMUTT_WSConsumer/WSConsumer_not_Storing_all_Nonce.asmx

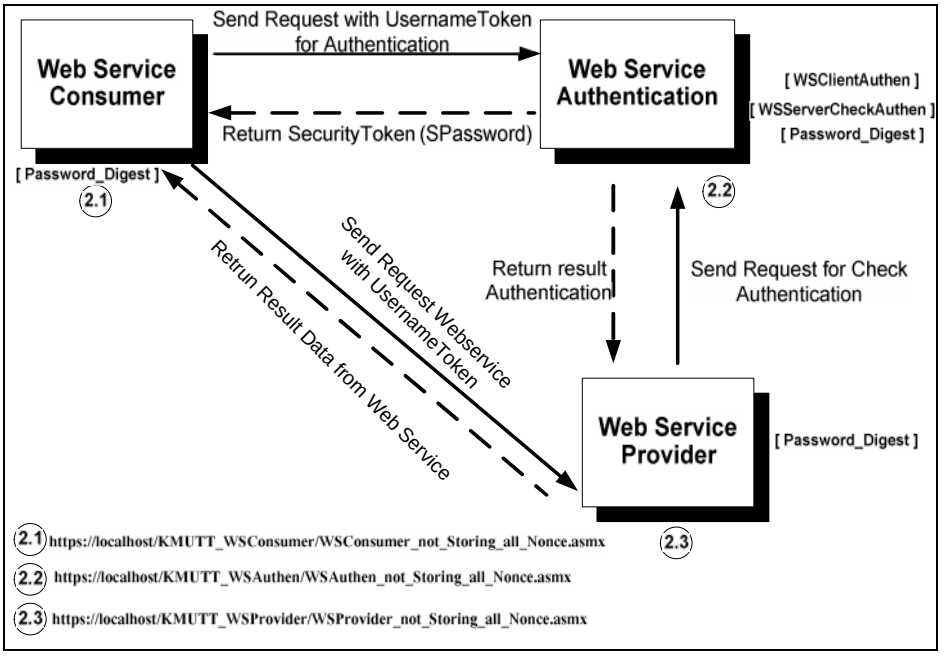
2.2.เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน

URL : https://localhost/KMUTT_WSAuthen/WSAuthen_not_Storing_all_Nonce.asmx

2.3.เว็บเซอร์วิสของผู้ให้บริการข้อมูล

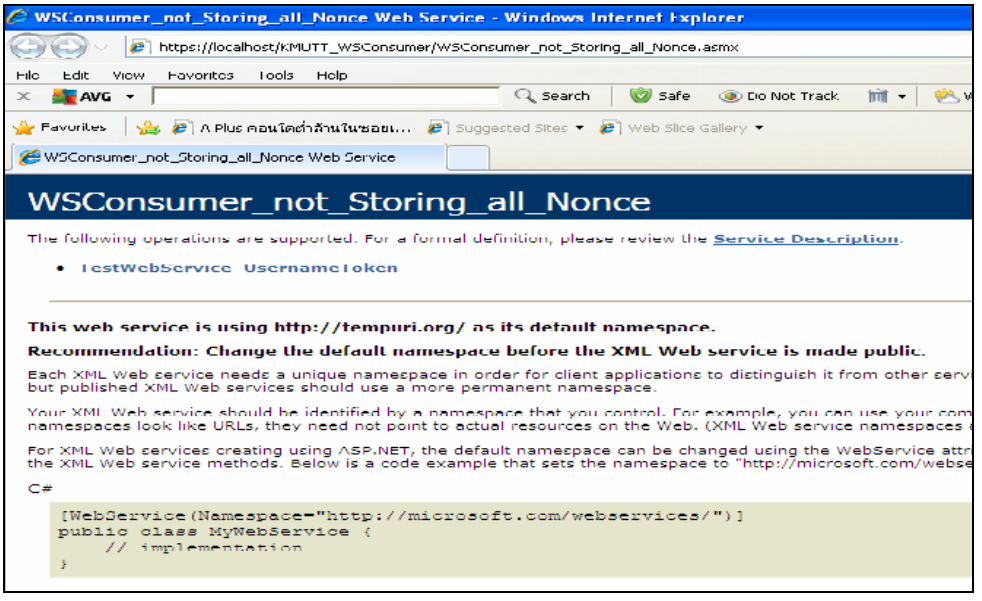
URL :

https://localhost/KMUTT_WSProvider/WSProvider_not_Storing_all_Nonce.asmx



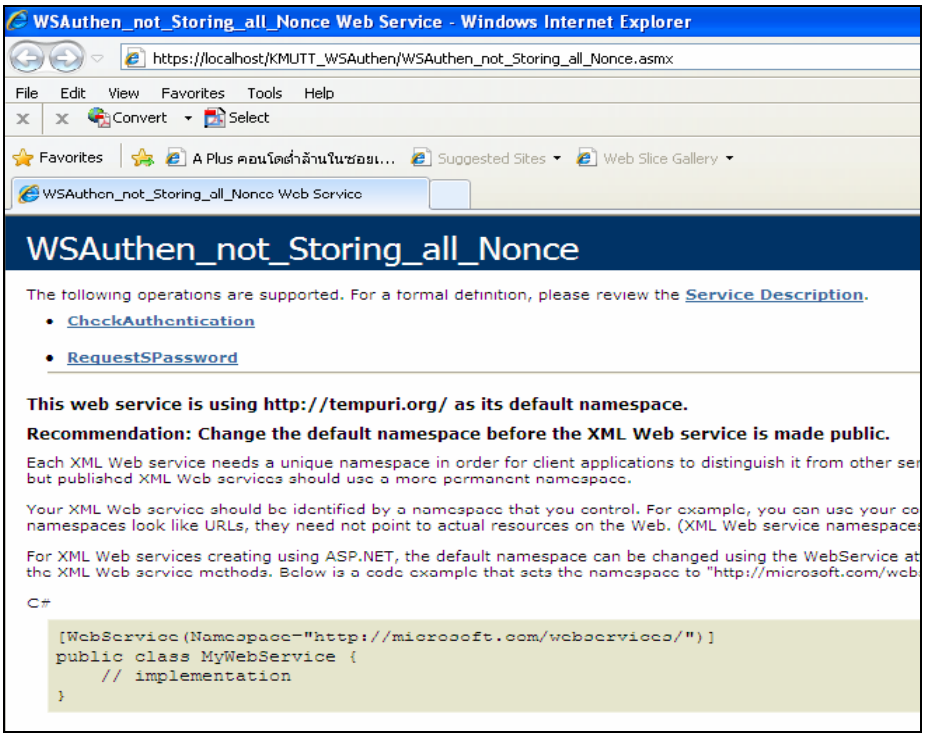
รูปที่ 4.7 รายละเอียดการจำลองสถานการณ์การติดต่อสื่อสารเว็บเซอร์วิสตามรูปแบบที่สอง

ในรูปที่ 4.7 แสดงรายละเอียดของการจำลองสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และ เว็บเซอร์วิสของผู้ให้บริการข้อมูลตามรูปแบบที่สอง การติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการเรียกใช้โพรซีเดอร์ในการจัดการหลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.3



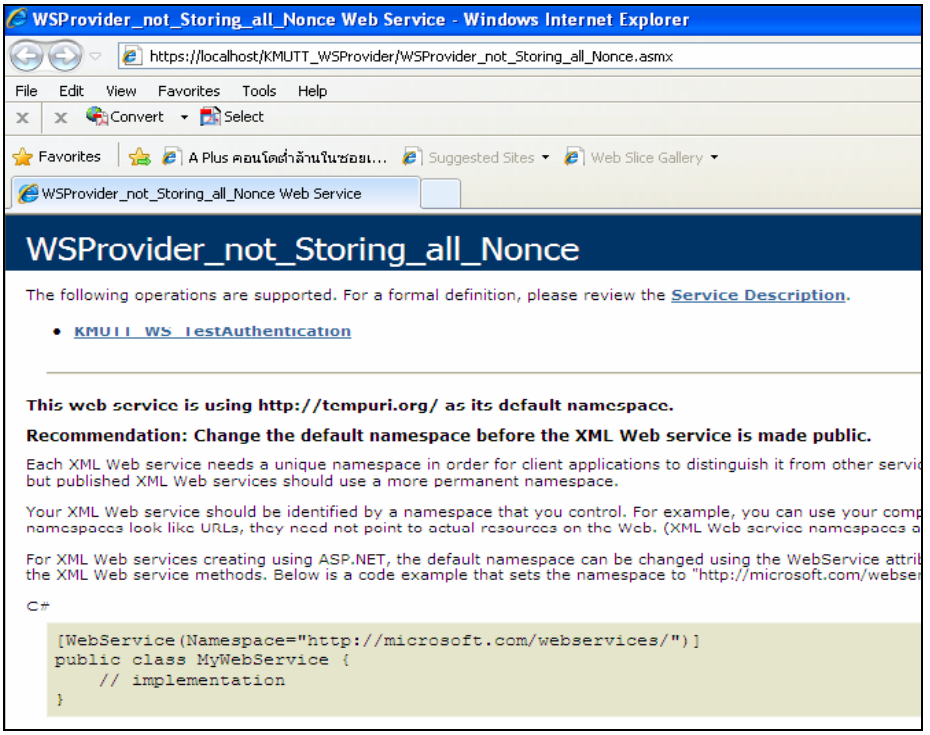
รูปที่ 4.8 เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลในการติดต่อสื่อสารตามรูปแบบที่สอง

ในรูปที่ 4.8 แสดงเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล โดยมีฟังก์ชันที่ชื่อว่า TestService_UsernameToken ภายในการทำงานของฟังก์ชันนี้ก็จะไปเรียกเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนโดยส่งคำร้องขอที่มียูสเซอร์เนมโทเคนส่งไปเพื่อขอ SPassword ซึ่งเป็น SecurityToken และการทำงานของฟังก์ชันนี้ยังมีส่งคำร้องขอที่มียูสเซอร์เนมโทเคนเรียกเว็บเซอร์วิสของผู้ให้บริการเพื่อขอข้อมูล



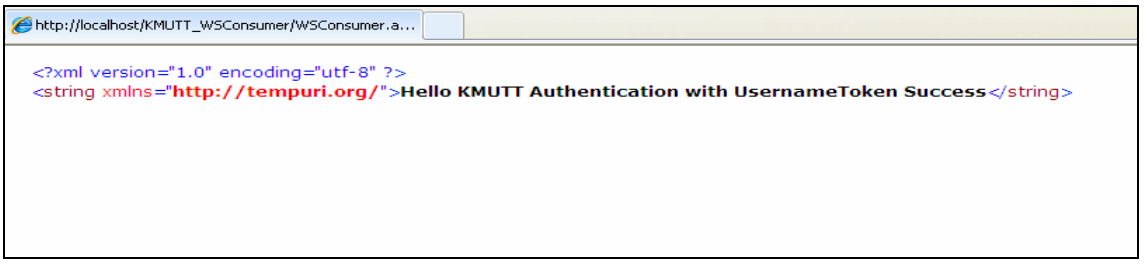
รูปที่ 4.9 เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนในการติดต่อสื่อสารตามรูปแบบที่สอง

ในรูปที่ 4.9 แสดงเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน โดยมีฟังก์ชันที่ชื่อว่า RequestSPassword ภายในการทำงานของฟังก์ชันนี้มีรองรับการร้องขอ SPassword ซึ่งเป็น SecurityToken จากทางเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลเป็นฟังก์ชันสร้าง SPassword ส่งเป็นข้อมูลกลับไปยังเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล และยังมีฟังก์ชันที่ชื่อว่า CheckAuthentication ฟังก์ชันนี้เป็นฟังก์ชันรองรับการร้องขอตรวจสอบยูสเซอร์เนมในการเข้าถึงข้อมูลจากเว็บเซอร์วิสผู้ให้บริการ โดยมีกระบวนการตรวจสอบพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคน เว็บเซอร์วิสผู้ให้บริการข้อมูลจะเรียกใช้ฟังก์ชันนี้ในการตรวจสอบค่าของยูสเซอร์เนมโทเคนที่ได้รับมาจากเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลว่าเป็นผู้มีสิทธิ์ในการเข้าถึงข้อมูลหรือไม่ มีกระบวนการเรียกใช้โพรซีเดอร์ในการจัดการ หลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.3



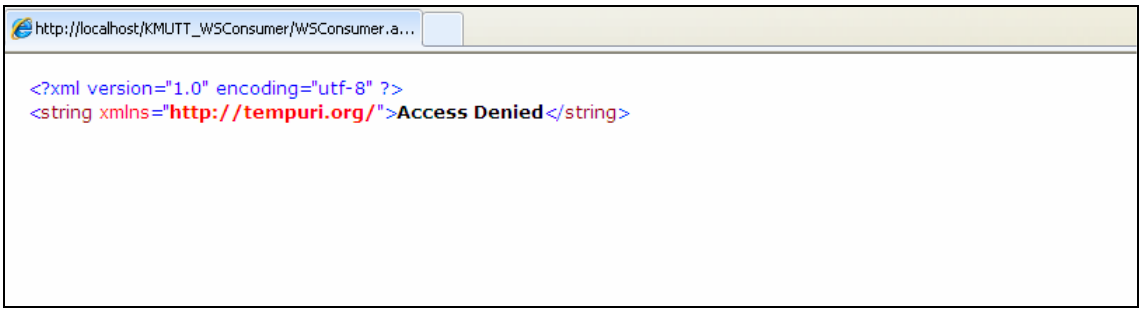
รูปที่ 4.10 เว็บเซอร์วิสของผู้ให้บริการข้อมูลในการติดต่อสื่อสารตามรูปแบบที่สอง

ในรูปที่ 4.10 แสดงเว็บเซอร์วิสของผู้ให้บริการข้อมูล โดยมีฟังก์ชันที่ชื่อว่า KMUTT_WS_TestAuthentication การทำงานของฟังก์ชันนี้จะมีหน้าที่รับการร้องขอจากเว็บเซอร์วิสของผู้ขอใช้ข้อมูลที่มีการส่งยูสเซอร์เนมโทเคนและ SPassword มาด้วยโดยฟังก์ชันนี้จะมีการส่งค่าทั้งสองไปยังเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนเพื่อขอทำการตรวจสอบว่ามีสิทธิ์ในการเข้าถึงข้อมูลหรือไม่ ถ้ามีสิทธิ์ก็ส่งส่งค่าข้อมูลที่สามารถเข้าถึงได้กลับไปยังเว็บเซอร์วิสของผู้ขอใช้ข้อมูล ถ้าไม่มีสิทธิ์ก็จะส่งค่าแจ้งกลับไปว่าไม่สามารถเข้าถึงข้อมูลที่ต้องการได้



รูปที่ 4.11 ผลลัพธ์ที่เว็บเซอร์วิสเมื่อมีสิทธิ์เข้าถึงข้อมูลในการติดต่อสื่อสารตามรูปแบบที่สอง

ในรูปที่ 4.11 เป็นค่าที่เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลได้รับจากทางเว็บเซอร์วิสของผู้ให้บริการข้อมูล เมื่อมีการตรวจสอบแล้วว่าเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลเป็นผู้สามารถเข้าถึงข้อมูลได้



รูปที่ 4.12 ผลลัพธ์ที่เว็บเซอร์วิสเมื่อไม่มีสิทธิ์เข้าถึงข้อมูลในการติดต่อสื่อสารตามรูปแบบที่สอง

ในรูปที่ 4.12 เป็นค่าที่เว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลได้รับจากทางเว็บเซอร์วิสของผู้ให้บริการข้อมูล เมื่อมีการตรวจสอบแล้วว่าเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูลเป็นผู้ไม่มีสิทธิ์เข้าถึงข้อมูลได้ ในการประเมินผลนั้นผู้วิจัยได้ทำการวัดค่าและเปรียบเทียบค่าเวลาที่ใช้ประมวลผลการทำรายการของการเรียกใช้บริการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสของผู้ขอใช้บริการข้อมูล เว็บเซอร์วิสเพื่อพิสูจน์ตัวตน และ เว็บเซอร์วิสของผู้ให้บริการข้อมูลทั้งสองรูปแบบที่ได้กล่าวข้างต้น โดยใช้โปรแกรม WAPT 3.0 ทำการจำลองการทำรายการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสทั้งสองรูปแบบ วัดค่าและเปรียบเทียบค่าเวลาที่ใช้ในการทำรายการตามจำนวนการทำรายการและเวลาที่กำหนด

4.2 การวัดประสิทธิภาพค่าเวลาการทำรายการ WS Storing All Nonce

การวัดค่าประสิทธิภาพการทำงานของเว็เซอร์วิสนั้นเป็นการวัดในด้านเวลาที่ใช้ในการทำรายการ โดยการทดลองมีการควบคุมจำนวนการทำรายการ ช่วงเวลาการทำรายการ และจำนวนการทำรายการพร้อมกัน ดำเนินการวัดเวลาที่ใช้ในการทำรายการของเว็บเซอร์วิสทั้งสองแบบ รูปแบบที่หนึ่ง WS Storing All Nonce เป็นการวัดค่าเวลาในการทำรายการของสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูล ในการทำการทดลองจำลองการทำรายการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสตามรูปแบบที่หนึ่ง WS Storing All Nonce นั้น มีการแบ่งลักษณะในการทดลองวัดค่าเวลาที่ใช้ในการทำรายการดังนี้

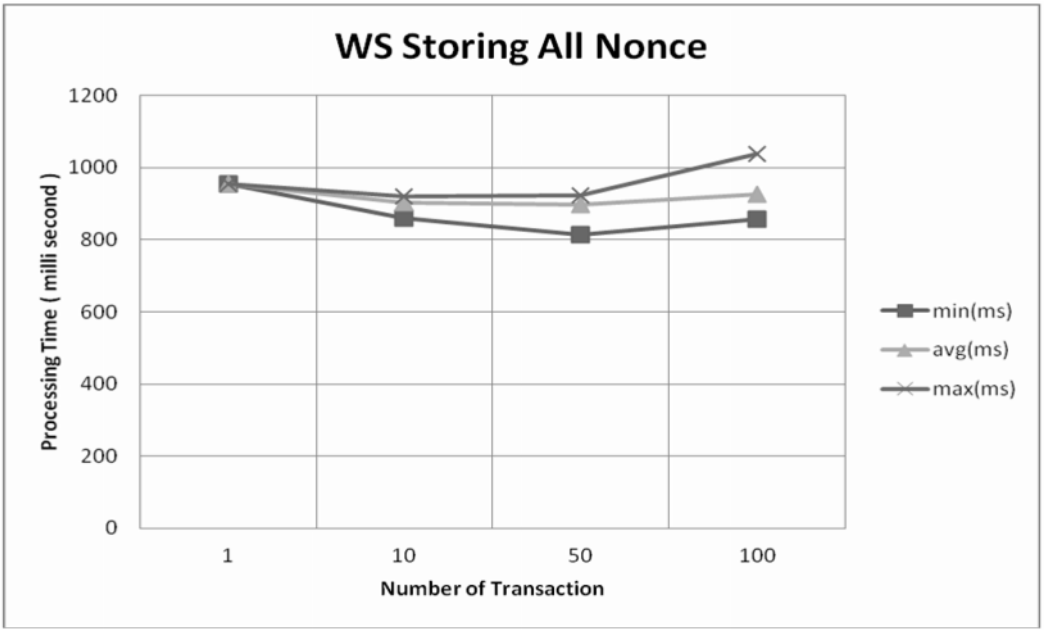
กรณีทดลองที่ 1 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่งโดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1 คน ทำรายการขอใช้บริการเว็บ

เซอร์วิสจำนวน 1, 10, 50,100 รายการ มีการดำเนินการลบค่า Nonce เมื่อถึงเวลาครบกำหนด ซึ่งกำหนดไว้ที่ทุกๆ 5 นาทีแล้ววัดค่าเวลาการทำรายการ ดังตารางที่ 1

ตารางที่ 4.1 ค่าเวลาการทำรายการ WS Storing All Nonce กรณีทดลองที่ 1

Transaction	**WS Storing All Nonce**		
No.Transaction	**min(ms)**	**avg(ms)**	**max(ms)**
1	956.07	956.07	956.07
10	858.79	901.79	920.64
50	813.06	898.37	923.60
100	856.45	926.47	1037.46

จากตารางที่ 4.1 เป็นค่าเวลาน้อยที่สุด ค่าเวลาเฉลี่ย และค่าเวลามากที่สุดที่ใช้ในการทำรายการ โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1 คน ทำรายการขอใช้บริการเว็บเซอร์วิสจำนวน 1, 10, 50,100 รายการ มีการดำเนินการลบค่า Nonce เมื่อถึงเวลาครบกำหนด ซึ่งกำหนดไว้ที่ทุกๆ 5 นาที ค่าที่ได้ปรากฏดังในตารางข้างต้นซึ่งเป็นการวัดค่าเวลาที่ใช้ในการทำรายการตั้งแต่ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอเพื่อขอเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิสจนถึงได้รับข้อมูลตอบกลับจากผู้ให้บริการเว็บเซอร์วิส ซึ่งมีกระบวนการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสในรูปแบบที่หนึ่ง WS Storing All Nonce สามารถนำค่าที่วัดได้ดังแสดงในตาราง 4.1 นำมาสร้างเป็นกราฟได้ดังรูปที่ 4.13



รูปที่ 4.13 กราฟแสดงค่าเวลาการทำรายการ WS Storing All Nonce กรณีทดลองที่ 1

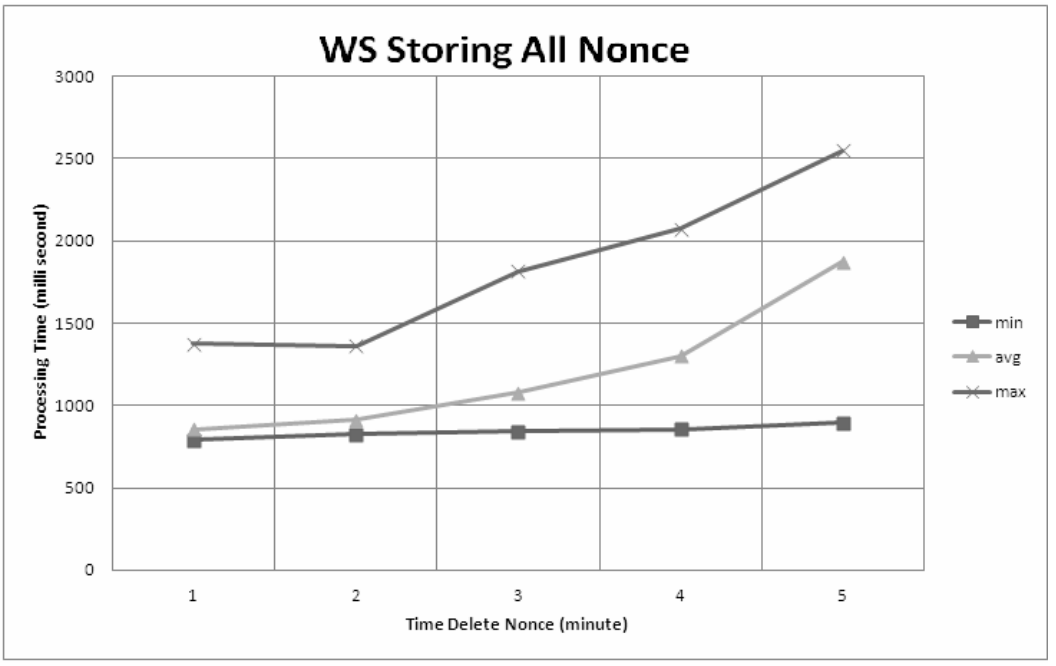
ในรูปที่ 4.13 แสดงกราฟผลลัพธ์จากการวัดค่าเวลาที่ใช้ในการร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1, 10, 50,100 ราย ซึ่งมีกระบวนการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสในรูปแบบที่หนึ่ง WS Storing All Nonce

กรณีทดลองที่ 2 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาที มีการดำเนินการลบค่า Nonce เมื่อถึงเวลาครบกำหนด ซึ่งกำหนดไว้ที่ทุกๆ 1, 2, 3, 4, 5 นาทีแล้ววัดค่าเวลาที่ใช้ทำรายการ

ตารางที่ 4.2 ค่าเวลาทำรายการ WS Storing All Nonce กรณีทดลองที่ 2

Delete nonce Time (minute)	**min (ms)**	**avg (ms)**	**max (ms)**
1	788.70	857.49	1374.80
2	823.93	910.91	1362.90
3	841.58	1079.33	1815.90
4	857.07	1303.13	2074.94
5	894.10	1874.16	2548.78

จากตารางที่ 4.2 เป็นค่าเวลาน้อยที่สุด ค่าเวลาเฉลี่ย และค่าเวลามากที่สุดที่ใช้ในการทำรายการ โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาทีมีการดำเนินการทำการทดลองลบค่า Nonce เมื่อถึงเวลาครบกำหนด ซึ่งแบ่งชุดการทดลองออกเป็นดังนี้ ชุดที่ 1 ลบค่า Nonce ทุก 1 นาที, ชุดที่ 2 ลบค่า Nonce ทุก 2 นาที, ชุดที่ 3 ลบค่า Nonce ทุก 3 นาที, ชุดที่ 4 ลบค่า Nonce ทุก 4 นาที, ชุดที่ 5 ลบค่า Nonce ทุก 5 นาทีซึ่งได้จำนวนการทำรายการในการทำการทดลองลบค่า Nonce ตามเวลาดังกล่าวในแต่ละชุดทำรายการได้ 3,185 รายการต่อชุดการทดลอง แล้ววัดค่าเวลาที่ใช้ในการทำรายการทุกรายการแล้วนำมาหาค่าเวลาน้อยที่สุด ค่าเวลาเฉลี่ย และค่าเวลามากที่สุดที่ใช้ในการทำรายการดังแสดงในตาราง 4.2 ซึ่งมีกระบวนการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสในรูปแบบที่หนึ่ง WS Storing All Nonce สามารถนำค่าที่วัดได้ดังแสดงในตาราง 4.2 นำมาสร้างเป็นกราฟได้ดังรูปที่ 4.14



รูปที่ 4.14 กราฟแสดงค่าเวลาทำรายการ WS Storing All Nonce กรณีทดลองที่ 2

ในรูปที่ 4.14 แสดงกราฟผลลัพธ์จากการวัดค่าเวลาที่ใช้ในการทำรายการ โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาทีมีการดำเนินการลบค่า Nonce เมื่อถึงเวลาครบกำหนด ซึ่งกำหนดไว้ที่ทุกๆ 1, 2, 3, 4, 5 นาที ซึ่งมีกระบวนการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสในรูปแบบที่หนึ่ง WS Storing All Nonce จากกราฟจะพบว่าค่าเวลาการทำรายการจะสูงขึ้นตามเวลาที่กำหนดให้ลบค่า Nonce ใน

ฐานข้อมูล เมื่อมีการกำหนดเวลาที่ทำการลบค่า Nonce มากขึ้นจะพบว่าเวลาที่ใช้ในการทำรายการก็จะมากขึ้นด้วย

4.3 การวัดประสิทธิภาพค่าเวลาการทำรายการ WS Not Storing All Nonce

การวัดประสิทธิภาพค่าเวลาการทำรายการรูปแบบที่สอง WS Not Storing All Nonce เป็นการวัดค่าเวลาในการทำรายการของสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการเรียกใช้โพรซีเดอร์ในการจัดการหลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูล ในการทำการทดลองจำลองการทำรายการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บเซอร์วิสตามรูปแบบที่สองนั้น มีการแบ่งลักษณะในการทดลองวัดค่าเวลาที่ใช้ในการทำรายการดังนี้

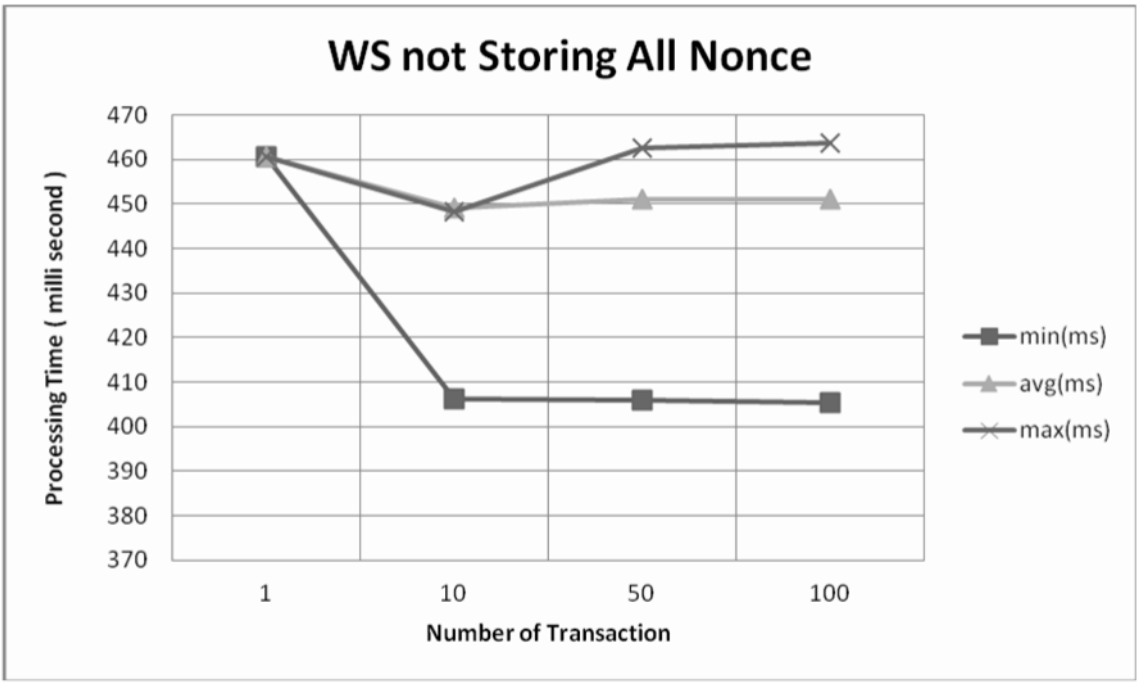
กรณีทดลองที่ 1 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่สอง WS Not Storing All Nonce โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1 คน ทำรายการขอใช้บริการเว็บเซอร์วิสจำนวน 1, 10, 50,100 รายการ แล้ววัดค่าเวลาการทำรายการ ดังตารางที่ 4.3

ตารางที่ 4.3 ค่าเวลาการทำรายการ WS Not Storing All Nonce กรณีทดลองที่ 1

	WS Not Storing All Nonce		
No.Transaction	**min(ms)**	**avg(ms)**	**max(ms)**
1	460.53	460.53	460.53
10	406.18	449.29	448.41
50	405.91	451.21	462.59
100	405.29	451.21	463.84

จากตารางที่ 4.3 เป็นค่าเวลาน้อยที่สุด ค่าเวลาเฉลี่ย และค่าเวลามากที่สุดที่ใช้ในการทำรายการ โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1 คน ทำรายการขอใช้บริการเว็บเซอร์วิสจำนวน 1, 10, 50,100 รายการ ค่าที่ได้ปรากฏดังในตารางข้างต้นซึ่งเป็นการวัดค่าเวลาที่ใช้ในการทำรายการตั้งแต่ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอเพื่อขอเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิสจนถึงได้รับข้อมูลตอบกลับจากผู้ให้บริการเว็บเซอร์วิส ซึ่งมีกระบวนการตามสถานการณ์การติดต่อสื่อสารระหว่างเว็บ

เซอร์วิสในรูปแบบที่สอง WS Not Storing All Nonce สามารถนำค่าที่วัดได้ดังแสดงในตาราง 4.3 นำมาสร้างเป็นกราฟได้ดังรูปที่ 4.15



รูปที่ 4.15 กราฟแสดงค่าเวลาการทำรายการ WS Not Storing All Nonce กรณีทดลองที่ 1

กรณีทดลองที่ 2 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่สอง WS Not Storing All Nonce โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาที แล้ววัดค่าเวลาที่ใช้ในการทำรายการ

ตารางที่ 4.4 ค่าเวลาการทำรายการ WS Not Storing All Nonce กรณีทดลองที่ 2

	Processing Time (Milisec)		
WS Not Storing All Nonce	**min(ms)**	**avg(ms)**	**max(ms)**
5 User 20 Min 3,185 Transaction	399.49	507.50	1391.45

จากตารางที่ 4.4 เป็นค่าเวลาน้อยที่สุด ค่าเวลาเฉลี่ย และค่าเวลามากที่สุดที่ใช้ในการทำรายการ โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาที ซึ่งจำนวนรายการที่ได้คือ 3,185 รายการ แล้ววัดค่าเวลาที่ใช้ในการทำรายการทุกรายการแล้วนำมาหาค่าเวลาน้อยที่สุด ค่าเวลาเฉลี่ย และค่าเวลามากที่สุดที่ใช้ในการทำรายการดังแสดง

ในตาราง ซึ่งในการทดลองวัดค่าการทำรายการนี้ไม่ต้องมีการกำหนดค่าเวลาที่ใช้ในการลบค่า Nonce ออกจากฐานข้อมูลเพราะกระบวนการตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่สอง WS Not Storing All Nonce จะเป็นการหลีกเลี่ยงการจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูลจึงไม่มีกระบวนการลบค่า Nonce ตามเวลาที่กำหนด

4.4 การเปรียบเทียบค่าเวลาการทำรายการ

จากการทดลองจำลองการติดต่อสื่อสารการขอใช้บริการข้อมูลสามารถนำขั้นตอนกระบวนที่เว็บเซอร์วิสสองรูปแบบใช้ในการพิสูจน์ตัวตนในกรณีสามารถผู้ขอใช้บริการเว็บเซอร์วิสสามารถเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิสได้ นำวิธีการมาเปรียบเทียบขั้นตอนการทำงานในรูปแบบตารางได้ดังนี้

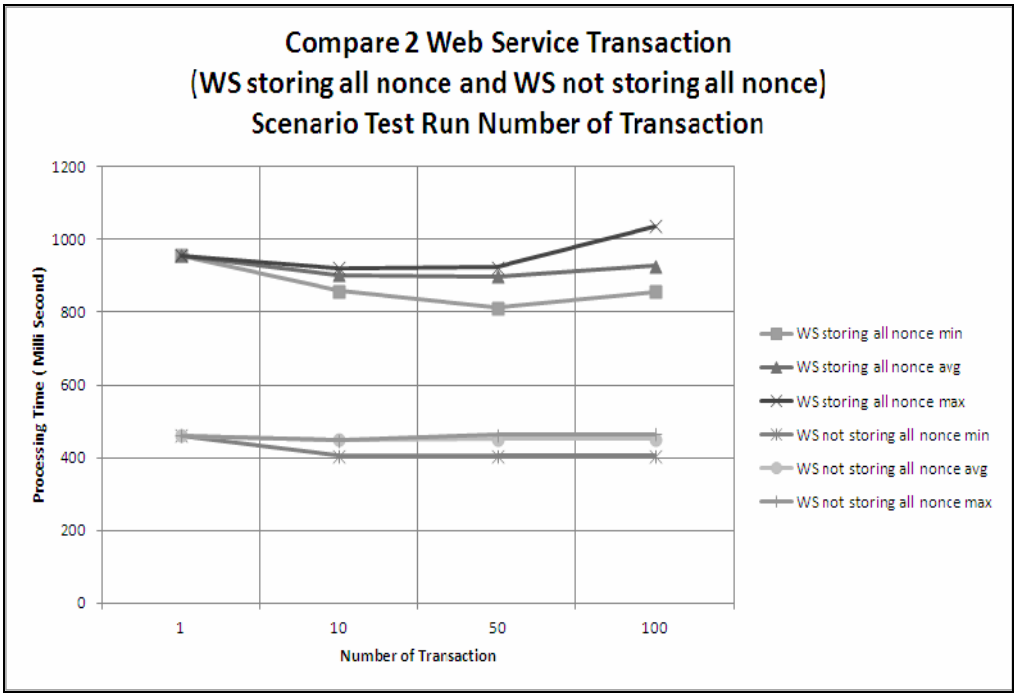
ตารางที่ 4.5 เปรียบเทียบกระบวนการพิสูจน์ตัวตนเพื่อขอเข้าถึงข้อมูล

เปรียบเทียบกระบวนการพิสูจน์ตัวตนเพื่อขอเข้าถึงข้อมูล	
WS Storing all Nonce	**WS not Storing all Nonce**
ขั้นตอนที่ 1 ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอไปร้องขอ Security Token จากเว็บเซอร์วิสเพื่อพิสูจน์ตัวตน	
1.1 เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนตรวจสอบค่า Username, Password ว่ามีค่าตรงกับข้อมูลในฐานข้อมูลหรือไม่ ดึงค่า Username, Password ในฐานข้อมูลเพื่อนำมาตรวจสอบ	1.1 เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนตรวจสอบค่า UsernameToken ว่ามีค่าข้อมูล ที่ได้รับมาว่าตรงกับข้อมูลในฐานข้อมูลหรือไม่ ดึงค่า CUsername, CPassword
1.2 เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนสร้าง Security Token และบันทึกค่า Security Token และ ค่า Security Token Expired Timeในฐานข้อมูล	1.2 เว็บเซอร์วิสเพื่อพิสูจน์ตัวตนอัพเดทบันทึกค่าข้อมูล CNonce, SNonce, CCreated และ SCreated ในฐานข้อมูล
ขั้นตอนที่ 2 ผู้ขอใช้บริการเว็บเซอร์วิสส่ง Soap Msg ที่มี UsenameToken และ Security Token ไปตรวจสอบสิทธิ์เข้าถึงข้อมูลจากผู้ให้บริการเว็บเซอร์วิส	
2.1 ผู้ให้บริการเว็บเซอร์วิสตรวจสอบค่า Nonce ว่ามีค่าซ้ำในฐานข้อมูลหรือไม่ ดึงค่า Nonce ออกมาจากฐานข้อมูลเพื่อใช้ตรวจสอบ	2.1 ผู้ให้บริการเว็บเซอร์วิสตรวจสอบค่า UsernameToken ว่ามีค่าข้อมูลที่ได้รับมาว่าตรงกับข้อมูลในฐานข้อมูลหรือไม่ ดึงค่า CUsername, CPassword, CNonce, SNonce, CCreated และ SCreated ในฐานข้อมูลเพื่อนำมาเข้ากระบวนการตรวจสอบ
2.2 ผู้ให้บริการเว็บเซอร์วิสจัดเก็บค่า Nonce ที่ได้รับมาในฐานข้อมูล	2.2 ผู้ให้บริการเว็บเซอร์วิสอัพเดทบันทึกค่าข้อมูล CNonce, SNonce, CCreated และ SCreated ในฐานข้อมูลจนถึงประมวลผลส่งค่ากลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส
2.3 ผู้ให้บริการเว็บเซอร์วิสตรวจสอบค่า Created เป็นเวลาที่ไม่น้อยกว่าค่าเวลาปัจจุบันของเซิร์ฟเวอร์ผู้ให้บริการ	
2.4 ผู้ให้บริการเว็บเซอร์วิสตรวจสอบค่า Security Token เป็นค่าที่มีในฐานข้อมูลและเป็นค่าที่ยังไม่หมดอายุ	
2.5 ผู้ให้บริการเว็บเซอร์วิสอัพเดทค่าข้อมูล Security Token ในฐานข้อมูลจนถึงประมวลผลส่งค่ากลับไปยังผู้ขอใช้บริการเว็บเซอร์วิส	

จากตาราง พบว่าการพิสูจน์ตัวตนของการติดต่อสื่อสารของเว็บเซอร์วิสแบบสองขั้นตอน ในรูปแบบที่หนึ่ง WS Storing All Nonce มีกระบวนการเริ่มจากผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอไปร้องขอ Security Token จากเว็บเซอร์วิสเพื่อพิสูจน์ตัวตนจนถึงได้รับข้อมูลจากผู้ให้บริการเว็บเซอร์วิส การพิสูจน์ตัวตนรูปแบบนี้ให้รูปแบบที่หนึ่ง WS Storing All Nonce กระบวนการตรวจสอบข้อมูลหลักอยู่ที่ 7 ขั้นตอน ซึ่งมีกระบวนการขั้นตอนพิสูจน์ตัวตนมากกว่าการติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่สอง WS Not Storing All Nonce ซึ่งมีขั้นตอนการตรวจสอบข้อมูลหลักอยู่ที่ 4 ขั้นตอน และการพิสูจน์ตัวตนรูปแบบที่สองนี้จะหลีกเลี่ยงการตรวจสอบและจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูลจึงไม่ต้องใช้กระบวนการดึงค่า Nonce ทุกค่าที่อยู่ในฐานข้อมูลขึ้นมาตรวจสอบกับค่า Nonce ที่ได้รับมาจากผู้ขอใช้บริการเว็บเซอร์วิส โดยจะใช้กระบวนการตรวจสอบค่าข้อมูลในการบ่งบอกตัวตนที่ได้รับมาจากขั้นตอนการพิสูจน์ตัวตนทั้งสองขั้นตอนมาเข้ากระบวนตรวจสอบค่าข้อมูลและใช้การอัพเดทค่ากลับไปยังฐานข้อมูล

จากการวัดค่าการทำรายการตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce ดังหัวข้อที่ 4.2 และ วัดค่าการทำรายการตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่สอง WS Not Storing All Nonce ดังหัวข้อที่ 4.3 สามารถนำค่าเวลาการทำรายการที่วัดได้มาสร้างเป็นกราฟเปรียบเทียบตามกรณีทดลองดังนี้

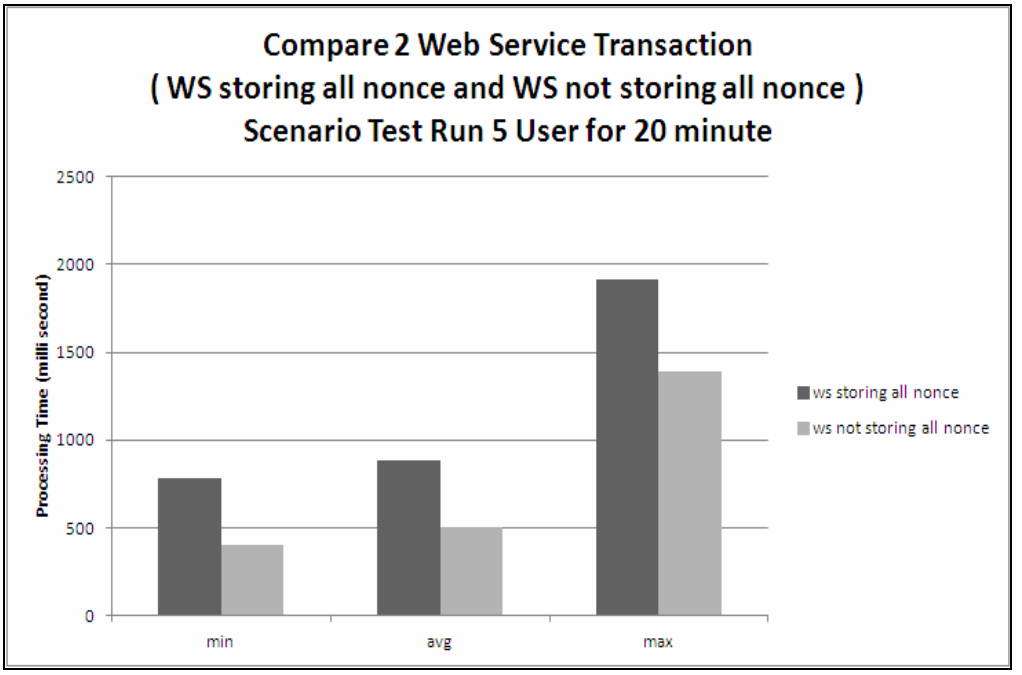
กรณีทดลองที่ 1 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce และรูปแบบที่สอง WS Not Storing All Nonce โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1 คน ทำรายการขอใช้บริการเว็บเซอร์วิสจำนวน 1, 10, 50,100 รายการ



รูปที่ 4.16 กราฟแสดงเปรียบเทียบค่าเวลาในการทำรายการ กรณีทดลองที่ 1

จากรูปที่ 4.16 เป็นกราฟแสดงเปรียบเทียบค่าเวลาในการทำรายการ กรณีทดลองที่ 1 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่งและรูปแบบที่สองโดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 1 คน ทำรายการขอใช้บริการเว็บเซอร์วิสจำนวน 1, 10, 50,100 รายการ พบว่าเวลาการทำรายการของการติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce ใช้เวลาในการทำรายการสูงกว่ารูปแบบที่สอง WS Not Storing All Nonce

กรณีทดลองที่ 2 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่สองโดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาที แล้ววัดค่าเวลาที่ใช้ในการทำรายการ



รูปที่ 4.17 กราฟแสดงเปรียบเทียบค่าเวลาในการทำรายการ กรณีทดลองที่ 2

จากรูปที่ 4.17 เป็นกราฟแสดงเปรียบเทียบค่าเวลาในการทำรายการ กรณีทดลองที่ 2 จำลองการทำรายการเว็บเซอร์วิสตามสถานการณ์การติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce ทีมีการลบค่า Nonce ในฐานข้อมูลทุก 3 นาที และรูปแบบที่สอง WS Not Storing All Nonce โดยจำลองผู้ร้องขอใช้บริการเว็บเซอร์วิสจำนวน 5 คน ทำรายการขอใช้บริการเว็บเซอร์วิสพร้อมกันเป็นเวลานาน 20 นาที แล้ววัดค่าเวลาที่ใช้ในการทำรายการ พบว่าเวลาการทำรายการของการติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce ใช้เวลาในการทำรายการสูงกว่ารูปแบบที่สอง WS Not Storing All Nonce

ในการเปรียบเทียบผลลัพธ์ค่าเวลาการทำรายการในการทดลองวัดประสิทธิภาพทั้งสองกรณี จากรูปที่ 4.16 และ รูปที่ 4.17 พบว่าเวลาการทำรายการของการติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce ใช้เวลาโดยเฉลี่ยในการทำรายการสูงกว่ารูปแบบที่สอง WS Not Storing All Nonce ในการติดต่อสื่อสารของเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing All Nonce จะมีกระบวนการตรวจสอบพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูล ทำให้ใช้เวลาในการทำรายการมากกว่ารูปแบบที่สอง WS Not Storing All Nonce ซึ่งใช้หลักการตรวจสอบและอัพเดทค่า Nonce ในฐานข้อมูลเป็นการหลีกเลี่ยงการจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูล

4.5 การเปรียบเทียบด้านการรักษาความมั่นคงปลอดภัย

ในด้านการป้องกันการโจมตีจากผู้ไม่ประสงค์ดีนั้น ผู้วิจัยได้ดำเนินการจำลองเหตุการณ์การโจมตีการเข้าถึงข้อมูลจากผู้ไม่ประสงค์ดีโดยจำลองเหตุการณ์สองเหตุการณ์คือ เหตุการณ์ที่หนึ่งผู้ไม่ประสงค์ดีทำการโจมตีแบบดักจับข้อมูล SOAP Message แล้วนำกลับมาใช้ใหม่ เรียกว่า Replay Attack และเหตุการณ์ที่สองผู้ไม่ประสงค์ดีทำการโจมตีแบบดักจับข้อมูล SOAP Message และดำเนินการแก้ไข SOAP Message แก้ไขข้อมูลของยูสเซอร์เนมโทเคนแล้วนำกลับมาใช้ใหม่ เรียกว่า Rewriting Attack เป็นการโจมตีเพื่อบิดเบือนข้อมูลว่าเป็นผู้มีสิทธิ์ในการเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิส โดยการจำลองการโจมตีทั้งสองเหตุการณ์นี้จะกระทำบนการติดต่อสื่อสารระหว่างเว็บเซอร์วิสสองรูปแบบคือ รูปแบบที่หนึ่ง WS Storing all Nonce และรูปแบบที่สอง WS not Storing all Nonce

- ในการจำลองเหตุการณ์การโจมตีจากผู้ไม่ประสงค์ดีบนการติดต่อสื่อสารระหว่างเว็บเซอร์วิสรูปแบบที่หนึ่ง WS Storing all Nonce พบว่าในกรณีที่โจมตีแบบ Replay Attack ดักจับ SOAP Message ในช่วงการติดต่อระหว่างผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอไปยังผู้ให้บริการเว็บเซอร์วิส และเกิดเหตุการณ์ถ้าทางฝั่งผู้ให้บริการเว็บเซอร์วิสมีการลบค่า Nonce ที่เก็บในฐานข้อมูลและค่า SecurityToken ยังไม่หมดอายุ ประกอบกับเวลาของเครื่องเซิร์ฟเวอร์ผู้ให้บริการเว็บเซอร์วิสและเวลาของเครื่องเซิร์ฟเวอร์ของผู้ไม่ประสงค์ดีมีค่าที่คลาดเคลื่อนกันอาจส่งผลให้ค่า Created ซึ่งเป็นค่าเวลาในยูสเซอร์เนมโทเคนที่ถูกดักจับและนำกลับมาใช้ใหม่นั้นยังคงอยู่ในช่วงเวลา Freshness Time ของทางฝั่งผู้ให้บริการเว็บเซอร์วิส ข้อมูลดังกล่าวมานั้นทำให้ผู้ไม่ประสงค์ดีสามารถนำข้อมูล SOAP Message มาใช้บิดเบือนข้อมูลว่าเป็นผู้มีสิทธิ์และสามารถเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิสได้

  ในการโจมตีแบบ Rewriting Attack พบว่าผู้ไม่ประสงค์ดีดักจับข้อมูล SOAP Message ดำเนินการแก้ไขข้อมูลในส่วนยูสเซอร์เนมโทเคนเช่นแก้ไขค่า Nonce เพื่อให้เป็นค่าใหม่ไม่ซ้ำกับค่า Nonce ที่บันทึกในฐานข้อมูลของผู้ให้บริการเวบเซอร์วิส แก้ไขค่า Created เพื่อให้เป็นเวลาที่ยังอยู่ในช่วง Freshness Time ของทางฝั่งผู้ให้บริการเว็บเซอร์วิส แต่ทางผู้โจมตีก็ต้องเดาค่ารหัสผ่านและต้องรู้วิธีการนำค่าต่างๆมาประกอบเป็นค่า Password ที่อยู่ในยูสเซอร์เนมโทเคนการโจมตีด้วยวิธีนี้จึงยากพอสมควรในการโจมตีเพื่อเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิส
- ในการจำลองเหตุการณ์การโจมตีจากผู้ไม่ประสงค์ดีบนการติดต่อสื่อสารระหว่างเว็บเซอร์วิสรูปแบบที่สอง WS not Storing all Nonce พบว่าในกรณีที่โจมตีแบบ Replay Attack นั้นถึงผู้โจมตีสามารถดักจับ SOAP Message ในช่วงการติดต่อระหว่างผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอไปยังผู้ให้บริการเว็บเซอร์วิสก็ไม่สามารถนำไปใช้งานได้เนื่องจากการตรวจสอบพิสูจน์ตัวตนนั้นต้องใช้ค่าข้อมูลยูสเซอร์เนมโทเคนในขั้นตอนแรกที่ผู้ขอใช้บริการเว็บเซอร์วิสส่งคำร้องขอไปยังเว็บเซอร์วิสพิสูน์ตัวตนใช้ประกอบกับข้อมูลยูสเซอร์เนมโทเคนที่

ส่งไปในครั้งที่สองเสมอ หรืออาจจะเรียกได้ว่าการร้องขอเพื่อเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิสต้องส่งคำร้องขอเข้าใช้งานทั้งสองครั้งเพื่อขอเข้าถึงข้อมูล เพราะการส่งข้อมูลยูสเซอร์เนมโทเคนทั้งสองขั้นตอนนั้น ข้อมูลที่ใช้ส่งไปเพื่อพิสูจน์ตัวตนมีความสัมพันธ์กันในการตรวจสอบความถูกต้อง เมื่อตรวจสอบแล้วข้อมูลยูสเซอร์เนมส่งมาทั้งสองครั้งพบว่าไม่ถูกต้องหรือไม่สัมพันธ์กันก็ไม่สามารถเข้าถึงข้อมูลได้ ถึงแม้ผู้ไม่ประสงค์ดีดักจับ SOAP Message ทั้งสองขั้นตอนแล้วนำกลับมาใช้ใหม่ก็ไม่สามารถเข้าถึงข้อมูลได้เพราะกระบวนการเทคนิคที่นำเสนอในงานวิจัยมีกระบวนการสร้างค่า SNonce และค่า SCreated เป็นค่าที่สร้างใหม่ทุกครั้งมาประกอบกับการพิสูจน์ตัวตนกับค่ายูสเซอร์เนมโทเคนทั้งสองขั้นตอนจึงทำให้ข้อมูล SOAP Message ที่ดักจับมาซึ่งเป็นค่าข้อมูลเดิมที่นำมาใช้นั้นเป็นข้อมูลที่ไม่ถูกต้อง วิธีการที่นำเสนอในงานวิจัยนี้ไม่ได้นำค่า Nonce มาเพื่อพิจารณาว่าซ้ำกับค่าที่เก็บในฐานข้อมูลทางผู้ให้บริการเว็บเซอร์วิสเพื่อป้องกันการ Replay Attack เพียงอย่างเดียว แต่เป็นการนำค่าต่างๆที่อยู่ในยูสเซอร์เนมโทเคนที่ส่งมาทั้งสองขั้นตอนกับค่าข้อมูลที่สร้างขึ้นใหม่ทุกครั้งของผู้ให้บริการเว็บเซอร์วิสนำมาประกอบพิจารณาความถูกต้องของข้อมูลที่ถูกส่งมาทั้งสองครั้งในการพิสูจน์ตัวตน ซึ่งต่างจากการติดต่อสื่อสารรูปแบบ WS Storing all Nonce มีการตรวจสอบพิสูจน์ตัวตนเข้าถึงข้อมูลผู้ให้บริการเว็บเซอร์วิสว่าคำร้องขอที่ได้รับมานั้นเป็นการถูก Replay Attack หรือไม่ ด้วยวิธีการพิจารณาค่า Nonce ที่ได้รับมาว่าซ้ำกับค่า Nonceที่เก็บในฐานข้อมูล จึงทำให้การติดต่อสื่อสารรูปแบบ WS not Storing all Nonce มีความสามารถป้องกันการโจมตีแบบ Replay Attack ได้ดีกว่ารูปแบบ WS Storing all Nonce

ในการโจมตีแบบ Rewriting Attack พบว่าผู้ไม่ประสงค์ดีดักจับข้อมูล SOAP Message ดำเนินการแก้ไขข้อมูลในส่วนยูสเซอร์เนมโทเคนในการติดต่อสื่อสารรูปแบบ WS not Storing all Nonce ทำได้ยากขึ้นมากกว่าเดิม เพราะต้องมีการส่งค่ายูสเซอร์โทเคนจำนวนสองครั้งเพื่อขอเข้าถึงข้อมูล ดังนั้นผู้ไม่ประสงค์ดีต้องดำเนินการแก้ไขค่าข้อมูลยูสเซอร์เนมโทเคนทั้งสองครั้งให้เป็นค่าที่มีความสัมพันธ์และถูกต้องด้วยและยังมีกระบวนการทางฝั่งผู้ให้บริการเว็บเซอร์วิสที่มีการสร้างค่า SNonce และ ค่า SCreated ใหม่ทุกครั้งเพื่อประกอบการพิสูจน์ตัวตนซึ่งผู้ไม่ประสงค์ดีก็ไม่สามารถทราบข้อมูลในส่วนนี้ได้เป็นส่วนเสริมการป้องกันการโจมตีจากผู้ไม่ประสงค์ดีให้มีความมั่นคงปลอดภัยเพิ่มขึ้นมากกว่าการติดต่อสื่อสารเว็บเซอร์วิสรูปแบบ WS Storing all Nonce

บทที่ 5
บทสรุป

ในงานวิจัยนี้ผู้วิจัยได้ดำเนินการศึกษาการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนของเว็บเซอร์วิสและยังได้ดำเนินการศึกษาและเสนอแนวคิดวิธีการเพิ่มเติมที่ช่วยให้การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนของเว็บเซอร์วิสนั้นไม่ต้องจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูล โดยผู้วิจัยทำการวัดประสิทธิภาพของการทำงานของเว็บเซอร์วิสที่มีการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนโดยแบ่งกลุ่มการติดต่อสื่อสารของเว็บเซอร์วิสออกเป็น 2 รูปแบบดังนี้ โดยรูปแบบที่หนึ่ง WS Storing All Nonce เป็นการติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.3 และรูปแบบที่สอง WS Not Storing All Nonce เป็นการติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการเรียกใช้โพรซีเดอร์ในการจัดการหลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.4 ผู้วิจัยดำเนินการวัดค่าเวลาในการทำรายการเว็บเซอร์วิสทั้งสองรูปแบบ

5.1 บทสรุปของงานวิจัย

จากงานวิจัยการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพื่อความมั่นคงปลอดภัยในเว็บเซอร์วิสสรุปได้ดังต่อไปนี้

1) การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนของเว็บเซอร์วิสเป็นวิธีการหนึ่งในการสร้างความมั่นคงปลอดภัยในระดับการเข้าถึงข้อมูลให้กับเว็บเซอร์วิส ในการนำวิธีการของยูสเซอร์เนมโทเคนมาใช้ในการพิสูจน์ตัวตนนั้นต้องมีการเก็บค่า Nonce ซึ่งเป็นค่าข้อความแบบสุ่มที่ทางผู้ขอเข้าใช้บริการเว็บเซอร์วิสต้องสร้างและส่งไปให้ผู้ให้บริการเว็บเซอร์วิสทุกครั้งเมื่อมีการติดต่อสื่อสารเพื่อขอเข้าถึงบริการข้อมูล ในการพิสูจน์ตัวตนของทางฝั่งผู้ให้บริการเว็บเซอร์วิสจึงต้องดำเนินการเก็บค่า Nonce ทุกครั้งที่ได้รับมาจากผู้ขอใช้บริการเว็บเซอร์วิสตามเวลาที่กำหนด เมื่อมีการส่งคำขอที่มียูสเซอร์เนมโทเคนจากทางผู้ขอใช้บริการเว็บเซอร์วิส ทางผู้ให้บริการเว็บเซอร์วิสต้องดำเนินการนำค่า Nonce ในยูสเซอร์เนมโทเคนที่ได้รับมานำมาตรวจสอบกับค่า Nonce ในฐานข้อมูลทุกค่าว่าซ้ำกับค่า Nonce เดิมที่เคยได้รับมาหรือไม่ กระบวนการนี้ทำให้ทางผู้ให้บริการเว็บเซอร์วิสต้องใช้เวลาหนึ่งในการตรวจสอบค่า Nonce ในกรณีที่มีจำนวนการทำรายการเข้ามาขอใช้บริการเว็บเซอร์วิสเป็นจำนวนมาก ค่า Nonceในฐานข้อมูลก็มีปริมาณมาก เป็นการเพิ่มต้นทุนในการทำงานของเว็บเซอร์วิสทำให้ผู้ให้บริการเว็บเซอร์วิสต้องใช้เวลาในการเปรียบเทียบค่า Nonce นั้นเพิ่มมากขึ้นจะเห็นได้จากการทดลองทำรายการของผู้ใช้งานเว็บเซอร์วิสพร้อมกันและมีการตั้งเวลาในการลบค่า Nonce ในฐานข้อมูลทุกๆ

1- 5 นาที พบว่าเวลาในการทำรายการของเว็บเซอร์วิสใช้เวลาเพิ่มขึ้นตามกำหนดเวลาที่ทำการลบค่า Nonce จึงสามารถกล่าวได้ว่าเวลาที่กำหนดไว้ในการลบค่า Nonce จากฐานข้อมูลนั้นมีผลต่อการเวลาที่ใช้ในการทำรายการของเว็บเซอร์วิส ถ้ากำหนดเวลาในการลบค่า Nonce จากฐานข้อมูลนาน เวลาที่ใช้ในการทำเว็บเซอร์วิสก็เพิ่มขึ้นด้วย

2) ผู้วิจัยได้ดำเนินการทดลองโดยจำลองการติดต่อสื่อสารของเว็บเซอร์วิสที่มีการพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนสองรูปแบบคือ รูปแบบที่หนึ่ง WS Storing All Nonce เป็นการติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.3 และ รูปแบบที่สอง WS Not Storing All Nonce เป็นการติดต่อสื่อสารระหว่างเว็บเซอร์วิสที่มีการใช้ยูสเซอร์เนมโทเคนในการพิสูจน์ตัวตนที่มีการเรียกใช้โพรซีเดอร์ในการจัดการหลีกเลี่ยงการจัดเก็บและตรวจสอบค่า Nonce ทุกค่าในฐานข้อมูลตามกระบวนการในบทที่ 3 หัวข้อที่ 3.4 ผู้วิจัยได้ดำเนินการวัดค่าเวลาที่ใช้ในการทำรายการของทั้งสองรูปแบบพบว่าค่าเวลาที่ใช้ในการทำรายการของรูปแบบที่หนึ่งมีค่าสูงกว่ารูปแบบที่สอง เนื่องจากรูปแบบที่สองใช้กระบวนการตรวจสอบและอัพเดทค่า Nonce ในฐานข้อมูลแทนการตรวจสอบและจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูล กระบวนการของรูปแบบที่สองช่วยลดเวลาในการทำรายการให้น้อยลงเนื่องจากทางฝั่งผู้ให้บริการเว็บเซอร์วิสไม่มีการจัดเก็บค่า Nonce ทุกค่าทุกครั้งในช่วงเวลาที่กำหนดซึ่งได้รับจากผู้ขอใช้บริการไว้ในฐานข้อมูลทำให้ไม่ต้องเสียเวลาในการตรวจสอบค่า Nonce ทุกค่าที่เก็บไว้ในฐานข้อมูล ยิ่งถ้ามีการขอใช้บริการเว็บเซอร์วิสจำนวนมากการจัดเก็บค่า Nonce ในฐานข้อมูลก็มากขึ้นเวลาที่ใช้ตรวจสอบว่าการทำรายการขอใช้บริการเว็บเซอร์วิสมีการส่งค่า Nonce เข้ามาซ้ำหรือไม่นั้นก็ใช้เวลามากตามไปด้วย กระบวนการที่นำเสนอเพิ่มเติมจึงช่วยเพิ่มประสิทธิภาพในจุดนี้ แต่กระบวนการที่นำเสนอเพิ่มเติมนี้ ก็มีข้อเสียเปรียบอยู่เช่นกัน ตัวอย่างเช่น กระบวนการที่เสนอนั้นเป็นเทคนิคที่ใช้ได้กับการทำรายการติดต่อระหว่างเว็บเซอร์วิสแบบสองขั้นตอนเท่านั้น เป็นวิธีที่ใช้กับเว็บเซอร์วิสที่ต้องการความปลอดภัยในการเข้าถึงข้อมูลอย่างมาก ซึ่งต้องมีการส่งคำขอสองครั้ง คือต้องมีการให้เว็บเซอร์วิสผู้ขอใช้บริการส่งคำขอ Security Token ก่อนทุกครั้งที่ต้องการขอใช้บริการ แล้วนำ Security Token พร้อมยูสเซอร์เนมโทเคนนำมาแนบกับคำร้องขอใช้บริการผ่าน SOAP Message ส่งไปขอใช้บริการกับเว็บเซอร์วิสผู้ให้บริการทำให้ผู้ขอใช้บริการเว็บเซอร์วิสต้องส่งคำขอสองครั้งเสมอถึงจะสามารถเข้าถึงข้อมูลทางฝั่งผู้ให้บริการเว็บเซอร์วิสได้

3) ในส่วนด้านความมั่นคงปลอดภัยของข้อมูลงานวิจัยนี้ในนำเสนอ SPassword ซึ่งเป็น Security Token เข้ามาเป็นส่วนหนึ่งร่วมกับยูสเซอร์เนมโทเคนเป็นการเพิ่มระดับช่วยเสริมในเรื่องการรักษาความปลอดภัยในการเข้าถึงข้อมูลป้องกันการโจมตีจากผู้ไม่ประสงค์ดีด้าน Replay Attack ให้ดียิ่งขึ้น ขั้นตอนการพิสูจน์ตัวตนที่นำเสนอเพิ่มเติมนั้นต้องมีการพิสูจน์ตัวตนแบบสองขั้นตอนและในการเข้าถึงข้อมูลจากผู้ให้บริการเว็บเซอร์วิสผู้ขอใช้บริการข้อมูลต้องขอ SPassword ใหม่ทุกครั้งเมื่อ

ต้องการขอเข้าถึงข้อมูล ผู้ขอใช้บริการข้อมูลจะไม่สามารถเข้าถึงข้อมูลได้ถ้าไม่มีการดำเนินการขอ SPassword ซึ่ง SPassword เป็นค่า Security Token ที่สร้างโดยหลักการนำข้อมูลที่ใช้ในการบ่งบอกตัวตนของผู้ที่ได้รับสิทธิ์ในการเข้าถึงข้อมูลและค่า SNonce เป็นค่าตัวอักษรที่เกิดจากการสุ่มทุกครั้งของทางฝั่งผู้ให้บริการเว็บเซอร์วิส เมื่อผู้ขอใช้บริการเว็บเซอร์วิสได้รับคำร้องขอ SPassword และนำค่าทั้งหมดมาเข้ารหัสสร้างเป็นค่ารหัสผ่านในยูสเซอร์เนมโทเคนเพื่อใช้ประกอบการพิสูจน์ตัวตนว่าสามารถเข้าถึงข้อมูลของทางฝั่งผู้ให้บริการเว็บเซอร์วิส วิธีการนี้จะทำให้ผู้ไม่ประสงค์ดีที่จะดำเนินการโจรกรรมข้อมูลนั้นสามารถโจมตีแบบ Replay Attack ได้ยากขึ้น เนื่องจากถ้าผู้ไม่ประสงค์ดีสามารถดักจับ SOAP Message ในขั้นตอนการขอ SPassword และดักจับ SOAP Message ในขั้นตอนการขอใช้บริการข้อมูลได้และดำเนินการส่งคำร้องซ้ำไปขอ SPassword จากผู้ให้บริการเว็บเซอร์วิสได้ จากนั้นผู้ไม่ประสงค์ดีดำเนินการส่งคำร้องเป็น SOAP Message ที่ดักจับในขั้นตอนขอเข้าถึงข้อมูลผู้ให้บริการเว็บเซอร์วิส ผู้ไม่ประสงค์ดีก็ไม่สามารถเข้าถึงข้อมูลได้เพราะ SOAP Message ที่ส่งมานั้นทางผู้ให้บริการเว็บเซอร์วิสจะนำข้อมูลยูสเซอร์เนมโทเคนใน SOAP Message นำมาถอดรหัสและตรวจสอบกับข้อมูลที่ทางผู้ให้บริการเว็บเซอร์วิสจัดเก็บในฐานข้อมูลซึ่งทำการตรวจสอบแล้วจะพบว่าเป็นข้อมูลที่ไม่ตรงกับข้อมูลที่ใช้ในการพิสูจน์ตัวตนที่เก็บในฐานข้อมูล เพราะค่า SNonce หรือค่าตัวอักษรแบบสุ่มเป็นค่าที่สำคัญที่ใช้ประกอบการพิสูจน์ตัวตนของทางผู้ให้ริการเว็บเซอร์วิสเป็นค่าตัวอักษรแบบสุ่มที่ต้องสร้างใหม่ทุกครั้งเมื่อได้รับคำร้องขอ SPassword ก็ทำให้ผู้ไม่ประสงค์ดีไม่สามารถนำ SOAP Message ที่ดักจับมาใช้เข้าถึงข้อมูลได้ เพราะเมื่อนำ SOAP Message ที่มีค่า SPassword ที่เป็นค่าเดิมในยูสเซอร์เนมโทเคนมาขอใช้เข้าถึงข้อมูลทำให้ผู้ให้บริการเว็บเซอร์วิสตรวจสอบพบว่าไม่มีสิทธิ์ในการเข้าถึงข้อมูลที่ให้บริการเพราะข้อมูลพิสูจน์ตัวตนไม่ถูกต้อง หรือจะนำ SOAP Message ที่ดักจับได้ในขั้นตอนขอเข้าถึงข้อมูลนำมาแก้ไขเปลี่ยนแปลง ผู้ไม่ประสงค์ดีก็ต้องทราบข้อมูลที่ใช้ประกอบการพิสูจน์ตัวตนทุกตัวและวิธีการนำค่าทั้งหมดมาเข้ารหัสถึงจะสามารถเข้าถึงข้อมูลได้ แต่การที่ผู้ที่ไม่ประสงค์ดีนั้นต้องทราบข้อมูลและวิธีการนำค่าทั้งหมดมาเข้ารหัสนั้นเป็นเรื่องที่ทำได้ยากมาก ดังนั้นวิธีการพิสูจน์ตัวตนที่งานวิจัยนำเสนอนั้นช่วยเพิ่มความมั่นคงปลอดภัยในการเข้าถึงข้อมูลของผู้ให้บริการเว็บเซอร์วิส

4) สำหรับเทคนิคกระบวนการที่นำเสนอในงานวิจัยนี้ เป็นการทำเสนอการพิสูจน์ตัวด้วยยูสเซอร์เนมโทเคนเป็นการรักษาความปลอดภัยในการเข้าถึงข้อมูลเว็บเซอร์วิสบนการติดต่อสื่อสารแบบสองขั้นตอน วิธีการที่นำเสนอนั้นเหมาะสำหรับนำไปประยุกต์ใช้กับงานในลักษณะที่มีการประมวลผลข้อมูลจำนวนมากเช่น การร้องขอเพื่อเข้าถึงข้อมูลเว็บเซอร์วิสแบบ Batch ที่มีการส่งคำร้องขอในการเข้าถึงข้อมูลครั้งละจำนวนมาก หรือการทำรายการที่ต้องมีการส่งคำสั่งเพื่อร้องขอเข้าถึงข้อมูลผู้ให้บริการเว็บเซอร์วิสด้วยผู้ใช้งานระบบเดิมแต่มีการร้องขอเข้าใช้บริการจำนวนมากหลายๆ ครั้ง เนื่องจากกระบวนการเทคนิคที่นำเสนอในงานวิจัยเป็นวิธีการที่ช่วยลดการจัดเก็บค่า Nonce ในฐานข้อมูลทางฝั่งผู้ให้บริการเว็บเซอร์วิส ซึ่งวิธีการเดิมเมื่อมีการร้องขอเข้าถึงข้อมูลเว็บเซอร์วิส

จำนวนมาก ผู้ให้บริการเว็บเซอร์วิสก็ต้องจัดเก็บค่า Nonce ที่ได้รับมาจากผู้ขอใช้บริการเว็บเซอร์วิสทุกค่าทุกครั้งในฐานข้อมูลในช่วงเวลาที่กำหนด เมื่อมีการร้องขอใช้บริการจำนวนมากค่า Nonce ที่เก็บในฐานข้อมูลจำนวนมากขึ้น เวลาที่ใช้ในการค้นหาเพื่อตรวจสอบค่า Nonce ก็เพิ่มมากขึ้นด้วย ดังนั้นกระบวนเทคนิคที่นำเสนอในงานวิจัยจึงมีประโยชน์ในด้านการจัดการค่า Nonce ในการพิสูจน์ตัวตนในกรณีที่มีการร้องขอเพื่อเข้าถึงข้อมูลผู้ให้บริการเว็บเซอร์วิสที่มีการทำรายการจำนวนที่มาก

5.2 แนวทางที่พัฒนาในอนาคตและข้อเสนอแนะ

สำหรับงานในอนาคตงานวิจัยนี้ผู้ที่สนใจสามารถนำกระบวนไปประยุกต์ใช้ในการจัดการการพิสูจน์ตัวตนเว็บเซอร์วิสด้วยยูสเซอร์เนมโทเคนในเว็บเซอร์วิสแบบขั้นตอนเดียวเพราะบางครั้งข้อมูลที่ให้บริการเป็นข้อมูลที่อาจจะไม่ต้องการความปลอดภัยมากไม่จำเป็นต้องร้องขอ Security Token ซึ่งผู้ขอใช้บริการเว็บเซอร์วิสสามารถส่งคำขอใช้บริการพร้อมยูสเซอร์เนมโทเคนเพียงครั้งเดียว และสามารถจัดการหลีกเหลี่ยงการจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูลได้ จึงเป็นส่วนที่ต้องการพัฒนาเพิ่มเติมในลำดับต่อไป

ในส่วนของข้อเสนอแนะ ในปัจจุบันเว็บเซอร์วิสเป็นเว็บให้บริการแลกเปลี่ยนข้อมูลดังนั้นความปลอดภัยของข้อมูลจึงเป็นสิ่งที่สำคัญมาก การนำยูสเซอร์เนมโทเคนไปใช้ในการพิสูจน์ตัวตนของเว็บเซอร์วิสเป็นทางเลือกหนึ่งในการรักษาความปลอดภัยระดับการเข้าถึงข้อมูล ผู้ที่สนใจสามารถนำแนวคิดเทคนิคที่นำเสนอเพิ่มเติมโดยหลีกเลี่ยงการจัดเก็บค่า Nonce ทุกค่าในฐานข้อมูลของงานวิจัยนี้ไปประยุกต์ใช้เพื่อรักษาความปลอดภัยข้อมูลของเว็บเซอร์วิสให้กับองค์กร ช่วยในด้านการรักษาความปลอดภัยในการเข้าถึงข้อมูลโดยเฉพาะข้อมูลที่มีความสำคัญมากควรมีการป้องกันผู้ไม่ประสงค์ดีในการโจรกรรมข้อมูล ในกระบวนการที่ใช้ในการรักษาความปลอดภัยนั้นต้องไม่ส่งผลกระทบต่อสมรรถภาพการทำงานของระบบด้วย

เอกสารอ้างอิง

1. Booth, D. and Haas, H., 2004, “Web Services Architecture”, **W3C Working Group Note 11 February 2004** [Online], Available : http://www.w3.org/TR/ws-arch/. [2012, February 11].

2. Pfleeger, C. and Pfleeger, S., 2006, **Security in computing**, Safari Books Online, United States of America, pp. 1-35.

3. Singhal, A., Winograd, T. and Scarfone, K., 2007, **Guide to Secure Web Services**, NIST Special Publication, United States of America, pp. 1-20.

4. Peterson, S., 1999, “Web Services Security UsernameToken Profile 1.1”, **OASIS Standard Specification** [Online], Available : http://docs.oasis-open.org/wss/v1.1/. [2012, March 1].

5. Peng, D., Li, C. and Huo, H., 2009, "An Extended UsernameToken-based Approach for REST-style Web Service Security Authentication", **2009 2nd IEEE International Conference on Computer Science and Information Technology**, 11 August 2009, Beijing, China, pp. 582-586.

6. Rahaman, M., Schaad, A. and Rits, M., 2006, "Towards Secure SOAP Message Exchange in SOA", **Proceedings of the 3rd ACM workshop on Secure web services**, 2006, New York, USA, pp. 77-84.

7. Alonso, G., Casati, F., Kuno, H. and Machiraju, V., 2004, “Web Services Concepts, Architectures and Applications”, **Springer-Verlag Berlin Heidelberg**, Germany, pp. 121-128.

8. Wei, X., Gao, J., Ding, X. and Yuan, S., 2007, “Platform EGO Web Service Gateway”, **2007 IEEE Asia-Pacific Services Computing Conference**, 11-14 DEC 2007, Tsukuba Science City, pp.283-290.

9. ธัชชัย รัศมีโรจน์,2553, **การพิสูจน์ตัวตน ณ จุดเดียวผ่านโปรแกรมประยุกต์บนเว็บด้วย SAML 2.0**, โครงการเฉพาะเรื่องปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมซอฟต์แวร์ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี, หน้า 9-33.

10. Gunzer, H., "Introduction to Web Services", **Borland** [Online], Available : http://edn.embarcadero.com/article/images/28818/webservices.pdf [2012, December 5].

11. Bhargavan, K., Fournet, C. and Gordon, A., 2008, "Verifying Policy-Based Web Services Security", **ACM Transactions on Programming Languages and Systems** [Elecronic], Vol. 30, No. 6, pp. 30-39, Available : ACM [2013,January 10].

12. Garcia, D. and Toledo, M., 2008, "Web Service Security Management Using Semantic Web Techniques", **ACM SAC'08**,16-20 March 2008, Fortaleza, Brazil,pp.2256-2260.

13. Gruschka, N., Jensen, M. and Dziuk, T., 2007, "Event-based Application of WS-SecurityPolicy on SOAP Messages", **ACM SWS'07**,02 November 2007, Virginia, USA,pp.1-8.

14. Bhargavan, K., Corin, R., Fournet, C. and Gordon, A., 2004, "Secure Sessions for Web Services", **ACM Workshop on Secure Web Services**, 29 October 2004, Fairfax VA, USA,pp.56-65.

15. Nadalin, A., Kaler, C., Monzillo, R. and Baker, P., 2006, Web Services Security:SOAP Message Security 1.1 (WS-Security 2004), **OASIS Standard Specification** [Online], Available : https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf [2012, December 12].

16. Hendrik R., "An introduction to Web Service Security using WSE Part-1", **CodeProject** [Online], Available : http://www.codeproject.com/Articles/7062/An-introduction-to-Web-Service-Security-using-WSE [2013, January 12].

17. Han, D., "WebService Authentication with UsernameToken in WSE 3.0", **CodeProject**[Online], Available :http://www.codeproject.com/Articles/19508/WebService-Authentication-with-UsernameToken-in-WS [2013, January 15].

18. Microsoft, “UsernameToken Class”, **Microsoft MSDN** [Online], Available : http://msdn.microsoft.com/en-us/library/microsoft.web.services3.security.token.usernametoken.aspx [2013, January 28].

ประวัติผู้วิจัย

ชื่อ – สกุล	นางสาวศิริรัตนา นิลน้อย
วัน เดือน ปีเกิด	11 มิถุนายน 2528
ประวัติการศึกษา	
ระดับมัธยมศึกษา	ประโยคมัธยมศึกษาตอนปลาย โรงเรียนรัตนราษฎร์บำรุง พ.ศ. 2546
ระดับปริญญาตรี	วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาตร์ วิทยาเขตกำแพงแสน พ.ศ. 2550
ระดับปริญญาโท	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี พ.ศ. 2556
ทุนการศึกษา หรือทุนวิจัย	ทุนการศึกษาระดับบัณฑิตศึกษา สาขาเทคโนโลยีสารสนเทศ ปีงบประมาณ 2556
ประวัติการทำงาน	โปรแกรมเมอร์อาวุโส บริษัท ธนาคารธนชาต จำกัด พ.ศ. 2551-2556
ผลงานที่ได้รับการตีพิมพ์	ศิริรัตนา นิลน้อย และ เกรียงไกร ปอแก้ว, 2556, “การพิสูจน์ตัวตนด้วยยูสเซอร์เนมโทเคนเพื่อความมั่นคงปลอดภัยในเว็บเซอร์วิส”, **การประชุมวิชาการเสนอผลงานวิจัยระดับบัณฑิตศึกษาแห่งชาติ,** ครั้งที่ 29, 24 – 25 ตุลาคม 2556**, มหาวิทยาลัยแม่ฟ้าหลวง**, หน้า 18-25.

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
ข้อตกลงว่าด้วยการโอนลิขสิทธิ์วิทยานิพนธ์

วันที่ 25 เดือน พฤศจิกายน พ.ศ. 2556

ข้าพเจ้า (~~นาย/นาง~~/นางสาว) ศิริรัตนา นิลน้อย รหัสประจำตัว 54440375 เป็นนักศึกษาของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ระดับปริญญา ☑ โท ☐ เอก หลักสูตร วิทยาศาสตรมหาบัณฑิต สาขาวิชา เทคโนโลยีสารสนเทศ คณะ เทคโนโลยีสารสนเทศ อยู่บ้านเลขที่ 143 ตรอก/ซอย - ถนน - ตำบล/แขวง ท่าผา อำเภอ/เขต บ้านโป่ง จังหวัด ราชบุรี รหัสไปรษณีย์ 70110 เป็น "ผู้โอน" ขอโอนลิขสิทธิ์วิทยานิพนธ์ให้ไว้กับมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี โดยมี รศ.ดร.นิพนธ์ เจริญกิจการ ตำแหน่ง คณบดีคณะเทคโนโลยีสารสนเทศ เป็นตัวแทน "ผู้รับโอน" สิทธิในทรัยพ์สินทางปัญญาและมีข้อตกลงดังนี้

1. ข้าพเจ้าได้จัดทำวิทยานิพนธ์เรื่อง การพิสูจน์ตัวตนด้วยลายเซ็นโดยใช้เทคนิคเพื่อความมั่นคงของลายเซ็นบนเว็บเซอร์วิส ซึ่งอยู่ในความควบคุมของ ผศ. ดร.เกรียงไกร ฟองแก้ว ตามมาตราพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และถือว่าเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

2. ข้าพเจ้าตกลงโอนลิขสิทธิ์จากผลงานทั้งหมดที่เกิดขึ้นจากการสร้างสรรค์ของข้าพเจ้าในวิทยานิพนธ์ให้กับมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี ตลอดอายุแห่งการคุ้มครองลิขสิทธิ์ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 ตั้งแต่วันที่ได้รับอนุมัติโครงร่างวิทยานิพนธ์จากมหาวิทยาลัย

3. ในกรณีที่ข้าพเจ้าประสงค์จะนำวิทยานิพนธ์ไปใช้ในการเผยแพร่ในสื่อใด ๆ ก็ตาม ข้าพเจ้าจะต้องระบุว่าวิทยานิพนธ์เป็นผลงานของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรีทุกครั้งที่มีการเผยแพร่

4. ในกรณีที่ข้าพเจ้าประสงค์จะนำวิทยานิพนธ์ไปเผยแพร่หรืออนุญาตให้ผู้อื่นทำซ้ำหรือดัดแปลงหรือเผยแพร่ต่อสาธารณชนหรือกระทำการอื่นใด ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 โดยมีค่าตอบแทนในเชิงธุรกิจ ข้าพเจ้าจะกระทำได้เมื่อได้รับความยินยอมเป็นลายลักษณ์อักษรจากมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรีก่อน

5. ในกรณีที่ข้าพเจ้าประสงค์จะนำข้อมูลจากวิทยานิพนธ์ไปประดิษฐ์หรือพัฒนาต่อยอดเป็นสิ่งประดิษฐ์หรืองานทรัพย์สินทางปัญญาประเภทอื่น ภายในระยะเวลา (10) ปีนับจากวันลงนามในข้อตกลงฉบับนี้ ข้าพเจ้าจะกระทำได้เมื่อได้รับความยินยอมเป็นลายลักษณ์อักษรจามหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี และมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรีมีสิทธิในทรัพย์สินทางปัญญานั้น พร้อมกับได้รับชำระค่าตอบแทนการอนุญาตให้ใช้สิทธิดังกล่าว รวมถึงการจัดสรร

ผลประโยชน์อันพึงเกิดขึ้นจากส่วนใดส่วนหนึ่งหรือทั้งหมดของวิทยานิพนธ์ในอนาคต โดยให้เป็นไปตามระเบียบสถาบันเทคโนโลยีพระจอมเกล้าธนบุรี ว่าด้วยการบริหารผลประโยชน์อันเกิดจากทรัพย์สินทางปัญญา พ.ศ. 2538

6. ในกรณีที่มีผลประโยชน์เกิดขึ้นจากวิทยานิพนธ์หรืองานทรัพย์สินทางปัญญาอื่นที่ข้าพเจ้าทำขึ้นโดยมีมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรีเป็นเจ้าของ ข้าพเจ้าจะมีสิทธิ์ได้รับการจัดสรรผลประโยชน์อันเกิดจากทรัพย์สินทางปัญญาดังกล่าวตามอัตราที่กำหนดไว้ในระเบียบสถาบันเทคโนโลยีพระจอมเกล้าธนบุรี ว่าด้วยการบริหารผลประโยชน์อันเกิดจากทรัพย์สินทางปัญญา พ.ศ. 2538

ลงชื่อ.....ศิริรัตนา นิลน้อย.....ผู้โอนลิขสิทธิ์
(นางสาวศิริรัตนา นิลน้อย)

ลงชื่อ.....ผู้รับโอนลิขสิทธิ์
(รศ.ดร.นิพนธ์ เจริญกิจการ)

ลงชื่อ.....พยาน
(นางสาวอาภรณ์ เชี่ยวชาญเกษตร)

ลงชื่อ.....พยาน
(นางถิรดา ยุกตะนันทน์)