ระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP

สิบเอกสุบัน โสวาที

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม บัณฑิตวิทยาลัย มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2554

Intrusion Warning System Using Voice Over IP Technology

Sergeant Suban Sowathee

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering

Department of Computer and Telecommunication Engineering

Graduate School, Dhurakij Pundit University

2011

กิตติกรรมประกาศ

การจัดทำวิทยานิพนธ์ฉบับนี้สำเร็จสมบูรณ์ลงได้ ด้วยความเมตตากรุณาจาก อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ให้ข้อคิดเห็น คำแนะนำที่เป็นประโยชน์ต่องานวิจัย อาจารย์ ดร.ธนัญ จารุวิทยโกวิท อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม ที่สละเวลาอันมีค่า คอยให้คำแนะนำให้คำปรึกษา ตลอดจนแนวทางในการแก้ไขปัญหาต่างๆ และเอาใจใส่ข้าพเจ้ามาโดยตลอด ข้าพเจ้ารู้สึกซาบซึ้งเป็นอย่างยิ่ง จึงขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอขอบพระคุณ อาจารย์ ดร.ประศาสน์ จันทราทิพย์ ที่กรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ และ รองศาสตราจารย์ปุณยวีร์ จามจรีกุล ที่กรุณารับเป็นคณะกรรมการสอบวิทยานิพนธ์ ซึ่งได้ให้คำชี้แนะ แก้ไขข้อบกพร่องของวิทยานิพนธ์ฉบับนี้จนสำเร็จสมบูรณ์ด้วยดี

ขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ประสิทธิประสาทวิชาความรู้ จนข้าพเจ้าประสบความสำเร็จในการศึกษา ขอขอบพระคุณเพื่อนร่วมรุ่น พี่ๆ น้องๆ ทุกๆ คน รวมถึงคณะเจ้าหน้าที่ประจำหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต และคณะเจ้าหน้าที่บัณฑิตวิทยาลัย ทุกท่าน ซึ่งไม่อาจกล่าวนามได้ทั้งหมดในที่นี้ ที่ได้ให้กำลังใจและช่วยเหลือข้าพเจ้ามาโดยตลอด

ขอขอบคุณ คุณกานต์พิชชา ยอดน้ำคำ คุณศกุนี อิ่มกระโทก และคุณทิพวรรณ กรสลี ที่คอยให้ความช่วยเหลือประสานงานทุกๆ ด้านตลอดมา

ขอขอบพระคุณ นายสนิท โสวาที และนางทองวัน โสวาที ผู้ซึ่งเป็นบิดา มารดา อันเป็นที่รักของข้าพเจ้า ที่ได้ให้ความรัก ให้คำปรึกษา ให้กำลังใจข้าพเจ้ามาโดยตลอดจนสำเร็จการศึกษา

ท้ายสุดนี้ คุณความดีและกุศลที่พึงบังเกิดมีจากการจัดทำวิทยานิพนธ์ของข้าพเจ้า ซึ่งสามารถก่อให้เกิดความรู้และข้อคิดอันควรค่าแก่การศึกษา หรือปฏิบัติให้เกิดประโยชน์ต่อส่วนรวม ข้าพเจ้าขอมอบระลึกบูชาคุณแด่ บิดา มารดา ครู อาจารย์ ผู้มีพระคุณ ตลอดจน ผู้แต่งหนังสือหรือตำราทุกท่าน ที่ข้าพเจ้าใช้อ้างอิงในวิทยานิพนธ์ฉบับนี้ ข้าพเจ้ามีความซาบซึ้งในความกรุณาอันดียิ่งจากทุกท่าน และขอกราบขอบพระคุณมา ณ โอกาสนี้ หากมีข้อบกพร่องประการใด ข้าพเจ้าขอน้อมรับไว้แต่เพียงผู้เดียว

ส.อ.สุบัน โสวาที

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

หัวข้อวิทยานิพนธ์ ระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP
ชื่อผู้เขียน ส.อ.สุบัน โสวาที
อาจารย์ที่ปรึกษา อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์
อาจารย์ที่ปรึกษาร่วม อาจารย์ ดร.ธนัญ จารุวิทยโกวิท
สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม
ปีการศึกษา 2553

บทคัดย่อ

ในปัจจุบันความต้องการในการรักษาความปลอดภัยทั้งในส่วนของทรัพย์สิน และอสังหาริมทรัพย์มีมากขึ้น การรักษาความปลอดภัยโดยใช้กล้องวงจรปิดสามารถตอบสนองต่อความต้องการเหล่านั้นได้ดีในระดับหนึ่ง โดยระบบจะแจ้งเตือนเป็นสัญญาณเสียงฉุกเฉินในที่เกิดเหตุ เพื่อให้ผู้บุกรุกตกใจกลัว ปัจจุบันกล้องวงจรปิดมีการพัฒนาจากระบบอนาล็อกไปสู่ระบบไอพี ทำให้ผู้ใช้งานสามารถดูภาพเหตุการณ์สด หรือภาพเหตุการณ์ย้อนหลังจากที่ใดก็ได้โดยการเชื่อมต่อผ่านอินเตอร์เน็ต แต่ระบบยังขาดความสามารถในการส่งเสียงเตือน ณ ที่เกิดเหตุเป็นเสียงพูด และการโทรศัพท์แจ้งการบุกรุกผ่านระบบไอพีไปยังผู้ใช้งานอย่างทันท่วงที ส่งผลให้ผู้ใช้งานระบบไม่สามารถรับทราบถึงการบุกรุกที่เกิดขึ้นอย่างทันท่วงที เพื่อให้ได้รับการป้องกันได้อย่างรวดเร็วที่สุด งานวิจัยนี้จึงเสนอแนวคิดที่จะนำเทคโนโลยี Voice over Internet Protocol (VoIP) ซึ่งเป็นเทคโนโลยีการสื่อสารแบบใหม่ที่สามารถ รับ – ส่ง สัญญาณเสียงผ่านทางเครือข่ายไอพี โดยอาศัยอุปกรณ์ (Hardware) และโปรแกรมคอมพิวเตอร์ (Software) มาประยุกต์เข้ากับระบบรักษาความปลอดภัยด้วยกล้องวงจรปิดแบบไอพี โดยเมื่อระบบ สามารถตรวจจับการบุกรุก ของผู้ไม่หวังดี ระบบจะส่งเสียงพูดที่ได้บันทึกไว้ในที่เกิดเหตุ ส่งอีเมล์ และโทรศัพท์ แจ้งให้ผู้ใช้งานทราบผ่านระบบ VoIP ผู้ใช้งานสามารถเชื่อมต่อผ่านอินเตอร์เน็ต เพื่อดูภาพเหตุการณ์ ในขณะนั้น หรือภาพเหตุการณ์ การบุกรุกที่บันทึกไว้ได้ ระบบที่พัฒนายังสามารถใช้งานร่วมกับกล้องวงจรปิดแบบไอพีได้จากหลายผู้ผลิตได้ ผลการทดสอบพบว่าระบบสามารถทำงาน ตามวัตถุประสงค์ที่ตั้งไว้ได้เป็นอย่างดี

Thesis Title	Intrusion Warning System Using VoIP Technology
Author	Sgt.Suban Sowathee
Thesis Advisor	Chiyaporn Khemapatapan, Ph.D
Co-Thesis Advisor	Tanun Jaruvitayakovit, Ph.D
Department	Computer and Telecommunication Engineering
Academic Year	2010

ABSTRACT

Currently, demand for security in parts of the property and real estate has increased. Security system using CCTV can meet those needs in a certain level. The system will alert the emergency signal at that place to panic an intruder. CCTV has now evolved from analog to IP systems. The new system allows users to view live event or recorded scene from anywhere by connecting to the Internet. Unfortunately, the system cannot alarm by human speech and immediately call via IP to the user to report the intrusion event. As the result, user can not acknowledge the intrusion that occurs in a timely manner. So, the system cannot be protected as quickly as possible. This research proposes an idea to use Voice over Internet Protocol (VoIP) technology, a new communications technology that can receive - send audio via IP networks based on device (hardware) and software, to apply to the security system using IP camera. When the system detects an intrusion of a non-wisher, the system will play the recorded human-voice at that place, email and phone to the user via VoIP. The user can connect through the Internet to view the intrusion recorded picture. The developed system can be used in conjunction with any IP camera in multi-vendors environment .Test results showed that the system can work well as the targeted purpose.

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันความต้องการในการรักษาความปลอดภัยทั้งในส่วนของทรัพย์สิน และอสังหาริมทรัพย์มีมากขึ้น การใช้เทคโนโลยีการรักษาความปลอดภัยสามารถตอบสนองต่อความต้องการเหล่านั้นได้เป็นอย่างดี ซึ่งสามารถรักษาความปลอดภัยได้ในระดับหนึ่ง โดยการแจ้งเตือนให้ผู้ที่เป็นเจ้าของทรัพย์สินได้ทราบ และสามารถดำเนินการต่อไปได้

ระบบรักษาความปลอดภัย หรือระบบกันขโมยปัจจุบันมีอยู่ด้วยกันหลายระบบ แต่หลักๆ แล้วจะใช้กันอยู่ 4 ระบบใหญ่ๆ คือระบบกล้องโทรทัศน์วงจรปิด (Clos Circuit Television: CCTV) ระบบสัญญาณกันขโมย (Alarm system) ระบบการควบคุมการเข้าออก (Access control) และระบบแจ้งเตือนอัคคีภัย (Fire alarm) ซึ่งแต่ละระบบนั้นมีวัตถุประสงค์ในการใช้งานแตกต่างกันอย่างสิ้นเชิง การที่จะเลือกใช้ระบบใดนั้น จึงขึ้นอยู่กับวัตถุประสงค์ที่ต้องการนั่นเอง กล้องวงจรปิดเป็นที่นิยมมากที่สุดในระบบการรักษาความปลอดภัยในขณะนี้ ซึ่งปัจจุบันมีการพัฒนาจากระบบอนาล็อกไปสู่ระบบไอพี ทำให้ผู้ใช้งานสามารถดูภาพเหตุการณ์สด หรือภาพเหตุการณ์ย้อนหลังจากที่ใดก็ได้โดยการเชื่อมต่อผ่านอินเตอร์เน็ต แต่ระบบยังขาดความสามารถในการส่งเสียงเตือน ณ ที่เกิดเหตุเป็นเสียงพูด และการโทรศัพท์แจ้งการบุกรุกผ่านระบบไอพีไปยังผู้ใช้งานอย่างทันท่วงที ส่งผลให้ผู้ใช้งานระบบไม่สามารถรับทราบถึงการบุกรุกที่เกิดขึ้นอย่างทันท่วงที เพื่อให้ได้รับการป้องกันได้อย่างรวดเร็วที่สุด งานวิจัยนี้จึงเสนอแนวคิดที่จะนำเทคโนโลยี Voice over Internet Protocol (VoIP) ซึ่งเป็นเทคโนโลยีการสื่อสารแบบใหม่ที่สามารถรับ – ส่ง สัญญาณเสียงผ่านทางเครือข่ายไอพี โดยอาศัยอุปกรณ์ (Hardware) และโปรแกรมคอมพิวเตอร์ (Software) มาประยุกต์เข้ากับระบบรักษาความปลอดภัยด้วยกล้องวงจรปิดแบบไอพี โดยเมื่อระบบสามารถตรวจจับการบุกรุกของผู้ไม่หวังดี ระบบจะส่งเสียงพูดที่ได้บันทึกไว้ในที่เกิดเหตุ ส่งอีเมล์และโทรศัพท์แจ้งให้ผู้ใช้งานทราบผ่านระบบ VoIP ผู้ใช้งานสามารถเชื่อมต่อผ่านอินเตอร์เน็ต เพื่อดูภาพเหตุการณ์ในขณะนั้น หรือภาพเหตุการณ์การบุกรุกที่บันทึกไว้ได้ ระบบที่พัฒนายังสามารถใช้งานร่วมกับกล้องวงจรปิดแบบไอพีได้จากหลายผู้ผลิตได้ผลการทดสอบพบว่าระบบสามารถทำงานตามวัตถุประสงค์ที่ตั้ง ไว้ได้เป็นอย่างดี

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษา ออกแบบ และพัฒนาระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี Voice over IP (VoIP) โดยการประยุกต์ใช้ซอฟต์แวร์ Asterisk (IP-PBX) และ Zoneminder (Digital Video Recorder)

2. เพื่อให้ผู้ใช้งานระบบได้รับการแจ้งการบุกรุก และมีการส่งเสียงเตือน ณ ที่เกิดเหตุโดยอัตโนมัติ

3. เพื่อจำลองสถานการณ์โดยการทดสอบระบบที่พัฒนา และพิสูจน์ว่าระบบสามารถใช้งานได้จริง

1.3 ขอบเขตงานวิจัย

ขอบเขตของการศึกษางานวิจัยนี้ ให้ความสำคัญกับระบบรักษาความปลอดภัยโดยการประยุกต์ใช้ Asterisk (IP-PBX) และ Zoneminder (Digital Video Recorder) ในการออกแบบระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP

1. ออกแบบและพัฒนาระบบการรักษาความปลอดภัยโดยมีคุณสมบัติดังนี้
   1) ใช้ Zoneminder ตรวจจับการเคลื่อนไหวในบริเวณที่ต้องการรักษาความปลอดภัย
   2) ผู้ใช้งานสามารถระบุตำแหน่งหรือบริเวณที่ต้องการตรวจจับการเคลื่อนไหวได้
   3) ในกรณีที่มีการตรวจพบการเคลื่อนไหวในบริเวณที่ระบุตำแหน่งไว้ ระบบสามารถ
      3.1) ส่งเสียงพูดที่ได้บันทึกไว้ ณ จุดเกิดเหตุเพื่อขับไล่ผู้บุกรุก
      3.2) ส่งอีเมล์ไปยังผู้ใช้ระบบ
      3.3) โทรศัพท์ผ่านระบบไอพีแจ้งผู้ใช้งาน หรือเจ้าหน้าที่รักษาความปลอดภัย
      3.4) เมื่อผู้ใช้งานได้รับแจ้งเหตุแล้วสามารถตรวจสอบภาพบริเวณที่เกิดเหตุผ่านโทรศัพท์มือถือ หรือเครื่องคอมพิวเตอร์เพื่อดูภาพเหตุการณ์จริง หรือเหตุการณ์การบุกรุกที่ระบบบันทึกไว้ได้
      3.5) ผู้ใช้งานสามารถโทรศัพท์ผ่านระบบไอพีเข้ามา ณ ที่เกิดเหตุ เพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุ

2. ภายหลังการพัฒนา จะมีการทดสอบการใช้งานระบบ ในเวลาที่มีปริมาณแสงสว่างมาก (เวลา 12.00 น.) และในเวลาที่มีปริมาณแสงสว่างน้อย (เวลา 18.00 น.) เพื่อตรวจสอบ ความถูกต้องในการทำงานของระบบ เป็นเวลาอย่างน้อย 3 วัน และจะมีการจำลองการบุกรุก อย่างน้อย 20 ครั้ง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ต้นแบบระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี Voice over IP (VoIP) โดยการประยุกต์ใช้ซอฟต์แวร์ Asterisk (IP-PBX) และ Zoneminder (Digital Video Recorder)

2. ผู้ใช้งานระบบได้รับการแจ้งการบุกรุก และมีการส่งเสียงเตือน ณ ที่เกิดเหตุโดยอัตโนมัติ

3. ด้วยการลงทุนที่ไม่มากจะทำให้ระบบดังกล่าวสามารถนำไปใช้ประโยชน์ได้อย่างกว้างขวาง ในด้านระบบการรักษาความปลอดภัย

4. เพิ่มประสิทธิภาพในการใช้งานระบบเครือข่ายอินเทอร์เน็ตที่มีอยู่ให้เกิดประโยชน์สูงสุด

5. สามารถนำไปพัฒนาต่อยอดให้ระบบสามารถนำไปใช้งานในเชิงพาณิชย์ได้

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในวิทยานิพนธ์ฉบับนี้ มีทฤษฎีที่เกี่ยวข้องในด้านต่างๆ เพื่อช่วยในการพัฒนาระบบ คือ ระบบกล้องวงจรปิด (CCTV), Zoneminder, VoIP, Asterisk, AGI - Asterisk Gateway Interface, PHP และ MySQL รวมถึงงานวิจัยและผลงานที่เกี่ยวข้อง

2.1 ระบบกล้องวงจรปิด (CCTV: Closed-Circuit Television) (ระบบโทรทัศน์วงจรปิด, 2553)

2.1.1 ระบบรักษาความปลอดภัย หรือระบบกันขโมยปัจจุบันมีอยู่ด้วยกันหลายประเภท แต่หลักๆ แล้ว จะใช้กันอยู่ 4 ระบบใหญ่ๆ คือ ระบบกล้องโทรทัศน์วงจรปิด, ระบบสัญญาณกันขโมย (Alarm system), ระบบการควบคุมการเข้าออก (Access control), ระบบแจ้งเตือนอัคคีภัย (Fire alarm) ซึ่งแต่ ระบบนั้นมีวัตถุประสงค์ในการใช้งานแตกต่างกันอย่างสิ้นเชิง การที่จะเลือกใช้ระบบใดนั้น จึงขึ้นอยู่กับ วัตถุประสงค์ที่ต้องการนั่นเอง

2.1.2 ประโยชน์ของกล้องวงจรปิด

1) ส่งสัญญาณเตือนหากทรัพย์สินที่มีค่าสูงถูกเคลื่อนย้ายออกจากจุดที่เคยอยู่เดิม

2) แจ้งเตือนหากมีผู้บุกรุกเข้ามาในเขตหวงห้าม และหากใช้ร่วมกับกล้องโทรทัศน์วงจรปิดชนิดหมุนได้รอบตัว จะสามารถติดตามความเคลื่อนไหวของบุคคลต้องสงสัยได้โดยอัตโนมัติ แม้จะไม่มีเจ้าหน้าที่ปฏิบัติงานในห้องควบคุม

2.1.3 ระบบกล้องโทรทัศน์วงจรปิด

ระบบโทรทัศน์วงจรปิด (CCTV System) เป็นการส่งสัญญาณภาพ จากกล้องโทรทัศน์วงจรปิดที่ ได้ติดตั้งตามที่ต่างๆ มายังส่วนรับภาพ/ดูภาพ ซึ่งเรียกว่า จอภาพ (Monitor) โดยทั่วไปจะติดตั้งอยู่คนละที่กับกล้อง กล้องโทรทัศน์วงจรปิดนั้นปัจจุบันแบ่งออกได้เป็น 2 ชนิด คือ IP camera และ Analog camera กล้องโทรทัศน์วงจรปิด นั้นเหมาะสำหรับการใช้ในจุดที่ต้องการเฝ้าระวังหรือต้องการบันทึกโดยต้องใช้งานร่วมกับระบบบันทึกภาพไม่ว่าจะเป็น DVR (digital video recording) หรือ NVR (network video recording) ในส่วนเฉพาะของตัวกล้องเองนั้นไม่มีคุณสมบัติในการป้องกันภัยหรือเตือนภัยได้ แม้ว่าจะมีระบบ Motion Detection ก็ตาม เนื่องจากอัตราการเกิดการเตือนภัยผิดพลาด (Fault alarm) ที่สูงมาก เพราะระบบการตรวจจับของกล้องโทรทัศน์วงจรปิดนั้นใช้อัลกอริทึม (Algorithm) แบบง่ายๆ ซึ่งเกี่ยวข้องกับหลายปัจจัย จึงทำให้ต้องสั่งปิดการใช้งานใน

Mode นี้ ในที่สุดเราจึงพบตามข่าวได้บ่อยครั้งว่าเกิดเหตุโจรปล้นแล้ว ตำรวจจึงนำภาพที่ได้จากกล้องโทรทัศน์วงจรปิดดูย้อนหลัง เพราะฉะนั้นจึงได้มีการพัฒนาซอร์ฟแวร์ขึ้นมาเพื่อตรวจจับ และเตือนภัยไปยังผู้ใช้งานระบบ หนึ่งในนั้นก็คือโปรแกรม Zoneminder ซึ่งสามารถตอบสนองต่อความต้องการนี้ได้ แต่ในที่สุดก็ยังขาดระบบการส่งเสียงแจ้งเตือนผู้บุกรุก ณ ที่เกิดเหตุ และการแจ้งเตือนในทันที (Real-time) ผู้พัฒนาระบบจึงได้นำเอาเทคโนโลยี VoIP โปรแกรม Asterisk มาประยุกต์ใช้เพื่อตอบสนองต่อความต้องการดังกล่าว

2.1.4 หน้าที่ของกล้องวงจรปิด

กล้องวงจรปิดทำหน้าที่รับภาพที่ปรากฏอยู่และทำการแปลงเป็นสัญญาณ และทำการส่งสัญญาณดังกล่าวไปในจุดที่ต้องการในลักษณะ point to point ซึ่งตัวรับภาพของกล้องวงจรปิดนั้นแบ่งได้เป็น 2 แบบ คือ

1) ซีมอส (Complementary Metal Oxide Semiconductor: CMOS) ซึ่งมีพื้นฐานมาจากเทคโนโลยีการผลิตสารกึ่งตัวนำ มีคุณสมบัติเด่นในเรื่องของการบริโภคพลังงานต่ำและมีความร้อนสะสมต่ำ โดยการทำงานอาศัยทรานซิสเตอร์พื้นฐานหลายๆตัว ซึ่งจะใช้กับกล้องวงจรปิดที่มีราคาถูก คุณภาพต่ำ

2) ซีซีดี (Charge-Coupled Device: CCD) ซึ่งผลิตขึ้นโดยเฉพาะเพื่อจุดประสงค์ให้เป็นอุปกรณ์รับแสงในรูปแบบต่างๆ โดยประกอบด้วย IC ที่จัดเรียงแถวเชื่อมต่อ หรือจับคู่กันเป็นจำนวนมาก และตัวเก็บประจุที่ไวต่อแสงจะใช้กับกล้องวงจรปิดที่มีคุณภาพปานกลาง-สูง ซึ่งในกล้องวงจรปิดในปัจจุบันนี้ ได้เลือกใช้ CCD Sensor ทั้งหมดแล้ว เนื่องจากราคาของ CCD Sensor ได้ลดลงมากแล้ว ซึ่งหากแบ่งตามรูปทรงการใช้งานนั้นจะสามารถแบ่งได้หลักๆ ดังนี้

2.1) กล้องวงจรปิดแบบโดม (Dome CCTV) ซึ่งก็มีทั้งแบบติดตั้งในอาคาร (Indoor) และติดตั้งนอกอาคาร (Outdoor) ซึ่งเหมาะสมติดตั้งในจุดที่ต้องการความเรียบร้อยและสวยงาม เนื่องจากจะดูกลมกลืน ไม่เกะกะสายตา

2.2) กล้องวงจรปิดแบบ C/CS Mount (C/CS Mount CCTV) ซึ่งมีแบบ ติดตั้งในอาคารเท่านั้น โดยสามารถ ติดตั้งในกล่องกันฝน เพื่อใช้งานติดตั้งนอกอาคารได้เช่นกัน และกล้องวงจรปิดชนิดนี้สามารถเปลี่ยนเลนส์เพื่อให้เหมาะสมกับการใช้งานได้หลากหลาย เช่น เลนส์หมุนกว้าง มุมแคบ และชนิดปรับลดแสงอัตโนมัติ (Auto Iris)

2.3) กล้องวงจรปิดแบบอินฟราเรด (Infrared CCTV) ซึ่งมีทั้งแบบติดตั้งในอาคารและติดตั้งนอกอาคาร โดยจะทำในหลายรูปแบบ เช่น Infrared Dome CCTV, Built-in Lens Infrared CCTV โดยกล้องวงจรปิดแบบนี้มีจุดเด่นที่สามารถรับภาพได้แม้ในที่มืดสนิท (0 Lux)

2.4.5 กล้องวงจรปิดส่วนมากที่ใช้งานในปัจจุบันนี้มี 2 ลักษณะ คือ

1) ติดตั้งตายตัว (Fixed Camera) หมายถึงตัวกล้องจะติดตั้งอยู่บนขากล้องหรืออื่นๆ ซึ่งไม่สามารถจะขยับ หรือหมุนเปลี่ยนทิศทางในการดูได้ ถ้าต้องการหมุนหรือเปลี่ยนทิศทางก็จะต้องถอดตัวกล้องแยกออกจากขากล้องจึงจะเปลี่ยนตำแหน่งได้

2) สามารถหมุนปรับทิศทางได้ (Moving Camera) เพื่อเป็นการเพิ่มประสิทธิภาพในการใช้งานระบบโทรทัศน์วงจรปิด จึงได้มีการเพิ่มอุปกรณ์ประกอบเข้าไป คือ ฐานกล้องหมุนปรับทิศได้ และเลนส์ปรับขนาดภาพได้

2.1) ฐานกล้องหมุนปรับทิศได้ (Pan & Tilt Unit) ช่วยเพิ่มประสิทธิภาพให้กล้องสามารถที่จะเปลี่ยนได้หลายทิศทาง ทั้งมุมต่ำ และมุมสูง เช่น กล้องที่ติดตั้งอยู่กับ Pan & Tilt Unit ติดตั้งบนเสามีความสูงประมาณ 10 เมตร สามารถที่จะปรับมุมก้มเพื่อจะดูวัตถุ หรือคนที่อยู่บนพื้นดิน ซึ่งมีระดับต่ำกว่าตำแหน่งที่ติดตั้งกล้อง หรือมุมเงย เพื่อมองไปยังอาคารที่สูงกว่า ไม่ว่าจะเป็นทิศทางตรงด้านหน้า หรือจะหมุนไปยังทิศทางอื่นๆ ก็สามารถทำได้

2.2) เลนส์ปรับขนาดภาพได้ (Zoom Lens) เป็นเลนส์ที่สามารถเปลี่ยนขนาดภาพได้ (เปลี่ยนความยาวโฟกัส) เลนส์ฯ ที่นำมาใช้กับกล้องที่มี Pan & Tilt Unit ส่วนมากจะเป็นชนิดที่ควบคุมการทำงานด้วยมอเตอร์ เราจึงเรียกว่า Motorized Zoom Lens การเลือกใช้ Motorized Zoom Lens ควร จะเลือกให้เหมาะกับงานที่จะใช้ เพราะว่า Motorized Zoom Lens มีหลายแบบหลายขนาดตามความยาวโฟกัส

2.1.6 ชนิดของกล้องวงจรปิด

ชนิดของกล้อง กล้องวงจรปิดมีหลายชนิดหลายแบบ โดยแบ่งได้คร่าวๆ ดังนี้

1) กล้องแบบ CS MOUNT เป็นกล้องที่ต้องใช้เลนส์ต่อกับกล้อง ทำให้เกิดภาพข้อดี คือ ภาพจะ ชัด เพราะเลนส์ที่ใช้เป็นเลนส์มาตรฐานขนาดใหญ่

2) กล้องแบบโดม เหมาะสำหรับสถานที่ที่ต้องการความสวยงามหรือไม่ต้องการให้สังเกตเห็นว่ามี การติดตั้งกล้องวงจรปิด

2.1.7 ความละเอียดของภาพ (RESOLUTION)

กล้องที่ให้ภาพจะชัดเจนหรือไม่ขึ้นอยู่กับชนิดของแผ่นรับภาพ CCD ซึ่งแบ่งได้ 2 แบบ คือ

1) NORMAL RESOLUTON เป็นแบบที่มีความละเอียดของภาพปกติประมาณ 330 - 380 TV LINE

2) HIGN RESOLUTION เป็นแบบที่มีความละเอียดของภาพสูงประมาณ 400 - 550 TV LINE หมายเหตุ กล้องที่มีความละเอียดของภาพสูงจะมีราคาสูงตามไปด้วย

2.1.8 กล้องไอพี (IP Camera)

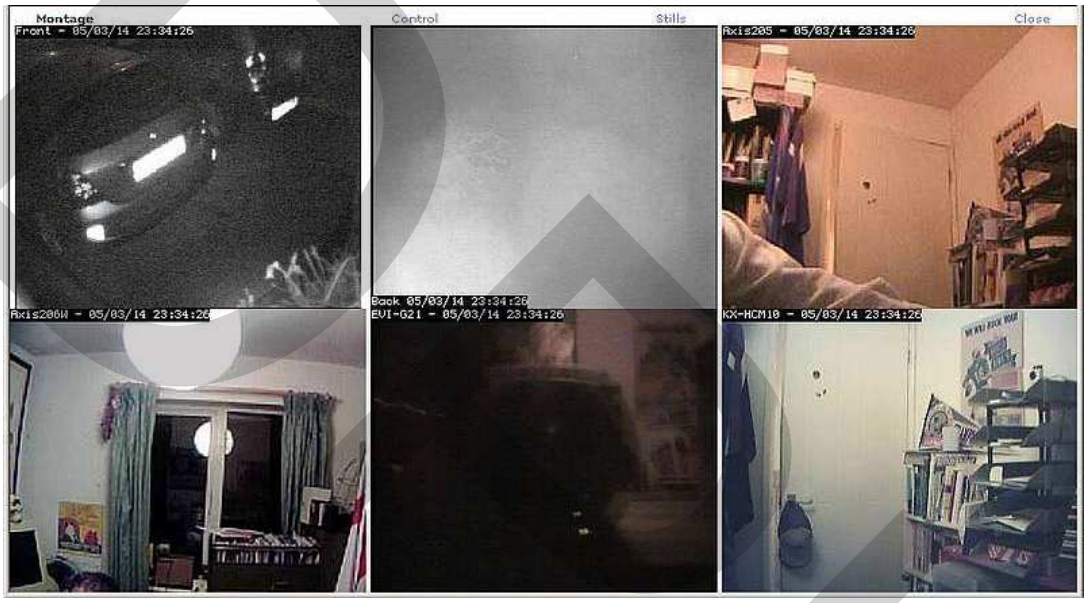
เราสามารถจะคิดได้ว่ากล้องไอพีก็คือกล้องโทรทัศน์วงจรปิดที่รวมเอาคอมพิวเตอร์เข้าไปอยู่ข้างในเป็นอันหนึ่งอันเดียวกัน จะเก็บภาพสถานการณ์สดๆ และยิงผ่านไปบนระบบเครือข่ายไอพี (IP) และอนุญาตให้ผู้ใช้สามารถมองเห็นเหตุการณ์จากระยะไกล และสามารถจัดเก็บภาพเห็นการณ์นั้น รวมถึงการควบคุมหรือตั้งค่ากล้องผ่านทางระบบไอพีได้ กล้องไอพีจะมีไอพีแอดเดรส (IP Address) เป็นของตัวเอง ไอพีแอดเดรสก็เปรียบเสมือนกับบ้านเลขที่ของเรา ทำให้ใครต่อใครรู้ว่าเราอยู่ที่ไหน ซึ่งก็เหมือนกับในกรณีของไอพีแอดเดรสผู้ใช้แค่ทราบข้อมูลไอพี ของกล้องเท่านั้นก็สามารถเรียกดูข้อมูลจากกล้องได้ โดยแค่พิมพ์ไอพีแอดเดรสของกล้องไปบนเบราว์เซอร์ (Browser)

กล้องไอพีไม่จำเป็นต้องต่อกับคอมพิวเตอร์อยู่ตลอดเวลา (ซึ่งจะต่างจากเว็บแคม เพราะจำเป็นต้องต่อกับคอมพิวเตอร์) สามารถทำงานได้ด้วยตัวเอง และสามารถที่จะเอาไปติดตั้งที่ไหนก็ได้ที่มีระบบเครือข่าย ที่มากไปกว่านั้นก็คือ กล้องไอพียังเพิ่มเติมฟังก์ชั่นการทำงานอื่นๆอีกมากมาย เช่น ฟังก์ชั่นตรวจจับการเคลื่อนไหว ซึ่งจะคอยเช็คดูว่ามีสิ่งผิดปกติเคลื่อนไหวผ่านหน้าไปหรือเปล่า หากพบว่ามีสิ่งผิดปกติก็จะถ่ายภาพเก็บไว้หรือไม่ก็มีการเตือนไปยังผู้ดูแลหรือส่งอีเมล์ไปถึงเจ้าของได้

2.2 Zoneminder (Zoneminder, 2553**)**

Zoneminder เป็นระบบ DVR (Digital Video Recorder) หรือระบบบันทึกกล้องวงจรปิด โดย Zoneminder จะทำงานผ่านเว็บ พัฒนาขึ้นโดยใช้ภาษา PHP, C/C++, LINUX script มีการเก็บข้อมูลต่างๆ ลงฐานข้อมูล MySQL และใช้ Apache ทำหน้าที่เป็น Web Server จุดเด่นของ Zoneminder คือระบบ Motion detect (ระบบตรวจจับการเคลื่อนไหว) ซึ่งก็มีหลาย algorithm ให้ใช้ตามสถานการณ์และความเหมาะสม Zoneminder สามารถใช้เพื่อแก้ปัญหาในการ Capture วิเคราะห์ บันทึก และการปฏิบัติงานที่เกี่ยวกับภาพเคลื่อนไหวจากกล้องวงจรปิด หรือกล้องวีดีโอที่ใช้ในการรักษาความปลอดภัย (Camera Video Security) กล้องวีดีโอทั่วไป กล้องที่เชื่อมต่อด้วยสาย USB และกล้อง IP (IP Network Camera) สามารถทำงานได้บนระบบปฏิบัติการ Linux Zoneminder ถูกออกแบบมาให้สามารถทำงานในระบบแบบกระจาย สามารถเชื่อมต่อกับกล้องได้หลายกล้อง ดังแสดงในภาพที่ 2.1 สามารถถ่ายโอนข้อมูลที่เป็นภาพวีดีผ่านทางระบบเครือข่ายคอมพิวเตอร์โดยเว็บบราวเซอร์ (Web Browser) และสามารถควบคุมการหมุน การขยายเข้า-ออกของตัวกล้องได้กึ่งอัตโนมัติ

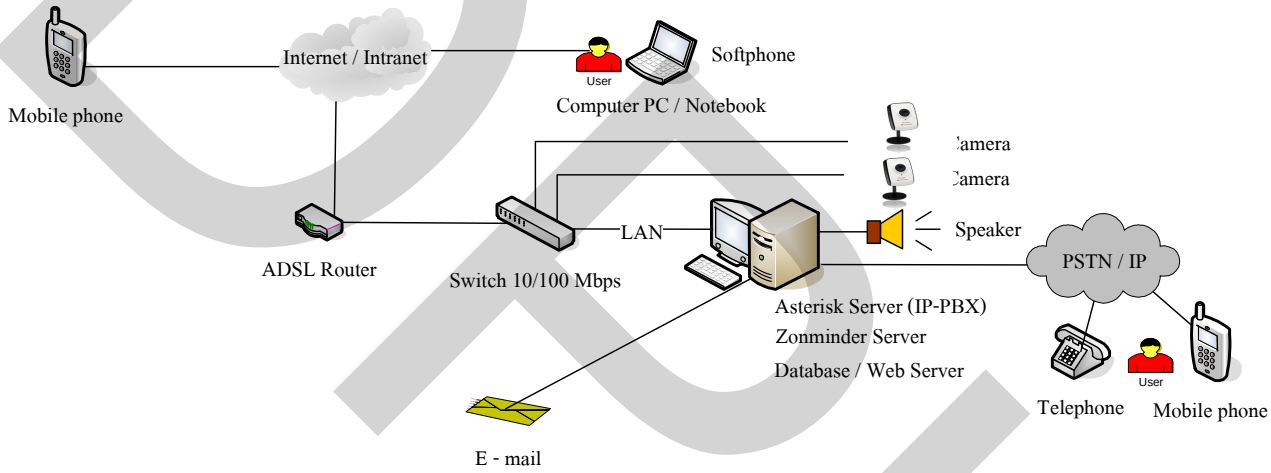
แนวคิดในการแก้ปัญหาเกี่ยวกับการรักษาความปลอดภัยหนึ่งก็คือการนำเอาเทคโนโลยี Open Source มาประยุกต์ใช้ในระบบรักษาความปลอดภัยจะช่วยลดต้นทุนในส่วนของซอฟต์แวร์ได้เป็นอย่างมาก จากแนวคิดนี้จึงได้นำเอาเทคโนโลยี Asterisk (IP-PBX) และ Zoneminder หรือเทคนิคการใช้กล้องวีดีโอเพื่อรักษาความปลอดภัย มาประยุกต์ใช้ในการรักษาความปลอดภัยเพื่อเป็นต้นแบบในการรักษาความปลอดภัยต่อไปในอนาคต



ภาพที่ 2.1 ตัวอย่างการใช้ Zoneminder เพื่อควบคุมกล้องวงจรปิดหลายกล้อง (Zoneminder, 2553)

ภาพที่ 2.2 ระบบตรวจจับการเคลื่อนไหว (Motion detect)

Zoneminder เป็นซอฟต์แวร์ที่สามารถบันทึกกล้องวงจรปิด โดยทำงานผ่านเว็บบราวเซอร์ (Browser) สามารถตรวจจับการเคลื่อนไหวดังแสดงในภาพที่ 2.2 ซึ่งมีหลาย algorithm ให้ใช้ตามสถานการณ์และความเหมาะสม Zoneminder สามารถ วิเคราะห์ บันทึก และดูภาพจากกล้องวงจรปิด กล้องวีดีโอทั่วไป กล้อง IP (IP Network Camera) เป็นต้น สามารถเชื่อมต่อกับกล้องได้หลายกล้อง สามารถถ่ายโอนข้อมูลที่เป็นภาพวีดีโอผ่านทางระบบเครือข่ายคอมพิวเตอร์ และสามารถควบคุมการหมุน การขยายเข้า-ออก ของตัวกล้องได้กึ่งอัตโนมัติ มีการเชื่อมต่อกับอุปกรณ์ต่างๆ ดังภาพที่ 2.3



ภาพที่ 2.3 การเชื่อมต่อ Zoneminder กับอุปกรณ์ต่างๆ

2.3 ทฤษฎีของระบบ Voice over Internet Protocol (VoIP)(กิตติพงษ์ สุวรรณราช, 2551)

Voice over Internet Protocol หรือที่เรียกสั้นๆ ว่า VoIP เป็นเทคโนโลยีการสื่อสารแบบใหม่ที่สามารถรับ – ส่ง สัญญาณเสียงผ่านทางเครือข่ายอินเทอร์เน็ตหรืออินทราเน็ตได้ โดยจะต้องอาศัยอุปกรณ์ (Hardware) หรือโปรแกรมคอมพิวเตอร์ (Software) ทำงานร่วมกัน เทคโนโลยี VoIP นี้ถูกคิดขึ้นโดยองค์กร Advanced Research Project Agency Network (ARPAnet) เมื่อปี ค.ศ.1973 เพื่อเป็นการคิดค้นเทคโนโลยีที่ช่วยในการผลิตต้นทุน และเป็นการเพิ่มมูลค่าการใช้งานเครือข่ายให้มีประโยชน์และมีประสิทธิภาพมากขึ้น ซึ่งการทำงานของ VoIP นั้นจะมีการแปลงสัญญาณเสียงจากต้นทางให้อยู่ในรูปแบบของแพกเก็จ (Packet) เล็กๆ แล้วส่งไปยังผู้รับปลายทางโดยอาศัยโปรโตคอลที่มีอยู่อย่างแพร่หลาย คือ Internet Protocol หรือที่รู้จักกันทั่วไปในนาม IP ซึ่งโดยปกติจะใช้ IP ในการส่งสัญญาณข้อมูลเท่านั้น แต่ด้วยเทคโนโลยี VoIP นี้ ทำให้สามารถพัฒนาการสื่อสารผ่านสัญญาณเสียงให้สามารถสื่อสารผ่าน IP ได้ ทำให้เป็นการประหยัดค่าใช้จ่ายในส่วนของ

เครือข่ายโทรศัพท์ได้มากขึ้นอีกด้วย ซึ่งการติดต่อสื่อสารทางโทรศัพท์แต่เดิมนั้นเป็นระบบ Analog ซึ่งเป็นความสิ้นเปลืองทั้งเวลาและการใช้อุปกรณ์ ตัวอย่างเช่นการใช้สายโทรศัพท์เส้นหนึ่งต่อเชื่อมโทรศัพท์ต้นทางและปลายทาง พอระบบต่อเชื่อมโทรศัพท์ได้แล้วก็หมายความว่า การจราจรบนเส้นสายโทรศัพท์เส้นนี้ถูกจองทั้งถนน เพื่อให้สัญญาณโทรศัพท์ทั้งสองเครื่องนี้ใช้สนทนากัน เมื่อสนทนากันเสร็จเรียบร้อยก็วางสาย สายโทรศัพท์เส้นนี้ก็จะว่าง ก็หมายถึงถนนว่างแล้วให้รถยนต์คันอื่นวิ่งบ้าง ตัวอย่างนี้เป็นแบบ Analog แต่ถ้าเป็นระบบ digital ใช้ถนนแบบเดียวกัน เพียงแต่ว่ามีหลายเลน มีหลายช่องจราจร มีหลายระดับความเร็วแบ่งกันใช้ เมื่อเอาโทรศัพท์ที่สามารถใช้ระบบ IP Telephony มาต่อเชื่อมก็เหมือนกับว่าโทรศัพท์สองเครื่องต่อผ่านสายโทรศัพท์เส้นหนึ่ง แต่การส่งสัญญาณกันไปมาจะถูกแพกย่อแล้วก็ทยอยส่ง ช่วงว่างก็จะเป็นโอกาสให้ผู้อื่นส่งบ้าง เรียกว่าไปด้วยกัน แบ่งเลนกัน แบ่งเวลากัน ดังนั้นช่วงเวลาเท่าๆ กันระบบ IP Telephony สามารถคุยกันได้

Voice over IP (VoIP) ถูกกล่าวถึงครั้งแรกในปี 1996 ในนิตยสาร CTI Magazine (ปัจจุบันเปลี่ยนชื่อเป็น Communication Solutions Magazine) CTI หรือ Computer Telephony Integration Magazine ได้มีการวิจารณ์เกี่ยวกับอุปกรณ์ที่ทำให้คอมพิวเตอร์และการโทรศัพท์สามารถทำงานร่วมกัน ซึ่งมีการใช้งานครั้งแรกในธุรกิจ Call Center โดยเป็นการทำงานร่วมกับเครื่องตอบรับโทรศัพท์อัตโนมัติ

2.3.1 ลักษณะโดยทั่วไปของ VoIP (VoIP,2553)

ลักษณะโดยทั่วไปของบริการ VoIP อาจจำแนกการใช้เป็น 2 ประเภทหลักๆ คือ

1) ประเภทที่มีความจำเป็นต้องอาศัยโครงข่ายอินเทอร์เน็ตสำหรับการติดต่อสื่อสาร โดยโครงข่ายดังกล่าวจะมีการเชื่อมต่อทั้งแบบ Public Network และ Private Network

2) ประเภทที่ผู้ให้บริการดำเนินการจัดการโครงข่าย IP ของตนเอง ซึ่งโดยประเภทนี้ผู้ให้บริการสามารถควบคุมระดับคุณภาพการให้บริการ (Quality of Service) ได้ตามที่ต้องการ

2.3.2 มาตรฐานเปิดสำหรับ VoIP (Open Standard for VoIP)

หลายองค์กรได้สนับสนุนมาตรฐานเปิดสำหรับ VoIP ขึ้น ทั้งสหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union, ITU) และ Internet Engineering Task Force (IETF) โดยได้จัดทำมาตรฐาน ดังนี้

1) H.323 โดย ITU

2) SIP (Session initiation protocol) โดย IETF

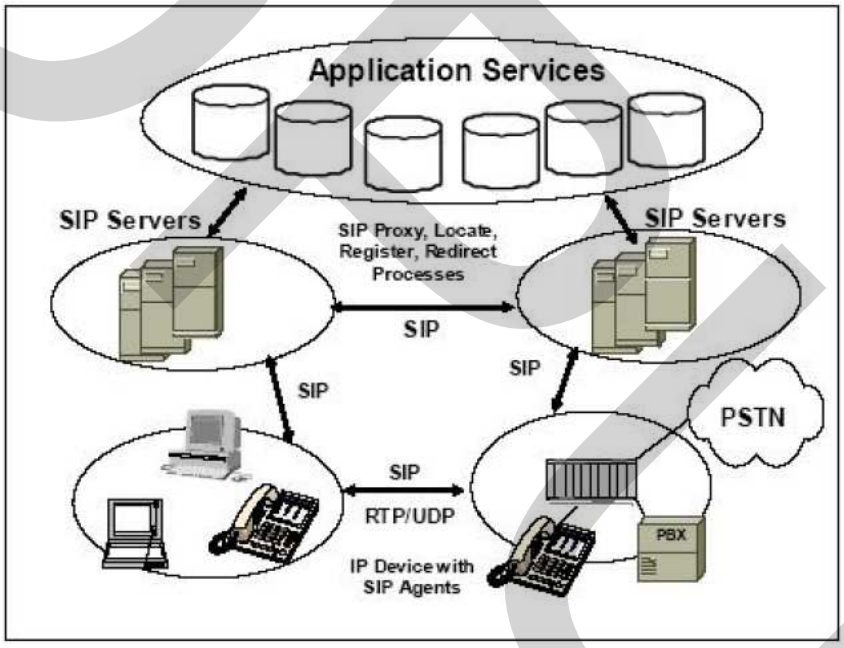
3) MGCP (Media gateway control protocol) โดย ITU

4) MEGACO โดย IETF/ITU

อย่างไรก็ตาม ยากที่จะชี้ชัดว่าโปรโตคอลใดเหนือกว่าโปรโตคอลใด เนื่องจากโปรโตคอลเหล่านี้ประกอบด้วยตัวแปรที่เหมือนๆ กัน

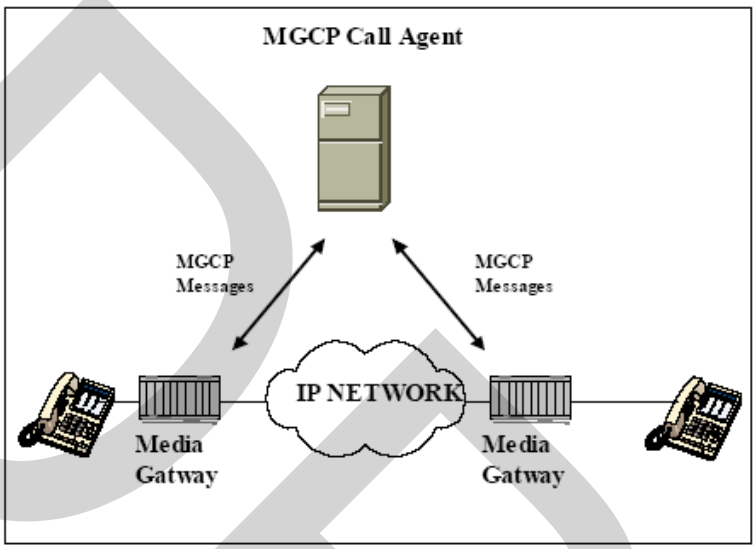
1) H.323 เป็นโปรโตคอลที่เก่าแก่สุด ซึ่งถูกพัฒนาโดย ITU โดยมีบริษัท Cisco Systemsเป็นผู้สนับสนุนหลักในการติดตั้งระบบ ซึ่งมีที่มาจากธุรกิจด้าน Local Area Network (LAN) และบริการ videoconference

2) SIP เป็นโปรโตคอลซึ่งถูกพัฒนาโดยองค์กรด้านอินเทอร์เน็ตและการสื่อสารข้อมูลที่รู้จักกันในนาม IETF โดยมีวัตถุประสงค์เพื่อส่งสัญญาณเสียงผ่านโครงข่ายสื่อสารข้อมูลแบบ Internet Protocol (IP-based data network) ซึ่งมีการใช้งานในกลุ่มผู้ให้บริการโทรศัพท์มีสถาปัตยกรรมของโครงข่าย และการให้บริการดังแสดงในภาพที่ 2.4



ภาพที่ 2.4 สถาปัตยกรรมของโครงข่าย และการให้บริการพื้นฐาน SIP โปรโตคอล (VoIP,2553)

3) MGCP เป็นโปรโตคอล Gateway สำหรับทั้ง H.323 และ SIP มีรูปแบบการสื่อสาร ดังภาพที่ 2.5



ภาพที่ 2.5 รูปแบบการสื่อสารของ MGCP โปรโตคอล (VoIP,2553)

4) MEGACO เป็นโปรโตคอล Gateway สำหรับทั้ง H.323 และ SIP แต่สามารถรองรับการทำงานร่วมกันของโครงข่าย IP ได้กว้างกว่า MGCP ทั้งยังสามารถรองรับการส่งสัญญาณของสื่อ (media types) ได้หลากหลายรูปแบบกว่าด้วย นอกจากโปรโตคอลที่กล่าวข้างต้นแล้ว ยังมีโปรโตคอลที่เป็นสิทธิเฉพาะของบริษัท (proprietary) อาทิโปรโตคอล “Skinny” ของบริษัท Cisco Systems เพื่อการใช้ระหว่าง Cisco call manager และ Cisco VoIP phone เป็นต้น
แต่ละโปรโตคอลมีคุณสมบัติต่างๆ ดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 การเปรียบเทียบแต่ละโปรโตคอล (VoIP,2553)

	H.323	SIP	MGCP	MEGACO
Architecture	Peer to Peer	Peer to Peer	Master/ Slave	Master/ Slave
Media Types	Voice, data, Limited Data	Voice, Video Data	Voice	Voice, Video
Scope of Network	Intranet and Internet	Intranet and Internet	Intranet Only	Intranet Only
Extensibility	Low	High	Medium	Medium
Scalability	Medium	High	Low	Low
Deploy Ease	Low	High	Medium	Medium
Standardization	ITU	IETF	IETF	IETF/ITU

ปัจจุบัน โปรโตคอล SIP เป็นโปรโตคอลที่มีการใช้งานอย่างแพร่หลาย โดยผู้ผลิตได้ผลิตอุปกรณ์ VoIP ออกสู่ตลาดแล้วทั้ง oriented phones, switches และ routers

2.3.3 ปัจจัยที่ทำให้เกิดการใช้ VoIP (VoIP,2553)

1) โอกาสที่จะติดต่อสื่อสารระหว่างประเทศ โดยผ่านเครือข่ายอินเทอร์เน็ต หรืออินทราเน็ต โดยมีราคาที่ถูกกว่าโครงข่ายโทรศัพท์ทั่วไป

2) การพัฒนารูปแบบการสื่อสารใหม่ๆ เพิ่มขึ้นในปัจจุบัน โดยที่ส่วนหนึ่งถูกพัฒนาขึ้นให้สามารถใช้งานใน VoIP ทำให้สามารถติดต่อสื่อสารได้กว้างไกลมากขึ้น

3) การเป็นที่ยอมรับ และรับเอาคอมพิวเตอร์เข้ามาใช้ในชีวิตประจำวัน ในช่วง 10 ปีที่ผ่านมาอย่างมากมาย รวมทั้งการเพิ่มจำนวนขึ้นของผู้ใช้งานอินเทอร์เน็ตในปัจจุบัน เป็นส่วนหนึ่งที่ทำให้ VoIP ได้รับความนิยมในการติดต่อสื่อสาร

4) มีการใช้ประโยชน์จากระบบ Network ที่มีการพัฒนาให้ดียิ่งๆ ขึ้นไปในปัจจุบัน ให้สามารถใช้งาน ได้ทั้งในการส่งข้อมูล และเสียงเข้าด้วยกัน

5) ความก้าวหน้าทางด้านการประมวลผลของคอมพิวเตอร์ ช่วยลดต้นทุนในการสร้างเครือข่ายของ VoIP ในขณะที่ ความสามารถ การให้บริการมีมากขึ้น ส่งผลให้ธุรกิจต่างๆ เข้ามาร่วมใน VoIP มากขึ้น

6) ความต้องการที่จะมีหมายเลขเดียวในการติดต่อสื่อสารทั่วโลก ทั้งด้านเสียง แฟกซ์ และข้อมูล ถึงแม้ว่าบุคคลนั้น จะย้ายไปที่ใด ก็ตามก็ยังคงสามารถใช้หมายเลขเดิมได้ เป็นความต้องการของผู้ใช้งานและธุรกิจ

7) การเพิ่มขึ้นอย่างมากมายของการทำรายการต่างๆ บน E-Commerce ในปัจจุบัน ผู้บริโภคต่างก็ต้องการการ บริการที่มีคุณภาพ และมีการโต้ตอบกันได้ระหว่างที่กำลังใช้อินเทอร์เน็ตอยู่ ซึ่ง VoIP สามารถเข้ามาช่วยในส่วนนี้ได้

8) การเติบโตอย่างรวดเร็วของ Wireless Communication ในปัจจุบัน ซึ่งผู้ใช้ในกลุ่มนี้ต้องการ การติดต่อสื่อสารที่ราคาถูกลง แต่มีความยืดหยุ่นในการใช้งาน ดังนั้นตลาดกลุ่มนี้ถือว่าเป็นโอกาสของ VoIP

2.3.4 ฟังก์ชันการทำงานของระบบ VoIP (Asteriskclub, 2553)

1) Addressing/Directories: ผู้ใช้ปลายทางจำเป็นจะต้องมองเห็นเบอร์โทรศัพท์ และ IP Address เครื่องคอมพิวเตอร์ที่ใช้เป็นเครื่องมือสื่อสารด้วยเสียงอาจต้องมีเบอร์โทรศัพท์ และโทรศัพท์ที่สามารถใช้ IP จะต้องมี IP Address และการให้บริการ Internet Directory จะต้องแสดงความสัมพันธ์ของ IP Address และเบอร์โทรศัพท์ด้วย

2) Authentication/Encryption VoIP รับประกันความปลอดภัยของระบบโทรศัพท์โดยการใช้บริการความปลอดภัยของ TCP/IP การโทรเรียกแบบส่วนตัวกระทำโดยการใช้ encryption

3) Configuration Management Interface ที่ใช้งานง่ายเป็นสิ่งจำเป็นในการจัดเรียงอุปกรณ์ มีพารามิเตอร์และตัวเลือกเข้ามาเกี่ยวข้องด้วยมากมาย ตัวอย่างเช่น telephony protocols การเลือกอัลกอริทึมที่ใช้บีบอัดสัญญาณ access control คุณสมบัติของการหันมาอาศัยชุมสายโทรศัพท์ การจัดเรียง port และ เครื่องจับเวลา Internet

4) การจัดการข้อผิดพลาด (Fault Management) ในการบริการและจัดการเครือข่ายต้องใช้อุปกรณ์ต่างๆ หลากชนิดและหลายยี่ห้อ ทำให้มีส่วนของการทำงานร่วมกับระบบจัดการเครือข่าย ซึ่งเรียกว่า เอเจนต์ (Agent) เอเจนต์เป็นส่วนของซอฟต์แวร์ที่อยู่ในอุปกรณ์ต่างๆ ที่เชื่อมอยู่ในเครือข่ายโดยมีคอมพิวเตอร์หลักเป็นตัวจัดการและบริหารเครือข่าย เพื่อความสะดวกในการจัดการโทรศัพท์ และจัดเก็บข้อมูลในรูปแบบต่างๆ เช่น การบันทึกข้อผิดพลาดของระบบ การบันทึกบทสนทนา

5) การคิดบัญชี/การคิดเงิน (Accounting/Billing) VoIP gateways มีหน้าที่นับจำนวนครั้งที่โทรสำเร็จและไม่สำเร็จ รายระเอียดเกี่ยวกับ call เช่น เวลาที่เริ่ม และยกเลิก call เบอร์ที่หมุน IP Address ของต้นสายกับปลายสาย Packet ที่ส่งและได้รับ เป็นต้น จะถูกบันทึกไว้ ข้อมูลเหล่านี้จะ

ถูกดำเนินการโดย accounting packages ภายนอกซึ่งถูกใช้สำหรับ PSTN call ผู้ใช้ปลายทางไม่จำเป็นต้องได้รับใบเสร็จรับเงินหลายใบ

2.3.5 ข้อดีของการนำเทคโนโลยี VoIP มาใช้งาน (กิตติพงษ์ สุวรรณราช, 2551)

1) ประหยัดงบประมาณในการลงทุน การนำเทคโนโลยี VoIP มาใช้งานนั้น สามารถนำมาประยุกต์ใช้กับระบบเครือข่ายการสื่อสารข้อมูลที่มีอยู่แล้ว เช่น อุปกรณ์ Router หรือ Switch ทำให้สามารถประหยัดค่าใช้จ่ายได้ เนื่องจากสามารถนำอุปกรณ์ที่มีอยู่เดิมมาใช้งานได้ และถ้าหากมีการนำเทคโนโลยี VoIP มาประยุกต์ใช้งานในลักษณะการสื่อสารระยะทางไกล เช่น ต่างจังหวัด หรือต่างประเทศ ก็จะทำให้สามารถประหยัดค่าบริการทางไกลของระบบโทรศัพท์แบบปกติได้อีกด้วย

2) เพิ่มมูลค่าของอุปกรณ์ การนำเทคโนโลยี VoIP มาใช้งานนั้น จะทำให้สามารถนำอุปกรณ์ที่มีการใช้งานอยู่แล้ว เช่น อุปกรณ์ Router Switch หรือแม้กระทั่งตู้ PBX นำมาประยุกต์ใช้ให้เกิดประโยชน์เพิ่มขึ้นจากที่เป็นอยู่เดิม ซึ่งถือเป็นการนำอุปกรณ์เดิมมาใช้ประโยชน์ให้สูงสุดด้วย

3) ลดค่าใช้จ่ายในการติดต่อสื่อสาร สำหรับองค์กรที่นำเทคโนโลยี VoIP ไปใช้งานเพื่อเป็นการติดต่อสื่อสารกันระหว่างสาขาที่อยู่ในระยะทางไกลกันนั้น จะทำให้องค์กรได้ประโยชน์ในแง่ของข้อมูลข่าวสารต่างๆ ระหว่างองค์กรมากยิ่งขึ้น เนื่องจากมีการสื่อสารแลกเปลี่ยนข่าวสารกันระหว่างสาขาขององค์กรมากยิ่งขึ้น โดยที่ไม่ต้องกังวลในเรื่องของค่าใช้จ่ายของการสื่อสารทางไกลอีกต่อไป ทำให้แต่ละสาขาได้รับข่าวสารข้อมูลล่าสุดขององค์กรอย่างทันท่วงที และไม่ต้องมีการรอซึ่งอาจนำมาซึ่งการล่าช้าในการปฏิบัติงานและการบริการ

4) ลดค่าใช้จ่ายในการใช้บริการโทรสาร (FAX) การนำ VoIP มาใช้งานนั้น ทำให้สามารถลดค่าใช้จ่ายในด้านต่างๆ ได้อย่างที่อาจจะไม่รู้ตัว ไม่ว่าจะเป็นค่าใช้จ่ายทางด้านค่าบริการโทรสาร โทรศัพท์ทางไกล ซึ่งถือเป็นปัจจัยสำคัญที่มีการนำเทคโนโลยี VoIP นี้มาใช้งาน หรือรวมทั้งการที่สามารถลดค่าใช้จ่ายทางด้านบุคลากรที่จะมาดูแลในเรื่องของการให้บริการทางโทรศัพท์ได้อีกด้วย เพราะสามารถใช้แค่คนคนเดียวเพื่อให้บริการลูกค้าผ่านระบบโทรศัพท์กลางขององค์กรและเชื่อมต่อไปยังสาขาต่างๆ ด้วยเทคโนโลยี VoIP

2.4 Asterisk (กิตติพงษ์ สุวรรณราช, 2551) (Asteriskclub, 2553)

Asterisk คือ ซอฟต์แวร์ระบบโทรศัพท์แบบ IP-PBX สมบูรณ์แบบ ซึ่งสามารถทำงานได้บนหลายๆ ระบบปฏิบัติการ เช่น Linux, Mac OS X, OpenBSD, FreeBSD และ Sun Solaris โดยได้มีการจัดเตรียมฟังก์ชันการใช้งานของตู้สาขาโทรศัพท์ PBX (Private Branch Exchange) คุณภาพสูงไว้ในตัว Asterisk รองรับกับระบบ VoIP หลายโปรโตคอล เช่น SIP H.323 IAX MGCP และ SCCP เป็นต้น ซึ่งรองรับกับอุปกรณ์โทรศัพท์ที่เป็นมาตรฐานและใช้ฮาร์ดแวร์ที่ราคา

ไม่แพง Asterisk มีการเผยแพร่แบบ Open Source ภายใต้ GUN General Public License (GPL) Asterisk ถูกพัฒนาและสร้างโดย Mr.Mark Spencer แห่งบริษัท Digium Inc. เมื่อปี ค.ศ. 1999 และได้มีการเผยแพร่โปรกรมไปยังทั่วโลกในกลุ่ม Open source เพื่อทดสอบและแก้ไขปัญหา (Bug) ของโปรแกรม Asterisk อย่างต่อเนื่อง

2.4.1 ความสามารถของ Asterisk (กิตติพงษ์ สุวรรณราช, 2551) (Asterisk, 2553)

Asterisk นั้นนับเป็นระบบโทรศัพท์ IP-PBX ตัวหนึ่งที่มีความสามารถเทียบเท่ากับระบบโทรศัพท์ราคาแพงที่มีประสิทธิภาพสูง ซึ่ง Asterisk เองได้มีความสามารถต่างๆ ดังต่อไปนี้

1) Switch (PBX) ตู้ชุมสาย Asterisk สามารถทำหน้าเป็นอุปกรณ์สลับสายโทรศัพท์ไม่ว่าจะเป็นระบบ IP หรือ hybridge สามรถทำการตั้งค่าเส้นทางการของการโทรศัพท์โดยตัวเอง, สามารถเพิ่มเติม feature ได้เช่น (ระบบ Voicemail: IVR) รองรับการเชื่อมต่อกับระบบโทรศัพท์พื้นฐานไม่ว่าจะเป็นแบบ analog หรือ digital (ISDN)

2) Gateway สามารถทำหน้าเป็นอุปกรณ์ที่ใช้ในการเชื่อมต่อระหว่าระบบโทรศัพท์พื้นฐานกับระบบ VoIP

3) Feature & Media Server อีก ความสามารถของ Asterisk คือสามารถทำเป็น ระบบตอบรับหรือระบบการประชุมทางโทรศัพท์ เพื่อให้ทำงานเข้ากับระบบโทรศัพท์ที่มีอยู่เดิม

4) Call Center รองรับการทำงานของระบบ Call-Center อย่างเต็มรูปแบบ เช่น ACD, Queue, IVR, Skill-based routing และอื่นๆ ความสามารถของ Asterisk ดังแสดงในตารางที่ 2.2

ตารางที่ 2.2 ความสามารถของ Asterisk (กิตติพงษ์ สุวรรณราช, 2551) (Asterisk, 2553)

ความสามารถด้าน	รองรับฟังก์ชันการทำงานต่างๆ ดังนี้
Call Features	Alarm Receiver Append Message Automated Attendant (ระบบตอบรับอัตโนมัติ) Blacklists (การทำ backlist ใช้ในการ filter ผู้ใช้งานโทรศัพท์ที่โทรเข้าได้) Blind Transfer (การโอนสายแบบโอนขาด หรือ โอนโดยไม่ถามผู้ที่เราจะโอนไปหาก่อน) Call Detail Records (การจัดเก็บข้อมูลการโทรศัพท์ในระบบโดยระเอียด) Call Forward on Busy (การโอนสายไปยังผู้อื่นในกรณีที่สายนั้นๆไม่ว่าง) Call Forward on No Answer (การโอนสายไปยังผู้อื่นในกรณีที่สายนั้นๆไม่รับสาย) Call Recording Database Store / Retrieve Database Integration Dial by Name Interactive Voice Response (IVR) Local and Remote Call Agents Music On Hold Music On Transfer: - Flexible Mp3-based System - Random or Linear Play - Volume Control Remote Office Support SMS Messaging Streaming Media Access VoIP Gateways

ตารางที่ 2.2 (ต่อ)

ความสามารถด้าน	รองรับฟังก์ชันการทำงานต่างๆ ดังนี้
Call Features	Voicemail: - Visual Indicator for Message Waiting - Stutter Dialtone for Message Waiting - Voicemail to email - Voicemail Groups - Web Voicemail Interface
Computer-Telephony Integration	AGI (Asterisk Gateway Interface) Graphical Call Manager Outbound Call Spooling TCP/IP Management Interface
Protocols	IAX™ (Inter-Asterisk Exchange) H.323 SIP (Session Initiation Protocol) MGCP (Media Gateway Control Protocol SCCP (Cisco® Skinny®)

สำหรับรายละเอียดเพิ่มเติมสามารถศึกษาได้จาก (กิตติพงษ์ สุวรรณราช, 2551)

2.4.2 เหตุผลที่เลือก Asterisk ในการประยุกต์ใช้กับระบบแจ้งเตือนระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP

1) ช่วยลดต้นทุน เพราะโปรแกรม Asterisk นั้นเราสามารถนำมาใช้งานได้ฟรี

2) สามารถเขียนโปรแกรมเพิ่มเติมเข้าไปในตัวโปรแกรม Asterisk โดยใช้ภาษาคอมพิวเตอร์ที่เราถนัดได้ เช่น ภาษา C Perl PHP เป็นต้น เพื่อให้ Asterisk ทำงานได้ตามคำสั่ง

3) Asterisk มีคุณสมบัติของระบบโทรศัพท์แบบอัจฉริยะอยู่ในตัว เช่น ระบบวอยว์เมล์ (Voice Mail) ระบบตอบรับอัตโนมัติ (Interactive Voice Response: IVR) เสียงเพลงรอสาย Music on Hold สายเรียกซ้อน (Call waiting) การโอนสาย (Call forwarding) และคุณสมบัติอื่นๆ อีกมากมาย

4) Asterisk เปิดโอกาสให้สามารถเขียนโปรแกรมในการสั่งงานการใช้โทรศัพท์ หรือที่เรียกว่า Dial Plan ซึ่งสามารถกำหนดเส้นทางและขั้นตอนของการใช้โทรศัพท์ได้ตามที่เราต้องการ

2.5 AGI - Asterisk Gateway Interface และ Asterisk Manager API (AGI-Asterisk Gateway Interface, 2553) (Asterisk AGI, 2553)

AGI (Asterisk Gateway Interface) เป็นช่องทางหรือชุดคำสั่ง ที่สามารถควบคุมช่องสัญญาณ (ZAP Channel) ผ่านทาง stdin และ stdout นั้นหมายความว่าสามารถใช้ภาษาอะไรก็ได้ไม่ว่าจะเป็น PERL PHP Pytho Ruby Java C/C++ NET language (C#,VB.NET,etc...) ไม่เว้นแม้แต่ shell ต่างๆ (bash, ash, korn, etc...) ติดต่อกับ AGI ได้อย่างง่ายดาย

1) AGI จะติดต่อกับ dialplan และจะถูกเรียกใช้จาก extensions.conf

2) EAGI จะติดต่อเกี่ยวกับ channel

3) DeadAGI จะใช้สำหรับติดต่อกับ channel หลังการวางหู

4) FastAGI ช่วยให้สามารถติดต่อ AGI ผ่าน TCP ได้ รายละเอียดสามารถศึกษาได้จาก (Asterisk+FastAGI, 2553) คำสั่ง AGI สามารถเข้าไปที่ Asterisk CLI แล้วพิมพ์คำสั่ง show agi [agi-command]

Asterisk Manager API (Asterisk Manager API, 2553) เป็นคำสั่ง API ทำงานติดต่อกับ Asterisk ผ่านทาง Socket เพื่อควบคุมการทำงานและอ่านสถานะของ PBX ผ่านโปรโตคอล TCP/IP stream ได้บนพอร์ท (port) หมายเลข 5038 (default) และแสดงวิธีการติดต่อผ่านทางเทลเนต (telnet) และซ็อกเก็ต (socket) ทำให้เราสามารถเพิ่มฟังก์ชันการทำงานตามต้องการได้ในการควบคุมการทำงานของ Asterisk เช่นระบบ Automated Attendant และการสั่งให้ระบบโทรออกเพื่อแจ้งเตือนไปยังผู้ใช้งานสามารถปรับแต่งพอร์ทที่ต้องการใช้ และ password ของ admin สำหรับใช้บริการ Asterisk Manager ได้ที่ไฟล์ /etc/asterisk/manager.conf ดังนี้ (Asterisk Manager API, 2553)

```
; Asterisk Call Management support
 [general]
enabled = yes
 port = 5038
bindaddr = 0.0.0.0
[admin]
secret = amp111
deny=0.0.0.0/0.0.0.0
```

```
permit=127.0.0.1/255.255.255.0
 read = system,call,log,verbose,command,agent,user
write = system,call,log,verbose,command,agent,user
#include manager_additional.conf
#include manager_custom.conf
```

secret = amp111 เป็นรหัส default ควรเปลี่ยนเป็นรหัสอื่นเพื่อเพิ่มความปลอดภัยเมื่อมีการใช้งานระหว่าง server-client อย่างไรก็ตาม เครื่องที่จะมาใช้งานได้นั้น ต้องเป็นเครื่องเดียวกันกับ Asterisk เนื่องจากมีการกำหนด permit=127.0.0.1/255.255.255.0 เอาไว้ โดยชุดคำสั่งนี้ส่วนใหญ่เป็นการเรียกขอข้อมูลของ channels หรือดัก events ต่างๆ ที่เกิดขึ้น เราสามารถดูคำสั่งเหล่านี้ได้โดยเข้าไปที่ Asterisk CLI และพิมพ์ show manager commands

ตัวอย่างการติดต่อกับ Asterisk Manager การติดต่อกับ TCP/IP Stream โดยใช้ เทลเนต

```
[root@asterisk1 asterisk]# telnet 127.0.0.1 5038
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
Escape character is '^]'.
Asterisk Call Manager/1.0
Action: login
Username: admin
Secret: amp111
```

การตอบสนองจากระบบ

```
Response: Success
Message: Authentication accepted
```

ลักษณะการทำงานจะเป็นดังนี้ เมื่อส่งคำสั่งเข้าไประบบก็จะตอบสนองกลับมา ระบบจะรู้ว่าคำสั่งของสิ้นสุดลงเมื่อมีบรรทัดว่างๆ เข้ามา เวลาออกก็ใช้คำสั่ง Action: Logoff ตัวอย่างการติดต่อกับ Asterisk Manager ผ่าน PHP ซึ่งเป็นการเปิด socket ธรรมดา ดังนี้

```
function info_queus($ip,$port,$login,$pass,$operation)
  {
  $oSocket = @fsockopen($ip,$port,$errnum, $errdesc);
     if($oSocket)
     {
          fputs($oSocket, "Action: login\r\n");
          fputs($oSocket, "Username: $login\r\n");
          fputs($oSocket, "Secret: $pass\r\n\r\n");
          fputs($oSocket, "Action: Queues\r\n");
          fputs($oSocket, "Queue: $operation\r\n\r\n");
          fputs($oSocket, "Action: Logoff\r\n\r\n");
          $infos=array();
            while (!feof($oSocket))
            {
              $inf_temp=explode("\r\n",fread($oSocket, 8192));
                    foreach($inf_temp as $tmp)
                          if($tmp!="")
                                array_push($infos,str_word_count($tmp,1,"0123456789/@"));
                       unset($tmp,$inf_tmp);
              }
          fclose($oSocket);
          return $infos;
     }return false;
  }
```

2.6 ภาษาพีเอชพี (PHP) (ภาษาพีเอชพี, 2553)

PHP (PHP Hypertext Preprocessor) คือ ภาษาคอมพิวเตอร์ในลักษณะเซิร์ฟเวอร์-ไซด์ สคริปต์ โดยลิขสิทธิ์อยู่ในลักษณะโอเพนซอร์ส ภาษาพีเอชพีใช้สำหรับจัดทำเว็บไซต์ และแสดงผลออกมาในรูปแบบเอชทีเอ็มแอล (HTML) โดยมีรากฐานโครงสร้างคำสั่งมาจากภาษา ภาษาซี ภาษาจาวา และ ภาษาเพิร์ล ซึ่ง ภาษาพีเอชพี นั้นง่ายต่อการเรียนรู้ ซึ่งเป้าหมายหลักของภาษานี้ คือให้นักพัฒนาเว็บไซต์สามารถเขียน เว็บเพจ ที่มีความตอบโต้ได้อย่างรวดเร็ว

2.6.1 คุณสมบัติของภาษาพีเอชพี

การแสดงผลของพีเอชพี จะปรากฏในลักษณะเอชทีเอ็มแอล ซึ่งจะไม่แสดงคำสั่งที่ผู้ใช้เขียน ซึ่งเป็นลักษณะเด่นที่พีเอชพีแตกต่างจากภาษาในลักษณะไคลเอนต์-ไซด์ สคริปต์ เช่น ภาษาจาวาสคริปต์ ที่ผู้ชมเว็บไซต์สามารถอ่าน ดูและคัดลอกคำสั่งไปใช้เองได้ นอกจากนี้พีเอชพียังเป็นภาษาที่เรียนรู้และเริ่มต้นได้ไม่ยาก โดยมีเครื่องมือช่วยเหลือและคู่มือที่สามารถหาอ่านได้ฟรีบนอินเตอร์เน็ต ความสามารถการประมวลผลหลักของพีเอชพี ได้แก่ การสร้างเนื้อหาอัตโนมัติจัดการคำสั่ง การอ่านข้อมูลจากผู้ใช้และประมวลผล การอ่านข้อมูลจากดาต้าเบส ความสามารถจัดการกับคุกกี้ ซึ่งทำงานเช่นเดียวกับโปรแกรมในลักษณะซีจีไอ (CGI) คุณสมบัติอื่นเช่น การประมวลผลตามบรรทัดคำสั่ง (command line scripting) ทำให้ผู้เขียนโปรแกรมสร้างสคริปต์พีเอชพี ทำงานผ่านพีเอชพีพาร์เซอร์ (PHP parser) โดยไม่ต้องผ่านเซิร์ฟเวอร์หรือ เบราว์เซอร์ซึ่งมีลักษณะเหมือนกับ Cron (ในยูนิกซ์หรือลีนุกซ์) หรือ Task Scheduler (ในวินโดวส์) สคริปต์เหล่านี้สามารถนำไปใช้ในแบบ Simple text processing tasks ได้

การแสดงผลของพีเอชพี ถึงแม้ว่าจุดประสงค์หลักใช้ในการแสดงผลเอชทีเอ็มแอล แต่ยังสามารถสร้างเอ็กเอชทีเอ็มแอล (XHTML) หรือเอ็กเอ็มแอล (XML) ได้ นอกจากนี้สามารถทำงานร่วมกับคำสั่งเสริมต่างๆ พีเอชพีมีความสามารถอย่างมากในการทำงานเป็นประมวลผลข้อความ จาก POSIX Extended หรือ รูปแบบเพิร์ลทั่วไป เพื่อแปลงเป็นเอกสารเอ็กเอ็มแอล

เมื่อใช้พีเอชพีในการทำอีคอมเมิร์ซสามารถทำงานร่วมกับโปรแกรมอื่น เช่น Cybercash Payment, CyberMUT, VeriSign Payflow Pro และ CCVS functions เพื่อใช้ในการสร้างโปรแกรมทำธุรกรรมทางการเงิน

2.6.2 การรองรับของภาษาพีเอชพี

คำสั่งของพีเอชพี สามารถสร้างผ่านทางโปรแกรมแก้ไขข้อความทั่วไป เช่น โน้ตแพด หรือ vi ซึ่งทำให้การทำงานพีเอชพี สามารถทำงานได้ในระบบปฏิบัติการหลักเกือบทั้งหมด โดยเมื่อเขียนคำสั่งแล้วนำมาประมวลผล Apache Microsoft Internet Information Services (IIS), Personal Web Server Netscape และ iPlanet servers Oreilly Website Pro server Caudium Xitami

OmniHTTPd และอื่นๆ อีกมากมาย. สำหรับส่วนหลักของภาษาพีเอชพี ยังมี Module ในการรองรับซีจีไอมาตรฐาน ซึ่งภาษาพีเอชพีสามารถทำงานเป็นตัวประมวลผลซีจีไอด้วย และด้วย ภาษาพีเอชพีมีอิสรภาพในการเลือกระบบปฏิบัติการ และเว็บเซิร์ฟเวอร์ นอกจากนี้ยังสามารถใช้สร้างโปรแกรมโครงสร้าง สร้างโปรแกรมเชิงวัตถุ (OOP) หรือสร้างโปรแกรมที่รวมทั้งสองอย่างเข้าด้วยกัน

ภาษาพีเอชพีสามารถทำงานร่วมกับฐานข้อมูลได้หลายชนิด ซึ่งฐานข้อมูลส่วนหนึ่งที่รองรับได้แก่ ออราเคิล dBase PostgreSQL IBM DB2 MySQL Informix ODBC โครงสร้างของฐานข้อมูลแบบ DBX ซึ่งทำให้พีเอชพีใช้กับฐานข้อมูลอะไรก็ได้ที่รองรับรูปแบบนี้ และภาษาพีเอชพียังรองรับ ODBC (Open Database Connection) ซึ่งเป็นมาตรฐานการเชื่อมต่อฐานข้อมูลที่ใช้กันแพร่หลายอีกด้วย คุณสามารถเชื่อมต่อกับฐานข้อมูลต่างๆ ที่รองรับมาตรฐานโลกนี้ได้

ภาษาพีเอชพียังสามารถรองรับการสื่อสารกับการบริการในโปรโตคอลต่างๆ เช่น LDAP, IMAP, SNMP, NNTP, POP3, HTTP, COM (บนวินโดวส์) และอื่นๆ อีกมากมาย สามารถเปิด Socket บนเครือข่ายโดยตรง และตอบโต้โดยใช้ โปรโตคอลใดๆก็ได้ ภาษาพีเอชพีมีการรองรับสำหรับการแลกเปลี่ยนข้อมูลแบบ WDDX Complex กับ Web Programming อื่นๆ ทั่วไปได้ ในส่วน Interconnection ภาษาพีเอชพีมีการรองรับสำหรับ Java objects ให้เปลี่ยนเป็น PHP Object แล้วใช้งาน และสามารถใช้รูปแบบ CORBA เพื่อเข้าสู่ Remote Object ได้เช่นกัน

2.7 MySQL (MySQL, 2553)

MySQL เป็นฐานข้อมูลแบบ open source ที่ได้รับความนิยมในการใช้งานสูงสุด โปรแกรมหนึ่งบนเครื่องให้บริการ มีความสามารถในการจัดการกับฐานข้อมูลด้วยภาษา SQL (Structures Query Language) อย่างมีประสิทธิภาพ มีความรวดเร็วในการทำงาน รองรับการทำงานจากผู้ใช้หลายๆ คนและหลายๆ งานได้ในขณะเดียวกัน

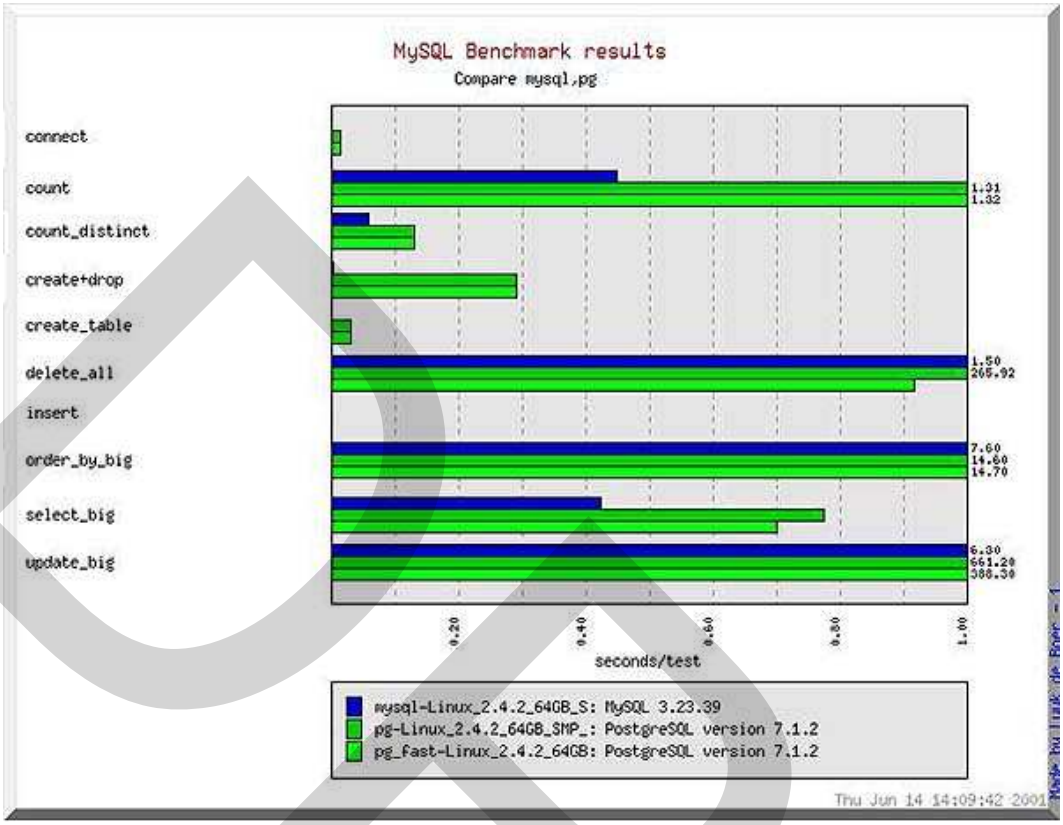
MySQL ถือเป็นระบบจัดการฐานข้อมูล (DataBase Management System (DBMS)) ฐานข้อมูลมีลักษณะเป็นโครงสร้างของการเก็บรวบรวมข้อมูล การที่จะเพิ่มเติม เข้าถึงหรือประมวลผลข้อมูลที่เก็บในฐานข้อมูลจำเป็นจะต้องอาศัยระบบจัดการฐานข้อมูล ซึ่งจะทำหน้าที่เป็นตัวกลางในการจัดการกับข้อมูลในฐานข้อมูลทั้งสำหรับการใช้งานเฉพาะ และรองรับการทำงานของแอพลิเคชันอื่นๆ ที่ต้องการใช้งานข้อมูลในฐานข้อมูล เพื่อให้ได้รับความสะดวกในการจัดการกับข้อมูลจำนวนมาก MySQL ทำหน้าที่เป็นทั้งตัวฐานข้อมูลและระบบจัดการฐานข้อมูล

MySQL เป็นระบบจัดการฐานข้อมูลแบบ relational ซึ่งจะทำการเก็บข้อมูลทั้งหมดในรูปแบบของตารางแทนการเก็บข้อมูลทั้งหมดลงในไฟล์เพียงไฟล์เดียว ทำให้ทำงานได้รวดเร็วและมี

ความยืดหยุ่น นอกจากนั้น แต่ละตารางที่เก็บข้อมูลสามารถเชื่อมโยงเข้าหากันทำให้สามารถรวมหรือจัดกลุ่มข้อมูลได้ตามต้องการ โดยอาศัยภาษา SQL ที่เป็นส่วนหนึ่งของโปรแกรม

MySQL แจกจ่ายให้ใช้งานแบบ open source นั่นคือ ผู้ใช้งาน MySQL ทุกคนสามารถใช้งานและปรับแต่งการทำงานได้ตามต้องการ สามารถดาวน์โหลดโปรแกรม MySQL ได้จากอินเทอร์เน็ตและนำมาใช้งานโดยไม่มีค่าใช้จ่ายใดๆ

ในระบบปฏิบัติการ Linux นั้น มีโปรแกรมที่สามารถใช้งานเป็นฐานข้อมูลให้ผู้ดูแลระบบสามารถเลือกใช้งานได้หลายโปรแกรม เช่น MySQL และ PostgreSQL ผู้ดูแลระบบสามารถเลือกติดตั้งได้ทั้งในขณะที่ติดตั้งระบบปฏิบัติการ Linux หรือจะติดตั้งภายหลังจากที่ติดตั้งระบบปฏิบัติการก็ได้ อย่างไรก็ตาม สาเหตุที่ผู้ใช้งานจำนวนมากนิยมใช้งานโปรแกรม MySQL คือ MySQL สามารถทำงานได้อย่างรวดเร็ว น่าเชื่อถือและใช้งานได้ง่าย เมื่อเปรียบเทียบประสิทธิภาพในการทำงานระหว่างโปรแกรม MySQL และ PostgreSQL โดยพิจารณาจากการประมวลผลแต่ละคำสั่งได้ผลลัพธ์ดังภาพที่ 2.6 นอกจากนั้น MySQL ถูกออกแบบและพัฒนาขึ้นมาเพื่อทำหน้าที่เป็นเครื่องให้บริการรองรับการจัดการกับฐานข้อมูลขนาดใหญ่ ซึ่งการพัฒนายังคงดำเนินอยู่อย่างต่อเนื่อง ส่งผลให้มีฟังก์ชันการทำงานใหม่ๆ ที่อำนวยความสะดวกแก่ผู้ใช้งานเพิ่มขึ้นอยู่ตลอดเวลา รวมไปถึงการปรับปรุงด้านความต่อเนื่อง ความเร็วในการทำงาน และความปลอดภัย ทำให้ MySQL เหมาะสมต่อการนำไปใช้งานเพื่อเข้าถึงฐานข้อมูลบนเครือข่ายอินเทอร์เน็ต



ภาพที่ 2.6 ผลการเปรียบเทียบการทำงานระหว่างโปรแกรม MySQL และ PostgreSQL (Mysql, 2553)

2.7.1 ภาษาสอบถามข้อมูล SQL (Structured Query Language) (SQL, 2553)

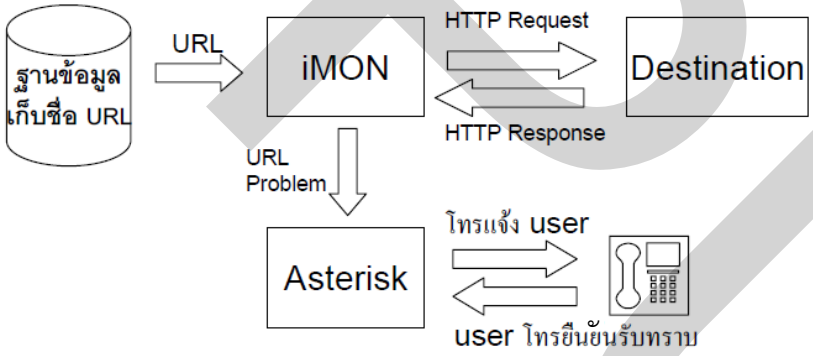
SQL คือ ภาษาสอบถามข้อมูล หรือภาษาจัดการข้อมูลอย่างมีโครงสร้าง มีการพัฒนาภาษาคอมพิวเตอร์ และโปรแกรมฐานข้อมูลที่รองรับมากมาย เพราะจัดการข้อมูลได้ง่าย เช่น MySQL, MsSQL, PostgreSQL หรือ MS Access เป็นต้น สำหรับโปรแกรมฐานข้อมูลที่ได้รับความนิยมคือ MySQL เป็น Open Source ที่ใช้งานได้ทั้งใน Linux และ Windows โดยที่ SQL เป็นภาษาที่ใช้ในการเขียนโปรแกรม เพื่อจัดการกับฐานข้อมูลโดยเฉพาะ เราสามารถแบ่งการทำงานได้เป็น 4 ประเภท ดังนี้

1) Select query ใช้สำหรับดึงข้อมูลที่ต้องการ
2) Update query ใช้สำหรับแก้ไขข้อมูล
3) Insert query ใช้สำหรับการเพิ่มข้อมูล
4) Delete query ใช้สำหรับลบข้อมูลออกไป

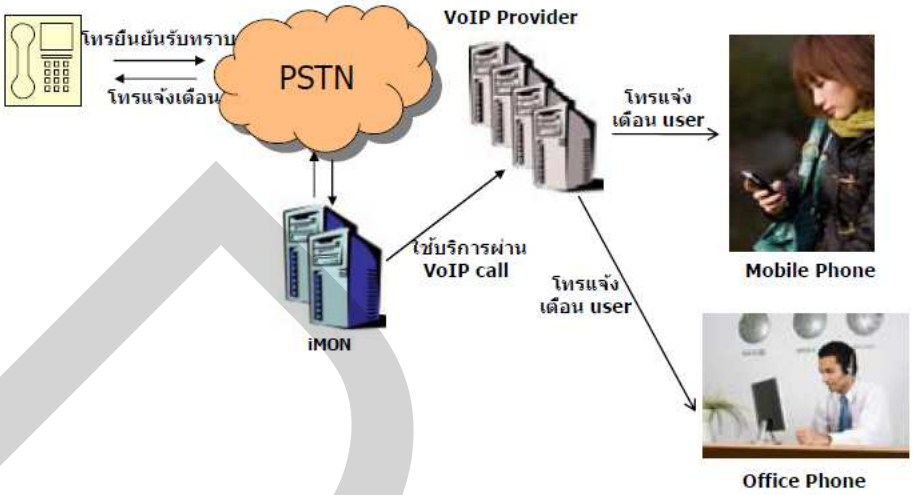
2.8 งานวิจัยหรือผลิตภัณฑ์ที่เกี่ยวข้อง

2.8.1 ระบบตรวจสอบและรายงานสภาพเว็บไซต์ผ่าน IVR (อนุวัตร์ , บุญชัย , 2552)

ระบบตรวจสอบและรายงานสถานะเว็บไซต์ผ่านระบบ IVR หรือเรียกว่า iMoN (IVR Monitoring system) มีการทำงานแสดงได้ดังภาพที่ 2.7 คือระบบจะคอยตรวจสอบสถานะการคงอยู่ของหน้าเว็บไซต์หรือ Service HTTP ด้วยการส่ง HTTP Request ไปที่หน้าเว็บไซต์หรือ URL ที่สมาชิกต้องการให้ระบบคอยตรวจสอบ แล้วบันทึกข้อความที่ตอบกลับจากเว็บไซต์ลงฐานข้อมูล ถ้าระบบตรวจสอบแล้วพบว่า Service HTTP นั้นไม่สามารถใช้งานได้ ระบบจะโทรแจ้งไปยังสมาชิกเจ้าของ Service HTTP นั้นทันที การแจ้งเตือนของระบบจะทำการโทรศัพท์ไปยังสมาชิกเพื่อแจ้งเตือนความผิดพลาดเรื่อยๆ จนกว่าสมาชิกจะทำการยืนยันการรับรู้หรือครบจำนวนครั้งที่สมาชิกได้กำหนดไว้ขึ้นอยู่กับการตั้งค่าการใช้งานระบบของสมาชิกแต่ละคนเมื่อทำการสมัครใช้งาน การยืนยันการรับรู้สมาชิกสามารถทำการยืนยันการรับรู้ได้ทั้งทางโทรศัพท์และทางหน้าเว็บไซต์ของระบบ



ภาพที่ 2.7 การทำงานของระบบตรวจสอบและรายงานสถานะเว็บไซต์ผ่านระบบ IVR (อนุวัตร์, บุญชัย, 2552)



ภาพที่ 2.8 โครงสร้างระบบการตรวจสอบสถานะเว็บไซต์ (อนุวัตร์ สมบุญ, บุญชัย งามวงศ์วัฒนา, 2552)

ระบบตรวจสอบและรายงานสถานะเว็บไซต์ผ่านระบบ IVR เป็นการทำงานร่วมกันระหว่างสคริปตรวจสอบสถานะเว็บไซต์ โปรแกรมสังเคราะห์เสียงภาษาไทยวาจา และโปรแกรม Asterisk ซึ่งทำหน้าที่เป็น IP PBX และทำงานฟังก์ชันโทรศัพท์ทำให้ระบบสามารถทำการตรวจสอบและรายงานสถานะเว็บไซต์ผ่านโทรศัพท์ โดยการส่งข้อความเสียงแจ้งให้ผู้ใช้บริการทราบ เพื่อผู้ใช้บริการสามารถทำการตรวจสอบและแก้ไขปัญหาได้ทันที ระบบตรวจสอบและรายงานสถานะเว็บไซต์ผ่านระบบ IVR เป็นต้นแบบระดับห้องปฏิบัติการที่ได้รับการทดสอบแล้วว่าสามารถทำการตรวจสอบและแจ้งรายงานสถานะแก่ผู้ใช้บริการได้จริงดังแสดงในภาพที่ 2.8 และช่วยลดค่าใช้จ่ายสำหรับการใช้ระบบส่งข้อความสำหรับการแจ้งเตือน ทำให้เว็บไซต์สามารถกลับมาใช้งานอย่างรวดเร็วเมื่อมีความผิดปกติ ทำให้เว็บไซต์มีความน่าเชื่อถือมากขึ้น

2.8.2 บริการพี่ไฟล์แจ้งเหตุ หรือ File Alert Service ของ CBB Broadband (บริการพี่ไฟล์แจ้งเหตุ, 2553)

บริการพี่ไฟล์แจ้งเหตุโดยระบบ File Alert จะทำการแจ้งเตือนผ่าน SMS ทันทีเมื่อมีความเคลื่อนไหวในบริเวณจุดเฝ้าระวัง พร้อมทั้งถ่ายรูปผู้บุกรุกส่งถึงผู้ใช้ทันที

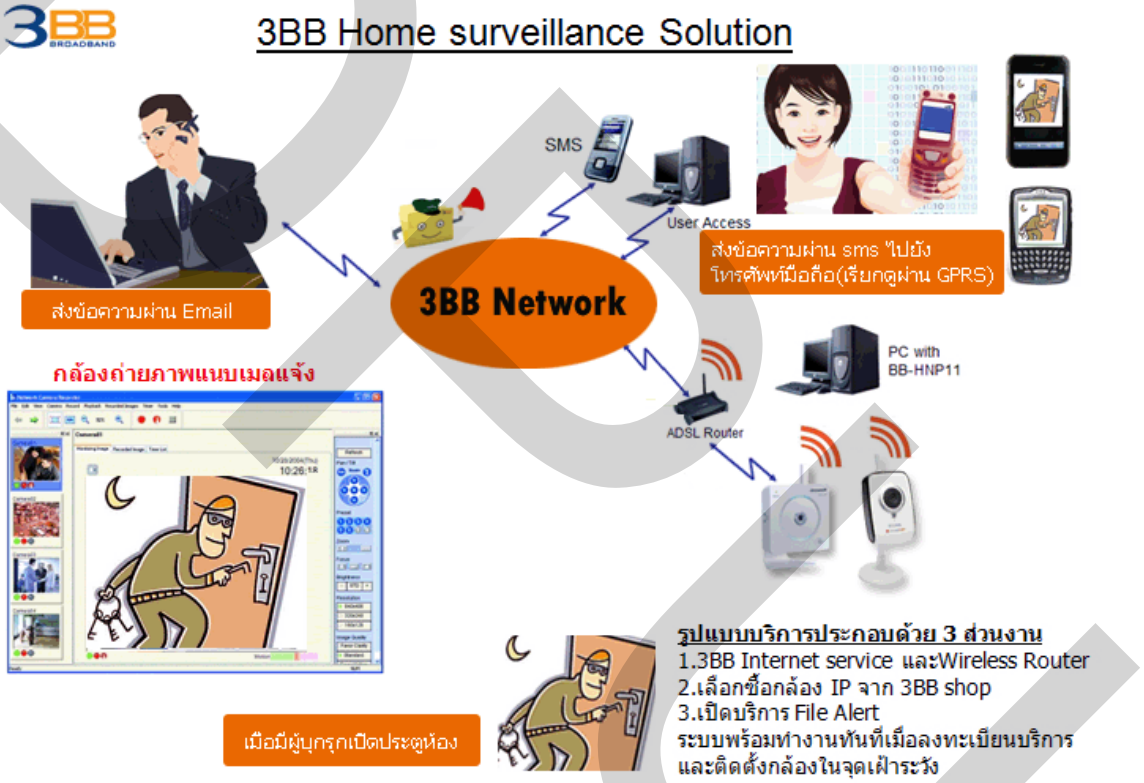
1) กรณีที่ “ไม่มี” เหตุผิดปกติ ลูกค้าเรียกดูความเรียบร้อยต่างๆ ภายในบ้านที่พักอาศัยได้ตลอดเวลา โดยเรียกดูผ่านระบบอินเทอร์เน็ต จากคอมพิวเตอร์ หรือ ผ่านโทรศัพท์มือถือ

2) กรณีมีการเคลื่อนไหวของผู้บุกรุก เข้ามาในบริเวณกล้องที่เฝ้าระวังเหตุร้าย กล้องจะทำการบันทึกภาพ พร้อมแจ้งเหตุทันทีแบบ Real Time ในรูปแบบข้อความ ผ่าน SMS และ

ส่งภาพเหตุการณ์ ผ่าน Email โดยเรียกดูจากคอมพิวเตอร์ หรือ โทรศัพท์มือถือ โครงสร้างดังแสดงในภาพที่ 2.9 และมีจุดเด่นของระบบ คือ

2.1) เรียกดูความเรียบร้อยภายในบ้านได้ตลอดเวลา ผ่าน Internet และโทรศัพท์มือถือ

2.2) แจ้งเตือนเหตุผิดปกติ กรณีมีผู้บุกรุกผ่านหน้ากล้อง โดยแจ้งผ่านทาง SMS และ E-mail (โดยมีระยะหวังผลจากจุดติดตั้งกล้องไม่เกิน 3 เมตร)



ภาพที่ 2.9 โครงสร้างของบริการพี่ไฟล์แจ้งเหตุ (บริการพี่ไฟล์แจ้งเหตุ , 2553)

2.8.3 สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือได้ 6 เบอร์ แบ่งโซนได้ 8 โซน (สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือ, 2553)

รายละเอียดและจุดเด่น สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือได้ 6 เบอร์ แบ่งโซนได้ 8 โซน ได้แก่

1) สามารถแจ้งเตือนด้วยเสียง

2) สามารถแจ้งเตือนผ่านโทรศัพท์ได้ถึง 6 เลขหมาย

3) มีระบบตรวจจับอินฟาเรด ตรวจจับการเคลื่อนไหว ระบบอินฟาเรด เมื่อมีผู้บุกรุกเดินผ่านบริเวณ รัศมีการตรวจจับ เครื่องจะส่งเสียงร้องเตือน และแจ้งเหตุผู้บุกรุกไปยังกล่องควบคุมทันที และแจ้งเหตุให้เจ้าบ้านทราบ

4) แยกโซนได้ 8 โซน

5) ตัวตรวจจับแถบแม่เหล็ก ใช้ติดที่ประตูบ้าน หรือขอบหน้าต่าง เมื่อผู้บุกรุกเปิดประตูหรือหน้าต่าง เครื่องจะส่งสัญญาณการบุกรุก ไปยังกล่องควบคุมเพื่อทำการเตือนภัย

มีโครงสร้างของระบบดังแสดงในภาพที่ 2.10

ภาพที่ 2.10 โครงสร้างของ สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือได้ 6 เบอร์ แบ่งโซนได้ 8 โซน (สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือ, 2553)

จากการศึกษาการใช้งานบริการต่างๆ และงานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์ที่นำเสนอ สามารถเปรียบเทียบคุณสมบัติได้ดังตารางที่ 2.3

ตารางที่ 2.3 การเปรียบเทียบคุณลักษณะของงานวิจัยและบริการที่เกี่ยวข้องกับวิทยานิพนธ์นี้

ลำดับ	ความสามารถของระบบ	IMoN	FAS	สัญญาณกันขโมย	SAIWS
1	โทรแจ้งเตือนผู้ใช้งาน	√		√	√
2	ส่งข้อความเสียงถึงผู้ใช้งาน	√			
3	ส่ง SMS ถึงผู้ใช้งาน		√		
4	ส่งอีเมล์ถึงผู้ใช้งาน		√		√
5	ส่งเสียงเตือน ณ จุดเกิดเหตุ	√	√	√	√
6	ระบบตรวจจับการเคลื่อนไหว		√	√	√
7	ตรวจดูภาพจากระบบผ่านระบบเครือข่าย	√	√		√
8	ตรวจดูภาพจากระบบผ่านโทรศัพท์มือถือ	√	√		√
9	เรียกดูข้อมูลย้อนหลัง	√	√		√
10	ผู้ใช้งานทำการยืนยันการรับรู้	√			
11	แยกโซน			√	√
12	ตัวตรวจจับแถบแม่เหล็ก			√	

หมายเหตุ: 1) IMoN = IVR Monitering System.

2) FAS = File Alert Service.

3) สัญญาณกันขโมย = สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือได้ 6 เบอร์ แบ่งโซนได้ 8 โซน

4) SAIWS = Sound – Alerting and Intrusion – Warning System Using VoIP Technology (งานวิจัยที่นำเสนอในวิทยานิพนธ์ฉบับนี้)

บทที่ 3
ระเบียบวิธีวิจัย

3.1 แนวทางการวิจัยและพัฒนา

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษา ออกแบบ และพัฒนาระบบส่งเสียงเตือนและแจ้งการบุกรุกด้วยเทคโนโลยี Voice over IP (VoIP) โดยการประยุกต์ใช้ซอฟต์แวร์ Asterisk (IP-PBX) และ Zoneminder (Digital Video Recorder) เพื่อให้ผู้ใช้งานระบบได้รับการแจ้งการบุกรุก และมีการส่งเสียงเตือน ณ ที่เกิดเหตุโดยอัตโนมัติ ให้ความสำคัญกับระบบรักษาความปลอดภัยทั้งในตัวอาคาร และภายนอกอาคาร โดยมีแนวทางในการวิจัยและพัฒนาดังนี้

1) ศึกษาและรวบรวมข้อมูล

1.1) ศึกษาการใช้งานของโปรแกรม Asterisk

1.2) ศึกษาการใช้งานของโปรแกรม Zoneminder

1.3) ศึกษาเพิ่มเติมการใช้งานภาษา PHP ฐานข้อมูล MySQL และการติดตั้ง Apache บนระบบปฏิบัติการ Linux

1.4) ศึกษาระบบการส่งข้อมูลที่เป็น Streaming ภาพวีดีโอและเสียงให้ได้คุณภาพที่เหมาะสม

1.5) ศึกษาการสร้างระบบฐานข้อมูลเพื่อเก็บข้อมูลที่จำเป็นไว้เป็นหลักฐานในการยืนยัน

2) การออกแบบระบบงาน

ออกแบบระบบส่งเสียงเตือนและแจ้งการบุกรุกด้วยเทคโนโลยี VoIP จุดเชื่อมต่อของอุปกรณ์ต่างๆ โดยศึกษาเครื่องมือและอุปกรณ์ที่ใช้พัฒนาอย่างละเอียด

3) พัฒนาระบบงาน

ทำการพัฒนาระบบให้สามารถทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้ มีการทดสอบย่อยเพื่อหาข้อผิดพลาดต่างๆ ภายในระบบ แล้วทำการแก้ไข

4) ทดสอบการใช้งาน

มีการทดสอบเพื่อดูประสิทธิภาพของทั้งระบบ คุณภาพของภาพและเสียง อัตราความผิดพลาดในการส่งข้อมูลด้วยการจำลองสถานการณ์ว่ามีผู้ไม่ประสงค์ดีเข้าไปในบ้านโดยไม่ได้รับอนุญาต

5) สรุปผลการพัฒนา

นำข้อมูลที่ได้ในการจำลองสถานการณ์มาสรุปผล เพื่อใช้ในการวิเคราะห์การทำงานและประเมินประสิทธิภาพของระบบ

3.2 เครื่องมือที่ใช้ในงานวิจัย

3.2.1 ฮาร์ดแวร์

1) คอมพิวเตอร์ ใช้เป็นเครื่อง Server ทั้ง Zoneminde Server และ Asterisk Server

CPU : Celeron 1.7 GHz

RAM : 512 MB

Hard disk : 40 GB

2) IP Camera (Dlink DCS-910, 2553, 1 ตุลาคม) กล้องแบบไอพีที่ใช้ในการทดสอบระบบ

ยี่ห้อ : DLINK

รุ่น : DCS-910 10/100 Fast Ethernet Network Camera

3) ADSL Modem + Router + Wireless ใช้ในการเชื่อมต่ออุปกรณ์ในระบบเครือข่าย

4) เครื่องโทรศัพท์ ในที่นี้หมายถึงโทรศัพท์มือถือ ซึ่งเป็นส่วนหนึ่งในการทดสอบระบบเพื่อดูภาพ และการบุกรุกผ่านโทรศัพท์มือถือ

3.2.2 ซอฟต์แวร์

1) Zoneminder เวอร์ชั่น 1.24.2 เป็นซอฟต์แวร์ระบบ DVR (Digital Video Recorder) หรือระบบบันทึกกล้องวงจรปิด

2) Asterisk เวอร์ชั่น 1.4 เป็นซอฟต์แวร์ระบบโทรศัพท์แบบ IP-PBX สมบูรณ์แบบ

3) ระบบปฏิบัติการ Linux (UBUNTU 10.04) UBUNTU เป็นระบบปฏิบัติการ Linux ที่ได้รับความนิยม ไม่ต้องมีค่าใช้จ่ายเรื่องซอฟต์แวร์ลิขสิทธิ์

4) Solfphone (eyeBeem, X-lite) เป็นโปรแกรมสำหรับใช้แทนโทรศัพท์จะเป็นซอฟต์แวร์มีทั้งบน Windows, Linux และ Mac โปรแกรมที่เราจะนำมาใช้นี้ชื่อโปรแกรม X-Lite และ eyebeam

3.3 แผนการดำเนินงาน

1) รวบรวมข้อมูลและปัญหาของระบบการรักษาความปลอดภัย

รวบรวมข้อมูลที่เกี่ยวข้องกับระบบการรักษาความปลอดภัย พร้อมทั้งศึกษาถึงปัญหา ขอบเขต ข้อจำกัดของระบบ และวิธีการแก้ปัญหา ซึ่งจะทำให้การออกแบบระบบการรักษาความปลอดภัยมีความเหมาะสมในการใช้งานมากขึ้น

2) ศึกษาการใช้งานของโปรแกรม Asterisk

ศึกษาทฤษฎีและหลักการเขียน Dial Plane เพื่อให้ Asterisk ทำงานตามความต้องการของระบบ การติดตั้งโปรแกรมบนระบบปฏิบัติการ Linux การตั้งค่าการใช้งาน และศึกษาการสร้างระบบฐานข้อมูล

3) ศึกษาการใช้งานของโปรแกรม Zoneminder

ศึกษาทฤษฎีและหลักการทำงานของคำสั่ง (Command line) การติดตั้งโปรแกรมบนระบบปฏิบัติการ Linux การตั้งค่าการใช้งานให้สามารถเชื่อมต่อกับอุปกรณ์จำพวกกล้องแบบต่างๆ ที่เหมาะสมกับระบบงาน ศึกษาเพิ่มเติมการใช้งานภาษา PHP ฐานข้อมูล MySQL และการติดตั้ง Apache บนระบบปฏิบัติการ Linux ศึกษาระบบการส่งข้อมูลที่เป็น Streaming ภาพวีดีโอและเสียงให้ได้คุณภาพที่เหมาะสม ศึกษาการสร้างระบบฐานข้อมูลเพื่อเก็บข้อมูลที่จำเป็นไว้เป็นหลักฐานในการยืนยัน

4) ออกแบบระบบงาน และรวบรวมอุปกรณ์ที่จำเป็นต้องใช้ในระบบ

ออกแบบระบบส่งเสียงเตือนและแจ้งการบุกรุกด้วยเทคโนโลยี VoIP จุดเชื่อมต่อของอุปกรณ์ต่างๆ โดยศึกษาเครื่องมือและอุปกรณ์ที่ใช้พัฒนาอย่างละเอียด พร้อมทั้งรวบรวมอุปกรณ์ในการพัฒนาระบบให้พร้อมที่สุด

5) พัฒนาระบบส่งเสียงเตือนและแจ้งการบุกรุกด้วยเทคโนโลยี VoIP

หลังจากเตรียมความพร้อมมาทั้งหมดแล้วก็ทำการพัฒนาระบบให้สามารถทำงานได้ตามวัตถุประสงค์ที่ตั้งไว้ มีการพัฒนาระบบไประยะหนึ่ง จะเริ่มทำการทดสอบย่อยเพื่อหาข้อผิดพลาดต่างๆ ภายในระบบ แล้วทำการแก้ไข

6) ทดสอบการใช้งาน

เมื่อแก้ไขการทำงานต่างๆของระบบเป็นที่เรียบร้อยแล้ว จะนำไปสู่การทดสอบเพื่อดูประสิทธิภาพของทั้งระบบ คุณภาพของภาพและเสียง อัตราความผิดพลาดในการส่งข้อมูลด้วยการจำลองสถานการณ์ว่ามีผู้ไม่ประสงค์ดีเข้าไปในบ้านโดยไม่ได้รับอนุญาต

7) สรุปผลการพัฒนา และประโยชน์ที่จะได้รับของระบบ

นำข้อมูลที่ได้ในการจำลองสถานการณ์มาสรุปผล เพื่อใช้ในการวิเคราะห์การทำงานและประเมินประสิทธิภาพของระบบ ดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 แผนการดำเนินงาน

เดือน / งาน	ม.ค. ก.พ. 53	มี.ค. เม.ย. 53	พ.ค. มิ.ย. 53	ก.ค. ส.ค. 53	ก.ย. ต.ค. 53	พ.ย. ธ.ค. 53	ม.ค. ก.พ. 54	มี.ค. เม.ย. 54	พ.ค. 54
รวบรวมข้อมูลและปัญหาของระบบการรักษาความปลอดภัย									
ศึกษาการใช้งาน ของโปรแกรม Asterisk									
ศึกษาการใช้งานของโปรแกรม Zoneminder									
ออกแบบระบบงานและรวบรวมอุปกรณ์ที่จำเป็นต้องใช้ในระบบ									
พัฒนาระบบ									
ทดสอบการใช้งาน									
สรุปผลการพัฒนา และประโยชน์ที่จะได้รับของระบบ									

3.4 ขั้นตอนและวิธีดำเนินงาน

3.4.1 แนวคิดการทำงานของโปรแกรม

ระบบส่งเสียงเตือนสำหรับแจ้งการบุกรุกด้วยเทคโนโลยี VoIP เป็นระบบที่พัฒนาขึ้นเพื่อนำไปใช้ในหน่วยงาน องค์กร หรือตามอาคารบ้านเรือนต่างๆ ที่ต้องมีระบบการรักษาความปลอดภัยสูง โดยระบบจะส่งเสียงพูดที่บันทึกไว้ ณ ที่เกิดเหตุ และแจ้งการบุกรุกได้อย่างทันท่วงทีไปยังผู้ใช้บริการ ซึ่งมีขั้นตอนการทำงาน ดังนี้

1) ใช้ Zoneminder ตรวจจับการเคลื่อนไหวในบริเวณที่ต้องการรักษาความปลอดภัย สามารถระบุตำแหน่งหรือบริเวณที่ต้องการตรวจจับการเคลื่อนไหวได้

2) ในกรณีที่มีการตรวจพบการเคลื่อนไหวในบริเวณที่ระบุตำแหน่งไว้ระบบจะทำการ

2.1) ส่งเสียงพูดที่ได้บันทึกไว้ ณ จุดเกิดเหตุเพื่อขับไล่ผู้บุกรุก

2.2) ส่งอีเมล์ไปยังผู้ใช้ระบบ

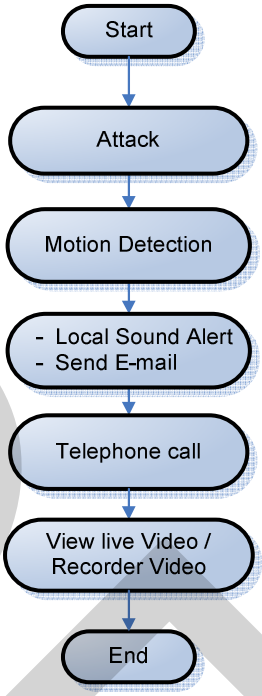
2.3) โทรศัพท์ผ่านระบบไอพีแจ้งเจ้าหน้าที่รักษาความปลอดภัย หรือผู้ใช้ระบบ

2.4) ถ้าผู้ใช้ได้รับแจ้งเหตุแล้วสามารถตรวจสอบภาพบริเวณที่เกิดเหตุผ่านโทรศัพท์มือถือ หรือเครื่องคอมพิวเตอร์เพื่อดูภาพเหตุการณ์จริง หรือเหตุการณ์การบุกรุกที่ระบบบันทึกไว้ได้

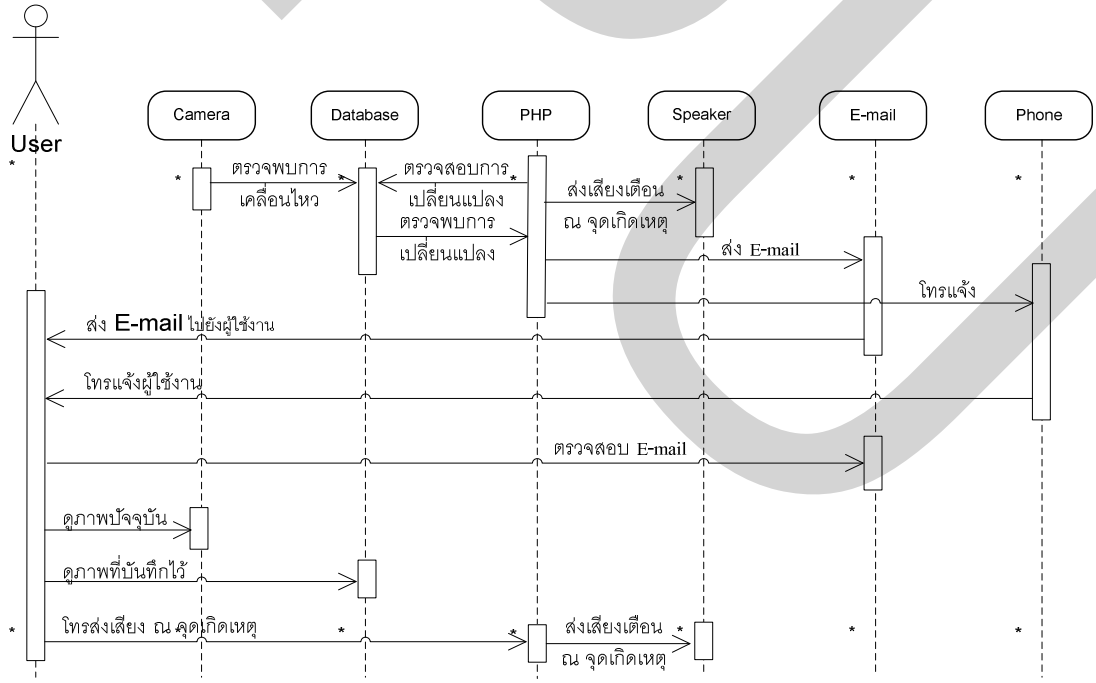
2.5) ผู้ใช้งานสามารถโทรศัพท์ผ่านระบบไอพีเข้ามา ณ ที่เกิดเหตุ เพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุ

3.4.2 การออกแบบระบบ

ระบบจะตรวจเช็คตลอดเวลา เมื่อระบบพบการเคลื่อนไหวในบริเวณที่กำหนดไว้ ระบบจะส่งเสียงพูดที่ได้บันทึกไว้ ณ จุดเกิดเหตุเพื่อขับไล่ผู้บุกรุก โดยเสียงที่บันทึกไว้จะถูกเปิดขึ้นมาไม่ซ้ำกันจนกว่าจะครบรอบตามที่กำหนด ในเวลาเดียวกันนั้นระบบส่งอีเมล์ไปยังผู้ใช้งานระบบรายละเอียดในอีเมล์จะบอกถึงหมายเลขเหตุการณ์ หมายเลขพร้อมชื่อของกล้องวงจรปิดแบบไอพี ความยาวของวีดีโอ เวลาเริ่มต้นและสิ้นสุดการบันทึก ภาพตัวอย่าง และมีจุดเชื่อมต่อเข้าไปสู่โปรแกรมเพื่อชมภาพ ณ ขณะนั้น รวมถึงสามารถดูภาพย้อนหลังได้ ในเวลาเดียวกันระบบก็จะโทรศัพท์แจ้งเจ้าหน้าที่รักษาความปลอดภัยที่เกี่ยวข้องหรือผู้ใช้งานให้รับทราบข้อมูลดังกล่าวเช่นกัน เมื่อผู้ใช้งานได้รับทราบการบุกรุกดังกล่าวแล้วสามารถที่จะโทรศัพท์เข้ามาในระบบเพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุได้ ขั้นตอนการทำงานของระบบที่พัฒนาสามารถแสดงในรูปแบบของ Flowchart ดังแสดงในภาพที่ 3.1



ภาพที่ 3.1 Flowchart แสดงขั้นตอนการทำงานของระบบส่งเสียงเตือนสำหรับแจ้งการบุกรุกด้วยเทคโนโลยี VoIP



ภาพที่ 3.2 Sequence diagram แสดงขั้นตอนการตรวจจับการเคลื่อนไหว และการแจ้งเตือนของระบบส่งเสียงเตือนสำหรับแจ้งการบุกรุกด้วยเทคโนโลยี VoIP

จากภาพที่ 3.2 Sequence diagram แสดงขั้นตอนการตรวจจับการเคลื่อนไหว และการแจ้งเตือนของระบบส่งเสียงเตือนสำหรับแจ้งการบุกรุกด้วยเทคโนโลยี VoIP สามารถอธิบายได้ว่า เมื่อกล้องแบบไอพีมีการตรวจพบการเคลื่อนไหวโดย Zoneminder ในบริเวณที่ระบุตำแหน่งไว้ ภาพจะถูกบันทึกและเก็บลงฐานข้อมูล ระบบจะมีสคริป PHP คอยตรวจสอบว่าฐานข้อมูลมีการเปลี่ยนแปลงหรือไม่ หากตรวจพบการเปลี่ยนแปลงระบบก็จะทำการ

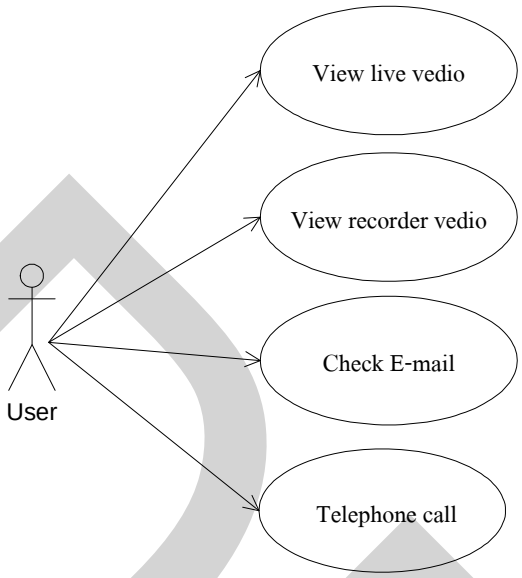
1) ส่งเสียงพูดที่ได้บันทึกไว้ ณ จุดเกิดเหตุเพื่อขับไล่ผู้บุกรุก

2) ส่งอีเมล์ไปยังผู้ใช้ระบบ

3) โทรศัพท์ผ่านระบบไอพีแจ้งเจ้าหน้าที่รักษาความปลอดภัย หรือผู้ใช้ระบบ

4) ถ้าผู้ใช้ได้รับแจ้งเหตุแล้วสามารถตรวจสอบอีเมล์ เพื่อดูรายละเอียดต่างๆ ที่ถูกส่งแนบมากับอีเมล์ดังกล่าว และสามารถดูภาพบริเวณที่เกิดเหตุผ่านโทรศัพท์มือถือ หรือเครื่องคอมพิวเตอร์เพื่อดูภาพเหตุการณ์จริง หรือเหตุการณ์การบุกรุกที่ระบบบันทึกไว้ได้ อีกทั้ง

5) ผู้ใช้งานสามารถโทรศัพท์ผ่านระบบไอพีเข้ามา ณ ที่เกิดเหตุ เพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุ



ภาพที่ 3.3 Use case แสดงความสามารถในการใช้งานระบบ ฯ ของผู้ใช้งาน

จากภาพที่ 3.3 Use case แสดงความสามารถในการใช้งานระบบฯ ซึ่งผู้ใช้งานระบบสามารถกระทำได้ดังนี้คือ

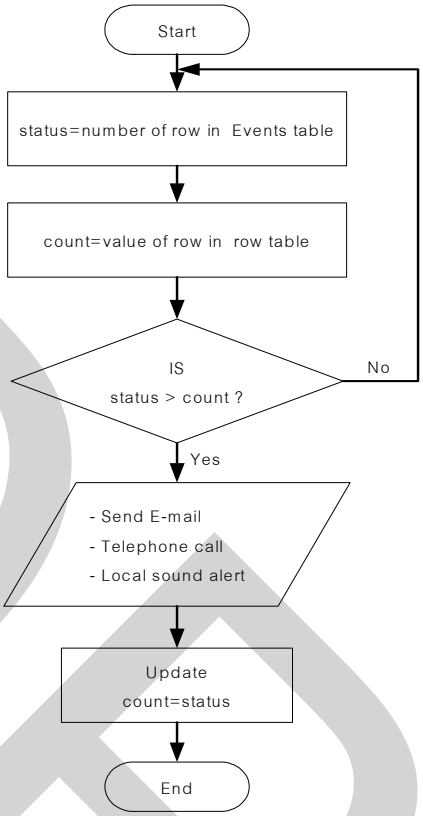
1) ดูภาพเหตุการณ์ ณ ปัจจุบัน

2) ดูภาพเหตุการณ์ที่บันทึกไว้

3) ตรวจสอบอีเมล์ที่ส่งมาจากระบบ เพื่อนำไปสู่การตัดสินใจต่อไป

4) โทรศัพท์เข้ามายังระบบ ระบบจะมีการรับสายโดยอัตโนมัติเพื่อให้ผู้ใช้งานสามารถส่งเสียงที่ต้องการ ณ ที่เกิดเหตุ

ในการออกแบบการทำงานในส่วนต่างๆ ของระบบ เช่น การตรวจจับการเคลื่อนไหว การส่งเสียงเตือน ณ ที่เกิดเหตุ การส่งอีเมล์โดยแนบรายละเอียดต่างๆ การโทรออกไปยังผู้ใช้งานเพื่อแจ้งเมื่อมีการบุกรุก และการดูภาพในขณะนั้น หรือภาพเหตุการณ์ย้อนหลัง มีการควบคุมการทำงานโดยใช้ PHP ในการจัดการทั้งหมด เมื่อ zoneminder สามารถตรวจพบการเคลื่อนไหว ก็จะทำการบันทึกลงฐานข้อมูล MySQL ระบบ ฯ ก็จะทำการตรวจสอบการเปลี่ยนแปลงของฐานข้อมูลเพื่อตรวจจับเหตุการณ์ที่เกิดขึ้น ดัง flowchart ในภาพที่ 3.4



ภาพที่ 3.4 การตรวจสอบการเปลี่ยนแปลงของฐานข้อมูล เพื่อตรวจจับเหตุการณ์ที่เกิดขึ้น

จากภาพที่ 3.4 สามารถอธิบายได้ว่า ตัวแปร status คือจำนวนแถวทั้งหมดในฐานข้อมูล Events เพื่อไปเก็บไว้ที่ตาราง row และตัวแปร count จะเก็บค่าในตาราง row เมื่อเปรียบเทียบสองค่าคือ status และ count ถ้าหาก status มีค่ามากกว่า count จะสั่งให้ระบบ

1) ส่งเสียงพูดที่ได้บันทึกไว้ ณ จุดเกิดเหตุเพื่อขับไล่ผู้บุกรุก

2) ส่งอีเมล์ไปยังผู้ใช้ระบบ

3) โทรศัพท์ผ่านระบบไอพีแจ้งเจ้าหน้าที่รักษาความปลอดภัย หรือผู้ใช้ระบบ หลังจากนั้นให้แก้ไขค่าของตัวแปร count ให้มีค่าเท่ากับ status แต่หากการเปรียบเทียบสองตัวแปรแล้ว status ไม่มากกว่า count ก็ให้กลับไปเริ่มต้นใหม่

ในส่วนของการโทรออกไปยังผู้ใช้งานเพื่อแจ้งเมื่อมีการบุกรุกจะเขียนโค้ดคำสั่ง API สั่งงาน Asterisk ผ่านทาง Socket เมื่อมีการตรวจพบการเคลื่อนไหวก็จะทำการโทรแจ้งไปยังผู้ใช้งาน หรือเจ้าหน้าที่รักษาความปลอดภัยโดยอัตโนมัติ คำสั่ง API สั่งงานผ่านทาง Socket (Asterisk Manager API, 2553) ดังแสดงตัวอย่างในภาพที่ 3.5

```
<?
function call()
{
$socket = fsockopen("localhost",5038, $errno,
$errstr, $timeout);
echo $this->userout;
fputs($socket, "Action: Login\r\n");
fputs($socket, "ActionID: 1\r\n");
fputs($socket, "UserName: admin\r\n");
fputs($socket, "Secret: 12345\r\n\r\n");
fputs ($socket, "Events: off\r\n\r\n");
sleep(1);
fputs($socket, "Action: Originate\r\n");
fputs($socket, "Channel: Zip/2000/".$this->
userout."\r\n");
fputs($socket, "Context: default\r\n");
fputs ($socket, "Extension: 2000\r\n");
fputs($socket, "Priority: 1\r\n");
fputs($socket, "CallerID: SAIWS callOut\r\n");
fputs($socket, "Async: true\r\n");
fputs($socket, "Variable: SERVNUM=".$this->server.
"|USERID=".$this->userid."\r\n\r\n");
sleep(2);
fputs($socket, "Action: Logoff\r\n\r\n");
return true;
}
```

แก้ไข Username และ Secret ที่ไฟล์ etc/asterisk/manager.conf

ที่ Context default ให้โทรออกเบอร์ที่กำหนด

ภาพที่ 3.5 ตัวอย่างโค้ดคำสั่ง API ผ่านทาง Socket เพื่อโทรแจ้งเมื่อตรวจพบการเคลื่อนไหว

ในส่วนของฐานข้อมูล Zoneminder จะประกอบด้วย 16 ตาราง ได้แก่ ตาราง Config, ControlPresets, Controls, Devices, Events, Filters, Frames, Groups, MonitorPresets, Monitors States, Stats, TriggersX10, Users, ZonePresets และตาราง Zones ผู้วิจัยได้สร้างตารางเพิ่มเติมอีก 4 ตาราง ได้แก่ ตาราง Email, Row, Number และตาราง Soundname เพื่อเก็บรายละเอียดต่างๆ ดังแสดงในพจนานุกรมข้อมูล ดังแสดงในตารางที่ 3.2 - 3.5

ตารางที่ 3.2 ตาราง Email

ฟิลด์	ชนิด	ว่างเปล่า (null)	ค่าปริยาย	หมายเหตุ
email	varchar(60)	ใช่	*NULL*	อีเมลล์ที่ส่งถึงผู้ใช้งาน

ตารางที่ 3.3 ตาราง Row

ฟิลด์	ชนิด	ว่างเปล่า (null)	ค่าปริยาย	หมายเหตุ
row	int(11)	ไม่		จำนวนแถวในตาราง Events

ตารางที่ 3.4 ตาราง Number

ฟิลด์	ชนิด	ว่างเปล่า (null)	ค่าปริยาย	หมายเหตุ
number	int(5)	ไม่		หมายเลขโทรศัพท์

ตารางที่ 3.5 ตาราง Soundname

ฟิลด์	ชนิด	ว่างเปล่า (null)	ค่าปริยาย	หมายเหตุ
sound_name	int(2)	ไม่		ชื่อของเสียงที่บันทึกไว้

จากที่ผู้วิจัยได้สร้างฐานข้อมูลเพิ่มเติมจากฐานข้อมูล Zoneminder โดยมีวัตถุประสงค์ ดังนี้

1) ตาราง Email เพื่อเก็บที่อยู่อีเมลล์ผู้ใช้งาน ที่ผู้ใช้งานกำหนดขึ้นเองจากหน้าเว็บรับข้อมูล

2) ตาราง Row เพื่อเก็บจำนวนแถวในตาราง Events เพื่อใช้เปรียบเทียบการเปลี่ยนแปลงของฐานข้อมูลที่เกิดขึ้น

3) ตาราง Number เพื่อเก็บหมายเลขโทรศัพท์ของผู้ใช้งานที่ต้องการให้ระบบโทรถึงเมื่อตรวจพบการบุกรุก

4) ตาราง Soundname เพื่อเก็บชื่อของเสียงที่บันทึกไว้ เพื่อแจ้งเตือนเมื่อมีการบุกรุก

รูปแบบการเข้าใช้งานระบบส่งเสียงเตือนสำหรับแจ้งการบุกรุกด้วยเทคโนโลยี VoIP สามารถใช้งานได้ 3 ทาง คือ ผ่านทางหน้าเว็บไซต์ของระบบ ผ่านทางโทรศัพท์มือถือ และผ่านทาง IP Phone หรือ Softphone บนเครื่องพีซีหรือโน๊ตบุ๊ค ซึ่งจะต้องเป็นอุปกรณ์ที่รองรับมาตรฐานSIP ได้เท่านั้น ดังนั้นจึงได้แบ่งการทำงานออกเป็น 4 ส่วน คือ ส่วนของการใช้งานผ่านเว็บไซต์ของระบบ ส่วนของการใช้งานผ่านโทรศัพท์มือถือ ส่วนของการใช้งานผ่านอุปกรณ์ที่รองรับ VoIP หรือ Softphone และส่วนของการส่งเสียงเตือนเพื่อขับไล่ผู้ไม่ ประสงค์ดี ดังนี้

ส่วนการใช้งานผ่านเว็บไซต์ของระบบ

เป็นส่วนที่ใช้ติดต่อกับระบบผ่านหน้าเว็บไซต์ ผู้ใช้สามารถเข้ามาใช้งานระบบจากคอมพิวเตอร์ที่เชื่อมต่ออยู่กับระบบเครือข่ายของระบบฯ ตัวอย่างหน้าเว็บไซต์หน้าแรกดังแสดงในภาพที่ 3.6 โดยในส่วนนี้จะประกอบด้วย

1) ส่วนแสดงผลภาพเหตุการณ์ที่บันทึกไว้ ผู้ใช้งานสามารถเลือกรายการที่ต้องการดูวีดีโอย้อนหลังได้ตามต้องการจากรายการที่ปรากฏ ดังแสดงในภาพที่ 3.7

2) ส่วนจัดการ ลบ แก้ไข ส่งออก ภาพหรือวีดีโอ ผู้ใช้งานสามารถจัดการกับรายการวีดีโอ โดยการ ลบ แก้ไข และทำการส่งออกเป็นภาพหรือวีดีโอได้จากรายการนี้ดังแสดงในภาพที่ 3.8

3) ส่วนจัดการ การตั้งค่า และการแสดงผลในรูปแบบต่างๆ ผู้ใช้งานสามารถตั้งค่าการแสดงผลในรูปแบบต่างๆ ตามต้องการ ดังแสดงในภาพที่ 3.9

4) ส่วนตั้งค่าให้อุปกรณ์ และการแสดงผลของกล้อง ผู้ใช้งานสามารถตั้งค่าอุปกรณ์อันได้แก่ กล้องแบบไอพี หรืออื่นๆ นอกจากนี้ยังสามารถตั้งค่าการแสดงผลของกล้องได้จากรายการนี้ ดังแสดงในภาพที่ 3.10

5) ส่วนตั้งค่าตัวกรองตามต้องการ ผู้ใช้งานสามารถตั้งค่าตัวกรองเพื่อคัดสรรรายการที่ต้องการค้นหาได้จากรายการนี้ ดังแสดงในภาพที่ 3.11

6) ส่วนตั้งค่า Bandwidth ผู้ใช้งานสามารถตั้งค่า Bandwidth ของการส่งผ่านสัญญาณสื่อสารเป็นการวัดช่วงความถี่ ที่สัญญาณใช้งานได้จากรายการนี้ ดังแสดงในภาพที่ 3.12

7) ส่วนควบคุมการทำงานของโปรแกรม ผู้ใช้งานสามารถสั่ง หยุด หรือเริ่มการทำงานใหม่ได้จากรายการนี้ ดังแสดงในภาพที่ 3.13

8) ส่วนกำหนดโซนที่ต้องการให้ทำการตรวจจับการเคลื่อนไหว ผู้ใช้งานสามารถกำหนดโซน หรือบริเวณที่ต้องการให้กล้องตรวจจับการเคลื่อนไหว เพื่อทำการแจ้งเตือนและบันทึกภาพตามคำสั่งได้จากรายการนี้ ดังแสดงในภาพที่ 3.14

9) ส่วนแสดงผลเป็นช่วงเวลา (Timeline) ผู้ใช้งานสามารถดูช่วงเวลาที่ได้ทำการบันทึกภาพ เมื่อนำเม้าไปชี้จะแสดงภาพตามช่วงเวลาที่ได้บันทึกไว้ เพื่อความสะดวกในการค้นหาภาพเหตุการณ์ตามที่ต้องการ ดังแสดงในภาพที่ 3.15

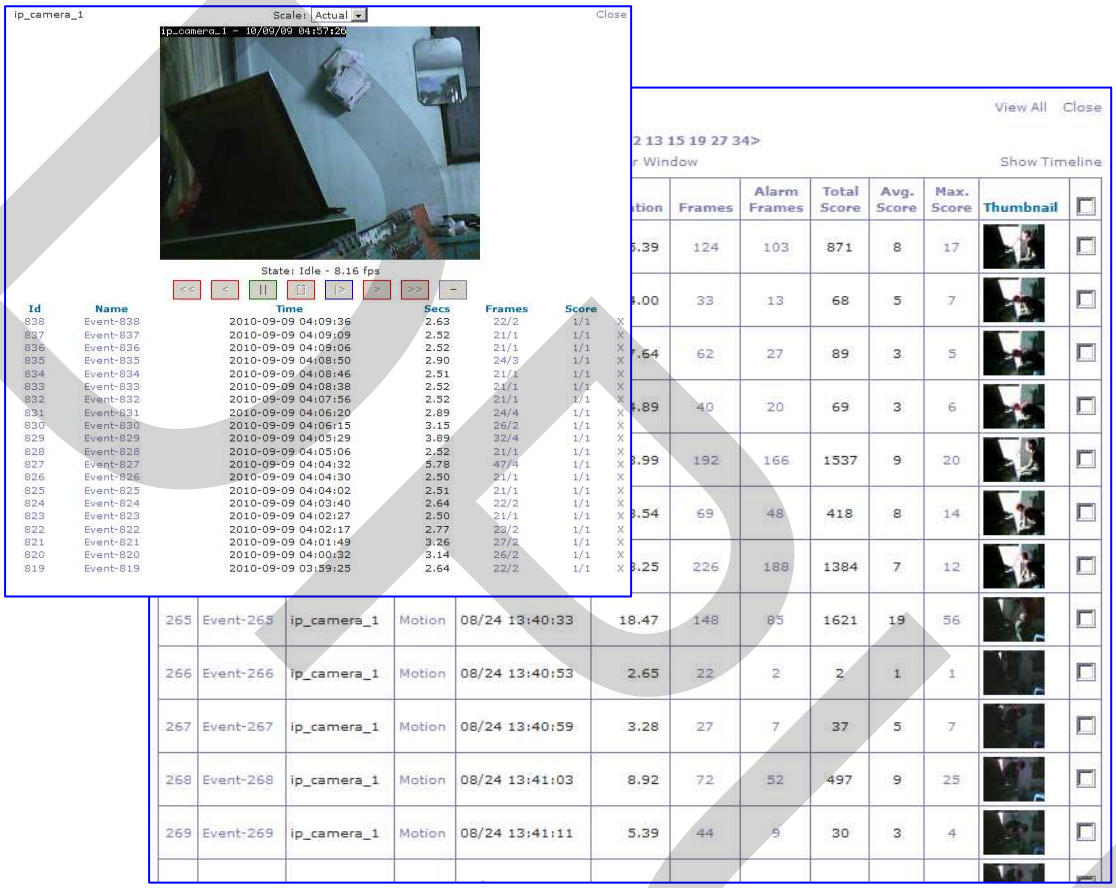
10) ส่วนของอีเมล์เมื่อตรวจพบการเคลื่อนไหว ผู้ใช้งานสามารถตรวจสอบอีเมล์ที่แจ้งเตือนมา ซึ่งในเนื้อหาจะแสดงถึงรายละเอียด ณ จุดเกิดเหตุ กล้อง ตัวอย่างภาพเหตุการณ์และรายการที่จะเชื่อมต่อไปยังภาพวีดีโอนั้นๆ ได้ ดังแสดงในภาพที่ 3.16

11) ส่วนของการเปลี่ยนแปลงที่อยู่อีเมล์ปลายทางของผู้ใช้งาน ดังแสดงในภาพที่ 3.17

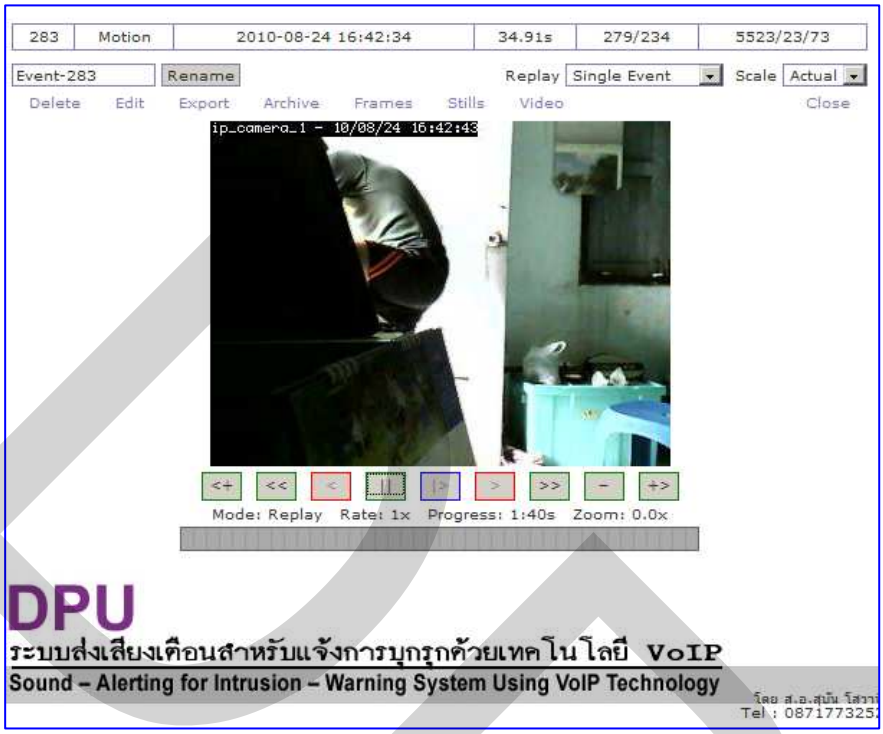
12) ส่วนของการเปลี่ยนแปลงที่เบอร์โทรปลายทางของผู้ใช้งาน ดังแสดงในภาพที่ 3.18

ภาพที่ 3.6 ตัวอย่างเว็บไซต์ของระบบที่พัฒนา

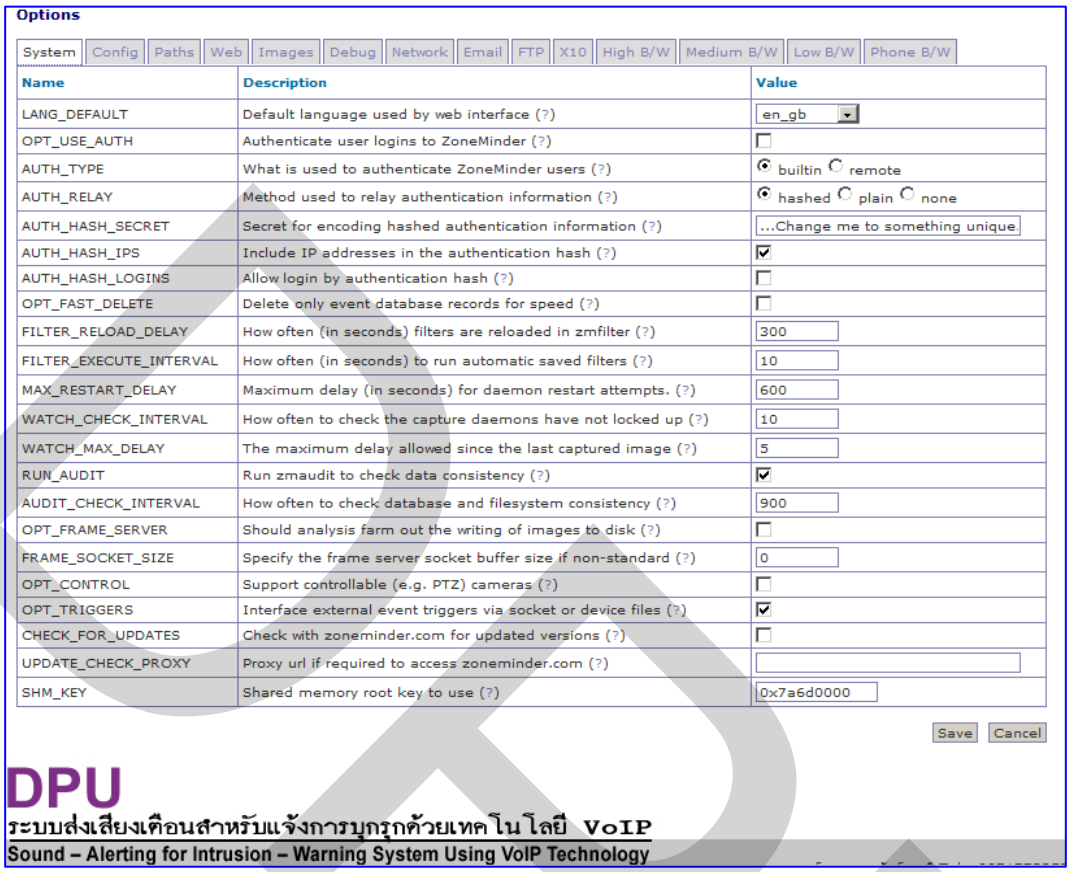
ส่วนแสดงผลภาพเหตุการณ์ที่บันทึกไว้ เป็นส่วนที่แสดงรายการเหตุการณ์ทั้งหมด พร้อมทั้งแสดง ภาพตัวอย่างขนาดเล็กที่ได้ทำการบันทึกไว้ เพื่อให้ผู้ใช้ งานสามารถเลือกดูรายการเหตุการณ์ต่างๆ ได้ตามต้องการดังแสดงในภาพที่ 3.7



ภาพที่ 3.7 ส่วนแสดงผลภาพเหตุการณ์ที่บันทึกไว้



ภาพที่ 3.8 ส่วนจัดการ ลบ แก้ไข ส่งออก ภาพหรือวีดีโอ



ภาพที่ 3.9 ส่วนจัดการ การตั้งค่า และการแสดงผลในรูปแบบต่างๆ

ส่วนของการตั้งค่าให้อุปกรณ์ และการแสดงผลของกล้อง จะได้กล่าวถึงวิธีการกำหนดค่าต่างๆ เพื่อให้โปรแกรม Zoneminder สามารถใช้งานร่วมกับกล้องแบบไอพีที่ได้จัดเตรียมไว้แล้วคือ กล้องแบบไอพี ยี่ห้อ DLINK รุ่น DCS-910 10/100 FAST ETHERNET NETWORK CAMERA (Dlink DCS-910, 2553, 1 ตุลาคม) มีการเชื่อมต่อ และตั้งค่าต่างๆ ดังนี้

General

1) Name ตั้งชื่อให้ตัวกล้อง ในที่นี้ตั้งชื่อเป็น IP_CAMERA_1

2) Source Type เลือกชนิดของทรัพยากรณ์ ในที่นี้ให้เลือกเป็น Remote เพื่อควบคุมจากระบบเครือข่ายระยะไกลได้

3) Function เลือกลักษณะการใช้งาน มีเมนูให้เลือกดังนี้

3.1) Non คือ ไม่สามารถดูภาพเหตุการณ์ปัจจุบันจากกล้องได้ แต่สามารถดูภาพย้อนหลังที่มีการบันทึกไว้ก่อนหน้า

3.2) Monitor คือ ดูภาพจากกล้องโดยไม่มีการบันทึก หรือแจ้งเตือนใดๆ

3.3) Modect คือ บันทึกเมื่อมีการตรวจพบการเคลื่อนไหว

3.4) Record คือ บันทึกต่อเนื่อง เช่นบันทึกการประชุม หรือการทดลองต่างๆ โดยไม่มีการตรวจจับการเคลื่อนไหว

3.5) Mocord คือ ผสมระหว่าง Modect และ Record กล่าวคือ มีทั้งการบันทึกต่อเนื่อง และมีการตรวจจับการเคลื่อนไหว เพื่อวิเคราะห์และเน้นเหตุการณ์ที่เกิดขึ้น

3.6) Nodect เป็นโหมดพิเศษ ซึ่งออกแบบมาให้สามารถใช้งานร่วมกับ Trigger ภายในได้ ไม่มีการตรวจจับการเคลื่อนไหว เหตุการณ์ต่างๆจะถูกบันทึกเมื่อตรงตามความต้องการของ Trigger ที่กำหนดไว้แล้ว

ในที่นี้ให้เลือกเป็น Modect เพื่อบันทึกเมื่อมีการตรวจพบการเคลื่อนไหว

Source

1) Remote Protocol กำหนดเป็น Http

2) Remote Host Name กำหนดเป็น admin:ban2000@192.168.1.4 ซึ่งมาจาก User:password@หมายเลข IP ของกล้องแบบไอพี

3) Remote Host Port กำหนดเป็นพอร์ท 80

4) Remote Host Path เป็น Host Path ที่ถูกกำหนดจากรุ่นและยี่ห้อของกล้อง ในที่นี้ให้กำหนดเป็น VIDEO.CGI?

5) Capture Width (pixels) เป็นการกำหนดความละเอียดของภาพแนวกว้าง ในที่นี้กำหนดเป็น 320 pixels

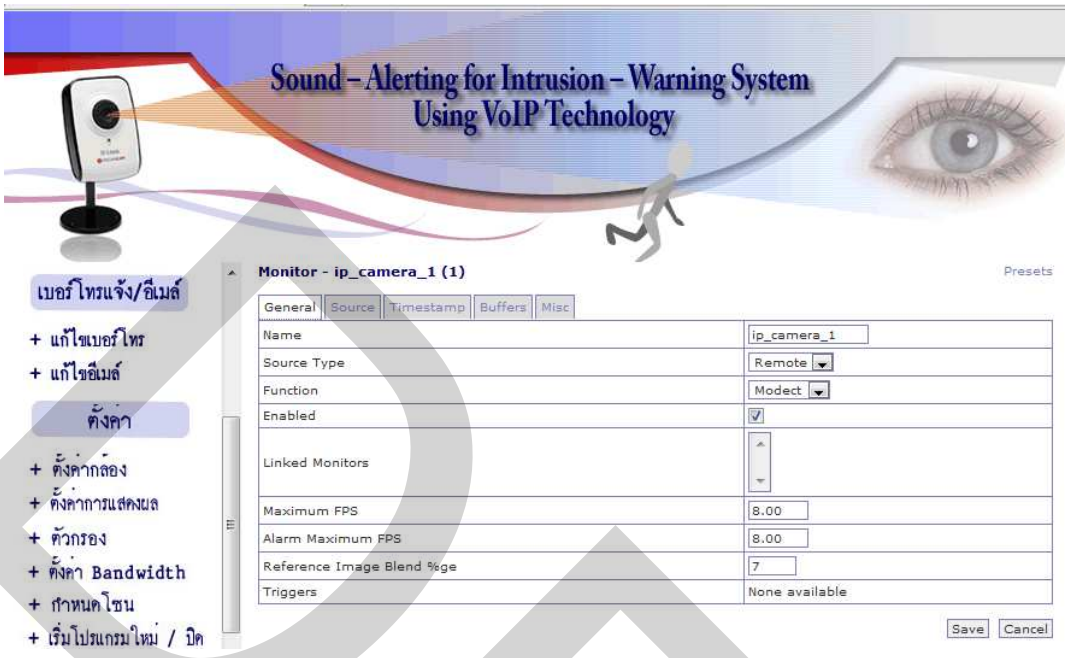
6) Capture Height (pixels) เป็นการกำหนดความละเอียดของภาพแนวสูง ในที่นี้กำหนดเป็น 240 pixels

Time stamp

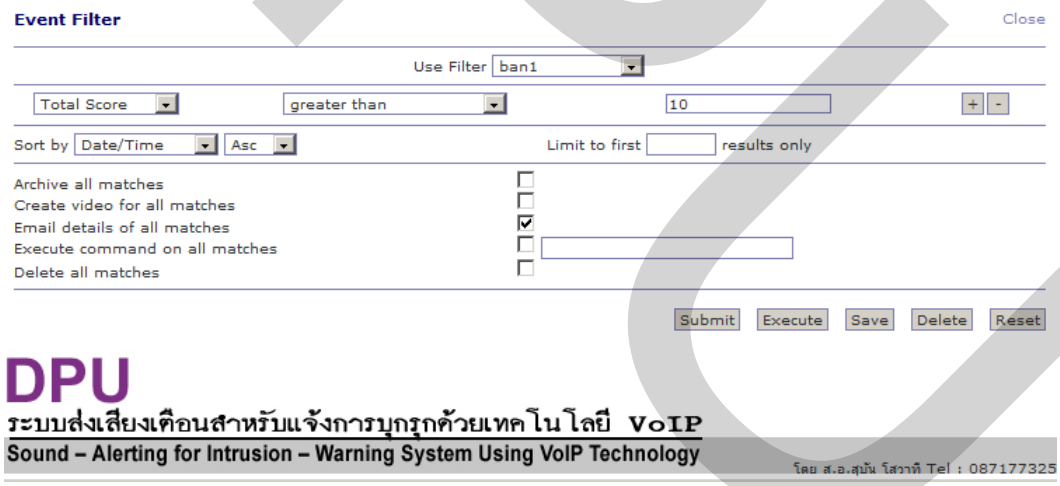
Timestamp Label Format เป็นรูปแบบเวลาที่ต้องการ เมื่อมีการบันทึกในที่นี้กำหนด ให้เป็น %y/%m/%d %H:%M:%S หมายถึง วัน/เดือน/ปี ชั่วโมง/นาที/วินาที

Misc

Event Prefix เป็นการใช้คำนำหน้าชื่อของเหตุการณ์ที่บันทึก เช่น door- ชื่อเหตุการณ์ที่บันทึกก็จะเป็น door-1, door-2…. ตามลำดับ

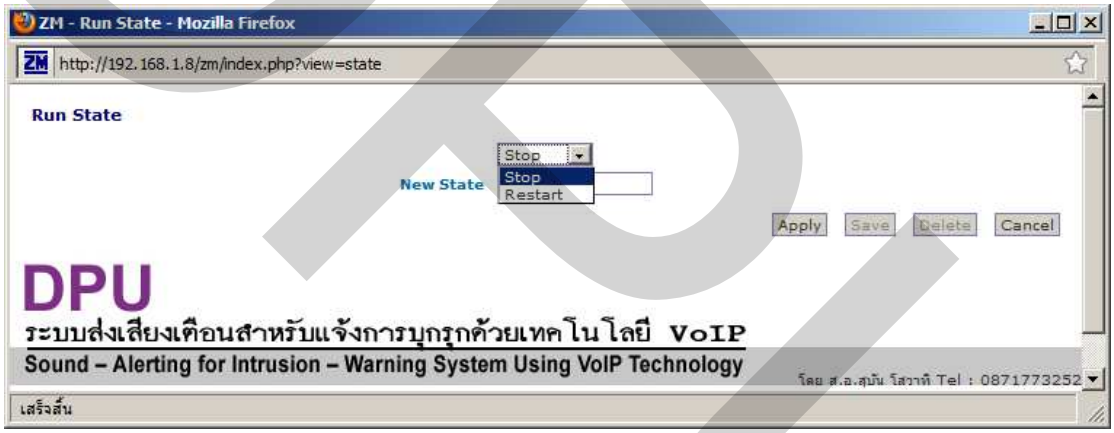


ภาพที่ 3.10 ส่วนตั้งค่าเพื่อเชื่อมต่อกับกล้องแบบไอพี และการตั้งค่าการแสดงผลของกล้อง



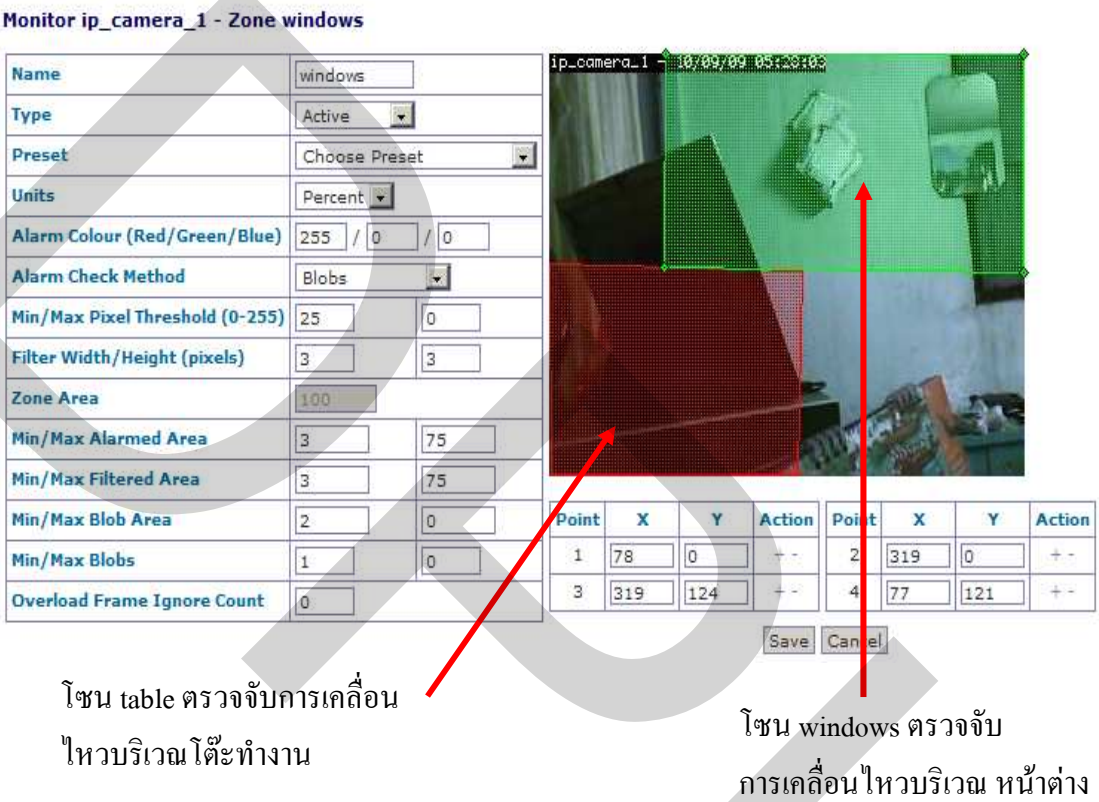
ภาพที่ 3.11 ส่วนตั้งค่าตัวกรองตามต้องการ

ภาพที่ 3.12 ส่วนตั้งค่า Bandwidth



ภาพที่ 3.13 ส่วนควบคุมการทำงานของโปรแกรม

ส่วนกำหนดบริเวณ (โซน) ที่ต้องการให้ทำการตรวจจับการเคลื่อนไหว เป็นส่วนที่ให้ผู้ใช้งานสามารถ กำหนดบริเวณที่ต้องการให้ระบบทำการตรวจจับการ เคลื่อนไหว สามารถกำหนดได้หลายโซน ซึ่งจะมีราย ละเอียดต่างๆ ให้กำหนด ดังแสดงในภาพที่ 3.14



ภาพที่ 3.14 ส่วนกำหนดโซนที่ต้องการให้ทำการตรวจจับการเคลื่อนไหว

ส่วนของอีเมล์เมื่อตรวจพบการเคลื่อนไหว เป็นส่วนที่แจ้งถึงผู้ใช้งานเมื่อมีการตรวจพบการเคลื่อนไหว ซึ่งจะมีรายละเอียดดังต่อไปนี้

1) Subject: ประกอบด้วย หมายเลข Alarm รหัส และชื่อของกล้องที่ตรวจพบการเคลื่อนไหว

2) Monitor: ประกอบด้วย รหัส และชื่อของกล้องที่ตรวจพบการเคลื่อนไหว

3) Events ID: ประกอบด้วย รหัสของเหตุการณ์ที่ตรวจพบการเคลื่อนไหว

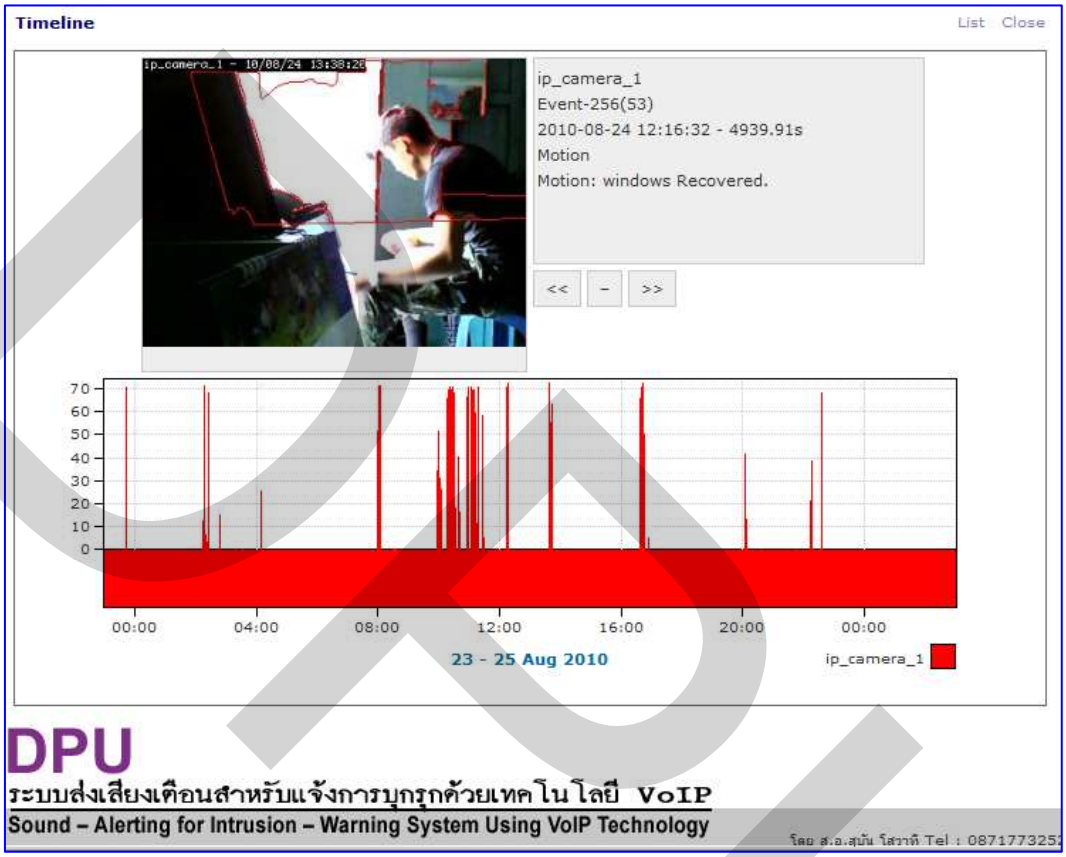
4) Length: ประกอบด้วยความยาวของวีดีโอที่บันทึกไว้ได้

5) Frame: ประกอบด้วยจำนวนเฟรมที่บันทึกเป็นภาพ

6) Time: ประกอบด้วยเวลาเมื่อเริ่มบันทึก และสิ้นสุดการบันทึก

7) จุดเชื่อมต่อไปยังภาพตัวอย่างจากเหตุการณ์

8) จุดเชื่อมต่อไปยังภาพวีดีโอเหตุการณ์ที่เกิดขึ้น ดังแสดงในภาพที่ 3.15



ภาพที่ 3.15 ส่วนแสดงผลเป็นช่วงเวลา (Timeline)

ส่วนของอีเมล์เมื่อตรวจพบการเคลื่อนไหว เป็นส่วนที่แจ้งถึงผู้ใช้งานเมื่อมีการตรวจพบการเคลื่อนไหว ซึ่งจะมีรายละเอียดดังต่อไปนี้

1) Subject: ประกอบด้วย หมายเลข Alarm รหัส และชื่อของกล้องที่ตรวจพบการเคลื่อนไหว

2) Monitor: ประกอบด้วย รหัส และชื่อของกล้องที่ตรวจพบการเคลื่อนไหว

3) Events ID: ประกอบด้วย รหัสของเหตุการณ์ที่ตรวจพบการเคลื่อนไหว

4) Length: ประกอบด้วยความยาวของวีดีโอที่บันทึกไว้ได้

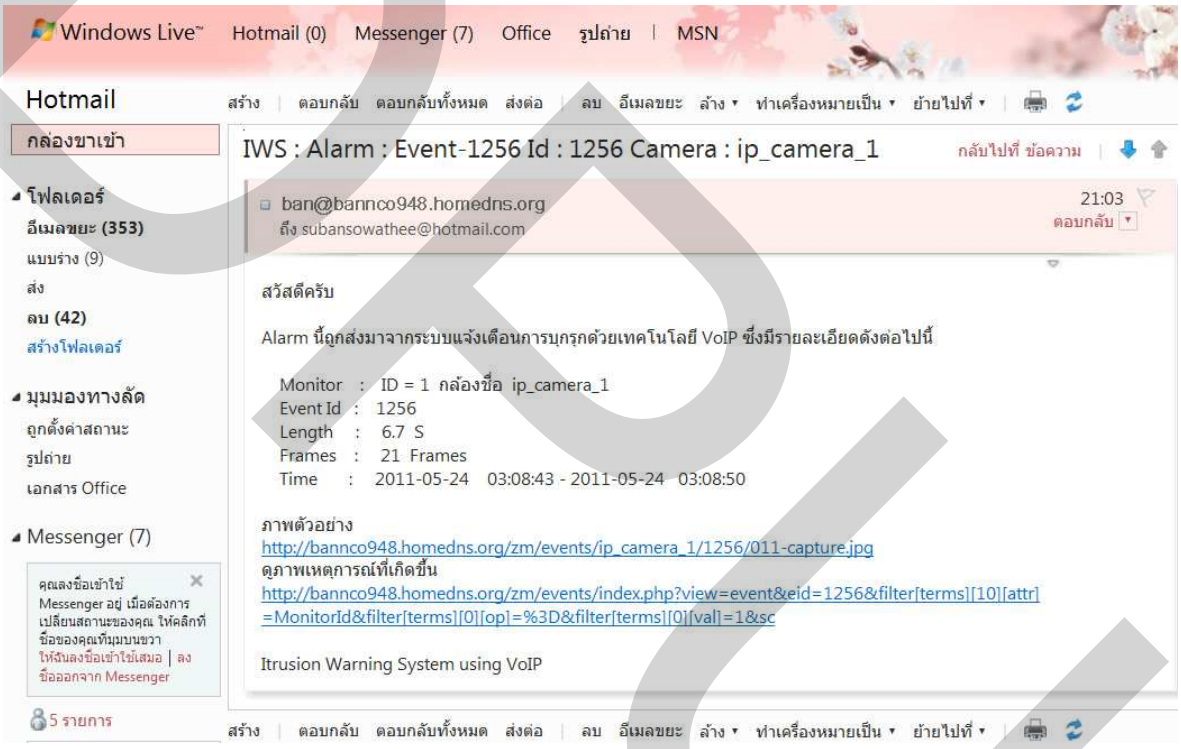
5) Frame: ประกอบด้วยจำนวนเฟรมที่บันทึกเป็นภาพ

6) Time: ประกอบด้วยเวลาเมื่อเริ่มบันทึก และสิ้นสุดการบันทึก

7) จุดเชื่อมต่อไปยังภาพตัวอย่างจากเหตุการณ์

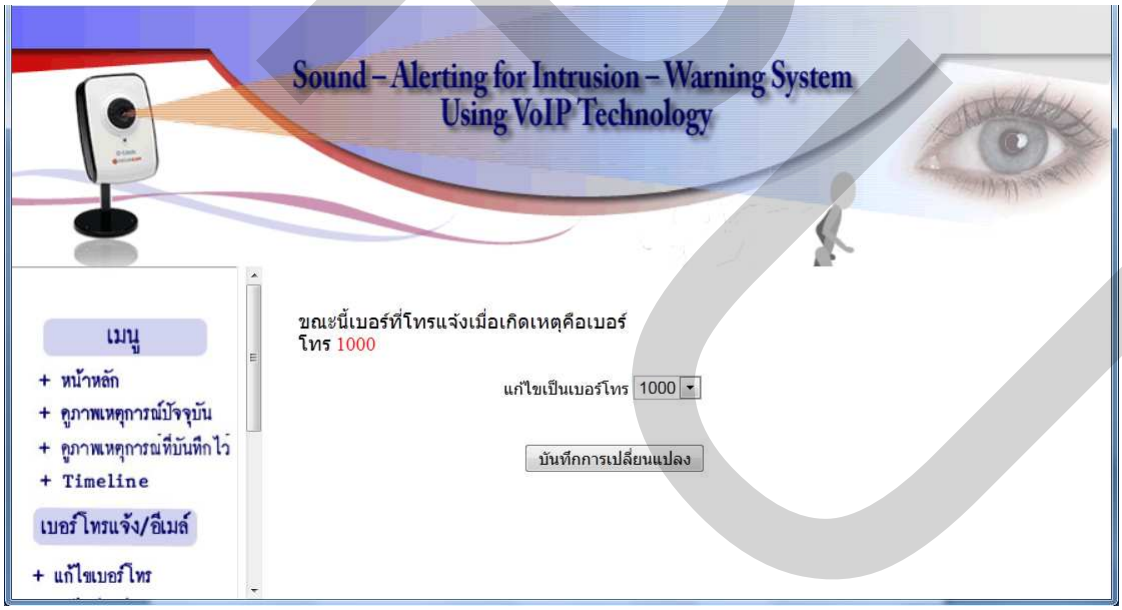
8) จุดเชื่อมต่อไปยังภาพเหตุการณ์ที่เกิดขึ้น

ระบบที่พัฒนาสามารถส่งอีเมล์หาอีเมล์เซอเวอร์ (Email server) ภายนอกได้ โดยมีการตั้งค่าที่ SmartHost ของ Postfix mail server ซึ่งผู้วิจัยใช้เป็นเมล์เซอเวอร์ท้องถิ่น โดย RelayHost ใน Postfix ให้ใส่ [ชื่อโฮสต์ หรือ ไอพีแอดเดรส] ตามด้วย: หมายเลขพอร์ต (ดีฟอลต์คือ 25) ในที่นี้ผู้วิจัยใช้บริการของทรูอินเตอร์เน็ตซึ่งมี RelayHost คือ SMTP ของทรูอินเทอร์เน็ตเป็น (mail.truemail.co.th) ก็จะได้เป็น relayhost = [mail.truemail.co.th]: 25 โดยในวิทยานิพนธ์นี้จะแสดงการส่งอีเมล์ตัวอย่างไปยัง hotmail ดังแสดงในรูปที่ 3.16



ภาพที่ 3.16 รายละเอียดของอีเมล์ที่ส่งเมื่อตรวจพบการเคลื่อนไหว

ภาพที่ 3.17 ส่วนของการเปลี่ยนแปลงที่อยู่อีเมล์ปลายทางของผู้ใช้งาน



ภาพที่ 3.18 ส่วนของการเปลี่ยนแปลงที่เบอร์โทรปลายทางของผู้ใช้งาน

ส่วนของการใช้งานผ่านโทรศัพท์มือถือ

เป็นส่วนที่ใช้ติดต่อกับระบบผ่านโทรศัพท์มือถือที่รองรับ GPRS หรือ WiFi เพื่อเชื่อมต่อระบบ เครือข่าย สามารถเข้าชมภาพเหตุการณ์ปัจจุบันได้ ดังแสดงในภาพที่ 3.19

ภาพที่ 3.19 ตัวอย่างการใช้งานผ่านโทรศัพท์มือถือ

ส่วนของการใช้งานผ่านอุปกรณ์ VoIP และ Softphone

เป็นส่วนที่ใช้โทรติดต่อไปยังเจ้าหน้าที่รักษาความปลอดภัย หรือผู้ใช้งานระบบเมื่อมีการตรวจพบการ เคลื่อนไหว ซึ่งมีคุณสมบัติ ดังต่อไปนี้

1) ระบบสามารถโทรแจ้งโดยอัตโนมัติเมื่อตรวจพบการเคลื่อนไหว และบอกได้ว่ากล้องที่เกิดเหตุ ชื่ออะไรเพื่อให้การตรวจสอบเป็นไปได้อย่างรวดเร็วและทันเหตุการณ์

2) สามารถกำหนดเบอร์โทรแจ้งเหตุปลายทางได้

3) เมื่อระบบแจ้งเตือนมายังผู้ใช้งาน ผู้ใช้งานดูภาพเหตุการณ์ที่เกิดขึ้นแล้ว ผู้บุกรุกยังคงอยู่ในที่เกิดเหตุ ผู้ใช้งานสามารถโทรศัพท์แบบไอพี (IP Phone หรือ Softphone) เข้ามาในระบบเพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุได้ โดยระบบจะทำการรับโทรศัพท์โดยอัตโนมัติ

ส่วนของการส่งเสียงเตือนเพื่อขับไล่ผู้ไม่ประสงค์ดี

เป็นส่วนที่จะช่วยให้ผู้ไม่ประสงค์ดีตกใจ และรีบออกไปให้ห่างจากบริเวณที่เกิดเหตุได้ โดยมีคุณสมบัติ ดังต่อไปนี้

1) ผู้ใช้งานสามารถบันทึกเสียงของตัวเองลงไปได้ โดยที่เสียงนั้นจะต้องมีน้ำหนักที่จะทำให้ผู้ไม่ประสงค์ดีตกใจ และขู่ขวัญให้เกรงกลัว

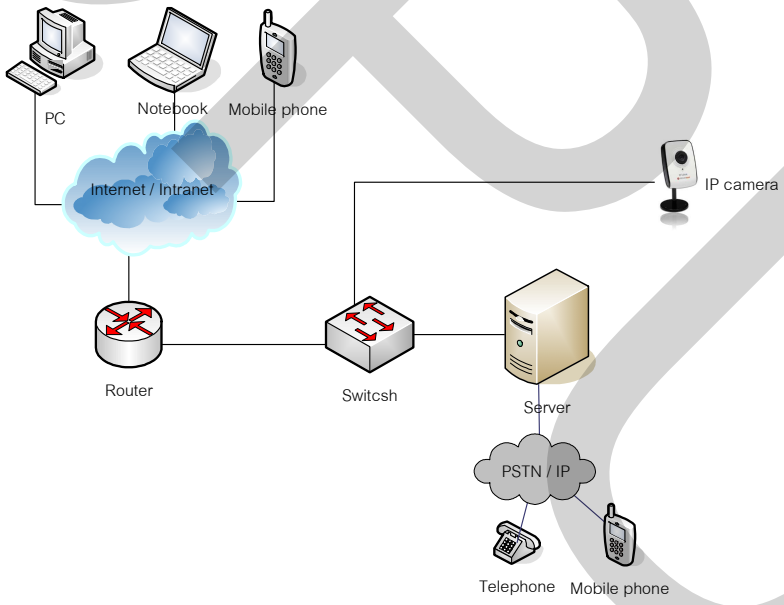
2) เสียงที่บันทึกจะถูกเปิดขึ้นมาตามลำดับเหตุการณ์ที่ตั้งไว้ เมื่อมีการตรวจพบการเคลื่อนไหว

เมื่อผู้ใช้งานทราบถึงการบุกรุก (ผ่านทางโทรศัพท์หรือ e-mail ที่ระบบแจ้ง) ผู้ใช้งานสามารถโทรศัพท์เข้ามาในระบบเพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุได้

บทที่ 4

การทดสอบระบบ

เนื้อหาในบทนี้จะกล่าวถึงการทดสอบระบบที่ได้พัฒนาขึ้น เพื่อประเมินผลการใช้งานและปรับปรุงข้อผิดพลาดที่เกิดขึ้น โดยได้ทำการทดสอบระบบที่สร้างขึ้น โดยจำลองสถานการณ์ขึ้นมา ในการทดสอบกำหนดให้มีกล้องไอพี จำนวน 1 ตัว ติดตั้งไว้บริเวณที่คาดว่ามีความเสี่ยงสูงต่อการถูกขโมย และผู้คนไม่พลุกพล่านจนเกินไป มีการติดตั้งอุปกรณ์การใช้งานของผู้ใช้งานในรูปแบบต่างๆ ดังแสดงในภาพที่ 4.1 ผลการทดสอบดังแสดงในตารางที่ 4.1 และตารางที่ 4.2



ภาพที่ 4.1 อุปกรณ์และเครือข่ายที่ใช้ในการทดสอบระบบ

กล้องไอพีที่ใช้ในการทดสอบ (Dlink DCS-910, 2553, 1 ตุลาคม)

ยี่ห้อ : DLINK

รุ่น : DCS-910 10/100 FAST ETHERNET NETWORK CAMERA

การทดสอบใช้ระบบ

ในการทดสอบการใช้งานระบบจะทำการทดสอบในเวลาที่มีแสงสว่างเท่านั้น เนื่องจากกล้องไอพีที่นำมาทดสอบไม่รองรับการทำงานในที่มืด หากต้องการให้สามารถใช้งานในที่มืดจะต้องใช้กล้องที่มีความสามารถพิเศษ เช่น กล้องอินฟาเรด เป็นต้น โดยการทดสอบได้กำหนดให้มีการเดินผ่านบริเวณที่ติดตั้งระบบซ้ำหลายๆ ครั้ง เพื่อทำการบันทึกการ ส่งเสียงเตือน ส่งอีเมล์และการโทรแจ้งไปยังผู้ใช้งาน ซึ่งได้ทำการทดลองดังนี้

กรณีที่ 1 ทดสอบเดินผ่านบริเวณที่ติดตั้งระบบในเวลาที่มีแสงสว่างมาก (เวลา 12.00 น.)

การทดสอบในส่วนนี้ได้ทำการเดินผ่านบริเวณที่ติดตั้งระบบจำนวน 20 ครั้ง แต่ละครั้งห่างกัน 5 วินาที การส่งเสียงเตือน ณ ที่เกิดเหตุ การส่งอีเมล์ไปยังผู้ใช้งาน และการโทรแจ้งไปยังผู้ใช้งาน ได้ผลดังแสดงในตารางที่ 4.1

ตารางที่ 4.1 ตารางแสดงผลการทดสอบในเวลาที่มีแสงสว่างมาก

รายการ	ส่ง / ครั้ง	ไม่ส่ง / ครั้ง	ความถูกต้องคิดเป็น %
ส่งเสียงเตือน	20	0	100 %
ส่งอีเมล์	20	0	100 %
โทรแจ้ง	20	0	100 %

กรณีที่ 2 ทดสอบเดินผ่านบริเวณที่ติดตั้งระบบในเวลาที่มีแสงสว่างน้อย (เวลา 18.00 น.)

การทดสอบในส่วนนี้ได้ทำการเดินผ่านบริเวณที่ติดตั้งระบบจำนวน 20 ครั้ง แต่ละครั้งห่างกัน 5 วินาที การส่งเสียงเตือน ณ ที่เกิดเหตุ การส่งอีเมล์ไปยังผู้ใช้งาน และการโทรแจ้งไปยังผู้ใช้งาน ได้ผลดังแสดงในตารางที่ 4.2

ตารางที่ 4.2 ตารางแสดงผลการทดสอบในเวลาที่มีแสงสว่างน้อย

รายการ	ส่ง / ครั้ง	ไม่ส่ง / ครั้ง	ความถูกต้องคิดเป็น %
ส่งเสียงเตือน	20	0	100 %
ส่งอีเมล์	20	0	100 %
โทรแจ้ง	20	0	100 %

เนื่องจากกล้องแบบไอพีที่นำมาทดสอบคือ DLINK DCS-910 ซึ่งสามารถจับภาพวิดีโอในสภาพแสงน้อยได้ (เซนเซอร์ระดับ1.0 Lux) ในกรณีในที่มืด (น้อยกว่า 1.0 Lux) จำเป็นที่จะต้องมีการเปลี่ยนกล้องวงจรปิดที่สามารถตรวจจับการเคลื่อนไหวในบริเวณที่มืดได้ ในที่นี้ผู้วิจัยขอแนะนำให้ใช้กล้องไอพียี่ห้อ Foscam รุ่น FI8908W ซึ่งสามารถรองรับการตรวจจับการใช้งานในที่มืด และใช้งานร่วมกับ Zoneminder ได้ (Zoneminder, 2553)

บทที่ 5
บทสรุป และข้อเสนอแนะ

ในบทนี้จะเป็นการอภิปรายเพื่อสรุปผลที่ได้จากการทดสอบงานวิจัย รวมทั้งข้อกำจัดของระบบที่พบจากการทดสอบระบบ และข้อเสนอแนะสำหรับแนวทางในการพัฒนางานวิจัยนี้ต่อไปเพื่อแก้ข้อบกพร่องของระบบให้มีประสิทธิภาพมากขึ้น

5.1 สรุปผลการวิจัย

5.1.1 สรุปผลตามวัตถุประสงค์ของงานวิจัย

1) ในการพัฒนาพัฒนาระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี Voice over IP (VoIP) ตามวัตถุประสงค์ของงานวิจัย คือสามารถศึกษา ออกแบบ และพัฒนาระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี Voice over IP (VoIP) โดยการประยุกต์ใช้ซอฟต์แวร์ Asterisk (IP-PBX) และ Zoneminder (Digital Video Recorder) ได้อย่างเหมาะสมและมีประสิทธิภาพ

2) ระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี Voice over IP (VoIP) สามารถแจ้งการบุกรุก และมีการส่งเสียงเตือน ณ ที่เกิดเหตุโดยอัตโนมัติไปยังผู้ใช้งานอย่างมีระบบ

3) ได้มีการจำลองสถานการณ์โดยการทดสอบระบบที่พัฒนา และพิสูจน์ว่าระบบสามารถใช้งานได้จริง

5.1.2 สรุปผลตามขอบเขตของงานวิจัย ซึ่งให้ความสำคัญกับระบบรักษาความปลอดภัยโดยการประยุกต์ใช้ Asterisk (IP-PBX) และ Zoneminder (Digital Video Recorder) ในการออกแบบระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP จากการทดสอบการทำงานต่างๆ ตามขอบเขตของระบบ สามารถสรุปผลได้ดังนี้

1) สามารถใช้ Zoneminder ตรวจจับการเคลื่อนไหวในบริเวณที่ต้องการรักษาความปลอดภัย

2) ผู้ใช้งานสามารถระบุตำแหน่งหรือบริเวณที่ต้องการตรวจจับการเคลื่อนไหวได้ และในกรณีที่มีการตรวจพบการเคลื่อนไหวในบริเวณที่ระบุตำแหน่งไว้ ระบบสามารถ

2.1) ส่งเสียงพูดที่ได้บันทึกไว้ ณ จุดเกิดเหตุเพื่อขับไล่ผู้บุกรุก

2.2) ส่งอีเมล์ไปยังผู้ใช้ระบบ

2.3) โทรศัพท์ผ่านระบบไอพีแจ้งผู้ใช้งาน หรือเจ้าหน้าที่รักษาความปลอดภัย

2.4) เมื่อผู้ใช้งานได้รับแจ้งเหตุแล้วสามารถตรวจสอบภาพบริเวณที่เกิดเหตุผ่านโทรศัพท์มือถือ หรือเครื่องคอมพิวเตอร์เพื่อดูภาพเหตุการณ์จริง หรือเหตุการณ์การบุกรุกที่ระบบบันทึกไว้ได้

2.5) ผู้ใช้งานสามารถโทรศัพท์ผ่านระบบไอพีเข้ามา ณ ที่เกิดเหตุ เพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุ

3) ภายหลังการพัฒนา ได้มีการทดสอบการใช้งานระบบ ในเวลาที่มีปริมาณแสงสว่างมาก (เวลา 12.00 น.) และในเวลาที่มีปริมาณแสงสว่างน้อย (เวลา 18.00 น.) เพื่อตรวจสอบความถูกต้องใน การทำงานของระบบ เป็นเวลา 3 วัน โดยมีการจำลอง การบุกรุก 20 ครั้ง ในแต่ละวัน ผลปรากฏว่าระบบสามารถทำงานได้ดีในบริเวณที่มีแสงสว่างเพียงพอสำหรับกล้องแบบไอพี (มากกว่า 0 ลักซ์) โดยไม่มีข้อผิดพลาดใดๆ

5.2 ข้อจำกัดของระบบ

ข้อจำกัดของระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP มีดังนี้

5.2.1 เนื่องจากกล้องที่นำมาทดลองสามารถใช้งานได้ดีในบริเวณที่มีแสงสว่างเพียงพอ (แสงสว่างมากกว่า 0 ลักซ์) จึงไม่สามารถใช้งานได้ในที่มืด (แสงสว่างน้อยกว่า 0 ลักซ์) หากต้องการให้สามารถใช้งานได้ดีในที่มืดก็สามารถใช้กล้องที่มีความสามารถพิเศษนั่นคือกล้องอินฟาเรด ซึ่งก็จะมีราคาแพงขึ้นด้วย อีกทั้งยังไม่มีการทดสอบกับกล้องมากกว่า 1 ตัว

5.2.2 ระบบยังขาดการแจ้งเตือนหากกล้องแบบไอพีชำรุด หรือถูกทำลายจากผู้ไม่ประสงค์ดี อย่างทันท่วงที

5.2.3 ระบบยังไม่มีระบบการยืนยันการรับรู้จากผู้ใช้งาน เพื่อให้มั่นใจว่าทุกการแจ้งเตือนผู้ใช้งานสามารรับรู้ และสามารถดำเนินการในขั้นตอนต่อไปได้

5.3 ข้อเสนอแนะ

งานวิจัยนี้นำเสนอระบบแจ้งเตือนการบุกรุกด้วยเทคโนโลยี VoIP ซึ่งเป็นการนำเทคโนโลยี VoIP มาประยุกต์ใช้งานร่วมกับระบบรักษาความปลอดภัยด้วยกล้องวงจรปิดแบบไอพี โดยใช้ Asterisk มาเป็นศูนย์กลางการโทรแจ้งผู้ใช้งานผ่านทางระบบโทรศัพท์ไอพี และ Zoneminder เป็นศูนย์กลาง การตรวจจับการเคลื่อนไหว อีกทั้งผู้ใช้งานยังสามารถเข้าใช้งานระบบผ่านทางเว็บเพจ หรือโทรศัพท์มือถือ เมื่อตรวจพบการเคลื่อนไหว ระบบจะส่งเสียงเตือนด้วยคำพูดที่ได้บันทึกไว้ ณ ที่เกิดเหตุพร้อมทั้งส่งอีเมล์ และโทรแจ้งให้ผู้ใช้งานได้รับทราบโดยอัตโนมัติ ทำให้ผู้ใช้งานสามารถติดตามเหตุการณ์ที่เกิดขึ้นได้อย่างทันทีทันใด นอกจากนั้นผู้ใช้งาน

ยังสามารถใช้โทรศัพท์แบบไอพีโทรเข้ามาในระบบเพื่อส่งเสียงที่ต้องการ ณ ที่เกิดเหตุได้ จากการทดลองการทำงานของระบบ พบว่าในส่วนของการใช้งานฟังก์ชั่นต่างๆ ได้แก่ส่วนการใช้งานผ่านเว็บไซต์ของระบบ ส่วนของการใช้งานผ่านอุปกรณ์ VoIP และ Softphone ส่วนการใช้งานผ่านโทรศัพท์มือถือ และส่วนของการส่งเสียงเตือนในที่เกิดเหตุสามารถทำงานได้ดีตามขอบเขตที่กำหนดไว้ และสามารถนำไปใช้งานได้จริงในกรณีที่มีปริมาณแสงสว่างเพียงพอสำหรับการทำงานของกล้องวงจรปิดแบบไอพี เนื่องจากระบบยังมีข้อจำกัดดังกล่าว ผู้วิจัยจึงมีข้อเสนอแนะดังนี้

5.3.1 ในกรณีการทำงานในที่มืดอาจจำเป็นต้องมีการเปลี่ยนกล้องวงจรปิดที่สามารถตรวจจับการเคลื่อนไหวในบริเวณที่มืดได้ ในที่นี้ผู้วิจัยขอแนะนำให้ใช้กล้องไอพียี่ห้อ Foscam รุ่น FI8908W ซึ่งสามารถรองรับการตรวจจับการใช้งานในที่มืด และใช้งานร่วมกับ Zoneminder ได้ (Zoneminder, 2553, 20 มกราคม) และให้มีการทดสอบระบบกับกล้องมากกว่า 1 ตัว

5.3.2 เนื่องจากระบบยังขาดการแจ้งเตือนหากกล้องแบบไอพีชำรุด หรือถูกทำลายจากผู้ไม่ประสงค์ดี อย่างทันท่วงที ผู้วิจัยขอแนะนำให้พัฒนาระบบการแจ้งเตือนเมื่อกล้องเสียหายโดยให้ระบบทำการถ่ายภาพเป็นช่วงเวลา แล้วนำภาพที่ได้มาเปรียบเทียบคุณสมบัติต่างๆ เช่น ขนาดความจุของภาพ เพราะโดยปกติแล้วภาพที่ถ่ายได้ในบริเวณเดียวกันโดยส่วนมากจะ มีขนาดที่ไม่แตกต่างกันมากนัก แต่ถ้าหากมีความแตกต่างกันมาก ก็อาจแสดงว่ามีความผิดปกติ เกิดขึ้นกล้องอาจชำรุด ให้ระบบทำการแจ้งเตือนไปยังผู้ใช้งานในทันที โดยการโทรแจ้ง หรือส่งอีเมล์ถึงผู้ใช้งาน เป็นต้น

5.3.3 เนื่องจากระบบยังไม่มีระบบการยืนยันการรับรู้จากผู้ใช้งาน เพื่อให้มั่นใจว่าทุกการแจ้งเตือนผู้ใช้งานสามารรับรู้ และสามารถดำเนินการในขั้นตอนต่อไปได้ ผู้วิจัยขอแนะนำ ให้มีการยืนยันการรับรู้จากผู้ใช้งาน โดยให้ระบบโทรออกมากกว่า 1 ครั้ง ถ้าโทรครั้งแรกแล้วไม่รับสายให้เว้นระยะเวลา 1 นาทีแล้วโทรใหม่เป็นจำนวน 3 ครั้ง ถ้าครบ 3 ครั้งแล้วยังไม่รับ ให้โทรออกไปยังเบอร์ที่ 2 และถ้าหากยังไม่มีใครรับสายให้ทำการบันทึกสถานะภาพลงฐานข้อมูล ว่ายังไม่มีการยืนยันการรับรู้จากผู้ใช้งาน และทำการแจ้งเตือนผ่านทางอีเมล์ เป็นต้น

5.3.4 หากมีความต้องการให้ระบบสามารถ โทรออกไปยังชุมสายโทรศัพท์พื้นฐานที่ใช้กันโดยทั่วไป (PSTN) ก็มีความจำเป็นต้องจัดหาการ์ดสายนอก หรือแอสเทอริคการ์ด (Asterisk Card) มาทำการติดตั้งเพิ่มเติม

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

หนังสือ

กิตติพงษ์ สุวรรณราช. (2551). **การออกแบบและติดตั้งระบบโทรศัพท์ IP-PBX ด้วย Asterisk.** กรุงเทพฯ: ออฟเซ็ท เพรส.

อนุวัตร์ สมบุญ และบุญชัย งามวงศ์วัฒนา. (2552). **ระบบตรวจสอบและรายงานสภาพเว็บไซต์ผ่าน IVR.** กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

สารสนเทศจากสื่ออิเล็กทรอนิกส์

การจัดการAsterisk API. (2553). สืบค้นเมื่อ 15 เมษายน 2553, จาก **http://www.voipinfo.org/wiki-Asterisk+manager+API**

การจัดการAsterisk API. (2553). สืบค้นเมื่อ 27 มกราคม 2553, จาก **http://gotoknow.org/blog/patrickz/111965**

การใช้งาน Asterisk+FastAGI. (2553). สืบค้นเมื่อ 27 มกราคม 2553, จาก **http://www.voipinfo.org/wiki/index.php?page=Asterisk+FastAGI**

กล้องแบบไอพี Dlink. (2553). DCS-910. สืบค้นเมื่อ 1 ตุลาคม 2553, จาก **http://www.dlink.com/products/?pid=DCS-910**

ชมรมแอสเทอริค (Asteriskclub). (2553). สืบค้นเมื่อ 20 มกราคม 2553, จาก **http://www.asteriskclub.com/**

ฐานข้อมูล Mysql. (2553). สืบค้นเมื่อ 15 มีนาคม 2553, จาก **http://www.thaicert.org/paper/unix_linux/mysql.php**

ภาษาพีเอชพี. (2553). สืบค้นเมื่อ 15 มีนาคม 2553, จาก **http://th.wikipedia.org/wiki/ภาษาพีเอชพี**

ภาษาเอสคิวแอล (SQL). (2553). สืบค้นเมื่อ 15 มีนาคม 2553, จาก **http://www.hostsiam.com/Thaiversion/support/sql.doc**

ระบบโทรทัศน์วงจรปิด. (2553). สืบค้นเมื่อ 15 มีนาคม 2553, จาก **http://www.thaipresentation.com/technology/cctv/index.php**

สัญญาณกันขโมย แจ้งเหตุร้ายทางมือถือ. (2553). สืบค้นเมื่อ 20 สิงหาคม 2553, จาก **http://www.thaibestcctv.com/**

เอจีไอ(AGI-Asterisk Gateway Interface). (2553). สืบค้นเมื่อ 27 มกราคม 2553, จาก **http://gotoknow.org/blog/patrickz/111963**

แอสเทอริค (Asterisk). (2553). Asterisk. สืบค้นเมื่อ 20 มกราคม 2553, จาก **http://asterisk.org/support /features**

แอสเทอริค เอจีไอ (Asterisk AGI). (2553). 15 เมษายน 2553, จาก **http://www.voip-info.org/wiki-Asterisk+ AGI**

Mysql คือ อะไร. (2553). สืบค้นเมื่อ 15 ตุลาคม 2552, จาก **http://www.choosak.com/page-tag/mysql-คือ/**

VoIP. (2553). สืบค้นเมื่อ 15 มีนาคม 2553, จาก **http://www.ntc.or.th/uploadfiles/1150274715_5)VoIP%20rev2.pdf**

VoIP. (2553). สืบค้นเมื่อ 15 มีนาคม 2553, จาก **http://www.nectec.or.th/bid/mkt_info_tech_voip.htm**

Zoneminder. (2553). Zoneminder. สืบค้นเมื่อ 20 มกราคม 2553, จาก **http://www.zoneminder.com/**

3BB. (2553). บริการพี่ไฟล์แจ้งเหตุ. สืบค้นเมื่อ 1 พฤษภาคม 2553, จาก **http://filealert.3bb.co.th/product1.php**

ภาษาต่างประเทศ

ARTICLES

Ale Imran, Mohammed A Qadeer. (2009). "Conferencing, Paging**, Voice** Mailing via Asterisk EPBX**." International Conference on Computer Engineering and Technology**

Mohammed A Qadeer, Ale Imran. (2008). "Asterisk Voice Exchange : An Alternative to Conventional EPBX." **International Conference on Computer and Electrical Engineering**

Saurabh Goel, Vikash Garg, Prashant Ranjan, Satyanarayan Rao, Mahua Bhattacharya. (2009). "ASR System Integration with Asterisk for SIP or IAX Softphone clients." **Conference on International Association of Computer Science and Information Technology**

ประวัติผู้เขียน

ชื่อ-นามสกุล	ส.อ.สุบัน โสวาที
ประวัติการศึกษา	วิทยาศาสตรบัณฑิต สำนักเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่ฟ้าหลวง จ.เชียงราย
สถานที่ทำงานปัจจุบัน	กองพันปฏิบัติการสงครามอิเล็กทรอนิกส์ กรมการสื่อสารทหาร กองบัญชาการกองทัพไทย