โปรแกรมตรวจสอบและวิเคราะห์ล็อกของเซิร์ฟเวอร์ซิสล็อก

Log Examination & Analysis Program of Syslog Server

ทรงวุฒิ นักรบ ฐิติพงษ์ สถิรเมธีกุล

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ กำแพงแสน มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตกำแพงแสน

ภัคพงศ์ ชิงชัย

บริษัท Credger จำกัด

บทคัดย่อ

เนื่องด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้กำหนดให้หน่วยงานจะต้องทำการเก็บข้อมูลจราจรทางคอมพิวเตอร์ ซึ่งถือเป็นข้อมูลสำคัญที่สามารถนำมาใช้ในการสืบสวนหรือสอบสวนการกระทำความผิดตาม พรบ. หรือนำไปใช้ประโยชน์อย่างอื่นได้ บทความนี้จึงได้นำเสนอความคิดที่จะนำเอาข้อมูลจราจรทางคอมพิวเตอร์มาตรวจสอบและวิเคราะห์ดูข้อมูลในการใช้งานคอมพิวเตอร์ของบุคลากรภายในหน่วยงาน และยังมีส่วนที่แสดงข้อมูลกิจกรรมทางคอมพิวเตอร์โดยรวมของบุคลากรทั้งหมดภายในหน่วยงานด้วย นอกจากนี้โปรแกรมดังกล่าวยังสามารถใช้ค้นหาผู้กระทำความผิดทางคอมพิวเตอร์ได้อีกด้วย

คำสำคัญ : ข้อมูลจราจรทางคอมพิวเตอร์, ล็อก, เซิร์ฟเวอร์ซิสล็อก

Abstract

Because the computer-related crime act defines that the authorities must collect the traffic data. This is important information that can be used in an investigation under the act or used for something else. This paper proposes an idea that is to take the traffic data to examine and analysis computer utilization of staff in the office. And also there is the part of all computer activities data of all staff in the office. In addition, this program can also search computer criminals too.

Keywords : Traffic Data, Log, Syslog Server

1. บทนำ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 [1] ได้มีการกำหนดเกี่ยวกับผู้ให้บริการที่หมายถึง ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ผู้ให้บริการเช่าระบบคอมพิวเตอร์หรือโปรแกรมประยุกต์ต่างๆ ผู้ให้บริการร้านอินเทอร์เน็ตและผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์ โดยได้กำหนดให้หน่วยงานหรือองค์กรเหล่านี้ จะต้องทำการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Data) ซึ่งเป็นข้อมูลสำคัญที่สามารถนำมาใช้ในการสืบสวนหรือสอบสวนการกระทำความผิดตาม พรบ. ดังกล่าว เป็นระยะเวลาอย่างน้อย 90 วัน แต่ไม่เกิน 1 ปี โดยได้มีการกำหนดประเภทของข้อมูลจราจรหรือข้อมูลล็อก (Log) ที่มีความจำเป็นต้องเก็บไว้ตามมาตรา 26 ซึ่งได้แก่ ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์

(E-mail Server) ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูล บนเครื่องให้บริการโอนแฟ้มข้อมูล ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ ข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet) ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น IRC หรือ IM เป็นต้น และข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)

บทความนี้จะนำเสนอโครงสร้างของระบบที่จะทำการศึกษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการเพื่อนำมาตรวจสอบและวิเคราะห์ข้อมูลการใช้บริการของผู้ใช้ โดยได้จัดทำเป็นระบบศึกษาพฤติกรรมการใช้งานคอมพิวเตอร์ของบุคลากรภายในหน่วยงานหรือพนักงานภายในบริษัท ซึ่งได้ทำการทดสอบการใช้งานจริงที่บริษัท Credger จำกัด ทั้งนี้เพื่อประโยชน์สำหรับผู้บริหารในการเรียกดูข้อมูลการใช้คอมพิวเตอร์ของพนักงานภายในบริษัท และยังสามารถใช้ค้นหาผู้กระทำความผิดทางคอมพิวเตอร์ได้อีกด้วย ในหัวข้อต่อไปจะกล่าวถึงทฤษฎีต่างๆที่ใช้ในการพัฒนาระบบดังกล่าว

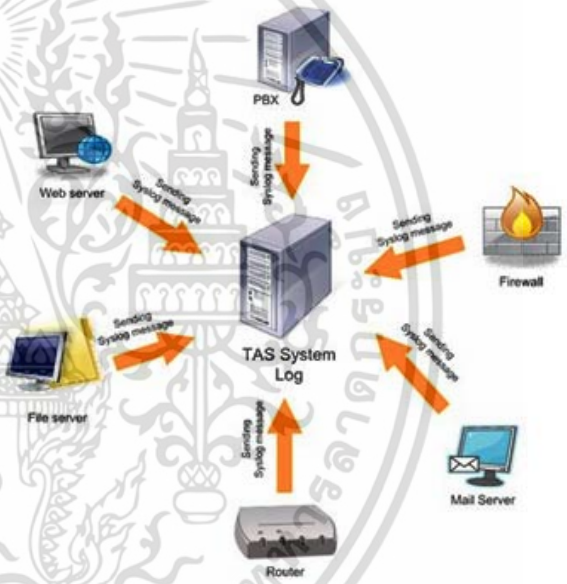
2. ทฤษฎีและงานที่เกี่ยวข้อง

ในงานนี้จะใช้หลักการของทฤษฎีและเทคโนโลยีต่างๆ ที่เกี่ยวข้องกับการพัฒนาระบบซึ่งสามารถที่จะนำมาประยุกต์ใช้กับงานนี้ได้ดังต่อไปนี้

2.1 Syslog Protocol

โพรโทคอลซิสล็อก (Syslog Protocol) พัฒนาขึ้นโดย Eric Allman เพื่อใช้งานกับระบบปฏิบัติการยูนิกซ์ (Unix) ได้รับการประกาศเป็นมาตรฐานโดยคณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต IETF (Internet Engineering Task Force) ของสหรัฐอเมริกาใน RFC 3164 [2] โดยได้นิยามไว้ว่า โพรโทคอลซิสล็อกจะทำหน้าที่ในการขนส่งข้อมูลจากเครื่องที่ส่งข้อความแจ้งเตือนผ่านเครือข่ายไอพีไปยังเครื่องที่ทำหน้าที่รวบรวมข้อความเหตุการณ์ต่างๆ เหล่านี้ ซึ่งเรียกว่า เซิร์ฟเวอร์ซิสล็อก (Syslog Server)

โปรแกรมซิสล็อกเป็น Log Daemon ที่ใช้จัดเก็บข้อมูลจราจรหรือเหตุการณ์ (Event) ต่างๆ ที่เกิดขึ้นในระบบ ดังแสดงในรูปที่ 1 ซึ่งเป็นมาตรฐานกลางที่ใช้กันทั่วโลก โปรแกรมซิสล็อกจะทำหน้าที่เป็นเซิร์ฟเวอร์ โดยทำการเปิดช่องทางเพื่อรอรับข้อมูลผ่านช่องทาง UDP 514 และนำข้อมูลที่ได้รับมาจัดเก็บลงไฟล์ข้อมูลหรือฐานข้อมูลต่อไป แต่จะไม่มีความสามารถอื่นๆ นอกจากการเก็บล็อกเท่านั้น ในปัจจุบันได้มีการเพิ่มเติมความสามารถต่างๆ ให้กับโปรแกรมซิสล็อก เช่น การกรองข้อมูล การแสดงผลข้อมูลตามสถิติ การแจ้งเตือนผู้ดูแลระบบเมื่อตรวจพบสิ่งผิดปกติ ทั้งนี้เพื่อช่วยให้ผู้ดูแลระบบสามารถทำงานได้ง่ายขึ้น และยังช่วยลดเวลาในการทำงานอีกด้วย ตัวอย่างโปรแกรมซิสล็อกซึ่งเป็นโปรแกรมฟรีแวร์ที่ได้รับความนิยม เช่น Kiwi Syslog Server [3] เป็นต้น ซึ่งล็อกที่ได้จากโปรแกรมซิสล็อกจะถูกตีความด้วยนิพจน์ปรกติ



รูปที่ 1 แสดงการทำงานของโปรแกรมซิสล็อก

2.2 Regular Expression

นิพจน์ปรกติ (Regular Expression) คือสายอักขระที่ใช้อธิบายถึงรูปแบบของ String ตามโครงสร้างของรูปแบบที่กำหนด ในภาษาโปรแกรมหลายภาษาได้รองรับการใช้นิพจน์ปรกติสำหรับการจัดการและปรับเปลี่ยนสายอักขระ [4] ซึ่งการใช้นิพจน์ปรกติอธิบายถึงรูปแบบของ String นั้นมักจะทำให้กระชับและรัดกุม โดยที่ไม่ต้องอธิบายเป็นนิพจน์ทั้งหมด เช่นคำว่า ปกติ และ ปรกติ สามารถเขียนได้เป็น ป(ร?)กติ เป็นต้น หรือตัวอย่างการใช้นิพจน์ปรกติที่ซ้ำซ้อนในการตรวจสอบการกรอกอีเมลและหมายเลขที่อยู่ไอพีก็สามารถทำได้ดังสมการที่ (1) และ (2) ตามลำดับ

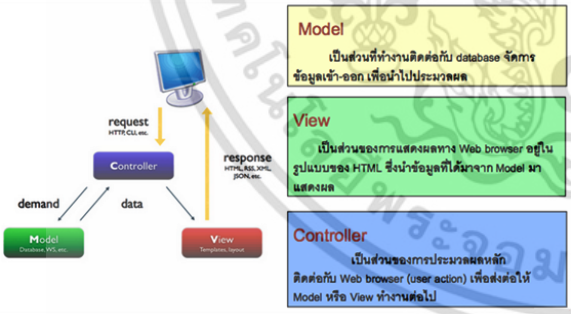
^[_a-z0-9-]+(\.[_a-z0-9-]+)*@[a-z0-9-]+(\.[a-z0-9-]+)*(\.[a-z]{2,3})$ (1)

^(0|[1-9]?\d|1\d\d|2[0-4]\d|25[0-5])\.(0|[1-9]?\d|1\d\d|2[0-4]\d|25[0-5])\.(0|[1-9]?\d|1\d\d|2[0-4]\d|25[0-5])\.(0|[1-9]?\d|1\d\d|2[0-4]\d|25[0-5])$ (2)

โดยในที่นี้จะใช้รูบีออนเรลส์ซึ่งรองรับการเขียนนิพจน์ปรกติสำหรับการพัฒนาระบบ

2.3 Ruby on Rails

ภาษารูบี (Ruby) เป็นภาษาสคริปต์เชิงวัตถุที่สั้นกระชับ ได้ใจความ และใกล้เคียงกับภาษามนุษย์ มีทางเลือกหลายแบบทำให้การเขียนหรือการกลับมาอ่านโปรแกรมในภายหลังทำได้ง่าย ส่วนสถาปัตยกรรมของเรลส์ (Rails) เป็นโครงสร้างแบบ MVC (Model View Controller) ที่ช่วยให้การสร้างแอปพลิเคชันเป็นสัดส่วนมากขึ้น โดยเรลส์จะมีส่วนสำหรับจัดเก็บคำสั่งและส่วนที่ติดต่อกับผู้ใช้แยกออกจากกัน รูบีออนเรลส์ (Ruby on Rails หรือ RoR) [5] เป็นระบบ Framework สำหรับเว็บแอปพลิเคชันที่พัฒนาด้วยภาษารูบี ทำให้การพัฒนา การนำไปใช้งาน และการดูแลรักษาเว็บแอปพลิเคชันง่ายขึ้น [6] โครงสร้างของรูบีออนเรลส์แสดงดังรูปที่ 2



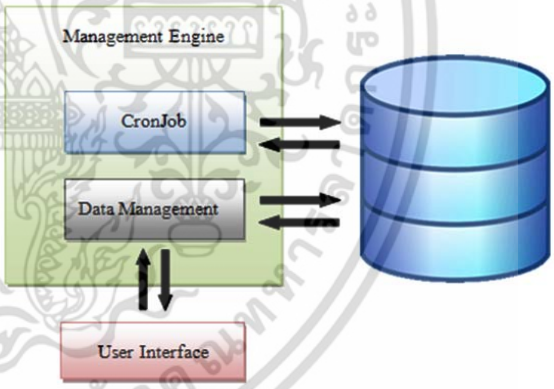
รูปที่ 2 แสดงโครงสร้างของรูบีออนเรลส์

2.4 งานที่เกี่ยวข้อง

โปรแกรมล็อกซิลลา (LogZilla) [7] เป็นซอฟต์แวร์ที่ทำงานบนเว็บไซต์ซึ่งใช้ในการดูสาร (Message) ของซิสล็อกที่ถูกจัดเก็บไว้ในฐานข้อมูลแบบเวลาจริง ช่วยให้จัดการกับสารที่ส่งมาจากอุปกรณ์หลายตัวได้ง่ายและรวดเร็วมากยิ่งขึ้น และยังสามารถแจ้งเตือนผ่านทางอีเมลแบบเวลาจริงได้อีกด้วย

3. การออกแบบและพัฒนาระบบ

สำหรับการทำงานของระบบจะแบ่งออกได้เป็นสามส่วนใหญ่ๆ โดยในส่วนแรกจะเป็นส่วนของการทำงานกับโปรแกรมช่วยวิเคราะห์ข้อมูลล็อก (CronJob) โดยมีหน้าที่หลักคือคอยเก็บข้อมูลเกี่ยวกับการเข้าเว็บไซต์และเวลาการเข้าออกงานของพนักงานในบริษัท ซึ่งได้จากล็อกที่ถูกตีความให้อยู่ในรูปแบบที่เข้าใจง่ายด้วยนิพจน์ปรกติ แล้วทำการเก็บลงในฐานข้อมูล ส่วนที่สองเป็นส่วนของการจัดการเกี่ยวกับข้อมูล (Data Management) จะเป็นการนำข้อมูลต่างๆ จากฐานข้อมูลออกมาใช้งาน เช่น ข้อมูลการเข้าเว็บไซต์ ข้อมูลเวลาการเข้าออกงาน ข้อมูลการขาดงาน เป็นต้น และสามารถนำข้อมูลดังกล่าวมาใช้ค้นหาผู้กระทำความผิดทางคอมพิวเตอร์ได้อีกด้วย สำหรับส่วนสุดท้ายเป็นส่วนต่อประสานกับผู้ใช้ (User Interface) โดยจะทำหน้าที่โต้ตอบกับผู้ใช้งาน เช่น การคัดกรองข้อมูล การเลือกข้อมูลที่ต้องการเข้าดู เป็นต้น โครงสร้างของระบบแสดงดังรูปที่ 3



รูปที่ 3 แสดงโครงสร้างของระบบ

ส่วนของ CronJob จะเป็นส่วนที่ทำงานอยู่ตลอดเวลา ซึ่งประกอบด้วยส่วนที่ทำหน้าที่เก็บข้อมูลล็อกของการเข้าเว็บไซต์ที่ผ่านการตีความโดยโปรแกรมช่วยวิเคราะห์ข้อมูลล็อก แต่เนื่องจากข้อมูลที่ได้จากล็อกที่ผ่านการตีความแล้วนั้นจะไม่สามารถระบุชื่อของผู้ใช้ได้ จึงต้องนำหมายเลขที่อยู่ไอพีของเครื่องที่ใช้บริการมาหาชื่อของผู้ใช้จากการพิสูจน์ตัวจริง (Authentication) และเมื่อหาผู้ใช้ได้แล้วก็จะนำข้อมูลที่ได้ทั้งหมดบันทึกลงในฐานข้อมูลต่อไป และยังมีส่วนที่ทำหน้าที่เก็บข้อมูลล็อกของเวลาเข้า

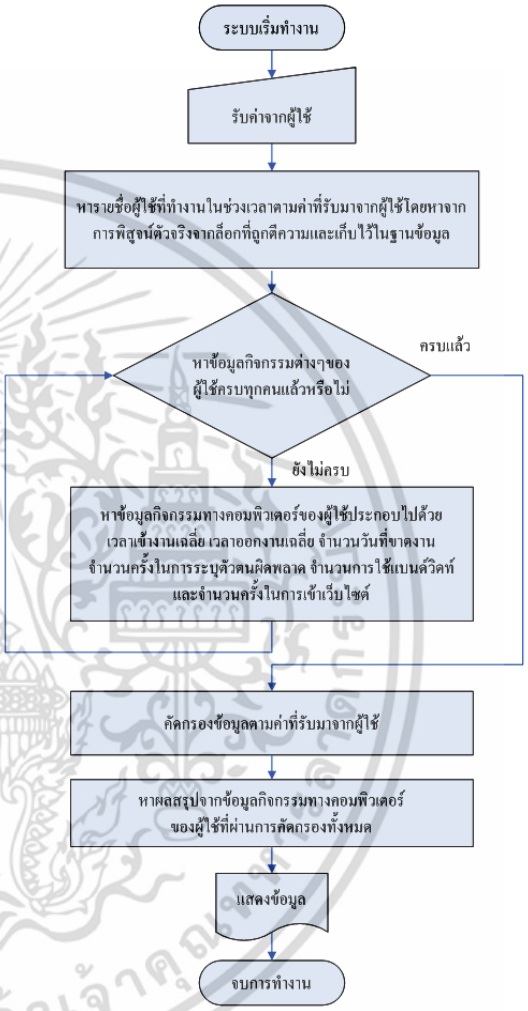
ออกงาน เพื่อนำข้อมูลมาวิเคราะห์ดูเวลาเข้าออกงานของผู้ใช้แต่ละคน แล้วจึงทำการบันทึกลงในฐานข้อมูลต่อไป

ส่วนของ Data Management จะทำหน้าที่เข้าถึงข้อมูลในฐานข้อมูลเพื่อนำข้อมูลมาวิเคราะห์ตามที่ผู้ใช้ร้องขอจากส่วนที่ติดต่อกับผู้ใช้ และทำการส่งผลลัพธ์ที่ได้กลับให้กับส่วนที่ติดต่อกับผู้ใช้ต่อไป นอกจากนี้ยังสามารถนำข้อมูลมาสร้างเป็นรายงานได้อีกด้วย สำหรับการค้นหาผู้กระทำความผิดทางคอมพิวเตอร์นั้นสามารถค้นหาได้จากตัวชี้แหล่งในอินเทอร์เน็ต (URL) หรือจากหมายเลขที่อยู่ไอพีสาธารณะ (Public IP) ของผู้เสียหายและหมายเลขที่อยู่ไอพีสาธารณะที่พนักงานในบริษัทใช้กระทำความผิด โดยระบบจะนำค่าที่รับจากผู้ใช้มาหาหมายเลขที่อยู่ไอพีส่วนตัว (Private IP) ของผู้กระทำความผิดจากข้อมูลล็อกของการแปลงไอพี (NAT) ที่เก็บอยู่ในฐานข้อมูลของโปรแกรมช่วยวิเคราะห์ข้อมูลล็อก เมื่อได้หมายเลขที่อยู่ไอพีส่วนตัวของผู้กระทำความผิดแล้ว ระบบจะนำหมายเลขที่อยู่ไอพีส่วนตัวของผู้กระทำความผิดนั้นมาหาผู้กระทำความผิดจากการพิสูจน์ตัวจริง และเมื่อระบบหาผู้กระทำความผิดได้แล้ว ระบบก็จะทำการส่งผลลัพธ์ไปยังส่วนต่อประสานกับผู้ใช้ต่อไป

ส่วนของ User Interface เป็นส่วนที่ติดต่อกับผู้ใช้ โดยมีโครงสร้างเป็นแบบเว็บแอปพลิเคชันที่ออกแบบด้วยภาษา Java และ HTML [8] ซึ่งประกอบด้วยส่วนที่ใช้ในการแสดงข้อมูลต่างๆ ตามที่ผู้ใช้ต้องการดู และส่วนของระบบคัดกรองข้อมูลเพื่อใช้ในการคัดกรองข้อมูลเมื่อผู้ใช้ต้องการที่จะดูข้อมูลอย่างระเอียด ซึ่งมีผังการทำงานของระบบในส่วนของ User Interface แสดงดังรูปที่ 4

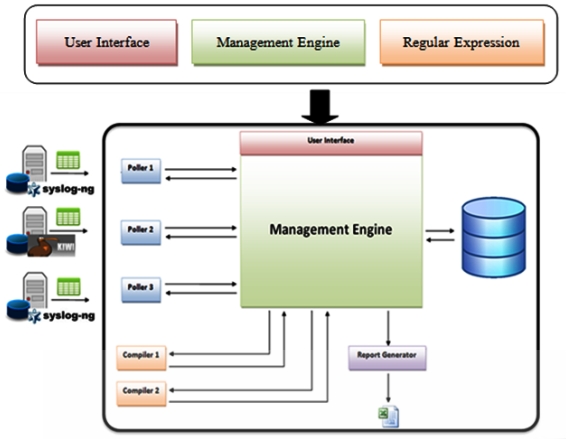
การออกแบบฐานข้อมูลโดยใช้ภาษา SQL [9] แบ่งออกได้เป็นสองส่วน ส่วนแรกทำหน้าที่ควบคุมการทำงานของระบบ ประกอบด้วยตารางควบคุมการทำงานของระบบเก็บข้อมูลการเข้าเว็บไซต์ และตารางควบคุมการทำงานของระบบเก็บข้อมูลเวลาเข้าออกงาน ส่วนที่สองทำหน้าที่เก็บข้อมูลต่างๆ ประกอบด้วยตารางเก็บข้อมูลการเข้าเว็บไซต์ และตารางเก็บข้อมูลเวลาเข้าออกงาน

ภาพรวมของระบบที่สมบูรณ์แสดงดังรูปที่ 5 ซึ่งแสดงให้เห็นถึงการติดต่อและการรับส่งข้อมูลระหว่างส่วนต่างๆของระบบ การทำงานของระบบเริ่มต้นจาก Poller ไปดึงล็อกจากเซิร์ฟเวอร์ล็อกต่างๆ และจัดรูปแบบให้อยู่ในรูปแบบที่ Management Engine ต้องการ แล้วจึงส่งล็อกที่ถูกจัดรูปแบบแล้วให้กับ Management Engine เพื่อบันทึกลงในฐานข้อมูล รวมทั้งนำล็อกที่ได้มาวิเคราะห์เพื่อส่งให้กับ Compiler ได้อย่างถูกต้องต่อไป



รูปที่ 4 แสดงผังการทำงานในส่วนของ User Interface

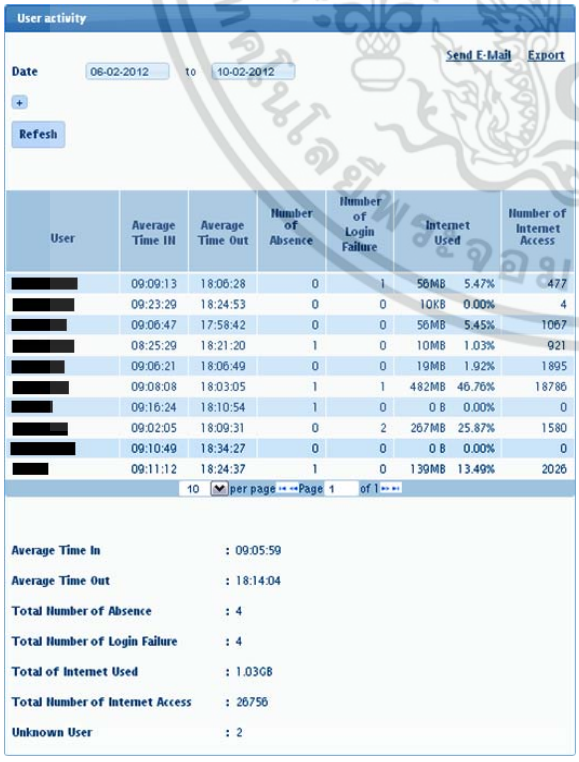
เมื่อ Compiler ได้รับล็อกมาแล้ว ก็จะนำล็อกที่ได้มาตีความและส่งผลลัพธ์กลับให้กับ Management Engine เพื่อบันทึกผลลงในฐานข้อมูลต่อไป นอกจากนี้เมื่อผู้ใช้ต้องการสร้างรายงาน Management Engine ก็จะนำผลลัพธ์ที่ได้จากการตีความแล้วส่งให้กับ Report Generator เพื่อทำการสร้างไฟล์รายงาน และเมื่อสร้างไฟล์รายงานเสร็จแล้ว Management Engine ก็จะส่งรายงานดังกล่าวผ่านทางอีเมลตามเวลาที่ผู้ใช้กำหนดต่อไป



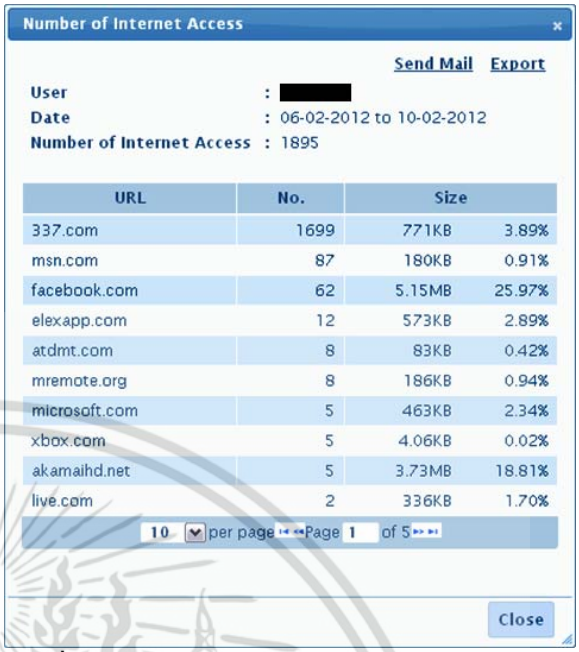
รูปที่ 5 แสดงภาพรวมของระบบที่สมบูรณ์

4. การทดสอบและวิเคราะห์ผล

หลังจากที่ได้พัฒนาระบบตามขั้นตอนที่ได้ออกแบบไว้ จึงได้ทำการทดสอบระบบทั้งหมดโดยแยกการทดสอบการทำงานของระบบออกเป็นส่วนๆ จนครบทุกส่วน โดยในที่นี้จะแสดงให้เห็นผลการทดสอบเป็นบางส่วน ได้แก่ ส่วนที่แสดงข้อมูลกิจกรรมทางคอมพิวเตอร์ของพนักงานในบริษัทดังแสดงในรูปที่ 6 และส่วนที่แสดงรายละเอียดการเข้าเว็บไซต์และการใช้แบนด์วิดท์ของพนักงานในบริษัทดังแสดงในรูปที่ 7 เป็นต้น



รูปที่ 6 แสดงหน้าข้อมูลกิจกรรมทางคอมพิวเตอร์



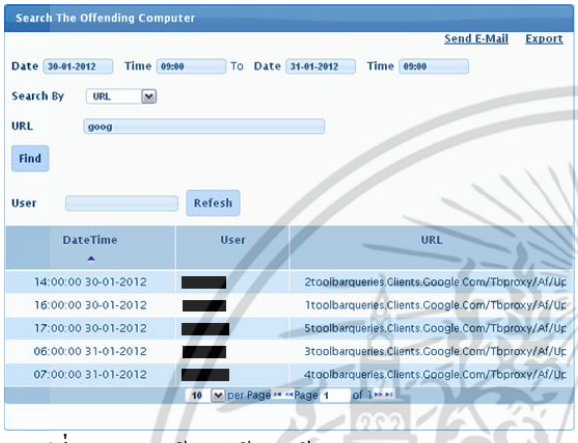
รูปที่ 7 แสดงหน้าการเข้าเว็บไซต์และการใช้แบนด์วิดท์

สำหรับในส่วนของการค้นหาผู้กระทำความผิดทางคอมพิวเตอร์นั้น ผู้ใช้สามารถเลือกค้นหาจากตัวชี้แหล่งในอินเทอร์เน็ตหรือจากหมายเลขที่อยู่ไอพี ถ้าผู้ใช้เลือกค้นหาจากตัวชี้แหล่งในอินเทอร์เน็ตจะมีช่องสำหรับรับค่า URL จากผู้ใช้ แต่ถ้าผู้ใช้เลือกค้นหาจากหมายเลขที่อยู่ไอพีจะมีช่องสำหรับรับค่าหมายเลขที่อยู่ไอพีของผู้เสียหายและของพนักงานในบริษัทที่ใช้กระทำความผิด ดังแสดงในรูปที่ 8 และ 9 ตามลำดับ จากผลลัพธ์ที่ได้จะช่วยให้ค้นหาผู้กระทำความผิดตาม พรบ. ได้ง่ายขึ้น และยังช่วยให้ค้นหาล็อกเพื่อใช้เป็นหลักฐานในการเอาผิดได้อีกด้วย

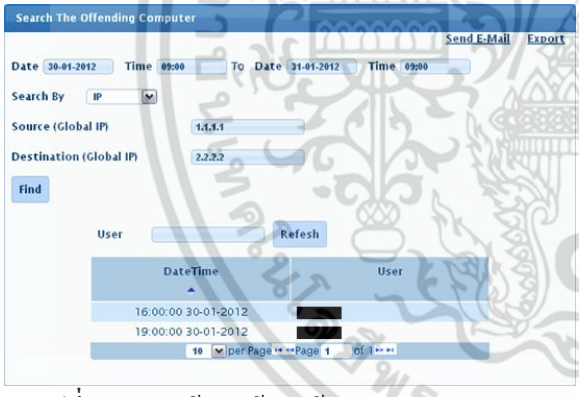
นอกจากนี้ยังได้ทำการทดสอบการสร้างรายงานข้อมูลต่างๆ ตัวอย่างเช่น รายงานข้อมูลเวลาเข้างานและออกงานของพนักงานในบริษัท ดังแสดงในรูปที่ 10 รวมทั้งการส่งไฟล์รายงานดังกล่าวผ่านทางอีเมลได้อีกด้วย

จากการทดสอบระบบทั้งหมดพบว่าระบบสามารถทำงานได้อย่างครบถ้วนสมบูรณ์ และให้ข้อมูลที่มีความถูกต้อง แต่ในกรณีที่มีข้อมูลจราจรหรือล็อกจำนวนมากๆ เช่น องค์การหรือบริษัทเอกชนขนาดใหญ่ ระบบจะใช้เวลาในการประมวลผลมากขึ้น เช่น ถ้าจำนวนล็อกเพิ่มขึ้นจากเดิมเป็น 2 เท่า ระบบจะต้องใช้เวลาในการสร้างรายงานเพิ่มขึ้นจากเดิมเป็น 1.5-1.7 เท่า และยังต้องใช้พื้นที่ในการ

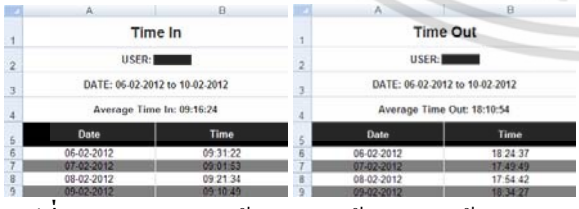
จัดเก็บข้อมูลเพิ่มขึ้นจากเดิมเป็น 2.3-2.5 เท่าอีกด้วย เมื่อเปรียบเทียบกับโปรแกรมที่มีการใช้งานอยู่ในปัจจุบัน เช่น Endian EnGarde หรือ PfSense จะพบว่าโปรแกรมนี้มีข้อดีคือสามารถตีความรูปแบบของล็อกได้หลากหลายกว่าไม่เฉพาะรูปแบบใดรูปแบบหนึ่ง และรองรับการเก็บรูปแบบของล็อกลงในฐานข้อมูลได้หลากหลายอีกด้วย แต่ข้อเสียของโปรแกรมนี้ก็คือไม่สามารถแสดงผลเป็นกราฟได้



รูปที่ 8 แสดงหน้าการค้นหาผู้กระทำความผิดจาก URL



รูปที่ 9 แสดงหน้าการค้นหาผู้กระทำความผิดจาก IP



รูปที่ 10 แสดงผลการสร้างรายงานข้อมูลเวลาเข้าออกงาน

5. สรุป

โปรแกรมตรวจสอบและวิเคราะห์ล็อกนี้สามารถแสดงข้อมูลกิจกรรมทางคอมพิวเตอร์ทั้งหมดของพนักงานในบริษัท ซึ่งประกอบด้วย เวลาเข้าออกงาน การขาดงาน การระบุตัวตนผิดพลาด การเข้าเว็บไซต์ต่างๆและจำนวนแบนด์วิดท์ที่ใช้ โดยสามารถแสดงเฉพาะข้อมูลของพนักงานแต่ละคนหรือแสดงข้อมูลรวมของพนักงานทั้งหมดได้ และผู้ใช้สามารถที่จะดูรายละเอียดของข้อมูลต่างๆได้ นอกจากนี้โปรแกรมยังสามารถสร้างไฟล์รายงานและส่งผ่านทางอีเมล รวมทั้งการค้นหาผู้กระทำความผิดทางคอมพิวเตอร์จาก URL หรือจาก IP ได้อีกด้วย ส่วนข้อจำกัดในการใช้งานโปรแกรมดังกล่าวนั่นคือเรื่องของความเร็วในการประมวลผล ซึ่งเป็นผลมาจากขั้นตอนวิธีที่เลือกใช้อาจยังไม่ดีพอ ทำให้ระบบทำงานได้ช้า ดังนั้นการพัฒนาต่อยอดในอนาคตจะมุ่งเน้นที่การพัฒนาขั้นตอนวิธีที่เหมาะสมเพื่อเพิ่มประสิทธิภาพของโปรแกรมในส่วนของการเก็บข้อมูลจากโปรแกรมช่วยวิเคราะห์ข้อมูลล็อก หรือในส่วนของการดึงข้อมูลไปแสดงที่ส่วนต่อประสานกับผู้ใช้ ก็จะช่วยลดปัญหาดังกล่าวได้

6. กิตติกรรมประกาศ

งานวิจัยนี้ได้รับการสนับสนุนเครื่องมือและอุปกรณ์จากบริษัท Credger จำกัด

7. เอกสารอ้างอิง

[1] http://www.mict.go.th/download/law/20070618_CC_Final.pdf

[2] Anand Deveriya, “Network Administrators Survival Guide,” Cisco Press, 2005.

[3] http://www.kiwisyslog.com/kiwi-syslog-server-overview/

[4] Jan Goyvaerts and Steven Levithan, “Regular Expressions Cookbook,” O’Reilly Media, 2009.

[5] http://rubyonrails.org

[6] Sam Ruby, Dave Thomas and David Heinemeier Hansson, “Agile Web Development with Rails,” The Pragmatic Programmers, 2011.

[7] http://www.logzilla.pro

[8] Eric Ladd and Jim O’Donnell, “Using HTML 4, XML and Java 1.2,” Que, 1998.

[9] Seyed M.M. Tahaghoghi and Hugh E. Williams, “Learning MySQL,” O’Reilly Media, 2006.