ระบบเฝ้าตรวจข้อมูลจราจรทางคอมพิวเตอร์สำหรับผู้ปกครองจากเครือข่ายในบ้านพักอาศัย

Parental Control System via Network Monitoring in Residential Network

สายัณ อินชะนะ

Sayan Inchana

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญา
วิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ
มหาวิทยาลัยสงขลานครินทร์

A Thesis Submitted in Partial Fulfillment 0f Requirements for the Degree of
Master of Science in Management of Information Technology
Prince of Songkla University
2555

ชื่อวิทยานิพนธ์ ระบบเฝ้าตรวจข้อมูลจราจรทางคอมพิวเตอร์สำหรับผู้ปกครองจากเครือข่ายในบ้านพักอาศัย

ผู้เขียน นายสายัณ อินชะนะ

สาขาวิชา การจัดการเทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	**คณะกรรมการสอบ**
.....	.....ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.สุนทร วิทูสุรพจน์)	(ผู้ช่วยศาสตราจารย์ ดร.พรชัย พฤกษ์ภัทรานนต์)
	.....กรรมการ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	(ผู้ช่วยศาสตราจารย์ ดร.สุนทร วิทูสุรพจน์)
.....	.....กรรมการ
(ดร.สมชัย หลิมศิโรรัตน์)	(ดร.สมชัย หลิมศิโรรัตน์)
	.....กรรมการ
	(ดร.สุรชัย จิตภักดีบดินทร์)

บัณฑิตวิทยาลัย มหาวิทยาลัยสงขลานครินทร์ อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาการจัดการเทคโนโลยีสารสนเทศ

.....

(ศาสตราจารย์ ดร.อมรรัตน์ พงศ์ดารา)

คณบดีบัณฑิตวิทยาลัย

ชื่อวิทยานิพนธ์ ระบบเฝ้าตรวจข้อมูลจราจรทางคอมพิวเตอร์สำหรับผู้ปกครองจากเครือข่ายในบ้านพักอาศัย

ผู้เขียน นายสายัณ อินชะนะ

สาขาวิชา การจัดการเทคโนโลยีสารสนเทศ

ปีการศึกษา 2554

บทคัดย่อ

วิทยานิพนธ์นี้ ได้ศึกษาคัดเลือกอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่เป็นคอมพิวเตอร์แบบฝังตัวและซอฟต์แวร์ที่จำเป็นในการใช้งาน เพื่อติดตั้งระบบจัดเก็บข้อมูลจราจรเครือข่ายคอมพิวเตอร์ภายในบ้านพักอาศัย โดยนำเอาแนวคิดของระบบเครื่องแม่ข่าย มาเป็นแนวทางในการพัฒนากลไกเพื่อจัดเก็บข้อมูลจราจร และการนำข้อมูลไปวิเคราะห์ผลการใช้งานอย่างชาญฉลาด โดยใช้เทคนิควิธีฟัซซีลอจิก เพื่อแก้ปัญหาความไม่ยืดหยุ่นในการตัดสินใจ จากผลการศึกษาทดลองพบว่าอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่เป็นคอมพิวเตอร์แบบฝังตัว และซอฟต์แวร์ที่คัดเลือกสามารถติดตั้งระบบจัดเก็บข้อมูลจราจรเครือข่ายได้ ทำให้ช่วยประหยัดค่าใช้จ่ายด้านพลังงานไฟฟ้าและราคาของอุปกรณ์อย่างชัดเจน ส่วนการนำเทคนิควิธีฟัซซีลอจิกมาใช้นั้นทำให้ระบบมีความยืดหยุ่นในการปรับเปลี่ยนกฎเกณฑ์การเฝ้าตรวจ สามารถประเมินจากกฎเกณฑ์จำนวนมาก และ มีความเป็นมิตรต่อผู้ใช้ในการแสดงผลลัพธ์การประเมิน การศึกษายังแสดงให้เห็นว่าควรนำข้อมูลบางส่วนของไฟล์ข้อมูลจราจรฯ ที่ได้จากเราเตอร์ไปใช้อย่างไร จึงจะเพียงพอต่อการสร้างตัวแปรและกฎเกณฑ์ฟัซซีต่างๆ ที่ใช้ในการตัดสินใจพร้อมยกตัวอย่างการวิเคราะห์ข้อมูลจริงและแสดงผลแนวคิดเชิงกราฟิกที่ง่ายต่อการทำความเข้าใจ

คำสำคัญ: คอมพิวเตอร์ฝังตัว, ข้อมูลจราจร, ฟัซซีลอจิก, การควบคุมโดยผู้ปกครอง

Thesis Title	Parental Control System via Network Monitoring in Residential Network
Author	Mr. Sayan Inchana
Major Program	Management of Information Technology
Academic Year	2011

ABSTRACT

This thesis was a selection of embedded system access point router and others necessary software for network traffic logs installation in residence. Computer server was used as a model in traffic logs development while fuzzy logic was employed for an analysis and for solving unflexibility in decision making. The experiment revealed that embedded system access point router and the selected software could be used for network traffic logs installation. Moreover, they helped save money on electricity and computer equipment. The application of fuzzy logic led to flexibility in the adjustment of monitoring rules; applicability for evaluation on a number of rules; and friendliness for showing evaluation results to users in a comprehensive manner. Furthermore, the study suggested how the partial data of network traffic log taken from the router should be used so that fuzzy variables and rules can be adequately defined. In addition, we give examples of analysis based on actual data and show graphical results for ease of understanding.

Keywords: Embedded System, Network Traffic, Fuzzy Logic, Parental Control.

กิตติกรรมประกาศ

ขอแสดงคำขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.สุนทร วิทูสุรพจน์ ประธานกรรมการที่ปรึกษางานวิจัย และ ดร.สมชัย หลิมศิโรรัตน์ กรรมการที่ปรึกษางานวิจัยร่วม ที่ได้กรุณาอุทิศเวลาให้คำปรึกษา แนะนำความรู้ในด้านการทำวิจัย เอกสาร ข้อมูลต่างๆ เป็นอย่างดี รวมทั้งแนวความคิดและกำลังใจในการแก้ปัญหา ตลอดจนตรวจทานแก้ไขวิทยานิพนธ์ให้ดำเนินไปอย่างสมบูรณ์

ขอขอบพระคุณ ผู้ช่วยศาสตราจารย์ ดร.พรชัย พฤกษ์ภัทรานนต์ ประธานกรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำปรึกษา คำแนะนำ และตรวจทานวิทยานิพนธ์ให้ดำเนินไปอย่างสมบูรณ์

ขอขอบพระคุณ ดร.สุรชัย จิตภักดีบดินทร์ กรรมการสอบวิทยานิพนธ์ ที่ได้กรุณาให้คำปรึกษา คำแนะนำ และตรวจทานวิทยานิพนธ์ให้ดำเนินไปอย่างสมบูรณ์

ขอขอบพระคุณ หลักสูตรการจัดการเทคโนโลยีสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตหาดใหญ่ ที่ให้การสนับสนุนห้องปฏิบัติการวิจัยและเพื่อนนักศึกษาทุกท่านที่ได้ให้ความช่วยเหลือมาโดยตลอด

ขอขอบคุณ พี่ๆ เพื่อนๆ น้องๆ และที่ทำงานทุกท่านที่ได้ให้คำปรึกษา คำแนะนำ และเป็นกำลังใจที่ดีมาโดยตลอด

สุดท้ายนี้ ข้าพเจ้าขอน้อมรำลึกถึงพระคุณของบิดามารดาและพี่สาวของข้าพเจ้า ที่ส่งเสริมสนับสนุน ให้คำแนะนำ ให้คำปรึกษา ให้กำลังใจ และให้ทุนทรัพย์แก่ข้าพเจ้าตลอดจนกระทั่งทำให้ข้าพเจ้าประสบความสำเร็จ

สายัณ อินชะนะ

สารบัญ

สารบัญ(ต่อ)

สารบัญ(ต่อ)

สารบัญภาพ

สารบัญภาพ (ต่อ)

รูปภาพประกอบ **หน้า**

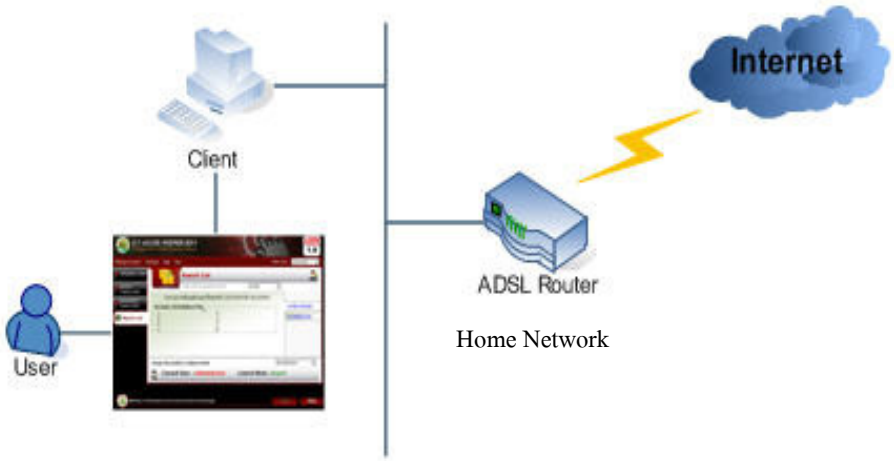
สารบัญตาราง

บทที่ 1

บทนำ

1.1 ความสำคัญและที่มาของการวิจัย

ปัจจุบันอินเตอร์เน็ตเป็นเครือข่ายสาธารณะที่มีผู้ใช้งานกันอย่างแพร่หลายที่สุด ครอบคลุมการใช้งานลักษณะต่างกัน เช่น การประกอบอาชีพ การศึกษาหาความรู้ และเพื่อความบันเทิง เป็นต้น อย่างไรก็ตาม มีผู้ใช้บางส่วนนำอินเตอร์เน็ตไปใช้ในทางที่ไม่เหมาะสม เช่น การแจ้งหรือกระจายข่าวอันเป็นเท็จ หลอกลวงให้เกิดความเสียหายต่อบุคคลหรือองค์กรต่างๆ ทำให้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ได้ออกพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พุทธศักราช 2550 [1] เพื่อบังคับให้มีการจัดทำระบบสำหรับการเฝ้าตรวจและบันทึกข้อมูลจราจรทางคอมพิวเตอร์ของเครือข่ายภายในองค์กร/ธุรกิจ/ร้านอินเทอร์เน็ตต่างๆ ที่ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ให้เก็บรักษาข้อมูลเพื่อการตรวจสอบย้อนหลังได้ และจากการศึกษาระบบที่มีการเฝ้าตรวจและบันทึกข้อมูลจราจรทางคอมพิวเตอร์ขององค์กร/ธุรกิจที่นิยมใช้ในปัจจุบัน 2 แบบ คือ ก) อุปกรณ์เครือข่ายสำเร็จรูปเชิงพานิชย์ และ ข) เครื่องคอมพิวเตอร์ที่เป็นแม่ข่าย ที่รองรับการให้บริการสำหรับองค์กร/ธุรกิจต่างๆ แต่เป็นที่น่าสังเกตว่าพระราชบัญญัติ ฉบับนี้ไม่ได้บังคับรวมไปถึงบ้านพักอาศัย เนื่องจากได้ระบุให้เป็นหน้าที่ของผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider หรือ ISP) ไว้แล้ว.ซึ่งหากมองย้อนกลับมายังบ้านพักอาศัยที่โดยส่วนใหญ่มีกลุ่มผู้ใช้งานที่แตกต่างกันและเป็นที่เป็นจุดเริ่มต้นของเยาวชนโดยเฉพาะบุตร/ธิดา ซึ่งอาจมีการเข้าใช้งานอินเทอร์เน็ตในทางที่ไม่เหมาะสมได้ ดังนั้นในบ้านพักอาศัยจึงมีความจำเป็นที่ผู้ปกครองควรเฝ้าระวังการใช้งานอินเทอร์เน็ตในทางที่ผิดหรืออาจไม่เหมาะสม และจากการศึกษาข้อมูลของระบบป้องกันการใช้งานพบว่ามีเพียงซอฟต์แวร์บางประเภทที่ช่วยในการป้องกันการเข้าใช้งานอินเทอร์เน็ตที่ไม่เหมาะสมได้ ตัวอย่างเช่น ซอฟต์แวร์ Web Nanny [2] หรือ ICT House Keeper [3] ของกระทรวง ICT ที่ง่ายสำหรับการนำมาใช้งาน โดยการดาวน์โหลดซอฟต์แวร์เพื่อติดตั้งในเครื่องของผู้ใช้งาน ซึ่งซอฟต์แวร์ทำหน้าที่ในการป้องกันการเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสมหรือที่ผู้ปกครองไม่อนุญาต ดังแสดงรูปที่ 1.1 แต่ซอฟต์แวร์ดังกล่าวมีแต่มีข้อด้อย ในเรื่องของการตั้งซอฟต์แวร์ลงบนเครื่องของผู้ใช้งานเท่านั้น และตามจำนวนของเครื่องคอมพิวเตอร์ที่ใช้งาน ซึ่งหากผู้ใช้งานมีทักษะความรู้ด้านคอมพิวเตอร์ก็อาจจะสามารถลบหรือป้องกันการทำงานของโปรแกรมได้ และการปิดกั้นการใช้งานในลักษณะนี้ทำให้ไม่สามารถติดตามหรือเฝ้าดูพฤติกรรมการใช้งานอินเทอร์เน็ตของ บุตร/ธิดาได้ว่าเป็นไปในทิศทางใดและมีการเข้าใช้งานเว็บไซต์ใดบ้าง



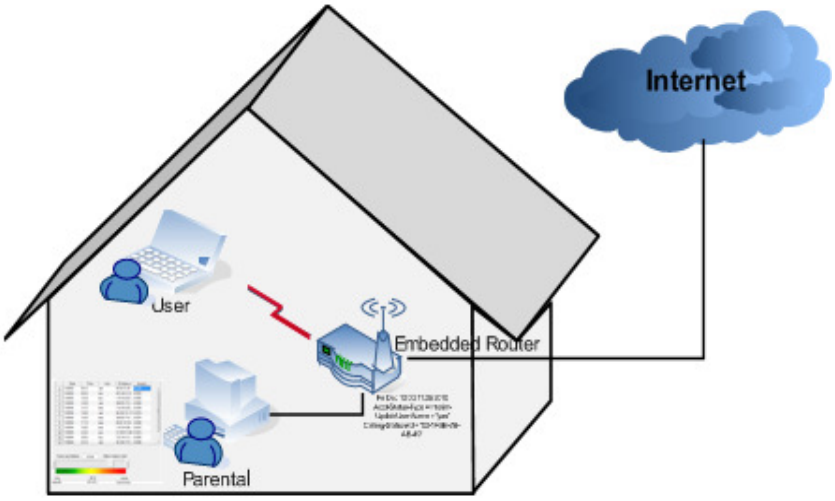
รูปที่ 1.1 การป้องกันการเข้าใช้งานโดยใช้ซอฟต์แวร์ติดตั้งบนเครื่องผู้ใช้งาน

อย่างไรก็ตาม หากมองถึงกลไกทำงานเพื่อการเฝ้าตรวจและบันทึกข้อมูลจราจรทางคอมพิวเตอร์ของหน่วยงาน องค์กร/ธุรกิจนั้น มีระบบที่เป็นศูนย์กลางการให้บริการเครือข่ายเพื่อจัดเก็บข้อมูล ซึ่งเป็นรูปแบบแนวทางที่น่าสนใจมากหากจะนำมาประยุกต์ใช้ในบ้านพักอาศัย โดยจากการศึกษาระบบให้บริการที่เป็นศูนย์กลางดังกล่าว พบว่าระบบมีความครอบคลุมในการให้บริการทั้งเครือข่ายสาย ไร้สายและมีระบบป้องกันการเข้าถึงหรือการแก้ไขข้อมูลได้ และมีศักยภาพที่ควรจะนำไปประยุกต์ใช้สำหรับผู้ปกครอง ให้สามารถติดตาม/แกะรอยหรือควบคุมการเข้าใช้เว็บไซต์อินเตอร์เน็ตที่อาจไม่เหมาะสมของบุตร/ธิดาจากบ้านพักอาศัยได้

อุปสรรคสำคัญที่ทำให้การประยุกต์ใช้ระบบ สำหรับการเฝ้าตรวจและบันทึกข้อมูลจราจรทางคอมพิวเตอร์ในเครือข่ายจากบ้านพักอาศัยไม่อาจทำได้ในลักษณะเดียวกับหน่วยงาน องค์กร/ธุรกิจนั้น เนื่องจากจำเป็นต้องใช้คอมพิวเตอร์จำนวนไม่น้อยกว่า 1 เครื่อง เปิดใช้ตลอดเวลาเพื่อทำหน้าที่ในการจัดเก็บบันทึกข้อมูลจราจรภายในเครือข่ายทั้งหมดและทำให้สิ้นเปลืองพลังงานเกินความจำเป็น การดูแลรักษาทำได้ยาก ดังนั้นจึงควรพิจารณาศึกษาอุปกรณ์ที่อาจจะสามารถทำงานได้ เช่น อุปกรณ์คอมพิวเตอร์แบบฝังตัวควบคุมภายในอุปกรณ์แอกเซสพ้อยน์เราเตอร์ ที่รองรับการให้บริการของเครือข่ายบ้านพัก มาศึกษาเพื่อใช้งานทดแทนเครื่องคอมพิวเตอร์ที่เป็นแม่ข่าย สำหรับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ข้างต้น เนื่องจากในปัจจุบันอุปกรณ์ของผู้ผลิตบางรุ่น เช่น อุปกรณ์รุ่น WRT54GL ของยี่ห้อ Linksys หรือ รุ่น WL500GP ของยี่ห้อ ASUS เป็นต้น ซึ่งเป็นอุปกรณ์ที่สามารถเปลี่ยนซอฟต์แวร์ควบคุมภายในให้กลายเป็นคอมพิวเตอร์แบบฝังตัว (Embedded Computer) โดยมีแพลทฟอร์มที่เป็นลินุกซ์ (Linux) [4] สามารถติดตั้งได้ทันที อย่างไรก็ตามการที่จะทำให้ได้ระบบบันทึกข้อมูลจราจรฯ ดังที่กล่าวมาแล้ว จำเป็นที่จะต้องศึกษาวิจัยเพิ่มเติมในประเด็นสำคัญๆ ต่อไปนี้

- ประเภทและจำนวนของซอฟต์แวร์แบบโอเพ่นซอร์สด้านการจัดการเครือข่าย ที่ควรจะนำมาใช้เพื่อการเฝ้าตรวจและบันทึกข้อมูลจราจร ทำงานภายใต้ข้อจำกัดด้านความเร็วของหน่วยประมวลผลกลาง และขนาดหน่วยความจำภายในระบบคอมพิวเตอร์ฝังตัวของอุปกรณ์แอกเซสพ้อยน์เราเตอร์ (ตัวอย่างเช่น ความเร็ว CPU ที่ 200 MHz และหน่วยความจำ 16 MB ของรุ่น WRT54GL เป็นต้น)
- แนวทางการวิเคราะห์ข้อมูลอย่างชาญฉลาด เพื่อให้สะดวกต่อการวิเคราะห์ข้อมูลของผู้ปกครอง กระจายปริมาณข้อมูลจราจรจัดเก็บอย่างเหมาะสม เพื่อนำไปประมวลผลยังคอมพิวเตอร์เครื่องอื่น ซึ่งรวมไปถึงแนวทางการนำข้อมูลเพื่อวิเคราะห์และตรวจสอบการเข้าใช้เว็บไซต์อินเตอร์เน็ตที่อาจไม่เหมาะสมได้ต่อไป

ปัจจุบัน แม้ว่าจะมีข้อมูลเผยแพร่วิธีการเพิ่มขยายหน่วยความจำให้กับคอมพิวเตอร์แบบฝังตัวของอุปกรณ์เกตเวย์ ทำให้โอกาสที่จะขยายพื้นที่สำหรับเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้รองรับจำนวนครั้งของการใช้งานอินเตอร์เน็ตภายในบ้านพักอาศัยได้อย่างเพียงพอในระดับหนึ่ง แต่ยังไม่พบงานวิจัยเผยแพร่ที่ได้นำอุปกรณ์แอกเซสพ้อยน์เราเตอร์นี้ไปใช้ในการบันทึกข้อมูลจราจรทางคอมพิวเตอร์และวิเคราะห์เพื่อการควบคุมการเข้าใช้เว็บไซต์อินเตอร์เน็ตที่ไม่เหมาะสมภายในบ้านพักอาศัย ดังนั้นหากนำอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่เป็นคอมพิวเตอร์แบบฝังตัวมาจัดทำเป็นระบบบันทึกข้อมูลจราจรทางคอมพิวเตอร์สำหรับบ้านพักอาศัย และมีการวิเคราะห์ข้อมูลย้อนหลังในการใช้งานอินเทอร์เน็ตที่สะดวกสำหรับการตรวจสอบความเหมาะสมจะทำให้มีผลดีต่อผู้ปกครองหรือผู้ดูแลสำหรับบ้านพักอาศัย ดังแสดงในรูปที่ 1.2



รูปที่ 1.2 แนวคิดระบบจัดเก็บข้อมูลจราจรเครือข่ายในบ้านพักอาศัย

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 ศึกษาคัดเลือกอุปกรณ์แอกเซสพ้อยน์เราเตอร์และออกแบบกลไกการทำงานของซอฟต์แวร์แบบโอเพ่นซอร์ส เพื่อให้มีการเก็บข้อมูลอย่างประหยัดและเหมาะกับทรัพยากรที่มีน้อยของอุปกรณ์

1.2.2 ศึกษาออกแบบและประยุกต์เทคนิควิธีฟัซซีลอจิก สำหรับวิเคราะห์ข้อมูลจราจรที่ได้จากอุปกรณ์เซสพ้อยน์เราเตอร์ เพื่อลดความซ้ำซ้อนจากผู้ใช้ทั่วไป

1.3 ขอบเขตของการวิจัย

1.3.1 การพิจารณาแอกเซสพ้อยน์เราเตอร์ แบบที่ปรับเปลี่ยนเฟิร์มแวร์ได้ พร้อมเกณฑ์การปรับแต่งซอฟต์แวร์ในการจัดทำระบบ

1.3.2 แนวทางการกรองข้อมูลที่จำเป็นในการวิเคราะห์ระบบ เพื่อให้ลดปริมาณของข้อมูลที่เกินความจำเป็น

1.3.3 การกำหนดค่าความเป็นสมาชิกของอินพุตและกำหนดกฎในการวิเคราะห์ข้อมูล

1.3.4 เสนอแนวทางของซอฟต์แวร์เพื่อการใช้งานในรูปแบบกราฟิกที่เข้าใจง่าย

1.4 ขั้นตอนและวิธีดำเนินการวิจัย

1.4.1 รวบรวมข้อมูล ศึกษาเปรียบเทียบพิจารณาแนวทางการคัดเลือกอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่สามารถปรับเปลี่ยนเฟิร์มแวร์ได้

1.4.2 ศึกษาซอฟต์แวร์โอเพ่นซอร์สของการจัดทำระบบวิเคราะห์ข้อมูลบนอุปกรณ์เครือข่าย

1.4.3 ศึกษาการออกแบบเทคนิควิธีฟัซซีลอจิกในการวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์

1.4.4 ทดสอบระบบการวิเคราะห์ข้อมูลแบบชาญฉลาด

1.4.5 พัฒนาแนวทางและรูปแบบของซอฟต์แวร์เบื้องต้น

1.4.6 จัดทำวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 แนวทางการคัดเลือกอุปกรณ์แอกเซสพ้อยน์เราเตอร์และปรับแต่งซอฟต์แวร์แบบโอเพ่นซอร์ส อย่างเหมาะสมต่อการเฝ้าตรวจข้อมูลจราจรเครือข่าย

1.5.2 แนวทางซอฟต์แวร์รายงานเชิงวิเคราะห์แบบชาญฉลาด ซึ่งเป็นกลไกหนึ่งที่ตรวจสอบการเข้าใช้เว็บไซต์อินเทอร์เน็ตที่ไม่เหมาะสมภายในบ้านพักอาศัย

1.5.3 การใช้ประโยชน์จากอุปกรณ์แอกเซสพ้อยน์เราเตอร์ แทนเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเก็บข้อมูลจราจรเครือข่าย ภายในบ้านพักอาศัย

1.5.4 เป็นแนวทางการพัฒนาต่อยอด เพื่อขยายระบบสำหรับจัดเก็บข้อมูลจราจรจำนวนมากขึ้น จากหลายแห่งแบบรวมศูนย์

1.6 โครงสร้างของวิทยานิพนธ์

วิทยานิพนธ์นี้ได้จัดวางโครงสร้างเป็นบทๆ รวมทั้งสิ้นเป็นจำนวน 5 บท ดังต่อไปนี้

- บทที่ 1 เป็นบทนำเริ่มต้นกล่าวถึงความสำคัญ ที่มาของปัญหาของการวิจัยที่จะดำเนินการรวมถึงวัตถุประสงค์ และขอบเขตของวิทยานิพนธ์
- บทที่ 2 เป็นการอธิบายทฤษฎีและหลักการที่เกี่ยวข้อง โดยเริ่มต้นจากการอธิบายข้อมูลจราจรทางคอมพิวเตอร์และระบบเฝ้าตรวจข้อมูลจราจรเครือข่าย กลไกการยืนยันตัวตนและความปลอดภัย อุปกรณ์คอมพิวเตอร์แบบฝังตัว และแนวคิดในการวิเคราะห์ข้อมูลด้วยฟัซซีลอจิก จากนั้นจึงเป็นการทบทวนวรรณกรรมที่เกี่ยวข้องกับงานวิจัย
- บทที่ 3 เป็นการอธิบายการออกแบบและพัฒนาระบบ ซึ่งกล่าวถึงแนวความคิดและสถาปัตยกรรมระบบ อธิบายแนวทางการพิจารนาเลือกอุปกรณ์และซอฟแวร์ที่จำเป็นพร้อมสรุปผลการเลือกใช้ และรูปแบบของข้อมูลที่ต้องการ เพื่อนำไปวิเคราะห์ต่อไป
- บทที่ 4 เป็นการอธิบายแนวคิดการประยุกต์ใช้ฟัซซีลอจิก และออกแบบค่าความสัมพันธ์ของอินพุตตลอดจนกฎเกณฑ์เพื่อการวิเคราะห์ผล โดยใช้โปรแกรมภาษาจาวา และนำเสนอแนวคิดของโปรแกรมสารสนเทศในการวิเคราะห์
- บทที่ 5 เป็นบทสรุปการวิจัยเพื่อวิทยานิพนธ์

บทที่ 2

ทฤษฎี และหลักการที่เกี่ยวข้อง

2.1 บทนำต้นเรื่อง

เป็นการกล่าวนำความรู้พื้นฐานของเทคโนโลยีที่เกี่ยวข้องกับประเด็นปัญหาของงานวิจัยในวิทยานิพนธ์นี้ โดยแบ่งเนื้อหาออกเป็นส่วนๆ เริ่มจากการแนะนำข้อมูลจราจรทางคอมพิวเตอร์และระบบเฝ้าตรวจข้อมูลจราจรเครือข่ายในปัจจุบัน ระบบป้องกันและตรวจสอบสิทธิการเข้าถึงเครือข่าย จากนั้นเป็นการแนะนำคอมพิวเตอร์แบบฝังตัวภายในแอกเซสพ้อยน์เราเตอร์และแนวคิดหลักการวิเคราะห์ข้อมูลด้วยเทคนิควิธีฟัซซีลอจิก ในส่วนสุดท้ายเป็นรายละเอียดของงานวิจัยที่เกี่ยวข้องในเรื่องของแนวทางการพัฒนาระบบจัดเก็บข้อมูล และแนวทางของงานวิจัยที่ใช้ฟัซซีลอจิก

2.2 เทคโนโลยีที่เกี่ยวข้อง

2.2.1 ข้อมูลจราจรทางคอมพิวเตอร์

ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลของผู้ใช้บริการไม่ว่าจะเป็นแหล่งกำเนิด ต้นทาง ปลายทาง วันที่ ปริมาณ เวลา ระยะเวลา เส้นทาง ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น [1] ซึ่งความสำคัญของข้อมูลจราจรทางคอมพิวเตอร์นั้นสามารถบอกข้อมูลต่างๆ ของผู้ใช้งานภายใต้การให้บริการและตรวจสอบการใช้งานได้หากมีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ โดยผู้ให้บริการนั้นต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เสมอ

สาเหตุที่ต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ เพื่อความปลอดภัยของข้อมูลในระบบและระบบที่ดีควรมีการจัดเก็บข้อมูลอย่างเป็นระบบและมีคุณภาพ ทั้งยังสามารถตรวจสอบความบกพร่องของระบบเพื่อให้มั่นใจว่าข้อมูลต่างๆ สามารถทำงานได้อย่างมีประสิทธิภาพอยู่เสมออีกทั้งเป็นการปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่กำหนดให้มีการจัดเก็บบันทึกข้อมูลจราจรเครือข่ายคอมพิวเตอร์เพื่อการตรวจสอบย้อนหลังได้และหากไม่ปฏิบัติตามจะต้องรับโทษทางกฎหมาย เพื่อใช้ข้อมูลที่ได้มาเป็นหลักฐานให้สามารถติดตามหรือแกะรอยผู้กระทำความผิดมาดำเนินคดีต่อไป ซึ่งยกตัวอย่างรูปแบบของข้อมูลจราจรเครือข่ายทางคอมพิวเตอร์ ดังแสดงในรูปที่ 2.1 ซึ่งข้อมูลจราจรดังกล่าวมีข้อมูล เดือน วัน เวลา อินพุทและเอาท์พุตที่ใช้ เครื่องต้นทาง/ปลายทางของไอพีแอดเดรสที่ใช้งาน หมายเลขไอดี โพรโตคอลสื่อสาร เป็นต้น

Nov 5	16:53:12	IN=br-wifi	OUT=eth0.1	SRC=192.168.182.5	DST=96.17.242.110	ID=4625	PROTO=TCP	STP=2618	DTP=80
Nov 6	20:55:27	IN=br-wifi	OUT=eth0.1	SRC=192.168.182.3	DST=110.164.252.222	ID=467	PROTO=UDP	STP=1025	DTP=53
Nov 7	21:30:27	IN=br-wifi	OUT=eth0.1	SRC=192.168.182.9	DST=203.153.50.16	ID=1022	PROTO=TCP	STP=1112	DTP=443

รูปที่ 2.1 ตัวอย่างข้อมูลจราจรทางคอมพิวเตอร์

จากการศึกษาความสำคัญข้อมูลจราจรเครือข่ายดังที่ได้กล่าวมาข้างต้นนั้น พบว่ามีรูปแบบของข้อมูลจราจรเครือข่ายมีความน่าสนใจมากในการนำมาประยุกต์ใช้ในงานวิจัยนี้ โดยจะเลือกใช้เฉพาะข้อมูลที่จำเป็นสำหรับการนำมาใช้ประโยชน์ในการวิเคราะห์การเข้าใช้งานภายในบ้านพักอาศัยเท่านั้น เช่น ข้อมูลผู้ใช้งาน วัน เวลา หมายเลขต้นทางหรือปลายทางที่ใช้ เป็นต้น ซึ่งรายละเอียดของแหล่งที่มาของข้อมูลจราจรจะกล่าวในหัวข้อสถาปัตยกรรมระบบเฝ้าตรวจข้อมูลจราจรเครือข่ายต่อไป

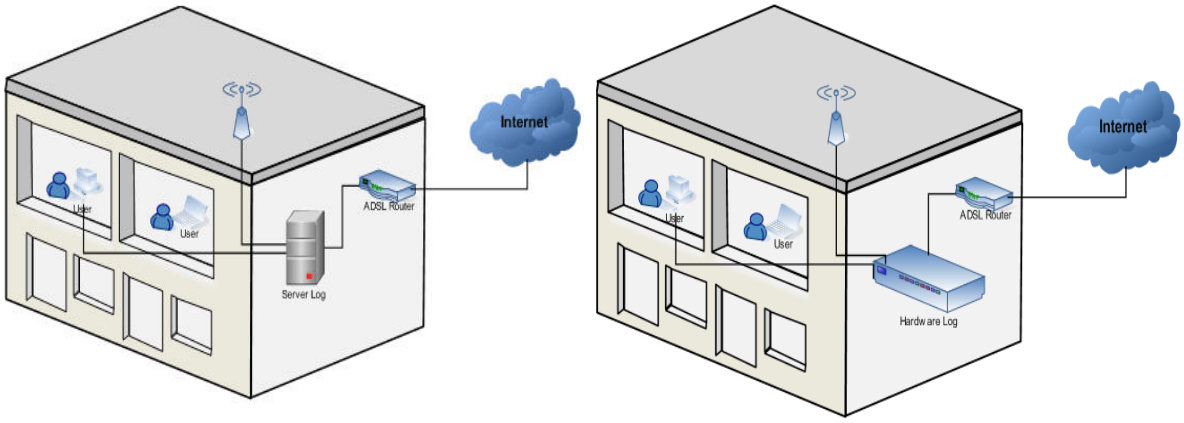
2.2.2 ระบบเฝ้าตรวจข้อมูลจราจรเครือข่าย

ระบบเฝ้าตรวจข้อมูลจราจรเครือข่าย หมายถึง ระบบที่มีศูนย์กลางการให้บริการเครือข่ายไม่ว่าจะเป็นหน่วยงาน องค์กร/ธุรกิจต่างๆ ที่มีหน้าที่ในการจัดเก็บบันทึกข้อมูลจราจรเครือข่ายทางคอมพิวเตอร์ โดยมีรูปแบบของข้อมูลจราจรเพื่อตรวจสอบข้อมูลย้อนหลัง ในรูปแบบต่างๆ ที่ได้กล่าวในข้อที่ผ่านมาแล้ว จากการศึกษาระบบเฝ้าตรวจข้อมูลจราจรเครือข่ายที่สามารถบันทึกข้อมูลจราจรเพื่อให้ได้รูปแบบข้อมูลที่ต้องการนั้น พบแนวทางเชิงสถาปัตยกรรมในปัจจุบันที่สามารถรองรับข้อมูลจราจรในลักษณะเดียวกันกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งสามารถจำแนกออกได้เป็น 2 ลักษณะที่นิยมใช้ในปัจจุบัน ดังต่อไปนี้

2.2.2.1 วิธีการติดตั้งบนเครื่องแม่ข่าย (Server-based Approach) สำหรับให้บริการในการจัดเก็บข้อมูลจราจรเครือข่าย [5] ภายในหน่วยงานหรือองค์กร/ธุรกิจต่างๆ โดยเป็นการติดตั้งซอฟต์แวร์บนเครื่องคอมพิวเตอร์ที่เป็นเครื่องแม่ข่าย ทำหน้าที่หลักในการให้บริการเก็บข้อมูลและเชื่อมต่อเครื่องลูกข่ายเข้าสู่เครือข่ายหลักเพื่อใช้งานร่วมกับอุปกรณ์ภายในเครือข่าย ให้สามารถออกสู่เครือข่ายอินเทอร์เน็ตต่อไป โดยใช้ซอฟต์แวร์โอเพ่นซอร์สที่นิยมใช้กันในการพัฒนาระบบ ยกตัวอย่างเช่น Plawan Central Log, CentOS Central Log, Ubuntu ที่สามารถติดตั้งซอฟต์แวร์เพิ่มเติมให้เป็นเซิร์ฟเวอร์ที่ให้บริการในการจัดเก็บข้อมูลจราจรเครือข่ายได้ ดังแสดงในรูปที่ 2.2 (ก)

2.2.2.2 วิธีการของอุปกรณ์เน็ตเวิร์ค(Network-based Approach) ซึ่งเป็นอุปกรณ์สำเร็จรูปเชิงพาณิชย์สำหรับให้บริการในการจัดเก็บข้อมูลจราจรเครือข่าย [6] ที่มีการทำงานในลักษณะเดียวกับการติดตั้งบนเครื่องแม่ข่ายที่ได้กล่าวไปในข้อที่ 2.2.2.1 แต่เป็นอุปกรณ์เครือข่ายสำเร็จรูปแทนเครื่องแม่ข่ายที่พัฒนาขึ้นเอง เพื่อให้บริการเครือข่ายสำหรับจัดเก็บข้อมูลจราจร ยกตัวอย่างเช่น SRAN LOG [6] และ Sniff-Log [7] เป็นต้น ซึ่งอุปกรณ์ถูกพัฒนาขึ้นเพื่อรองรับระเบียบพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 ในการควบคุมการใช้งานและติดตามผู้การกระทำความผิดสำหรับใช้ในหน่วยงานหรือองค์กรที่ต้องการความสะดวกต่อการ

ดูแลและง่ายขึ้นสำหรับการใช้งานเมื่อเทียบกับระบบที่เป็นเครื่องคอมพิวเตอร์แม่ข่ายที่ได้กล่าวมา แสดงดังรูปที่ 2.2 (ข) และตารางเปรียบเทียบที่ 2.1



รูปที่ 2.2 วิธีการติดตั้งบนเครื่องแม่ข่าย (ก) และวิธีการการใช้อุปกรณ์เน็ตเวิร์ค (ข)

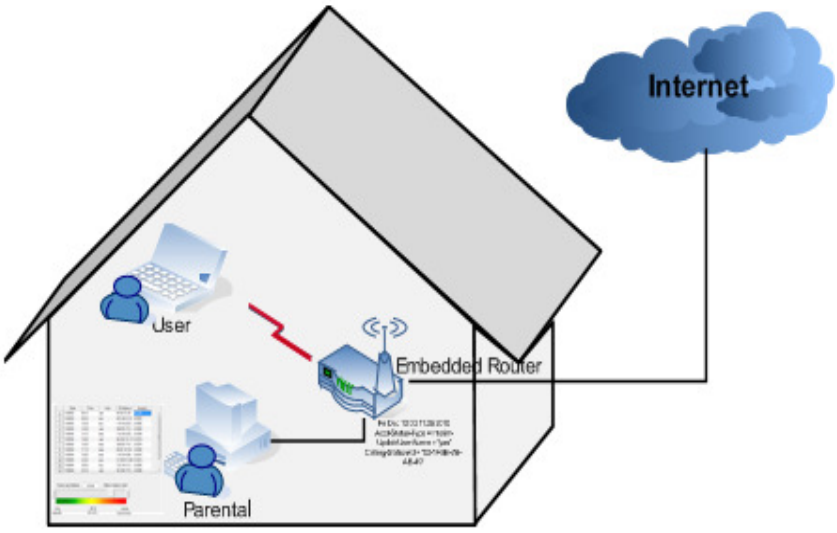
ตารางที่ 2.1 เปรียบเทียบข้อดี-ข้อเสีย ของสถาปัตยกรรมทั้งสองระบบ

วิธีการ	ข้อดี	ข้อเสีย
1) การติดตั้งเครื่องแม่ข่าย (Server-based Approach)	▪ ดำเนินการเฉพาะที่เซิร์ฟเวอร์ ▪ มีข้อมูลการติดตั้งเผยแพร่มาก	▪ การใช้งานหรือแก้ไข/เปลี่ยนแปลงต้องมีทักษะสูง ▪ จำเป็นต้องติดตั้งซอฟต์แวร์จำนวนมากเพื่อทำงานร่วมกัน
2) อุปกรณ์สำเร็จรูปเชิงพาณิชย์ (Network-based Approach)	▪ ดำเนินการเฉพาะที่อุปกรณ์ ▪ ง่ายต่อการติดตั้ง/บำรุงรักษาเนื่องจากเป็นระบบปิดที่สมบูรณ์ในตัวเอง	▪ ราคาแพง ▪ ไม่มีข้อมูลการติดตั้ง/แก้ไขเผยแพร่ ▪ เป็นระบบปิดเชิงพาณิชย์

หากพิจารณาเปรียบเทียบข้อมูลทั้งสองแนวทางข้างต้นดังที่กล่าวมาแล้วนั้น สำหรับนำมาจัดทำเป็นระบบบันทึกข้อมูลจราจรเครือข่าย เพื่อตรวจสอบการใช้งานเว็บไซต์ที่ไม่เหมาะสมแล้ว พบว่าแนวทางการติดตั้งเครื่องแม่ข่าย มีเหมาะสมในการศึกษา เพื่อหาแนวทางในการพัฒนาระบบภายในบ้านพักอาศัย เนื่องจากมีข้อดีที่ใช้ซอฟต์แวร์โอเพ่นซอร์สทั้งหมด ทำให้ประหยัดค่าใช้จ่าย การติดตั้งและใช้งานระบบมีข้อมูลเผยแพร่มาก โดยดำเนินการเฉพาะที่เครื่องแม่ข่ายเท่านั้น ซึ่งสามารถทำงานได้โดยไม่จำเป็นต้องมีการเพิ่มเติม/แก้ไขที่เครื่องคอมพิวเตอร์อื่นๆ ทำให้ผู้ใช้งานไม่สามารถ

ปรับปรุงหรือแก้ไขข้อมูลของระบบได้ โดยมีระบบพิสูจน์ตัวตนที่สามารถกำหนดสิทธิและบันทึกการใช้งานแบบ AAA (Authentication, Authorization and Accounting) ซึ่งจะกล่าวในหัวข้อระบบป้องกันและตรวจสอบสิทธิการเข้าถึงเครือข่ายต่อไป อย่างไรก็ตามข้อเสียสำคัญของระบบนี้อยู่ที่การต้องใช้คอมพิวเตอร์จำนวน 1 เครื่อง เพื่อทำหน้าที่เป็นเซิร์ฟเวอร์ประมวลผลการจัดเก็บข้อมูลจราจรเครือข่าย [5] จึงต้องเปิดใช้งานไว้ตลอดเวลา ทำให้สิ้นเปลืองทรัพยากรเกินความจำเป็นสำหรับบ้านพักอาศัย ที่ไม่ต้องการข้อมูลจราจรทางคอมพิวเตอร์มากนัก

งานวิจัยนี้จึงมุ่งที่จะหาแนวทางในการแก้ไขข้อด้อยของระบบที่เป็นเครื่องแม่ข่าย โดยการที่นำมาประยุกต์ใช้กับอุปกรณ์แอกเซสพ้อยน์เราเตอร์ ที่มีความสามารถในการปรับเปลี่ยนแพลทฟอร์มที่เป็นโอเพ่นซอร์สและการแก้ไขคอนฟิกค่าการใช้งาน [8] ให้สามารถจัดเก็บข้อมูลและสามารถตรวจสอบการเข้าใช้งานเครือข่ายที่อาจไม่เหมาะสมได้ แต่ด้วยข้อจำกัดของหน่วยความจำของตัวอุปกรณ์ที่มีน้อย จึงจำเป็นต้องหาเทคนิคกลไกเพื่อติดตั้งซอฟต์แวร์ในการให้บริการอินเทอร์เน็ตภายในบ้านพักอาศัย เพื่อให้มีความสามารถในลักษณะเดียวกันกับเครื่องคอมพิวเตอร์ที่เป็นเครื่องแม่ข่าย (Server-based Approach) ช่วยให้ประหยัดค่าใช้จ่ายของผู้ใช้งานอย่างเห็นได้ชัดและผู้ใช้ไม่จำเป็นต้องมีทักษะด้านการใช้งานคอมพิวเตอร์สูงมากนัก อีกทั้งง่ายต่อการนำไปใช้งานและการบำรุงรักษาเพราะอุปกรณ์ที่ใช้เป็นลักษณะของอุปกรณ์คอมพิวเตอร์แบบฝังตัวที่สามารถรีเซตการทำงานใหม่ได้ง่าย ดังแสดงรูปที่ 2.3



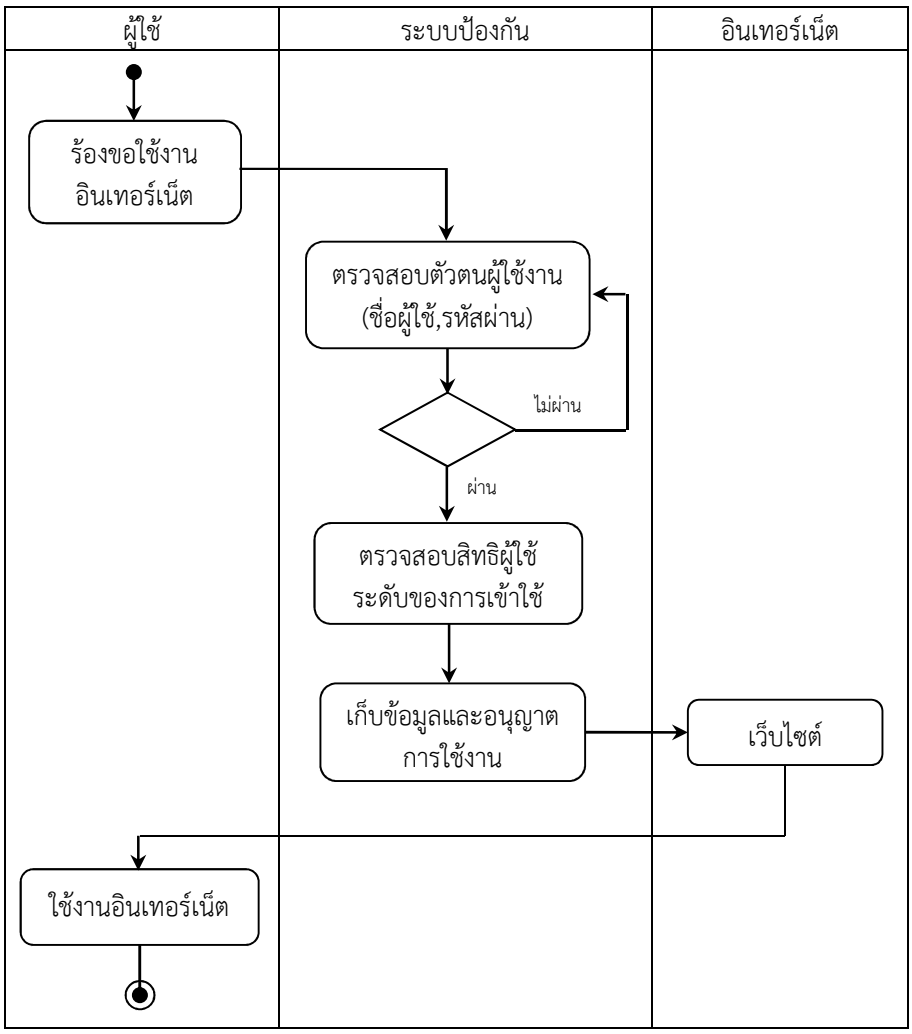
รูปที่ 2.3 แนวทางการนำอุปกรณ์แอกเซสพ้อยน์เราเตอร์มาใช้ในบ้านพักอาศัย

2.2.3 ระบบป้องกันและตรวจสอบสิทธิการเข้าถึงเครือข่าย

การเข้าใช้งานเครือข่ายจำเป็นต้องมีระบบความปลอดภัยซึ่งจุดประสงค์หลักของความปลอดภัยทางข้อมูลและการเข้าใช้งานเครือข่ายภายในองค์กร โดยการควบคุมความปลอดภัยถือเป็นองค์ประกอบที่สำคัญ ซึ่งส่วนหนึ่งของความมั่นคงปลอดภัยจัดเป็นการกำหนดการควบคุม ทั้งบุคคลที่เข้าสู่ระบบและข้อมูลภายใน เพื่อกระทำการใดได้บ้างอนุญาตตามระดับความสำคัญของข้อมูลรวมไปถึงการจัดเก็บพฤติกรรมการใช้งานของบุคคลในระบบทั้งหมด เพื่อการตรวจสอบข้อมูลและติดตามการเข้าใช้งานได้

การป้องกันและตรวจสอบสิทธิการเข้าใช้งาน เป็นเทคโนโลยีมาตรฐานที่นิยมใช้กันมากในองค์กรเพื่อป้องกันการเข้าถึงเครือข่ายในการให้บริการ โดยใช้ RADIUS (Remote Access Dial-Up User Service) [9] ซึ่ง RADIUS จะมีโครงสร้างของชื่อผู้ใช้และรหัสผ่านสำหรับตรวจสอบความถูกต้องขณะที่มีการตรวจสอบสิทธ์ ถูกสร้างขึ้นมาเพื่อใช้ในกระบวนการ AAA (Authentication, Authorization and Accounting) เพื่อควบคุมการเข้าใช้ (Access control) โดยมีกระบวนการทำงานของระบบ แสดงดังรูปที่ 2.4 เมื่อมีการเชื่อมต่อเครื่องลูกข่ายเพื่อขอใช้งานอินเทอร์เน็ต ซึ่งขั้นตอนแรกของการขอใช้งานอินเทอร์เน็ตจะมีการปิดกั้นการเข้าใช้งานของระบบ เพื่อให้เข้าสู่กระบวนการ Authentication สำหรับตรวจสอบตัวตนการเข้าใช้งาน โดยเมื่อผู้ใช้งานเครื่องลูกข่ายส่งข้อมูลยืนยันตัวตน อาจเป็นชื่อและรหัสผ่านของผู้ใช้ หรือข้อมูลอื่นๆ แล้วแต่วิธีการพิสูจน์ตัวตนที่ผู้ดูแลเครือข่ายกำหนด เข้ามายังระบบจัดการเครือข่ายเพื่อยืนยันตัวตนแล้ว จะเข้าสู่กระบวนการ Authorization เพื่อตรวจสอบสิทธิการเข้าใช้งานในระดับใด และจะเข้าสู่กระบวนการ Accounting เพื่อเก็บข้อมูลการเข้าใช้งานของเครื่องลูกข่ายผู้ใช้งาน และจะอนุญาตให้เครื่องลูกข่ายสามารถใช้งานอินเทอร์เน็ตได้ แต่หากเป็นผู้ใช้ที่ไม่มีสิทธิใช้งานเครือข่ายระบบจะปิดกันการใช้งานไม่ให้เครื่องลูกข่ายสามารถใช้งานอินเทอร์เน็ตได้จนกว่าจะมีการพิสูจน์ตัวตนถูกต้อง

ดังนั้นส่วนสำคัญของระบบการป้องกันและตรวจสอบสิทธิการเข้าเครือข่าย ที่ต้องศึกษาการทำงาน คือ อุปกรณ์/ซอฟต์แวร์จัดการเครือข่ายและเครื่องแม่ข่ายพิสูจน์ตัวตน โดยมุ่งศึกษาการกำหนดให้มีรูปแบบของการเชื่อมต่อในลักษณะเดียวกันกับระบบเครื่องแม่ข่าย ภายใต้อุปกรณ์แอกเซสพ้อยน์เราเตอร์ ซึ่งได้นำแนวทางที่กล่าวในข้างต้นมาใช้กับระบบจัดเก็บข้อมูลจราจรเครือข่ายในบ้านพักอาศัย เพื่อเป็นมาตรฐานของความปลอดภัยในการเข้าใช้งานในกรณีของเครือข่ายไร้สาย



รูปที่ 2.4 การทำงานของระบบจัดการเครือข่ายข่ายเพื่อขอใช้งานอินเทอร์เน็ต

2.2.4 คอมพิวเตอร์แบบฝังตัวภายในอุปกรณ์แอกเซสพ้อยน์เราเตอร์

อุปกรณ์แอกเซสพ้อยน์เราเตอร์ในปัจจุบัน มีหน้าหลักสำหรับให้บริการเชื่อมต่อเครือข่ายอินเตอร์เน็ตไม่ว่าจะเป็น บ้านพักอาศัย โรงแรม หรือองค์กร โดยมีมาตรฐานของความเร็วในการให้บริการที่แตกต่างกัน อุปกรณ์ดังกล่าวสามารถแบ่งออกเป็น 2 แบบ คือ แบบที่ (1) มีความสามารถในการให้บริการด้านต่างๆ โดยรองรับการใช้งานตามค่ามาตรฐานของแต่ละรุ่นเท่านั้น ซึ่งเป็นข้อกำหนดที่เป็นค่าของบริษัทผู้ผลิตกำหนดไว้ และแบบที่ (2) มีความสามารถในลักษณะคล้ายกับแบบที่ 1 แต่ยังมีความสามารถในการปรับเปลี่ยนซอฟต์แวร์/เฟิร์มแวร์ภายในให้กลายเป็นแฟลทฟอร์มที่ต้องการได้ ซึ่งทำหน้าที่เป็นคอมพิวเตอร์แบบฝังตัวภายในอุปกรณ์ โดยในงานวิจัยนี้ได้ศึกษาคอมพิวเตอร์แบบฝังของอุปกรณ์แอกเซสพ้อยน์เราเตอร์ดังกล่าวมาใช้ในการทดลอง โดยอุปกรณ์มีคุณลักษณะพื้นฐานของความสามารถที่แตกต่างกันไปในแต่ละรุ่นหรือยี่ห้อ ยกตัวอย่างเช่น

ยี่ห้อLinksys รุ่น WRT54GL ยี่ห้อ Asus รุ่น WL500GP และยี่ห้อ Netgear รุ่น WGT634U [10] แสดงดังรูปที่ 2.5 เป็นต้น

Linksys WRT54GL Asus WL500GP Netgear WGT634U

รูปที่ 2.5 อุปกรณ์แอกเซสพ้อยน์เราเตอร์

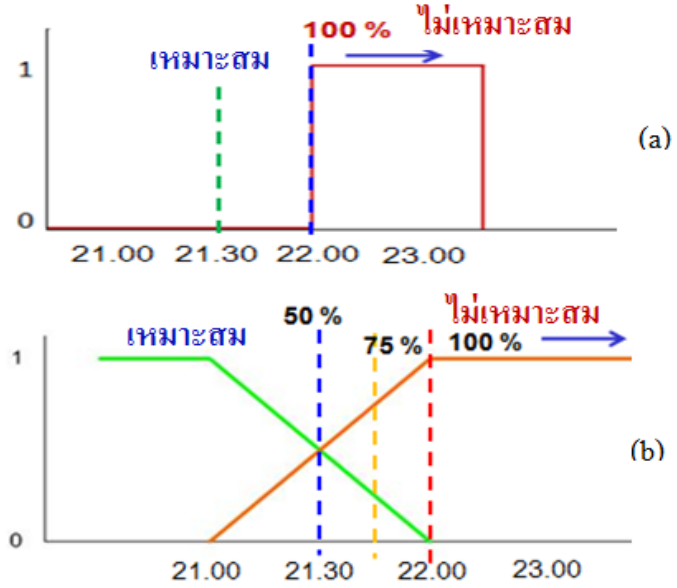
2.2.5 แนวคิดและหลักการวิเคราะห์ข้อมูลด้วยเทคนิควิธีฟัซซีลอจิก

การวิเคราะห์ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ เพื่อตรวจสอบการเข้าใช้งานอินเทอร์เน็ตต่างๆ ล้วนแล้วแต่มีวิธีในการวิเคราะห์ข้อมูลหลายแบบ เพื่อให้ได้ผลของการเข้าใช้งานที่สามารถสรุปและค้นหาเพื่อตรวจสอบข้อมูลย้อนหลังได้ เช่น ข้อมูลผู้ใช้ เวลาที่ใช้งาน จำนวนครั้งที่ใช้งาน เป็นต้น ซึ่งข้อมูลดังกล่าวเป็นข้อมูลพื้นฐานที่ไม่สามารถแยกแยะและตัดสินความเหมาะสมหรือประเมินผลการวิเคราะห์ข้อมูลได้ ซึ่งหากนำข้อมูลมาใช้สำหรับบ้านพักอาศัยจำเป็นต้องเพิ่มระบบที่สามารถคิดวิเคราะห์ข้อมูลจราจรเครือข่ายและตัดสินความเหมาะสมหรือแยกแยะการตัดสินใจได้ โดยจากการศึกษาพบว่ามีระบบที่ช่วยในตัดสินใจการวิเคราะห์ผลในลักษณะข้อมูลที่ซับซ้อนและชาญฉลาด เช่น โครงข่ายประสาทเทียม [11] (Neural Network) ที่มีจุดเด่นด้านการเรียนรู้ข้อมูล และสามารถฝึกฝนการทำงานได้เหมือนสมองของมนุษย์ แต่มีจุดด้อยในด้านการตีความหาเหตุผล ที่ไม่สามารถให้เหตุผลได้ว่าเพราะเหตุใดจึงมีข้อสรุปออกมาดังที่ปรากฏในผลของเอาต์พุต และการตัดสินใจแบบฟัซซีลอจิก [11][12] (Fuzzy Logic) ที่มีโครงสร้างตรรกะอยู่บนพื้นฐานความจริงว่า บนโลกแห่งความจริงไม่ได้มีเฉพาะสิ่งที่แน่นอนเท่านั้น แต่มีหลายสิ่งและหลายเหตุการณ์ที่เกิดขึ้นอาจเป็นสิ่งที่คลุมเครือไม่ใช่ชัดเจนทำให้ต้องใช้องค์ประกอบร่วมกันจากหลายเหตุผลเพื่อตัดสินใจผลข้อมูล เป็นต้น

ในงานวิจัยนี้ได้นำเทคนิควิธีการตัดสินใจแบบฟัซซีลอจิก (Fuzzy Logic) มาช่วยในการวิเคราะห์ข้อมูลจราจรเครือข่ายสำหรับบ้านพักอาศัย เพราะฟัซซีลอจิกมีความสามารถในการคำนวณและตัดสินใจค่าความไม่แน่นอนได้ โดยไม่จำเป็นต้องมีการสอนหรือการเรียนรู้ข้อมูลเพื่อตีความหาเหตุผล

2.2.5.1 พื้นฐานแนวคิดแบบฟัซซีลอจิก

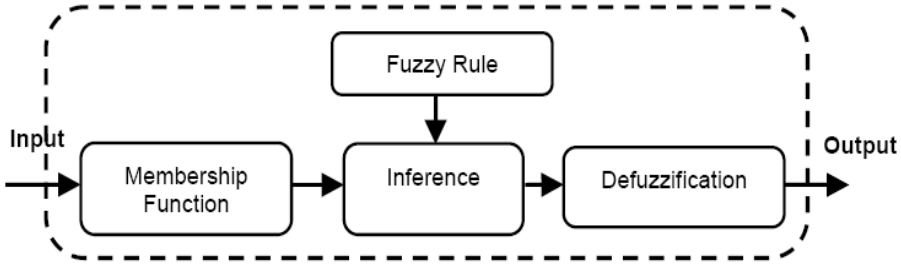
ฟัซซีลอจิก (Fuzzy Logic) เป็นเครื่องมือที่ช่วยในการตัดสินใจภายใต้ความไม่แน่นอนของข้อมูลโดยยอมให้มีความยืดหยุ่นได้ ซึ่งมีลักษณะที่พิเศษกว่าตรรกะแบบจริงเท็จ (Boolean logic) เป็นแนวคิดที่มีการต่อขยายในส่วนของความจริง (Partial True) โดยค่าความจริงจะอยู่ในช่วงระหว่างจริง (Completely True) กับเท็จ (Completely False) มีข้อดีในแง่ของการวิเคราะห์เชิงตรรกะยังใช้วิธีการเดิม คือ ใช้และ (And) หรือ (Or) ถ้าแล้ว (If-Then) ได้เหมือนเดิม ซึ่งสอดคล้องกับตรรกะความคิดของมนุษย์ เพียงแต่ฟัซซีลอจิกจะช่วยในการตัดสินความถูกผิดแบบคลุมเครือ ไม่ใช่ผิดหรือถูกเพียงสองสถานะ แต่จะเป็นดีกรีของความถูกหรือผิด ดังแสดงในรูปที่ 2.6 ซึ่งเป็นเหตุการณ์ที่เกิดขึ้นในธรรมชาติอยู่แล้ว [11] โดยยกตัวอย่างความเหมาะสมของเวลาในการใช้งานอินเทอร์เน็ต เช่น ในรูปที่ 2.6 (a) การเข้าถึงข้อมูลหรือเข้าใช้งานอินเทอร์เน็ตหลังเวลา 22:00 น. ถือว่าไม่เหมาะสม แต่หากเป็นเวลา 21:59 น. ถือว่าเหมาะสม ซึ่งจากรูปจะเห็นได้ว่ามีความแตกต่างของเวลาเพียงแค่นาทีเดียวก็ตัดสินความเหมาะสมไปแล้ว ดังนั้นในงานวิจัยนี้จึงใช้หลักการของวิธีที่ช่วยในการตัดสินใจโดยใช้ฟัซซีลอจิกเข้ามาช่วยในการตัดสินใจความคลุมเครือ ดังแสดงในรูปที่ 2.6 (b) ซึ่งเป็นการเข้าถึงหรือใช้งานอินเทอร์เน็ตหลังเวลา 22:00 น. ถือว่าไม่เหมาะสมมากแต่หากเป็นช่วงเวลา 21:00-22:00 น. ถือว่าไม่เหมาะสมน้อยโดยมีดีกรีของความไม่เหมาะสมเพิ่มขึ้นจนถึงเกณฑ์ความไม่เหมาะสมที่กำหนดไว้ เป็นต้น



รูปที่ 2.6 ตรรกะแบบจริงเท็จและตรรกะแบบคลุมเครือของเวลา

2.2.5.2 ขั้นตอนการประมวลผลแบบตรรกะแบบคลุมเครือ

ฟัซซีลอจิกมีการขั้นตอนการนำเข้าข้อมูลและการประมวลผลแบบตรรกะแบบคลุมเครือมีรูปแบบการทำงานเป็น 4 ส่วน แสดงดังรูปที่ 2.7



รูปที่ 2.7 ขั้นตอนการประมวลผลของฟัซซีลอจิก

- ฟังก์ชันความเป็นสมาชิก (Membership Function) เป็นการกำหนดระดับความเป็นสมาชิกของตัวแปรในเซตของความคลุมเครือแบบต่างๆ และจะนำไปใช้ในการกำหนดกฎในการวิเคราะห์
- กฎการวิเคราะห์ (Fuzzy Rule) เป็นการสร้างความสัมพันธ์ของค่าฟังก์ชันความเป็นสมาชิกแต่ละตัวโดยมีเงื่อนไขต่างๆ เพื่อนำไปใช้ในการวิเคราะห์และแปลความข้อมูล ซึ่งรูปแบบของระบบกฎฟัซซีลอจิก ในการประมาณค่าฟังก์ชันที่ใช้มี 3 ชนิดใหญ่ๆ [11] ได้แก่ แบบที่ 1 คือ รูปแบบ Madani ซึ่งใช้หลักการการรวมผลการอนุมาน (inference) ของกฎ โดยวิธีการซ้อนทับจากกฎหลายๆ ข้อ (superimposition) ซึ่งไม่เป็นแบบวิธีการนำมาบวกกัน จึงเรียกระบบแบบนี้ว่าเป็น Nonadditive Rule Model แบบที่ 2 คือ รูปแบบ Takagi-Sugeno-Kang (TSK) และ แบบที่ 3 คือ รูปแบบ Standard Additive Model (SAM) ทั้งรูปแบบ 2 และ 3 นี้ ใช้การการอนุนามแบบรวมค่าน้ำหนัก (Weighted Sum) จากหลาย ๆ กฎ เพื่อรวมเป็นข้อสรุปสุดท้าย จึงเรียกระบบแบบนี้ว่า Additive Rule Model

  สำหรับในทางปฏิบัติระบบกฎฟัซซีลอจิกแบบ Mamdani เป็นระบบที่มีความนิยมใช้มากที่สุดระบบหนึ่งในทางปฏิบัติและนำมาใช้ในงานวิจัยนี้ เพราะเป็นระบบที่ใช้ตัวแปรภาษาทั้งในข้อตั้งและข้อตามเพื่อจัดเทียบฟังก์ชันจากข้อมูลที่เป็นฟัซซีลอจิกเอาต์พุต โดยการใช้ค่าต่ำสุด (Minimum) สำหรับการเชื่อมประโยคแบบ And และใช้ค่าสูงสุด (Maximum) สำหรับการเชื่อมประโยคแบบ Or เพื่อนำค่าที่ได้ไปคำนวณหาจุดศูนย์ถ่วงค่าน้ำหนักในการวิเคราะห์ผลต่อไป

- การอนุมาน (Inference) เป็นการตรวจสอบหรือการแปลความของค่าความเป็นสมาชิกเพื่อหาผลลัพธ์ของกฎที่ได้ ด้วยการดำเนินการทางตรรกะแบบต่างๆ (เช่น if, and, or) กับฟังก์ชันซีลอจิกที่เกี่ยวข้องโดยการใช้ค่าต่ำสุด (Minimum) สำหรับการเชื่อมประโยคแบบ And และใช้ค่าสูงสุด (Maximum) สำหรับการเชื่อมประโยคแบบ Or เพื่อนำค่าที่ได้ไปคำนวณหาผลลัพธ์ต่อไป
- การคำนวณหาผลลัพธ์ (Defuzzification) เป็นขั้นตอนการสรุปเหตุผลทั้งหมดจากผลลัพธ์ของกฎแต่ละข้อและแปลงข้อมูลให้อยู่ในรูปแบบเดิมเพื่อแสดงผลการตัดสินใจ

$$C = \frac{\sum M\,A(x)x}{\sum M\,A(x)}$$

C เป็นค่าจุดศูนย์ถ่วงของการคำนวณ
$M_{A(x)}$ เป็นฟังก์ชันความเป็นสมาชิก
x เป็นค่าอินพุตที่สนใจ

จากขั้นตอนและวิธีการประมวลผลของฟัซซีลอจิกที่นำมาใช้ในงานวิจัยนี้ มีแนวทางการแบ่งฟังก์ชันความเป็นสมาชิกและกฎในการวิเคราะห์ ตลอดจนการแปลความและการหาผลลัพธ์ของการวิเคราะห์ข้อมูลที่ได้จากตัวอุปกรณ์นั้นจะขอกล่าวรายละเอียดของเนื้อหาในบทที่ 4 เรื่องแนวความคิดการประยุกต์ใช้ฟัซซีลอจิกต่อไป

2.3 งานวิจัยที่เกี่ยวข้อง

2.3.1 แนวทางการประยุกต์ใช้อุปกรณ์แอกเซสพ้อยน์เราเตอร์เพื่อพัฒนาระบบตรวจสอบการเข้าใช้งานอินเตอร์เน็ต

ในวิทยานิพนธ์นี้ได้ศึกษางานวิจัยที่มีความเกี่ยวข้องกับการนำเสนอกลไกทำงานให้รองรับบริการแบบกลุ่มสื่อสารปลอดภัยในการใช้งาน ซึ่งพบการเผยแพร่งานวิจัยดังต่อไปนี้

สัมพันธ์ ลิ้มปิติ [13] ได้นำเสนอระบบจัดการเครือข่ายไร้สายแบบซอฟต์แวร์โอเพ่นซอร์สเพื่อเปรียบเทียบกับระบบแบบเบ็ดเสร็จ ซึ่งระบบที่พัฒนาขึ้นมีความสามารถในการพิสูจน์ตัวตนของผู้ใช้งานแบบ AAA การกำหนดมาตรฐานความปลอดภัย และสิทธิการใช้งานของผู้ใช้ โดยเป็นศูนย์กลางในการให้บริการเครือข่ายและจัดเก็บข้อมูลในองค์กร

ธนัชพัทธ์ กรีธาสันต์ [5] ได้นำเสนอระบบบริหารจัดการค่าใช้จ่ายและเวลาการใช้งานเครือข่ายอินเทอร์เน็ตขนาดกลาง เช่น หอพัก หรืออพาร์ตเม้นต์ โดยพิจารณาเลือกแนวทางการจัดการด้วยโอเพ่นซอร์ส เช่น ซอฟต์แวร์สำหรับการพิสูจน์ตัวตนของผู้ใช้งาน การเฝ้าตรวจเพื่อจับเวลาการใช้งาน การเปลี่ยนทิศทางไปยังตำแหน่งเว็บที่ต้องการขณะที่เริ่มต้นใช้งานอินเทอร์เน็ต และการจัดทำรายงานข้อมูลการเข้าใช้งานเครือข่าย เพื่อตรวจสอบข้อมูลย้อนหลังได้ เป็นต้น

ดังนั้นระบบที่ได้กล่าวดังกล่าวมาข้างต้น มีความน่าสนใจมากที่จะศึกษาขั้นตอนและแนวทางการนำมาใช้ประโยชน์ เพื่อออกแบบและพัฒนาระบบที่มีความสามารถในการให้บริการเข้าถึงและจัดเก็บข้อมูล มาทดลองใช้กับอุปกรณ์ที่มีขนาดเล็กกว่า ภายในระบบคอมพิวเตอร์ฝังตัวของอุปกรณ์แอกเซสพ้อยน์เราเตอร์

2.3.2 แนวทางการนำฟัซซีลอจิกมาใช้

งานวิจัยที่เกี่ยวข้องกับการนำฟัซซีลอจิกมาใช้สำหรับวิเคราะห์ข้อมูลทั่วไปและการวิเคราะห์ข้อมูลด้านเครือข่ายหรือใช้กับงานด้านเน็ตเวิร์คซึ่งพบงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

ทองรัก พัวพรสวรรค์ [14] ได้นำเสนอการใช้ฟัซซีลอจิกควบคุม การแปลงไฟฟ้ากระแสสลับในการเชื่อมต่อกับกริดระบบไฟฟ้า โดยโปรแกรมจำลองแบบทางคณิตศาสตร์ จำลองระบบควบคุมเพื่อเปรียบเทียบกับวิธีการแบบเดิม จากผลการทดลองพบว่าระบบควบคุมทั้งสองให้สัญญาณใกล้เคียงกัน โดยวิธีการนำฟัซซีลอจิกมาใช้มีความผิดเพี้ยนรวมน้อยกว่า 5 % และฟัซซีลอจิกมีข้อได้เปรียบในการปรับเปลี่ยนกฎในการควบคุมที่ง่ายกว่า

สุรกฤษฎ์ นาทธราดล [15] ได้เสนอการประยุกต์ใช้วิธีฟัซซีลอจิกเพื่อวิเคราะห์ความคลุมเครือในการคัดเลือกผู้ส่งมอบของอุตสาหกรรมยานยนต์และอิเล็กทรอนิกส์ เพื่อลดต้นทุนการผลิตและสามารถเพิ่มประสิทธิภาพในการส่งมอบ โดยมีกระบวนการมีการพิจารณาที่หลากหลาย และบางหลักเกณฑ์มีความขัดแย้งกันทำให้เป็นปัญหาในการพิจารณาเลือกผู้ส่งมอบ ซึ่งผลจากการทดลองในส่วนของอุตสาหกรรมยานยนต์ พบว่าค่าน้ำหนักของความสำคัญในการพิจารณา มีความแตกต่างกับอุตสาหกรรมอิเล็กทรอนิกส์ มีการแก้ปัญหาโดยวิธีปรับปรุงข้อมูลอินพุตให้เหมาะสมกับหลักเกณฑ์ตามแต่ละอุตสาหกรรมทำให้เพิ่มมีประสิทธิภาพในการใช้งานและมีความแม่นยำขึ้น

S. Lekcharoen และ C. C. Fung [16] ได้นำเสนอการประยุกต์เทคนิควิธีฟัซซีลอจิก เพื่อจุดประสงค์ในการปรับแต่งข้อมูลจราจรเครือข่ายฯ (Traffic Shaping) สำหรับการบริหารจัดการหน่วยความจำบัฟเฟอร์ จากปริมาณความหนาแน่นของชุดข้อมูลภายในอุปกรณ์เครือข่าย ให้มีการกระจายความหนาแน่นในการเชื่อมต่อได้อย่างราบรื่นโดยไม่สูญเสียประสิทธิภาพของการทำงาน ด้วยการจำลองข้อมูลสำหรับการวิเคราะห์ ซึ่งผลจากการจำลองแบบแสดงให้เห็นว่า อินพุตที่เข้ามามีการจัดคิวเพื่อควมคุมปริมาณของข้อมูลแบ่งออกเป็นเฟรมที่เท่าๆกัน ทำให้ผลลัพธ์ที่ได้มีประสิทธิภาพมากขึ้นและจะขึ้นอยู่กับการให้ค่าความสำคัญของกฎในอินพุตของข้อมูลด้วย

Rahman และคณะ [17] ได้เสนอแนะการนำเทคนิควิธีฟัซซีลอจิกเข้ามาใช้ในการวิเคราะห์แบบจำลองข้อมูลจราจรที่เป็นจริงของเครือข่ายคอมพิวเตอร์ แบบบรอดแบนด์ความเร็วสูง แทนการใช้แบบจำลองทางคณิตศาสตร์ที่สร้างจากสถิติของแพ็กเก็ตข้อมูลด้านต่างๆ เช่น ค่าระยะเวลาในการเดินทางมาถึงของแพ็กเก็ตข้อมูล หรือค่าระยะเวลาไปกลับโดยรวม (Round-trip time) เป็นต้น ซึ่งผลจากการวิเคราะห์ข้อมูลพบว่าใช้เวลาดำเนินการนานกว่ามากเมื่อเทียบกับระบบเดิม จึงเหมาะสมกับการใช้งานในเครือข่ายความเร็วต่ำถึงปานกลางเท่านั้น

ดังนั้นจากตัวอย่างงานวิจัยข้างต้นแสดงให้เห็นว่าฟัซซีลอจิกสามารถเข้ามามีบทบาทเพื่อช่วยในการวิเคราะห์ข้อมูลด้านต่างๆและสามารถวิเคราะห์ข้อมูลด้านการจัดการเครือข่ายคอมพิวเตอร์ได้ ในวิทยานิพนธ์นี้ได้สนใจการนำเทคนิควิธีของฟัซซีลอจิกมาใช้สำหรับการวิเคราะห์ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ เพื่อเฝ้าตรวจพฤติกรรมและติดตามการใช้อินเทอร์เน็ตของบุตร/ธิดาในบ้านพักอาศัย

บทที่ 3

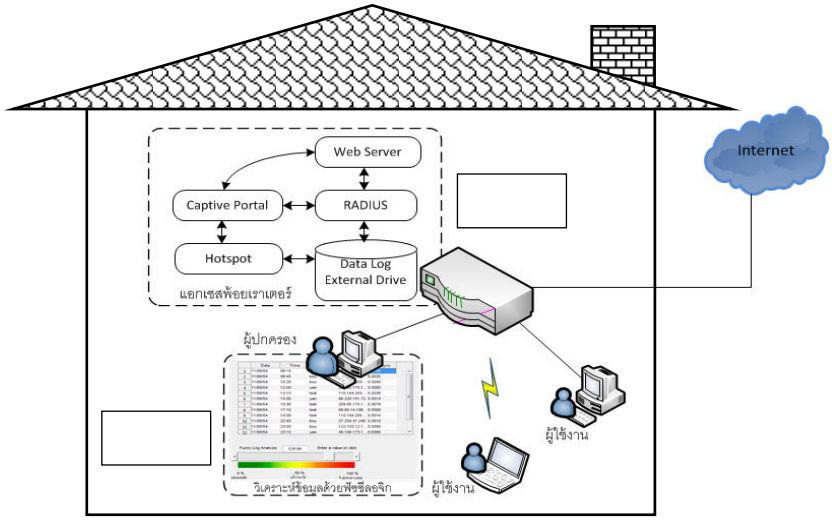
การออกแบบและพัฒนาระบบ

3.1 บทนำต้นเรื่อง

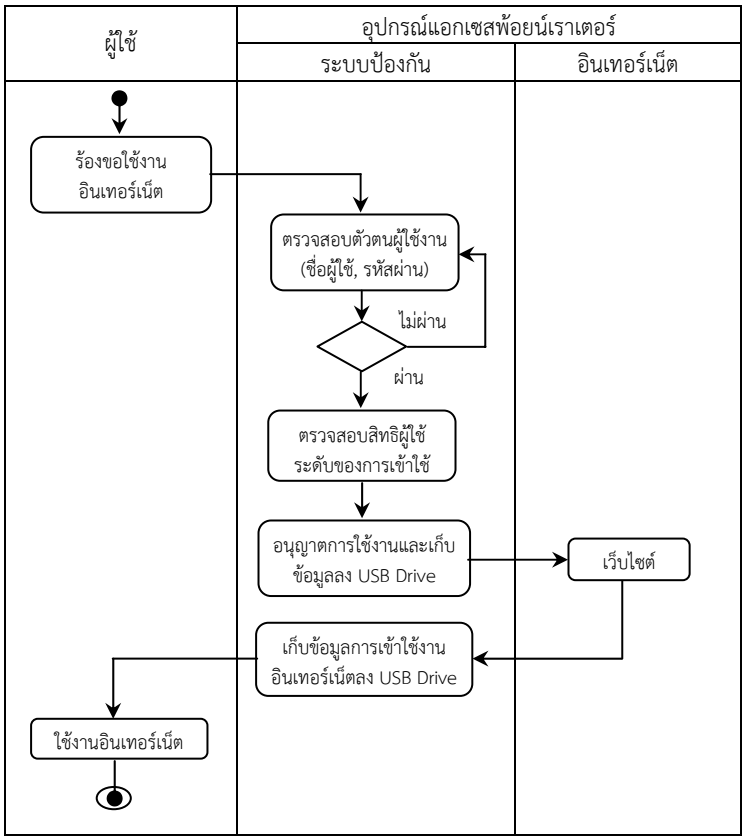
เป็นการกล่าวถึงรายละเอียดกลไกทำงานเพื่อแก้ปัญหาต่างๆ ซึ่งได้อธิบายในบทที่ผ่านมา โดยเริ่มจากอธิบายแนวคิดและสถาปัตยกรรมระบบ จากนั้นจะเป็นแนวทางการพิจารณาเลือกผลิตภัณฑ์คอมพิวเตอร์แบบฝังตัวและซอฟต์แวร์ที่จำเป็นในการจัดเก็บข้อมูลจราจรเครือข่ายพร้อมสรุปผล ในส่วนสุดท้ายเป็นรายละเอียดรูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการเพื่อวิเคราะห์ผลด้วยฟัซซีลอจิก

3.2 แนวความคิดและสถาปัตยกรรมระบบ

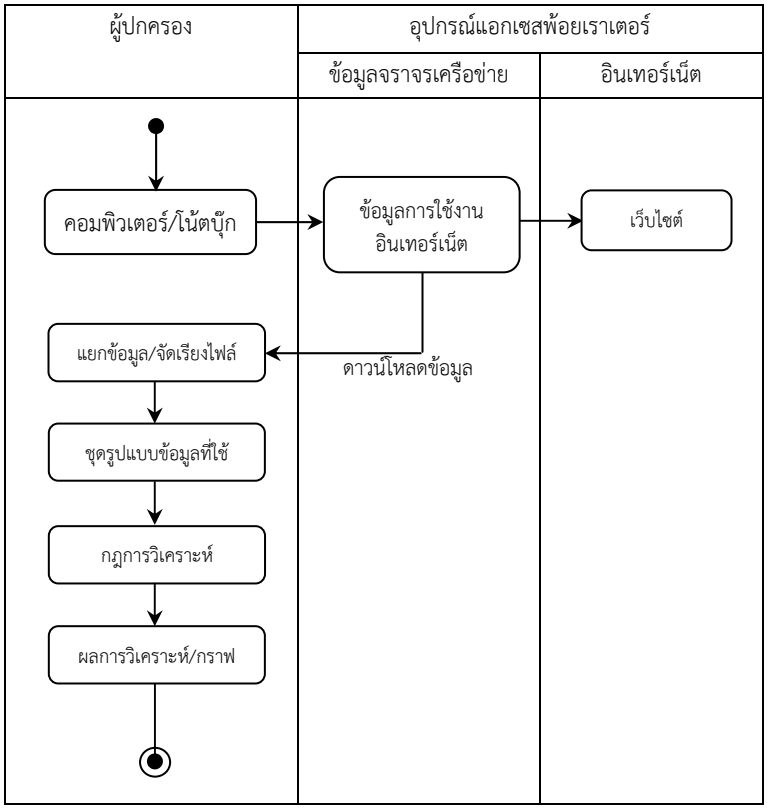
ระบบจัดเก็บข้อมูลจราจรโดยใช้เครื่องคอมพิวเตอร์แม่ข่ายดังที่ได้กล่าวไปในบทที่ผ่านมานั้น เป็นแนวทางที่น่าสนใจมากในการศึกษาเพื่อพัฒนาระบบจัดเก็บข้อมูลจราจรสำหรับบ้านพักอาศัย ในการเฝ้าตรวจและบันทึกข้อมูลการใช้งานอินเทอร์เน็ต ซึ่งระบบดังกล่าวมีหน้าที่หลักในการให้บริการและเชื่อมต่อเครื่องลูกข่ายเข้าสู่เครือข่ายหลัก เพื่อใช้งานในเครือข่ายให้ออกสู่อินเทอร์เน็ตได้ โดยสามารถนำแนวคิดของสถาปัตยกรรมระบบจัดเก็บข้อมูลจราจรที่เป็นเครื่องแม่ข่ายมาประยุกต์ใช้กับอุปกรณ์แอกเซสพ้อยน์เราเตอร์เพื่อจัดการเครือข่ายสายและไร้สายสำหรับบ้านพักอาศัยในการจัดเก็บข้อมูลการใช้งานตามวัตถุประสงค์ของงานวิจัย โดยมีแนวคิดสถาปัตยกรรมของระบบและสถาปัตยกรรมซอฟต์แวร์ของอุปกรณ์ แสดงดังรูปที่3.1ซึ่งสามารถแบ่งออกเป็น 2 ส่วน โดยส่วนที่ 1 เป็นขั้นตอนของสถาปัตยกรรมซอฟต์แวร์ของผู้ใช้งาน ซึ่งมีอุปกรณ์แอกเซสพ้อยน์เราเตอร์เป็นตัวกลางในการให้บริการเครือข่ายภายในประกอบด้วยซอฟต์แวร์ที่ช่วยในการจัดการเครือข่ายมีหน้าที่หลักๆ คือ ให้บริการในรูปแบบเว็บโดยมีระบบพิสูจน์ตัวตน การกำหนดสิทธิและบันทึกการใช้เข้างานในลักษณะเดียวกันกับระบบเครื่องแม่ข่ายและจัดเก็บบันทึกข้อมูลการเข้าใช้งานลงในหน่วยความจำภายนอกแบบ USB ที่เพิ่มเติมสำหรับใช้ในการจัดเก็บข้อมูลจราจรเครือข่าย และในส่วนที่ 2 เป็นขั้นตอนโดยแสดงเป็นโครงสร้างสถาปัตยกรรมการทำงานสามารถแสดงเป็น (Work Flow)ซึ่งเป็นการแบ่งกลุ่ม Activity และกำหนดแต่ละช่องด้วยชื่อ Object ไว้ด้านบน ซึ่งจะช่วยให้การมองภาพของผู้รับผิดชอบได้ชัดเจนขึ้นแผนภาพกิจกรรม ดังแสดงในรูปที่ 3.2 และในรูปที่ 3.3 แสดงการนำเข้าสู่กระบวนการวิเคราะห์ในเครื่องผู้ปกครอง ซึ่งในส่วนนี้จะเป็นการแยกข้อมูลจราจรเครือข่ายที่จำเป็นของข้อมูลจราจรที่ต้องการโดยใช้ช่องว่างข้อมูลแต่ละบรรทัดในการเลือกข้อมูลเฉพาะที่ต้องการซึ่งจะกล่าวรายละเอียดในหัวข้อต่อไป



รูปที่ 3.1แนวความคิดของระบบและสถาปัตยกรรมซอฟต์แวร์ของอุปกรณ์



รูปที่ 3.2 แนวความคิดการทำงานของซอฟต์แวร์สำหรับผู้ใช้งาน



รูปที่ 3.3 แนวความคิดขั้นตอนการวิเคราะห์ข้อมูลสำหรับผู้ปกครอง

3.3 แนวทางการพิจารณาเลือกผลิตภัณฑ์แอกเซสพ้อยน์เราเตอร์

การพิจารณาเลือกผลิตภัณฑ์ของอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่เป็นคอมพิวเตอร์แบบฝังตัว ในการพัฒนาระบบจะต้องคำนึงถึงประสิทธิภาพและความต้องการในการใช้งาน ซึ่งในงานวิจัยนี้ได้พิจารณาโดยใช้องค์ประกอบที่สำคัญคือ สามารถรองรับการปรับเปลี่ยนแพลทฟอร์มแบบโอเพ่นซอร์สราคาถูก และมีคุณลักษณะของตัวอุปกรณ์ที่มีหน่วยประมวลผลกลางไม่น้อยกว่า200 MHz. หน่วยความจำหลัก 16 MB. เพื่อรองรับแพลทฟอร์มและการติดตั้งซอฟต์แวร์สำหรับระบบจัดเก็บข้อมูล ซึ่งจากการศึกษาพบว่าอุปกรณ์คอมพิวเตอร์แบบฝังตัวมีให้เลือกมากมายหลายยี่ห้อมีความสามารถแตกต่างกันตามรุ่นและคุณลักษณะของอุปกรณ์ตามความต้องการของผู้ใช้งาน เช่น มาตรความเร็วของตัวอุปกรณ์และหน่วยประมวลผลการทำงาน เป็นต้นสามารถยกตัวอย่างอุปกรณ์ดังกล่าวที่สามารถรองรับการพัฒนาระบบจัดเก็บข้อมูลจราจรเครือข่ายได้ เช่น อุปกรณ์แอกเซสพ้อยน์ยี่ห้อ Asus รุ่นWL-500GPยี่ห้อ Linksysรุ่น WRT54GLและยี่ห้อNetgear รุ่น WGT634U [10] เป็นต้นและรายละเอียดคุณสมบัติของอุปกรณ์ ดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 รายละเอียดคุณลักษณะของอุปกรณ์

อุปกรณ์	ซีพียู	หน่วยความจำข้อมูล	หน่วยความจำหลัก	หน่วยความจำภายนอก	ราคา (มิ.ย. 54)
1. Linksys รุ่น WRT54GL	200 MHz	4 MB	16 MB	ไม่มี	2,500 .-
3. Netgearรุ่น WGT634U	200 MHz	8 MB	32 MB	USB 2.0	4,290 .-
2. ASUS รุ่น WL500gP V2	240 MHz	8 MB	32 MB	USB 2.0	3,250 .-

3.4 แนวการพิจารณาเลือกซอฟต์แวร์ในการจัดเก็บข้อมูลจราจรเครือข่าย

การศึกษาพิจารณาคัดเลือกซอฟต์แวร์สำหรับอุปกรณ์นั้น จำเป็นต้องศึกษารายละเอียดของระบบปฏิบัติการภายในหรือที่เรียกว่าแพลทฟอร์ม ที่สนับสนุนและรองรับการทำงานของตัวอุปกรณ์ให้สามารถทำงานได้ซึ่งจากการศึกษาพบว่ามีซอฟต์แวร์โอเพ่นซอร์สที่สนับสนุนการทำงานภายในของตัวอุปกรณ์ได้อย่างเหมาะสม และนิยมใช้กันอย่างแพร่หลาย เช่นDD-WRT และ OpenWRT เวอร์ชั่น 0.9 (White Russian) หรือ OpenWRT เวอร์ชั่น 8.09.1 (Kamikaze)เป็นต้นโดยแพลทฟอร์มสามารถทำงานร่วมกับซอฟต์แวร์สนับสนุนต่างๆ เพื่อให้เกิดประโยชน์สำหรับการติดตั้งระบบจัดทำระบบจัดเก็บข้อมูลจราจรเครือข่าย ซึ่งซอฟต์แวร์ที่จำเป็นสำหรับระบบมีความสามารถหรือมีการใช้งานยากง่ายแตกต่างกันจึงควรพิจารณาเลือกใช้อย่างเหมาะสมที่สุดดังแสดงในตารางที่ 3.1 ประกอบด้วยรายละเอียดของแพลทฟอร์มและซอฟต์แวร์สนับสนุนที่จำเป็นสำหรับการติดตั้งระบบ

3.4.1 ซอฟต์แวร์ที่ทำหน้าเป็นเว็บเซิร์ฟเวอร์

เป็นซอฟต์แวร์ที่จำเป็นสำหรับระบบ ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์(Web Server)[18] ในการให้บริการเว็บเพจ เพื่อให้อุปกรณ์สามารถรองรับการอินเตอร์เฟสผ่านเว็บได้เช่น Apache,Lighthttpd และ Busybox เป็นต้น

3.4.2 ซอฟต์แวร์ที่ทำหน้าที่โต้ตอบกับผู้ใช้งาน

เป็นซอฟต์แวร์โต้ตอบผู้ใช้งาน (UI) ทำงานร่วมกับเว็บเซิร์ฟเวอร์ โดยมีรูปแบบเป็นเว็บอินเตอร์เฟสสำหรับการใช้งานและแสดงผลในรูปแบบเว็บเช่น ระบบบริหารเว็บไซต์ CMS, Luci, WebIFเป็นต้น

3.4.3 ซอฟต์แวร์ที่ทำหน้าที่เว็บคอยตรวจสอบการใช้ไอพีแอดเดรส

เป็นซอฟต์แวร์ตรวจจับการใช้งานในเครือข่ายของผู้ขอใช้บริการ (Captive Portal)[19] ซึ่งเป็นศูนย์กลางในการจัดการเครือข่าย โดยมีรูปแบบการLogin เข้าสู่ระบบ มีความสามารถในการให้บริการเครือข่ายเพื่อการพิสูจน์ตัวตนเช่น Nocatsplash, Wifi Dog, Chillispot, Coova Chilli โดยมีรูปแบบลักษณะการทำงานในลักษณะเดียวกัน เป็นต้น

3.4.4 ซอฟต์แวร์ที่ทำหน้าที่ตรวจสอบสิทธิยืนยันตัวตน

เป็นซอฟต์แวร์ตรวจสอบสิทธิและการยืนยันตัวตนเพื่อเข้าใช้งานเครือข่าย (Authentication) [9] โดยมีโครงสร้างชื่อผู้ใช้และรหัสผ่าน เช่น เมื่อป้อนชื่อผู้ใช้และรหัสผ่าน ข้อมูลจะถูกส่งผ่านเครือข่าย เพื่อตรวจสอบให้ถูกต้องก่อน จึงอนุญาตตามสิทธิเฉพาะผู้มีข้อมูลอยู่ในระบบเท่านั้นให้เข้าถึงเครือข่ายได้ เช่น Freeradius, Ldap, Open Radiusเป็นต้น

3.4.5 ซอฟต์แวร์ที่ทำหน้าที่จัดเก็บสถานะ

เป็นซอฟต์แวร์จัดเก็บสถานะของการทำงานภายในตัวระบบต่างๆ และข้อมูลการใช้งานเครือข่าย สามารถเรียกดูข้อมูลย้อนหลังได้ เรียกอีกอย่างหนึ่งว่า Logging [20]เช่น Syslog-ng, Ulogd, Scanlogd เป็นต้น

ตารางที่ 3.2 รายละเอียดประเภทของซอฟต์แวร์ที่รองรับของแพลทฟอร์ม

ซอฟต์แวร์หลัก	**รายละเอียดซอฟต์แวร์ที่รองรับ**	**แพลทฟอร์ม**		
		DD-WRT v24 sp1 (Update Jun 2009) (Size 3.59 MB.)	White Russianrc6 (Update Nov 2006) (Size 1.42MB.)	Kamikaze 8.09.1 (Update Jun 2009) (Size 2.17MB.)
Web Server	Apache	●		●
	Lighthttpd	●	●	●
	Busybox		●	●
UI	Luci			●
	WebIF		●	●
Captive Portal	Chillispot	●	●	●
	Coova Chilli			●
	Nocatsplash		●	●
Authentication	Freeradius	●	●	●
	OpenRadius		●	●
	Ldap	●		
Logging	Syslog-ng	●		●
	Ulogd	●	●	●
	Scanlogd			●

3.5 ผลการศึกษา

3.5.1 การเลือกอุปกรณ์คอมพิวเตอร์แบบฝังตัวและแพลทฟอร์ม

3.5.1.1 จากการศึกษารายละเอียดของอุปกรณ์คอมพิวเตอร์แบบฝังตัวพบว่าการพิจารณาคัดเลือกอุปกรณ์สำหรับนำมาพัฒนาร่วมกับซอฟต์แวร์ที่จำเป็นในการติดตั้งระบบที่สามารถใช้งานได้ โดยในวิทยานิพนธ์นี้เลือกใช้อุปกรณ์ ยี่ห้อAsus รุ่น WL500GP กล่าวคือ การพิจารณาความคุ้มค่าด้านราคาและคุณลักษณะของตัวอุปกรณ์มีความเหมาะสม โดยมีหน่วยประมวลผลกลางขนาด 240 MHz. หน่วยความจำหลัก 32 MB. หน่วยความจำข้อมูล 8 MB. และรองรับหน่วยความจำภายนอกแบบ USB 2.0 ได้ ดังตารางที่ 3.1 โดยไม่ต้องปรับแต่งด้านฮาร์ดแวร์ใดๆและเอื้อให้ผู้ใช้สามารถปรับเปลี่ยนแพลทฟอร์มและซอฟต์แวร์แบบโอเพ่นซอร์ส สำหรับนำมาทดลองประยุกต์ใช้สำหรับการติดตั้งระบบจัดเก็บข้อมูลจราจรเครือข่ายสำหรับบ้านพักอาศัย

3.5.1.2 จากการศึกษารายละเอียดของแพลทฟอร์มแบบโอเพ่นซอร์ส ที่รองรับการทำงานของอุปกรณ์พบว่าแพลทฟอร์มที่เหมาะสมสำหรับนำมาประยุกต์ใช้ OpenWRT เวอร์ชั่น 8.09.1Kamikaze ซึ่งจากการศึกษาและเปรียบเทียบข้อมูลซอฟต์แวร์ที่สนับสนุนต่างๆพบว่ามีความเหมาะสมที่สุดดังตารางที่ 3.2เนื่องจากสามารถรองรับซอฟต์แวร์ที่หลากหลายและมีข้อมูลเผยแพร่มาก และสามารถรองรับการทำงานของซอฟต์แวร์ Coova Chilli [21] ซึ่งเป็นซอฟต์แวร์เวอร์ชั่นใหม่ที่พัฒนาต่อจาก Chillispot ทำให้สามารถง่ายต่อการติดตั้งระบบเมื่อใช้งานร่วมกับ Freeradius เป็นต้น

3.5.2 การเลือกใช้ซอฟต์แวร์ต่างๆ เพื่อการจัดเก็บข้อมูลจราจรเครือข่าย

จากการศึกษารายละเอียดของซอฟต์แวร์พื้นฐานดังที่ได้กล่าวมาในข้อที่ 3.3 นั้น สำหรับการพัฒนาระบบจัดเก็บข้อมูลเครือข่ายในบ้านพักอาศัย สามารถเลือกใช้ซอฟต์แวร์ระบบต่างๆ ซึ่งอธิบายโดยสรุปได้ดังนี้

3.5.2.1 ซอฟต์แวร์เว็บเซิร์ฟเวอร์ (Web Server) เลือกใช้ซอฟต์แวร์ Busybox เนื่องจากเป็นพื้นฐานของแพลทฟอร์ม Kamikaze 8.09.1 อยู่แล้วทำให้สามารถใช้งานได้ทันทีโดยไม่ต้องติดตั้งเพิ่มเติมและมีข้อดีเนื่องจากขนาดของซอร์ฟแวร์เล็กทำให้ประหยัดพื้นที่ในการใช้งานเมื่อเทียบกับ Web Server แบบ Apache และ Lighthttpd เป็นต้น

3.5.2.2 ซอฟต์แวร์ติดต่อผู้ใช้งาน(UI)เลือกใช้ซอฟต์แวร์ WebIF เนื่องจากรองรับการทำงานสำหรับแฟลทฟอร์ม OpenWRTKamikaze 8.09.1และรองรับโมดูลซอฟต์แวร์ที่เลือกใช้เช่น Coova Chilli ทำให้ลดขั้นตอนในการติดตั้งระบบเป็นต้น

3.5.2.3 ซอฟต์แวร์ตรวจสอบการใช้ไอพีแอดเดรส (Captive Portal) ในเครือข่ายของผู้ขอใช้บริการเลือกใช้ซอฟต์แวร์ Coova Chilli เนื่องจากรองรับเวอร์ชั่นใหม่ที่พัฒนามาจาก Chillispot ซึ่งรองรับการทำงานของ User Interface แบบWebIF ทำให้ลดปัญหาในการปรับตั้งค่าการทำงานของระบบ

3.5.2.4 ซอฟต์แวร์ตรวจสอบสิทธิยืนยันตัวตน(RADIUS)เพื่อเข้าใช้งานเครือข่ายเลือกใช้ซอฟต์แวร์ Freeradiusเนื่องจากใช้พื้นที่ในการติดตั้งไม่มากนัก ซึ่งเป็นที่ยอมรับและมีข้อมูลเผยแพร่มากในการติดตั้งระบบมีความสามารถในลักษณะเดียวกันคือการตรวจสอบสิทธิยืนยันตัวตน ในส่วนของขนาดพื้นที่ของซอฟต์แวร์จะไม่แตกต่างกันมากจึงเหมาะสำหรับนำมาใช้ในการพัฒนาระบบ

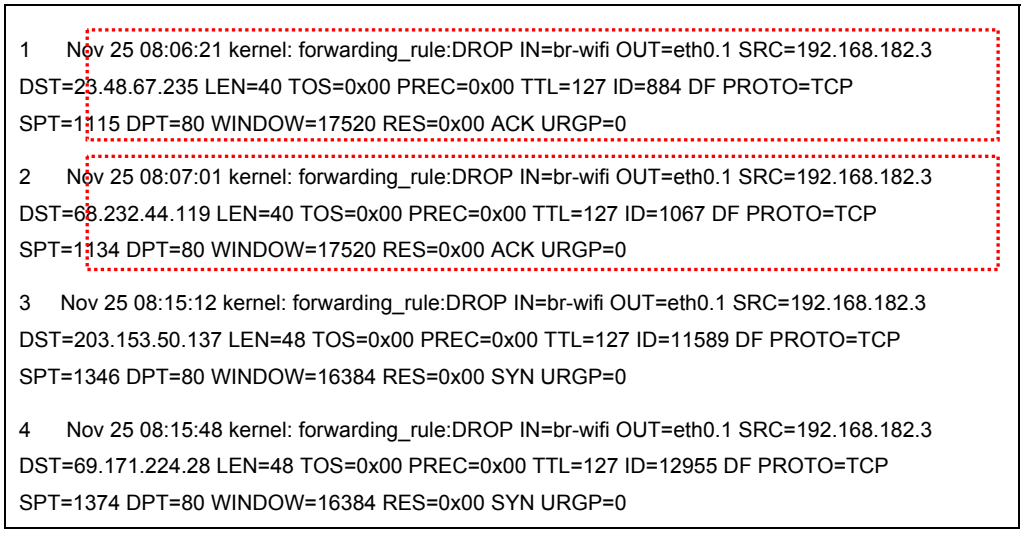
3.5.2.5 ซอฟต์แวร์ที่ทำหน้าที่จัดเก็บสถานการณ์ทำงาน (Logging)และข้อมูลจราจรเครือข่ายเลือกใช้ซอฟต์แวร์ Syslog-ng เนื่องจากเป็นพื้นฐานของแพลทฟอร์มที่ติดตั้งอยู่ภายในแล้วทำให้ไม่ต้องมีการติดตั้งซอฟต์แวร์เพิ่มเติมสามารถเรียกใช้งานได้ทันทีทำให้ช่วยประหยัดพื้นที่ในการติดตั้งภายในตัวอุปกรณ์

ดังนั้นเมื่อเลือกอุปกรณ์และแนวทางของซอฟแวร์สำหรับติดตั้งระบบแล้ว ขั้นตอนต่อไปจะเป็นรายละเอียดของของเทคนิควิธีการติดตั้งลงบนอุปกรณ์และการปรับตั้งค่าการใช้งานต่างๆ เพื่อให้สามารถใช้งานได้ในลักษณะเดียวกับกับเครื่องแม่ข่าย แต่จะขอกล่าวรายละเอียดของขั้นตอนการติดตั้งในส่วนของ ภาคผนวก ข.

3.6 รูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการ

ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ไม่ว่าจะเป็นแหล่งกำเนิด ต้นทาง ปลายทาง หรือข้อมูลอื่นๆที่ได้กล่าวไปในบทที่ผ่านมานั้น สำหรับในส่วนของข้อมูลที่จำเป็นเพื่อประกอบการวิเคราะห์ในบ้านพักอาศัย ซึ่งจะเลือกใช้ชุดรูปแบบข้อมูลที่จำเป็นเท่านั้น ซึ่งรูปแบบของข้อมูลที่จราจรเครือข่ายที่ได้จากการทดลองของตัวอุปกรณ์ มีข้อมูลมากเกินความจำเป็น ดังแสดงในรูปที่ 3.4 ซึ่งในงานวิจัยนี้จึงได้คัดเลือกเฉพาะข้อมูลที่ต้องการเบื้องต้นคือข้อมูลวัน/เวลาการติดต่อของเครือข่ายที่เข้าใช้บริการข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้หมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้ข้อมูลที่บอกถึงหมายเลขปลายทางที่เรียกใช้ โพรโตคอลและพอร์ทสื่อสาร โดยมีการเลือกข้อมูล แสดงดังรูปที่ 3.5 ซึ่งจากรูปข้อมูลภายในกรอบจะเป็นชุดข้อมูลที่ต้องการในการนำไปใช้งาน โดยใช้วิธีการตัดข้อมูลออกเป็นชุดเพื่อให้ได้ข้อมูลที่ต้องการ ดังแสดงในตารางที่ 3.3และสำหรับข้อมูลผู้ใช้งานที่มีรายละเอียดทั้งหมด เช่น วัน/เดือน/ปี ผู้ใช้ ชนิดของการให้บริการ เวลาเริ่มและสิ้นสุดการใช้งาน พอร์ทและไอดีต่างๆ เป็นต้น ซึ่งจะเลือกใช้เฉพาะข้อมูลที่เกี่ยวข้องเช่นกัน คือ ข้อมูลวันเวลาที่เริ่มและสิ้นสุดการใช้งานหมายเลขไอพีแอดเดรสของเครื่องผู้ใช้งาน ตามรายละเอียดดังแสดงดังตารางที่3.4 เพื่อเป็นข้อมูลในการใช้งานร่วมกันกับข้อมูล ในตารางที่ 3.3

เมื่อทำการแยกข้อมูลที่จำเป็นเบื้องต้นแล้ว ในส่วนของการนำข้อมูลไปใช้งานซึ่งจะต้องมีกระบวนการนำข้อมูลที่ได้ทั้งสองมาใช้งานร่วมกัน โดยเข้าสู่กระบวนการรวมข้อมูลทั้งสองตารางเข้าด้วยกัน(Join Table)แสดงดังรูปที่ 3.7 เพื่อให้ได้ข้อมูลที่พร้อมสำหรับนำไปทำการวิเคราะห์ผลตามกระบวนการของฟัซซีลอจิกในบทต่อไปแสดงดังในตารางที่ 3.5



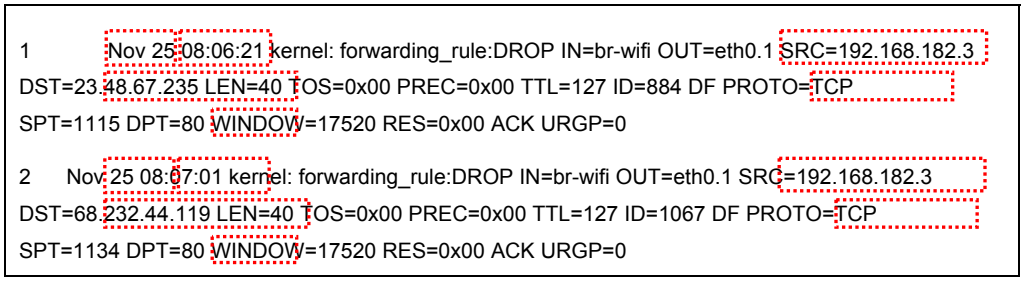
1 Nov 25 08:06:21 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=23.48.67.235 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=884 DF PROTO=TCP SPT=1115 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

2 Nov 25 08:07:01 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=68.232.44.119 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1067 DF PROTO=TCP SPT=1134 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

3 Nov 25 08:15:12 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=203.153.50.137 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=11589 DF PROTO=TCP SPT=1346 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0

4 Nov 25 08:15:48 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=69.171.224.28 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=12955 DF PROTO=TCP SPT=1374 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0

รูปที่ 3.4รูปแบบของข้อมูลจราจรเครือข่ายจากตัวอุปกรณ์



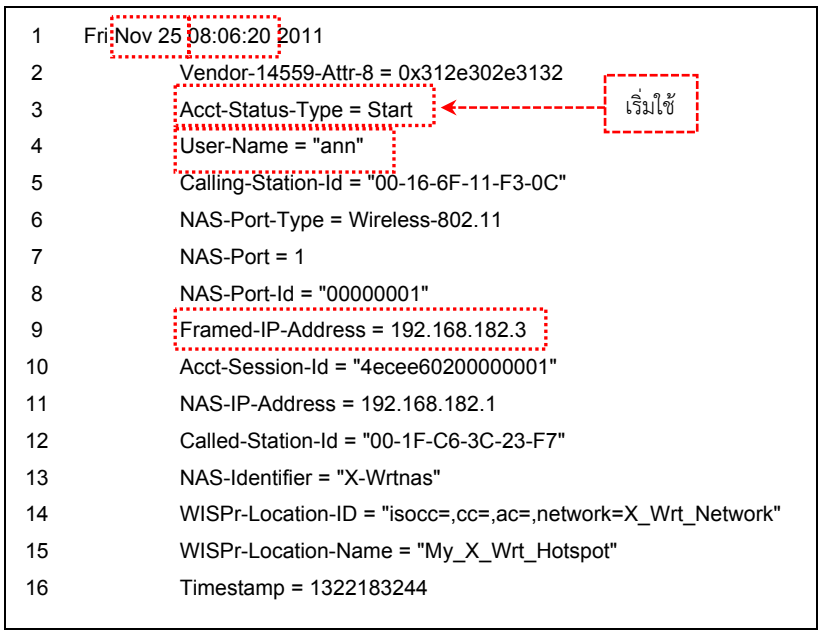
1 Nov 25 08:06:21 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=23.48.67.235 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=884 DF PROTO=TCP SPT=1115 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

2 Nov 25 08:07:01 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=68.232.44.119 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1067 DF PROTO=TCP SPT=1134 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

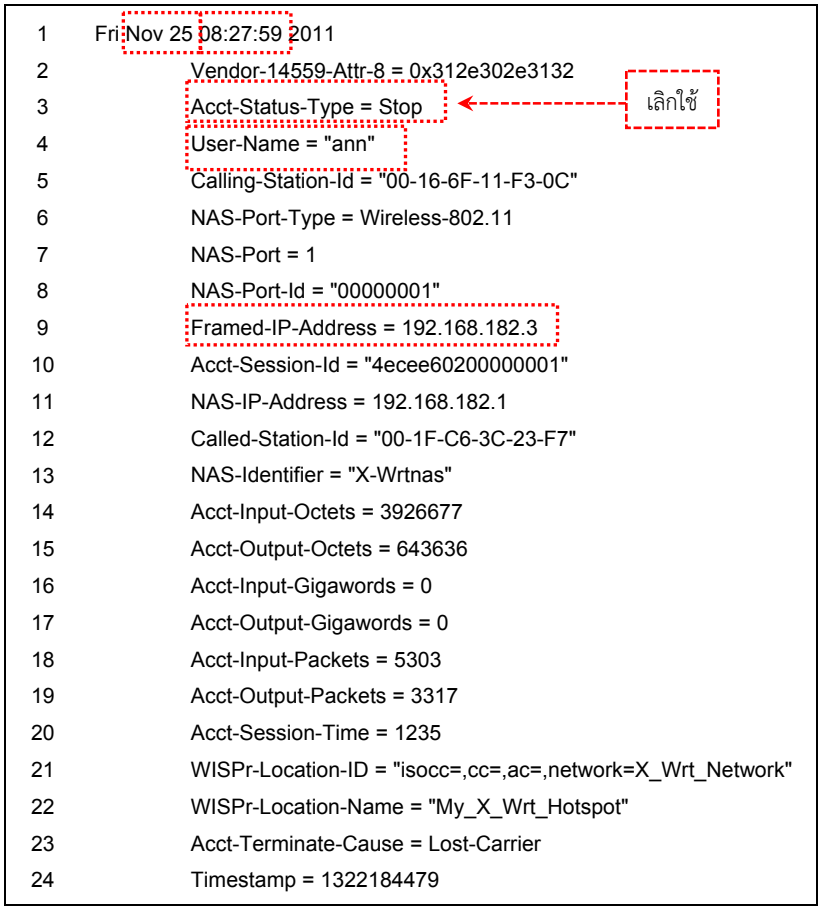
รูปที่ 3.5ชุดของรูปแบบของข้อมูลจราจรเครือข่ายที่จำเป็น

ตารางที่3.3รูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการ

Date	Time	Source IP	Destination IP	Protocol	Dest. Port
Nov25	08:06:21	192.168.182.3	23.48.67.235	TCP	80
Nov25	20:56:24	192.168.182.3	72.14.203.139	TCP	80
Nov25	22:25:11	192.168.182.3	203.8.110.64	TCP	80



(ก)

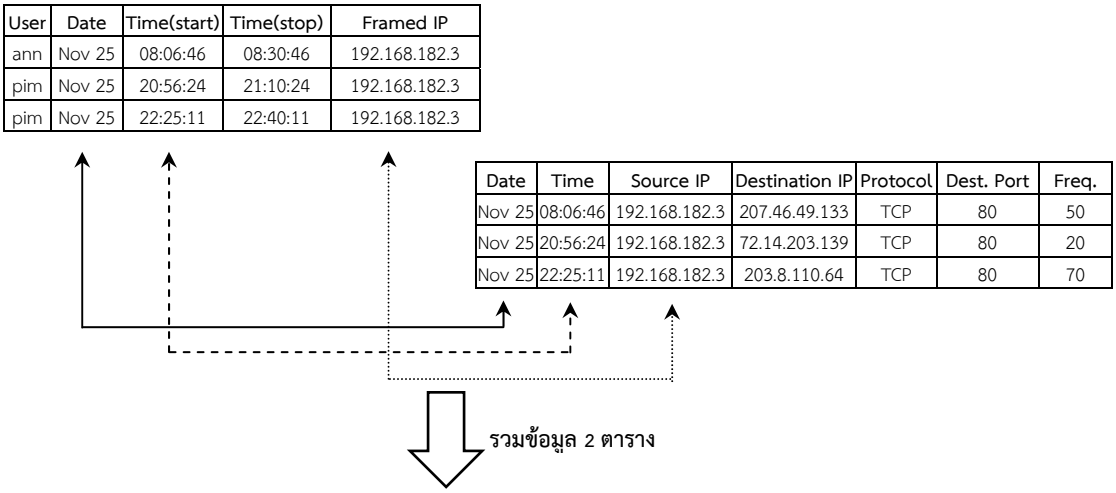


(ข)

รูปที่ 3.6 รูปแบบของข้อมูลของเวลาเริ่มใช้งาน(ก)และเวลาเลิกใช้งาน(ข)

ตารางที่3.4รูปแบบของข้อมูลผู้ใช้งานที่ต้องการ

User	Date	Time(start)	Time(stop)	Framed IP
ann	Nov 25	08:06:46	08:30:46	192.168.182.3
pim	Nov 25	20:56:24	21:10:24	192.168.182.3
Pim	Nov 25	22:25:11	22:40:11	192.168.182.3



User	Date	Time(start)	Time(stop)	Source IP	Destination IP	Protocol	Dest. Port	Freq.
ann	Nov 25	08:06:46	08:30:46	192.168.182.3	207.46.49.133	TCP	80	50
pim	Nov 25	20:56:24	21:10:24	192.168.182.3	72.14.203.139	TCP	80	20
pim	Nov 25	22:25:11	22:40:11	192.168.182.3	203.8.110.64	TCP	80	70

รูปที่ 3.7รูปแบบวิธีการรวมข้อมูลจาก 2 ตาราง

ตารางที่3.5รูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการ

User	Date	Time(start)	Time(stop)	Source IP	Destination IP	Protocol	Dest. Port	Freq.
ann	Nov 25	08:06:46	08:30:46	192.168.182.3	207.46.49.133	TCP	80	50
pim	Nov 25	20:56:24	21:10:24	192.168.182.3	72.14.203.139	TCP	80	20
pim	Nov 25	22:25:11	22:40:11	192.168.182.3	203.8.110.64	TCP	80	70

บทที่ 3

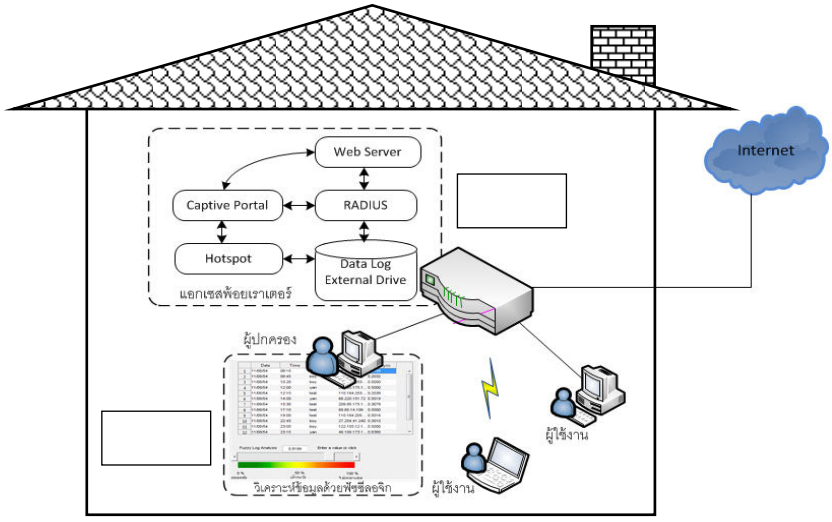
การออกแบบและพัฒนาระบบ

3.1 บทนำต้นเรื่อง

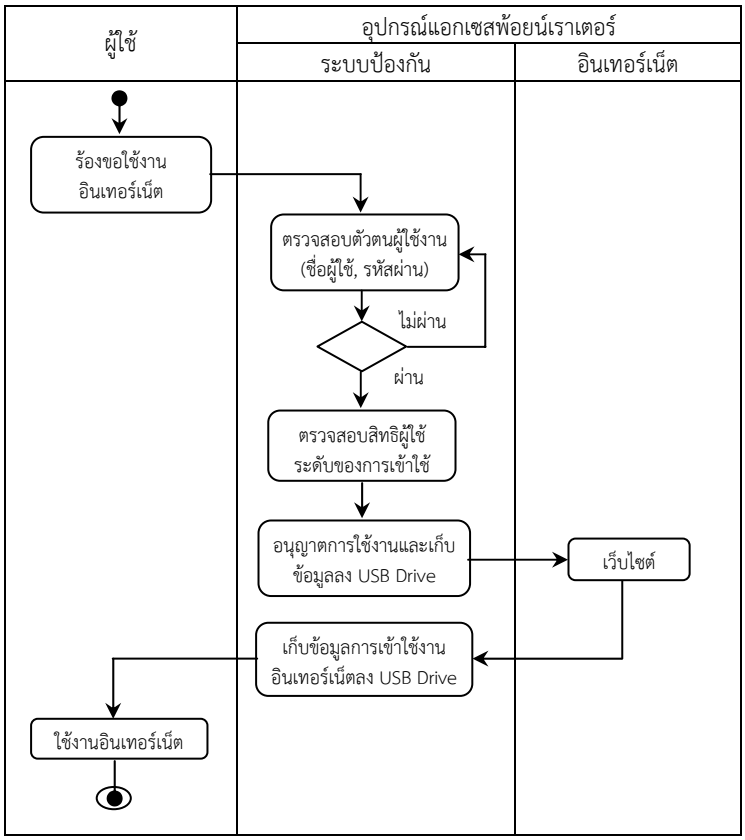
เป็นการกล่าวถึงรายละเอียดกลไกทำงานเพื่อแก้ปัญหาต่างๆ ซึ่งได้อธิบายในบทที่ผ่านมา โดยเริ่มจากอธิบายแนวคิดและสถาปัตยกรรมระบบ จากนั้นจะเป็นแนวทางการพิจารณาเลือกผลิตภัณฑ์คอมพิวเตอร์แบบฝังตัวและซอฟต์แวร์ที่จำเป็นในการจัดเก็บข้อมูลจราจรเครือข่ายพร้อมสรุปผล ในส่วนสุดท้ายเป็นรายละเอียดรูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการเพื่อวิเคราะห์ผลด้วยฟัซซีลอจิก

3.2 แนวความคิดและสถาปัตยกรรมระบบ

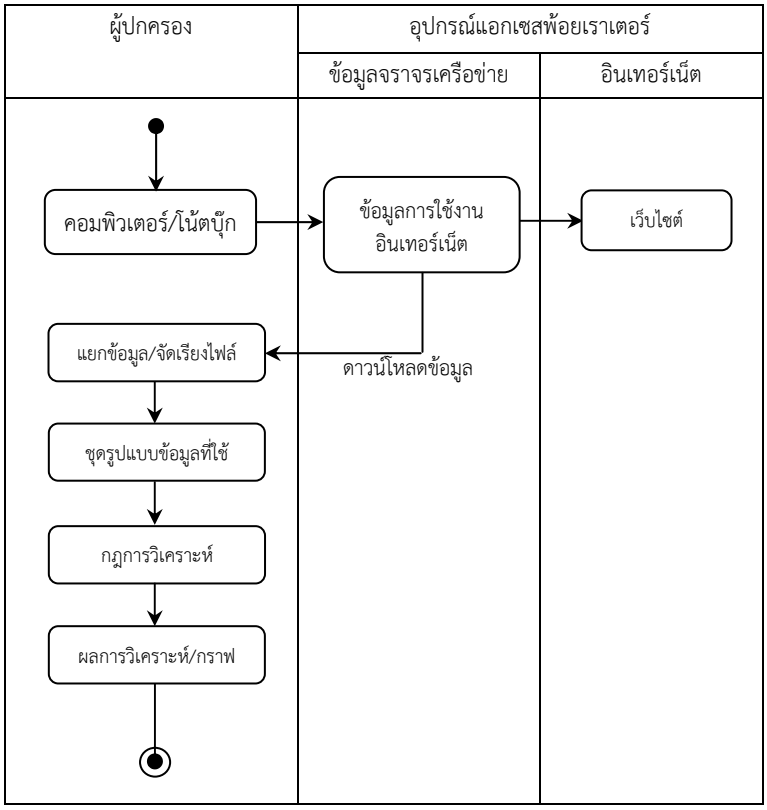
ระบบจัดเก็บข้อมูลจราจรโดยใช้เครื่องคอมพิวเตอร์แม่ข่ายดังที่ได้กล่าวไปในบทที่ผ่านมานั้น เป็นแนวทางที่น่าสนใจมากในการศึกษาเพื่อพัฒนาระบบจัดเก็บข้อมูลจราจรสำหรับบ้านพักอาศัย ในการเฝ้าตรวจและบันทึกข้อมูลการใช้งานอินเทอร์เน็ต ซึ่งระบบดังกล่าวมีหน้าที่หลักในการให้บริการและเชื่อมต่อเครื่องลูกข่ายเข้าสู่เครือข่ายหลัก เพื่อใช้งานในเครือข่ายให้ออกสู่อินเทอร์เน็ตได้ โดยสามารถนำแนวคิดของสถาปัตยกรรมระบบจัดเก็บข้อมูลจราจรที่เป็นเครื่องแม่ข่ายมาประยุกต์ใช้กับอุปกรณ์แอกเซสพ้อยน์เราเตอร์เพื่อจัดการเครือข่ายสายและไร้สายสำหรับบ้านพักอาศัยในการจัดเก็บข้อมูลการใช้งานตามวัตถุประสงค์ของงานวิจัย โดยมีแนวคิดสถาปัตยกรรมของระบบและสถาปัตยกรรมซอฟต์แวร์ของอุปกรณ์ แสดงดังรูปที่3.1ซึ่งสามารถแบ่งออกเป็น 2 ส่วน โดยส่วนที่ 1 เป็นขั้นตอนของสถาปัตยกรรมซอฟต์แวร์ของผู้ใช้งาน ซึ่งมีอุปกรณ์แอกเซสพ้อยน์เราเตอร์เป็นตัวกลางในการให้บริการเครือข่ายภายในประกอบด้วยซอฟต์แวร์ที่ช่วยในการจัดการเครือข่ายมีหน้าที่หลักๆ คือ ให้บริการในรูปแบบเว็บโดยมีระบบพิสูจน์ตัวตน การกำหนดสิทธิและบันทึกการใช้เข้างานในลักษณะเดียวกันกับระบบเครื่องแม่ข่ายและจัดเก็บบันทึกข้อมูลการเข้าใช้งานลงในหน่วยความจำภายนอกแบบ USB ที่เพิ่มเติมสำหรับใช้ในการจัดเก็บข้อมูลจราจรเครือข่าย และในส่วนที่ 2 เป็นขั้นตอนโดยแสดงเป็นโครงสร้างสถาปัตยกรรมการทำงานสามารถแสดงเป็น (Work Flow)ซึ่งเป็นการแบ่งกลุ่ม Activity และกำหนดแต่ละช่องด้วยชื่อ Object ไว้ด้านบน ซึ่งจะช่วยให้การมองภาพของผู้รับผิดชอบได้ชัดเจนขึ้นแผนภาพกิจกรรม ดังแสดงในรูปที่ 3.2 และในรูปที่ 3.3 แสดงการนำเข้าสู่กระบวนการวิเคราะห์ในเครื่องผู้ปกครอง ซึ่งในส่วนนี้จะเป็นการแยกข้อมูลจราจรเครือข่ายที่จำเป็นของข้อมูลจราจรที่ต้องการโดยใช้ช่องว่างข้อมูลแต่ละบรรทัดในการเลือกข้อมูลเฉพาะที่ต้องการซึ่งจะกล่าวรายละเอียดในหัวข้อต่อไป



รูปที่ 3.1แนวความคิดของระบบและสถาปัตยกรรมซอฟต์แวร์ของอุปกรณ์



รูปที่ 3.2 แนวความคิดการทำงานของซอฟต์แวร์สำหรับผู้ใช้งาน



รูปที่ 3.3 แนวความคิดขั้นตอนการวิเคราะห์ข้อมูลสำหรับผู้ปกครอง

3.3 แนวทางการพิจารณาเลือกผลิตภัณฑ์แอกเซสพ้อยน์เราเตอร์

การพิจารณาเลือกผลิตภัณฑ์ของอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่เป็นคอมพิวเตอร์แบบฝังตัว ในการพัฒนาระบบจะต้องคำนึงถึงประสิทธิภาพและความต้องการในการใช้งาน ซึ่งในงานวิจัยนี้ได้พิจารณาโดยใช้องค์ประกอบที่สำคัญคือ สามารถรองรับการปรับเปลี่ยนแพลทฟอร์มแบบโอเพ่นซอร์สราคาถูก และมีคุณลักษณะของตัวอุปกรณ์ที่มีหน่วยประมวลผลกลางไม่น้อยกว่า200 MHz. หน่วยความจำหลัก 16 MB. เพื่อรองรับแพลทฟอร์มและการติดตั้งซอฟต์แวร์สำหรับระบบจัดเก็บข้อมูล ซึ่งจากการศึกษาพบว่าอุปกรณ์คอมพิวเตอร์แบบฝังตัวมีให้เลือกมากมายหลายยี่ห้อมีความสามารถแตกต่างกันตามรุ่นและคุณลักษณะของอุปกรณ์ตามความต้องการของผู้ใช้งาน เช่น มาตรความเร็วของตัวอุปกรณ์และหน่วยประมวลผลการทำงาน เป็นต้นสามารถยกตัวอย่างอุปกรณ์ดังกล่าวที่สามารถรองรับการพัฒนาระบบจัดเก็บข้อมูลจราจรเครือข่ายได้ เช่น อุปกรณ์แอกเซสพ้อยน์ยี่ห้อ Asus รุ่นWL-500GPยี่ห้อ Linksysรุ่น WRT54GLและยี่ห้อNetgear รุ่น WGT634U [10] เป็นต้นและรายละเอียดคุณสมบัติของอุปกรณ์ ดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 รายละเอียดคุณลักษณะของอุปกรณ์

อุปกรณ์	ซีพียู	หน่วยความจำข้อมูล	หน่วยความจำหลัก	หน่วยความจำภายนอก	ราคา (มิ.ย. 54)
1. Linksys รุ่น WRT54GL	200 MHz	4 MB	16 MB	ไม่มี	2,500 .-
3. Netgearรุ่น WGT634U	200 MHz	8 MB	32 MB	USB 2.0	4,290 .-
2. ASUS รุ่น WL500gP V2	240 MHz	8 MB	32 MB	USB 2.0	3,250 .-

3.4 แนวการพิจารณาเลือกซอฟต์แวร์ในการจัดเก็บข้อมูลจราจรเครือข่าย

การศึกษาพิจารณาคัดเลือกซอฟต์แวร์สำหรับอุปกรณ์นั้น จำเป็นต้องศึกษารายละเอียดของระบบปฏิบัติการภายในหรือที่เรียกว่าแพลทฟอร์ม ที่สนับสนุนและรองรับการทำงานของตัวอุปกรณ์ให้สามารถทำงานได้ซึ่งจากการศึกษาพบว่ามีซอฟต์แวร์โอเพ่นซอร์สที่สนับสนุนการทำงานภายในของตัวอุปกรณ์ได้อย่างเหมาะสม และนิยมใช้กันอย่างแพร่หลาย เช่นDD-WRT และ OpenWRT เวอร์ชั่น 0.9 (White Russian) หรือ OpenWRT เวอร์ชั่น 8.09.1 (Kamikaze)เป็นต้นโดยแพลทฟอร์มสามารถทำงานร่วมกับซอฟต์แวร์สนับสนุนต่างๆ เพื่อให้เกิดประโยชน์สำหรับการติดตั้งระบบจัดทำระบบจัดเก็บข้อมูลจราจรเครือข่าย ซึ่งซอฟต์แวร์ที่จำเป็นสำหรับระบบมีความสามารถหรือมีการใช้งานยากง่ายแตกต่างกันจึงควรพิจารณาเลือกใช้อย่างเหมาะสมที่สุดดังแสดงในตารางที่ 3.1 ประกอบด้วยรายละเอียดของแพลทฟอร์มและซอฟต์แวร์สนับสนุนที่จำเป็นสำหรับการติดตั้งระบบ

3.4.1 ซอฟต์แวร์ที่ทำหน้าเป็นเว็บเซิร์ฟเวอร์

เป็นซอฟต์แวร์ที่จำเป็นสำหรับระบบ ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์(Web Server)[18] ในการให้บริการเว็บเพจ เพื่อให้อุปกรณ์สามารถรองรับการอินเตอร์เฟสผ่านเว็บได้เช่น Apache,Lighthttpd และ Busybox เป็นต้น

3.4.2 ซอฟต์แวร์ที่ทำหน้าที่โต้ตอบกับผู้ใช้งาน

เป็นซอฟต์แวร์โต้ตอบผู้ใช้งาน (UI) ทำงานร่วมกับเว็บเซิร์ฟเวอร์ โดยมีรูปแบบเป็นเว็บอินเตอร์เฟสสำหรับการใช้งานและแสดงผลในรูปแบบเว็บเช่น ระบบบริหารเว็บไซต์ CMS, Luci, WebIFเป็นต้น

3.4.3 ซอฟต์แวร์ที่ทำหน้าที่เว็บคอยตรวจสอบการใช้ไอพีแอดเดรส

เป็นซอฟต์แวร์ตรวจจับการใช้งานในเครือข่ายของผู้ขอใช้บริการ (Captive Portal)[19] ซึ่งเป็นศูนย์กลางในการจัดการเครือข่าย โดยมีรูปแบบการLogin เข้าสู่ระบบ มีความสามารถในการให้บริการเครือข่ายเพื่อการพิสูจน์ตัวตนเช่น Nocatsplash, Wifi Dog, Chillispot, Coova Chilli โดยมีรูปแบบลักษณะการทำงานในลักษณะเดียวกัน เป็นต้น

3.4.4 ซอฟต์แวร์ที่ทำหน้าที่ตรวจสอบสิทธิยืนยันตัวตน

เป็นซอฟต์แวร์ตรวจสอบสิทธิและการยืนยันตัวตนเพื่อเข้าใช้งานเครือข่าย (Authentication) [9] โดยมีโครงสร้างชื่อผู้ใช้และรหัสผ่าน เช่น เมื่อป้อนชื่อผู้ใช้และรหัสผ่าน ข้อมูลจะถูกส่งผ่านเครือข่าย เพื่อตรวจสอบให้ถูกต้องก่อน จึงอนุญาตตามสิทธิเฉพาะผู้มีข้อมูลอยู่ในระบบเท่านั้นให้เข้าถึงเครือข่ายได้ เช่น Freeradius, Ldap, Open Radiusเป็นต้น

3.4.5 ซอฟต์แวร์ที่ทำหน้าที่จัดเก็บสถานะ

เป็นซอฟต์แวร์จัดเก็บสถานะของการทำงานภายในตัวระบบต่างๆ และข้อมูลการใช้งานเครือข่าย สามารถเรียกดูข้อมูลย้อนหลังได้ เรียกอีกอย่างหนึ่งว่า Logging [20]เช่น Syslog-ng, Ulogd, Scanlogd เป็นต้น

ตารางที่ 3.2 รายละเอียดประเภทของซอฟต์แวร์ที่รองรับของแพลทฟอร์ม

ซอฟต์แวร์หลัก	**รายละเอียดซอฟต์แวร์ที่รองรับ**	**แพลทฟอร์ม**		
		DD-WRT v24 sp1 (Update Jun 2009) (Size 3.59 MB.)	White Russianrc6 (Update Nov 2006) (Size 1.42MB.)	Kamikaze 8.09.1 (Update Jun 2009) (Size 2.17MB.)
Web Server	Apache	●		●
	Lighthttpd	●	●	●
	Busybox		●	●
UI	Luci			●
	WebIF		●	●
Captive Portal	Chillispot	●	●	●
	Coova Chilli			●
	Nocatsplash		●	●
Authentication	Freeradius	●	●	●
	OpenRadius		●	●
	Ldap	●		
Logging	Syslog-ng	●		●
	Ulogd	●	●	●
	Scanlogd			●

3.5 ผลการศึกษา

3.5.1 การเลือกอุปกรณ์คอมพิวเตอร์แบบฝังตัวและแพลทฟอร์ม

3.5.1.1 จากการศึกษารายละเอียดของอุปกรณ์คอมพิวเตอร์แบบฝังตัวพบว่าการพิจารณาคัดเลือกอุปกรณ์สำหรับนำมาพัฒนาร่วมกับซอฟต์แวร์ที่จำเป็นในการติดตั้งระบบที่สามารถใช้งานได้ โดยในวิทยานิพนธ์นี้เลือกใช้อุปกรณ์ ยี่ห้อAsus รุ่น WL500GP กล่าวคือ การพิจารณาความคุ้มค่าด้านราคาและคุณลักษณะของตัวอุปกรณ์มีความเหมาะสม โดยมีหน่วยประมวลผลกลางขนาด 240 MHz. หน่วยความจำหลัก 32 MB. หน่วยความจำข้อมูล 8 MB. และรองรับหน่วยความจำภายนอกแบบ USB 2.0 ได้ ดังตารางที่ 3.1 โดยไม่ต้องปรับแต่งด้านฮาร์ดแวร์ใดๆและเอื้อให้ผู้ใช้สามารถปรับเปลี่ยนแพลทฟอร์มและซอฟต์แวร์แบบโอเพ่นซอร์ส สำหรับนำมาทดลองประยุกต์ใช้สำหรับการติดตั้งระบบจัดเก็บข้อมูลจราจรเครือข่ายสำหรับบ้านพักอาศัย

3.5.1.2 จากการศึกษารายละเอียดของแพลทฟอร์มแบบโอเพ่นซอร์ส ที่รองรับการทำงานของอุปกรณ์พบว่าแพลทฟอร์มที่เหมาะสมสำหรับนำมาประยุกต์ใช้ OpenWRT เวอร์ชั่น 8.09.1Kamikaze ซึ่งจากการศึกษาและเปรียบเทียบข้อมูลซอฟต์แวร์ที่สนับสนุนต่างๆพบว่ามีความเหมาะสมที่สุดดังตารางที่ 3.2เนื่องจากสามารถรองรับซอฟต์แวร์ที่หลากหลายและมีข้อมูลเผยแพร่มาก และสามารถรองรับการทำงานของซอฟต์แวร์ Coova Chilli [21] ซึ่งเป็นซอฟต์แวร์เวอร์ชั่นใหม่ที่พัฒนาต่อจาก Chillispot ทำให้สามารถง่ายต่อการติดตั้งระบบเมื่อใช้งานร่วมกับ Freeradius เป็นต้น

3.5.2 การเลือกใช้ซอฟต์แวร์ต่างๆ เพื่อการจัดเก็บข้อมูลจราจรเครือข่าย

จากการศึกษารายละเอียดของซอฟต์แวร์พื้นฐานดังที่ได้กล่าวมาในข้อที่ 3.3 นั้น สำหรับการพัฒนาระบบจัดเก็บข้อมูลเครือข่ายในบ้านพักอาศัย สามารถเลือกใช้ซอฟต์แวร์ระบบต่างๆ ซึ่งอธิบายโดยสรุปได้ดังนี้

3.5.2.1 ซอฟต์แวร์เว็บเซิร์ฟเวอร์ (Web Server) เลือกใช้ซอฟต์แวร์ Busybox เนื่องจากเป็นพื้นฐานของแพลทฟอร์ม Kamikaze 8.09.1 อยู่แล้วทำให้สามารถใช้งานได้ทันทีโดยไม่ต้องติดตั้งเพิ่มเติมและมีข้อดีเนื่องจากขนาดของซอร์ฟแวร์เล็กทำให้ประหยัดพื้นที่ในการใช้งานเมื่อเทียบกับ Web Server แบบ Apache และ Lighthttpd เป็นต้น

3.5.2.2 ซอฟต์แวร์ติดต่อผู้ใช้งาน(UI)เลือกใช้ซอฟต์แวร์ WebIF เนื่องจากรองรับการทำงานสำหรับแฟลทฟอร์ม OpenWRTKamikaze 8.09.1และรองรับโมดูลซอฟต์แวร์ที่เลือกใช้เช่น Coova Chilli ทำให้ลดขั้นตอนในการติดตั้งระบบเป็นต้น

3.5.2.3 ซอฟต์แวร์ตรวจสอบการใช้ไอพีแอดเดรส (Captive Portal) ในเครือข่ายของผู้ขอใช้บริการเลือกใช้ซอฟต์แวร์ Coova Chilli เนื่องจากรองรับเวอร์ชั่นใหม่ที่พัฒนามาจาก Chillispot ซึ่งรองรับการทำงานของ User Interface แบบWebIF ทำให้ลดปัญหาในการปรับตั้งค่าการทำงานของระบบ

3.5.2.4 ซอฟต์แวร์ตรวจสอบสิทธิยืนยันตัวตน(RADIUS)เพื่อเข้าใช้งานเครือข่ายเลือกใช้ซอฟต์แวร์ Freeradiusเนื่องจากใช้พื้นที่ในการติดตั้งไม่มากนัก ซึ่งเป็นที่ยอมรับและมีข้อมูลเผยแพร่มากในการติดตั้งระบบมีความสามารถในลักษณะเดียวกันคือการตรวจสอบสิทธิยืนยันตัวตน ในส่วนของขนาดพื้นที่ของซอฟต์แวร์จะไม่แตกต่างกันมากจึงเหมาะสำหรับนำมาใช้ในการพัฒนาระบบ

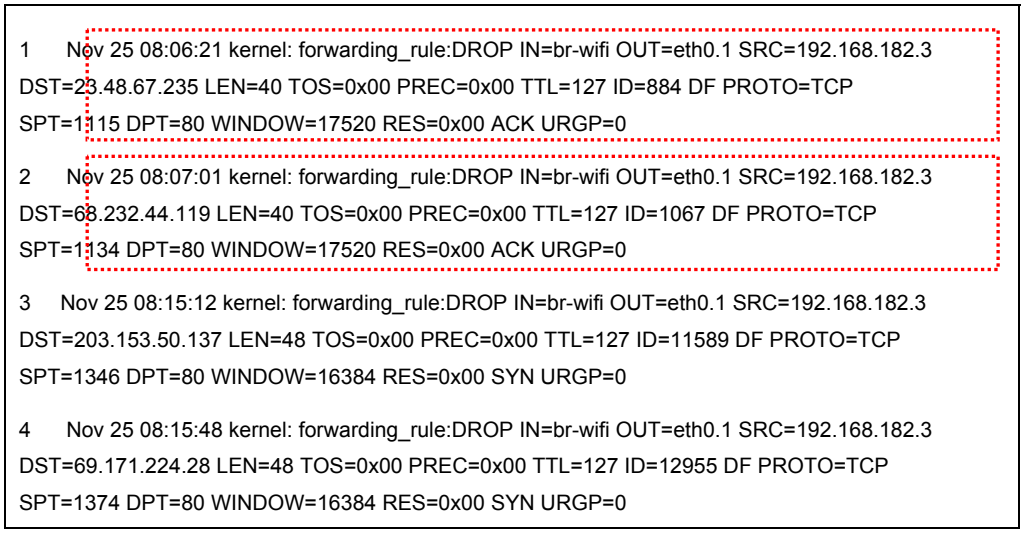
3.5.2.5 ซอฟต์แวร์ที่ทำหน้าที่จัดเก็บสถานการณ์ทำงาน (Logging)และข้อมูลจราจรเครือข่ายเลือกใช้ซอฟต์แวร์ Syslog-ng เนื่องจากเป็นพื้นฐานของแพลทฟอร์มที่ติดตั้งอยู่ภายในแล้วทำให้ไม่ต้องมีการติดตั้งซอฟต์แวร์เพิ่มเติมสามารถเรียกใช้งานได้ทันทีทำให้ช่วยประหยัดพื้นที่ในการติดตั้งภายในตัวอุปกรณ์

ดังนั้นเมื่อเลือกอุปกรณ์และแนวทางของซอฟแวร์สำหรับติดตั้งระบบแล้ว ขั้นตอนต่อไปจะเป็นรายละเอียดของของเทคนิควิธีการติดตั้งลงบนอุปกรณ์และการปรับตั้งค่าการใช้งานต่างๆ เพื่อให้สามารถใช้งานได้ในลักษณะเดียวกับกับเครื่องแม่ข่าย แต่จะขอกล่าวรายละเอียดของขั้นตอนการติดตั้งในส่วนของ ภาคผนวก ข.

3.6 รูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการ

ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ไม่ว่าจะเป็นแหล่งกำเนิด ต้นทาง ปลายทาง หรือข้อมูลอื่นๆที่ได้กล่าวไปในบทที่ผ่านมานั้น สำหรับในส่วนของข้อมูลที่จำเป็นเพื่อประกอบการวิเคราะห์ในบ้านพักอาศัย ซึ่งจะเลือกใช้ชุดรูปแบบข้อมูลที่จำเป็นเท่านั้น ซึ่งรูปแบบของข้อมูลที่จราจรเครือข่ายที่ได้จากการทดลองของตัวอุปกรณ์ มีข้อมูลมากเกินความจำเป็น ดังแสดงในรูปที่ 3.4 ซึ่งในงานวิจัยนี้จึงได้คัดเลือกเฉพาะข้อมูลที่ต้องการเบื้องต้นคือข้อมูลวัน/เวลาการติดต่อของเครือข่ายที่เข้าใช้บริการข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้หมายเลขชุดอินเทอร์เน็ตที่ถูกกำหนดให้ข้อมูลที่บอกถึงหมายเลขปลายทางที่เรียกใช้ โพรโตคอลและพอร์ทสื่อสาร โดยมีการเลือกข้อมูล แสดงดังรูปที่ 3.5 ซึ่งจากรูปข้อมูลภายในกรอบจะเป็นชุดข้อมูลที่ต้องการในการนำไปใช้งาน โดยใช้วิธีการตัดข้อมูลออกเป็นชุดเพื่อให้ได้ข้อมูลที่ต้องการ ดังแสดงในตารางที่ 3.3และสำหรับข้อมูลผู้ใช้งานที่มีรายละเอียดทั้งหมด เช่น วัน/เดือน/ปี ผู้ใช้ ชนิดของการให้บริการ เวลาเริ่มและสิ้นสุดการใช้งาน พอร์ทและไอดีต่างๆ เป็นต้น ซึ่งจะเลือกใช้เฉพาะข้อมูลที่เกี่ยวข้องเช่นกัน คือ ข้อมูลวันเวลาที่เริ่มและสิ้นสุดการใช้งานหมายเลขไอพีแอดเดรสของเครื่องผู้ใช้งาน ตามรายละเอียดดังแสดงดังตารางที่3.4 เพื่อเป็นข้อมูลในการใช้งานร่วมกันกับข้อมูล ในตารางที่ 3.3

เมื่อทำการแยกข้อมูลที่จำเป็นเบื้องต้นแล้ว ในส่วนของการนำข้อมูลไปใช้งานซึ่งจะต้องมีกระบวนการนำข้อมูลที่ได้ทั้งสองมาใช้งานร่วมกัน โดยเข้าสู่กระบวนการรวมข้อมูลทั้งสองตารางเข้าด้วยกัน(Join Table)แสดงดังรูปที่ 3.7 เพื่อให้ได้ข้อมูลที่พร้อมสำหรับนำไปทำการวิเคราะห์ผลตามกระบวนการของฟัซซีลอจิกในบทต่อไปแสดงดังในตารางที่ 3.5



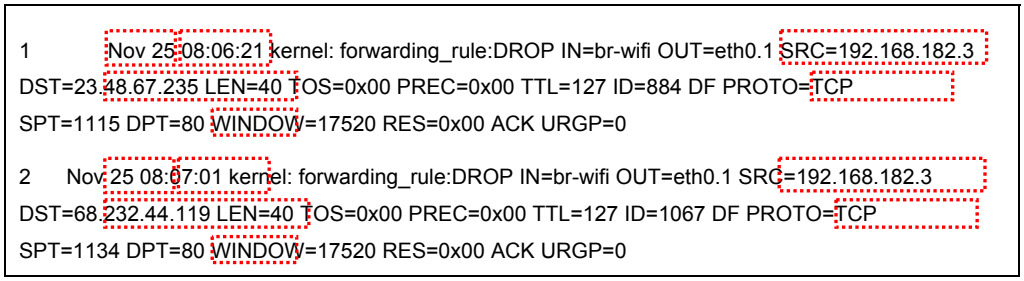
1 Nov 25 08:06:21 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=23.48.67.235 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=884 DF PROTO=TCP SPT=1115 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

2 Nov 25 08:07:01 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=68.232.44.119 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1067 DF PROTO=TCP SPT=1134 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

3 Nov 25 08:15:12 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=203.153.50.137 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=11589 DF PROTO=TCP SPT=1346 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0

4 Nov 25 08:15:48 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=69.171.224.28 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=12955 DF PROTO=TCP SPT=1374 DPT=80 WINDOW=16384 RES=0x00 SYN URGP=0

รูปที่ 3.4รูปแบบของข้อมูลจราจรเครือข่ายจากตัวอุปกรณ์



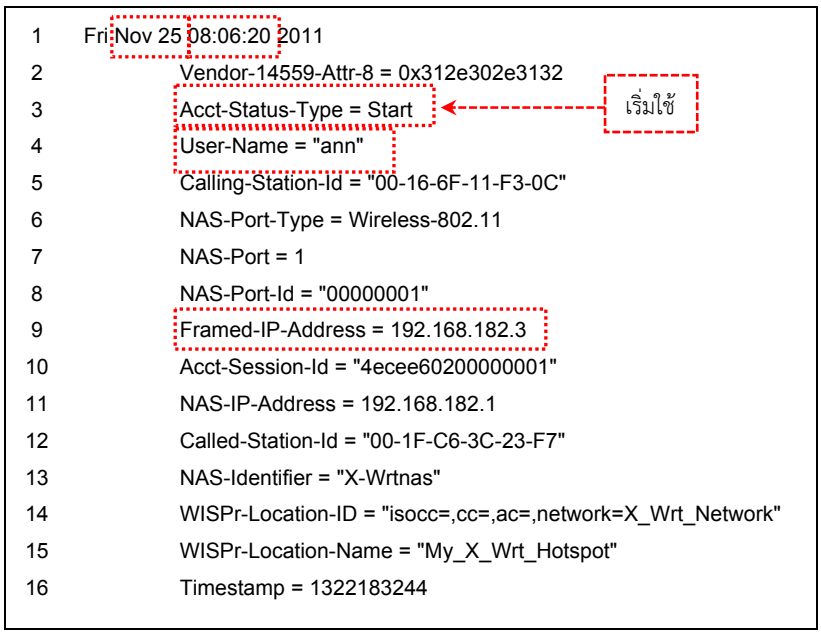
1 Nov 25 08:06:21 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=23.48.67.235 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=884 DF PROTO=TCP SPT=1115 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

2 Nov 25 08:07:01 kernel: forwarding_rule:DROP IN=br-wifi OUT=eth0.1 SRC=192.168.182.3 DST=68.232.44.119 LEN=40 TOS=0x00 PREC=0x00 TTL=127 ID=1067 DF PROTO=TCP SPT=1134 DPT=80 WINDOW=17520 RES=0x00 ACK URGP=0

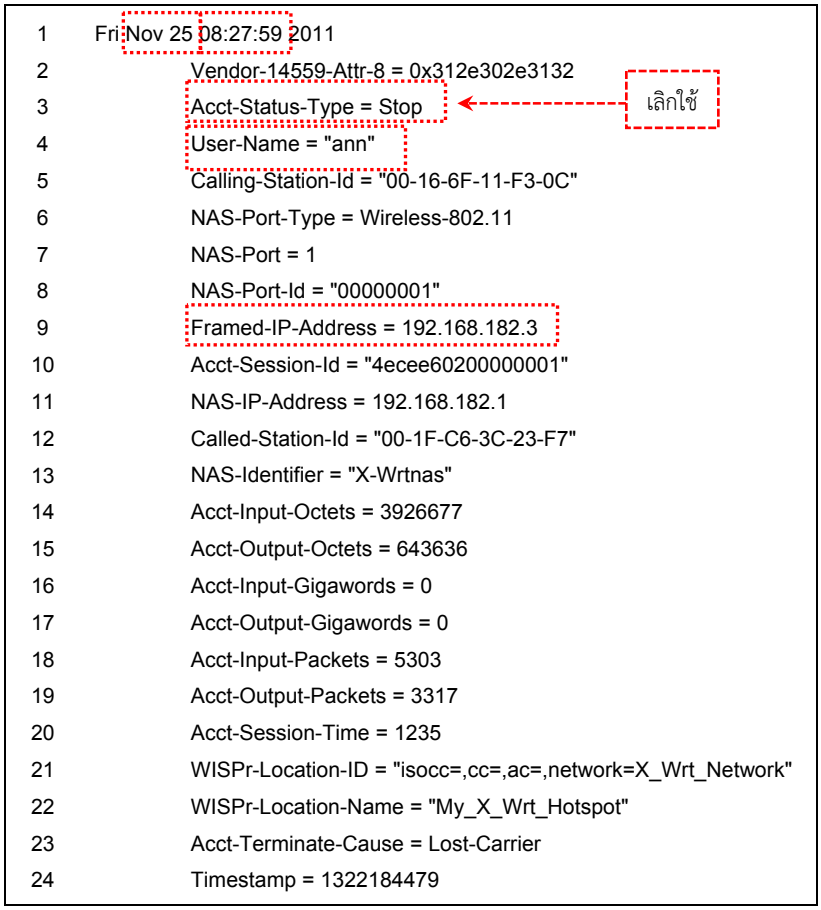
รูปที่ 3.5ชุดของรูปแบบของข้อมูลจราจรเครือข่ายที่จำเป็น

ตารางที่3.3รูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการ

Date	Time	Source IP	Destination IP	Protocol	Dest. Port
Nov25	08:06:21	192.168.182.3	23.48.67.235	TCP	80
Nov25	20:56:24	192.168.182.3	72.14.203.139	TCP	80
Nov25	22:25:11	192.168.182.3	203.8.110.64	TCP	80



(ก)

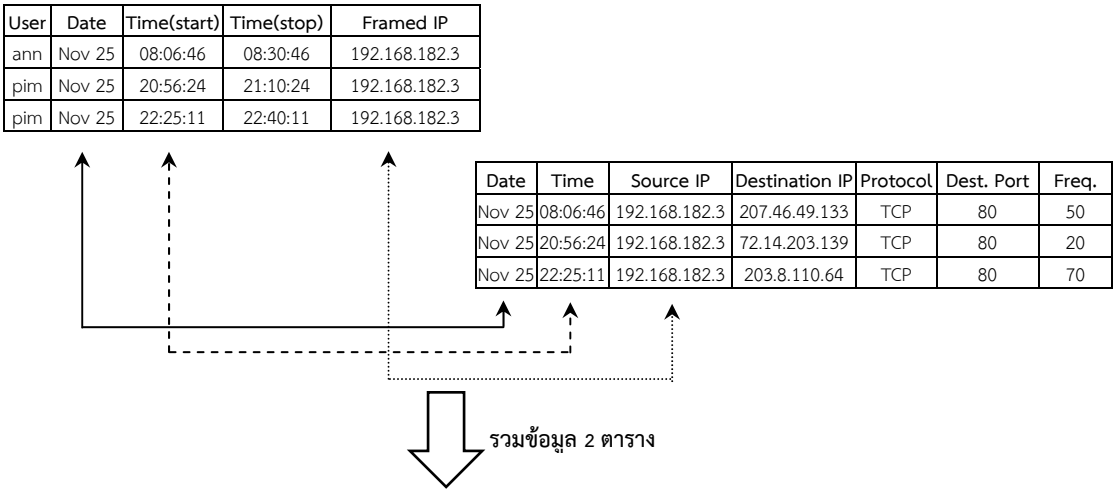


(ข)

รูปที่ 3.6 รูปแบบของข้อมูลของเวลาเริ่มใช้งาน(ก)และเวลาเลิกใช้งาน(ข)

ตารางที่3.4รูปแบบของข้อมูลผู้ใช้งานที่ต้องการ

User	Date	Time(start)	Time(stop)	Framed IP
ann	Nov 25	08:06:46	08:30:46	192.168.182.3
pim	Nov 25	20:56:24	21:10:24	192.168.182.3
Pim	Nov 25	22:25:11	22:40:11	192.168.182.3



User	Date	Time(start)	Time(stop)	Source IP	Destination IP	Protocol	Dest. Port	Freq.
ann	Nov 25	08:06:46	08:30:46	192.168.182.3	207.46.49.133	TCP	80	50
pim	Nov 25	20:56:24	21:10:24	192.168.182.3	72.14.203.139	TCP	80	20
pim	Nov 25	22:25:11	22:40:11	192.168.182.3	203.8.110.64	TCP	80	70

รูปที่ 3.7รูปแบบวิธีการรวมข้อมูลจาก 2 ตาราง

ตารางที่3.5รูปแบบของข้อมูลจราจรเครือข่ายที่ต้องการ

User	Date	Time(start)	Time(stop)	Source IP	Destination IP	Protocol	Dest. Port	Freq.
ann	Nov 25	08:06:46	08:30:46	192.168.182.3	207.46.49.133	TCP	80	50
pim	Nov 25	20:56:24	21:10:24	192.168.182.3	72.14.203.139	TCP	80	20
pim	Nov 25	22:25:11	22:40:11	192.168.182.3	203.8.110.64	TCP	80	70

บทที่ 4

ผลการวิจัย

4.1 บทนำต้นเรื่อง

เป็นกล่าวถึงรายละเอียดการนำแนวคิดของฟัซซีลอจิกเข้ามาใช้งานตามรูปแบบของอินพุตได้อธิบายในบทที่ผ่านมาซึ่งเป็นการอธิบายแนวคิดการออกแบบอินพุตค่าความสัมพันธ์ของฟังชันความเป็นสมาชิกและการออกแบบกฎเกณฑ์สำหรับการวิเคราะห์ข้อมูล จากนั้นจึงเป็นการอธิบายผลการทดลองการวิเคราะห์ข้อมูล โดยมีการวิเคราะห์ด้วยข้อมูลจำลองและข้อมูลจริงจากตัวอุปกรณ์เครือข่าย และในส่วนสุดท้ายเป็นรายละเอียดแสดงผลของแนวคิดโปรแกรมสารสนเทศในการวิเคราะห์ข้อมูลจราจรเครือข่าย

4.2 แนวความคิดการประยุกต์ใช้ฟัซซีลอจิก

ฟัซซีลอจิกหรือตรรกะแบบคลุมเครือ (Fuzzy) ช่วยในการสนับสนุนการตัดสินใจ การพยากรณ์ การคาดการเหตุการณ์ เช่น ข้อมูลจราจรในการใช้งานอินเตอร์เน็ตมีปริมาณมากและปลายทางมีหลายประเภท ทำให้ผู้ปกครองแยกแยะความเหมาะสมหรือไม่เหมาะสมของการเข้าใช้งานของบุตร/ธิดาได้ยากลำบากและการใช้เกณฑ์ที่ชัดเจนแน่นอนมาตัดสินความเหมาะสมอาจจะใช้ไม่ได้กับทุกกรณีมีลักษณะพิเศษกว่าตรรกะแบบจริงเท็จ เช่น การเข้าถึงหลัง 22:00 น. ถือว่าไม่เหมาะสม แต่หากเป็น 21:59 น. ถือว่าเหมาะสม ดังที่ได้กล่าวไปแล้วในบทที่ผ่านมานั้น ในงานวิจัยนี้จึงเลือกใช้หลักการของฟัซซีลอจิกในการนำมาวิเคราะห์ผลของการเข้าใช้งานอินเทอร์เน็ตในบ้านพักอาศัยอย่างชาญฉลาด โดยกำหนดเงื่อนไขความเป็นสมาชิกของอินพุตต่างๆ นำเข้าสู่กระบวนสร้างกฎเกณฑ์การวิเคราะห์ เพื่อให้ได้เอาต์พุตของการเข้าใช้งานอินเทอร์เน็ตด้วยฟัซซีลอจิก และแบ่งความไม่เหมาะสมออกเป็น 3 ระดับ คือ ปลอดภัย เฝ้าระวังและไม่เหมาะสม เป็นต้น

4.2.1 การออกแบบอินพุตและค่าความสัมพันธ์

จากการศึกษาข้อมูลจราจรเครือข่ายคอมพิวเตอร์และข้อมูลจราจรที่จำเป็นดังที่ได้นำเสนอในบทที่ผ่านมา ซึ่งรูปแบบของข้อมูลที่จำเป็นสำหรับวิเคราะห์การใช้งานภายในบ้านพักอาศัยสามารถนำข้อมูลอินพุตเพื่อใช้งานร่วมกับฟัซซีลอจิกในการกำหนดค่าความเป็นสมาชิก (Membership Function) ของอินพุตและเอาต์พุต(Time, Entertainment, Advice, Frequency-Site และ Output) ให้มีความสัมพันธ์กัน เพื่อใช้สำหรับประเมินการวิเคราะห์ผลความเหมาะสมของการใช้งานอินเทอร์เน็ต (ซึ่งในส่วนของการแบ่งเวลาและค่าอินพุตต่างๆในงานวิจัยนี้เพื่อมุ่งหาแนวทางในการ

ทดสอบและวิเคราะห์ข้อมูลการใช้งานของบ้านพักอาศัยเท่านั้น ซึ่งหากนำไปใช้งานจริงอาจมีการแบ่งค่าที่ต่างกันได้) มีรายละเอียดดังต่อไปนี้

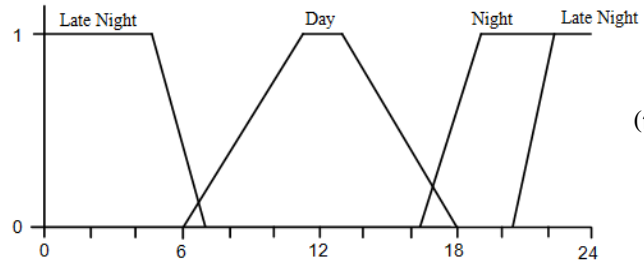
ก) อินพุตที่ 1 คือ เวลา (Time) กำหนดให้มีคะแนนตามความเป็นจริงตามชั่วโมงคือ ตั้งแต่ 0 ไปจนถึง 24 ชั่วโมง สามารถแบ่งฟังก์ชันความเป็นสมาชิกของอินพุตเป็น 3 ช่วงเวลา คือช่วงเวลากลางวัน (Day) ให้ค่าความเป็นสมาชิกตั้งแต่ช่วงเวลา 06:00-18:00 น.ช่วงเวลากลางคืน (Night) ให้ค่าความเป็นสมาชิกตั้งแต่เวลา 17:00-22:00 น. และช่วงเวลาดึก (Late Night) ให้ค่าความเป็นสมาชิกตั้งแต่เวลา 21:00 น. เป็นต้นไป แสดงดังรูปที่ 4.1(ก)

ข) อินพุตที่ 2 คือ กลุ่มความบันเทิง (Entertainment) กำหนด ให้การแบ่งฟังก์ชันความเป็นสมาชิกของอินพุตออกเป็น 10 ช่วง จากระดับความบันเทิงน้อย (Less Entertainment) ที่ค่า 0 จนถึงระดับความบันเทิงมาก (High Entertainment) ที่ค่า 1 แสดงดังรูปที่ 4.1(ข) ยกตัวอย่าง เช่น หากผู้ใช้กำหนดให้เว็บประเภทฟังเพลงและดูหนังด้วยกัน เช่น www.kapook.com อยู่ในเกณฑ์ระดับ 5 ผู้ใช้ก็อาจจะกำหนดให้เว็บประเภทเกมส์ล้วน เช่น www.meegame.com อยู่ในเกณฑ์ที่สูงกว่าระดับ 5 ขึ้นไปได้เป็นต้น

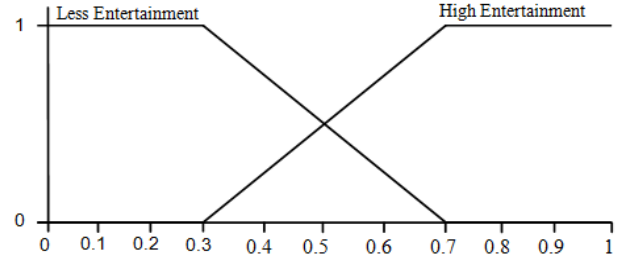
ค) อินพุตที่ 3 คือ กลุ่มที่ควรให้คำแนะนำ (Advice) ใช้แนวทางตามพระราชบัญญัติภาพยนตร์และวีดิทัศน์ พ.ศ. 2551[22] เพื่อแบ่งความเป็นสมาชิกเป็น 2 กลุ่ม คือ กลุ่มทุกช่วงวัย (All-Ages) เริ่มตั้งแต่ เหมาะกับทุกวัย, ควรให้คำแนะนำสำหรับ 9+, 13+, 15 และกลุ่มที่อายุมากกว่า 18 ปี (Web18+) ตั้งแต่ 18 ปีขึ้นไป โดยแบ่งจากเนื้อหาของเว็บที่ควรแนะนำให้เหมาะกับวัยตามลำดับเป็น 5 ช่วงคะแนนช่วงละเท่าๆกัน แสดงดังรูปที่ 4.1(ค)

ง) อินพุตที่ 4 คือ กลุ่มของความถี่ไอพีแอดเดรส (Frequency-Site) แบ่งความเป็นสมาชิกได้ 3 ช่วง คือ น้อย (Low), ปานกลาง (Medium) และมาก (High) โดยแบ่งจากใช้ไอพีแอดเดรสที่ซ้ำๆกันเป็นตัวบอกความถี่ (ดูตัวอย่างเกณฑ์ในตารางที่ 1 ประกอบ) แสดงดังรูปที่ 4.1(ง)

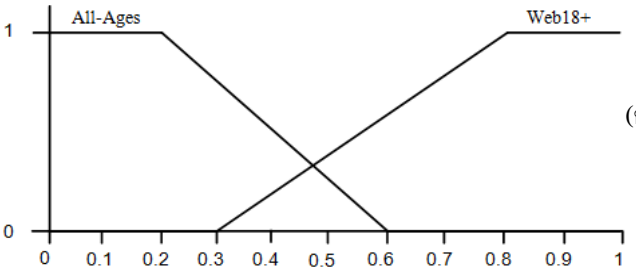
จ) เอาต์พุต คือ ผลการวิเคราะห์ (Analysis) แบ่งความเป็นสมาชิกเป็น 3 ระดับ คือ ปลอดภัย (Safe), เฝ้าระวัง (Monitoring) และไม่เหมาะสม (Inappropriate) โดยแบ่งคะแนนค่าความเป็นสมาชิกของความปลอดภัยตั้งแต่ 0 ไปจนถึง 0.4 ระดับการเฝ้าระวังตั้งแต่ 0.25 ถึง 0.75 และมากกว่า 0.6 ถึง 1 ให้เป็นคะแนนระดับความไม่เหมาะสมในการใช้งานอินเทอร์เน็ตแสดงดังรูปที่ 4.1(จ)



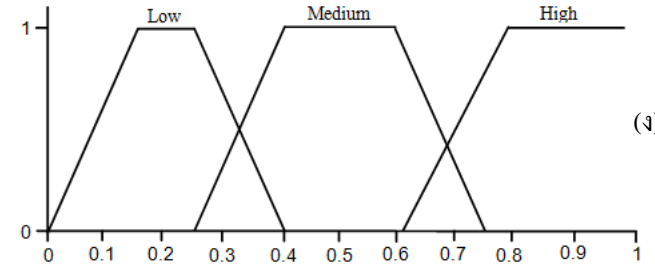
(ก) เวลา



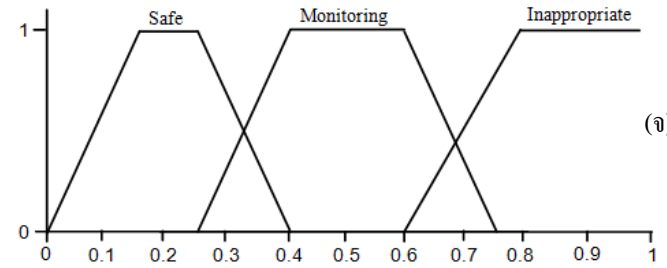
(ข) ความบันเทิง



(ค) ควรให้คำแนะนำ



(ง) ความถี่ไอพีแอดเดรส



(จ) ผลการวิเคราะห์

รูปที่ 4.1การกำหนดอินพุตและเอาต์พุตของฟังก์ชันความเป็นสมาชิก

4.2.2 การออกแบบกฎ

สำหรับการออกแบบและสร้างกฎในการวิเคราะห์ข้อมูลโดยมีเงื่อนไขต่างๆ ในการออกแบบตามความเหมาะสมซึ่งในงานวิจัยนี้ เน้นเรื่องของช่วงเวลาการเข้าใช้งาน กลุ่มของไอพีแอดเดรสและความถี่ในการใช้งานเว็บในกลุ่มต่างๆเป็นหลัก ซึ่งการสร้างกฎเกณฑ์เพื่อการวิเคราะห์ข้อมูลสำหรับหาค่าผลลัพธ์นั่นสามารถอธิบายกฎเกณฑ์ โดยแบ่งเป็นส่วนๆ ซึ่งจะยกตัวอย่างในส่วนที่เป็นปัจจัยหลักในการวิเคราะห์ คือ ด้าน เวลาและความไม่เหมาะสม ความไม่เหมาะสมเกิดขึ้นได้จากสาเหตุต่างๆเช่น เข้าใช้งานเวลาดึกและเว็บที่อยู่ในกลุ่มบันเทิงหรือเป็น 18+ และมีความถี่มากในการเข้าใช้งานเว็บนั้นๆ เป็นต้นสามารถอธิบายได้ดังต่อไปนี้

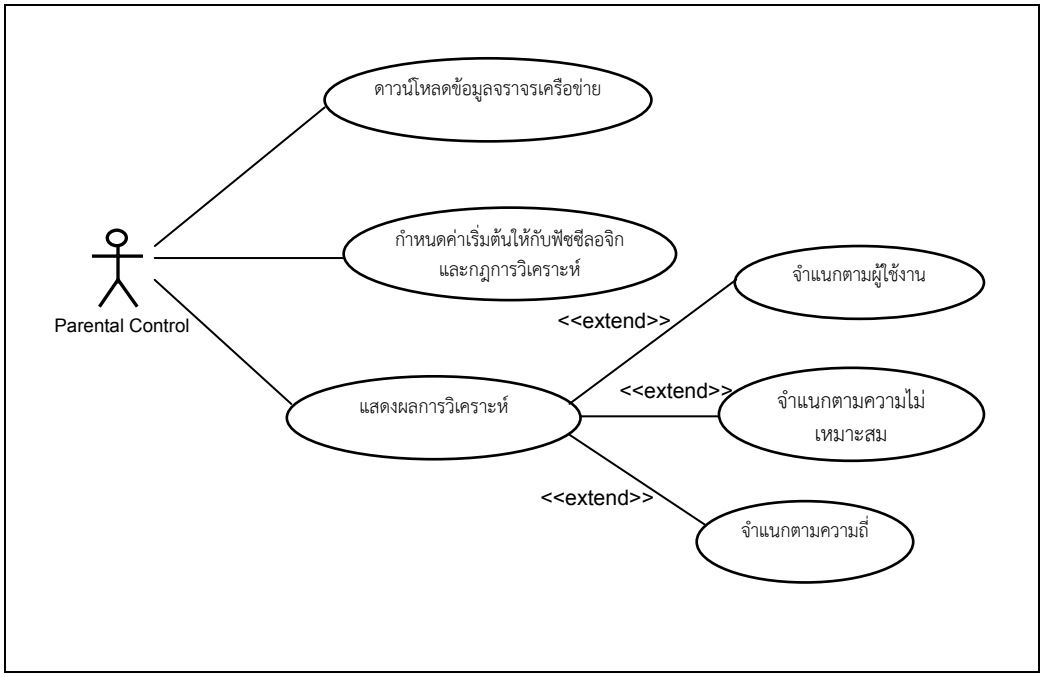
- กฎข้อที่ 1-3 เป็นการแบ่งกลุ่มการวิเคราะห์ของช่วงเวลาดึก
  - กฎข้อที่ 1If (Late-Night) and (Less-Entertainment) and (All-Ages) and (Freq.-not-High) Then (output is Safe) หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลาดึกและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงน้อย และเป็นเว็บที่จัดอยู่ในกลุ่มสำหรับบุคคลทุกช่วงวัย และความถี่การเข้าใช้งานอยู่ในช่วงน้อยถึงปานกลาง ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ปลอดภัย
  - กฎข้อที่ 2 If (Late-Night) and (High-Entertainment) and (All-Ages) and (Freq.-not-High) Then (output is Monitoring) หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลาดึกและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงมาก และเป็นเว็บที่จัดอยู่ในกลุ่มสำหรับบุคคลทุกช่วงวัย และความถี่การเข้าใช้งานอยู่ในช่วงน้อยถึงปานกลาง ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ควรเฝ้าระวัง
  - กฎข้อที่ 3 If (Late-Night) and (Less-Entertainment) and (Web 18+) and (Freq.-not-Low) Then (output is Inappropriate) หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลาดึกและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงน้อย และเป็นเว็บที่จัดอยู่ในกลุ่ม 18+ และมีความถี่การเข้าใช้งานอยู่ในช่วงปานกลางถึงมาก ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ไม่เหมาะสม
- กฎข้อที่ 4-7 เป็นการแบ่งกลุ่มการวิเคราะห์ของช่วงเวลากลางคืน
  - กฎข้อที่ 4 If (Night) and (High-Entertainment) and (All-Ages) and (Freq.-not-Low) Then (output is Inappropriate)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางคืนและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงมาก และเป็นเว็บที่จัดอยู่ในกลุ่มสำหรับบุคคลทุกช่วงวัย และมีความถี่การเข้าใช้งานอยู่ในช่วงปานกลางถึงมาก ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ไม่เหมาะสม

- กฎข้อที่ 5 If (Night) and (High-Entertainment) and (Web18+) and (Freq.-High) Then (output is Inappropriate)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางคืนและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงมาก และเป็นเว็บที่จัดอยู่ในกลุ่ม 18+ และมีความถี่การเข้าใช้งานมาก ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ไม่เหมาะสม
- กฎข้อที่ 6 If (Night) and (Less-Entertainment) and (All-Ages) and (Freq.-High) Then (output is Monitoring)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางคืนและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงน้อย และเป็นเว็บที่จัดอยู่ในกลุ่มสำหรับบุคคลทุกช่วงวัย และมีความถี่การเข้าใช้งานมาก ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ควรเฝ้าระวัง
- กฎข้อที่ 7 If (Day) and (Less-Entertainment) and (All-Ages)and (Freq.-not-Low) Then (output is Safe)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางวันและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงน้อย และเป็นเว็บที่จัดอยู่ในกลุ่มสำหรับบุคคลทุกช่วงวัย ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ปลอดภัย

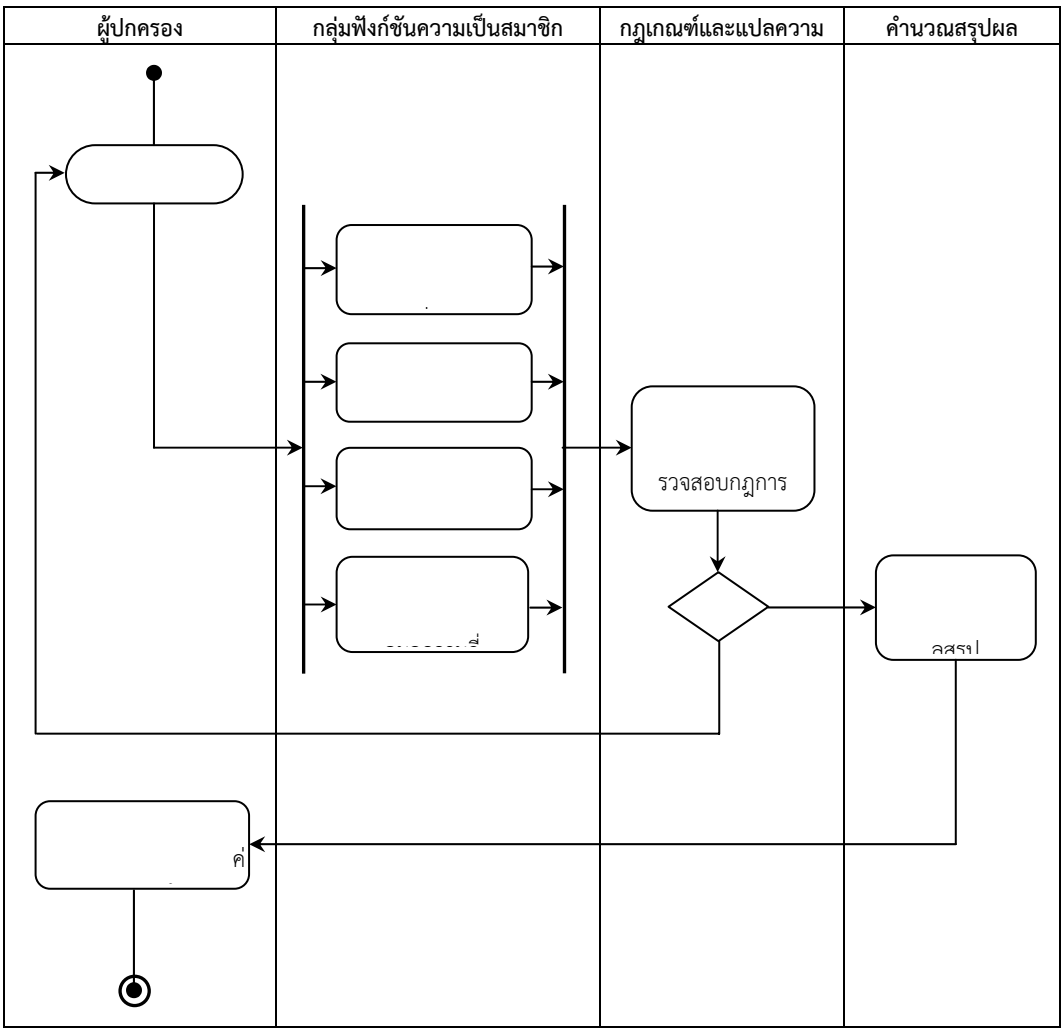
- กฎข้อที่ 8-10 เป็นการแบ่งกลุ่มการวิเคราะห์ของช่วงเวลากลางวัน
  - กฎข้อที่ 8 If (Day) and (Less-Entertainment) and (Web18+) and (Freq.-not-High) Then (output is Monitoring)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางวัน และเว็บไซต์ที่เข้าใช้งานมีความบันเทิงน้อย และเป็นเว็บที่จัดอยู่ในกลุ่ม 18+ และมีความถี่การเข้าใช้งานอยู่ในช่วงน้อยถึงปานกลาง ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ควรเฝ้าระวัง
  - กฎข้อที่ 9 If (Day) and (High-Entertainment) and (Web18+) and (Freq.-High) Then (output is Inappropriate)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางวัน และเว็บไซต์ที่เข้าใช้งานมีความบันเทิงมาก และเป็นเว็บที่จัดอยู่ในกลุ่ม 18+ และมีความถี่การเข้าใช้งานมาก ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ไม่เหมาะสม
  - กฎข้อที่ 10 If (Day) and (High-Entertainment) and (All-Ages) and (Freq.-High) Then (output is Monitoring)หมายถึง เมื่อมีผู้ใช้มีการเข้าใช้งานเวลากลางวันและเว็บไซต์ที่เข้าใช้งานมีความบันเทิงมาก และเป็นเว็บที่จัดอยู่ในกลุ่มสำหรับบุคคลทุกช่วงวัย และมีความถี่การเข้าใช้งานมาก ผลของเกณฑ์การวิเคราะห์ข้อมูลคือ ควรเฝ้าระวัง

4.3 โปรแกรมสารสนเทศเพื่อวิเคราะห์ข้อมูลด้วยฟัซซีลอจิก

กระบวนการวิเคราะห์ข้อมูลของโปรแกรมสารสนเทศโดยข้อมูลที่ออกแบบขึ้นเพื่อนำข้อมูลจราจรเครือข่ายที่ได้จากอุปกรณ์แอกเซสพ้อยน์เราเตอร์มาทำการวิเคราะห์ผลการเข้าใช้งานโดยมีแนวคิดในการพัฒนาโปรแกรมสารสนเทศขึ้นมาเพื่อให้ง่ายต่อการเรียกใช้ในการแสดงผลในการวิเคราะห์ข้อมูลและเพื่อให้สะดวกต่อการใช้งานสำหรับผู้ปกครอง ซึ่งสามารถอธิบายการทำงาน แสดงดังรูปที่4.2ซึ่งรูปแบบของการทำงานจะประกอบด้วยข้อมูลจราจรเครือข่ายที่ได้จากอุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่ผ่านการจัดเรียงข้อมูลให้อยู่ในรูปแบบที่ต้องการดังที่ได้กล่าวไว้ในบทที่ผ่านมาซึ่งจะนำชุดข้อมูลเข้าสู่ระบบเพื่อวิเคราะห์ด้วยฟัซซีลอจิก โดยขั้นตอนแรกเป็นการกำหนดฟังก์ชันความเป็นสมาชิกของอินพุตต่างๆ เพื่อส่งข้อมูลเข้าสู่กระบวนการวิเคราะห์และแปลความตามกฎเกณฑ์การคำนวณผลสรุปรวมจากกฎทุกข้อเพื่อแสดงผลการวิเคราะห์ข้อมูลในรูปแบบกราฟที่สามารถเข้าใจได้ง่าย



รูปที่ 4.2 Use Case Diagram ของระบบการวิเคราะห์ข้อมูล



รูปที่ 4.3 รายละเอียดกระบวนการวิเคราะห์ข้อมูล

4.4 ผลการทดลองการวิเคราะห์ข้อมูลจราจรเครือข่าย

4.4.1 การวิเคราะห์ด้วยข้อมูลจำลอง

เป็นการจำลองรูปแบบของข้อมูลอินพุตต่างๆ ก่อนนำข้อมูลจริงมาใช้งาน ในส่วนรูปแบบของข้อมูลจะเป็นข้อมูลที่ผ่านการแบ่งค่าอินพุตฟังก์ชั่นความเป็นสมาชิกมาแล้ว เช่น ข้อมูลแถวที่ 6ค่า 22 (เวลา:จะต้องแปลงเป็นค่าจำนวนเต็มเพื่อคำนวณผลการวิเคราะห์) 0.6 เท่ากับความบันเทิงเป็น0.9 เท่ากับเว็บที่ควรให้คำแนะนำ 1 ค่าความถี่ที่ใช้งาน และ 0.83 คือผลของฟัซซีลอจิกจากการคำนวณ ดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 ข้อมูลตัวอย่างการจำลองเพื่อวิเคราะห์ข้อมูลด้วยฟัซซีลอจิก

No.	Time	Entertainment	Advice	Frequency	Output Analysis
1	8	0.2	0.2	0.8	0.20
2	14	0.6	0.1	0.6	0.20
3	10.8	0.3	0.4	0.2	0.30
4	18	0.8	0.3	0.9	0.52
5	20	0.7	0.3	0.4	0.50
6	22	0.6	0.9	1	0.83
7	23.5	0.8	0.5	0.3	0.67

4.4.2 การเก็บข้อมูลกลุ่มตัวอย่าง

การนำอุปกรณ์จัดเก็บข้อมูลกลุ่มตัวอย่างเพื่อนำข้อมูลเข้าสู่กระบวนการวิเคราะห์สำหรับทดสอบการใช้งานจริง โดยเบื้องต้นได้ทดลองเก็บข้อมูลตัวอย่างจากบ้านพักจำนวน 3 หลัง ในพื้นที่อำเภอเมือง จังหวัดปัตตานี ซึ่งเน้นรายละเอียดของข้อมูลตัวอย่างของผู้ใช้งานสามารถแจกแจงรายละเอียดของผู้ใช้งานได้ดังแสดงในตารางที่ 4.2 เพื่อนำข้อมูลที่ได้เข้าสู่กระบวนการวิเคราะห์ด้วยฟัซซีลอจิกต่อไป

ตารางที่ 4.2 รายละเอียดเบื้องต้นของผู้ใช้งานกลุ่มตัวอย่าง

ข้อมูลตัวอย่าง	**หลังที่ 1**	**หลังที่ 2**	**หลังที่ 3**
1. ช่วงอายุ	11 ปี	14 ปี	9 ปี และ 15 ปี
2. ระดับชั้น	ป.6	ม.2	ป.4 และ ม.3
3. เพศ	หญิง	ชาย	หญิง
4. จำนวน	1 คน	1 คน	2 คน

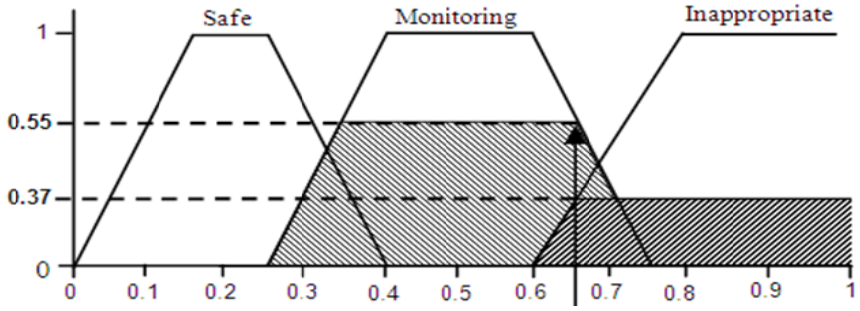
4.4.3 การวิเคราะห์ด้วยข้อมูลจราจรเครือข่ายจริง

จากข้อมูลจำลองในข้อที่ 4.2.1 ซึ่งเป็นแนวทางในการทดสอบการวิเคราะห์ข้อมูล สำหรับข้อมูลจริงที่ได้จากตัวอุปกรณ์ผ่านกระบวนการแปลงข้อมูลให้อยู่ในรูปแบบที่สามารถวิเคราะห์ข้อมูลได้ในลักษณะเดียวกันและการนำข้อมูลที่ได้จากการเก็บข้อมูลกลุ่มตัวอย่างในข้อที่ 4.4.2 สามารถยกตัวอย่างของข้อมูลจริง ซึ่งสามารถแสดงตัวอย่างการวิเคราะห์ข้อมูลในช่วงเวลากลางวัน และช่วงดึก ดังต่อไปนี้

ตารางที่ 4.3 รายการข้อมูลใช้งานช่วงกลางวัน

User	Month	Date	Time	IP Source	IP Destination	Protocal	Port	Frq.
Boy	Dec	11	14:09:10	192.168.182.2	209.85.175.101	TCP	80	80

จากตารางที่ 4.3ผู้ใช้งาน Boy เข้าใช้งานวันที่ 11 ธันวาคม เมื่อเวลา 14:09:10 น. จากไอพีแอดเดรส 192.168.182.2 ไปยังเว็บไซต์ปลายทางที่หมายเลข 209.85.175.101 (ซึ่งจัดอยู่ในกลุ่มของความบันเทิงมาก) โดยมีคะแนนจากการคำนวณของกลุ่มเว็บ คือ ความเป็นบันเทิง0.9 กลุ่มที่ควรให้คำแนะนำ 0.37 ความถี่ของไอพีแอดเดรส 0.88 ซึ่งเมื่อผลของแต่ละอินพุตถูกคำนวณร่วมกันจากกฎแต่ละข้อ (Defuzzification) จะได้ค่าเอาต์พุตเป็น 0.55 ซึ่งหมายถึง ควรมีการเฝ้าระวังและติดตามการใช้งาน โดยผลของการวิเคราะห์ข้อมูลจากตัวอย่างนี้เข้ากฎข้อที่ 9 และข้อที่ 10 แสดงดังรูปที่ 4.4

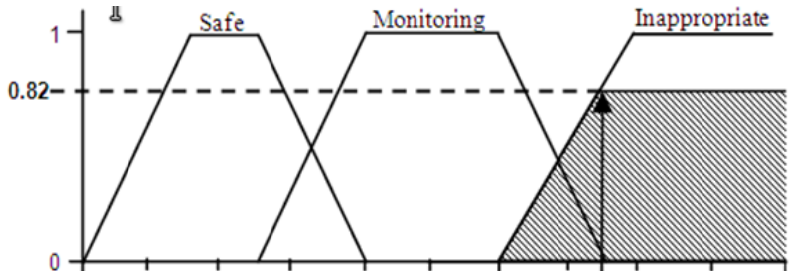


รูปที่ 4.4 ผลจากการคำนวณเข้ากฎข้อที่ 9 และ 10

ตารางที่ 4.4รายการข้อมูลใช้งานช่วงดึก

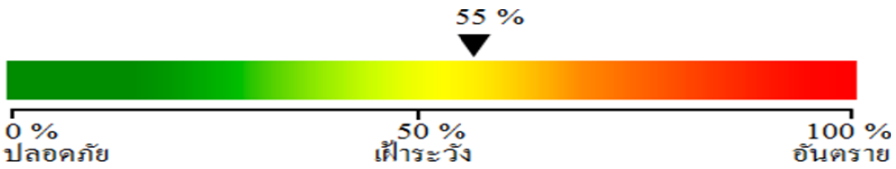
User	Month	Date	Time	IP Source	IP Destination	Protocal	Port	Freq.
Boy	Dec	11	22:06:09	192.168.182.2	209.85.175.101	TCP	80	80

ตัวอย่างการใช้งานในตารางที่ 4.4มีความเหมือนกับตัวอย่างที่ 1 ข้างต้น โดยมีความแตกต่างกันที่มีข้อมูลการใช้งานช่วงดึกในเวลาดึก คือ 22:06:09 น. ซึ่งจากผลของการวิเคราะห์ข้อมูลเข้ากฎข้อที่ 3, 4 และ 5 ได้ข้อสรุปผลการคำนวณเอาต์พุต (แสดงดังรูปที่ 4.5) มีค่าความไม่เหมาะสมของการใช้งานที่ 0.82ซึ่งหมายถึงว่าอาจจะมีการใช้งานเว็บไซต์ที่ไม่เหมาะสม (Inappropriate) ได้ และผู้ปกครองควรตรวจสอบ

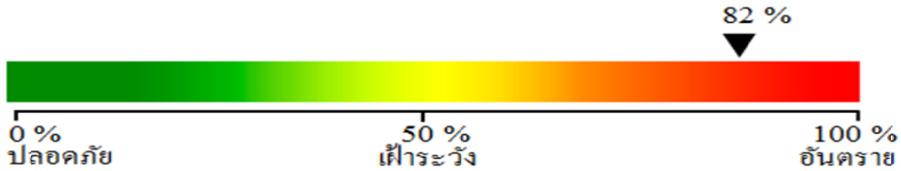


รูปที่ 4.5 ผลจากการคำนวณเข้ากฎข้อที่ 3 และ 5

จากตัวอย่างการคำนวณเชิงตัวเลขด้วยเทคนิควิธีฟัซซีข้างต้น หากนำเสนอภายในโปรแกรมสารสนเทศด้วยลักษณะของแถบสี (Color Bar) พร้อมลูกศรกำกับค่าผลลัพธ์ที่ได้ (ดูรูปที่ 4.6(a)และ (b) ประกอบ) ก็สามารถช่วยให้ผู้ใช้โปรแกรมสามารถ ทำความเข้าใจผลลัพธ์ได้รวดเร็วยิ่งขึ้น



(ผลลัพธ์ของกราฟรูปที่ 4.6)



(ผลลัพธ์ของกราฟรูปที่4.6)

รูปที่ 4.6ตัวอย่างการแสดงผลเชิงกราฟิกที่เป็นมิตรกับผู้ใช้

4.5 ผลการทดลองโปรแกรมสารสนเทศในการวิเคราะห์ข้อมูลจราจรเครือข่าย

4.5.1 แนวทางการพัฒนาโปรแกรมด้วย jfuzzlogic

การพัฒนาเป็นโปรแกรมสารสนเทศเพื่อวิเคราะห์ผลบนเครื่องของผู้ดูแลหรือผู้ปกครองนั้นมีแนวทางการพัฒนาโปรแกรมให้สามารถใช้งานได้สะดวก โดยมีซอฟต์แวร์ที่สนับสนุนการทำงานของการวิเคราะห์ข้อมูลด้วยฟัซซีลอจิก ที่สามารถนำมาใช้งานในการพัฒนาเป็นระบบสารสนเทศเพื่อการใช้งาน ในรูปแบบของโปรแกรมภาษา Java ซึ่งรองรับการหลักการวิเคราะห์ของฟัซซีลอจิก เรียกว่า jfuzzlogic[23]ซึ่งมีความสามารถในการตัดสินใจคำนวณและวิเคราะห์ผลการทำงานได้โดยสามารถแสดงตัวอย่างการพัฒนาโปรแกรมและอธิบายการทำงานได้ซึ่งมีรูปแบบของการใช้งานJfuzzylogic ในการเขียนโปรแกรมภาษา Javaและนำเข้าไฟล์ที่สนับสนุนการทำงานของเกี่ยวข้อง Jfuzzylogicคือ jFuzzyLogic_v2.1.jar เป็นการสร้างฟังก์ชัน *main ()*มีลำดับการทำงาน ดังต่อไปนี้

1) เรียกใช้งานไฟล์เพื่อนำเข้าข้อมูลไฟล์ main.javaดังแสดงในรูปที่ 4.7และกำหนดการทำงานของระบบสำหรับเรียกใช้ไฟล์ .fcl (fuzzy logic control)ร่วมกัน เพื่อแสดงเป็นรูปแบบกราฟของฟังก์ชันความเป็นสมาชิกของแต่ละอินพุตตามค่าที่กำหนดไว้ในไฟล์ parental.fclโดยมีค่าอินพุต คือ Time, Entertainment, Advice, FrequencySite และค่าเอาท์พุต Analysis ดังแสดงในรูปที่ 4.8 (ก), (ข), (ค), (ง), (จ) และ (ฉ) เป็นต้น

```
1   import net.sourceforge.jFuzzyLogic.FIS;
2   /**
3    * Test Parental Control System an FCL file
4    */
5   public class main {
6       public static void main(String[] args) throws Exception {
7           // Load from 'FCL' file
8           String fileName = "fcl/parental.fcl";
9          // String fileName = "fcl/tipper.fcl";
10          FIS fis = FIS.load(fileName,true);
11          // Error while loading?
12          if( fis == null ) {
13              System.err.println("Can't load file: '"
14                                      + fileName + "'");
15              return;
16          }
17
18  // Show
19          fis.chart();
20
21          // Set inputs
22          fis.setVariable("Time", 23.4);
23          fis.setVariable("Entertainment", 0.8);
24          fis.setVariable("Advice", 0.5);
25          fis.setVariable("FrequencySite", 0.3);
26
27          // Evaluate
28          fis.evaluate();
29
30          // Show output variable's chart
31          fis.getVariable("Analysis").chartDefuzzifier(true);
32
33          // Print ruleSet
34          System.out.println(fis);
35      }
36  }
37
```

รูปที่ 4.7การสร้างไฟล์เพื่อทดสอบโปรแกรมการวิเคราะห์ข้อมูล

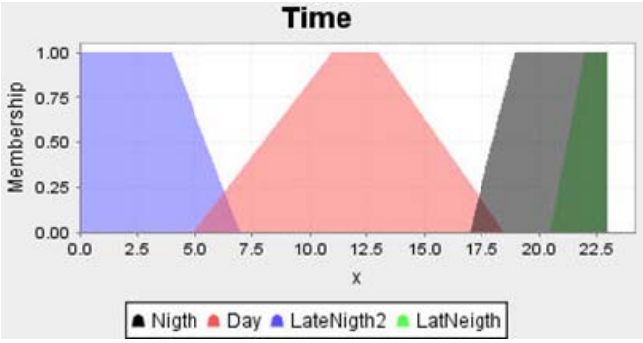
2) ฟังก์ชัน fis.setVariable สำหรับนำค่าอินพุตที่กำหนดไว้ เช่น "Time" = 23.4 (23.4 เป็นค่าจำนวนเต็มเทียบได้กับค่าเวลา คือ 23:40 น.) "Entertainment" = 0.8(0.8 เป็นค่าที่กำหนดไว้สำหรับความบันเทิงมาก) "Advice" = 0.5 (เป็นค่าที่กำหนดไว้สำหรับความเหมาะสมสำหรับทุกชวงวัย) และ "FrequencySite" = 0.3 (เป็นค่าที่กำหนดไว้

สำหรับความจำนวนความถี่ที่ใช้งาน เช่น 80 ครั้ง) เป็นต้น และฟังก์ชัน fis.evaluate() เพื่อเข้าสู่กระบวนการวิเคราะห์ตามกฎเกณฑ์ที่กำหนดไว้ 10 ข้อ ในไฟล์ parental.fcl ดังแสดงในรูปที่ 4.9

3) ฟังก์ชัน fis.getVariable("Analysis").chartDefuzzifier(true) สำหรับนำค่าที่ได้จากการวิเคราะห์ร่วมกับค่าความเป็นสมาชิกของเอาท์พุต "Analysis" เข้าสู่กระบวนการ Defuzzification และนำผลลัพธ์ที่ได้ออกมาแสดงเป็นกราฟค่าการวิเคราะห์ด้วยคำสั่ง System.out.println(fis) แสดงดังรูปที่ 4.10

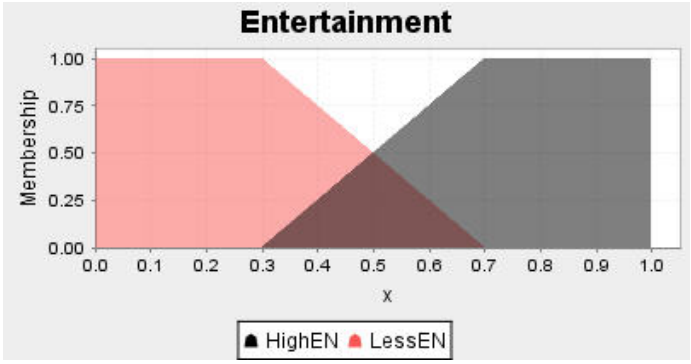
```
1   FUNCTION_BLOCK parental
2   VAR_INPUT                   // Define input variables
3           Entertainment : REAL;
4           Time : REAL;
5           Advice  : REAL;
6           FrequencySite  : REAL;
7   END_VAR
8
9   VAR_OUTPUT                  // Define output variable
10          Analysis : REAL;
11  END_VAR
```

รูปที่ 4.8(ก) การประกาศค่าตัวแปล FUNCTION_BLOCK parentalสำหรับการทำงาน



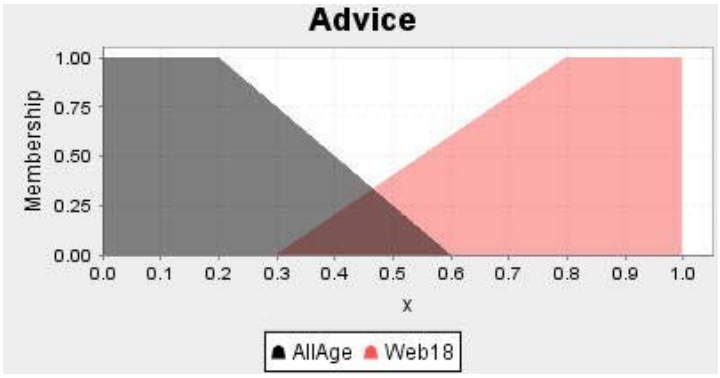

```
12  FUZZIFY Time        // Fuzzify input variable 'Time'
13          TERM  LateNigth2 := (0, 1) (4, 1) (7,0) ;
14          TERM Day :=  (5, 0) (11, 1) (13, 1) (18.5, 0) ;
15          TERM Nigth := (17, 0) (19,1) (21,1);
16          TERM LatNeigth := (20.5, 0) (22,1) (23.5,1);
17  END_FUZZIFY
```

รูปที่ 4.8(ข) กำหนดกราฟอินพุตฟังก์ชั่นความเป็นสมาชิกของเวลา



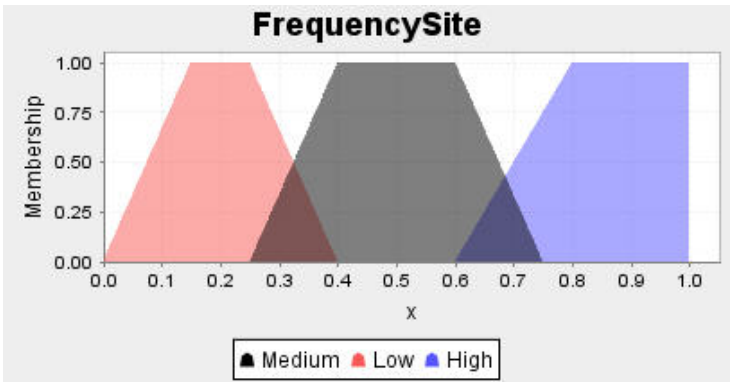

```
18    FUZZIFY Entertainment          // Fuzzify input variable 'Entertainment'
19                TERM LessEN := (0, 0.1) (0.3, 0.1) (0.7, 0) ;
20                TERM HighEN := (0.3, 0) (0.7, 0.1) (1, 0.1) ;
21                //TERM excellent := (0.6, 0) (0.9, 0.1);
22    END_FUZZIFY
```

รูปที่ 4.8(ค) กำหนดกราฟอินพุตฟังก์ชั่นความเป็นสมาชิกของความบันเทิง



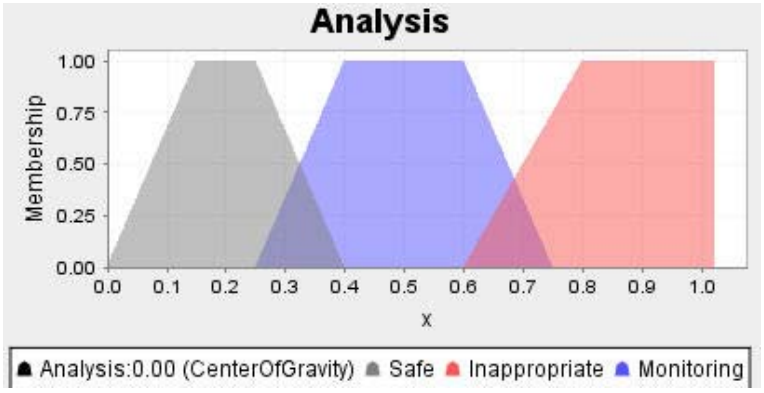

```
23    FUZZIFY Advice                 // Fuzzify input variable 'Advice'
24                TERM AllAge := (0, 0.1) (0.2, 0.1) (0.6, 0) ;
25                TERM Web18 := (0.3, 0) (0.8, 0.1) (1, 0.1) ;
26    END_FUZZIFY
```

รูปที่ 4.8(ง) กำหนดกราฟอินพุตฟังก์ชั่นความเป็นสมาชิกของความเหมาะสมกับช่วงวัย




```
27      FUZZIFY FrequencySite          // Fuzzify input variable 'FrequencySite'
28                TERM Low := (0, 0) (0.15, 0.1) (0.25, 0.1) (0.4, 0) ;
29                TERM Medium := (0.25, 0) (0.4, 0.1) (0.6, 0.1) (0.75,0) ;
30                TERM High := (0.6, 0) (0.8, 0.1) (1, 0.1) ;
31      END_FUZZIFY
```

รูปที่ 4.8(จ) กำหนดกราฟอินพุตฟังก์ชั่นความเป็นสมาชิกของความถี่การใช้งาน

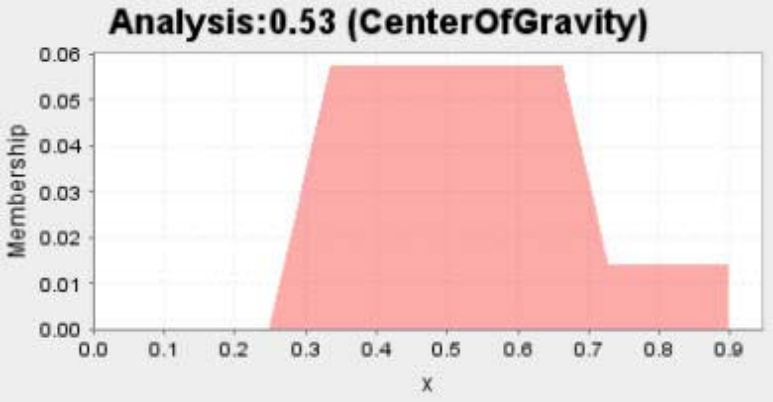



```
32      DEFUZZIFY Analysis             // Defzzzify output variable 'Analysis'
33                TERM Safe := (0, 0) (0.15, 0.1) (0.25, 0.1) (0.4, 0) ;
34                TERM Monitoring := (0.25, 0) (0.4, 0.1) (0.6, 0.1) (0.75,0) ;
35                TERM Inappropriate := (0.6, 0) (0.8, 0.1) (1, 0.1) ;
36                METHOD : COG;     // Use 'Center Of Gravity' defuzzification method
37                DEFAULT := 0;     // Default value is 0 (if no rule activates defuzzifier)
38      END_DEFUZZIFY
```

รูปที่ 4.8(ฉ) กำหนดกราฟเอาท์พุตฟังก์ชั่นความเป็นสมาชิกของการวิเคราะห์

```
39  RULEBLOCK No1
40  AND : MIN;// Use 'min' for 'and' (also implicit use 'max' for 'or' to fulfill DeMorgan's Law)
41  ACT : MIN;          // Use 'min' activation method
42  ACCU : MAX;         // Use 'max' accumulation method

43      RULE 1 :IF Time IS LatNeigth AND Entertainment IS LessEN AND Advice IS AllAge
                AND FrequencySite IS NOT High THEN Analysis IS Safe;
44      RULE 2 :IF Time IS LatNeigth AND Entertainment IS HighEN AND Advice IS AllAge
                AND FrequencySite IS High THEN Analysis IS Monitoring;
45      RULE 3 : IF Time IS LatNeigth AND Entertainment IS NOT LessEN AND Advice IS
                Web18AND FrequencySite IS NOT Low THEN Analysis IS Inappropriate;
46      RULE 4 : IF Time IS Nigth AND Entertainment IS HighEN AND Advice IS AllAge AND
                FrequencySite IS NOT Low THEN Analysis IS Monitoring;
47      RULE 5 : IF Time IS Nigth AND Entertainment IS HighEN AND Advice IS Web18 AND
                FrequencySite IS HighTHEN Analysis IS Inappropriate;
48      RULE 6 : IF Time IS Nigth AND Entertainment IS LessEN AND Advice IS AllAge AND
                FrequencySite IS High THEN Analysis IS Monitoring;
49      RULE 7 : IF Time IS Day AND Entertainment IS LessEN AND Advice IS AllAge THEN
                Analysis IS Safe;
50      RULE 8 : IF Time IS Day AND Entertainment IS LessEN AND Advice IS Web18 AND
                FrequencySite IS NOTHigh THEN Analysis IS Monitoring;
51      RULE 9 : IF Time IS Day AND Entertainment IS HighEN AND Advice IS Web18 AND
                FrequencySite IS HighTHEN Analysis IS Inappropriate;
52      RULE 10 : IF Time IS Day AND Entertainment IS HighEN AND Advice IS AllAge AND
                FrequencySite IS High THEN Analysis IS Monitoring;
53  END_RULEBLOCK
    END_FUNCTION_BLOCK
54
55
```

รูปที่4.9กฎเกณฑ์การวิเคราะห์ข้อมูลอินพุตจากไฟล์ main.java

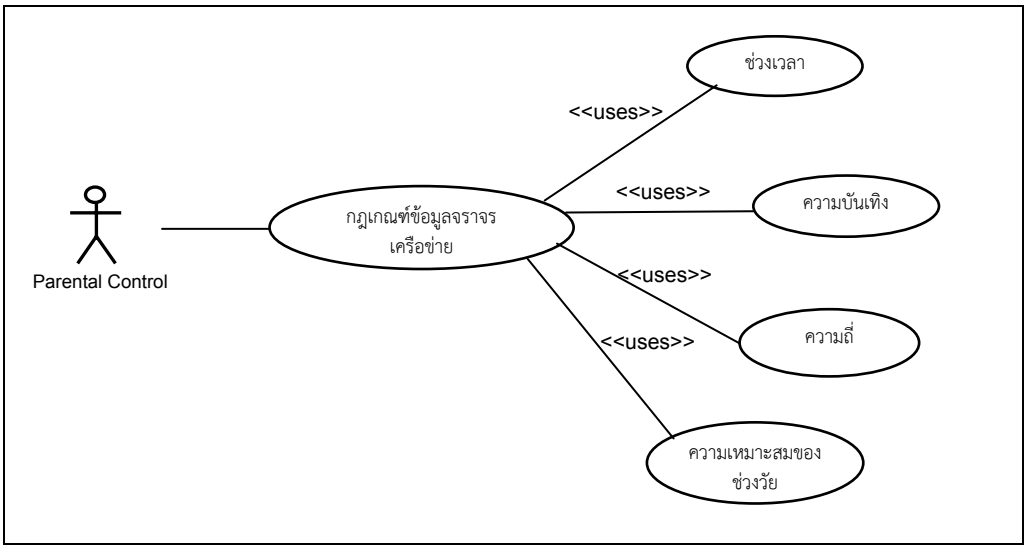


รูปที่4.10กราฟแสดงผลการวิเคราะห์ข้อมูลจากโปรแกรม

4.5.2 แนวทางการสร้างกฎเกณฑ์ของผู้ใช้งาน

กฎเกณฑ์สำหรับการวิเคราะห์ข้อมูลเพื่อให้ผู้ดูแลหรือผู้ปกครองสามารถเข้าใจได้ง่ายโดยการสร้างกฎเกณฑ์สามารถกำหนดเกณฑ์พื้นฐานของการวิเคราะห์ที่ตอบสนองต่อการใช้งานโดยทั่วไปเพื่อตรวจสอบรายการใช้งานหรือผลลัพธ์ในลักษณะต่างๆ เช่น ตรวจสอบข้อมูลเฉพาะช่วงเวลาเฉพาะผู้ใช้งาน หรือเฉพาะเว็บที่เข้าใช้งานบ่อยที่สุด เป็นต้น

ในงานวิจัยนี้ขอยกตัวอย่างแนวทางการพัฒนาโปรแกรมสารสนเทศโดยจำลองการสร้างกฎเกณฑ์ในการวิเคราะห์ ระบบของ Use Case Diagram ดังแสดงในรูปที่ 4.9 และหน้าต่างโปรแกรมดังแสดงในรูปที่ 4.11ที่ผู้ปกครองหรือผู้ดูแลต้องป้อนข้อมูลใหม่ ซึ่งประกอบด้วยไอพีแอดเดรสปลายทางที่ไม่ได้อยู่ในกลุ่มใดๆหรือไอพีแอดเดรสใหม่ ซึ่งจำเป็นต้องรู้จักเว็บปลายทางนั้นก่อนจึงสามารถแบ่งกฎการแยกแยะได้ เช่น ไอพีแอดเดรสปลายทาง 69.171.228.11เป็นเว็บไซต์ www.facebook.com ผู้ใช้สามารถกำหนดกฎเกณฑ์ได้เอง เช่น เว็บไซต์นี้มีความเป็นบันเทิงเท่ากับ 0.6ควรให้คำแนะนำเท่ากับ 0.4และความถี่ในการเข้าใช้งานเท่ากับ 0.8เป็นต้น



รูปที่ 4.11 Use Case Diagram การแบ่งเกณฑ์การวิเคราะห์ข้อมูล

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทนำต้นเรื่อง

ในบทนี้จะกล่าวถึงบทสรุปของงานวิจัยในวิทยานิพนธ์นี้ ที่ต้องการศึกษากลไกของระบบจัดเก็บข้อมูลจราจรเครือข่ายทางคอมพิวเตอร์ ที่ใช้ซอฟแวร์โอเพ่นซอร์สทำงานบนเครื่องคอมพิวเตอร์แม่ข่าย เพื่อเป็นแนวทางในการพัฒนาระบบจัดเก็บข้อมูลจราจรเครือข่ายภายในบ้านพักอาศัย โดยใช้อุปกรณ์แอกเซสพ้อยน์เราเตอร์ที่เป็นคอมพิวเตอร์แบบฝังตัวในการทดลอง และแนวทางการใช้ฟัซซีลอจิกวิเคราะห์ข้อมูลที่คลุมเคลืออย่างชาญฉลาดเพื่อแสดงผลบนเครื่องผู้ปกครองหรือผู้ดูแล ซึ่งในที่นี้ผู้วิจัยได้เสนอแนะการจัดการปัญหาข้างต้นโดยสามารถแยกสรุปปัญหาวิจัยออกเป็น 3 ส่วน ดังต่อไปนี้

5.2 สรุปสิ่งที่นำเสนอในวิทยานิพนธ์

5.2.1 การใช้คอมพิวเตอร์แบบฝังตัวจัดเก็บข้อมูลจราจรเครือข่าย

เป็นการนำเอาแนวคิดของระบบจัดเก็บข้อมูลจราจรเครือข่ายที่ใช้เครื่องแม่ข่าย มาเป็นแนวทางในการพัฒนาระบบสำหรับบ้านพักอาศัย โดยเลือกใช้คอมพิวเตอร์แบบฝังตัวเป็นอุปกรณ์แอกเซสพ้อยน์เราเตอร์ ยี่ห้อ Asus รุ่น WL500GP V2 และซอฟต์แวร์ที่จำเป็นสำหรับการติดตั้งระบบจัดเก็บข้อมูลจราจรเครือข่าย มาใช้งานแทนเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งมีรายละเอียดดังที่กล่าวไว้ในบทที่ 3 แสดงให้เห็นประสิทธิภาพของอุปกรณ์ทำให้ช่วยประหยัดค่าใช้จ่ายด้านพลังงานไฟฟ้าและราคาของอุปกรณ์อย่างชัดเจน ดังรายละเอียดการเปรียบเทียบอุปกรณ์ในบทที่ 4 ข้อที่ 4.6 ซึ่งตัวอุปกรณ์สามารถใช้งานได้ง่าย โดยผู้ใช้ไม่จำเป็นต้องมีทักษะด้านคอมพิวเตอร์มากนักก็สามารถดูแลและใช้งานได้อย่างสะดวกและคุ้มค่า เป็นต้น

5.2.2 การนำฟัซซีลอจิกมาช่วยในการวิเคราะห์ข้อมูลจราจรเครือข่าย

เป็นการนำเทคนิควิธีฟัซซีลอจิกมาช่วยในการแก้ปัญหาความซ้ำซ้อนไม่ยืดหยุ่นหรือความคลุมเครือในการตัดสินใจเพื่อวิเคราะห์ข้อมูล ดังที่ได้ยกตัวอย่างข้อมูลด้านเวลา เพื่อช่วยตัดสินใจค่าความดึกของการใช้งานอินเทอร์เน็ตเป็นต้น และยังสามารถนำมาใช้ในการพัฒนาระบบการวิเคราะห์ข้อมูลการเข้าใช้งานอินเทอร์เน็ต โดยแบ่งกลุ่มของไอพีแอดเดรสปลายทาง ซึ่งประกอบด้วยข้อมูลด้านเวลาที่เข้าใช้ ความบันเทิง ความเหมาะสมของช่วงวัย ความถี่ในการใช้งานแต่ละเว็บ และการกำหนดค่าความเป็นสมาชิก ซึ่งมีรายละเอียดดังที่กล่าวไว้ในหัวข้อที่ 4.4 โดยเนื้อหาในส่วนนี้

ได้นำเสนอเป็นบทความวิจัยชื่อ “การวิเคราะห์ข้อมูลจราจรเครือข่ายด้วยฟัซซีลอจิกเพื่อตรวจการใช้อินเทอร์เน็ตบุตรธิดา” และได้นำเสนอในการประชุมวิชาการระดับชาติด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ครั้งที่ 7 (NCCIT 2011), กรุงเทพ, ประเทศไทย, 11-12 พฤษภาคม 2554

5.2.3 แนวคิดของการพัฒนาโปรแกรมสารสนเทศของข้อมูลจราจรเครือข่าย

เป็นการนำเสนอแนวความคิดในการนำเทคนิคการวิเคราะห์ข้อมูลด้วยเทคนิควิธีฟัซซีลอจิกที่นำเสนอข้างต้น มากพัฒนาต่อยอดให้เป็นโปรแกรมสารสนเทศ โดยยกตัวอย่างของการนำซอฟต์แวร์สนับสนุน Jfuzzylogic เข้ามาใช้ประมวลผลกฎเกณฑ์แบบฟัซซีกับโปรแกรมที่พัฒนาขึ้นด้วยภาษา Java ซึ่งมีรายละเอียดดังที่กล่าวไว้ในหัวข้อที่ 4.5

5.3 ปัญหาและอุปสรรค

5.3.1 ปัญหาในการแบ่งกฎเกณฑ์สำหรับฟัซซีลอจิก

จากการทดลองนำฟัซซีลอจิกมาใช้ในการวิเคราะห์ข้อมูลดังที่ได้กล่าวสรุปไปแล้วในข้อที่ 5.2.2 นั้น โดยกำหนดกฎเกณฑ์ของการวิเคราะห์เบื้องต้นซึ่งพบอุปสรรคของการวิเคราะห์ข้อมูล เช่น 1) มาตรฐานของผู้ปกครองไม่เท่าเทียมกัน ทำให้กฎเกณฑ์ที่กำหนดขึ้นสำหรับการวิเคราะห์ผลจำเป็นต้องปรับเปลี่ยนรูปแบบการให้คะแนนเพื่อความยืดหยุ่นสำหรับผู้ปกครอง 2) ขอมูลของเว็บปลายทางที่ไม่สามารถระบุได้เนื่องจากมีข้อมูลที่หลากหลายซึ่งเป็นหมายเลขปลายทางเดียวกัน เช่น www.manager.co.th/Entertainment และ www.manager.co.th/Game เป็นต้น และ 3) ผู้ปกครองหรือผู้ดูแลจำเป็นต้องตรวจสอบเว็บไซต์ของไอพีแอดเดรสปลายทางก่อน เพื่อตรวจสอบข้อมูลการให้บริการและกำหนดระดับของเกณฑ์ต่างๆ เช่น ความบันเทิงหรือความไม่เหมาะสม ตามที่ต้องการได้

5.3.2 ปัญหาการนำไปใช้งาน

การวิเคราะห์ข้อมูลจราจรเครือข่ายในงานวิจัยนี้ มุ่งเน้นที่จะ “เฝ้าตรวจ” และ “วิเคราะห์” ข้อมูลการใช้งานอินเทอร์เน็ตย้อนหลังของบุตร/ธิดาภายในบ้านพักอาศัยในรูปแบบที่ง่ายต่อการทำความเข้าใจเท่านั้น ดังนั้น จึงไม่ครอบคลุมไปถึงคุณลักษณะในการ “ป้องกันหรือปิดกั้น” การใช้งานเว็บไซต์ที่อาจเป็นอันตรายแต่อย่างใด

5.4 ข้อเสนอแนะและงานในอนาคต

หากมีหน่วยงานหรือองค์กรที่ดูแลด้านการแบ่งแยกของเว็บไซต์ต่างๆ ได้ตามเกณฑ์ต่างๆ กัน เช่น ระดับของความบันเทิง หรือระดับของความรุนแรงในเนื้อหา เป็นต้น ก็สามารถจะช่วยลดภาระงานในด้านการตัดสินหรือประเมินเกณฑ์สำหรับผู้ปกครองได้สะดวกมากขึ้น

บรรณานุกรม

[1] คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550, 2552.

[2] Thai Web Nanny. (Online) Available, http://4ever.thaiware.com/main/info.php?id=8121, September 2009.

[3] ICT HOUSE KEEPER Program, (Online) Available,www.icthousekeeper.com, February 2010.

[4] Embedded Linux, (Online) Available, http://en.wikipedia.org/wiki/Embedded_linux,February 2010.

[5] ธนัชพัทธ์ กรีธาสันต์,“พัฒนาระบบให้บริการคิดราคาอินเตอร์เน็ตตามระยะเวลาใช้งาน”,สารนิพนธ์วิทยาศาสตร์มหาบัณฑิต, มหาวิทยาลัยสงขลานครินทร์,2552.

[6] Hardware Log SRAN, (Online) Available,http://http://www.gbtech.co.th/th/product/usm,.

[7] Hardware Log Sniff-Log, (Online) Available,http://www.sgc.co.th/sniff_log.php, March 2010.

[8] Upgrade Firmware Router, (Online) Available,http://www.sys2u.com/xpert/viewtopic.php?f=3&t=62,February 2010.

[9] Free RADIUS, (Online) Available, http://freeradius.org,June 2010.

[10] B. Andy, &T. Nicolas, “OpenWRT”, (Online) Available, www.openwrt.org, April 2010.

[11] พยุง มีสัจ,“ระบบฟัซซี่และโครงข่ายประสาทเทียม”, เอกสารประกอบการสอนคณะเทคโนโลยีสารสนเทศ, สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ, 2551.

[12] Y. John, “Fuzzy System”, Prentice-Hell : New Jersey, 1999.

[13] สัมพันธ์ ลิ้มปิติ,“การศึกษาเปรียบเทียบระบบการจัดการเครือข่ายไร้สาย”, สารนิพนธ์วิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยสงขลานครินทร์, 2552.

[14] ทองรัก พัวพรสวรรค์, “การออกแบบและสร้างอินเวอร์เตอร์เฟสเดียวต่อเข้ากับกริดระบบไฟฟ้าโดยใช้วิธีคุมแบบฟัซซีลอจิก”, วิทยานิพนธ์วิศวกรรมศาสตร์มหาบัณฑิต, มหาวิทยาลัยเชียงใหม่, 2547.

[15] สุรกฤษฎ์ นาทธราดล, “การประยุกต์ใช้กระบวนการลำดับชั้นเชิงวิเคราะห์ความคลุมเครือในการคัดเลือกผู้ส่งมอบของอุตสาหกรรมยานยนต์และอิเล็กทรอนิกส์”, วิทยานิพนธ์วิศวกรรมศาสตร์มหาบัณฑิต,มหาวิทยาลัยเชียงใหม่, 2551.

[16] S. Lekcharoen and C. C. Fung, “An Adaptive Fuzzy Control Traffic Shaping Scheme over Wireless Networks,” Proc. of Asia-Pacific Conf. on Comm., Bangkok, Thailand, Oct., 2007.

[17] A. Rahman, P. Kennedy, A. Simmonds and J. Edwards, “Fuzzy Logic Based Modelling and Analysis of Network Traffic,” IEEE Int. Conference,Sydney, Australia,2008.

[18] J. Mohammed, Apache Server2 Bible. New York : Hungry Minds,2002.

[19] Chillispot Main Page, (Online) Available, www.chillispot.info, March 2010.

[20] ภูวดล ด่านระหาญ,“Syslog-ng”, (ออนไลน์) เข้าถึงได้จาก, www.thaicert.nectec.or.th/paper/unix_linux/syslog-ng.php, May 2010.

[21] Coova-Clilli, (Online) Available, http://coova.org/CoovaChilli, July 2010.

[22] พระราชบัญญัติภาพยนตร์และวีดิทัศน์ พ.ศ. 2551, ราชกิจจานุเบกษา เล่ม 125 ตอนที่ 42 ก มาตรา 26.

[23] jFuzzyLogic, (Online) Available,http://jfuzzylogic.sourceforge.net,Fabruay 2011.

[24] A. Paul, &P. Larry, “Linksys WRT54GL Ultimate Hacking”, United States :Syngress Publishing, 2007.

[25] C. Ben, “Artificial Intelligence Illuminated”, 1 st ed., Malloy : Jones and Bartlett, 2004.

[26] GREGOR, N. PURDY, “Linux Iptables Pocket Reference”, 1 st ed., United States : O’Reilly Media,2004.

ภาคผนวก

ภาคผนวก ก : ผลงานวิจัยตีพิมพ์

สายัณ อินชะนะ สุนทร วิทูสุรพจน์ และ สมชัย หลิมศิโรรัตน์. 2553. การวิเคราะห์ข้อมูลจราจรเครือข่ายด้วยฟัซซีลอจิกเพื่อตรวจการใช้อินเทอร์เน็ตบุตรธิดา. การประชุมทางวิชาการระดับชาติ ด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ครั้งที่ 7, 11-12 พฤษภาคม 2554.

การวิเคราะห์ข้อมูลจราจรเครือข่ายด้วยฟัซซีลอจิกเพื่อตรวจการใช้อินเทอร์เน็ตบุตรธิดา

Fuzzy Logic Based Analysis of Network Traffic for Parental Control

สายัณ อินชะนะ (Sayan Inchana)[1], สุนทร วิทูสุรพจน์ (Suntorn Witosurapot)[2]

และสมชัย หลิมศิโรรัตน์ (Somchai Limsiroratana)[3]

[1,2,3] หลักสูตรมหาบัณฑิตการจัดการเทคโนโลยีสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์

in_say@bunga.pn.psu.ac.th, wsuntorn@coe.psu.ac.th, somchai@coe.psu.ac.th

บทคัดย่อ

บทความนี้เสนอแนะให้นำเทคนิคฟัซซีลอจิกเข้ามาช่วยการวิเคราะห์ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ เพื่อประเมินความเหมาะสมในการใช้อินเทอร์เน็ตของบุตรธิดาจากบ้านพักอาศัย เนื่องจากมีลักษณะเด่นหลายประการได้แก่ ก) ความยืดหยุ่นในการปรับเปลี่ยนกฎเกณฑ์การเฝ้าตรวจ ข) ความสะดวกในการประเมินจากกฎเกณฑ์จำนวนมาก และ ค) ความเป็นมิตรต่อผู้ใช้ในการแสดงผลลัพธ์การประเมิน ในที่นี้ได้แสดงให้เห็นว่าควรนำข้อมูลบางส่วนของไฟล์ข้อมูลจราจรฯ ที่ได้จากเราเตอร์ไปใช้อย่างไร จึงจะเพียงพอต่อการสร้างตัวแปรและกฎเกณฑ์ฟัซซีต่างๆ ที่ใช้ในการตัดสินใจพร้อมยกตัวอย่างการวิเคราะห์ข้อมูลจริงและแสดงผลเชิงกราฟิกที่ง่ายต่อการทำความเข้าใจ

คำสำคัญ: ข้อมูลจราจร ฟัซซีลอจิก การควบคุมโดยผู้ปกครอง

Abstract

This paper advocates the use of the fuzzy logic in the analysis of network traffic for the parental control from residential networks. This is due to the salient features such as a) flexibility in the adjustment of monitoring rules b) applicability for evaluation on a number of rules and c) friendliness for showing evaluation results to users in a comprehensive manner. In this paper, we suggest how the partial data of network traffic log taken from the router should be used so that fuzzy variables and rules can be adequately defined. In addition, we give examples of analysis based on actual data and show graphical results for ease of understanding.

Keyword: Network traffic, Fuzzy logic, Parental Control.

1. บทนำ

ด้วยสาเหตุที่การใช้งานอินเทอร์เน็ตของบุตรธิดาจากบ้านพักอาศัย (Residential Networks) มีอัตราการเพิ่มสูงขึ้นอย่างรวดเร็ว จนอาจทำให้ผู้ปกครองเกิดความวิตกกังวลและประสงค์ที่จะตรวจสอบเพื่อเฝ้าระวังการใช้งานอินเทอร์เน็ตที่ไม่เหมาะสม (ตามเกณฑ์ที่ตนเองต้องการ) อย่างไรก็ตาม วิธีการติดตั้งซอฟต์แวร์ควบคุมการใช้งานเว็บที่ไม่เหมาะสม (เช่น โปรแกรม ICT Housekeeper [1] เป็นต้น) มีข้อด้อยที่ผู้ใช้คอมพิวเตอร์บนเครื่องนั้นๆ หากมีทักษะด้านคอมพิวเตอร์บ้างก็สามารถหลีกเลี่ยงหรือยกเลิกการป้องกันดังกล่าวได้ วิธีการวิเคราะห์จากไฟล์ข้อมูล (Log File) จราจรทางคอมพิวเตอร์ (Network Traffic) จึงมีความน่าสนใจมากกว่า เนื่องจากข้อมูลจราจรฯ ทั้งหมดในเครือข่ายคอมพิวเตอร์ของบ้านพักอาศัยจะบันทึกเป็นไฟล์แบบเวลาจริง จัดเก็บอยู่ภายในอุปกรณ์เราเตอร์ (Router) และอนุญาตสิทธิ์ในการเข้าถึงไฟล์เฉพาะกับผู้ดูแลระบบเท่านั้น จึงหลีกเลี่ยงข้อด้อยที่พบในวิธีการแรกได้ แต่อาจจะประสบปัญหาความยุ่งยากในการวิเคราะห์หรือแปลความข้อมูลจราจรทางคอมพิวเตอร์ที่จัดเก็บอยู่ภายในไฟล์นั้นได้

การแก้ปัญหาความยุ่งยากข้างต้นโดยการพัฒนาโปรแกรมสารสนเทศด้วยเทคนิคการโปรแกรมที่ทำงานอยู่บนพื้นฐานของเงื่อนไขทางตรรกะ (If-else statements) โดยลำพังนั้นจะสร้างความซับซ้อนในการโปรแกรม เนื่องจากจำนวนของกฎเกณฑ์ที่นำมาใช้ประกอบการตัดสินใจต่างๆ จากข้อมูลหลายด้านที่นำมาพิจารณาร่วมกัน (ซึ่งอาจมีจำนวนมากได้) และรูปแบบของการตัดสินใจที่ไม่ได้อยู่เพียงในลักษณะของตรรกะแบบทวิภาค (ค่าจริงหรือค่าเท็จ) เท่านั้น ในบทความนี้จะแสดงให้เห็นว่าการนำเทคนิควิธีฟัซซีลอจิก (Fuzzy Logic) [2] เข้ามาใช้งานร่วมในการ

พัฒนาโปรแกรมสารสนเทศ ไม่เพียงสามารถหลีกเลี่ยงข้อจำกัดที่กล่าวถึงข้างต้นได้เท่านั้น แต่ยังช่วยให้สามารถนำกฎเกณฑ์แบบคลุมเครือต่างๆ ของผู้ปกครอง เข้ามาร่วมพิจารณากันได้โดยสะดวก และง่ายต่อการปรับเปลี่ยนในภายหลังด้วย

บทความนี้ได้จัดวางโครงสร้างไว้ดังต่อไปนี้ ในหัวข้อที่ 2 เป็นการทบทวนวรรณกรรมที่เกี่ยวข้องในการนำเทคนิควิธีฟัซซีไปใช้ในงานเกี่ยวกับจราจรเครือข่ายคอมพิวเตอร์ ในหัวข้อที่ 3 จึงเริ่มต้นด้วยการให้รายละเอียดของเทคนิควิธีฟัซซีลอจิก จากนั้นจึงเป็นแนวคิดในการกำหนดฟังก์ชันความเป็นสมาชิกและกฎของฟัซซีลอจิกที่นำเสนอขึ้น เพื่อใช้กับข้อมูลจราจรเครือข่ายคอมพิวเตอร์ ในหัวข้อที่ 4 จึงเป็นการวิเคราะห์ข้อมูลตัวอย่างด้วยเทคนิคฟัซซีลอจิกตามที่ได้กล่าวผ่านมา และในหัวข้อที่ 5 เป็นการสรุปและวิจารณ์ผลบทความ

2. วรรณกรรมที่เกี่ยวข้อง

แม้ว่าเทคนิควิธีฟัซซีลอจิกจะพบมากในงานควบคุมต่างๆ แต่การนำมาประยุกต์ใช้ที่เกี่ยวข้องกับข้อมูลเครือข่ายคอมพิวเตอร์พบว่ายังมีอยู่น้อย ตัวอย่างเช่น

- S. Lekcharoen และ C. C. Fung [3] ได้นำเสนอการประยุกต์เทคนิควิธีฟัซซีลอจิก เพื่อจุดประสงค์ในการปรับแต่งข้อมูลจราจรเครือข่ายฯ (Traffic Shaping) สำหรับการบริหารจัดการหน่วยความจำบัฟเฟอร์ที่อยู่ภายในอุปกรณ์เครือข่าย ผลจากการจำลองแบบแสดงให้เห็นว่า ได้ผลลัพธ์ที่มีประสิทธิภาพดีกว่าระบบพื้นฐานทั่วไปมาก
- Rahman และคณะ [4] ได้เสนอแนะการนำเทคนิควิธีฟัซซีลอจิกเข้ามาใช้ในการวิเคราะห์แบบจำลองข้อมูลจราจรที่เป็นจริงของเครือข่ายคอมพิวเตอร์แบบบรอดแบนด์ความเร็วสูง แทนการใช้แบบจำลองทางคณิตศาสตร์ที่สร้างจากสถิติของแพ็กเก็ตข้อมูลด้านต่างๆ เช่น ค่าระยะเวลาในการเดินทางมาถึงของแพ็กเก็ตข้อมูล หรือค่าระยะเวลาไปกลับโดยรวม (Round-trip time) เป็นต้น ซึ่งใช้เวลาดำเนินการนานกว่ามาก จึงเหมาะสมกับการใช้งานในเครือข่ายความเร็วต่ำถึงปานกลางเท่านั้น

ดังนั้น งานวิจัยทั้งสองข้างต้นเสนอแนะการประยุกต์ใช้เทคนิควิธีฟัซซีลอจิกเพื่อการวิเคราะห์ข้อมูลจราจรเครือข่ายฯ กับอุปกรณ์ที่อยู่ภายในเครือข่ายคอมพิวเตอร์ ซึ่งแตกต่างไปจากงานที่นำเสนอในบทความนี้ ที่มุ่งวิเคราะห์ประวัติการใช้งานเครือข่ายฯ ของผู้ใช้งานเป็นสำคัญ

3. วิธีการดำเนินการวิจัย

3.1 ข้อมูลจราจรเครือข่ายคอมพิวเตอร์

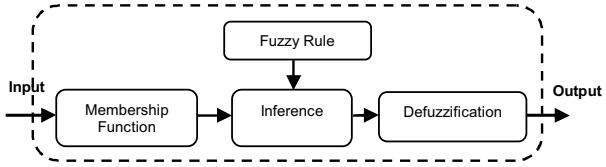
แม้ว่า พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะได้กำหนดให้หน่วยงานต้องเก็บไฟล์บันทึกข้อมูลจราจรเครือข่ายคอมพิวเตอร์เพื่อการตรวจสอบย้อนหลังได้ แต่ยกเว้นสำหรับเครือข่ายบ้านพักอาศัย อย่างไรก็ตาม ในงานวิจัยนี้เสนอให้ใช้กลไกทำงานด้านซอฟต์แวร์เพื่อการเก็บบันทึกข้อมูลจราจรฯ ข้างต้นเช่นกัน แต่สามารถดำเนินการให้จัดเก็บแบบเบ็ดเสร็จอยู่ภายในอุปกรณ์เราเตอร์บางรุ่นได้โดยตรง เช่น อุปกรณ์ Linksys รุ่น WRT54GL หรือ ASUS รุ่น WL500GP V2 เป็นต้น (ซึ่งขอยกเว้นการกล่าวถึงรายละเอียดในที่นี้) อย่างไรก็ตาม ในการวิเคราะห์ข้อมูลที่นำเสนอในบทความนี้ ต้องนำมาประมวลผลเบื้องต้น (Pre-processing) เพื่อดึงเฉพาะสดมภ์ที่ต้องการมาจากรายการภายในไฟล์บันทึกข้อมูลจราจรฯ ที่ได้จากอุปกรณ์เราเตอร์ และจัดเก็บในรูปแบบ (ดูรูปที่ 1) ดังต่อไปนี้ 1) ชื่อผู้ใช้ (User) 2) วันที่ใช้งาน (Date) 3) เวลาที่เข้าใช้ (Time) 4) ไอพีแอดเดรสต้นทาง (Source IP) 5) ไอพีแอดเดรสปลายทาง (Destination IP) 6) โพรโตตอลสื่อสาร (Protocol) 7) พอร์ตสื่อสาร (Dest. Port) ซึ่งโปรแกรมวิเคราะห์ผลจะคัดเลือกสดมภ์ที่สนใจเพื่อนำไปประมวลผลต่อไป

User	Date	Time	Source IP	Destination IP	Protocal	Dest. Port
boy	Dec 13	21:56:46	192.168.182.3	207.46.49.133	TCP	80
boy	Dec 13	21:56:24	192.168.182.3	72.14.203.139	TCP	80
boy	Dec 13	21:56:23	192.168.182.3	72.14.203.139	TCP	80
boy	Dec 13	21:56:23	192.168.182.3	58.181.243.137	TCP	80

ภาพที่ 1: ตัวอย่างข้อมูลที่ถูกจัดเก็บ

3.2 หลักการของฟัซซีลอจิก

ฟัซซีลอจิก [2] นำมาใช้ตัดสินใจในความไม่แน่นอนความคลุมเครือโดยยอมให้มีความยืดหยุ่นได้ ซึ่งข้อดีของลักษณะการวิเคราะห์เชิงตรรกะเช่นนี้ สอดคล้องกับตรรกะความคิดของมนุษย์ที่สามารถช่วยในการตัดสินความถูกผิดแบบคลุมเครือไม่ใช่ผิดหรือถูกเพียงสองสถานะ ฟัซซีลอจิกมีขั้นตอนในการประมวลผลการทำงานแบ่งออกเป็น 4 ส่วน ดังแสดงในรูปที่ 2



ภาพที่ 2: ขั้นตอนในการประมวลผลแบบฟัซซีลอจิก

3.2.1 ฟังก์ชันความเป็นสมาชิก (Membership Function) เป็นการกำหนดระดับความเป็นสมาชิกของตัวแปรในเซตของความคลุมเครือแบบต่างๆ และจะนำไปใช้ในการกำหนดกฎในการวิเคราะห์

3.2.2 กฎการวิเคราะห์ (Fuzzy Rule) เป็นการสร้างความสัมพันธ์ของค่าฟังก์ชันความเป็นสมาชิกแต่ละตัวโดยมีเงื่อนไขต่างๆ เพื่อนำไปใช้ในการวิเคราะห์และแปลความข้อมูล

3.2.3 การอนุมาน (Inference) เป็นการตรวจสอบหรือการแปลความของค่าความเป็นสมาชิกเพื่อหาผลลัพธ์ของกฎที่ได้ด้วยการดำเนินการทางตรรกะแบบต่างๆ (เช่น if, and, or) กับฟังก์ชันฟัซซีลอจิกที่เกี่ยวข้องโดยการใช้ค่าต่ำสุด (Minimum) สำหรับการเชื่อมประโยคแบบ And และใช้ค่าสูงสุด (Maximum) สำหรับการเชื่อมประโยคแบบ Or เพื่อนำค่าที่ได้ไปคำนวณหาผลลัพธ์ต่อไป

3.2.4 การคำนวณหาผลลัพธ์ (Defuzzification) เป็นขั้นตอนการสรุปเหตุผลทั้งหมดจากผลลัพธ์ของกฎแต่ละข้อและแปลงข้อมูลให้อยู่ในรูปแบบเดิมเพื่อแสดงผลการตัดสินใจ เขียนได้ดังสมการต่อไปนี้

$$C = \frac{\sum M\,A(x)x}{\sum M\,A(x)} \qquad (1)$$

C เป็นค่าจุดศูนย์ถ่วงของการคำนวณ

$M_{A(x)}$ เป็นฟังก์ชันความเป็นสมาชิก ในส่วนของพื้นที่แรเงา ดังแสดงในรูปที่ 4 และ 5

x เป็นค่าอินพุตที่สนใจ

3.3 ฟังก์ชันความเป็นสมาชิกสำหรับข้อมูลจราจรฯ

จากข้อมูลภายในไฟล์ข้อมูลจราจรเครือข่ายฯ ทั้ง 7 ตัวที่ได้กล่าวถึงในหัวข้อที่ 3.1 สามารถนำไปใช้ในการกำหนดเป็นฟังก์ชันอินพุตให้กับระบบฟัซซีลอจิก รวมถึงการกำหนดฟังก์ชันเอาต์พุตที่ใช้ประเมินความเหมาะสมหรือไม่เหมาะสมของการใช้งานอินเทอร์เน็ตได้ ดังต่อไปนี้

a) อินพุตที่ 1 คือ เวลา (Time) กำหนดให้มีคะแนนตามความเป็นจริงตามชั่วโมงคือ ตั้งแต่ 0 ไปจนถึง 24 ชั่วโมง สามารถแบ่งฟังก์ชันความเป็นสมาชิกของอินพุตเป็น 3 ช่วงเวลา คือ กลางวัน (Day) กลางคืน (Night) และ ดึก (Late Night) แสดงดังรูปที่ 3(a)

b) อินพุตที่ 2 คือ กลุ่มความบันเทิง (Entertainment) กำหนดให้การแบ่งฟังก์ชันความเป็นสมาชิกของอินพุตออกเป็น 10 ช่วง จากระดับความบันเทิงน้อย (Less Entertainment) ที่ค่า 0 จนถึงระดับความบันเทิงมาก (High Entertainment) ที่ค่า 1 แสดงดังรูปที่ 3(b) ยกตัวอย่าง เช่น หากผู้ใช้กำหนดให้เว็บประเภทฟังเพลงและดูหนังด้วยกัน เช่น www.kapook.com อยู่ในเกณฑ์ระดับ 5 ผู้ใช้ก็อาจจะกำหนดให้เว็บประเภทเกมส์ล้วน เช่น www.meegame.com อยู่ในเกณฑ์ที่สูงกว่าระดับ 5 ขึ้นไปได้ เป็นต้น

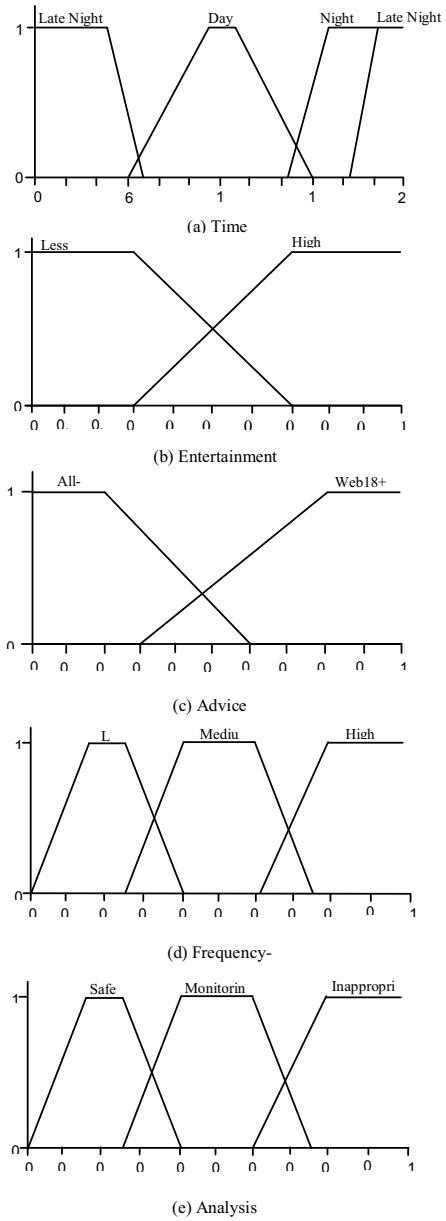
c) อินพุตที่ 3 คือ กลุ่มที่ควรให้คำแนะนำ (Advice) ใช้แนวทางตามพระราชบัญญัติภาพยนตร์และวีดิทัศน์ พ.ศ. 2551 [6] เพื่อแบ่งความเป็นสมาชิกเป็น 2 กลุ่ม คือ กลุ่มทุกช่วงวัย (All-Ages) เริ่มตั้งแต่ เหมาะกับทุกวัย, ควรให้คำแนะนำสำหรับ 9+, 13+, 15 และกลุ่มที่อายุมากกว่า 18 ปี (Web18+) ตั้งแต่ 18 ปีขึ้นไป โดยแบ่งจากเนื้อหาของเว็บที่ควรแนะนำให้เหมาะกับวัยตามลำดับเป็น 5 ช่วงคะแนนช่วงละเท่าๆกัน แสดงดังรูปที่ 3(c)

d) อินพุตที่ 4 คือ กลุ่มของความถี่ไอพีแอดเดรส (Frequency-Site) แบ่งความเป็นสมาชิกได้ 3 ช่วง คือ น้อย (Low), ปานกลาง (Medium) และมาก (High) โดยแบ่งจากใช้ไอพีแอดเดรสที่ซ้ำๆกันเป็นตัวบอกความถี่ (ดูตัวอย่างเกณฑ์ในตารางที่ 1 ประกอบ) แสดงดังรูปที่ 3(d)

e) เอาต์พุต คือ ผลการวิเคราะห์ (Analysis) แบ่งความเป็นสมาชิกเป็น 3 ระดับ คือ ปลอดภัย (Safe), เฝ้าระวัง (Monitoring) และไม่เหมาะสม (Inappropriate) โดยแบ่งคะแนนค่าความเป็นสมาชิกของความปลอดภัยตั้งแต่ 0 ไปจนถึง 0.4 ระดับการเฝ้าระวังตั้งแต่ 0.25 ถึง 0.75 และมากกว่า 0.6 ถึง 1 ให้เป็นคะแนนระดับความไม่เหมาะสมในการใช้งานอินเทอร์เน็ตแสดงดังรูปที่ 3(e)

3.4 กฎของฟัซซีลอจิก

การสร้างกฎในการวิเคราะห์ข้อมูลในการทดลองนี้ เน้นเรื่องของช่วงเวลาการเข้าใช้งาน กลุ่มของไอพีแอดเดรสและความถี่ในการใช้งานเว็บในกลุ่มต่างๆเป็นหลัก สามารถสร้างกฎเกณฑ์เพื่อการวิเคราะห์ข้อมูลได้ดังต่อไปนี้



ภาพที่ 3*:* ฟังก์ชันการความเป็นสมาชิกแบบต่างๆ ที่ใช้วิเคราะห์ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ด้วยฟัซซีลอจิก

ตารางที่ 1: ตัวอย่างกลุ่มของความถี่ของไอพีแอดเดรส

ฟังก์ชันความเป็นสมาชิก	ความถี่การใช้งานเว็บซ้ำๆ/ครั้ง	คะแนนความเป็นสมาชิก/คะแนน
น้อย	น้อยกว่า 20	0 - 0.2
ปานกลาง	มากกว่า 20ไม่เกิน 40	0.2 - 0.4
มาก	มากกว่า 40	0.4 – 1

กฎข้อที่ 1 If (Late-Night) and (Less-Entertainment) and (All-Ages) and (Freq.-not-High) Then (output is Safe)

กฎข้อที่ 2 If (Late-Night) and (High-Entertainment) and (All-Ages) and (Freq.-not-High) Then (output is Monitoring)

กฎข้อที่ 3 If (Late-Night) and (Less-Entertainment) and (Web 18+) and (Freq.-not-Low) Then (output is Inappropriate)

กฎข้อที่ 4 If (Night) and (High-Entertainment) and (All-Ages) and (Freq.-not-Low) Then (output is Inappropriate)

กฎข้อที่ 5 If (Night) and (High-Entertainment) and (Web18+) and (Freq.-High) Then (output is Inappropriate)

กฎข้อที่ 6 If (Night) and (Less-Entertainment) and (All-Ages) and (Freq.-High) Then (output is Monitoring)

กฎข้อที่ 7 If (Day) and (Less-Entertainment) and (All-Ages) and (Freq.-not-Low) Then (output is Safe)

กฎข้อที่ 8 If (Day) and (Less-Entertainment) and (Web18+) and (Freq.-not-High) Then (output is Monitoring)

กฎข้อที่ 9 If (Day) and (High-Entertainment) and (Web18+) and (Freq.-High) Then (output is Inappropriate)

กฎข้อที่ 10 If (Day) and (High-Entertainment) and (All-Ages) and (Freq.-High) Then (output is Monitoring)

3 ผลการวิเคราะห์ข้อมูล

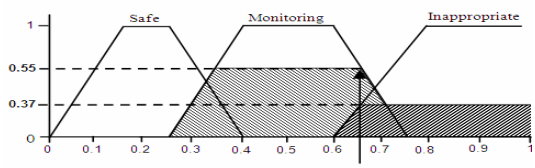
เมื่อทดลองวิเคราะห์ข้อมูลตามกฎที่กำหนดของฟัซซีลอจิกในข้อที่ 3.4 แล้ว สามารถแสดงตัวอย่างการวิเคราะห์ข้อมูลในช่วงเวลากลางวัน กลางคืน และช่วงดึก ดังนี้

ตัวอย่างที่ 1 รายการข้อมูลใช้งานช่วงกลางวัน

User	Month	Date	Time	IP Source	IP Destination	Protocal	Port	Frq.
Boy	Dec	11	14:09:10	192.168.182.2	209.85.175.101	TCP	80	50

จากตารางผู้ใช้งาน Boy เข้าใช้งานวันที่ 11 ธันวาคม เมื่อเวลา 14:09:10 น. จากไอพีแอดเดรส 192.168.182.2 ไปเว็บไซต์ปลายทางที่หมายเลข 209.85.175.101 (ซึ่งอยู่ในกลุ่มของความบันเทิงมาก) โดยมีคะแนนจากการคำนวณของกลุ่มเว็บ คือ ความเป็นบันเทิง 0.9 กลุ่มที่ควรให้คำแนะนำ 0.37 ความถี่ของไอพีแอดเดรส 0.88 ซึ่งเมื่อผลของแต่ละอินพุตถูกคำนวณ

ร่วมกันจากกฎแต่ละข้อ (Defuzzification) จะได้ค่าเอาต์พุตเป็น 0.55 ซึ่งหมายถึง ควรมีการเฝ้าระวังและติดตามการใช้งาน โดยผลของการวิเคราะห์ข้อมูลจากตัวอย่างนี้เข้ากฎข้อที่ 9 และข้อที่ 10 ดังแสดงในรูปที่ 4

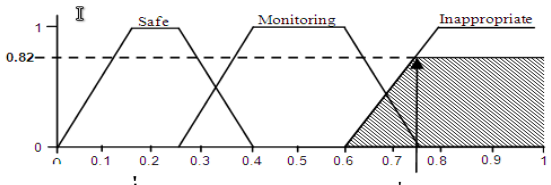


ภาพที่ 4: ผลจากการคำนวณเข้ากฎข้อที่ 9 และ 10

ตัวอย่างที่ 2 รายการข้อมูลใช้งานช่วงดึก

User	Month	Date	Time	IP Source	IP Destination	Protocal	Port	Frq.
Boy	Dec	11	22:06:09	192.168.182.2	209.85.175.101	TCP	80	50

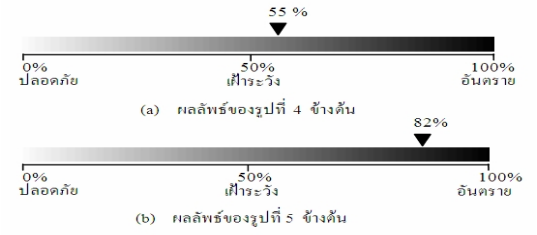
รายการใช้งานนี้มีความเหมือนกับตัวอย่างที่ 1 ข้างต้น เพียงแต่แตกต่างกันที่เป็นการใช้งานช่วงดึกในเวลา 22:06:09 น. จากผลของการวิเคราะห์ข้อมูลเข้ากฎข้อที่ 3, 4 และ 5 ได้ข้อสรุปผลการคำนวนเอาต์พุต (ดูรูปที่ 5) มีค่าความไม่เหมาะสมของการใช้งานที่ 0.82 ซึ่งหมายถึงว่าอาจจะมีการใช้งานเว็บไซต์ที่ไม่เหมาะสม (Inappropriate) ได้ และผู้ปกครองควรตรวจสอบ



ภาพที่ 5: ผลจากการคำนวณเข้ากฎข้อที่ 3 และ 5

จากตัวอย่างการคำนวณเชิงตัวเลขด้วยเทคนิควิธีฟัซซีข้างต้น หากนำเสนอภายในโปรแกรมสารสนเทศด้วยลักษณะของแถบสี (Color Bar) พร้อมลูกศรกำกับค่าผลลัพธ์ที่ได้ (ดูรูปที่ 6 (a) และ (b) ประกอบ) ก็สามารถช่วยให้ผู้ใช้โปรแกรมสามารถ ทำความเข้าใจผลลัพธ์ได้รวดเร็วยิ่งขึ้น

การพัฒนาโปรแกรมสารสนเทศที่ทำงานอยู่บนพื้นฐานของเทคนิควิธีฟัซซีลอจิกข้างต้นสามารถดำเนินการได้โดยสะดวก เนื่องจากมีไลบรารีสนับสนุนโดยตรง ตัวอย่างเช่น jFuzzyLogic library [7] สำหรับการพัฒนาโปรแกรมด้วยภาษา JAVA หรือ fuzzylite [8] สำหรับภาษา C++ เป็นต้น



ภาพที่ 6: ตัวอย่างการแสดงผลเชิงกราฟิกที่เป็นมิตรกับผู้ใช้

4 สรุปและวิจารณ์ผล

เทคนิควิธีฟัซซีลอจิกสามารถนำมาใช้ในการวิเคราะห์ข้อมูลจราจรเครือข่ายคอมพิวเตอร์ที่นำมาจากอุปกรณ์เราเตอร์ได้เป็นอย่างดี โดยในที่นี้ได้นำเสนอตัวอย่างการใช้ข้อมูล 5 ตัว สำหรับกำหนดเป็นฟังก์ชันสมาชิก และนำมาพิจารณาร่วมกับเงื่อนไขต่างๆ ที่ผู้ปกครองต้องการในลักษณะของกฎฟัซซี เทคนิควิธีนี้ไม่เพียงแต่จะช่วยให้เกิดความยืดหยุ่นในการปรับเปลี่ยนกฎอย่างอิสระ โดยไม่มีผลกระทบกับตัวโปรแกรมแล้ว ยังจะช่วยให้แสดงผลการวิเคราะห์ในลักษณะของกราฟิกที่ง่ายต่อการทำความเข้าใจได้ดีอีกด้วย อย่างไรก็ตาม ข้อจำกัดสำคัญของเทคนิควิธีที่นำเสนอในบทความนี้ ต้องการให้ผู้ปกครองตรวจสอบเว็บไซต์ของไอพีแอดเดรสปลายทางที่ไม่คุ้นเคยในเบื้องต้นก่อน เพื่อจะสามารถกำหนดเกณฑ์ของระดับความบันเทิง และระดับการให้คำแนะนำ ได้ตามที่ต้องการ

เอกสารอ้างอิง

[1] ICT HOUSE KEEPER Program, available at www.icthousekeeper.com, access at 27 Feb. 2011.

[2] Y. John,*Fuzzy System*, Prentice-Hell: New Jersey. 1999.

[3] S. Lekcharoen and C. C. Fung, “An Adaptive Fuzzy Control Traffic Shaping Scheme over Wireless Networks,” *Proc. of Asia-Pacific Conf. on Comm.,* Bangkok, Thailand, Oct., 2007.

[4] A. Rahman, P. Kennedy, A. Simmonds and J. Edwards, “Fuzzy Logic Based Modelling and Analysis of Network Traffic,” *IEEE Int. Conference*,Sydney, Australia,2008.

[5] คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์, พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550.

[6] พระราชบัญญัติภาพยนตร์และวีดิทัศน์ พ.ศ. 2551, ราชกิจจานุเบกษา เล่ม 125 ตอนที่ 42 ก มาตรา 26.

[7] fuzzylite, available at http://code.google.com/p/fuzzy-lite/, access at 28 Mar. 2011.

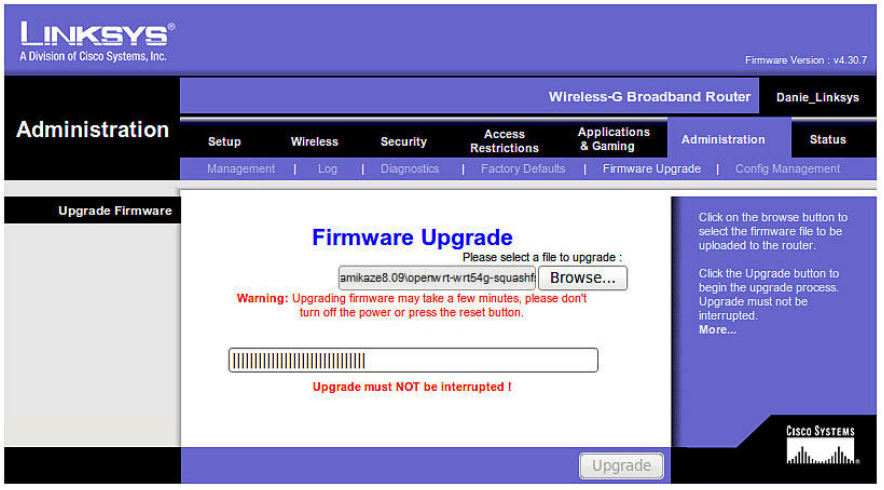
[8] jFuzzyLogic, available at http://jfuzzylogic.sourceforge.net, access at 28 Mar. 2011.

ภาคผนวก ข : การติดตั้งและใช้งานอุปกรณ์แอกเซสพ้อยน์เราเตอร์

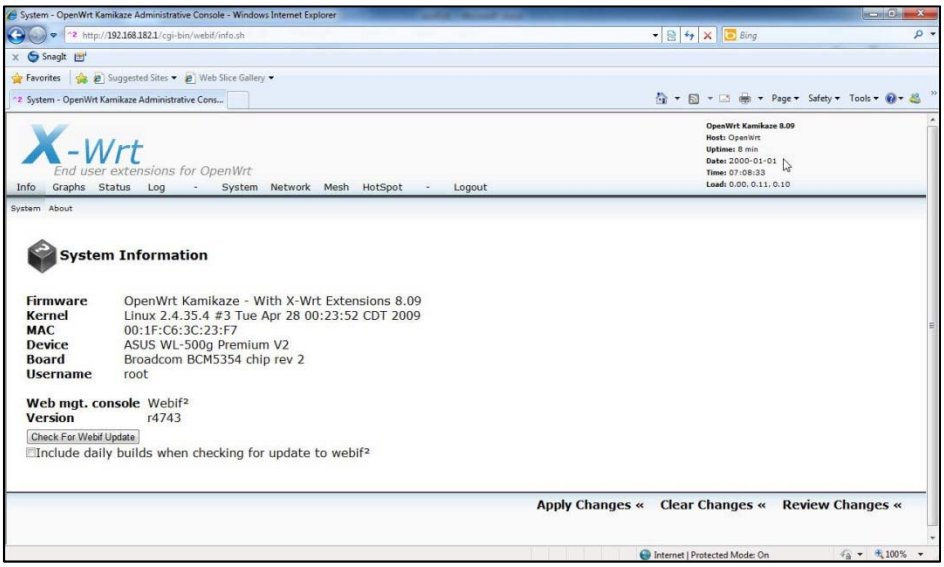
การทดลองติดตั้งระบบจัดเก็บข้อมูลจราจรเครือข่ายทางคอมพิวเตอร์ ในเบื้องต้นได้ศึกษานำอุปกรณ์ ยี่ห้อ Linksys รุ่น WRT54GL ซึ่งเป็นคอมพิวเตอร์แบบฝังตัวที่มีขนาดหน่วยประมวลผล 200 MHz หน่วยความจำหลัก 16 MB. และหน่วยความจำข้อมูล 4 MB. เพื่อหาความเป็นไปได้ในการนำเฟิร์มแวร์ที่เป็นแพลทฟอร์มโอเพ่นซอร์ส OpenWRT เวอร์ชั่น 7.09 (Kamikaze) มาทดลองเพื่อติดตั้งระบบซอฟแวร์ที่จำเป็น ในแบบฉบับของแนวทางซอฟต์แวร์ที่ใช้สำหรับคอมพิวเตอร์แม่ข่ายในการเก็บข้อมูลจราจร และได้มีการดัดแปลงอุปกรณ์ให้สามารรองรับหน่วยความจำภายนอกเพิ่มขึ้นแบบ SDHC Card เพื่อขยายพื้นที่สำหรับติดและจัดเก็บข้อมูล ดังแสดงในรูปที่ 6.1 และต่อมาได้เปลี่ยนเฟิร์มแวร์เป็นเวอร์ชั่นที่สูงขึ้นคือ 8.09 (Kamikaze) เนื่องจากสามารถรองรับซอฟต์แวร์ CoovaChilli ที่มีขั้นตอนปรับตั้งค่าการใช้งานให้ง่ายขึ้น และเกิดปัญหาเนื้อที่ของอุปกรณ์ในการติดตั้งไม่เพียงพอสำหรับส่วนของระบบหลัก หน่วยความจำที่เพิ่มเติมได้เพียงแค่จัดเก็บส่วนข้อมูลเท่านั้น จึงได้เปลี่ยนอุปกรณ์ที่พัฒนาเดิมมาเป็น ยี่ห้อ ASUS รุ่น WL500GP V2 ที่มีขนาดหน่วยความจำข้อมูลมากกว่าและเพียงพอสำหรับการติดตั้ง คือ 8 MB. ทำให้ระบบสามารถใช้งานได้ตามวัตถุประสงค์

ข.1 การ Upgrade Firmware โอเพ่นซอร์สให้กับตัวอุปกรณ์ สามารถดาวน์โหลดโปรแกรมได้ที่ http://downloads.openwrt.org/kamikaze/8.09/brcm-2.4/openwrt-brcm-2.4-squashfs.trx และเปิดอุปกรณ์แอกเซสพ้อยและเชื่อมต่อสายสัญญาณเน็ตเวิร์ค โดยใช้ Internet Explorer ไปที่แอดเดรส 192.168.1.1 ซึ่งจะพบเฟิร์มแวร์เดิมของอุปกรณ์ ให้ทำการเปลี่ยนเฟิร์มแวร์ใหม่ โดยใช้เฟิร์มแวร์ที่ได้ดาวน์โหลดมาทำการ Upgrade Firmware ใหม่ โดยเข้าไปที่เมนู Administration เลือกเมนูย่อย Config Management แสดงดังในรูปที่ 6.2 เลือกเฟิร์มแวร์และกดปุ่ม Upgrade รอจนกว่าจะเสร็จระบบจะทำการ restart อัตโนมัติ และให้เปิด Internet Explorer ไปที่แอดเดรส 192.168.1.1 อีกครั้งหนึ่งจะพบว่าผลจากการเปลี่ยนเฟิร์มแวร์ใหม่ แสดงดังรูปที่ 6.3 และส่วนอื่นๆ ของซอฟต์แวร์ที่นำเสนอต่อไปนี้ ซึ่งได้มีรายละเอียดและความสำคัญไปแล้วในบทที่ 3 ในส่วนนี้จะขอกล่าวเฉพาะรายละเอียดที่จำเป็นสำหรับการติดตั้งเท่านั้น

รูปที่ 6.1 การเพิ่มหน่วยความจำข้อมูลให้กับอุปกรณ์ Linksys WRT54GL



รูปที่ 6.2 การเปลี่ยนเฟิร์มแวร์ใหม่เป็น OpenWRT (Kamikaze)

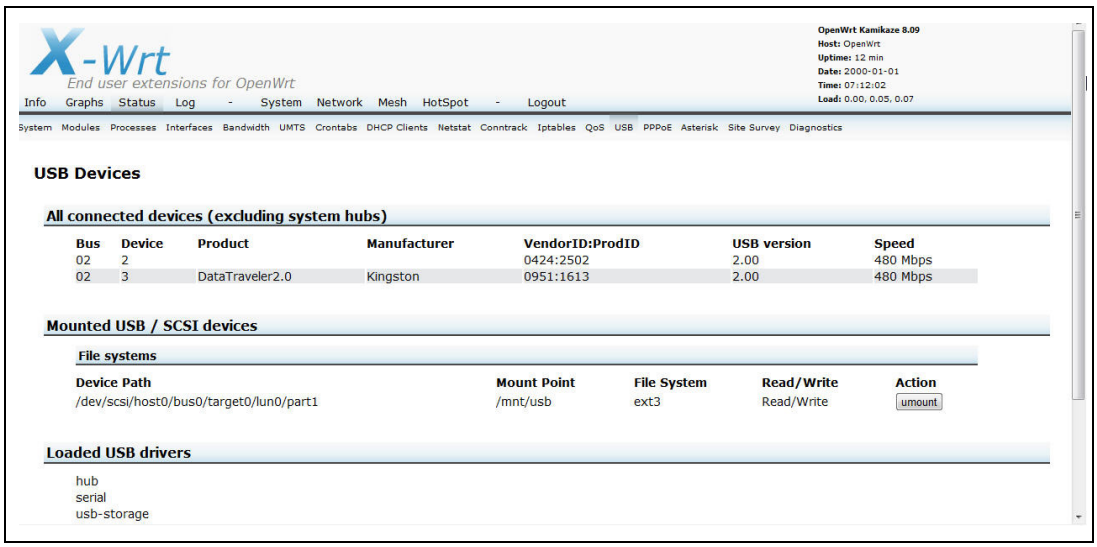


รูปที่ 6.3 ผลของเฟิร์มแวร์ที่ต้องการ

ข.2 การติดตั้งซอฟต์แวร์ที่จำเป็นสำหรับระบบ จำเป็นต้องเพิ่มโมดูลเพื่อรองรับการทำงานของระบบ เช่น fdisk และ kmod-fs-ext3 เพื่อรองรับพื้นที่ใช้งานที่เป็นฟอร์แมท ext3 ดังแสดงในรูปที่ 6.4 การเพิ่มหน่วยความจำข้อมูลภายนอกแบบ USB ขาด 4 GB. ดังแสดงในรูปที่ 6.5 และรายละเอียดซอฟต์แวร์ที่ใช้งานทั้งหมดดังตารางที่ 6.1

```
# opkg update
.....
# opkg install kmod-vfat
.....
# opkg install e2fsprogs
.....
# opkg install kmod-fs-ext3
.....
# opkg install fdisk
.....
```

รูปที่ 6.4 โมดูลเพิ่มเติมที่จำเป็นสำหรับระบบ



รูปที่ 6.5 เพิ่มหน่วยความจำแบบ USB ให้กับอุปกรณ์

ตารางที่ 6.1 รายละเอียดซอฟแวร์ระบบที่ใช้งาน

Package	Version	Package	Version
base-files-brcm-2.4	14-r15452	kmod-scsi-core	2.4.35.4-brcm-2.4-1
Bridge	1.0.6-1	kmod-tun	2.4.35.4-brcm-2.4-1
busybox	1.11.2-2	kmod-usb-core	2.4.35.4-brcm-2.4-1
coova-chilli	1.0.12-1	kmod-usb-ohci	2.4.35.4-brcm-2.4-1
dnsmasq	2.46-1	kmod-usb-serial	2.4.35.4-brcm-2.4-1
dropbear	0.51-2	kmod-usb-storage	2.4.35.4-brcm-2.4-1
e2fsprogs	1.40.11-1	kmod-usb-uhci	2.4.35.4-brcm-2.4-1
fdisk	2.13.0.1-2	kmod-usb2	2.4.35.4-brcm-2.4-1
firewall	1-Jan	kmod-wlcompat	2.4.35.4-brcm-2.4-2
freeradius	1.1.6-1	Libblkid	1.40.11-1
freeradius-mod-chap	1.1.6-1	Libelf	0.8.10-1
freeradius-mod-detail	1.1.6-1	libext2fs	1.40.11-1
freeradius-mod-files	1.1.6-1	Libgcc	3.4.6-14
freeradius-mod-pap	1.1.6-1	Libltdl	1.5.24-1
freeradius-mod-radutmp	1.1.6-1	Liblua	5.1.4-2
freeradius-mod-realm	1.1.6-1	libopenssl	0.9.8i-3.1
iptables	1.3.8-4	libpthread	0.9.29-14.1
iptables-mod-conntrack	1.3.8-4	libreadline	5.2-1
iptables-mod-filter	1.3.8-4.1	Libuci	0.7.3-1
iptables-mod-nat	1.3.8-4	libuci-lua	0.7.3-1
kernel	2.4.35.4-brcm-2.4-1	Libusb	0.1.12-2
kmod-brcm-wl	2.4.35.4+4.150.10.5.3-brcm-2.4-2	Libuuid	1.40.11-1
kmod-fs-ext3	2.4.35.4-brcm-2.4-1	Lua	5.1.4-2
kmod-fs-vfat	2.4.35.4-brcm-2.4-1	Luac	5.1.4-2
kmod-ipt-nat	2.4.35.4-brcm-2.4-1	ntpclient	2007_365-1
kmod-ipt-nathelper	2.4.35.4-brcm-2.4-1	Ntpdate	4.2.4p6-2.1
kmod-nls-cp437	2.4.35.4-brcm-2.4-1	Nvram	1
kmod-nls-iso8859-1	2.4.35.4-brcm-2.4-1	Olsrd	0.5.6-r3-2
kmod-ppp	2.4.35.4-brcm-2.4-1	olsrd-mod-dyn-gw	0.5.6-r3-2
kmod-pppoe	2.4.35.4-brcm-2.4-1	olsrd-mod-httpinfo	0.5.6-r3-2
openssh-sftp-server	5.0p1-1	Webif	0.3-4709
Ppp	2.4.3-10	webif-iw-lua	0.1-1
ppp-mod-pppoe	2.4.3-10	webif-iw-lua-coovachilli	0.1-1
privoxy	3.0.8-3	webif-iw-lua-freeradius	0.1-1
pure-ftpd	1.0.22-1	webif-mesh	0.1-beta
stunnel	4.25-1	wireless-tools	29-2
Uclibc	0.9.29-14	Zlib	1.2.3-5

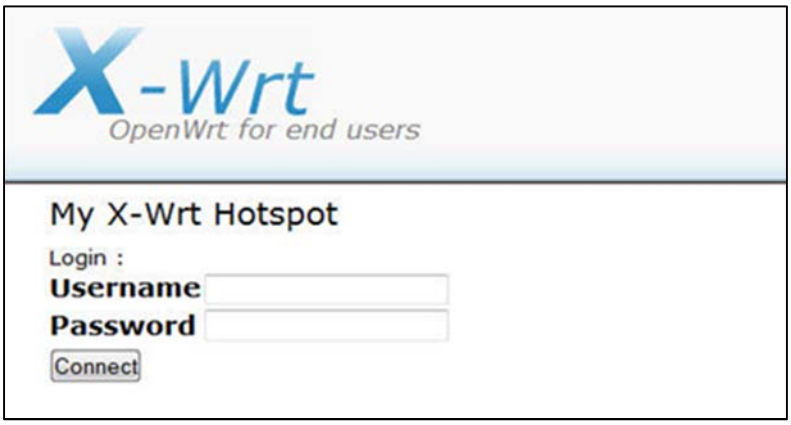
ข.3 การปรับตั้งค่าระบบให้บริการล็อกอิน โดยหลักการทำงานและการให้บริการในการเข้าถึงเครือข่ายอินเตอร์เน็ตซึ่งโปรแกรม Coova-Chilli จะทำการ Redirect หน้าของระบบล็อกอิน เพื่อขอใช้งานเครือข่ายอินเตอร์เน็ตเมื่อมีผู้ใช้บริการ ภายในไฟล์ /etc/chilli/config และ /etc/chilli/ main.conf ดังแสดงในรูปที่ 6.7 และการปรับตั้งค่าการใช้งาน ดังแสดงในรูปที่ 6.8 เพื่อให้ได้หน้าล็อกอิน ดังแสดงในรูปที่ 6.9 เป็นต้น

```
#### This conf file was writed by webif-iw-lua-coovachilli-apply ####
HS_LANIF=br-wifi
HS_LOC_NETWORK="X-Wrt Network"
HS_RADSECRET=testing123
HS_RADAUTH=1812
HS_RADIUS2=127.0.0.1
HS_LOC_NAME="My X-Wrt Hotspot"
HS_DNS2=202.69.137.138
HS_DNS1=192.168.182.1
HS_UAMSERVER=192.168.182.1
HS_RADIUS=127.0.0.1
HS_UAMPORT=3990
HS_ANYDNS=on
HS_NETMASK=255.255.255.0
HS_NASID=X-Wrtnas
HS_NETWORK=192.168.182.0
HS_MODE=hotspot
HS_UAMLISTEN=192.168.182.1
HS_RADACCT=1813
HS_UAMHOMEPAGE=http://192.168.182.1/cgi-bin/login/home
HS_UAMFORMAT=http://192.168.182.1/cgi-bin/login/login
HS_UAMALLOW=202.69.137.138,coova.org,127.0.0.1,192.168.182.1,x-wrt.org,openwrt.org
```

รูปที่ 6.7 แสดงการแก้ไขไฟล์ config ของตัว Coova-Chilli

```
# THIS FILE IS AUTOMATICALLY GENERATED
cmdsocket       /var/run/chilli.sock
pidfile         /var/run/chilli.pid
net             192.168.182.0/255.255.255.0
uamlisten       192.168.182.1
uamport         3990
dhcpif          br-wifi
adminuser       chillispot
adminpasswd     chillispot
uamallowed      coova.org,192.168.182.1,127.0.0.1
uamanydns

domain lan
dns1 192.168.182.1
dns2 202.69.137.138
uamhomepage http://192.168.182.1/cgi-bin/login/home
locationname "My X-Wrt Hotspot"
radiuslocationname My_X_Wrt_Hotspot
radiuslocationid isocc=,cc=,ac=,network=X_Wrt_Network
radiusserver1   127.0.0.1
radiusserver2   127.0.0.1
radiussecret    testing123
radiusauthport  1812
radiusacctport  1813
uamserver       http://192.168.182.1/cgi-bin/login/login
radiusnasid     X-Wrtnas
```

รูปที่ 6.8 แสดงการแก้ไขไฟล์ main.conf ของตัว Coova-Chilli



รูปที่ 6.9 ผลการทำงานของโปรแกรม Coova-Chilli

ข.3 การปรับตั้งค่าระบบให้บริการพิสูจน์ตัวตน โดยใช้ซอฟต์แวร์ Freedadius ซึ่งมีหลักการทำงานร่วมกับ Coova-Chilli เพื่อตรวจสอบค่าที่ส่งมาการใช้งาน โดยมีไฟล์หลักที่ปรับตั้งค่าการใช้งาน คือ /etc/freeradius/radiusd.conf, /etc/freeradius /users, /etc/freeradius/clients.conf แสดงรายละเอียดดังต่อไปนี้

- ประมาณบรรทัดที่ 207 เปลี่ยนพอร์ทการใช้งาน จาก port = 0 เป็น port = 1812
- ประมาณบรรทัดที่ 283 ตรง Regular expressions ให้แก้ข้อความเป็น yes ดังต่อไปนี้

```
.....
regular_expressions     = yes
extended_expressions    = yes
.....
```

- ประมาณบรรทัดที่ 297 ในส่วนของ Log authentication re□uests to the log file ให้แก้ข้อความเป็น yes ดังต่อไปนี้ log_auth = yes
- ประมาณบรรทัดที่ 307 ในส่วนของ Log passwords with the authentication re□uests ให้แก้ข้อความเป็น yes ดังต่อไปนี้

```
.....
log_auth_badpass = yes
log_auth_goodpass = yes
.....
```

- ประมาณบรรทัดที่ 576 ในส่วนของ modules ให้เปิดการใช้งานโมดูล pap และ chap แสดงดังต่อไปนี้

```
pap {
        auto_header = yes
}
```

และ

```
chap {
        authtype = CHAP
}
```

- ประมาณบรรทัดที่ 1788 ในส่วนของโมดูล authorize ให้เปิดการใช้งานโมดูลต่างๆ โดยการเอาเครื่อง หมาย # ข้างหน้าออก ดังต่อไปนี้ auth_log, chap และ pap
- ประมาณบรรทัดที่ 1911 ในส่วนของโมดูล authenticate แก้ข้อความตรงประมาณบรรทัดที่ 1925

```
Auth-Type CHAP {
        chap
        }
```

- ในส่วนของ log file เพิ่มเติมในการเก็บข้อมูลต่างๆ ลงในการ์ดหน่วยความจำ จำเป็นต้องเปิดการใช้งานและแก้ไขค่าการทำงานต่างๆ ของโมดูล detail ดังต่อไปนี้
- ประมาณบรรทัดที่ 1104 เปิดการใช้งาน

```
detailfile = ${radacctdir}/%{Client-IP-Address}/detail-%Y%m%d
```

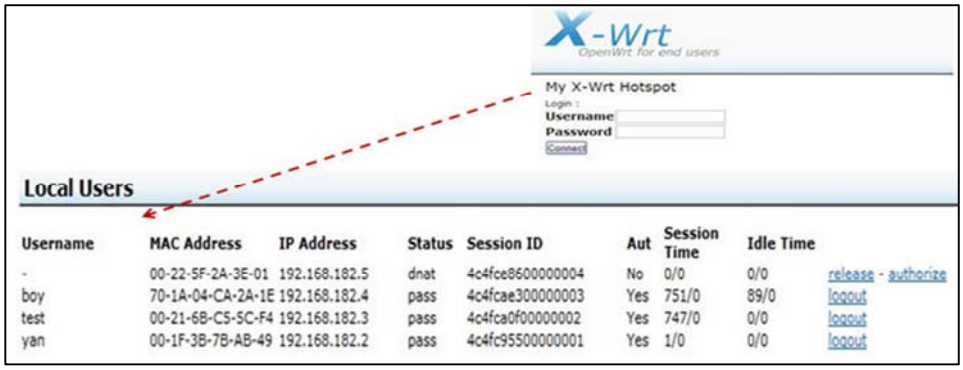
- ประมาณบรรทัดที่ 1137 เปิดการใช้งาน detail auth_log และค่าดังต่อไปนี้

```
detail auth_log {
        detailfile = ${radacctdir}/%{Client-IP-Address}/auth-detail-%Y%m%d

        #
        #  This MUST be 0600, otherwise anyone can read
        #  the users passwords!
        detailperm = 0600
}
```

- ประมาณบรรทัดที่ 1154 เปิดการใช้งาน detail reply_log และค่าดังต่อไปนี้

```
detail reply_log {
        detailfile = ${radacctdir}/%{Client-IP-Address}/reply-detail-%Y%m%d

        #
        #  This MUST be 0600, otherwise anyone can read
        #  the users passwords!
        detailperm = 0600
}
```

- ผลจากการติดตั้งระบบในการทดสอบการใช้งาน จะปรากฏหน้าต่างล็อกอินเมื่อมีผู้ขอใช้งานเว็บไซต์ต่างๆ ดังแสดงในรูปที่ 6.10 และผู้ดูแลสามารถตรวจสอบสถานะการเข้าใช้ของผู้ใช้งานแต่ละคนได้โดยผ่านเว็บไซต์ของตัวอุปกรณ์ WL500GP V2 เป็นต้น



รูปที่ 6.10 รายละเอียดสถานะของผู้ใช้บริการ

ประวัติผู้เขียน

ชื่อ สกุล นายสายัณ อินชะนะ

รหัสประจำตัวนักศึกษา 5110121101

วุฒิการศึกษา

วุฒิ	ชื่อสถาบัน	ปีที่สำเร็จการศึกษา
คบ. (คอมพิวเตอร์ศึกษา)	มหาวิทยาลัยราชภัฏยะลา	2549

ทุนการศึกษา (ที่ได้รับในระหว่างการศึกษา)

ทุนอุดหนุนการศึกษาระดับบัณฑิตศึกษา คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี ประจำปีการศึกษา 2551

ทุนอุดหนุนการศึกษาระดับบัณฑิตศึกษา มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี ประจำปีการศึกษา 2552

ตำแหน่งและสถานที่ทำงาน

ตำแหน่ง นักวิทยาศาสตร์

สถานที่ทำงาน งานระบบเครือข่ายและโทรศัพท์ผ่านโครงข่ายไอพี หน่วยคอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ วิทยาเขตปัตตานี

การตีพิมพ์เผยแพร่งาน

สายัณ อินชะนะ สุนทร วิทูสุรพจน์ และ สมชัย หลิมศิโรรัตน์. 2553. การวิเคราะห์ข้อมูลจราจรเครือข่ายด้วยฟัซซีลอจิกเพื่อตรวจการใช้อินเทอร์เน็ตบุตรธิดา. การประชุมทางวิชาการระดับชาติ ด้านคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ครั้งที่ 7, 11-12 พฤษภาคม 2554.