

บทที่ 5

สรุป อภิปรายผล และข้อเสนอแนะ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อนำเสนอแนวทางในการจัดทำระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟต์แวร์รหัสเปิดที่สามารถใช้งานได้จริงและสอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ระบุไว้ว่า ผู้ให้บริการอินเทอร์เน็ตทั้งภาครัฐและเอกชน รวมถึงผู้ประกอบการรายย่อยที่เกี่ยวข้องกับการให้บริการอินเทอร์เน็ตมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ในหน่วยงานของตนเองไว้ไม่น้อยกว่า 90 วัน ไม่เช่นนั้นแล้วจะมีความผิดกฎหมายทางอาญาตามที่ระบุไว้ในพระราชบัญญัติ ซึ่งระบบที่จัดทำขึ้นในครั้งนี้ใช้แนวทางของประสิทธิภาพที่ได้ ความประหยัด และรวดเร็วในการจัดทำโดยใช้อุปกรณ์ฮาร์ดแวร์ที่สามารถหาได้ง่าย ต้นทุนต่ำ โดยเฉพาะใช้ซอฟต์แวร์รหัสเปิดหรือที่รู้จักกันในนามโอเพ่นซอร์ส (Open Source) เป็นซอฟต์แวร์ที่ได้รับความนิยมอย่างสูงในปัจจุบันและที่สำคัญนั้น โอเพ่นซอร์สเป็นซอฟต์แวร์ในลักษณะแจกจ่ายให้ใช้ได้ฟรี ไม่มีค่าลิขสิทธิ์ใดๆ แต่มีประสิทธิภาพสูงเนื่องจากมีลักษณะของการเปิดเผยซอร์สโค้ดที่เขียน หากผู้ใดต้องการแก้ไขหรือพัฒนาให้มีความสามารถมากขึ้นก็สามารถทำได้เพียงแต่เมื่อมีการแก้ไขแล้วต้องมีการบอกต่อและแจกจ่ายให้คนอื่นได้ใช้ร่วมกันห้ามนำไปเพื่อทำการค้าหรือแอบอ้างเป็นเจ้าของโดยเด็ดขาด

5.1 สรุปผลการวิจัย

ผลการวิจัยในครั้งนี้เป็นไปตามเป้าหมายและการออกแบบที่ออกแบบไว้ทุกประการสามารถทำงานได้อย่างถูกต้องแม่นยำ สามารถจัดเก็บร่องรอยการใช้งานของผู้ใช้ได้ครบถ้วนตามวัตถุประสงค์ที่ตั้งไว้ ซึ่งสรุปผลการทำงานได้ดังนี้

ในระบบเครือข่ายเดิมก่อนติดตั้งระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟต์แวร์รหัสเปิด นั้น ผู้ใช้งานสามารถเข้าใช้งานเครือข่ายอินเทอร์เน็ตได้ทันทีจากที่ใดก็ได้เพียงผู้ใช้มีอุปกรณ์ที่ใช้เชื่อมต่อเช่น เครื่องพีซี หรือเครื่องคอมพิวเตอร์พกพา เชื่อมต่อด้วยสายหรือไร้สายก็ได้ โดยผู้ใช้จะไม่ถูกควบคุมการใช้งานสามารถมีอิสระในการใช้งาน และไม่สามารถทราบร่องรอยใดๆ ได้ว่าผู้ใช้รายใด ทำอะไร เมื่อไร เวลาใด จากที่ใด

เมื่อทำการติดตั้งระบบที่จัดทำขึ้นเพิ่มเข้าไปในระบบเดิมที่มีอยู่โดยทำการเพิ่มเครื่องคอมพิวเตอร์แม่ข่ายที่ได้ติดตั้งซอฟต์แวร์ที่จำเป็นต่างๆ ไว้ภายใน ทำให้ระบบมีการทำงานเปลี่ยนไปจากเดิม ดังนี้

เมื่อผู้ใช้เข้าใช้งานเครือข่ายอินเทอร์เน็ต ผู้ใช้จะพบว่า มีหน้าต่างหรือที่เรียกว่า pop up ปรากฏขึ้นมาให้ผู้ใช้ได้มีการยืนยันตัวตนโดยการกรอก Username และ Password เสียก่อนจึงจะสามารถเข้าใช้งานอินเทอร์เน็ตได้ ในส่วนการทำงานตรงนี้ใช้ความสามารถของซอฟต์แวร์ที่ชื่อ Squid Proxy ทำงาน โดยการให้ผู้ใช้ได้มีการยืนยันตัวตน และจัดเก็บร่องรอยของผู้ใช้แต่ละรายไว้ในฐานข้อมูลซึ่งในที่นี้ใช้ซอฟต์แวร์ที่ชื่อว่า MySQL Database สำหรับจัดเก็บข้อมูลประวัติผู้ใช้ และร่องรอยการใช้งานทั้งหมดของผู้ใช้เพื่อให้สะดวกในการสืบค้นในภายหลังและสามารถนำส่งข้อมูลย้อนหลังให้เจ้าพนักงานที่มีการร้องขอข้อมูลได้ ซึ่งตามข้อกำหนดของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บอกไว้ว่าต้องสามารถเก็บร่องรอยผู้ใช้ย้อนหลังได้ไม่น้อยกว่า 90 วัน ซึ่งระบบที่จัดทำขึ้นก็สามารถตอบสนองของความต้องการตรงนี้ได้และสามารถจัดเก็บข้อมูลให้คงอยู่ได้มากกว่า 90 วันด้วย เพราะข้อมูลทุกอย่างถูกบันทึกลงในฐานข้อมูล ดังนั้นไม่ว่ากี่วันก็สามารถกำหนดได้ในตัวฐานข้อมูลเอง ซึ่งผลจากการนำระบบไปทดสอบและปรากฏว่าสามารถทำงานได้เป็นอย่างดี

จากเอกสารงานวิจัยที่เกี่ยวข้องพบว่า มีผู้เสนอแนวทางการพิสูจน์ตัวตนด้วยเทคนิควิธีต่างๆหลายรูปแบบ มีการพัฒนาระบบจัดเก็บข้อมูลหรือร่องรอยของผู้ใช้งานอินเทอร์เน็ตในรูปแบบต่างๆ เพื่อให้สามารถใช้งานและรองรับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พบว่ายังไม่มีการพูดถึงการนำเอาไอเฟ่นซอร์สหรือซอฟต์แวร์รหัสเปิดมาใช้งานหรือประยุกต์ใช้กันอย่างจริงจัง เป็นการนำบางซอฟต์แวร์มาประยุกต์ร่วมผสมผสานกับซอฟต์แวร์ที่มีลิขสิทธิ์ซึ่งค่าใช้จ่ายสูง และนอกจากนั้นส่วนสำคัญที่สุดที่จะต้องพิจารณาในการพัฒนาระบบคือ การออกแบบที่ให้ความสำคัญกับข้อมูลรายละเอียดของผู้ใช้แต่ละรายเพื่อใช้ในการตรวจสอบและติดตามได้อย่างมีประสิทธิภาพ หากดูจากงานวิจัยที่เกี่ยวข้อง โดม เจริญยศ (2551) ใช้ Radius ในการพิสูจน์ตัวตนโดยมีการจัดการข้อมูลสมาชิกผ่าน Web Browser ระบบได้ทำการเก็บข้อมูลผู้ใช้บริการ จากชื่อผู้ใช้และรหัสผ่านเท่านั้น ซึ่งระบบนี้ไม่มีการกำหนดให้เก็บข้อมูลอย่างอื่น เช่น หมายเลขบัตรประจำตัวประชาชน นอกจากนี้ยังไม่มียังมีระบบสำรองข้อมูลสูญหาย การค้นหาข้อมูลทำได้ยาก โดยหากเปรียบเทียบกับระบบที่ผู้วิจัยสร้างขึ้นจะพบว่าประการแรกคือการระบุเครื่องมือในการจัดทำชัดเจนว่าใช้ซอฟต์แวร์รหัสเปิดทั้งหมด โดยประกอบไปด้วยซอฟต์แวร์ประเภทต่างๆที่แยกหน้าที่การทำงานได้อย่างเหมาะสม สามารถแก้ปัญหาต่างๆที่กล่าวมาแล้วได้อย่างครบสมบูรณ์และทำงานได้อย่างถูกต้องแม่นยำตรงตามวัตถุประสงค์ที่ตั้งไว้ทุกประการ

5.2 อภิปรายผล

ในการพัฒนาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟต์แวร์รหัสเปิด สามารถสรุปสิ่งที่ได้จากการพัฒนาระบบ ดังนี้

5.2.1 ระบบที่พัฒนาขึ้นสามารถบังคับให้ผู้ใช้ต้องมีการยืนยันตัวตนก่อนเข้าใช้งานอินเทอร์เน็ต โดยปรากฏหน้าล็อกอินให้ผู้ใช้ใส่ Username และ Password หากข้อมูลถูกต้องจึงสามารถเข้าใช้งานได้ แต่หากไม่ถูกต้องระบบจะปฏิเสธการใช้งานและไม่สามารถเข้าใช้งานได้ อย่างเด็ดขาด

5.2.2 มีระบบจัดเก็บข้อมูลผู้ใช้รายบุคคลที่สามารถระบุและติดตามตัวตนได้อย่างถูกต้อง

5.2.3 มีระบบตรวจสอบวัน/เวลาเข้าใช้เครือข่ายอินเทอร์เน็ตของผู้ใช้ โดยอ้างอิงระบบเวลาที่นาฬิกาเชื่อถือและสามารถนำไปอ้างอิงเมื่อเกิดเหตุ โดยใช้การเทียบเวลามาตรฐาน Stratum0 ซึ่งเชื่อมโยงกับเซิร์ฟเวอร์ผู้ให้บริการจากภายนอกที่เรียกว่า NTP Server

5.2.4 มีระบบจัดเก็บหมายเลขไอพีแอดเดรสของเครื่องคอมพิวเตอร์ผู้ใช้รวมถึงรายละเอียดที่จำเป็น เช่น ชื่อเครื่อง (Computer Name) เป็นต้น

5.2.5 มีระบบจัดเก็บข้อมูลที่เป็นมาตรฐาน คงทน และน่าเชื่อถือ ในรูปแบบ Centralized Log Server ในการบริหารจัดการ Log File รวมถึงความสามารถในการย้ายโอนข้อมูล การสำรองข้อมูล การกู้คืนข้อมูล โดยจัดเก็บอยู่ในฐานข้อมูล

5.2.6 มีความสามารถในการเก็บข้อมูลเพื่อใช้ในการค้นหาข้อมูลในช่วงเวลาต่างๆ เช่น ข้อมูลปัจจุบัน ข้อมูลย้อนหลังรายวัน รายสัปดาห์ หรือรายเดือน เพื่อให้ข้อมูลกรณีเจ้าพนักงานมีการร้องขอข้อมูล ซึ่งจากการทดสอบพบว่าสามารถจัดเก็บได้อย่างครบถ้วน และถูกต้อง แม่นยำ

5.3 ข้อเสนอแนะ

จากการพัฒนาระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ด้วยซอฟต์แวร์รหัสเปิดนั้น มีข้อจำกัดบางประการที่เป็นปัญหาและอุปสรรคในการนำไปใช้งานที่ผู้จัดทำพบและจะต้องหาทางแก้ไขให้เหมาะสมกับสภาพแวดล้อมในการใช้งานของแต่ละเครือข่าย ดังนี้

5.3.1 ระบบที่จัดทำขึ้นอาศัยหลักการทำงานของพรีอ็อกซีเซิร์ฟเวอร์ ซึ่งจำเป็นต้องตั้งค่าไอพีแอดเดรสของพรีอ็อกซีเซิร์ฟเวอร์ให้กับเครื่องคอมพิวเตอร์ทุกเครื่อง อาจทำให้เกิดความไม่สะดวกกับระบบเครือข่ายที่มีเครื่องคอมพิวเตอร์ถูกข่ายจำนวนมาก

5.3.2 ควรแก้ปัญหาของระบบพร็อกซีเซิร์ฟเวอร์ให้สามารถทำงานในรูปแบบ Transparent proxy ซึ่งเป็นการทำงานที่เหมาะสมกับเครือข่ายที่มีเครื่องคอมพิวเตอร์ลูกข่ายจำนวนมาก

5.3.3 เพื่อให้การทำงานของระบบสามารถทำงานได้อย่างรวดเร็ว ควรจัดให้เครื่องคอมพิวเตอร์แม่ข่ายที่ทำหน้าที่เป็นพร็อกซีเซิร์ฟเวอร์มีหน่วยความจำสูงๆ จะทำให้การสนองตอบต่อเครื่องผู้ใช้เป็นไปอย่างรวดเร็ว