ระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น

ปฐมพงศ์ ประไพย์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม คณะวิศวกรรมศาสตร์
มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2560

Fraud Detection System on Next Generation Network

Patompong Prapai

A Thesis Submitted in Partial Fulfillment of the Requirements

for the Degree of Master of Engineering

Department of Computer and Telecommunication Engineering

Faculty of Engineering, Dhurakij Pundit University

2016

ใบรับรองวิทยานิพนธ์

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

หัวข้อวิทยานิพนธ์ ระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น

เสนอโดย นายปฐมพงศ์ ประไพย์

สาขาวิชา วิศวกรรมคอมพิวเตอร์และโทรคมนาคม

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.เนื่องวงศ์ ทวยเจริญ

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบวิทยานิพนธ์แล้ว

.....ประธานกรรมการ

(อาจารย์ ดร.ประศาสน์ จันทราทิพย์)

.....กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์

(ผู้ช่วยศาสตราจารย์ ดร.เนื่องวงศ์ ทวยเจริญ)

..... กรรมการ

(อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์)

Kuetida Rojtanalai กรรมการ

(รองศาสตราจารย์ ดร.กุลธิดา โรจน์วิบูลย์ชัย)

วิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์รับรองแล้ว

..... คณบดีวิทยาลัยนวัตกรรมด้านเทคโนโลยีและวิศวกรรมศาสตร์

(ผู้ช่วยศาสตราจารย์ ดร.ณรงค์เดช กีรติพรานนท์)

วันที่ 18 เดือน ก.ค. พ.ศ. 2560

หัวข้อวิทยานิพนธ์	ระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น
ชื่อผู้เขียน	ปฐมพงศ์ ประไพย์
อาจารย์ที่ปรึกษา	ผศ.ดร. เนื่องวงศ์ ทวยเจริญ
สาขาวิชา	วิศวกรรมคอมพิวเตอร์และโทรคมนาคม
ปีการศึกษา	2559

บทคัดย่อ

งานวิจัยนี้นำเสนอตัวแบบในการตรวจจับการลักลอบใช้บริการโทรศัพท์บนโครงข่ายเอ็นจีเอ็น โดยใช้ตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียมมาประยุกต์ ในการออกแบบได้ใช้ตัวแบบนาอีฟเบย์เซียนสำหรับการคำนวณเพื่อเป็นข้อมูลนำเข้าให้กับตัวแบบโครงข่ายประสาทเทียม และได้ทำการปรับปรุงในส่วนของการตัดสินใจโดยอาศัยข้อมูลในอดีตของการเกิดการลักลอบใช้ในแต่ละเลขหมายประกอบ ในการทดลองได้ทำการนำข้อมูลการโทรของผู้ให้บริการรายหนึ่งตั้งแต่ปี ค.ศ. 2013 ถึงเดือนมิถุนายน ค.ศ. 2016 โดยในการฝึกหัดพบว่าจำนวนโหนดซ่อนของตัวแบบโครงข่ายประสาทเทียมที่เหมาะสมที่สุดคือ 4 โหนดและพบว่าสามารถตรวจจับการลักลอบใช้ได้ถูกต้อง 93.10 เปอร์เซ็นต์

Thesis Title	Fraud Detection System on Next Generation Network
Author	Patompong Prapai
Thesis Advisor	Asst.Prof. Nuengwong Tuaycharoen, Ph. D.
Department	Computer and Telecommunication Engineering
Academic Year	2016

ABSTRACT

This research focuses on developing of fraud detection model on Next Generation Network. The model was designed using Naïve Bayesian and Artificial Neural Network model. The Naïve Bayesian model is used to calculate the input data for the Artificial Neural Network model. The fraud decision model was improved by using each fraud numbering historical data. The experimental training and testing data set of one service provider is used from 2013 to June 2016. The appropriate hidden node of Artificial Neural Network on training step is 4 nodes with 93.10 percent accuracy on testing step.

กิตติกรรมประกาศ

วิทยานิพนธ์นี้สำเร็จลุล่วงไปได้ด้วยความกรุณาเป็นอย่างยิ่งจาก ผศ.ดร.เนื่องวงศ์ ทวยเจริญ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่คอยให้คำแนะนำ ตลอดจนเปิดโลกทรรศน์ในการค้นคว้าข้อมูลให้แก่ผู้วิจัย ขอขอบพระคุณอาจารย์ ดร.ประศาสน์ จันทราทิพย์ อาจารย์ ดร.ชัยพร เขมะภาตะพันธ์ และ รศ.ดร.กุลธิดา โรจน์วิบูลย์ชัย กรรมการสอบวิทยานิพนธ์ ซึ่งสละเวลามาเป็นกรรมการสอบวิทยานิพนธ์และได้ให้ข้อคิดเห็นที่เป็นประโยชน์ต่องานวิจัย นอกจากนี้ผู้วิจัยขอขอบพระคุณคณาจารย์ทุกๆ ท่านในคณะวิศวกรรมศาสตร์ ที่ได้ถ่ายทอดความรู้แก่ผู้วิจัยตลอดระยะเวลาการศึกษา

ผู้วิจัยขอขอบพระคุณ เจ้าหน้าที่ที่เกี่ยวข้องทุกท่าน ในคณะวิศวกรรมศาสตร์ ที่คอยให้ความช่วยเหลือ ตลอดจนแนะนำกระบวนการในการทำงานให้แก่ผู้วิจัยด้วยดีเสมอมา

ผู้วิจัยขอขอบคุณเพื่อนๆ ร่วมรุ่นทุกคน ที่ช่วยเหลือและให้กำลังใจกันเสมอมาตลอดระยะเวลาการศึกษา

ท้ายสุดนี้ ขอกราบขอบพระคุณ คุณพ่อ คุณแม่และครอบครัว ที่คอยเป็นกำลังใจและให้การสนับสนุนผู้วิจัยในทุกๆ ด้านเสมอมาจวบจนสำเร็จการศึกษา

ปฐมพงศ์ ประไพย์

สารบัญ

หน้า

บทคัดย่อภาษาไทย..... ฆ

บทคัดย่อภาษาอังกฤษ..... ง

กิตติกรรมประกาศ..... จ

สารบัญตาราง..... ซ

สารบัญภาพ..... ญ

บทที่

1. บทนำ..... 1

1.1 ที่มาและความเป็นมาของปัญหา..... 1

1.2 วัตถุประสงค์ของการศึกษา..... 3

1.3 ขอบเขตของการศึกษา..... 3

1.4 ประโยชน์ที่คาดว่าจะได้รับ..... 3

1.5 การทดสอบระบบ..... 3

1.6 วัสดุอุปกรณ์..... 4

1.7 แผนการดำเนินงาน..... 4

1.8 ความรู้ใหม่ที่ได้..... 5

1.9 การตอบรับการตีพิมพ์..... 5

1.10 โครงสร้างของรายงานส่วนที่เหลือ..... 5

2. แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง..... 6

2.1 ความรู้เกี่ยวกับการลักลอบใช้บริการโทรศัพท์บนโครงข่าย..... 6

2.2 การสื่อสารทางเสียงผ่านอินเทอร์เน็ต

(VoIP: Voice over Internet Protocal) 8

2.3 มาตรฐานโปรโตคอลของระบบวีไอพี..... 10

2.4 โครงข่ายยุคต่อไป (NGN : Next Generation Network) 13

2.5 ประเด็นเรื่องความมั่นคงบนโครงข่ายโทรคมนาคม VoIP..... 16

2.6 งานวิจัยที่เกี่ยวข้อง..... 20

สารบัญ (ต่อ)

บทที่	หน้า
3. การดำเนินงาน	27
3.1 ภาพรวมการทำงานของระบบ	27
3.2 การออกแบบระบบ	28
4. ผลการวิจัย	59
4.1 ตัวอย่างข้อมูลการเกิดการลักลอบใช้งานจริง	59
4.2 การทดลองตรวจจับตามเงื่อนไขที่กำหนด	61
4.3 การทดลองตรวจจับโดยตัวแบบที่ได้ทำการออกแบบและพัฒนา	63
4.4 การทดสอบระบบที่ทำการพัฒนาเพื่อใช้ตรวจจับการลักลอบ	80
5. สรุปผลการวิจัยและข้อเสนอแนะ	87
5.1 การวิเคราะห์ผลการทดลอง	87
5.2 สรุปผลการทดลอง	88
5.3 ข้อจำกัดของระบบ	89
5.4 ข้อเสนอแนะ	89
5.5 สรุป	90
บรรณานุกรม	91
ประวัติผู้เขียน	94

สารบัญตาราง

ตารางที่		หน้า
1.1	แผนการดำเนินงาน	5
2.1	ข้อความร้องขอของซิพและความหมาย	12
2.2	ข้อความตอบสนองของซิพและความหมาย	12
2.3	แสดงการเปรียบเทียบความสามารถของระบบแต่ละงานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์ที่นำเสนอ	25
3.1	อธิบายความหมายของข้อมูลนำเข้าโมดูลการประมวลผลข้อมูลเบื้องต้น	32
3.2	ประเภทของชุมสายที่กำหนดทั้งหมดบนโครงข่าย	32
3.3	รูปแบบในการคำนวณประเภทการโทร	33
3.4	การแทนค่าพารามิเตอร์สำหรับการโทรภายในโครงข่ายเดียวกัน	33
3.5	การแทนค่าพารามิเตอร์สำหรับการโทรนอกโครงข่ายภายในประเทศ	34
3.6	การแทนค่าพารามิเตอร์สำหรับการโทรนอกโครงข่ายระหว่างประเทศ	35
3.7	ข้อมูลส่งออกสำหรับส่วนของตัวแบบนาอีฟเบย์เซียน	36
3.8	รายละเอียดแต่ละแอททริบิวท์ของตาราง CDR	46
3.9	รายละเอียดแต่ละแอททริบิวท์ของตาราง preProcessData	47
3.10	รายละเอียดแต่ละแอททริบิวท์ของตาราง weightBeforeHiddenData	48
3.11	รายละเอียดแต่ละแอททริบิวท์ของตาราง weightAfterHiddenData	48
3.12	รายละเอียดของตารางข้อมูล Prefix	49
3.13	รายละเอียดของตารางข้อมูล Country	49
3.14	รายละเอียดของตารางข้อมูล Fraud	50
3.15	รายละเอียดของตารางข้อมูล fraudStatus	50
3.16	รายละเอียดของตารางข้อมูล fraudBoard	51
3.17	รายละเอียดของตารางข้อมูล fraudWhiteList	51
4.1	ผลการทดสอบของระบบตรวจจับการลักลอบใช้งานในปริมาณข้อมูลที่แตกต่างกัน	61
4.2	ผลการทดสอบความถูกต้องของระบบตรวจจับการลักลอบใช้งาน	62
4.3	ผลการทดลองโดยใช้ตัวแบบนาอีฟย์เบย์เซียน	64

สารบัญตาราง (ต่อ)

ตารางที่ **หน้า**

4.4 ผลการทดลองโดยใช้ตัวแบบโครงข่ายประสาทเทียม..... 66
4.5 ค่าเฉลี่ยความถูกต้องในการตรวจจับแยกตามจำนวนโหนดซ่อน..... 72
4.6 ผลการทดลองโดยประยุกต์ตัวแบบนาอีฟย์เบย์เซียน
และโครงข่ายประสาทเทียมรวมถึงการนำไวท์ลิสต์มาประยุกต์..... 73
4.7 ค่าเฉลี่ยความถูกต้องในการตรวจจับแยกตามจำนวนโหนดซ่อน..... 79
5.1 สรุปผลการทดสอบตามขอบเขตของงานวิจัย..... 89

สารบัญภาพ

ภาพที่ **หน้า**

1.1 วิธีการลักลอบโดยแบ่งปันรายได้จากการโทรระหว่างประเทศ..... 1
2.1 เปรียบเทียบโมเดลโอเอสไอกับเทคโนโลยีวีโอไอพี..... 9
2.2 การสื่อสารทางโทรศัพท์แบบปกติ..... 9
2.3 การสื่อสารทางโทรศัพท์ผ่านอินเทอร์เน็ต..... 10
2.4 ตัวอย่างการติดต่อสื่อสารในรูปแบบจุดต่อจุดของโปรโตคอลซิพ..... 13
2.5 โครงสร้างพื้นฐานของโครงข่ายโทรคมนาคม NGN..... 14
2.6 องค์ประกอบของโครงข่ายโทรคมนาคม NGN..... 15
2.7 สถาปัตยกรรมโครงข่ายประสาทเทียม..... 21
2.8 เปรียบเทียบจำนวนโหนดซ่อนและประสิทธิภาพ
ในการตรวจจับได้บนโครงข่ายประสาทเทียม..... 21
2.9 โครงสร้างของระบบป้องกันการลักลอบใช้บนพื้นฐาน
ของการจำแนกแบบนาอีฟและเบย์เซียน..... 23
2.10 การไหลของข้อมูลภายในระบบ STR..... 23
2.11 แผนภาพโครงสร้างต้นไม้การตัดสินใจ..... 24
3.1 แผนภาพโครงข่ายระบบตรวจจับการลักลอบใช้บริการ
บนโครงข่ายเอ็นจีเอ็น..... 27
3.2 แผนภาพตัวแบบที่ทำการออกแบบในการวิเคราะห์แนวโน้ม
โอกาสที่จะเกิดการลักลอบใช้..... 30
3.3 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูล
การประมวลผลข้อมูลเบื้องต้น..... 31
3.4 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูลตัวแบบนาอีฟเบย์เซียน..... 36
3.5 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูล
ตัวแบบโครงข่ายประสาทเทียม..... 43
3.6 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูล
ตัวแบบโครงข่ายประสาทเทียม..... 44
3.7 ส่วนของโมดูลการตัดสินใจ..... 45

สารบัญภาพ (ต่อ)

ภาพที่ **หน้า**

3.8 ผังการทำงานส่วนของการประมวลผลข้อมูลและวิเคราะห์ข้อมูล..... 52
3.9 แผนภาพลำดับการทำงานในส่วนของผู้ใช้ระบบ..... 53
3.10 หน้า Login ใช้สำหรับให้เจ้าหน้าที่เข้าสู่ระบบ..... 54
3.11 หน้า Dashboard แสดงรายละเอียดการแจ้งเตือนต่างๆ..... 54
3.12 หน้า Webboard ใช้สำหรับให้เจ้าหน้าที่สามารถแลกเปลี่ยนพูดคุย..... 55
3.13 หน้า Search ใช้สำหรับค้นหาข้อมูลที่ตรวจจับได้บนระบบ..... 55
3.14 หน้า Config เป็นการปรับแต่งค่าที่เกี่ยวข้อง..... 56
3.15 หน้า Help เป็นหน้าที่รวบรวมเนื้อหาต่างๆเกี่ยวกับการใช้งานระบบ..... 56
3.16 หน้า Tools เป็นการรวบรวมเครื่องมือต่างๆ..... 57
3.17 หน้า Contact Us ใช้สำหรับติดต่อผู้พัฒนาระบบ
กรณีมีข้อขัดข้องทางเทคนิคของเว็บ..... 57
4.1 รายละเอียดตัวอย่างการลักลอบโทรไปยังประเทศกลุ่มเสี่ยงหลากหลาย..... 59
4.2 รายละเอียดตัวอย่างการลักลอบโทรด้วยค่าโทรที่สูงผิดปกติ..... 60
4.3 รายละเอียดตัวอย่างการลักลอบโทรไปกลุ่มเดิมซ้ำๆ หลากหลาย..... 60
4.4 กราฟแสดงค่าความต่างของเวลาที่ตรวจจับได้กับเวลาจริง
โดยเฉลี่ยของข้อมูลแต่ละขนาด..... 61
4.5 กราฟความสัมพันธ์ระหว่างจำนวนโหนดซ่อนและ
% ความถูกต้องของแต่ละวิธี..... 80
4.6 การเข้าสู่ระบบ (1)..... 80
4.7 การเข้าสู่ระบบ (2)..... 81
4.8 การค้นหาข้อมูลการเกิดการลักลอบ..... 81
4.9 การเข้าดูรายการข้อมูลบน Webboard..... 82
4.10 การเข้าปรับแต่งข้อมูล Config..... 82
4.11 การเข้าดูรายการข้อมูลเครื่องมือ..... 83
4.12 การเข้าดูรายการข้อมูลช่วยเหลือ..... 83
4.13 การเข้าดูรายการติดต่อผู้ดูแลระบบ..... 84

สารบัญภาพ (ต่อ)

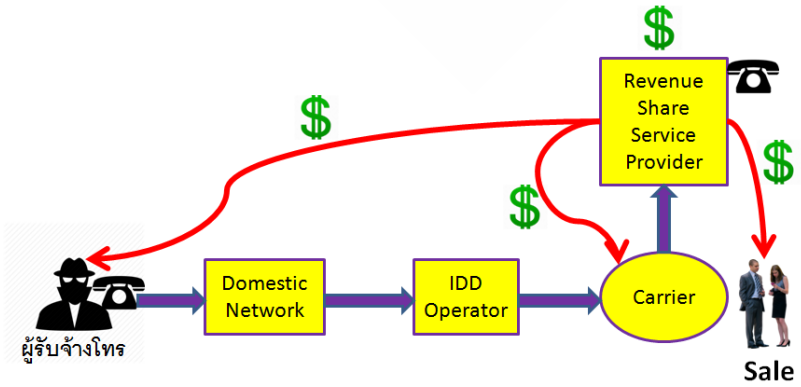
ภาพที่ **หน้า**

4.14 การทดสอบการเข้าใช้งานผ่าน Google Chrome..... 84
4.15 การทดสอบการเข้าใช้งานผ่าน Mozilla Firefox..... 85
4.16 การทดสอบการเข้าใช้งานผ่าน Internet Explorer..... 85
4.17 การทดสอบการเข้าใช้งานผ่าน Smart Phone ด้วย Safari..... 86

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ระบบตรวจจับการลักลอบใช้บริการนับเป็นส่วนหนึ่งที่ผู้ให้บริการควรตระหนักถึงความสำคัญเป็นอย่างมาก ในปัจจุบันมีการพัฒนาระบบตรวจจับในหลากหลายแขนงเพื่อป้องกันความสูญเสียที่เกิดขึ้น ในระบบการให้บริการทางโทรคมนาคมก็เช่นกัน ได้มีการพัฒนามาใช้โครงข่ายผ่านอินเทอร์เน็ตโปรโตคอล ทำให้ผู้ใช้งานสามารถโทรได้ในราคาประหยัดช่วยลดต้นทุนให้องค์กร แต่เนื่องด้วยเทคโนโลยีดังกล่าวอยู่บนโลกของอินเทอร์เน็ต ทำให้ประเด็นเรื่องความปลอดภัยนับเป็นปัจจัยหนึ่งที่ทางผู้ให้บริการและผู้รับบริการต้องพิจารณา สมาคมควบคุมการลักลอบใช้บริการด้านการสื่อสาร (CFCA: Communications Fraud Control Association) กล่าวว่าในปีค.ศ. 2015 ประมาณการรายได้ทั่วโลกด้านการสื่อสารประมาณ 2.25 ล้านล้านเหรียญสหรัฐ[1] โดยประมาณการการสูญเสียรายได้จากการให้บริการเนื่องจากการลักลอบใช้ประมาณ 38.1 พันล้านเหรียญสหรัฐ ซึ่งเปอร์เซ็นต์ความสูญเสียอยู่ที่ 1.69% ซึ่งลดลงจากปี 2005 ที่มีเปอร์เซ็นต์ความสูญเสียมากถึง 5% แต่ก็นับเป็นปริมาณความสูญเสียที่ค่อนข้างมาก นอกจากนี้แล้วยังพบว่าประเภทของการลักลอบที่มากที่สุดคือวิธีการลักลอบโดยแบ่งปันรายได้จากการโทรระหว่างประเทศ (IRSF: International Revenue Share Fraud) ซึ่งมีประมาณ 10.76 พันล้านบาท โดยลักษณะดังกล่าวดังภาพที่ 1.1



ภาพที่ 1.1 วิธีการลักลอบโดยแบ่งปันรายได้จากการโทรระหว่างประเทศ

[1] สมาคมควบคุมการลักลอบใช้บริการด้านการสื่อสาร (CFCA: Communications Fraud Control Association) (2558). 2015 Global Fraud Lost Survey.

โดยเริ่มจากพนักงานขายของ Carrier ทำการตกลงในเรื่องส่วนแบ่งกับทางผู้ให้บริการในประเทศนั้นๆในการเป็นตัวแทนนำการโทร (Call Traffic) ลงและจัดทำข้อเสนอในด้านราคาให้กับผู้ให้บริการโทรระหว่างประเทศของประเทศต้นทาง (IDD Operator) ซึ่งตามข้อตกลงเมื่อมีการโทรจากต้นทางไปยังประเทศปลายทาง จะต้องมีค่าส่วนแบ่ง (IC: Inter-Connection) จากนั้นก็เป็นหน้าที่ของ Carrier ที่ไปประกาศหาคนที่จะดำเนินการโทรเข้ามาซึ่งใช้ค่าส่วนแบ่งในการชักจูง โดยคนที่โทรเข้ามาอาจเป็นผู้ลักลอบใช้ที่ได้บัญชีผู้ใช้ของลูกค้าจริงไปทำการลงทะเบียนและทำการโทรโดยใช้คนโทรหรือใช้เครื่องแม่ข่ายเพื่อโทรแบบอัตโนมัติ สมมติว่าทุกๆการโทร 1 นาทีจะต้องเสียค่าส่วนแบ่ง 10 บาท ดังนั้นหากมีการโทรทั้งหมด 1 ล้านนาที ประเทศต้นทางต้องเสียค่าส่วนแบ่งจำนวน 10 ล้านบาท ซึ่งพอไปเก็บค่าโทรจากลูกค้าจริงที่ใช้เลขหมายนั้นก็จะถูกปฏิเสธการจ่ายเงินเนื่องจากไม่ได้ทำการโทรเอง โดยอ้างว่าถูกลักลอบใช้บัญชีเลขหมายนั้น ซึ่งจะส่งผลให้ผู้ให้บริการจากประเทศต้นทางต้องสูญเสียรายได้โดยที่ไม่สามารถไปเก็บค่าบริการจากลูกค้าได้ โดยเงินที่สูญไปนั้นผู้ที่ได้รับประโยชน์ได้แก่ Carrier, Revenue Share Service Provider, Sale และผู้รับจ้างโทร

ในการป้องกันปัญหาดังกล่าวโดยทั่วไปจะใช้อุปกรณ์รักษาความปลอดภัยหลักๆ เช่น ไฟล์วอล (Firewall) ไอดีเอส (IDS: Intrusion Detection System) ไอพีเอส (IPS: Intrusion Prevention System) ซึ่งก็ช่วยป้องกันได้ในระดับหนึ่ง แต่ก็ไม่สามารถป้องกันได้บางกรณีที่ทางผู้ให้บริการต้องการ นอกจากนี้แล้วยังมีการนำระบบการป้องกันการลักลอบใช้บริการมาใช้งานซึ่งเป็นระบบเก่าใช้งานมานาน รวมถึงไม่รองรับกับเทคโนโลยีที่เป็นไอพี โดยซอฟต์แวร์ที่ใช้ตรวจจับส่วนมากจะนำเข้าจากต่างประเทศ ซึ่งมีต้นทุนที่ค่อนข้างสูงกอปรกับมีความสามารถไม่ตรงตามที่ผู้ให้บริการโทรคมนาคมต้องการ

เพื่อแก้ปัญหาดังกล่าวจึงจำเป็นต้องมีซอฟต์แวร์ที่ช่วยในการป้องกันการลักลอบใช้งานโดยดูจากพฤติกรรมการใช้งาน รวมถึงเงื่อนไขและกฎเกณฑ์ต่างๆ ที่ทางชุมสายโทรศัพท์เป็นผู้กำหนด ในงานวิจัยนี้ได้กำหนดเงื่อนไขที่จะศึกษาและพัฒนา ได้แก่ การใช้งานเป็นเวลานานจนเกิดผิดสังเกต การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด การมีพฤติกรรมการโทรแปลกๆ โดยมีการเข้ามาลักษณะตรวจสอบโครงข่ายแล้วกระหน่ำโทร ซึ่งพฤติกรรมเหล่านี้หากตรวจจับได้รวดเร็วจะช่วยป้องกันการสูญเสียรายได้ของผู้ให้บริการ

ดังนั้นเราจึงได้ทำการพัฒนาระบบการตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็นขึ้น โดยจะนำมาตรวจจับลักษณะพฤติกรรมการลักลอบใช้ตามที่ได้กล่าวข้างต้นรวมถึงได้นำตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียมมาประยุกต์ โดยระบบสามารถแจ้งเตือนให้กับผู้ใช้ผ่านเว็บบราวเซอร์ว่ามีลักษณะพฤติกรรมการลักลอบใช้เกิดขึ้น เพื่อให้ทางผู้ใช้สามารถ

ทำการตรวจสอบ หากเป็นการลักลอบใช้งานจริงก็จะทำการบล็อกเลขหมายดังกล่าวไม่ให้ใช้งานชั่วคราวทำให้ช่วยป้องกันการสูญเสียรายได้อันเนื่องมาจากการลักลอบใช้บริการได้

1.2 วัตถุประสงค์

1. เพื่อศึกษาและพัฒนาขั้นตอนวิธีในการตรวจจับการลักลอบใช้งานบนโครงข่ายเอ็นจีเอ็น
2. เพื่อพัฒนาระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น

1.3 ขอบเขต

ขอบเขตการศึกษาในการวิจัยครั้งนี้ ผู้ศึกษาจะศึกษาถึงพฤติกรรมต่างๆและพัฒนาระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น โดยขอบเขตพฤติกรรมที่ต้องการศึกษาได้แก่

การใช้งานเป็นเวลานานจนเกิดผิดสังเกต

การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง

การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด

การมีพฤติกรรมตรวจสอบโครงข่ายแล้วกระหน่ำโทร

นอกจากข้างต้นยังมีส่วนของการพัฒนาโมเดลการตรวจจับโดยใช้เทคนิคที่เกี่ยวข้องได้แก่ การใช้ตัวแบบโครงข่ายประสาทเทียม ตัวแบบนาอีฟเบย์เซียน เป็นต้น โดยซอฟต์แวร์ที่ได้จะสามารถแจ้งเตือนผ่านเว็บบราวเซอร์หากมีลักษณะพฤติกรรมที่คาดว่าจะเป็นการลักลอบใช้บริการเกิดขึ้น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้ความรู้ในเรื่องลักษณะพฤติกรรมการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น
2. ได้ตัวแบบที่เหมาะสมสำหรับการนำไปประยุกต์กับระบบตรวจจับการลักลอบใช้บริการโทรศัพท์ บนโครงข่ายเอ็นจีเอ็น
3. ได้ระบบตรวจจับการลักลอบการใช้บริการบนโครงข่ายเอ็นจีเอ็นตามเงื่อนไขและตัวแบบที่กำหนด

1.5 การทดสอบระบบ

ในการทดสอบระบบจะทำการทดสอบในแง่ของประสิทธิภาพทางเวลาในการประมวลผลและความถูกต้องของการตรวจจับได้ของระบบ โดยในการทดสอบจะเริ่มจากการใช้ชุดข้อมูลในการฝึกสอนโดยเป็นข้อมูลตั้งแต่เดือนมกราคม ปี พ.ศ. 2556 ถึงเดือนธันวาคม ปี พ.ศ. 2557

ในการทดสอบจะใช้ชุดข้อมูลตั้งแต่เดือน มกราคม ปี พ.ศ. 2558 ถึงเดือนมิถุนายน ปี พ.ศ. 2559 โดยทำการฝึกสอนเพื่อให้ได้ค่าน้ำหนักและจำนวนโหนดที่เหมาะสมสำหรับตัวแบบโครงข่ายประสาทเทียม จากนั้นทำการทดสอบโดยเปรียบเทียบผลที่ได้กับความเป็นจริงที่เกิดขึ้นจากการเกิดการลักลอบใช้งานจริงคิดเป็นเปอร์เซ็นต์ความถูกต้องที่ตรวจจับได้

1.6 วัสดุอุปกรณ์

1. ฮาร์ดแวร์ (Hardware)

1) เครื่องแม่ข่ายสำหรับจัดเก็บข้อมูลการโทร (CDR Server: Call Detail Record Server)

2) เครื่องแม่ข่าย (Server) ใช้สำหรับการประมวลผลข้อมูลการโทร และเป็นเครื่องให้บริการเว็บ (Web Server)

3) สวิตซ์ (Switch) ใช้สำหรับการเชื่อมโยงโครงข่ายในแต่ละส่วน

4) คอมพิวเตอร์ส่วนบุคคล (Personal Computer) ใช้สำหรับการทดสอบการทำงาน

2. ซอฟต์แวร์ (Software)

1) เน็ตบีนส์ ไอดีอี เวอร์ชัน 8.0.2 (Netbeans IDE 8.0.2) ใช้สำหรับวิเคราะห์และประมวลผลข้อมูลการเกิดการลักลอบ โดยใช้ภาษา JAVA ในการพัฒนา

2) โค้ดล็อบสเตอร์ (Code Lobster) ใช้สำหรับเขียนโปรแกรมภาษา PHP และ HTML เพื่อพัฒนาระบบในส่วนของเว็บ

3) แอพเซิร์ฟ เวอร์ชัน 2.5.9 (AppServ 2.5.9) ใช้สำหรับเป็นซอฟต์แวร์สำหรับเว็บเซิร์ฟเวอร์ ซึ่งประกอบด้วยตัวอะพาเชร์ (Apache) พีเอ็ชพี (PHP) มายเอสคิวแอล (MySQL)

4) ไมโครซอฟต์วิชวลสตูดิโอ เวอร์ชัน 2015 คอมมิวนิตี้ (Microsoft Visual Studio 2015 Community Edition) ใช้สำหรับประมวลผลข้อมูลในขั้นตอนการทำการประมวลผลข้อมูลเบื้องต้น โดยใช้ภาษา C# ในการพัฒนา

5) ไมโครซอฟต์เอสคิวแอลเซิร์ฟเวอร์ 2008 อาร์ 2 (Microsoft SQL Server 2008R2) ใช้สำหรับจัดเก็บข้อมูลที่ได้หลังจากขั้นตอนการทำการประมวลผลข้อมูลเบื้องต้น

1.7 แผนการดำเนินงาน

ในการดำเนินการวิจัยได้ตั้งแผนดำเนินการดังตารางที่ 1.1

ตารางที่ 1.1 แผนการดำเนินงาน

รายการดำเนินงาน	ระยะเวลา (เดือน)						
	1	2	3	4	5	6	7
1. ศึกษาค้นคว้าและรวบรวมข้อมูล							
2. ออกแบบภาพรวมของระบบ							
3. เขียนโปรแกรมตัวประมวลผลข้อมูลที่ได้จากเครื่องแม่ข่ายสำหรับจัดเก็บข้อมูลการโทร							
4. เขียนโปรแกรมส่วนวิเคราะห์และแสดงผลบนเว็บ							
5. ทดสอบระบบ							
6. วิเคราะห์ข้อมูลและปรับปรุงแก้ไข							
7. สรุปการดำเนินงานและจัดทำรูปเล่ม							

1.8 ความรู้ใหม่ที่ได้

1. ความรู้ในเรื่องของลักษณะพฤติกรรมการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น
2. การพัฒนาซอฟต์แวร์ที่นำไปใช้กับระบบการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น

1.9 การตอบรับการตีพิมพ์

งานวิจัยนี้ได้รับการตอบรับให้ตีพิมพ์โดยมีรายละเอียดดังนี้

1) หัวข้อ “ระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น” การประชุมวิชาการงานวิจัย และพัฒนาเชิงประยุกต์ ครั้งที่ 5 (ECTI-CARD 2013) ปี พ.ศ. 2556 หน้า 405-410.

2) หัวข้อ “การพัฒนาตัวแบบตรวจจับการลักลอบใช้บริการโทรศัพท์ บนโครงข่ายเอ็นจีเอ็น” โครงการประชุมวิชาการระดับนานาชาติและระดับชาติด้านเทคโนโลยีคอมพิวเตอร์และระบบสารสนเทศประยุกต์ครั้งที่ 11 และการประชุมวิชาการ ระดับชาติด้านบริหารธุรกิจ 2017-1 (ACTIS & NCOBA) ปี พ.ศ. 2560 หน้า 192-197.

1.10 โครงสร้างของรายงานส่วนที่เหลือ

บทที่ 2 กล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง

บทที่ 3 กล่าวถึงการออกแบบระบบ

บทที่ 4 กล่าวถึงการทดลองที่จะใช้ในวิทยานิพนธ์

บทที่ 5 กล่าวถึงบทสรุปของงานที่จะใช้ในวิทยานิพนธ์นี้

บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

การวิจัยเรื่องระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น จำเป็นที่จะต้องศึกษาตั้งแต่ ความรู้ทั่วไปเกี่ยวกับการลักลอบใช้บริการโทรศัพท์บนโครงข่ายการสื่อสารทางเสียงผ่านอินเทอร์เน็ต การสื่อสารทางเสียงผ่านอินเทอร์เน็ต โพรโตคอลซิพ ลักษณะของโครงข่ายเอ็นจีเอ็น ลักษณะพฤติกรรมการลักลอบใช้บนโครงข่ายไอพี รวมถึงงานวิจัยที่เกี่ยวข้อง ในบทนี้จะกล่าวถึงประเด็นที่สำคัญโดยมีรายละเอียดดังนี้

2.1 ความรู้ทั่วไปเกี่ยวกับการลักลอบใช้บริการโทรศัพท์บนโครงข่ายการสื่อสารทางเสียงผ่านอินเทอร์เน็ต

Abdallah และคณะ [11] ได้ให้คำจำกัดความของคำว่าการลักลอบใช้ว่าเป็นการใช้โอกาสเพื่อเจตนาใช้ในทางที่ผิดหรือการใช้ทรัพยากรหรือทรัพย์สินขององค์กรที่ไม่เหมาะสม การสื่อสารทางเสียงผ่านอินเทอร์เน็ตก็เป็นเทคโนโลยีแขนงหนึ่งซึ่งมักมีประเด็นเรื่องความปลอยภัยในการใช้บริการมาเกี่ยวข้อง เนื่องจากระบบโทรศัพท์ผ่านโครงข่ายอินเทอร์เน็ตสามารถเชื่อมต่อได้ทั่วโลก นั่นคือเพียงแค่มีอุปกรณ์ เช่น โทรศัพท์ที่รองรับอินเทอร์เน็ตโปรโตคอล ซอฟต์โฟนที่ติดตั้งผ่านโทรศัพท์มือถือ เป็นต้น โดยใช้เพียงเลขหมายและรหัสผ่านก็สามารถเข้าใช้ระบบได้แล้ว ดังนั้นการรักษารหัสผ่านหรือการป้องกันไม่ให้ผู้ไม่หวังดีเข้ามาโจมตีเพื่อได้มาซึ่งการยึดครองอุปกรณ์เพื่อใช้งานนั้นนับเป็นสิ่งสำคัญที่ผู้ใช้งานควรตระหนักถึง รวมถึงผู้ให้บริการเองก็ควรให้ความสำคัญเพื่อป้องกันความสูญเสียที่เกิดขึ้น โดยตัวอย่างลักษณะของการได้มาซึ่งการลักลอบใช้มีรายละเอียดดังนี้

2.1.1 การลักลอบใช้โดยการได้มาซึ่งข้อมูลการเข้าใช้งานเลขหมาย

การลักลอบใช้โดยการได้มาซึ่งข้อมูลการเข้าใช้งานเลขหมายเป็นวิธีการหนึ่งที่ง่ายที่สุด หากผู้ที่ถือครองเลขหมายไม่รักษาความปลอดภัยในการใช้งาน เช่น ไม่เก็บรหัสผ่านไว้ในที่ปลอดภัย หรือมีคนที่ทราบรหัสผ่านดังกล่าวหลายคน หากมีการนำไปลงทะเบียนเพื่อเข้าใช้งานเลขหมายก็จะไม่ทราบว่าใครเป็นผู้ใช้งานจริง ซึ่งสิ่งที่จะทราบได้หลักคือ ไอพีต้นทาง อุปกรณ์ที่ใช้งาน เบอร์ปลายทางที่ติดต่อ เป็นต้น ซึ่งหากเจ้าของเลขหมายปฏิเสธการใช้งานดังกล่าวก็จำเป็นต้องไปทำการตรวจสอบว่าเจ้าของเลขหมายไม่ได้ใช้งานจริงหรือไม่ หากพบว่าโดนนำไปลักลอบใช้งาน

ก็จะทำให้เจ้าของเลขหมายมีสิทธิ์ปฏิเสธที่จะชำระค่าบริการได้ ทำให้ฝั่งของผู้ให้บริการสูญเสียรายได้จากการให้บริการได้ นอกจากนี้แล้วในกรณีลูกค้าที่นำไปใช้ในลักษณะเป็นตู้สาขา (Hosted PBX) [10],[14] ลักษณะที่ถูกลักลอบหนึ่งในวิธีนี้คือการสแกนวิธีการเชื่อมต่อ [6] เช่น ทำการสุ่มว่ามีการกำหนดเบอร์ต่อ (Extension Number) ไว้เป็นเบอร์ใดบ้าง โดยวิธีการนี้จะดูที่ผลตอบกลับข้อความซิพ (SIP Message Response) โดยหากพบว่าการตอบกลับทีค่าเป็น 403 Forbidden ก็จะทราบได้ว่าเบอร์ต่อที่ทำการสุ่มลงทะเบียนเข้าไปนั้นมีตัวตนอยู่จริงแต่รหัสผ่านที่ส่งเข้าไปยังผิดอยู่ ซึ่งในขั้นตอนต่อไปของผู้ลักลอบใช้คือการกวาดหารหัสผ่านที่ถูกต้องเพื่อนำไปใช้งาน เป็นต้น โดยการป้องกันเบื้องต้นจะมุ่งไปที่การเปิดให้ผู้ใช้เรียกได้จำกัด [13] เช่น เรียกได้บางประเทศที่ใช้งานบ่อย แลพิจารณาเปิดให้เป็นรายครั้งไป หรือการกำหนดเครดิตในการใช้งาน เป็นต้น

2.1.2 การลักลอบใช้โดยการได้มาซึ่งการยึดครองเครื่องแม่ข่ายที่ให้บริการโทรศัพท์

การยึดครองเครื่องแม่ข่ายที่ให้บริการมักเกิดขึ้นกรณีที่ผู้ใช้งานเป็นลักษณะของผู้ให้บริการแบบขายส่ง (Wholesale) โดยเป็นการส่งผ่านการจราจร (Traffic) ไปยังผู้ให้บริการ (Service Provider) ซึ่งส่วนของผู้ให้บริการเองจะเปิดให้ลูกค้ารายดังกล่าวสามารถส่งต่อปริมาณการจราจรเป็นจำนวนมาก ดังนั้นการยึดครองจะทำได้เมื่อสามารถหาช่องโหว่ของระบบ [12] เช่น การเปิดพอร์ตที่ไม่จำเป็นต่อการใช้งาน ทำให้ผู้ลักลอบใช้ช่องโหว่ดังกล่าวเข้ามายังระบบได้ โดยหากเข้าถึงข้อมูลการปรับแต่ง (Configuration) ก็สามารถปรับแต่งให้รับข้อมูลการโทรจากที่อื่นเพื่อส่งผ่านเครื่องแม่ข่ายนี้ไปยังผู้ให้บริการได้

2.1.3 การลักลอบใช้โดยการปรับแต่งค่าจากอุปกรณ์ต้นทาง

การลักลอบใช้โดยการปรับแต่งค่าจากอุปกรณ์ต้นทาง เช่น การปรับเปลี่ยน (Modify) การส่งเลขหมายต้นทาง (Caller ID) ซึ่งหากผู้ให้บริการไม่ได้มีการป้องกันการเปลี่ยนเลขหมายต้นทาง เมื่อมีการส่งข้อมูลเลขหมายต้นทางที่เปลี่ยนไป จะไม่สามารถไปเรียกเก็บค่าบริการจากลูกค้ารายนั้นได้ เช่น ลูกค้าใช้เลขหมาย 021050000 เมื่อมีการโทรออกก็เปลี่ยนเป็นเลขหมาย 999999999 เมื่อมีการเรียกเก็บเงินก็จะพบว่าเลขหมายดังกล่าวไม่มีอยู่บนระบบจริงจะไม่สามารถไปเรียกเก็บค่าบริการได้ ในการป้องกันจำเป็นที่จะต้องแก้ไขที่ระบบผู้ให้บริการโดยการป้องกันการเปลี่ยนเลขหมายต้นทางรวมถึงการสกรีนเลขหมายก่อนการส่งต่อไปยังปลายทาง

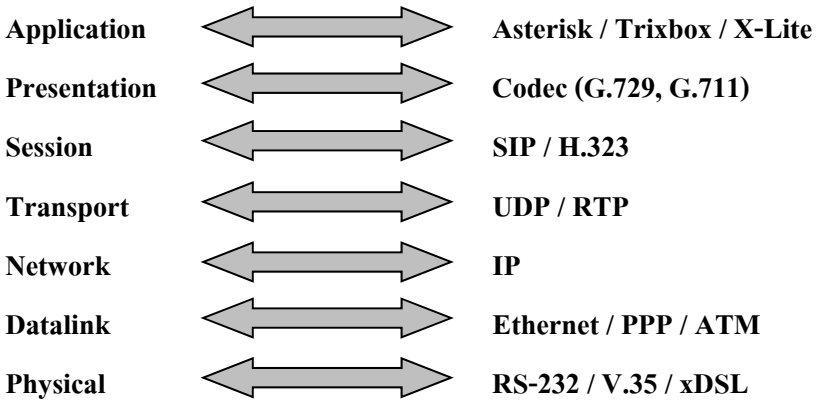
2.1.4 การลักลอบใช้โดยการใช้ช่องโหว่ของระบบให้บริการโทรศัพท์

ช่องโหว่ของระบบการให้บริการจะเกิดขึ้นเมื่อผู้ให้บริการไม่ได้ป้องกันกรณีการตรวจสอบเลขหมายอย่างครอบคลุม เช่น กรณีที่มีการเรียกออกไปยังต่างประเทศ ด้วยรหัส 00x เมื่อผู้ใช้พบช่องโหว่ว่าหากต้องการเรียกไปยังต่างประเทศ เรียกโดยการกด 660x ตามด้วยเบอร์ปลายทางต่างประเทศ แทนที่จะกด 00x เมื่อส่งต่อเข้าไปยังชุมสาย จะมีการแปลง 66 ซึ่งเป็นรหัส

ประเทศไทยเป็น 0 ซึ่งจะมองว่าผู้ใช้งานต้องการกดไปยังเลขหมายปลายทางต่างประเทศ แต่เมื่อไปเข้าสู่กระบวนการประมวลผลการคิดค่าบริการจะเห็นว่าเลขหมายปลายทางของลูกค้าเป็น 660x ซึ่งมองว่าเป็นเลขหมายปลายทางในประเทศ จะทำให้คิดค่าบริการผิด เช่น ค่าโทรไปต่างประเทศของเลขหมายนั้นเป็น 2 บาทต่อนาที แต่พอไปคิดเงินจริงเป็น 0.50 บาทต่อนาที หากค่าการเชื่อมต่อระหว่างโครงข่าย (Inter-Connection) ที่ได้ตกลงกับปลายทางไว้เป็น 1 บาทต่อนาที จะทำให้ผู้ให้บริการต้องจ่ายค่าการเชื่อมต่อระหว่างโครงข่ายเพิ่ม

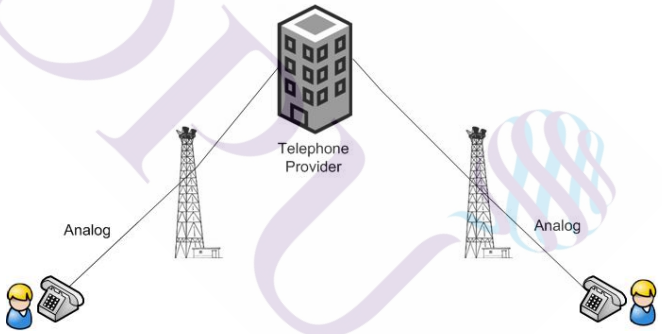
2.2 การสื่อสารทางเสียงผ่านอินเทอร์เน็ต (VoIP: Voice over Internet Protocol) [1]

การสื่อสารทางเสียงผ่านอินเทอร์เน็ตหรือที่เรียกว่าโทรศัพท์ระบบวีโอไอพี (VoIP: Voice over Internet Protocol) เป็นเทคโนโลยีที่เราสามารถรับส่งสัญญาณเสียงผ่านทางเครือข่ายอินเทอร์เน็ตหรืออินทราเน็ตได้ เทคโนโลยีวีโอไอพีนี้ถูกคิดค้นขึ้นโดยองค์กรอาร์พาเน็ต (ARPANET: Advanced Research Projects Agency Network) เมื่อปี ค.ศ. 1973 เพื่อช่วยประหยัดต้นทุนและใช้งานโครงข่ายให้มีประสิทธิภาพมากยิ่งขึ้น การทำงานของระบบวีโอไอพีนั้นจะมีการแปลงสัญญาณเสียงจากต้นทางให้อยู่ในรูปของแพ็คเกจ (Packet) เล็กๆ แล้วส่งไปยังปลายทางโดยอาศัยอินเทอร์เน็ตโปรโตคอล ในการแปลงสัญญาณเสียงนั้นจะทำการแปลงเสียงจากผู้ส่งที่เป็นสัญญาณอนาล็อกให้เป็นสัญญาณดิจิตอลผ่านอุปกรณ์เครือข่ายแล้วส่งต่อผ่านทางเครือข่ายอินเทอร์เน็ตไปยังผู้รับจากนั้นจะทำการแปลงสัญญาณกลับจากดิจิตอลให้เป็นอนาล็อกผ่านทางอุปกรณ์เครือข่ายเพื่อให้ผู้รับได้ยินเสียงที่ส่งไป โดยทั่วไปแล้วหลังจากที่สัญญาณเสียงถูกแบ่งย่อยออกเป็นแพ็คเกจมักจะถูกส่งไปแบบ UDP มากกว่า TDP เนื่องจากการส่งข้อมูลแบบ UDP มีความรวดเร็วกว่าจึงเหมาะในการนำมาใช้ในการส่งข้อมูลเสียงบนโครงข่ายอินเทอร์เน็ต การส่งข้อมูลเสียงจะต้องอาศัยโปรโตคอลหลักที่ใช้ในการส่งสัญญาณระหว่างต้นทางและปลายทาง เช่น โปรโตคอล SIP จึงจะทำให้ต้นทางและปลายทางสื่อสารกันได้ เพื่อให้เข้าใจการทำงานสามารถนำมาเปรียบเทียบกับโมเดลโอเอสไอ (OSI Model) เพื่อให้เข้าใจว่าเราสามารถสื่อสารด้วยเทคโนโลยีวีโอไอพีได้นั้นมีความสอดคล้องอย่างไรกับโมเดลโอเอสไอ ดังภาพที่ 2.1



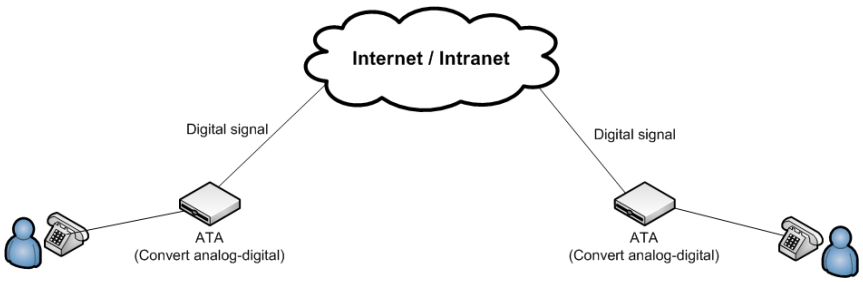
ภาพที่ 2.1 เปรียบเทียบโมเดลโอเอสไอกับเทคโนโลยีวีโอไอพี

ในการแปลงสัญญาณเสียงโดยปกติแล้วเวลาที่มีการพูดคุยผ่านโทรศัพท์เสียงที่พูดนั้นจะถูกส่งจากต้นทางไปยังปลายทางโดยเป็นแบบสัญญาณอนาล็อก (Analog) ดังภาพที่ 2.2



ภาพที่ 2.2 การสื่อสารทางโทรศัพท์แบบปกติ

เมื่อมีการนำสัญญาณเสียงแบบอนาล็อกมาใช้กับเทคโนโลยีวีโอไอพีนั้น จะต้องมีการแปลงสัญญาณเสียงแบบอนาล็อกให้อยู่ในรูปของสัญญาณดิจิตอลก่อนจึงจะสามารถส่งผ่านไปยังโครงข่ายได้ ซึ่งกระบวนการนี้เรียกว่าพีซีเอ็ม (PCM: Pulse Code Modulation) โดยการสื่อสารทางโทรศัพท์ผ่านอินเทอร์เน็ตนั้นดังแสดงในภาพที่ 2.3



ภาพที่ 2.3 การสื่อสารทางโทรศัพท์ผ่านอินเทอร์เน็ต

2.3 มาตรฐานโปรโตคอลของระบบวีโอไอพี

ในการสร้างระบบการสื่อสารวีโอไอพีนั้นสิ่งที่สำคัญมากในการสร้างระบบคือการเลือกใช้งานโปรโตคอลในการสื่อสารให้เหมาะกับอุปกรณ์ที่ได้จัดเตรียมไว้เพื่อให้สามารถรับส่งข้อมูลได้ถูกต้องและมีประสิทธิภาพ โดยทั่วไปแล้วโปรโตคอลที่นิยมใช้ได้แก่

2.3.1) มาตรฐาน H.323

มาตรฐาน H.323 จัดว่าเป็นมาตรฐานการสื่อสารสำหรับวีโอไอพียุดแรกๆ เดิมทีมีการนำไปใช้งานกับระบบการประชุมผ่านวีดีโอ (Video Conference) เป็นหลัก แต่ได้นำมาประยุกต์ในระบบวีโอไอพีด้วย และยังรองรับการทำงานบนระบบไอพีได้ดี มาตรฐาน H.323 นี้ถูกพัฒนาโดย ITU เมื่อปี 1996 สามารถรองรับการส่งข้อมูลทั้งภาพ เสียง และแฟ็กซ์ได้เป็นอย่างดี รวมถึงยังสามารถทำงานร่วมกับโครงข่ายไอเอสดีเอ็น (ISDN: Integrated Service Digital Network) โครงข่ายพีเอสทีเอ็น (PSTN: Public Switched Telephone Network) หรือ SS7 (Signaling System 7) หากต้องการทำงานในสภาวะเครือข่าย NAT จะต้องอาศัย Gate Keeper เพื่อทำหน้าที่เป็น proxy server ในการรับส่งข้อมูลจึงจะสามารถทำงานได้อย่างมีประสิทธิภาพ

2.3.2) มาตรฐาน SIP

มาตรฐาน SIP เป็นมาตรฐานที่ใช้ในการรับส่งข้อมูลกับเครือข่ายวีโอไอพีที่ได้รับความนิยมมากที่สุดในปัจจุบัน เนื่องจากผู้ผลิตมีการผลิตอุปกรณ์ โปรแกรมต่างๆ ที่อิงกับมาตรฐาน SIP กันมากขึ้น โดยโปรโตคอล SIP ถูกออกแบบโดย Henning Schulzrinne ในปี ค.ศ. 1996 และเมื่อปี ค.ศ.2000 ได้มีการประกาศเป็นมาตรฐาน RFC 2361 โดยกลุ่ม IETF (Internet Engineering Task Force) SIP Working Group มีวัตถุประสงค์เพื่อใช้ในการติดต่อสื่อสารระหว่างอุปกรณ์มัลติมีเดียร์ (Multimedia Device) โดยปกติโปรโตคอล SIP จะมีการใช้งานพอร์ต TCP หรือ UDP ที่ 5060 ในการส่งสัญญาณการลงทะเบียน และมีการส่งสัญญาณเสียงโดยพอร์ต UDP ระหว่าง 10000 ถึง 20000 ส่วนประกอบของโปรโตคอล SIP สามารถแบ่งได้เป็น 2 ส่วนได้แก่

1) User Agents แบ่งได้เป็น 2 ส่วนย่อยคือ ยูเอซี (UAC: User Agent Client) และยูเอเอส (UAS: User Agent Server) โดยในการสื่อสารในระบบวีโอไอพีนั้นจะเป็นการสื่อสารในลักษณะ Client-Server โดยจะเริ่มจากยูเอซีทำการส่ง SIP request message ไปยังยูเอเอส หากยูเอเอสได้รับข้อมูลก็จะทำการตอบกลับไปยังยูเอซีด้วย SIP response message

2) SIP Server แบ่งได้เป็น 3 ประเภทได้แก่

2.1) Proxy Server มีหน้าที่เป็นตัวกลางติดต่อสื่อสารระหว่าง SIP Client ที่ต้องการติดต่อสื่อสารกัน โดยสร้างกระบวนการติดต่อสื่อสารระหว่าง SIP Client ทั้งสองโดยจะมีการส่งผ่าน SIP Message ผ่าน Proxy Server ระหว่าง SIP Client ทั้งสองเพื่อรายงานสถานการณ์ทำงาน เมื่อติดต่อกันได้แล้วก็จะเป็นการส่งข้อมูลเสียงหรือข้อมูลสนทนาโดยตรงระหว่าง SIP Client ทั้งสองฝั่งโดยผ่านโปรโตคอลอาร์ทีพี (RTP: Real-time Transport Protocol)

2.2) Registrar Server มีหน้าที่ในการรับขึ้นทะเบียน SIP Client ที่มีการส่งข้อมูลการลงทะเบียนเข้ามาเพื่อเป็นการบอกให้ทราบว่าปัจจุบัน SIP Client หมายเลขดังกล่าวมาจากที่ใด เมื่อมี SIP Client อื่นติดต่อเข้ามาจะสามารถส่งข้อมูลไปยัง SIP Client ดังกล่าวได้

2.3) Redirect Server เป็นเครื่องแม่ข่ายที่ทำการเปลี่ยนหรือกำหนดเส้นทางโดยอาศัยข้อความร้องขอ (Request Message) เพื่อส่งต่อไปยังเครื่องแม่ข่ายปลายทางที่ต้องการ

ในส่วนของข้อความซิพ (SIP Message) นั้นจะเป็นข้อความร้องขอและตอบรับจากทั้ง SIP Client และ SIP Server ซึ่งจะทำให้สามารถทราบถึงขั้นตอนการทำงานได้ โดยข้อความซิพที่จะเห็นนั้นสามารถเปิดดูได้โดยอาศัยโปรแกรมเฝ้าดูเครือข่าย เช่น Ethereal, Wire Shark เป็นต้น โดยทั่วไปแล้วข้อความซิพสามารถแบ่งออกเป็น 2 ประเภทคือ

1) SIP request messages เป็นข้อความในการร้องขอโดยที่ฝั่ง SIP Client จะเป็นผู้สร้างข้อความนี้ขึ้น โดยทั่วไปแล้วสามารถแบ่งย่อยได้เป็น 6 ข้อความอ้างอิงตามมาตรฐาน RFC 3261 ดังตารางที่ 2.1

ตารางที่ 2.1 ข้อความร้องขอของซิพและความหมาย

SIP requests messages	ความหมาย
INVITE	เป็นข้อความในการเชิญติดต่อสื่อสาร
ACK	เป็นข้อความการตอบรับจากผู้สนทนา
OPTION	เป็นข้อความที่สอบถามถึงความสามารถของทั้ง SIP Client และ SIP Server
BYE	เป็นข้อความสิ้นสุดการติดต่อสื่อสาร
CANCEL	เป็นข้อความยกเลิกการติดต่อสื่อสาร
REGISTER	เป็นข้อความสำหรับการลงทะเบียนกับ SIP Server

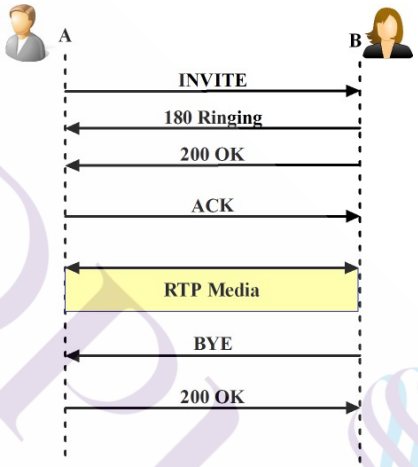
2) SIP response messages เป็นข้อความตอบรับจาก SIP Server ที่ใช้ตอบสนองเมื่อมีข้อความร้องขอซิพส่งเข้ามา ซึ่งปกติแล้วสามารถแบ่งออกเป็น 6 กลุ่ม ดังตารางที่ 2.2

ตารางที่ 2.2 ข้อความตอบสนองของซิพและความหมาย

SIP response message	ความหมาย
1XX	Provisional -- request received, continuing to process the request
2XX	Success -- the action was successfully received, understood and accepted
3XX	Redirection -- further action needs to be taken in order to complete the request
4XX	Client Error -- the request contains bad syntax or cannot be fulfilled at this server
5XX	Server Error -- the server failed to fulfill an apparently valid request
6XX	Global Failure -- the request cannot be fulfilled at any server

ที่มา: http://tools.ietf.org/html/rfc3261#page-26 RFC-3261

ในหลักการทำงานของ SIP จะทำงานโดยเริ่มจาก A มีการร้องขอติดต่อสื่อสารกับ B นั่นคือจะทำการส่งข้อความร้องขอ INVITE ไปยัง B โดยระหว่างนั้น B จะตอบกลับข้อความ 180 Ringing นั่นคือ B จะได้ยินเสียงสัญญาณโทรเข้าดังขึ้น หาก B ทำการยกหูก็จะได้รับข้อความ 200 OK เกิดขึ้น และ A จะทำการส่ง ACK เพื่อเริ่มต้นการสนทนาโดยในการสนทนานั้นจะทำผ่านโปรโตคอล RTP หากการสนทนาสิ้นสุดเมื่อ B ทำการวางสายก็จะทำการส่งข้อความ BYE ไปให้กับ A และหาก A วางหูก็จะทำการส่งข้อความ 200 OK ไปให้กับ B นั่นคือสิ้นสุดการสนทนา ซึ่งจากตัวอย่างการสนทนาที่ได้กล่าวมาเป็นลักษณะการสนทนาแบบจุดต่อจุด (Point to Point) โดยแสดงแผนผังได้ดังภาพที่ 2.4



ภาพที่ 2.4 ตัวอย่างการติดต่อสื่อสารในรูปแบบจุดต่อจุดของโปรโตคอลซิพ

2.4 โครงข่ายยุคต่อไป (NGN: Next Generation Network) [2]

สหภาพโทรคมนาคมระหว่างประเทศ (ITU: International Telecommunication Union) ได้ให้คำนิยามของ NGN ว่าเป็นโครงข่ายโทรคมนาคมแบบแพ็คเกจที่สามารถให้บริการสื่อสารโทรคมนาคมและบรอดแบนด์ที่หลากหลายรูปแบบ สามารถใช้เทคโนโลยีการส่งผ่านข้อมูลที่ให้คุณภาพบริการ มีฟังก์ชันการให้บริการแยกเป็นอิสระจากเทคโนโลยีการส่งผ่านข้อมูลที่รองรับ ผู้ใช้บริการบนโครงข่ายโทรคมนาคมแบบ NGN จะต้องสามารถเลือกใช้บริการใดๆจากผู้ให้บริการรายอื่นๆได้ โดยใช้เทคโนโลยีเชื่อมต่อปลายทางใดๆ ได้โดยไร้ขีดจำกัด โครงข่ายโทรคมนาคมนี้รองรับการใช้บริการแบบเคลื่อนที่ได้ทุกที่ทุกเวลาอย่างต่อเนื่อง

หลักการของ NGN อยู่บนพื้นฐานแนวคิดที่จะพัฒนาเทคโนโลยีโครงข่ายโทรคมนาคมให้เป็นแบบ IP-Based ซึ่งจะรองรับบริการทางโทรคมนาคมได้ทั้งบริการโทรศัพท์ประจำที่ บริการโทรศัพท์เคลื่อนที่ และบริการอินเทอร์เน็ตไปพร้อมกัน โดยระยะแรกโครงข่ายโทรคมนาคมแบบ

NGN ถูกพัฒนาเพื่อใช้งานในระดับ Core Network ก่อน ต่อมาได้มีการพัฒนาในระดับ Access Network ไปสู่ผู้ใช้บริการปลายทาง

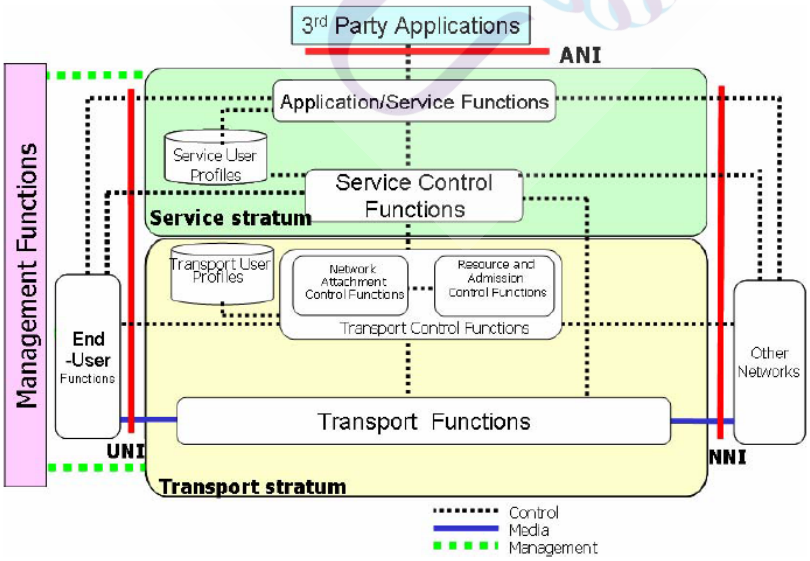
โดยทั่วไปแล้วโครงสร้างสถาปัตยกรรมของโครงข่าย NGN จะประกอบด้วย 3 ระดับ ดังในภาพที่ 2.5 ซึ่งประกอบไปด้วย

1) ระดับชั้นบริการ (Service Stratum) เป็นส่วนที่เกี่ยวข้องกับการจัดการและควบคุมในบริการต่างๆ โดยจะจัดการสัญญาณควบคุม (Signaling) ในการรับส่งข้อมูลและบริการต่างๆ ทั้งเก่าและใหม่ในลักษณะของ IP Circuit

2) ระดับชั้นขนส่ง (Transport Stratum) เป็นส่วนที่เกี่ยวข้องกับการรับส่งข้อมูล ทำหน้าที่ในการนำพาข้อมูลหรือแพ็คเกจซึ่งมีอยู่ในบริการต่างๆ จากที่หนึ่งไปสู่อีกที่หนึ่งสำหรับในการติดต่อสื่อสารระหว่างกัน

3) ระดับชั้นการเข้าถึง (Access Stratum) เป็นส่วนที่เกี่ยวข้องกับการเชื่อมต่อปลายทางไปยังผู้ใช้บริการ (End User) โดยสามารถเชื่อมต่อได้กับอุปกรณ์ทุกรูปแบบ ได้แก่ โทรศัพท์มือถือ โน้ตบุ๊ค โทรศัพท์แบบไอพี แท็บเล็ต และอุปกรณ์ที่จะเกิดขึ้นใหม่ในอนาคต

จากโครงสร้างสถาปัตยกรรมของโครงข่าย NGN ซึ่งมีการแบ่งแยกหน้าที่การทำงานของแต่ละระดับชั้นทำให้มีความสามารถในการเพิ่มหรือขยายความสามารถของโครงข่ายรวมถึงการปรับปรุงโครงข่ายในอนาคตได้ โดยจะไม่กระทบกันในแต่ละระดับชั้น



ภาพที่ 2.5 โครงสร้างพื้นฐานของโครงข่ายโทรคมนาคม NGN

ที่มา: http://www.nbtc.go.th

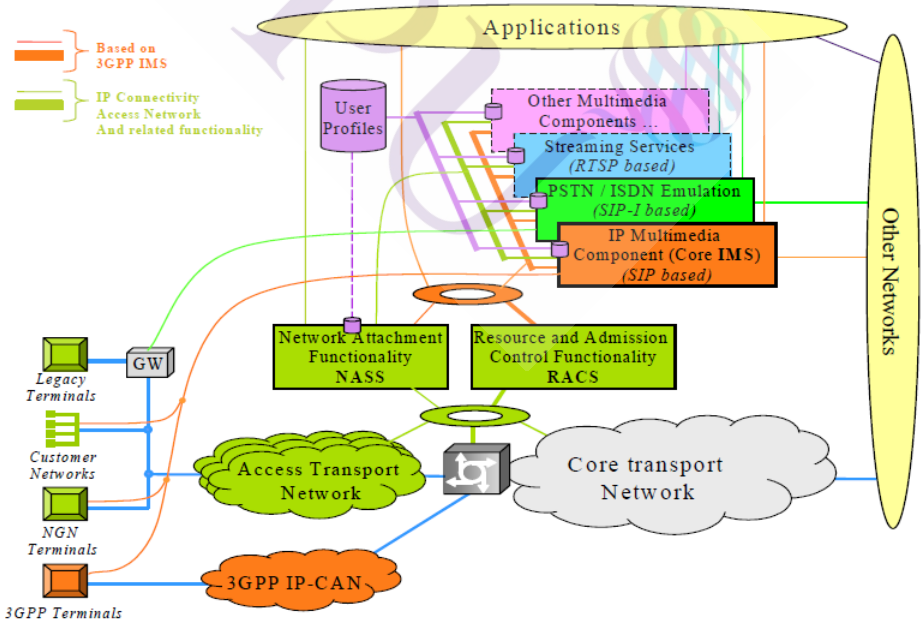
ในส่วนขององค์ประกอบภายในโครงข่ายโทรคมนาคม NGN ดังในภาพที่ 2.6 โดยแบ่งฟังก์ชันการทำงานออกเป็นกลุ่มๆ ดังนี้

1) ระบบย่อยในการขนส่ง (Transport Subsystem) คือ โครงข่ายที่ทำหน้าที่ในการส่งผ่านข้อมูลต่างๆ ภายใน ซึ่งเป็นลักษณะ Packet based โดยจะครอบคลุมไปถึงโครงข่าย IP และโครงข่ายเชื่อมต่อต่างๆ

2) NASS และ RACS ทำหน้าที่ดูแลการใช้งานทรัพยากรของระบบ โดยประสานงานกับกับระบบย่อยในการขนส่งเพื่อดูสถานะของทรัพยากรรวมถึงการทำงานร่วมกับระบบย่อยในการควบคุม (Control Subsystem) เพื่อควบคุมไม่ให้มีการใช้งานทรัพยากรบนระบบมากเกินที่ระบบสามารถรองรับได้ รวมไปถึงควบคุมในเรื่องคุณภาพบริการ (QoS: Quality of Service) ของระบบ

3) ระบบย่อยในการควบคุม (Control Subsystem) ทำหน้าที่ในการควบคุมการทำงานของโครงข่ายในส่วนการให้บริการ เช่น ควบคุมบริการทางเสียง ทางวีดิโอ เชื่อมต่อกับแอพพลิเคชันเพื่อควบคุมการใช้งานบริการเสริม

4) แอพพลิเคชัน (Application) คือบริการต่างๆสำหรับผู้ใช้บริการ โดยการใช้งานแอพพลิเคชันจะทำโดยผ่านการควบคุมของระบบย่อยในการควบคุม



ภาพที่ 2.6 องค์ประกอบของโครงข่ายโทรคมนาคม NGN

ที่มา: http://www.nbtc.go.th

2.5 ประเด็นเรื่องความมั่นคงบนโครงข่ายโทรคมนาคม VoIP [3]

ในเรื่องของการโจมตีระบบ VoIP นั้นสามารถแยกได้เป็น 3 กลุ่มหลักโดยจะแบ่งได้เป็น Denial of Service, Fraud and Abuse และ Data Confidentiality ซึ่งแต่ละกลุ่มนั้นส่งผลกระทบต่อการให้บริการ VoIP ในแง่ลบ ซึ่งรายละเอียดของรูปแบบการโจมตีแต่ละรูปแบบมีรายละเอียดดังนี้

1. การโจมตีเพื่อขัดขวางการให้บริการ (DoS: Denial of Service Attacks) เป็นการโจมตีแบบหนึ่งที่พบเห็นได้บ่อยครั้งบนอินเทอร์เน็ต ซึ่งอาศัยช่องโหว่ของซอฟต์แวร์ในระบบโครงข่ายที่เราใช้งานอยู่ ซึ่งจะส่งผลทำให้อุปกรณ์ในระบบโครงข่ายต้องสูญเสียทรัพยากรที่ต้องการไปโดยไม่จำเป็น และอาจจะไปรบกวนโพรโตคอลที่ให้บริการ รวมทั้งมีการประมวลผลกระบวนการที่ไม่จำเป็น ส่งผลให้องค์กรไม่สามารถให้บริการที่ตอบสนองกับสมาชิกได้ตามที่ต้องการ ซึ่งในการโจมตีโดยส่วนใหญ่แล้วจะมุ่งเป้าไปที่อุปกรณ์ต่างๆ ในระบบโครงข่าย แต่ก็มีบางครั้งที่โจมตีไปที่อุปกรณ์ของลูกค้า (CPE: Customer Premises Equipment) เช่นกัน อย่างในกรณีของอุปกรณ์ในโครงข่ายนั้นจะเป็นองค์ประกอบที่จำเป็นทั้งต่อการสร้างสัญญาณโทรศัพท์และกำหนดเส้นทางในการติดต่อของระบบ โดยอุปกรณ์แต่ละตัวก็จะมีระบบปฏิบัติการของมันเองที่ใช้เพื่อเชื่อมต่อระหว่างอุปกรณ์ที่เป็นฮาร์ดแวร์ภายในตัวมัน และแอพพลิเคชันที่ติดตั้งอยู่ภายใน ซึ่งจะช่วยให้อุปกรณ์ดังกล่าวทำงานได้อย่างถูกต้อง รูปแบบการโจมตี แบบ DoS นั้น มีอยู่หลายแบบด้วยกัน วิธีหนึ่งก็คือการบังคับให้ระบบปฏิบัติการของอุปกรณ์โครงข่ายตัวใดตัวหนึ่งหยุดทำงานหรือทำงานผิดพลาด ซึ่งจะส่งผลต่อการทำงานของตัวมันเอง แล้วทำให้ระบบโดยรวมไม่สามารถใช้การได้ หรือมีประสิทธิภาพต่ำลงกว่าที่ลูกค้าคาดหวังเอาไว้ ส่วนอีกวิธีหนึ่งที่ใช้กันมากก็คือการเข้าไปปรับให้อุปกรณ์โครงข่าย หรือ CPE รับข้อความที่ผิดพลาดเข้าไปจากหลายๆ โพรโตคอลที่ใช้ในบริการดังกล่าว ซึ่งข้อความที่ผิดพลาดนี้จะเข้าไปรบกวนการทำงานปกติของบริการทำให้ระบบเข้าใจผิดและต้องเสียเวลาในการตัดสินใจ ซึ่งก็จะส่งผลให้คุณภาพของการบริการต่ำลง ส่วนการโจมตีที่เราเรียกว่า การโจมตีแบบ DDoS (Distributed Denial of Service) นั้นเป็นการโจมตีที่คล้ายๆ กันแต่จะส่งผลให้ทรัพยากรของโครงข่ายส่วนใหญ่หายไปในทันที และระบบต้องรับภาระจำนวนมหาศาล เพราะ DDoS จะเป็นเหมือนการบังคับให้ทรัพยากรทั้งหมดไม่ว่าจะเป็นซีพียูหรือหน่วยความจำในเครื่องต้องรับมือกับการร้องขอที่ผิดพลาดจำนวนมากที่ส่งเข้ามา ซึ่งจะส่งผลกระทบทำให้ระบบมีคุณภาพต่ำลงทันที จนอาจจะทำงานไม่ได้เลยทีเดียว

2. การขโมยใช้บริการ (Fraud and Abuse) เกิดจากกรณีที่บุคคลใดก็ตามสามารถใช้บริการหรือทรัพยากรได้มากกว่าสิทธิที่เขาควรจะมี ซึ่งถ้าแบ่งเป็นประเภทแล้วก็ยังสามารถพิจารณาได้เป็นสองประเภทหลักๆ ก็คือ การขโมยใช้งานเต็มรูปแบบก็คือมีการเข้าใช้บริการโดยที่ผู้ใช้ไม่มี

สิทธิในการใช้งานเลย หรือไม่ได้ลงทะเบียนเป็นสมาชิกเอาไว้ กับอีกประเภทหนึ่งคือการขโมยใช้งานบางส่วน ซึ่งเป็นการใช้งานของสมาชิกที่มีอยู่ในระบบแต่ใช้งานเกินกว่าสิ่งที่ได้รับ อนุญาตเอาไว้ หรือว่ามากกว่าที่เขาจ่ายค่าบริการลงไป แต่ไม่ว่าจะเป็นแบบใดก็ตาม ถ้าหากมีการใช้งานนอกเหนือไปจากนโยบายที่กำหนดเอาไว้ในระบบก็ถือว่าเป็นการขโมยใช้งานโดยทั้งสิ้น ซึ่งพฤติกรรมของผู้ใช้เองอาจจะมีทั้งจงใจขโมยใช้งานหรือใช้เกินขอบเขตโดยไม่ได้ตั้งใจ อย่างกรณีแรกนั้นคงชัดเจนในตัวอยู่แล้ว แต่การใช้งานโดยไม่ได้ตั้งใจนั้น อาจจะเกิดจากพนักงานไม่ทราบสิทธิที่แท้จริงของตน แต่ระบบยอมให้ทำได้เนื่องจากการจัดการระบบผิดพลาดหรือว่าดูแลไม่ทั่วถึงนั่นเอง แต่ทั้งการโจมตีแบบการขโมยใช้บริการนั้นในวันนี้ถือว่าเป็นเรื่องที่ค่อนข้างใหม่สำหรับระบบ VoIP ซึ่งอาจจะเกิดขึ้นได้โดยง่ายเมื่อมีการติดตั้งคุณลักษณะใหม่ๆ หรือคุณลักษณะขั้นสูงเพิ่มเติมลงไปในระบบ โดยที่ไม่มีการป้องกันเอาไว้อย่างดีเพียงพอ และเนื่องจากระบบ VoIP นั้นก็ยังถือว่าเป็นของใหม่สำหรับโลกในปัจจุบัน เพราะแม้ว่าจะมีการพัฒนามานับสิบปีแล้วก็ตาม แต่การนำมาใช้งานนั้นยังไม่กว้างขวางและยังไม่กลายเป็นอุปกรณ์พื้นฐานเสียทีเดียว ดังนั้นเทคนิคในการหลอกลวงหรือขโมยใช้ระบบก็ยังมีเกิดขึ้นใหม่อยู่เรื่อยๆ และก็เป็นตัวผลักดันให้มีการพัฒนาระบบป้องกันให้ดีขึ้นตามไปด้วยเช่นกัน

3. ความเป็นส่วนตัวของข้อมูลและความเชื่อมั่น (Confidentiality and Data Privacy) สำหรับในเรื่องของความเป็นส่วนตัวของข้อมูลนั้น ถูกมองว่าเป็นเรื่องสำคัญจึงต้องป้องกันสิทธิของผู้ใช้เอาไว้โดยการปกป้อง ข้อมูลส่วนตัวของผู้ใช้ให้ปลอดภัยตามไปด้วยเช่นกัน ข้อมูลหลายอย่างของสมาชิกนั้นมีความจำเป็นในการเข้าสู่ระบบ ซึ่งข้อมูลดังกล่าวนั้นอาจจะเก็บเอาไว้ในฐานข้อมูลอื่นๆ ภาย ในระบบ ดังนั้นการโจมตีที่เกิดขึ้นในส่วนนี้ จะโจมตีเข้าไปที่ไอพีและละเมิดความเป็นส่วนตัวของเจ้าของทันที โดยเจาะตรงไปที่อุปกรณ์บนโครงข่ายหรือโจมตีเข้าไปที่ฐานข้อมูลของระบบที่บรรจุข้อมูลส่วนตัวของลูกค้าเอาไว้ ซึ่งหากโจมตีสำเร็จข้อมูลดังกล่าวก็จะตกไปอยู่ในมือของแฮกเกอร์(Hacker) และสามารถนำมาใช้เพื่อการย้อนกลับเข้าสู่ระบบในภายหลังหรือแม้แต่นำไปใช้ในเรื่องอื่นๆ ก็ยังได้เช่นกัน ข้อมูลต่างๆ ของผู้ใช้ในระบบ VoIP นั้น จะถูกมองว่าเป็นข้อมูลลับ และเป็นข้อมูลส่วนตัวที่รั่วไหลไม่ได้ แต่ขณะเดียวกันก็จะต้องถูกส่งออกแบบร่วมกับเสียงที่วิ่งผ่านในระบบรวมไปถึงโพรโตคอลสื่อสารที่ใช้อีกด้วย ซึ่งข้อมูลส่วนตัวที่อยู่ภายในโพรโตคอลสัญญาณนั้นอาจจะรวมตั้งแต่หมายเลขโทรศัพท์ปลายทางที่กำลังติดต่อไป หรืออาจจะมีข้อมูลต้นทาง และอื่นๆ รวมไปด้วยเช่นกัน ซึ่งทั้งเสียงและสัญญาณที่ไม่ได้มีการป้องกันและส่งผ่านโครงข่ายแบบไอพีที่ใช้งานร่วมกันกับผู้อื่น หรือระบบสาธารณะนั้นอาจจะถูกดับจับและโจมตีได้โดยง่าย แต่แม้ว่าป้องกันเอาไว้แล้ว ก็อาจจะมีข้อมูลบางส่วนที่ถอดรหัสออกมาได้เช่นกัน

การรักษาความปลอดภัยของ VoIP ให้มีประสิทธิภาพสูงสุดนั้นจะรวมทั้งกลไกพื้นฐานของการรักษาความปลอดภัยในระบบเครือข่ายแบบไอพีและกลไกการรักษาความปลอดภัยเพิ่มเติมสำหรับ VoIP ด้วย โดยสามารถแยกออกมาได้ดังนี้

1. นโยบายรักษาความปลอดภัย ระบบการรักษาความปลอดภัยเริ่มต้นจากการกำหนดนโยบายหรือเงื่อนไขต่างๆ ในการใช้งานเพื่อให้ครอบคลุมการใช้งานได้อย่างถูกต้องที่สุด โดยที่นโยบายสำหรับ VoIP นั้นเปรียบได้เหมือนกับการเป็นศูนย์กลางสำหรับการทำงานในเรื่องการรักษาความปลอดภัยอื่นๆ ที่เกี่ยวข้องกันทั้งหมด การสร้างระบบขึ้นมาจากพื้นฐานนโยบายนี้จะช่วยให้กระบวนการติดตั้งระบบ VoIP นั้น กลายเป็นเรื่องง่าย และสามารถควบคุมสิทธิในการใช้งานของผู้ใช้ทุกๆ คนได้ตั้งแต่เริ่มต้นวางแผนติดตั้งระบบ ซึ่งไม่จำเป็นว่าจะต้องติดตั้งระบบลงไปก่อนเสียด้วยซ้ำ เพราะว่าการกำหนดนโยบายนั้นสามารถทำได้ตั้งแต่ในกระบวนการของเอกสารหรือแม้แต่ในส่วนของการวางแผนโครงการ ซึ่งอาจจะต้องแบ่งกลุ่มผู้ใช้หรือระดับผู้ใช้ไปจนถึงแบ่งเขตพื้นที่รับผิดชอบต่างๆ เอาไว้ให้ชัดเจน เมื่อควบคุมโครงสร้างของนโยบายได้แล้ว ที่เหลือก็เพียงแค่นำไปประกอบเข้ากับระบบ VoIP ที่ติดตั้งแล้วเท่านั้น ซึ่งก็เป็นขั้นตอนที่สามารถแยกกันทำได้โดยอิสระ และสามารถปรับแต่งเพิ่มเติมได้ โดยการกำหนดนโยบายย่อยในภายหลังเช่นกัน

2. ป้องกันความเสียหายจากการโจมตีแบบ DoS ซึ่ง DoS นับว่าเป็นเรื่องร้ายแรงและอันตรายเป็นอย่างมากสำหรับระบบ VoIP เนื่องจากระบบ VoIP นั้น ต้องการประสิทธิภาพในการทำงานค่อนข้างสูงเพื่อที่คงไว้ซึ่งการส่งผ่านข้อมูลเสียงได้ในแบบเรียลไทม์ หากว่าไม่สามารถส่งแพ็กเกจได้แบบเรียลไทม์ระบบนี้ก็จะหมดความหมายในทันที ซึ่งสำหรับการโจมตี DoS นั้นจะต้องวางแผนรับมือเอาไว้ในทุกๆ ส่วนของโครงข่ายที่ระบบ VoIP ของเราต้องวิ่งผ่าน ไม่ว่าจะเป็นในส่วนของ LAN, WAN หรือโครงข่ายอื่นที่จำเป็นต้องเข้าถึงเพื่อกำหนดเป็นเส้นทางสำหรับ VoIP เป็นต้น โดยปกติแล้วในกลไกการรับมือ DoS นั้น จะต้องติดตั้งเอาไว้ในระดับโครงสร้างพื้นฐานของระบบ โดยที่ขอบระหว่างโครงข่ายนั้น อุปกรณ์โครงข่ายจะต้องมีอุปกรณ์ป้องกันสำหรับ VoIP ติด ตั้งเอาไว้และต้องสามารถบล็อกข้อมูลที่ไม่ถูกต้องหรือการโจมตีให้หยุดตั้งแต่จุดดังกล่าวได้เสียก่อน เงื่อนไขในการป้องกันระบบโครงข่ายก็จะต้องอนุญาตให้เฉพาะบริการ และเฉพาะไอพีที่กำหนดเท่านั้นที่สามารถวิ่งผ่านเข้าหรือออกจากเครือข่ายที่เราดูแลได้ ส่วนในการคอนฟิกไฟร์วอล เราเตอร์ สวิตซ์ หรือเซิร์ฟเวอร์จะต้องลดผลกระทบจากการ flood หรือการโจมตี DoS แบบอื่นๆ ให้ได้ทั้งหมดเช่นกัน ซึ่งการตรวจสอบอุปกรณ์โครงข่ายทุกตัวรวมทั้งเครื่องพีซีทั้งหมดอยู่เป็นประจำจะช่วยลดปัญหาดังกล่าวนี้ไปได้มากและยังช่วยอัพเดตระบบให้ทันสมัยอยู่ตลอดเวลาเช่นเดียวกัน ส่วนในการป้องกัน DDoS นั้นนับเป็นส่วนจำเป็นที่จะต้องติดตั้งเอาไว้เพื่อปกป้องจากการโจมตีโดยการ flood โดย ที่อุปกรณ์โครงข่ายต่างๆ นั้นจะต้องกำหนดขอบเขตความสามารถเพื่อ

ใช้จำกัดปริมาณของทรัพยากรที่จำเป็นต้องใช้งานสำหรับบริการ ซึ่งในส่วนนี้ถือเป็นเรื่องสำคัญในการบริหารจัดการบริการเพื่อให้รองรับกับ ความต้องการใช้งานได้ตลอดเวลา ซึ่งเมื่อพบว่ามีการโจมตีเข้ามาในระบบ การรับมือกับปัญหาก็จะทำได้อย่างรวดเร็วทั้งในการสืบหาที่มา และรับมือกับปัญหาทั้งหมด ก่อนที่จะเกิดผลกระทบต่อระบบ

3. รักษาความปลอดภัยสำหรับคุณลักษณะขั้นสูงของ VoIP จุดเด่นที่นับเป็นข้อได้เปรียบของ VoIP ก็คือการรวมกันระหว่างทั้งเสียงกับเว็บ โดยผู้ใช้ VoIP นั้นสามารถบริหารจัดการบัญชีผู้ใช้ (User Account) ของตนเองได้ และเลือกใช้คุณลักษณะขั้นสูง รวมทั้งเข้าถึงบัญชีผู้ใช้ของตนเองได้จากระยะไกลผ่านทางเว็บ ดังนั้นในการเข้าถึงคุณลักษณะขั้นสูงต่างๆ เหล่านี้ล้วนแต่จำเป็นต้องมีการระบุตัวตนและป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ยิ่งไปกว่านั้นแล้วคุณลักษณะขั้นสูงทุกอย่างจำเป็นต้องถูกตรวจสอบเรื่องการรักษาความปลอดภัยพื้นฐานด้วยเสมอ และต้องมั่นใจได้ว่าไม่มีโอกาสที่จะต้องเสี่ยงกับจากโจมตีหรือขโมยใช้งานอีกด้วยส่วนคุณลักษณะใดๆ ก็ตามที่ไม่ได้ใช้งานก็ควรจะต้องปิดเอาไว้ก่อนเสมอ เพื่อจำกัดโอกาสที่ผู้โจมตีจะใช้ช่องทางดังกล่าวในการโจมตีเข้ามาในระบบ

4. รักษาความปลอดภัยกับเสียงและสัญญาณ เสียงและสัญญาณอื่นๆ ที่สัมพันธ์กันนั้นควรจะถูกแยกออกมาเป็นอิสระจากช่องทางข้อมูลอื่นทั่วไป เพื่อที่จะได้สามารถเพิ่มการรักษาความปลอดภัยลงไปได้ ซึ่งในจัดนี้นั้นข้อมูล VoIP จะต้องถูกฟิลเตอร์ออกมาจากข้อมูลทั่วไป และต้องแยกออกมาจากข้อมูล VoIP แปลกปลอมอื่นๆ อีกด้วย โดยกลไกที่ทำงานบนโครงข่ายนั้นค่อนข้างจำเป็นในการคัดแยกข้อมูลดังกล่าว นี้ออกมา อย่างเช่น VPN อาจจะต้องนำมาใช้กับ WAN เพื่อจัดการทั้งในเรื่องของความปลอดภัย และ QoS ไปพร้อมๆ กันส่วนการเข้ารหัสและการป้องกันระดับข้อมูลสำหรับทั้งสัญญาณและเสียงนั้นก็จะช่วยให้มั่นใจยิ่งขึ้นจากการโจมตี DoS ในบางประเภท

5. การตรวจจับและการป้องกันการลักลอบใช้ (Fraud Prevention and Detection) ในส่วนนี้เป็นกลไกสำหรับตรวจสอบการขโมยเข้าใช้งานในเซอร์วิสโทรศัพท์ที่มีอยู่ในระบบ ซึ่งสามารถใช้เซอร์วิสธรรมดาในการตรวจสอบกับ VoIP ได้เช่นกัน โดยอุปกรณ์ในโครงข่าย VoIP นั้น จำเป็นต้องได้รับการตรวจสอบที่ดีกว่าเพื่อสามารถกำหนดสิทธิในการใช้งานได้ อย่างชัดเจนมากยิ่งขึ้น ไม่ต่างจากระบบตู้สาขาที่สามารถจำกัดสิทธิการใช้งานได้อย่างอิสระ VoIP ก็จำเป็นต้องทำได้เช่นกัน โดยกลไกในการป้องกันระบบนั้นจำต้องมีทั้งการรักษาความปลอดภัยในทางกายภาพเพื่อจำกัดการเข้าถึงระบบโดยตรง และการรักษาความปลอดภัยในส่วนของการปรับแต่งเพื่อป้องกันในส่วนของการเข้าถึงแบบรีโมทแอคเซสอีกด้วย นอกจากนี้จะต้องมีระบบบันทึกข้อมูล (Log) เพื่อเฝ้าระวังและตรวจสอบการเข้าใช้งานโดยไม่ได้รับอนุญาตอยู่อย่างต่อเนื่องเช่นกัน สำหรับ

ผู้ให้บริการก็ยังมีความจำเป็นต้องพัฒนาอัลกอริธึมในการป้องกันการลักลอบใช้งานเพิ่มเติมอีกด้วย เพื่อเตรียมตัวรับมือกับการโจมตี VoIP ในรูปแบบใหม่ๆ ที่กำลังจะเกิดขึ้น

6. รักษาความปลอดภัยที่ปลายทาง ที่ปลายทางของ VoIP นั้น มักจะเป็นอุปกรณ์ที่ออกแบบมาเฉพาะและค่อนข้างฉลาดพอ แต่ก็จำเป็นต้องป้องกันเอาไว้ด้วยเช่นกัน ซึ่งรวมถึงจะต้องมีการหาและป้องกันช่องโหว่ของระบบทันทีที่ตรวจสอบพบ รวมถึงมีการปรับปรุงอยู่อย่างต่อเนื่อง โดยสำหรับปลายทางของ VoIP นั้น จะต้องมีการควบคุมการดาวน์โหลดซอฟต์แวร์ หรือการรีโมทแอคเซสเพื่อให้ทุกอย่างเป็นไปอย่างปลอดภัยเช่นกัน และแน่นอนว่าการเข้าถึงโดยตรงที่อุปกรณ์ปลายทางของ VoIP นั้น ก็จำเป็นต้องทำเสมอ เพื่อปกป้องระบบของเราเช่นกัน ไม่ต่างจากโทรศัพท์อื่นๆ ภายในองค์กรที่หากใครเดินเข้าไปใช้งานได้ก็สามารถต่อไปยังปลายทางได้ทันที โดยที่องค์กรจะทราบเพียงแค่จุดต่อภายในว่ามาจากที่ใด แต่ไม่มีทางทราบได้ว่าใครเป็นผู้โทรติดต่อ

7. รักษาความปลอดภัยกับโครงสร้างพื้นฐาน กลไกในการรักษาความปลอดภัยสำหรับโครงสร้างพื้นฐานของระบบนั้น จะต้องติดตั้งเอาไว้เป็นระดับชั้นหลายๆ ชั้น ซึ่งถ้าหากในขณะใช้งาน มีระบบใดเกิดความเสียหายไม่สามารถทำงานได้ขึ้นมา ก็ยังจะมีระบบรักษาความปลอดภัยอื่นๆ ที่คอยปกป้องเอาไว้อีกด้วยเช่นกัน โดยจะต้องแบ่งการรักษาความปลอดภัยออกเป็นส่วนๆ เช่น รักษาความปลอดภัยที่เซิร์ฟเวอร์ และอุปกรณ์ปลายทาง รักษาความปลอดภัยของเครือข่าย อัพเดตและปรับปรุงซอฟต์แวร์รักษาความปลอดภัยเป็นประจำ ตรวจสอบช่วงโหว่ในการรักษาความปลอดภัยทั้งสำหรับผลิตภัณฑ์ที่ออกวางจำหน่าย แล้วและมีแผนการวางจำหน่าย(สำหรับผู้ผลิต)

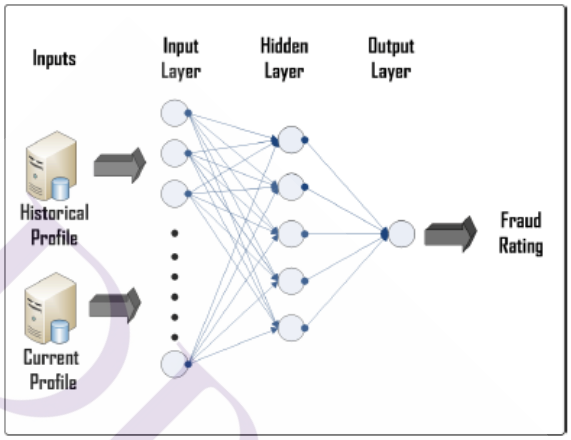
ระบบการรักษาความปลอดภัย นั้นนับเป็นส่วนหนึ่งภายในระบบรวมของ VoIP จำเป็นต้องติดตั้งและให้ความสำคัญ โดยการรักษาความปลอดภัยจะต้องรวมไว้ตั้งแต่จุดเริ่มต้นในกระบวนการติดตั้ง ตลอดจนถึงช่วงอายุตลอดการใช้งาน และยังจะต้องให้ความสำคัญในทุกๆ ระดับเพื่อให้เกิดสภาพแวดล้อมในการทำงานที่ปลอดภัยอย่างแท้จริง กลไกการรักษาความปลอดภัยยังจำเป็นต้องมีการตรวจสอบและพัฒนา

2.6 งานวิจัยที่เกี่ยวข้อง

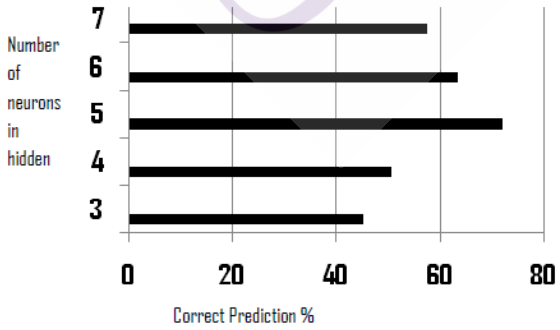
2.6.1 การประยุกต์โครงข่ายประสาทเทียม

Qayyum และคณะได้ทำการศึกษาและพัฒนาระบบตรวจจับการลักลอบใช้บนโครงข่ายมือถือ [4] โดยโครงข่ายที่ทำการพัฒนาเป็นแบบเพอร์เซพตรอนหลายระดับ ในงานวิจัยกำหนดไว้ 3 ระดับด้วยกันโดยมี ส่วนนำเข้า ส่วนซ่อน ส่วนนำออก และส่วนในการจัดระดับของลูกค้าจะอาศัยข้อมูลประวัติการโทรของลูกค้า อัตราการเรียนรู้และค่าน้ำหนักจะถูกนำเข้าสู่โครงข่ายที่กำหนด

การเปลี่ยนแปลงของจำนวนของนิวรอล (จำนวนโหนดซ่อน) ทำให้ผลที่ออกมามีความแตกต่างกัน ดังนั้นสถาปัตยกรรมทั้งหมดมีการถูกวิเคราะห์และถูกทดสอบในกรณีที่จะค้นหาโครงข่ายที่เหมาะสมดังภาพที่ 2.8 สำหรับวัตถุประสงค์ของงานวิจัยนี้จะทดสอบผลของโครงข่ายด้วยจำนวนที่แตกต่างของโหนดซ่อนโดยใช้ activation function เป็นฟังก์ชันซิกมอยด์ (Sigmoid Function) จากผลการทดลองพบว่าโครงข่ายประสาทเทียมที่ได้พัฒนาขึ้นประกอบด้วย 14 นิวรอลนำเข้า 5 นิวรอลชั้นซ่อนและ 1 นิวรอลนำออกมีความเหมาะสมที่สุด โดยมีผลการเปรียบเทียบดังภาพที่ 2.9



ภาพที่ 2.7 สถาปัตยกรรมโครงข่ายประสาทเทียม

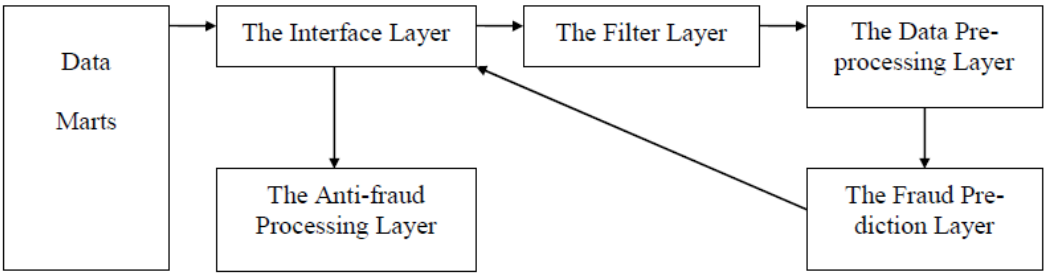


ภาพที่ 2.8 เปรียบเทียบจำนวนโหนดซ่อนและประสิทธิภาพในการตรวจจับได้บนโครงข่ายประสาทเทียม

ในงานวิจัยเรื่องการใช้เทคนิคแบบไม่ต้องเรียนรู้สำหรับการตรวจจับการลักลอบใช้บนโครงข่ายทางเสียงผ่านอินเทอร์เน็ต [7] ได้ทำการแบ่งช่วงเวลาในการโทรเป็น 4 ช่วง ได้แก่ กลางคืน (00 am - 06 am) ช่วงเช้า (06 am - 12 am) ช่วงกลางวัน (12 pm - 06 pm) และช่วงเย็น (06 pm - 00 am) แล้วนำมาหาจำนวนครั้งการโทรไปยังเลขหมายพิเศษ การโทรไปต่างประเทศ การโทรไปยังเบอร์โทรศัพท์มือถือ จากนั้นนำมาหาค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน โดยงานวิจัยนี้ได้นำวิธีโครงข่ายประสาทแบบไม่มีผู้สอน (NN-SOM: Neural Network Self Organizing Map) มาประยุกต์ พบว่าสามารถตรวจจับได้อย่างน้อย 88% ในงานวิจัยเรื่องแบบจำลองการล้มละลายในอุตสาหกรรมโทรคมนาคมเคลื่อนที่ [8] ได้ทำการประยุกต์ตัวแบบโครงข่ายประสาทเทียมโดยได้ทำการศึกษาเปรียบเทียบกับตัวแบบการตัดสินใจแบบต้นไม้ (Decision Tree) โดยงานวิจัยได้ศึกษาถึงกรณีที่ผู้ให้บริการสูญเสียรายได้จากกรณีที่ผู้ใช้ไม่ได้ชำระบิลเนื่องด้วยหลากหลายปัจจัย โดยในการพยากรณ์จะดูแนวโน้มของผู้ใช้ในการชำระเงิน โดยจากการศึกษาพบว่าการใช้โครงข่ายประสาทเทียมนั้นมีความเสถียรกว่าการใช้ตัวแบบตัดสินใจต้นไม้และมีประสิทธิภาพมากกว่า

2.6.2 การประยุกต์การจำแนกแบบนาอีฟและเบย์เซียน [5]

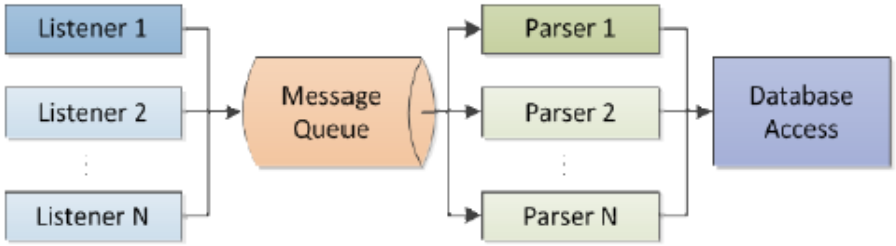
Lun-feng และคณะกล่าวว่าเรามีข้อมูลการดำเนินการทั้งในอดีตและปัจจุบันเป็นจำนวนมาก เช่น ฐานข้อมูลสารสนเทศของผู้ใช้ ฐานข้อมูลการโทร ฐานข้อมูลการแจ้งบิล และฐานข้อมูลอื่นๆ ในอุตสาหกรรมด้านโทรคมนาคมโดยทำการใช้ฐานข้อมูลเหล่านี้และใช้การจำแนกแบบนาอีฟและเบย์เซียน เราสามารถค้นหาการดำเนินการของแต่ละฝ่ายจากข้อมูลในอดีต ทำนายแนวทางในอนาคตและวิเคราะห์นิสัยในการจ่ายเงินของลูกค้าจากข้อมูลที่ผ่านมาในอดีต กำหนดให้ X คือข้อมูลตัวอย่างด้วยคลาสที่ไม่ทราบและ H คือชนิดของสมมติฐาน สำหรับการจำแนกจะต้องทำการระบุค่า P(H/X) โดยเป็นค่าความน่าจะเป็นภายหลังของ H ภายใต้เงื่อนไข X ในการลักลอบใช้โทรศัพท์แบบใช้สายในระยะทางไกล จะอาศัยข้อมูลการวิเคราะห์อัตราการเติบโตด้านการโทร ความถี่ในการโทร ค่าใช้จ่ายรายเดือนที่สูงขึ้น และเครดิตของลูกค้า ในทางตรงกันข้าม P(H) คือความน่าจะเป็นก่อนของ H ค่าของ P(H/X) ตั้งอยู่บนพื้นฐานของข้อมูลที่มีปริมาณมาก มากกว่าค่าความน่าจะเป็นก่อน P(H) ขณะที่ความน่าจะเป็นก่อน P(H) ไม่ขึ้นกับ X เหมือนๆกับว่า P(X/H) คือความน่าจะเป็นหลังของ X ภายใต้เงื่อนไข H หรือพูดอีกนัยว่าจะรู้ว่า X คือกลุ่มของลูกค้าประเภทไหน ในการออกแบบตัวแบบของระบบ โครงสร้างของระบบจะแบ่งออกเป็น 5 ส่วน ได้แก่ ส่วนติดต่อผู้ใช้ ส่วนกรองข้อมูล ส่วนประมวลผลข้อมูล ส่วนตรวจจับ และส่วนประมวลผลหลัก โดยรายละเอียดดังภาพที่ 2.10 โดยผลการทดลองพบว่ามีอัตราการตรวจจับได้มากกว่า 90%



ภาพที่ 2.9 โครงสร้างของระบบป้องกันการลักลอบใช้บนพื้นฐานของการจำแนกแบบนาอีฟและเบย์เซียน

2.6.3 โมเดลการตรวจจับการลักลอบโทร [6]

ระบบ STR ถูกเขียนด้วยภาษาจาวา โดยใช้ jNetPcap wrapper สำหรับ libpcap/ WinPcap โดยระบบ STR นี้จะสามารถใช้ได้กับหลายๆแพลตฟอร์ม มีการออกแบบซอฟต์แวร์ในเชิงวัตถุซึ่งง่ายต่อการขยายเพิ่มและการปรับเปลี่ยนไปยังแอพพลิเคชันที่แตกต่างกัน ฟังก์ชันการทำงานของระบบ STR ประกอบด้วย 3 โมดูลที่แตกต่างกัน โมดูลแรกจะเป็นตัวที่คอยรับ (Listener) ทำการตรวจจับทราฟฟิคบนโครงข่ายและทำการกรองเฉพาะข้อมูล SIP โดยข้อมูล SIP ถูกส่งผ่านไปยังโมดูลที่สองที่เรียกว่าพาสเซอร์ (Parser) ซึ่งจะทำการสกัดค่าของส่วนหัว (Header) ของ SIP ข้อความในคิวจะถูกใช้ในการส่งผ่านจากส่วนตัวรับมายังส่วนตัวแยกวิเคราะห์ ซึ่งจากหลักการนี้เองจะเป็นประโยชน์ว่าส่วนตัวรับและตัวแยกวิเคราะห์จะทำงานได้พร้อมๆ กันและการที่มีซีพียูหลายๆ ตัวสามารถนำมาใช้ประโยชน์ได้ นอกจากนี้แล้วส่วนตัวรับและพาสเซอร์จะไม่ได้จำกัดที่หนึ่งงานต่อโมดูล หนึ่งคิวข้อความสามารถที่จะถูกใช้โดยหลายๆตัวรับที่ทำงานสอดคล้องกันหรือตัวแยกวิเคราะห์หลายตัว ข้อมูลที่ถูกสกัดจะทำการจัดเก็บลงไปยังระบบฐานข้อมูลที่มีความสัมพันธ์กันโดยโมดูลที่สามสำหรับการวิเคราะห์ต่อมา และเลือกที่จะเข้ารหัสได้

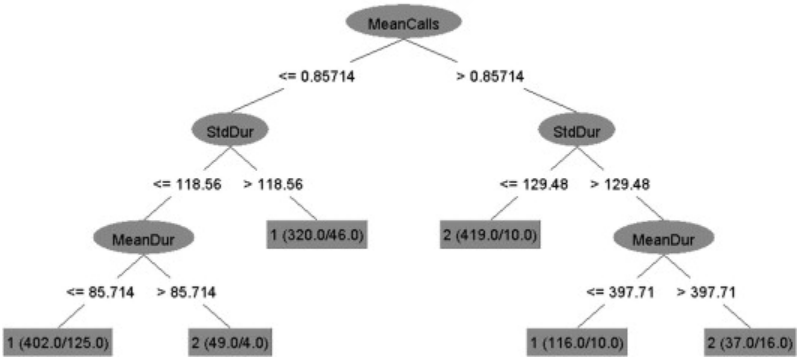


ภาพที่ 2.10 การไหลของข้อมูลภายในระบบ STR

จากภาพที่ 2.11 แสดงการไหลของข้อมูล SIP ระหว่าง 3 โมดูล อย่างน้อยจะมี 1 โมดูลของการรับที่จะทำการเก็บข้อมูลและทำการจัดคิวให้กับระบบ อินสแตนท์จำนวนหนึ่งตัวหรือมากกว่าของตัวแยกวิเคราะห์โมดูลจะทำการกรองข้อมูล SIP และทำการจัดเก็บลงในโมดูลฐานข้อมูล คุณสมบัติและฟังก์ชันการทำงานของทั้ง 3 โมดูลนี้ ได้แก่ เว็บอินเตอร์เฟสถูกใช้สำหรับการวิเคราะห์แบบอัตโนมัติของการบันทึกข้อมูล ในส่วนโมดูลการวิเคราะห์ประกอบด้วยหลายปลั๊กอิน ปลั๊กอินแต่ละอันจะรันคำสั่งที่แตกต่างกัน เช่น SIP แพ็กเกจต่อวันหรือแผนภูมิตำแหน่งทางภูมิศาสตร์ ที่มีผลการตรวจแสดงบนเว็บไซต์ของการจัดการ ปลั๊กอินจะขึ้นอยู่กับคำสั่ง SQL และภาษา และได้กำหนดกลุ่มการโจมตีต่อไปนี้เพื่อให้ได้รับความเข้าใจที่ดีขึ้นของการพยายามโจมตีที่เกิดขึ้น ได้แก่ การสแกนหาเครื่องแม่ข่าย สแกนเบอร์ต่อ การลงทะเบียนและการลักลอบโทร ในขณะที่การโจมตีถูกจัดกลุ่มโดยที่มาของ IP Address การโจมตีถูกนับเป็นสองความพยายามที่จะโจมตีหากแหล่ง IP มีการเปลี่ยนแปลงที่อยู่ในระหว่างการโจมตี ในระหว่างการวิจัยยังไม่ได้สนใจการเปลี่ยนแปลงใดๆ ของที่อยู่ IP ในระหว่างขั้นตอนการโจมตี โดยการจัดกลุ่มที่เกี่ยวข้องของข้อความและการไม่คำนึงถึงจำนวนข้อความที่เราได้รับมุมมองที่ชัดเจนของความพยายามการโจมตีที่เกิดขึ้นจริง

2.6.4 การประยุกต์เหมืองข้อมูล

ในงานวิจัยเรื่องการออกแบบระบบผู้เชี่ยวชาญในการตรวจจับการลักลอบใช้ในโครงข่ายโทรคมนาคมเฉพาะ [9] ได้ทำการศึกษาโดยเป้าหมายคือกลุ่มโทรศัพท์สำหรับองค์กร (Hosted PBX) ซึ่งมีผู้ใช้งานมากกว่า 5,000 คน โดยได้ทำการใช้ขั้นตอนวิธี C4.5 ในการจำแนกประเภทการโทรออกเป็น 2 กลุ่ม ได้แก่ กลุ่มการใช้งานปกติ และกลุ่มที่ใช้งานแบบผิดปกติ ซึ่งเป็นการจำแนกเป็นรายสัปดาห์ดังภาพที่ 2.12



ภาพที่ 2.11 แผนภาพโครงสร้างต้นไม้การตัดสินใจ

โดยค่าที่พิจารณาคือ ค่าเฉลี่ยของจำนวนครั้งการโทร ส่วนเบี่ยงเบนมาตรฐานของเวลาในการโทร และค่าเฉลี่ยของเวลาในการโทร ซึ่งข้อมูลการใช้งานของผู้ใช้หากพบว่ามีการเปลี่ยนแปลงหรือเบี่ยงเบนไปมากก็จะมีโอกาสเข้าข่ายว่าเป็นการลักลอบใช้ โดยในการออกแบบระบบผู้เชี่ยวชาญจะอาศัยกฎที่ได้จากข้างต้นไปทำการประเมิน

จากการศึกษางานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์ที่นำเสนอ สามารถเปรียบเทียบความสามารถของระบบ แต่ละงานวิจัยได้ดังตารางที่ 2.3

ตารางที่ 2.3 แสดงการเปรียบเทียบความสามารถของระบบแต่ละงานวิจัยที่เกี่ยวข้องกับวิทยานิพนธ์ที่นำเสนอ

ลำดับ	ความสามารถของระบบ	โมเดลการตรวจจับโดยใช้โครงข่ายประสาทเทียม	โมเดลการจำแนกนาอีฟและเบย์เซียน	โมเดลการตรวจจับด้วยโมดูล STR	วิทยานิพนธ์ที่นำเสนอ
1	สามารถตรวจจับในลักษณะแบบ Real Time	✓	✓	✓	✓
2	สามารถพยากรณ์ได้ว่าอาจมีการเกิดการลักลอบใช้งาน	✓	✓		✓
3	สามารถแสดงผลการตรวจจับได้ในรูปแบบของเว็บแอพพลิเคชัน			✓	✓
4	สามารถเชื่อมต่อเข้ากับระบบโครงข่ายโดยผ่านอุปกรณ์จัดเก็บข้อมูลการโทร				✓

ตารางที่ 2.3 (ต่อ)

ลำดับ	ความสามารถของระบบ	โมเดลการตรวจจับโดยใช้โครงข่ายประสาทเทียม	โมเดลการจำแนกนาอีฟและเบย์เซียน	โมเดลการตรวจจับด้วยโมดูล STR	วิทยานิพนธ์ที่นำเสนอ
5	สามารถประมวลผลข้อมูลการโทรแบบคู่ขนาน (Parallel)			✓	✓
	สามารถแสดงผลรายงานออกมาเป็นกราฟและตาราง				✓
7	สามารถแจ้งเตือนกรณีการเกิดการลักลอบใช้ผ่านทาง E-mail ของผู้ดูแลระบบ				✓
8	สามารถเชื่อมต่อเพื่อใช้ตรวจจับการลักลอบใช้กับโครงข่ายอื่น				✓

สรุป

จากงานวิจัยที่ได้ศึกษามายังมีส่วนที่สามารถพัฒนาต่อได้ดังนี้คือ การเชื่อมต่อเข้ากับเครื่องแม่ข่ายจัดเก็บข้อมูลการโทร การประมวลผลข้อมูลเบื้องต้น การแสดงผลรายงานออกมาเป็นกราฟและตาราง การแจ้งเตือนกรณีการเกิดการลักลอบใช้ผ่านทาง E-mail ของผู้ดูแลระบบ และเชื่อมต่อเพื่อใช้ตรวจจับการลักลอบใช้กับโครงข่ายอื่น ในส่วนของงานวิจัยที่นำเสนอนี้ได้นำเอาส่วนที่สามารถพัฒนาต่อได้ของงานวิจัยที่ได้ศึกษา มาทำการพัฒนาต่อยอด เพื่อให้การตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็นมีประสิทธิภาพที่ดียิ่งขึ้น นอกจากนี้แล้วยังมีส่วนของการนำตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียมมาประยุกต์ในงานวิจัยนี้ด้วย

บทที่ 3
การดำเนินงาน

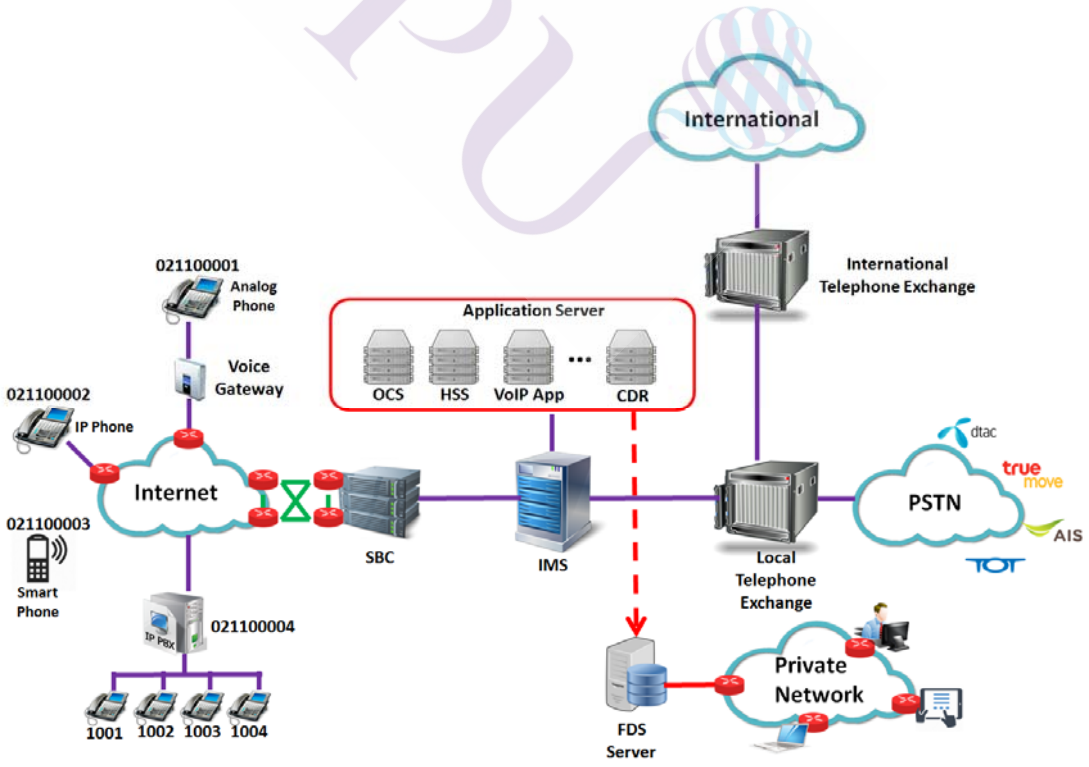
เนื้อหาในส่วนนี้จะประกอบไปด้วยส่วนของการวิเคราะห์และออกแบบภาพรวมของงานวิจัย ซึ่งมีหัวข้อดังต่อไปนี้

3.1 ภาพรวมการทำงานของระบบ (System Overview)

3.2 การออกแบบระบบ (System Design)

3.1 ภาพรวมการทำงานของระบบ

ในการทำงานของระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็นนั้นประกอบไปด้วย 3 ส่วนหลักๆ ได้แก่ ส่วนการประมวลผลข้อมูลที่ได้จากเครื่องแม่ข่ายจัดเก็บข้อมูลการโทร (CDR Server) ส่วนการประมวลผลข้อมูลการตรวจจับการลักลอบใช้บริการ และส่วนการให้บริการข้อมูลผ่านเครื่องแม่ข่าย โดยรายละเอียดดังภาพที่ 3.1



ภาพที่ 3.1 แผนภาพโครงข่ายระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น

จากภาพที่ 3.1 เป็นแผนภาพแสดงโครงข่ายเอ็นจีเอ็นซึ่งมีอุปกรณ์ที่สำคัญได้แก่ เอสบีซี (SBC: Session Border Controller) ทำหน้าที่เป็นหน้าด่านในการเข้ามาใช้งานของโทรศัพท์ โดยควบคุมการเข้าออกของการโทร การลงทะเบียนเข้าใช้ระบบ การควบคุมจำนวนการโทรพร้อมกันของเลขหมาย การควบคุมไอพีแอดเดรสที่เข้ามา เป็นต้น อุปกรณ์ต่อมาที่มีความสำคัญมากในระบบคือ ไอเอ็มเอส (IMS : IP Multimedia Subsystem) เป็นตัวเชื่อมต่อที่หลอมรวมระบบมัลติมีเดียเข้าด้วยกันทำให้สามารถควบคุมและบริหารจัดการได้ง่าย นอกจากนี้ยังมีในส่วนอุปกรณ์ที่ทำหน้าที่เป็นเครื่องแม่ข่ายแอพพลิเคชัน โดยระบบการทำงานเริ่มจากเลขหมายมีการเข้ามาลงทะเบียนกับระบบก่อนที่จะมีการเรียกเข้าหรือโทรออก โดยทุกๆ ครั้งที่มีการเรียกเข้าหรือโทรออก จะมีการบันทึกข้อมูลการโทรหรือที่เรียกอีกอย่างว่าซีดีอาร์ (CDR: Call Detail Record) ซึ่งจะเป็นข้อมูลที่สามารถนำไปใช้ประโยชน์ เช่น การทำบิลเรียกเก็บค่าใช้งาน การนำไปตรวจสอบคุณภาพบริการการจ่ายส่วนแบ่งทางโทรคมนาคม และโดยเฉพาะอย่างยิ่งของงานวิจัยนี้คือการนำไปใช้ตรวจสอบความผิดปกติของการใช้งาน

ในการทำงานของระบบเริ่มจากเครื่องแม่ข่ายระบบตรวจจักการลักลอบใช้บริการ (FDS: Fraud Detection System) ทำหน้าที่ในการรวบรวมข้อมูลการโทรที่ได้จากอุปกรณ์จัดเก็บข้อมูลการโทร โดยลักษณะของข้อมูลจะอยู่ในรูปแบบของไฟล์ข้อความ (Text File) ซึ่งถูกแปลงจากรูปแบบไฟล์ ASN.1 มาเป็น ASCII ก่อนที่จะนำไปประมวลต่อ โดยข้อมูลที่สำคัญได้แก่ เบอร์ต้นทาง เบอร์ปลายทาง ระยะเวลาการโทร เวลาที่โทร เป็นต้น ซึ่งจะนำมาเข้าจัดเก็บบนฐานข้อมูลเอสคิวแอลเซิร์ฟเวอร์ (SQL Server) จากนั้นจะทำการประมวลผลข้อมูลเบื้องต้นในรูปแบบที่ต้องการนำไปเป็นข้อมูลนำเข้าสำหรับตัวแบบที่ทำการออกแบบ เมื่อได้ข้อมูลจากการประมวลผลเบื้องต้นแล้วจะผ่านขั้นตอนของการฝึกสอน (Training) กรณีที่เป็นความรู้ใหม่หรือการเพิ่มข้อมูลความรู้ที่ได้เข้าไปยังระบบ จากนั้นจะทำการทดสอบเพื่อที่จะทราบว่ามีการลักลอบใช้งานหรือไม่ โดยเบื้องต้นในขั้นตอนการปฏิบัติจะมีการโทรสอบถามถึงการใช้งานจากลูกค้าว่าเป็นการใช้งานจริงหรือไม่ หากพบว่าลูกค้าไม่ได้ใช้งานแต่เกิดลักษณะผิดปกติขึ้น ก็จะทำการระงับเลขหมายนั้นไว้ชั่วคราวเพื่อป้องกันการสูญเสียที่เกิดขึ้น

3.2 การออกแบบระบบ

ในการออกแบบระบบนั้นประกอบไปด้วย การออกแบบตัวแบบในการตรวจจับการลักลอบใช้งานบนโครงข่ายเอ็นจีเอ็น การออกแบบตัวแบบความสัมพันธ์ระหว่างข้อมูล การออกแบบผังการทำงานของระบบ และการออกแบบส่วนต่อประสานกับผู้ใช้

3.2.1 การออกแบบตัวแบบในการตรวจจับการลักลอบใช้งานบนโครงข่ายเอ็นจีเอ็น

ในการออกแบบระบบตรวจจับการลักลอบใช้งานจะประกอบด้วยตัวแบบในการตรวจจับ 4 รูปแบบ โดยมีรายละเอียดดังนี้

1) การใช้งานเป็นเวลานานจนเกิดผิดสังเกต (Long call duration)

โดยปกติแล้วทางชุมสายจะมีการตั้งค่าไว้ที่ประมาณ 30 นาที หากมากกว่านี้ถือว่ามีการใช้งานที่นาน นอกจากจะดูจากค่าดังกล่าวแล้ว จะต้องเทียบดูสถิติหรือแนวโน้มในการใช้งานของลูกค้าประกอบด้วย ดังนั้นในระบบที่ออกแบบจะทำการเก็บสะสมค่าสถิติการใช้งานย้อนหลัง 1 ปี เพื่อเป็นข้อมูลในการประกอบการตัดสินใจว่าเป็นการใช้งานที่ผิดปกติหรือไม่

2) การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง

ระบบจะทำการตรวจสอบจากกลุ่มประเทศโดยดูจากเลขหมายที่ถูกเรียกใช้งาน ซึ่งระบบจะทำการกรองจากรหัสประเทศ หากเป็นประเทศที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยงซึ่งเป็นประเทศที่มีค่าบริการสูงๆ เช่น ซิมบับเว หรือประเทศในทวีปแอฟริกาใต้ เป็นต้น

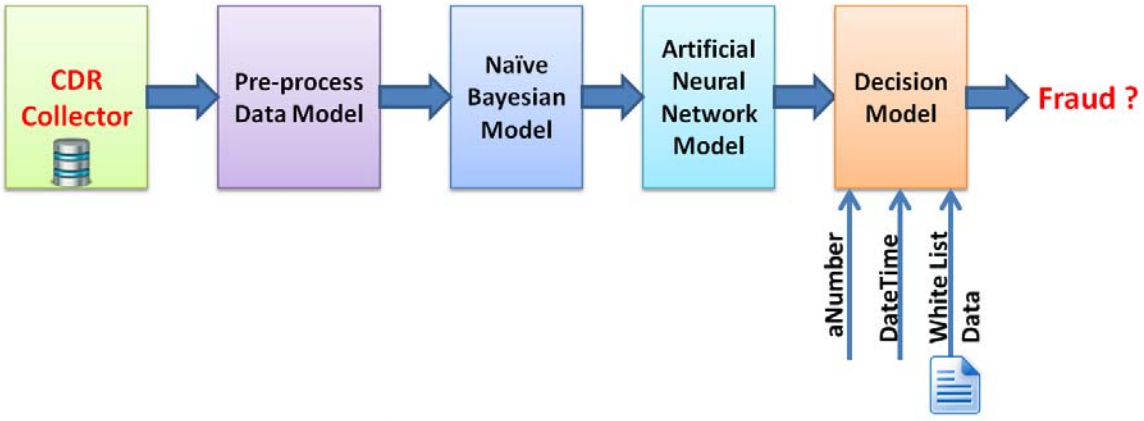
3) การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด

ค่ามาตรฐานต่างๆได้แก่ ยอดเงินที่ใช้ต่อชั่วโมง ปริมาณการเรียกออกต่อชั่วโมง การเปลี่ยนไอพีในการขอเข้าใช้งานบ่อย

4) การมีพฤติกรรมการโทรแปลกๆ โดยมีการเข้ามาตรวจสอบโครงข่ายแล้วกระหน่ำโทร

ระบบจะดูจากความถี่ในการโทร เช่น 1 นาที มีการกดสายเรียกออกในปริมาณที่มากเกินกว่าที่มนุษย์ทั่วไปจะทำได้ ซึ่งโดยส่วนใหญ่แล้วจะเป็นการใช้เครื่องแม่ข่ายทำการส่งคำร้องขอมาที่ระบบในปริมาณที่มาก หรือเป็นการปล่อยให้มีการจราจรบนโครงข่ายเอ็นจีเอ็นในปริมาณที่หนาแน่น

นอกจากตัวแบบทั้ง 4 ตัวแบบที่ทำการออกแบบแล้วยังมีในส่วนของตัวแบบที่ช่วยในการวิเคราะห์แนวโน้มทางสถิติของการเกิดการลักลอบใช้งานบนโครงข่ายนั้นได้ทำการออกแบบโดยวิธีการทำงานร่วมกันระหว่างตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียม (NBANN: Naïve Bayesian and Artificial Neural Network) โดยการผสมผสานกันในการคำนวณค่าความน่าจะเป็นของการเกิดการลักลอบใช้บริการบนโครงข่าย โดยมีรายละเอียดของตัวแบบดังภาพที่ 3.2



ภาพที่ 3.2 แผนภาพตัวแบบที่ทำการออกแบบในการวิเคราะห์แนวโน้มโอกาสที่จะเกิดการลักลอบใช้

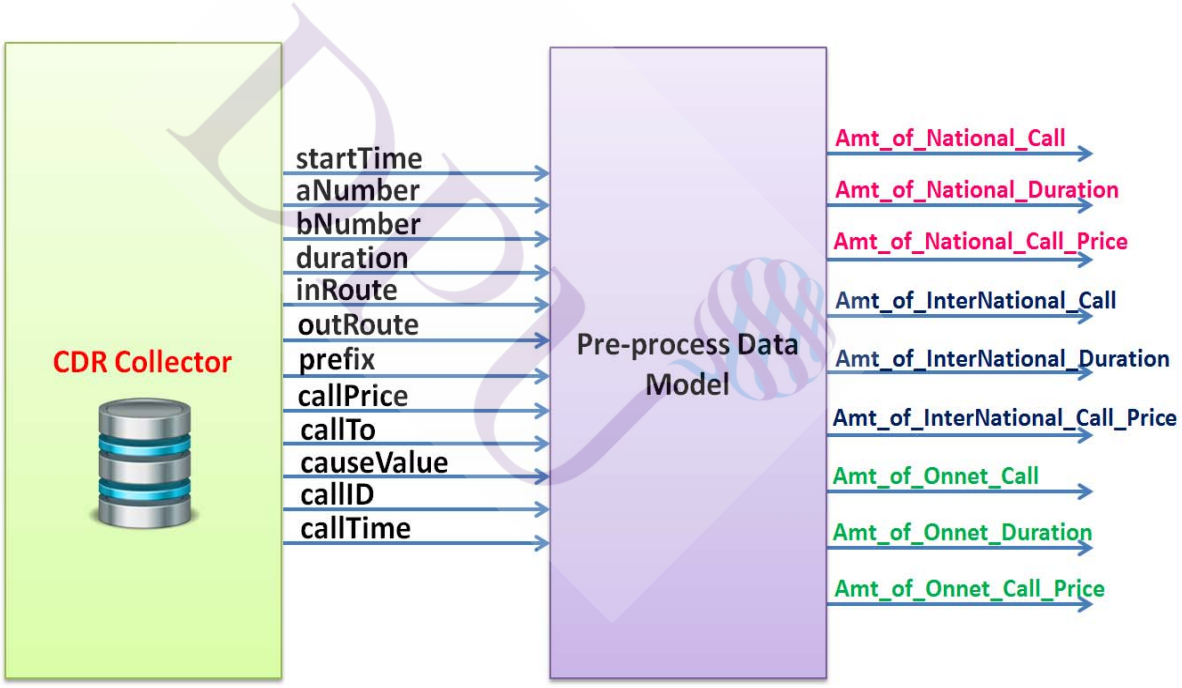
จากภาพที่ 3.2 เริ่มจากการดึงข้อมูลการโทรจากอุปกรณ์เครื่องแม่ข่ายในการจัดเก็บข้อมูลการโทรหรืออุปกรณ์รวบรวมข้อมูลการโทร (CDR Collector) เพื่อนำไปประมวลผลจัดเก็บในรูปแบบของฐานข้อมูล จากนั้นจะทำการประมวลผลข้อมูลเบื้องต้นให้อยู่ในรูปแบบที่ต้องการเพื่อใช้สำหรับการนำเข้าไปคำนวณในตัวแบบนาอีฟย์เบย์เซียน ในส่วนของโมดูลการคำนวณนาอีฟย์เบย์เซียนจะทำการประมวลผลข้อมูลเพื่อใช้เป็นข้อมูลนำเข้าของโมดูลตัวแบบโครงข่ายประสาทเทียมต่อไป เมื่อตัวแบบโครงข่ายประสาทเทียมทำการคำนวณผลออกมา จะทราบได้ว่าข้อมูลใดเป็นการลักลอบใช้หรือไม่ โดยอาศัยข้อมูลที่ได้จากการฝึกหัดเพื่อให้ได้ค่าน้ำหนัก (Weight) ที่เหมาะสมของโครงข่ายประสาทเทียมไปคำนวณ

ในการเลือกพารามิเตอร์สำหรับแต่ละโมดูลนั้นเริ่มจากในส่วนของการประมวลผลเบื้องต้นซึ่งเป็นการนำข้อมูลดิบที่มาจากรายละเอียดข้อมูลการโทรมาทำการประมวลผลเพื่อให้ได้ข้อมูลที่จำเป็นสำหรับการนำไปวิเคราะห์โดยการนำข้อมูลเข้าสู่โมดูลนาอีฟเบย์เซียนนั้นประกอบไปด้วยข้อมูลการโทรระหว่างโครงข่ายทั้งในและต่างประเทศ รวมถึงการโทรภายในโครงข่ายเดียวกัน โดยข้อมูลที่สำคัญในการนำไปวิเคราะห์คือ จำนวนการโทร ระยะเวลาการโทร ราคาค่าโทร ซึ่งเป็นปัจจัยหลักในการนำไปพิจารณาการเกิดการลักลอบหรือไม่ เมื่อทำการคำนวณในส่วนของโมดูลนาอีฟเบย์เซียนเสร็จแล้วจะได้ข้อมูลปัจจัยการโทรซึ่งจะได้เป็นข้อมูลพารามิเตอร์ของภาพรวมการโทรในประเทศ ระหว่างประเทศ และการโทรภายในโครงข่ายเดียวกัน ซึ่งจะเป็นปัจจัยที่สำคัญสำหรับการนำเข้าไปสู่โมดูลโครงข่ายประสาทเทียม นอกจากนี้แล้วยังมีข้อมูลนำเข้า

อีก 1 โหนด ได้แก่ ค่าปัจจัยการโทรไปประเทศกลุ่มเสี่ยง โดยเป็นปัจจัยหลักในการเข้าสู่กระบวนการฝึกหัดเพื่อให้ได้จำนวนโหนดซ่อนที่เหมาะสมในการนำไปทดสอบต่อไป

ในการตัดสินใจว่าเป็นกรณีการเกิดการลักลอบจริงหรือไม่ เมื่อพบว่าค่าผลลัพธ์ที่ออกมาจากการคำนวณทั้งสองตัวแบบแล้วมีค่าเป็นการลักลอบเกิดขึ้น จะอาศัยข้อมูลไวท์ลิสต์ (White List Data) ซึ่งเป็นข้อมูลที่เป็นประวัติกรณีที่เคยเกิดการตรวจจับได้แต่เคยได้รับการยืนยันจากลูกค้าว่าเป็นกรณีที่มีการใช้งานจริง หากพบว่ามีประวัติการใช้งานในลักษณะดังกล่าวจริง ระบบก็จะสามารถแจ้งเตือนให้ทราบโดยไม่ถือว่าเป็นการลักลอบจริง โดยรายละเอียดข้อมูลนำเข้าและส่งออกแต่ละโมดูลมีรายละเอียดดังนี้

1) โมดูลการประมวลผลข้อมูลเบื้องต้น (Pre-process Data Model) ประกอบด้วยข้อมูลนำเข้า ดังภาพที่ 3.3



ภาพที่ 3.3 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูลการประมวลผลข้อมูลเบื้องต้น

โดยความหมายของข้อมูลในส่วนของข้อมูลนำเข้าในส่วนของโมดูลประมวลผลข้อมูลเบื้องต้นดังตารางที่ 3.1

ตารางที่ 3.1 อธิบายความหมายของข้อมูลนำเข้าโมดูลการประมวลผลข้อมูลเบื้องต้น

ข้อมูล	ความหมาย	ตัวอย่าง
startTime	เวลาที่ทำการโทร	2016-26-06 T15:57:34.8+0700
aNumber	เลขหมายต้นทาง	6621053000
bNumber	เลขหมายปลายทาง	00985291270508
Duration	ระยะเวลาการโทรในหน่วยวินาที	25
Cause Value	Release code	16 = Normal Call Clearing
callID	รหัสอ้างอิงการโทร	87dfe6bfef60190baea912da156683c7
inRoute	เส้นทางตั้งต้น	IMS
outRoute	เส้นทางสิ้นสุด	OFFNET_NATL, OFFNET_INTL
Prefix	001/009+รหัสประเทศ+รหัสพื้นที่	0098529
callPrice	ราคาค่าโทร (บาท)	154
callTime	ช่วงเวลาที่โทร (24H)	23
callTo	ประเภทการโทร	INTL

ประเภทของชุมสายที่กำหนดทั้งหมดบนโครงข่ายประกอบด้วยตารางที่ 3.2 และรูปแบบในการคำนวณประเภทการโทร ดังตารางที่ 3.3

ตารางที่ 3.2 ประเภทของชุมสายที่กำหนดทั้งหมดบนโครงข่าย

ชุมสาย	ความหมาย
IMS	เลขหมายนั้นอยู่บนโครงข่าย IMS
OFFNET_NATL	เลขหมายนั้นอยู่นอกโครงข่าย IMS และเป็นเลขหมายภายในประเทศ
OFFNET_INTL	เลขหมายนั้นอยู่นอกโครงข่าย IMS และเป็นเลขหมายต่างประเทศ

ตารางที่ 3.3 รูปแบบในการคำนวณประเภทการโทร

ต้นทาง	ปลายทาง	ประเภทการโทร
IMS	IMS	Onnet (โทรในโครงข่าย)
IMS	OFFNET_NATL	NATL (โทรในประเทศ)
IMS	OFFNET_INTL	INTL (โทรต่างประเทศ)

โดยเมื่อนำข้อมูลนำเข้าไปยังโมดูลการประมวลผลข้อมูลเบื้องต้นแล้ว จะทำการคำนวณโดยมีการแบ่งออกเป็นการคำนวณ 3 อย่าง ได้แก่ การคำนวณลักษณะการโทรในโครงข่ายเดียวกัน การโทรนอกโครงข่ายภายในประเทศ และการโทรนอกโครงข่ายระหว่างประเทศ โดยจะใช้เงื่อนไขการพิจารณาดังต่อไปนี้

การคำนวณลักษณะการโทรในโครงข่ายเดียวกัน

ในการคำนวณลักษณะการโทรในโครงข่ายเดียวกันจะใช้เงื่อนไขหลักคือ ต้นทางเป็นชุมสาย IMS และปลายทางเป็นชุมสาย IMS จากนั้นจะทำการคำนวณผลรวมใน 1 ชั่วโมงของจำนวนครั้งที่โทร ระยะเวลาการโทร และค่าใช้จ่ายในการโทร จากนั้นจะทำการแปลงค่าดังกล่าวให้เป็นค่าที่เหมาะสม โดยในการแปลงจะใช้เงื่อนไขดังตารางที่ 3.4

ตารางที่ 3.4 การแทนค่าพารามิเตอร์สำหรับการโทรภายในโครงข่ายเดียวกัน

พารามิเตอร์	ความหมาย	การแทนค่า
Amt_of_Onnet_Call	ระดับจำนวนการโทรในโครงข่าย	1 แทน LOW (0-9 Calls) 2 แทน MEDIUM (10-99 Calls) 3 แทน HIGH (>=100 Calls)
Amt_of_Onnet_Duration	ระดับระยะเวลาการโทรในโครงข่าย	1 แทน SHORT (0-15 Minutes) 2 แทน MEDIUM (16-30 Minutes) 3 แทน LONG (>30 Minutes)
Amt_of_Onnet_Call_Price	ระดับค่าใช้จ่ายในการโทรในโครงข่าย	1 แทน LOW (0-99 บาท) 2 แทน MEDIUM (100-500 บาท) 3 แทน HIGH (>500 บาท)

ก) การคำนวณลักษณะการโทรนอกโครงข่ายภายในประเทศ

ในการคำนวณลักษณะการโทรนอกโครงข่ายภายในประเทศจะใช้เงื่อนไขหลักคือ ต้นทางเป็นชุมสาย IMS และปลายทางเป็นชุมสาย OFFNET_NATL จากนั้นจะทำการคำนวณผลรวมใน 1 ชั่วโมงของจำนวนครั้งที่โทร ระยะเวลาการโทร และค่าใช้จ่ายในการโทร จากนั้นจะทำการแปลงค่าดังกล่าวให้เป็นค่าที่เหมาะสม โดยในการแปลงจะใช้เงื่อนไขดังตารางที่ 3.5

ตารางที่ 3.5 การแทนค่าพารามิเตอร์สำหรับการโทรนอกโครงข่ายภายในประเทศ

พารามิเตอร์	ความหมาย	การแทนค่า
Amt_of_National_Call	ระดับจำนวนการโทรนอกโครงข่ายภายในประเทศ	1 แทน LOW (0-9 Calls) 2 แทน MEDIUM (10-99 Calls) 3 แทน HIGH (>=100 Calls)
Amt_of_National_Duration	ระดับระยะเวลาการโทรนอกโครงข่ายภายในประเทศ	1 แทน SHORT (0-15 Minutes) 2 แทน MEDIUM (16-30 Minutes) 3 แทน LONG (>30 Minutes)
Amt_of_National_Call_Price	ระดับค่าใช้จ่ายในการโทรนอกโครงข่ายภายในประเทศ	1 แทน LOW (0-99 บาท) 2 แทน MEDIUM (100-500 บาท) 3 แทน HIGH (>500 บาท)

ข) การคำนวณลักษณะการโทรนอกโครงข่ายระหว่างประเทศ

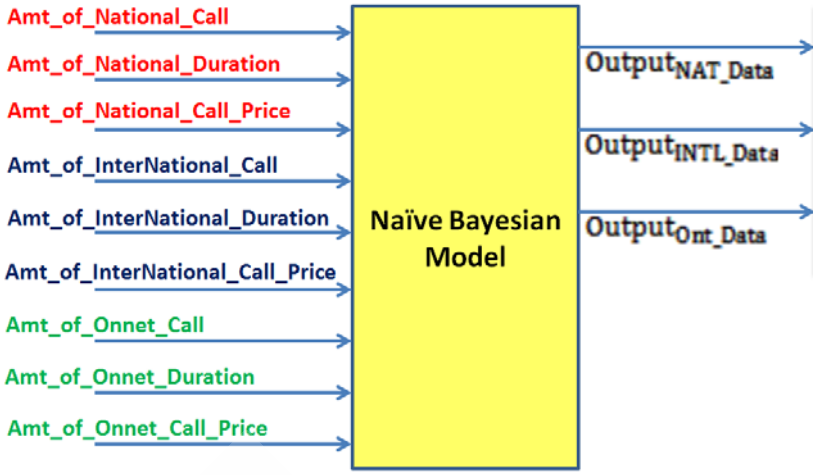
ในการคำนวณลักษณะการโทรนอกโครงข่ายระหว่างประเทศจะใช้เงื่อนไขหลักคือ ต้นทางเป็นชุมสาย IMS และปลายทางเป็นชุมสาย OFFNET_INTL จากนั้นจะทำการคำนวณผลรวมใน 1 ชั่วโมงของจำนวนครั้งที่โทร ระยะเวลาการโทร และค่าใช้จ่ายในการโทร จากนั้นจะทำการแปลงค่าดังกล่าวให้เป็นค่าที่เหมาะสม โดยในการแปลงจะใช้เงื่อนไขดังตารางที่ 3.6

ตารางที่ 3.6 การแทนค่าพารามิเตอร์สำหรับการโทรนอกโครงข่ายระหว่างประเทศ

พารามิเตอร์	ความหมาย	การแทนค่า
Amt_of_InterNational_Call	ระดับจำนวนการโทรนอกโครงข่ายระหว่างประเทศ	1 แทน LOW (0-9 Calls) 2 แทน MEDIUM (10-99 Calls) 3 แทน HIGH (>=100 Calls)
Amt_of_InterNational_Duration	ระดับระยะเวลาการโทรนอกโครงข่ายระหว่างประเทศ	1 แทน SHORT (0-15 Minutes) 2 แทน MEDIUM (16-30 Minutes) 3 แทน LONG (>30 Minutes)
Amt_of_InterNational_Call_Price	ระดับค่าใช้จ่ายในการโทรนอกโครงข่ายระหว่างประเทศ	1 แทน LOW (0-99 บาท) 2 แทน MEDIUM (100-500 บาท) 3 แทน HIGH (>500 บาท)

1) โมดูลตัวแบบนาอีฟเบย์เซียน

หลังจากที่ได้ทำการประมวลผลข้อมูลเบื้องต้นแล้ว จะเข้าสู่ตัวแบบนาอีฟเบย์เซียนเพื่อทำการคำนวณในการนำเข้าสู่ตัวแบบโครงข่ายประสาทเทียมต่อไป โดยข้อมูลนำเข้าจะได้มาจากโมดูลการประมวลผลข้อมูลเบื้องต้น ประกอบด้วย ระดับการโทร ระยะเวลาการโทร และค่าใช้จ่ายในการโทร ทั้งในส่วนของการโทรภายในโครงข่างเดียวกัน การโทรนอกโครงข่ายภายในประเทศ และการโทรนอกโครงข่ายระหว่างประเทศ โดยในการคำนวณในส่วนของตัวแบบนาอีฟเบย์เซียนจะทำการคำนวณเพื่อให้ได้ค่าพารามิเตอร์ที่เหมาะสมของแต่ละประเภทการโทร ดังภาพที่ 3.4 และในส่วนของข้อมูลส่งออกมีรายละเอียดดังตารางที่ 3.7



ภาพที่ 3.4 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูลตัวแบบนาอีฟเบย์เซียน

ตารางที่ 3.7 ข้อมูลส่งออกสำหรับส่วนของตัวแบบนาอีฟเบย์เซียน

พารามิเตอร์	ความหมาย	การแทนค่า
$Output_{\text{NAT\_Data}}$	ข้อมูลค่าปัจจัยในการโทรนอกโครงข่ายภายในประเทศ	1 แทน LOW 2 แทน MEDIUM 3 แทน HIGH
$Output_{\text{INTL\_Data}}$	ข้อมูลค่าปัจจัยในการโทรนอกโครงข่ายระหว่างประเทศ	1 แทน LOW 2 แทน MEDIUM 3 แทน HIGH
$Output_{\text{Ont\_Data}}$	ข้อมูลค่าปัจจัยในการโทรภายในโครงข่ายเดียวกัน	1 แทน LOW 2 แทน MEDIUM 3 แทน HIGH

ในส่วนของการคำนวณเพื่อให้ได้ค่าพารามิเตอร์ที่เหมาะสม มีรายละเอียดในการคำนวณดังนี้

ก) ทำการประเมินค่าประเภทการโทรภายในประเทศ

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของจำนวนการโทรในประเทศ

$$P(Fraud|nCallNAT) = P(Fraud) \times P(nCallNAT_{LOW}|Fraud) \times P(nCallNAT_{MED}|Fraud) \times P(nCallNAT_{HIGH}|Fraud)$$

$$= \frac{nCallNAT_{Fraud}}{nCallFraud} \times \frac{nCallNAT_{LOW}}{nCallNAT_{Fraud}} \times \frac{nCallNAT_{MED}}{nCallNAT_{Fraud}} \times \frac{nCallNAT_{HIGH}}{nCallNAT_{Fraud}}$$

$$= P_1 \quad (3.1)$$

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของระยะเวลาการโทรในประเทศ

$$P(Fraud|DuraNAT) = P(Fraud) \times P(DuraNAT_{LOW}|Fraud) \times P(DuraNAT_{MED}|Fraud) \times P(DuraNAT_{HIGH}|Fraud)$$

$$= \frac{nCallNAT_{Fraud}}{nCallFraud} \times \frac{nDuraNAT_{SHORT}}{nCallNAT_{Fraud}} \times \frac{nDuraNAT_{MED}}{nCallNAT_{Fraud}} \times \frac{nDuraNAT_{LONG}}{nCallNAT_{Fraud}}$$

$$= P_2 \quad (3.2)$$

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของราคาการโทรในประเทศ

$$P(Fraud|PriceNAT) = P(Fraud) \times P(PriceNAT_{LOW}|Fraud) \times P(PriceNAT_{MED}|Fraud) \times P(PriceNAT_{HIGH}|Fraud)$$

$$= \frac{nCallNAT_{Fraud}}{nCallFraud} \times \frac{nPriceNAT_{LOW}}{nCallNAT_{Fraud}} \times \frac{nPriceNAT_{MED}}{nCallNAT_{Fraud}} \times \frac{nPriceNAT_{HIGH}}{nCallNAT_{Fraud}}$$

$$= P_3 \quad (3.3)$$

$$Sum_{Weight}(NAT) = \sum_{i=1}^{3} P_i$$

$$= P_1 + P_2 + P_3 \quad (3.4)$$

$$W_{nCallNAT} = \frac{P_1}{Sum_{Weight}(NAT)} \quad (3.5)$$

$$W_{DuraNAT} = \frac{P_2}{Sum_{Weight}(NAT)} \quad (3.6)$$

$$W_{callPriceNAT} = \frac{P_3}{Sum_{Weight}(NAT)} \quad (3.7)$$

$$Output_{NAT\_Data} = \lceil (Input_{nCallNAT} \times W_{nCallNAT}) + (Input_{DuraNAT} \times W_{DuraNAT}) + (Input_{callPriceNAT} \times W_{callPriceNAT}) \rceil \quad (3.8)$$

โดย

$Output_{NAT\_Data}$ คือค่าที่ได้จากการคำนวณด้วยปัจจัยที่มีผลต่อการนำเข้าไปยังโมเดลโครงข่ายประสาทเทียม

$Sum_{Weight}(NAT)$ คือค่าผลรวมความน่าจะเป็นที่เกิดการลักลอบใช้ในแต่ละเหตุการณ์ของการโทรในประเทศ

$W_{nCallNAT}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของจำนวนการโทรในประเทศ

$W_{DuraNAT}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของระยะเวลาการโทรในประเทศ

$W_{callPriceNAT}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของราคาการโทรในประเทศ

$nCallNAT_{Fraud}$ คือจำนวนครั้งของการโทรภายในประเทศและเป็นการลักลอบใช้

$nCallFraud$ คือจำนวนครั้งของการเกิดการลักลอบใช้ทั้งหมด

$nCallNAT_i$ คือจำนวนของการโทรในระดับที่ $i \in \{LOW, MEDIUM, HIGH\}$

$nPriceNAT_i$ คือจำนวนของการโทรในระดับที่ $i \in \{LOW, MEDIUM, HIGH\}$

$nDuraNAT_i$ คือจำนวนของการโทรในระดับที่ $i \in \{SHORT, MEDIUM, LONG\}$

ก) ทำการประเมินค่าประเภทการโทรไปยังต่างประเทศ

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของจำนวนการโทรไปยังต่างประเทศ

$$P(Fraud|nCallINTL)$$
$$= P(Fraud) \times P(nCallINTL_{LOW}|Fraud) \times P(nCallINTL_{MED}|Fraud) \times P(nCallINTL_{HIGH}|Fraud)$$
$$= \frac{nCallINTL_{Fraud}}{nCallFraud} \times \frac{nCallINTL_{LOW}}{nCallINTL_{Fraud}} \times \frac{nCallINTL_{MED}}{nCallINTL_{Fraud}} \times \frac{nCallINTL_{HIGH}}{nCallINTL_{Fraud}}$$
$$= P_1 \quad (3.9)$$

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของระยะเวลาการโทรไปยังต่างประเทศ

$$P(Fraud|DuraINTL)$$
$$= P(Fraud) \times P(DuraINTL_{LOW}|Fraud) \times P(DuraINTL_{MED}|Fraud) \times P(DuraINTL_{HIGH}|Fraud)$$

$$= \frac{nCallINTL_{Fraud}}{nCallFraud} \times \frac{nDuraINTL_{SHORT}}{nCallINTL_{Fraud}} \times \frac{nDuraINTL_{MED}}{nCallINTL_{Fraud}} \times \frac{nDuraINTL_{LONG}}{nCallINTL_{Fraud}}$$
$$= P_2 \quad (3.10)$$

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของราคาการโทรไปยังต่างประเทศ

$$P(Fraud|PriceINTL)$$
$$= P(Fraud) \times P(PriceINTL_{LOW}|Fraud) \times P(PriceINTL_{MED}|Fraud) \times P(PriceINTL_{HIGH}|Fraud)$$

$$= \frac{nCallINTL_{Fraud}}{nCallFraud} \times \frac{nPriceINTL_{LOW}}{nCallINTL_{Fraud}} \times \frac{nPriceINTL_{MED}}{nCallINTL_{Fraud}} \times \frac{nPriceINTL_{HIGH}}{nCallINTL_{Fraud}}$$
$$= P_3 \quad (3.11)$$

$$Sum_{Weight}(INTL) = \sum_{i=1}^{3} P_i$$
$$= P_1 + P_2 + P_3 \quad (3.12)$$

$$W_{nCallINTL} = \frac{P_1}{Sum_{Weight}(INTL)} \quad (3.13)$$

$$W_{DuraINTL} = \frac{P_2}{Sum_{Weight}(INTL)} \quad (3.14)$$

$$W_{callPriceINTL} = \frac{P_3}{Sum_{Weight}(INTL)} \quad (3.15)$$

$$Output_{INTL\_Data} = \lceil (Input_{nCallINTL} \times W_{nCallINTL}) + (Input_{DuraINTL} \times W_{DuraINTL}) + (Input_{callPriceINTL} \times W_{callPriceINTL}) \rceil \quad (3.16)$$

โดย

$Output_{INTL\_Data}$ คือค่าที่ได้จากการคำนวณด้วยปัจจัยที่มีผลต่อการนำเข้าไปยังโมเดลโครงข่ายประสาทเทียม

$Sum_{Weight}(INTL)$ คือค่าผลรวมความน่าจะเป็นที่เกิดการลักลอบใช้ในแต่ละเหตุการณ์ของการโทรต่างประเทศ

$W_{nCallINTL}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของจำนวนการโทรต่างประเทศ

$W_{DuraINTL}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของระยะเวลาการโทรต่างประเทศ

$W_{callPriceINTL}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของราคาการโทรต่างประเทศ

$nCallINTL_{Fraud}$ คือจำนวนครั้งของการโทรต่างประเทศและเป็นการลักลอบใช้

nCallFraud คือจำนวนครั้งของการเกิดการลักลอบใช้ทั้งหมด

$nCallINTL_i$ คือจำนวนของการโทรในระดับที่ $i \in \{LOW, MEDIUM, HIGH\}$

$nPriceINTL_i$ คือจำนวนของการโทรในระดับที่ $i \in \{LOW, MEDIUM, HIGH\}$

$nDuraINTL_i$ คือจำนวนของการโทรในระดับที่ $i \in \{SHORT, MEDIUM, LONG\}$

ข) ทำการประเมินค่าประเภทการโทรภายในโครงข่ายเดียวกัน

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของจำนวนการโทรโครงข่ายเดียวกัน

$$P(Fraud|nCallOnt)$$
$$= P(Fraud) \times P(nCallOnt_{LOW}|Fraud) \times P(nCallOnt_{MED}|Fraud) \times P(nCallOnt_{HIGH}|Fraud)$$
$$= \frac{nCallOnt_{Fraud}}{nCallFraud} \times \frac{nCallOnt_{LOW}}{nCallOnt_{Fraud}} \times \frac{nCallOnt_{MED}}{nCallOnt_{Fraud}} \times \frac{nCallOnt_{HIGH}}{nCallOnt_{Fraud}}$$
$$= P_1 \quad (3.17)$$

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของระยะเวลาการโทรโครงข่ายเดียวกัน

$$P(Fraud|DuraOnt) = P(Fraud) \times P(DuraOnt_{LOW}|Fraud) \times P(DuraOnt_{MED}|Fraud) \times P(DuraOnt_{HIGH}|Fraud)$$

$$= \frac{nCallOnt_{Fraud}}{nCallFraud} \times \frac{nDuraOnt_{SHORT}}{nCallOnt_{Fraud}} \times \frac{nDuraOnt_{MED}}{nCallOnt_{Fraud}} \times \frac{nDuraOnt_{LONG}}{nCallOnt_{Fraud}}$$

$$= P_2 \quad (3.18)$$

คำนวณความน่าจะเป็นที่จะเกิดการลักลอบใช้ในเหตุการณ์ที่เกิดระดับของราคาการโทรโครงข่ายเดียวกัน

$$P(Fraud|PriceOnt) = P(Fraud) \times P(PriceOnt_{LOW}|Fraud) \times P(PriceOnt_{MED}|Fraud) \times P(PriceOnt_{HIGH}|Fraud)$$

$$= \frac{nCallOnt_{Fraud}}{nCallFraud} \times \frac{nPriceOnt_{LOW}}{nCallOnt_{Fraud}} \times \frac{nPriceOnt_{MED}}{nCallOnt_{Fraud}} \times \frac{nPriceOnt_{HIGH}}{nCallOnt_{Fraud}}$$

$$= P_3 \quad (3.19)$$

$$Sum_{Weight}(Ont) = \sum_{i=1}^{3} P_i = P_1 + P_2 + P_3 \quad (3.20)$$

$$W_{nCallOnt} = \frac{P_1}{Sum_{Weight}(Ont)} \quad (3.21)$$

$$W_{DuraOnt} = \frac{P_2}{Sum_{Weight}(Ont)} \quad (3.22)$$

$$W_{callPriceOnt} = \frac{P_3}{Sum_{Weight}(Ont)} \quad (3.23)$$

$$Output_{Ont\_Data} = \lceil (Input_{nCallOnt} \times W_{nCallOnt}) + (Input_{DuraOnt} \times W_{DuraOnt}) + (Input_{callPriceOnt} \times W_{callPriceOnt}) \rceil \quad (3.24)$$

โดย

$Output_{Ont\_Data}$ คือค่าที่ได้จากการคำนวณด้วยปัจจัยที่มีผลต่อการนำเข้าไปยังโมเดลโครงข่ายประสาทเทียม

$Sum_{Weight}(Ont)$ คือค่าผลรวมความน่าจะเป็นที่เกิดการลักลอบใช้ในแต่ละเหตุการณ์ของการโทรโครงข่ายเดียวกัน

$W_{nCallOnt}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของจำนวนการโทรโครงข่ายเดียวกัน

$W_{DuraOnt}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของระยะเวลาการโทรโครงข่ายเดียวกัน

$W_{callPriceOnt}$ คือค่าน้ำหนักสำหรับการพิจารณาค่าข้อมูลดิบในส่วนของราคาการโทรโครงข่ายเดียวกัน

$nCallOnt_{Fraud}$ คือจำนวนครั้งของการโทรโครงข่ายเดียวกันและเป็นการลักลอบใช้

nCallFraud คือจำนวนครั้งของการเกิดการลักลอบใช้ทั้งหมด

$nCallOnt_i$ คือจำนวนของการโทรในระดับที่ $i \in \{LOW, MEDIUM, HIGH\}$

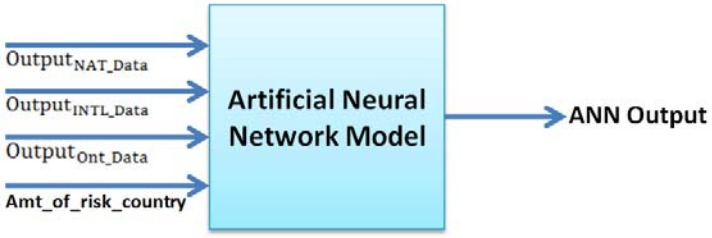
$nPriceOnt_i$ คือจำนวนของการโทรในระดับที่ $i \in \{LOW, MEDIUM, HIGH\}$

$nDuraIOnt_i$ คือจำนวนของการโทรในระดับที่ $i \in \{SHORT, MEDIUM, LONG\}$

จากการคำนวณข้างต้นจะทำให้ได้ค่าข้อมูลนำเข้าไปยังตัวแบบโครงข่ายประสาทเทียม ซึ่งประกอบด้วยข้อมูลปัจจัยการโทรนอกโครงข่ายในประเทศ ข้อมูลปัจจัยการโทรนอกโครงข่ายระหว่างประเทศ ข้อมูลปัจจัยการโทรภายในโครงข่ายเดียวกัน

3) โมดูลตัวแบบโครงข่ายประสาทเทียม

หลังจากที่ได้ทำการประมวลผลจากตัวแบบนาอีฟเบย์เซียนแล้ว จะได้ค่าพารามิเตอร์ที่เป็นข้อมูลนำเข้าสู่ตัวแบบโครงข่ายประสาทเทียมได้แก่ ข้อมูลปัจจัยการโทรนอกโครงข่ายในประเทศ ข้อมูลปัจจัยการโทรนอกโครงข่ายระหว่างประเทศ ข้อมูลปัจจัยการโทรภายในโครงข่ายเดียวกัน นอกจากนี้แล้วยังมีข้อมูลระดับการโทรไปยังประเทศกลุ่มเสี่ยง ดังภาพที่ 3.5



ภาพที่ 3.5 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูลตัวแบบโครงข่ายประสาทเทียม

ในการคำนวณซึ่งประกอบไปด้วยโหนดนำเข้าจำนวน 4 โหนด โหนดส่งออกจำนวน 1 โหนด โดยเริ่มจากการทำการฝึกหัด (Training) เพื่อให้ได้ค่าน้ำหนักและจำนวนโหนดซ่อน (Hidden Node) ที่เหมาะสม โดยในที่นี้จะพิจารณาที่จำนวนชั้น (Layer) ที่ 1 ชั้น เมื่อได้จำนวนโหนดซ่อนที่เหมาะสมแล้วจะเข้าสู่กระบวนการทดสอบ (Testing) ต่อไป

โดยในการคำนวณมีรายละเอียดดังนี้

1) การคำนวณจากชั้นนำเข้าสู่ชั้นซ่อน

$$N_j = \sum_{i=0}^{N-1} X_i W_{ij} \qquad (3.25)$$

โดย

N_j แทนโหนดซ่อนที่อยู่ภายในชั้นซ่อน

X_i แทนโหนดข้อมูลนำเข้า

W_{ij} แทนค่านำหนักระหว่างโหนดนำเข้าที่ i และโหนดซ่อนที่ j

2) การคำนวณจากชั้นซ่อนสู่ชั้นนำออก

$$Z_k = \sum_{j=0}^{N-1} N_j W_{jk} \qquad (3.26)$$

โดย

Z_k แทนโหนดข้อมูลนำออก

N_j แทนโหนดซ่อน

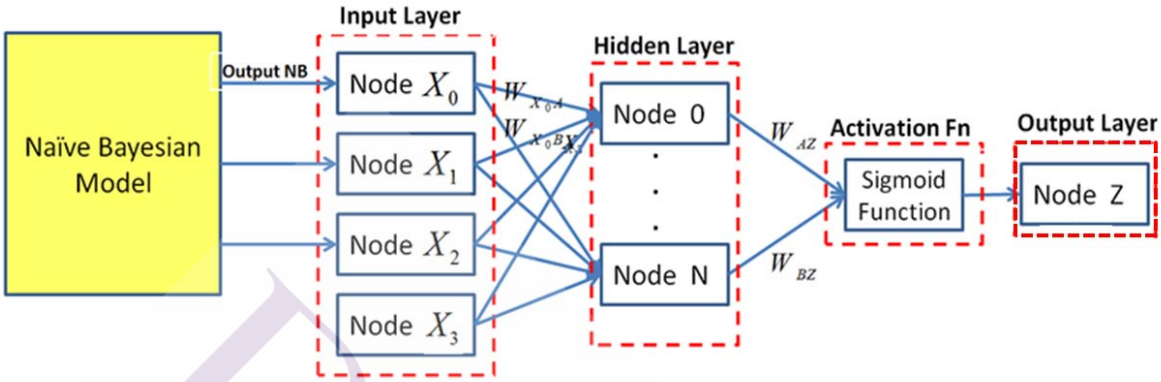
W_{jk} แทนค่านำหนักระหว่างโหนดซ่อนที่ j และโหนดนำออกที่ k

3) การใช้ฟังก์ชันกระตุ้น (Activation Function) โดยในที่นี้ใช้ซิกมอยด์ฟังก์ชันในการกระตุ้น

$$f(x) = \frac{1}{1+e^{-jx}} \tag{3.27}$$

โดย

j แทนค่าคงที่ ในที่นี่กำหนดให้เป็น 1

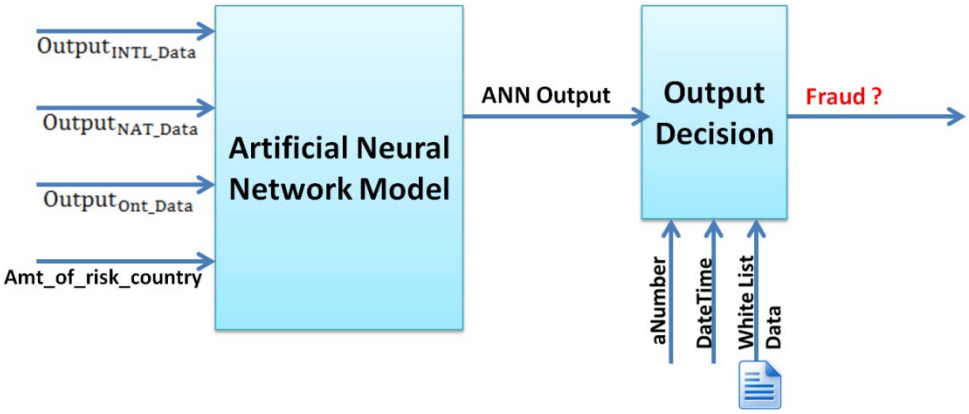


ภาพที่ 3.6 ส่วนของข้อมูลนำเข้าและส่งออกสำหรับโมดูลตัวแบบโครงข่ายประสาทเทียม

จากภาพที่ 3.6 ในส่วนของชั้นข้อมูลนำเข้าประกอบด้วย 4 โหนด ได้แก่ ค่าปัจจัยการโทรภายในโครงข่ายเดียวกัน ค่าปัจจัยการโทรนอกโครงข่ายภายในประเทศ ค่าปัจจัยการโทรนอกโครงข่ายระหว่างประเทศ และระดับการโทรไปยังประเทศกลุ่มเสี่ยง ซึ่งแทนด้วย X_0 - X_3 ตามลำดับ ในส่วนของชั้นซ่อนจะประกอบไปด้วย 1 ชั้น โดยการระบุจำนวนโหนดซ่อนเริ่มจากการเพิ่มจำนวนโหนดทุกๆ 1 โหนดในการฝึกหัดแต่ละครั้งเพื่อที่จะได้ค่าน้ำหนักและจำนวนโหนดซ่อนที่เหมาะสมสำหรับโครงข่าย ในส่วนของฟังก์ชันกระตุ้น (Activation Function) จะใช้ฟังก์ชันซิกมอยด์ (Sigmoid Function) ในการกระตุ้น

4) โมดูลการตัดสินใจ

หลังจากที่ได้ค่าผลลัพธ์ออกมาแล้วหากพบว่าเป็นกรณีที่ผิดปกติก็จะทำการตรวจสอบว่าในอดีตเลขหมายนี้เคยเกิดเหตุการณ์ในลักษณะที่เป็นการลักลอบใช้หรือไม่ และมีการยืนยันว่าเป็นการใช้งานที่ปกติจากลูกค้าหรือไม่ หากพบว่าบนไวท์ลิสต์เคยบันทึกไว้ว่าเป็นการใช้งานปกติก็จะถูกเตือนในสถานะแจ้งระวัง (Warning) หากไม่เคยมีบันทึกไว้ในไวท์ลิสต์ก็จะถูกเตือนในสถานะวิกฤติ (Critical) ดังภาพที่ 3.7



ภาพที่ 3.7 ส่วนของโมดูลการตัดสินใจ

3.2.2 การออกแบบตัวแบบความสัมพันธ์ระหว่างข้อมูล

ในส่วนของข้อมูลที่นำมาใช้จะประกอบด้วย 2 ส่วนคือ ส่วนของข้อมูลที่ได้จากเครื่องแม่ข่ายสำหรับจัดเก็บข้อมูลการโทร (CDR Server) และส่วนของข้อมูลที่ได้ทำการวิเคราะห์ว่ามีแนวโน้มในลักษณะของการลักลอบใช้งาน โดยมีรายละเอียดดังต่อไปนี้

1) ข้อมูลที่ได้จากเครื่องแม่ข่ายสำหรับจัดเก็บข้อมูลการโทร

ในส่วนของข้อมูลที่ได้จากเครื่องแม่ข่ายสำหรับจัดเก็บข้อมูลการโทรนั้นจะมีการเก็บในลักษณะแบบใกล้เวลาจริง (Near Real Time) โดยลักษณะการจัดเก็บนั้นจะนำข้อมูลที่ได้จากอุปกรณ์เครื่องแม่ข่ายแอพพลิเคชันวีโอไอพี (VoIP Application Server) โดยรายละเอียดของข้อมูลมีดังนี้

1.1) ตารางรายละเอียดการใช้งาน (CDR: Call Detail Record)

CDR(startTime,aNumber,bNumber,Duration,causeValue,callID,inRoute,outRoute, Prefix, callPrice,callTime,callTo)

โดยรายละเอียดของแต่ละแอททริบิวท์ (Attribute) ดังตารางที่ 3.8

ตารางที่ 3.8 รายละเอียดแต่ละแอททริบิวท์ของตาราง CDR

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	ตัวอย่างข้อมูล
startTime	เวลาที่ทำการโทร	nvarchar(50)	2016-26-06 T15:57:34.8+0700
aNumber	เลขหมายต้นทาง	nvarchar(50)	6621053000
bNumber	เลขหมายปลายทาง	nvarchar(50)	00985291270508
Duration	ระยะเวลาการโทรในหน่วยวินาที	int	25
causeValue	Release code	int	16 = Normal Call Clearing
callID	รหัสอ้างอิงการโทร	nvarchar(50)	87dfe6bfef60190baea912da156683c7
inRoute	เส้นทางตั้งต้น	nvarchar(20)	IMS
outRoute	เส้นทางสิ้นสุด	nvarchar(20)	OFFNET_NATL, OFFNET_INTL
Prefix	001/009+รหัสประเทศ+รหัสพื้นที่	nvarchar(20)	0098529
callPrice	ราคาค่าโทร (บาท)	real	154
callTime	ช่วงเวลาที่โทร (24H)	int	23
callTo	ประเภทการโทร	nvarchar(20)	INTL

1.2) ตาราง Preprocess Data ทำหน้าที่ในการจัดเก็บข้อมูลที่ได้หลังจากการประมวลผลข้อมูลเบื้องต้นแล้วมีรายละเอียดดังนี้

preProcessData(dateStart,aNumber,callTime,nCallNational,durationsNational,callPriceNational,nCallInternational,durationsInternational,CallPriceInternational,nCallOnnet,durationsOnnet,callPriceOnnet,callRiskCountry,isFraud)

โดยรายละเอียดของแต่ละแอททริบิวท์ (Attribute) ดังตารางที่ 3.9

ตารางที่ 3.9 รายละเอียดแต่ละแอททริบิวท์ของตาราง preProcessData

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
dateStart	วันและเวลาการโทร	nvarchar(25)	
aNumber	เลขหมายต้นทาง	nvarchar(50)	
callTime	ช่วงเวลาที่ทำการโทร	int	1 แทน Night (00:00-08:59 น.) 2 แทน Morning (09:00-16:59 น.) 3 แทน Evening (17:00-23:59 น.)
nCallNational	จำนวนครั้งการโทรนอกโครงข่ายภายในประเทศ	int	
durationsNational	ระยะเวลาการโทรนอกโครงข่ายภายในประเทศ	real	
callPriceNational	ค่าใช้จ่ายในการโทรนอกโครงข่ายภายในประเทศ	real	
nCallInternational	จำนวนครั้งการโทรนอกโครงข่ายระหว่างประเทศ	int	
durationsInternational	ระยะเวลาการโทรนอกโครงข่ายระหว่างประเทศ	real	
CallPriceInternational	ค่าใช้จ่ายในการโทรนอกโครงข่ายระหว่างประเทศ	real	
nCallOnnet	จำนวนครั้งการโทรภายในโครงข่ายเดียวกัน	int	
durationsOnnet	ระยะเวลาการโทรภายในโครงข่ายเดียวกัน	real	
callPriceOnnet	ค่าใช้จ่ายในการโทรภายในโครงข่ายเดียวกัน	real	
callRiskCountry	ระดับการโทรไปประเทศกลุ่มเสี่ยง	int	1 แทน Low 2 แทน High
isFraud	ระบุว่าเป็นการลักลอบหรือไม่	int	1 แทน ลักลอบ 0 แทน ไม่ลักลอบ

1.3) ตาราง Weight before hidden Data ทำหน้าที่ในการจัดเก็บข้อมูลค่าน้ำหนักที่เหมาะสมสำหรับตัวแบบโครงข่ายประสาทเทียมในส่วนของโครงข่ายก่อนเข้าสู่โหนดซ่อน มีรายละเอียดดังนี้

weightBeforeHiddenData (index_i,index_j,weight)

โดยรายละเอียดของแต่ละแอททริบิวท์ (Attribute) ดังตารางที่ 3.10

ตารางที่ 3.10 รายละเอียดแต่ละแอททริบิวท์ของตาราง weightBeforeHiddenData

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
Index_i	Index ของ Array ในมิติ 1	int	
Index_j	Index ของ Array ในมิติ 2	int	
weight	ค่าน้ำหนัก	double	

1.4) ตาราง Weight after hidden Data ทำหน้าที่ในการจัดเก็บข้อมูลค่าน้ำหนักที่เหมาะสมสำหรับตัวแบบโครงข่ายประสาทเทียมในส่วนของโครงข่ายหลังออกจากโหนดซ่อน มีรายละเอียดดังนี้

WeightAfterHiddenData (index_i,index_j,weight)

โดยรายละเอียดของแต่ละแอททริบิวท์ (Attribute) ดังตารางที่ 3.11

ตารางที่ 3.11 รายละเอียดแต่ละแอททริบิวท์ของตาราง weightAfterHiddenData

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
Index_i	Index ของ Array ในมิติ 1	int	
Index_j	Index ของ Array ในมิติ 2	int	
weight	ค่าน้ำหนัก	double	

1.5) ตาราง Prefix จะทำการบอกรายละเอียดว่ารหัสประเทศแต่ละประเทศมีรหัสอะไรบ้าง ซึ่งอาจลงลึกไปถึงระดับเมือง โดยมีรายละเอียดดังนี้

Prefix (PrefixID,PrefixPrice,CountryID)

โดยคำอธิบายของแต่ละแอททริบิวท์ มีรายละเอียดดังตารางที่ 3.12

ตารางที่ 3.12 รายละเอียดของตารางข้อมูล Prefix

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
PrefixID	ลำดับของรหัสประเทศ	Integer(10)	Primary Key
PrefixPrice	ค่าโทรของรหัสนี้	Double	
CountryID	ลำดับของประเทศ	Integer(3)	

1.6) ตาราง Country จะทำการบอกรายละเอียดชื่อประเทศต่างๆ ในโลก โดยมีรายละเอียดดังนี้

Country (CountryID,CountryName,BlackListStatus)

โดยคำอธิบายของแต่ละแอททริบิวท์ มีรายละเอียดดังตารางที่ 3.13

ตารางที่ 3.13 รายละเอียดของตารางข้อมูล Country

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
CountryID	ลำดับของประเทศ	Integer(3)	Primary Key
CountryName	ชื่อของประเทศ	Varchar(100)	
BlackListStatus	แสดงสถานะของประเทศว่าเป็นประเทศที่มีความเสี่ยงในการเรียกออกหรือไม่	Boolean (T/F)	

2. ข้อมูลที่ได้ทำการวิเคราะห์ว่ามีแนวโน้มในลักษณะของการลักลอบใช้งาน

ข้อมูลที่ได้จากการวิเคราะห์แนวโน้มในลักษณะของการลักลอบใช้งานนั้นจะนำข้อมูลที่ได้จากส่วนของข้อมูลที่ได้จากเครื่องแม่ข่ายจัดเก็บข้อมูลการใช้งาน จากนั้นจะเข้าสู่กระบวนการในการประมวลผลเบื้องต้นให้ได้รูปแบบที่ต้องการสำหรับนำเข้าตัวแบบเพื่อทำการวิเคราะห์หาว่าพบกรณีการลักลอบหรือไม่ โดยหลังจากที่ตรวจสอบแล้วพบกรณีการลักลอบเกิดขึ้น จะถูกนำมาจัดเก็บไว้เพื่อทำการแจ้งเตือนให้กับผู้ดูแลระบบทราบต่อไป ซึ่งรายละเอียดของข้อมูลมีรายละเอียดดังนี้

2.1) ตาราง Fraud จะทำการบอกว่าแต่ละชุดข้อมูลที่มีแนวโน้มว่าเป็นการลักลอบใช้มีลักษณะรายละเอียดของการลักลอบใช้อย่างไรบ้าง โดยมีรายละเอียดดังนี้

Fraud (fraudID,aNumber,dateTime,callTime,fraudLevel,StatusID)

โดยคำอธิบายของแต่ละแอททริบิวท์ มีรายละเอียดดังตารางที่ 3.14

ตารางที่ 3.14 รายละเอียดของตารางข้อมูล Fraud

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
fraudID	ลำดับของการลักลอบ	varchar(20)	
aNumber	หมายเลขต้นทาง	varchar(50)	
dateTime	วันและเวลาที่พบว่ามีแนวโน้มว่าลักลอบใช้	datetime	
callTime	ช่วงเวลาที่ทำการโทร	int	1 แทน Night (00:00-08:59 น.) 2 แทน Morning (09:00-16:59 น.) 3แทน Evening (17:00-23:59 น.)
fraudLevel	ระดับการลักลอบ	varchar(25)	Major, Minor, No
fraudStatusID	สถานะของ Fraud	Integer(2)	

2.2) ตาราง Fraud Status จะทำการบอกรายละเอียดสถานะของข้อมูลที่มีแนวโน้มว่าเป็นการลักลอบใช้บริการ โดยมีรายละเอียดดังนี้

fraudStatus (fraudStatusID,fraudStatusDetail)

โดยคำอธิบายของแต่ละแอททริบิวท์ มีรายละเอียดดังตารางที่ 3.15

ตารางที่ 3.15 รายละเอียดของตารางข้อมูล fraudStatus

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
fraudStatusID	ลำดับของสถานะ	Integer(2)	Primary Key
fraudStatusDetail	รายละเอียดของสถานะ	varchar(20)	

2.3) ตาราง Fraud Board จะทำการบันทึกรายการที่เกี่ยวข้องกับประวัติการตรวจสอบหรือรายละเอียดที่ต้องการแจ้งให้ผู้ที่เกี่ยวข้องทราบ โดยอยู่ในรูปของบอร์ด โดยมีรายละเอียดดังนี้

fraudBoard (fraudID,fraudBoardDetail,createDate,createBy)

โดยคำอธิบายของแต่ละแอททริบิวท์ มีรายละเอียดดังตารางที่ 3.16

ตารางที่ 3.16 รายละเอียดของตารางข้อมูล fraudBoard

แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
fraudID	ลำดับของการลักลอบ	Varchar (20)	
fraudBoardDetail	รายละเอียดของโพสต์	text	
createDate	วันที่ทำการโพสต์	dateTime	
createBy	ผู้ที่ทำการสร้างโพสต์	Varchar (150)	

2.4) ตาราง Whitelist จะทำการบันทึกรายการเลขหมายที่เคยตรวจจับได้ว่าเข้าข่ายลักลอบใช้แต่ลูกค้ายืนยันว่ามีการใช้งานจริง โดยมีรายละเอียดดังนี้

fraudWhiteList (numbering)

โดยคำอธิบายของแต่ละแอททริบิวท์ มีรายละเอียดดังตารางที่ 3.17

ตารางที่ 3.17 รายละเอียดของตารางข้อมูล fraudWhiteList

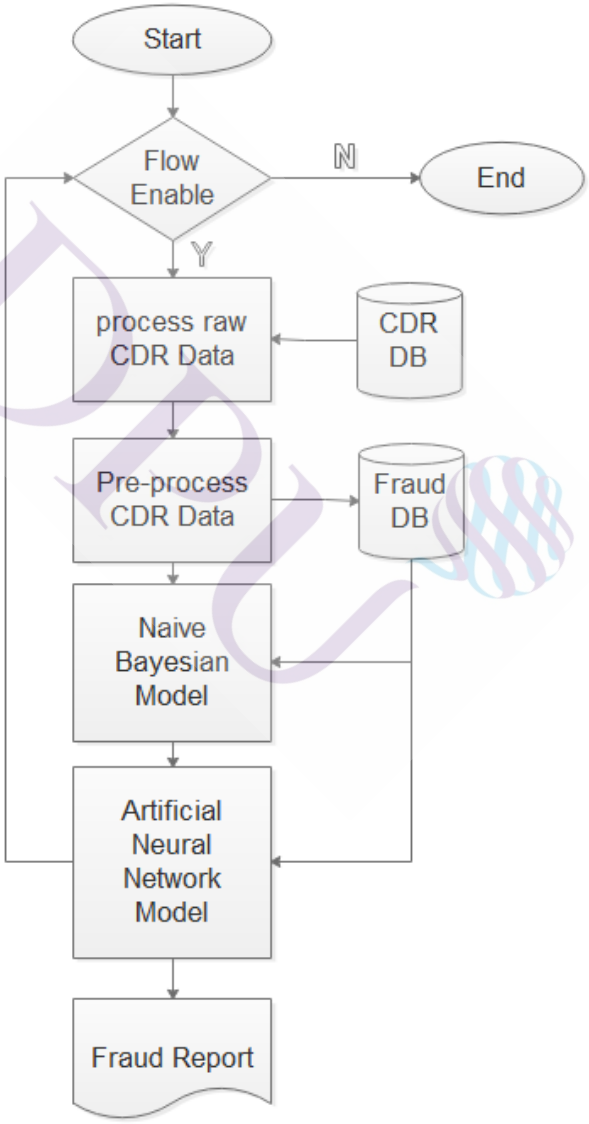
แอททริบิวท์	ความหมาย	ชนิดข้อมูล	หมายเหตุ
numbering	เลขหมายที่ถูกบันทึกว่าเป็นไวท์ลิสต์	varchar(25)	

3.2.3 การออกแบบผังการทำงานของระบบ

ในการออกแบบผังการทำงานของระบบนั้นสามารถแยกได้เป็น 2 ผังหลักคือ ผังแรกเป็นการทำงานของฝั่งการประมวลผลข้อมูลและทำการวิเคราะห์ว่ามีแนวโน้มในการลักลอบใช้งานหรือไม่ ผังที่สองเป็นผังการทำงานในส่วนของผู้ใช้ระบบ ซึ่งทั้ง 2 ผังการทำงานมีรายละเอียดดังนี้

3.2.3.1) ผังการทำงานส่วนของการประมวลผลข้อมูลและวิเคราะห์ข้อมูล

ในส่วนของการประมวลผลข้อมูลและการวิเคราะห์ข้อมูล เป็นกระบวนการที่ทำการประมวลผลเบื้องหลังของระบบ (Background Process) ซึ่งหน้าที่หลักคือการทำการแปลงข้อมูลการคำนวณโดยตัวแบบ และการจัดเก็บข้อมูลที่มีลักษณะการใช้งานผิดปกติไปยังระบบจัดการฐานข้อมูล เพื่อที่จะให้แจ้งต่อไปยังส่วนต่อประสานผู้ใช้งานระบบ โดยออกมาเป็นลักษณะของรายงานผ่านเว็บบราวน์เซอร์ โดยรายละเอียดของขั้นตอนการทำงาน ดังภาพที่ 3.8

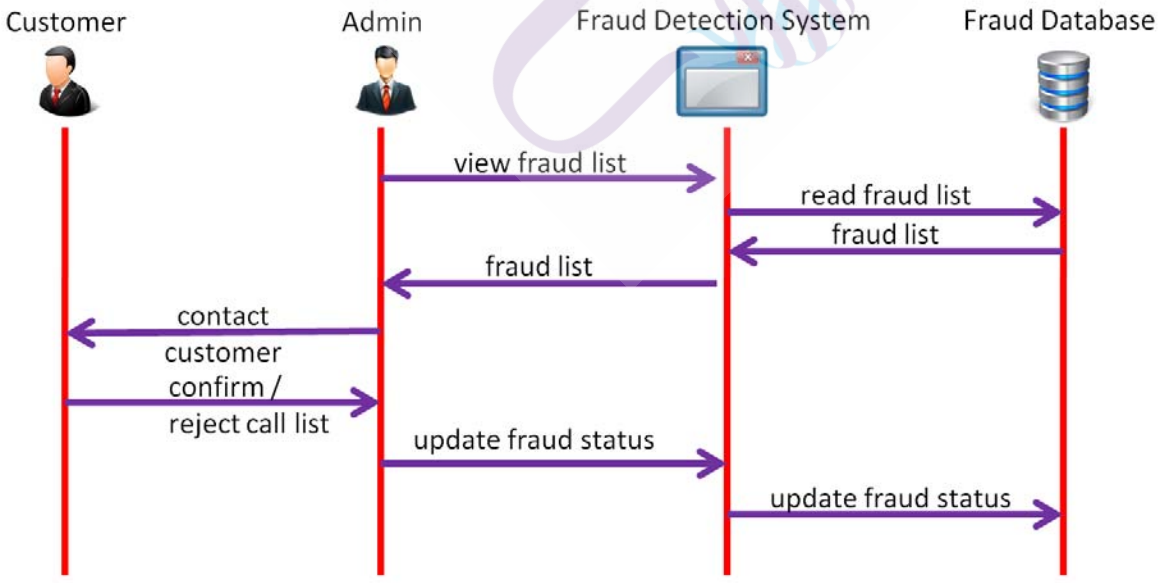


ภาพที่ 3.8 ผังการทำงานส่วนของการประมวลผลข้อมูลและวิเคราะห์ข้อมูล

จากภาพที่ 3.8 เริ่มการทำงานโดยทำการตรวจสอบว่าระบบอนุญาตให้ทำการประมวลผล (Flow Enable) หรือไม่ หากไม่ก็หยุดทำงาน หากใช่ก็ทำการประมวลผลข้อมูลดิบรายละเอียดการใช้งาน (raw CDR) ก่อนเข้าสู่กระบวนการประมวลผลข้อมูลเบื้องต้น หลังจากนั้นเมื่อได้ข้อมูลเบื้องต้นจะเข้าสู่กระบวนการคำนวณในตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียมตามลำดับ เมื่อตรวจพบลักษณะผิดปกติจะรายงานการลักลอบใช้งานออกมา (Fraud Report) จากนั้นจะทำตามขั้นตอนดังที่กล่าวมานี้ซ้ำไปเรื่อยๆจนกว่าจะมีการหยุดการทำงานระบบ

3.2.3.2) ผังการทำงานของส่วนผู้ใช้ระบบ

ในการทำงานส่วนของผู้ใช้ระบบ เริ่มจากระบบมีการตรวจสอบว่ามีรายการแจ้งเตือนที่ถูกจัดเก็บลงบนฐานข้อมูลหรือไม่ หากพบว่ามีรายการแจ้งเตือนก็จะทำการแสดงให้ผู้ใช้งานทราบผ่านเว็บ บราวน์เซอร์ หลังจากนั้นผู้ใช้งานระบบสามารถนำข้อมูลดังกล่าวไปตรวจสอบว่าลูกค้ามีการใช้งานจริงหรือถูกลักลอบใช้ โดยทำการติดต่อประสานงานไปยังลูกค้า หากมีการยืนยันว่ามีการใช้งานจริงระบบก็จะบันทึกรายการที่เกิดขึ้นว่าเป็นไวท์ลิสต์ หากลูกค้าแจ้งว่าไม่ได้ใช้งานจริงก็จะทำการบล็อคการโทรออกที่ชุมสายเพื่อลดการสูญเสียที่เกิดขึ้นจากการโดนลักลอบใช้งาน และรายการดังกล่าวจะถูกบันทึกไว้ว่าเป็นการลักลอบใช้งานจริง โดยรายละเอียดแผนภาพลำดับดังภาพที่ 3.9

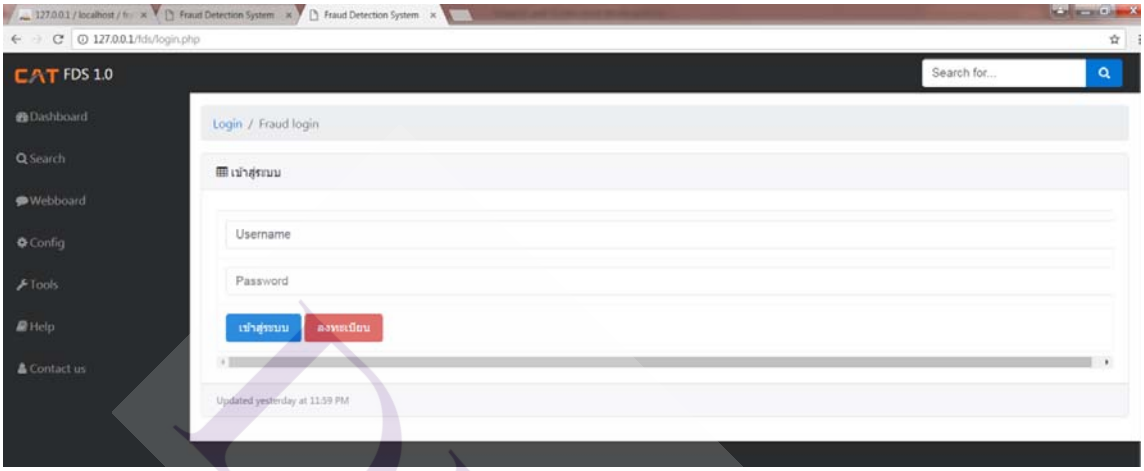


ภาพที่ 3.9 แผนภาพลำดับการทำงานในส่วนของผู้ใช้ระบบ

3.2.4 การออกแบบส่วนต่อประสานกับผู้ใช้

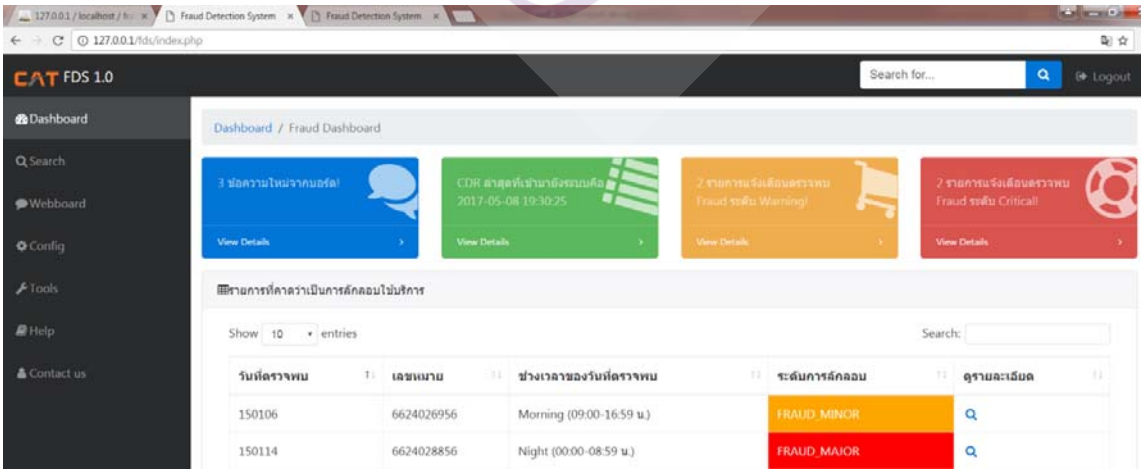
ในการออกแบบส่วนต่อประสานสำหรับเจ้าหน้าที่ที่เฝ้าระวังการลักลอบใช้บริการมีรายละเอียดดังต่อไปนี้

รายละเอียด : หน้า Login ใช้สำหรับให้เจ้าหน้าที่เข้าสู่ระบบ ดังภาพที่ 3.10



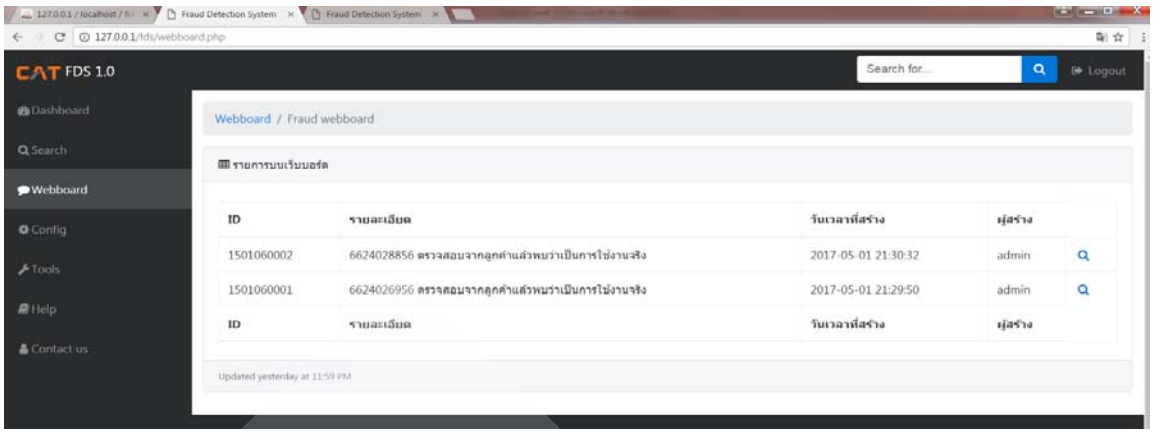
ภาพที่ 3.10 หน้า Login ใช้สำหรับให้เจ้าหน้าที่เข้าสู่ระบบ

รายละเอียด : หน้า Dashboard แสดงรายละเอียดการแจ้งเตือนต่างๆ ดังภาพที่ 3.11



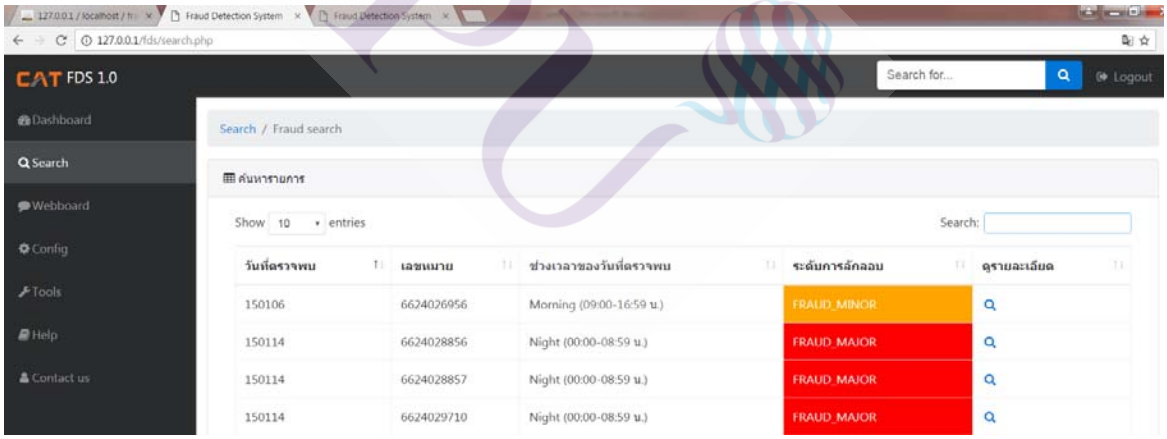
ภาพที่ 3.11 หน้า Dashboard แสดงรายละเอียดการแจ้งเตือนต่างๆ

รายละเอียด : หน้า Webboard ใช้สำหรับให้เจ้าหน้าที่สามารถแลกเปลี่ยนพูดคุย รวมถึงแจ้งการอัพเดตข้อมูลให้กับเจ้าหน้าที่ท่านอื่น ดังภาพที่ 3.12



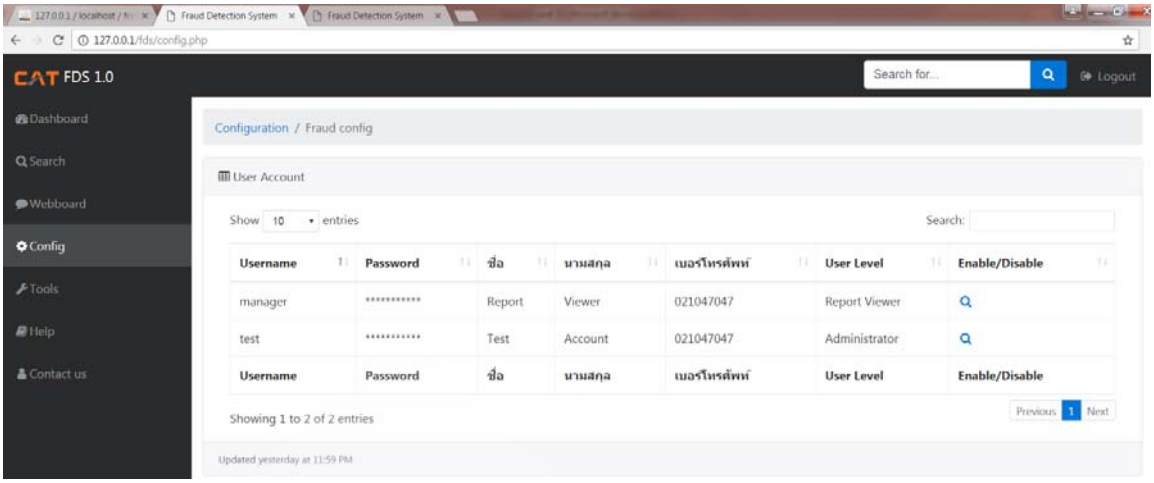
ภาพที่ 3.12 หน้า Webboard ใช้สำหรับให้เจ้าหน้าที่สามารถแลกเปลี่ยนพูดคุย

รายละเอียด : หน้า Search ใช้สำหรับค้นหาข้อมูลที่ตรวจจับได้บนระบบ ดังภาพที่ 3.13



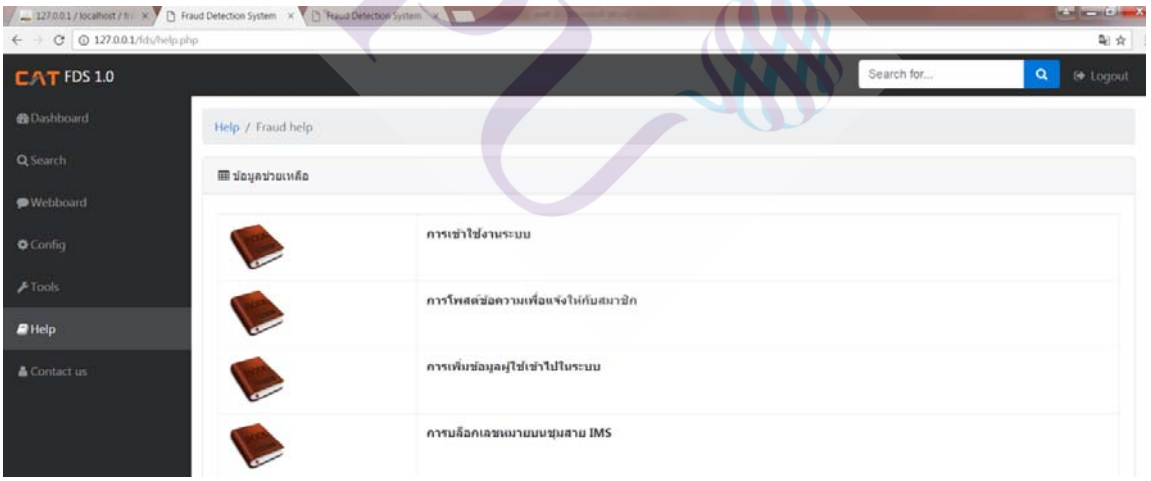
ภาพที่ 3.13 หน้า Search ใช้สำหรับค้นหาข้อมูลที่ตรวจจับได้บนระบบ

รายละเอียด : หน้า Config เป็นการปรับแต่ค่าที่เกี่ยวข้อง ดังภาพที่ 3.14



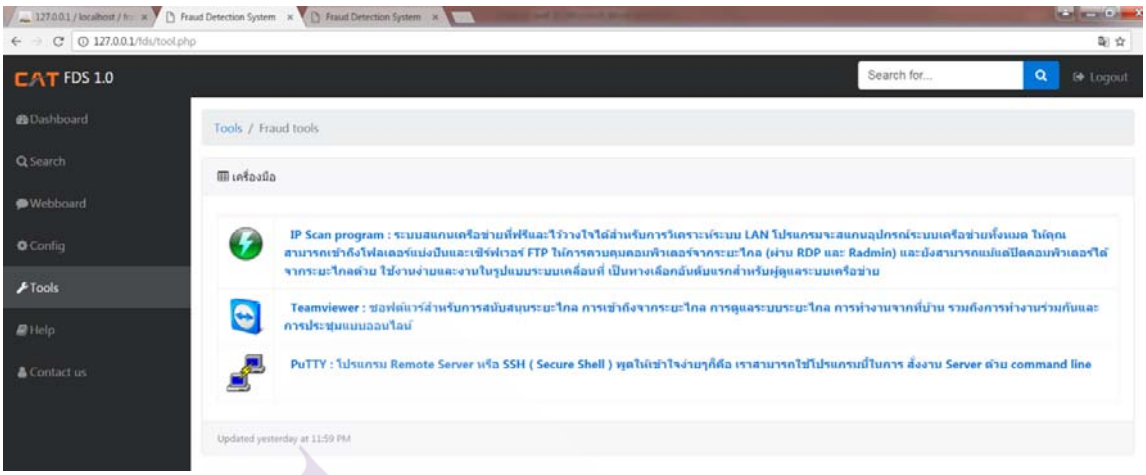
ภาพที่ 3.14 หน้า Config เป็นการปรับแต่ค่าที่เกี่ยวข้อง

รายละเอียด : หน้า Help เป็นหน้าที่รวบรวมเนื้อหาต่างๆเกี่ยวกับการใช้งานระบบ ดังภาพที่ 3.15



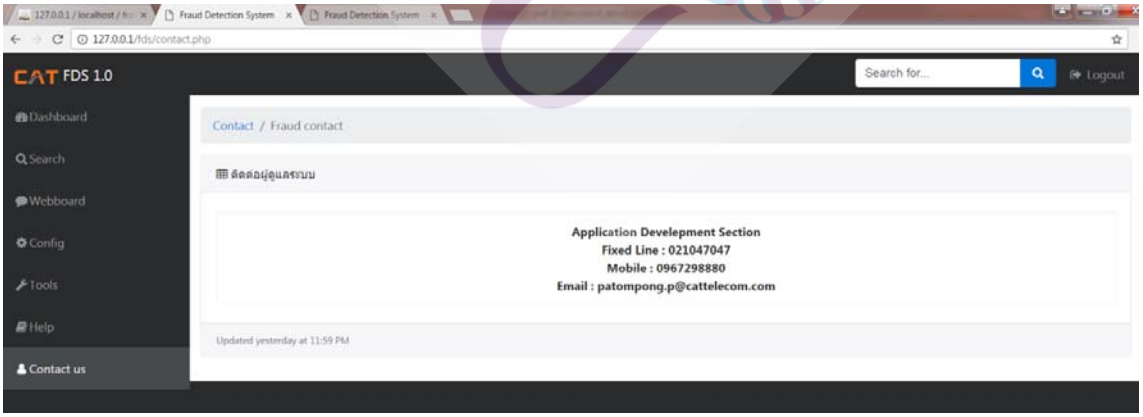
ภาพที่ 3.15 หน้า Help เป็นหน้าที่รวบรวมเนื้อหาต่างๆเกี่ยวกับการใช้งานระบบ

รายละเอียด : หน้า Tools เป็นการรวบรวมเครื่องมือต่างๆ ที่ช่วยในการวิเคราะห์ข้อมูลการโทร ดังภาพที่ 3.16



ภาพที่ 3.16 หน้า Tools เป็นการรวบรวมเครื่องมือต่างๆ

รายละเอียด : หน้า Contact Us ใช้สำหรับติดต่อผู้พัฒนาระบบกรณีมีข้อขัดข้องทางเทคนิคของเว็บ ดังภาพที่ 3.17



ภาพที่ 3.17 หน้า Contact Us ใช้สำหรับติดต่อผู้พัฒนาระบบกรณีมีข้อขัดข้องทางเทคนิคของเว็บ

บทสรุป จากการออกแบบงานวิจัยนี้มีส่วนที่สำคัญอยู่ 3 ส่วนด้วยกันคือ

1) ส่วนของการออกแบบตัวแบบในการตรวจจับซึ่งในที่นี้ใช้วิธีการตรวจจับโดยเงื่อนไข 4 ตัวแบบตามที่ได้กล่าวมาและการนำตัวแบบโครงข่ายประสาทเทียมและตัวแบบนาอีฟเบย์เซียนมาประยุกต์

2) ส่วนของการเชื่อมต่อเข้ากับเครื่องแม่ข่ายจัดเก็บข้อมูลการโทร รวมถึงการพัฒนาซอฟต์แวร์ในการตรวจจับ

3) ส่วนต่อประสานกับผู้ใช้ โดยผู้ใช้สามารถใช้งานผ่านเว็บบราวเซอร์ได้ และมีการแจ้งเตือนผ่านหน้าเว็บรวมถึงอีเมล์ด้วย

ในส่วนของการทดสอบจะทำการแปลงข้อมูลที่ได้จากฐานข้อมูลจริงของโครงข่ายเอ็นจีเอ็น บมจ. กสท โทรคมนาคม เพื่อให้อยู่ในภาพที่ สามารถนำไปใช้วิเคราะห์ได้ รวมถึงจะทำการเปรียบเทียบค่าความถูกต้องของการตรวจจับการลักลอบใช้ รวมถึงประสิทธิภาพในการประมวลผลของข้อมูลที่มีขนาดเล็กจนถึงขนาดใหญ่ ดังจะกล่าวในบทต่อไป

บทที่ 4
ผลการวิจัย

ในส่วนของผลการวิจัยจะกล่าวถึงตัวอย่างข้อมูลที่เกิดการลักลอบใช้งานจริง โดยผลการวิจัยแบ่งออกเป็น 3 ส่วน คือ การทดสอบตามเงื่อนไขการตรวจจับที่ได้กำหนดไว้ ได้แก่ การใช้งานเป็นเวลานานจนเกิดผิดสังเกต การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด สุดท้ายคือการมีพฤติกรรมตรวจสอบโครงข่ายแล้วกระหน่ำโทร และส่วนต่อมาคือการทดสอบตามตัวแบบนาอีฟย์เบย์เซียน ตัวแบบโครงข่ายประสาทเทียม และตังแบบที่ได้ทำการออกแบบและพัฒนา ส่วนสุดท้ายคือการทดสอบระบบที่ทำการพัฒนาเพื่อใช้ตรวจจับการลักลอบ โดยมีรายละเอียดดังนี้

4.1 ตัวอย่างข้อมูลการเกิดการลักลอบใช้งานจริง

ในส่วนของตัวอย่างข้อมูลการลักลอบใช้งานจริงนั้น จะยกตัวอย่างลักษณะการลักลอบใช้โดยประกอบด้วยรายละเอียดดังนี้

ก) การโทรไปยังประเทศกลุ่มเสี่ยง

ในกรณีนี้เลขหมาย 0440097XX โทรไปประเทศปลายทางกลุ่มเสี่ยงหลากหลายโดยส่วนใหญ่ทำการเรียกออกไปยังปลายทางด้วยอัตราค่าโทรพิเศษ (CAT001) ซึ่งมีอัตราค่าโทรที่สูง ดังภาพที่ 4.1

	A	B	C	D	E	F	G	H	I	J	K
1	A No	B No	Country	Sec	Price	In Route	Out Route	Date	Start Time	Service	B Prefix
2	440097	3876505	BOSNIA-HERZEGOVI	18.00	22.00	1CTBI1I	USSSC2O	150205	052955	CAT 001	001
3	440097	3876342	BOSNIA-HERZEGOVI	0.00	0.00	1CTBI1I	USASC2O	150205	052955	CAT 001	001
4	440097	3876659	BOSNIA-HERZEGOVI	0.00	0.00	1CTBI1I	USSSC2O	150205	052941	CAT 001	001
5	440097	9944002	AZERBAIJAN	0.00	0.00	1CTBI1I	USASC2O	150205	052915	CAT 001	001
6	440097	9945523	AZERBAIJAN	0.00	0.00	1CTBI1I	GBRCC2O	150205	052914	CAT 001	001
7	440097	3554575	ALBANIA	0.00	0.00	1CTBI1I	TI45I1O	150205	052827	CAT 001	001
8	440097	3556634	ALBANIA	0.00	0.00	1CTBI1I	TI45I1O	150205	052810	CAT 001	001
9	440097	9725928	ISRAEL	0.00	0.00	1CTBI1I	ISREC2O	150205	052755	CAT 009	009
10	440097	9725928	ISRAEL	0.00	0.00	1CTBI1I	ISREC2O	150205	052731	CAT 001	001
11	440097	9725928	ISRAEL	0.00	0.00	1CTBI1I	ISREC2O	150205	023134	CAT 001	001
12	440097	9725928	ISRAEL	0.00	0.00	1CTBI1I	ISREC2O	150205	023131	CAT 001	001
13	440097	9725928	ISRAEL	0.00	0.00	1CTBI1I	ISREC2O	150205	023115	CAT 001	001

ภาพที่ 4.1 รายละเอียดตัวอย่างการลักลอบโทรไปยังประเทศกลุ่มเสี่ยงหลากหลาย

ข) การโทรเป็นระยะเวลานานจนเกิดค่าโทรที่สูงผิดปกติ

ในกรณีนี้เลขหมาย 0420997XX โทรไปประเทศปลายทางต่างประเทศด้วยจำนวนค่าโทรที่สูงผิดปกติ โดยส่วนใหญ่ทำการเรียกออกไปยังปลายทางด้วยอัตราค่าโทรพิเศษ (CAT001) ซึ่งมีอัตราค่าโทรที่สูง ดังภาพที่ 4.2

	A	B	C	D	E	F	G	H	I	J	K
1	A No	B No	Country	Sec	Price	In Route	Out Route	Date	Start Time	Service	B Prefix
2	420997	5324413	CUBA	10.00	28.00	1CTBI1I	SUBUC2O	150216	154359	CAT 001	001
3	420997	5324413	CUBA	350.00	168.00	1CTBI1I	SUBUC2O	150216	153845	CAT 001	001
4	420997	5324413	CUBA	11.00	28.00	1CTBI1I	SUBUC2O	150216	153820	CAT 001	001
5	420997	5324413	CUBA	11.00	28.00	1CTBI1I	SUBUC2O	150216	153736	CAT 001	001
6	420997	5324413	CUBA	10.00	28.00	1CTBI1I	SUBUC2O	150216	153701	CAT 001	001
7	420997	5324413	CUBA	424.00	224.00	1CTBI1I	SUBUC2O	150216	153626	CAT 001	001
8	420997	5348123	CUBA	4.00	28.00	1CTBI1I	SUBUC2O	150216	153537	CAT 001	001
9	420997	5343130	CUBA	0.00	0.00	1CTBI1I	SUBEC2O	150216	153504	CAT 001	001
10	420997	1404260	U.S.A.	1.00	3.00	1CTBI1I	USASC2O	150216	153431	CAT 001	001

ภาพที่ 4.2 รายละเอียดตัวอย่างการลักลอบโทรด้วยค่าโทรที่สูงผิดปกติ

ค) การโทรไปเบอร์กลุ่มเดิมซ้ำแต่หลากหลาย

ในกรณีนี้เลขหมาย 0210530XX โทรไปกลุ่มเลขหมายเดิมซ้ำๆหลากหลายดังภาพที่ 4.3

	A	B	C	D	E	F	G	H	I	J	K
1	A No	B No	Country	Sec	Price	In Route	Out Route	Date	Start Time	Service	B Prefix
2	210530	140 5391	U.S.A.	1.00	3.00	1CTBI1I	USASC2O	150216	150517	CAT 001	001
3	210530	972 67421	ISRAEL	0.00	0.00	1CTBI1I	AUSSC2O	150216	150536	CAT 001	001
4	210530	534 056	CUBA	8.00	28.00	1CTBI1I	SUBUC2O	150216	150657	CAT 001	001
5	210530	533 162	CUBA	5.00	28.00	1CTBI1I	SUBUC2O	150216	150853	CAT 001	001
6	210530	534 700	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	150930	CAT 001	001
7	210530	534 602	CUBA	5.00	28.00	1CTBI1I	SUBUC2O	150216	150955	CAT 001	001
8	210530	532 166	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	151019	CAT 001	001
9	210530	535 151	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	151152	CAT 001	001
10	210530	535 620	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	151222	CAT 001	001
11	210530	532 103	CUBA	9.00	28.00	1CTBI1I	SUBUC2O	150216	151233	CAT 001	001
12	210530	532 105	CUBA	417.00	196.00	1CTBI1I	SUBUC2O	150216	151648	CAT 001	001
13	210530	532 106	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	151728	CAT 001	001
14	210530	532 105	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	151825	CAT 001	001
15	210530	532 107	CUBA	0.00	0.00	1CTBI1I	SUBUC2O	150216	151855	CAT 001	001
16	210530	532 107	CUBA	789.00	392.00	1CTBI1I	SUBUC2O	150216	151905	CAT 001	001
17	210530	532 105	CUBA	1,142.00	560.00	1CTBI1I	SUBUC2O	150216	152452	CAT 001	001
18	210530	532 107	CUBA	318.00	168.00	1CTBI1I	SUBUC2O	150216	153357	CAT 001	001
19	210530	532 107	CUBA	3.00	28.00	1CTBI1I	SUBUC2O	150216	153941	CAT 001	001
20	210530	532 105	CUBA	6.00	28.00	1CTBI1I	SUBUC2O	150216	154010	CAT 001	001
21	210530	532 105	CUBA	9.00	28.00	1CTBI1I	SUBUC2O	150216	154059	CAT 001	001
22	210530	532 105	CUBA	8.00	28.00	1CTBI1I	SUBUC2O	150216	154132	CAT 001	001
23	210530	532 107	CUBA	11.00	28.00	1CTBI1I	SUBUC2O	150216	154200	CAT 001	001
24	210530	532 107	CUBA	5.00	28.00	1CTBI1I	SUBUC2O	150216	154241	CAT 001	001
25	210530	532 107	CUBA	374.00	196.00	1CTBI1I	SUBUC2O	150216	154256	CAT 001	001

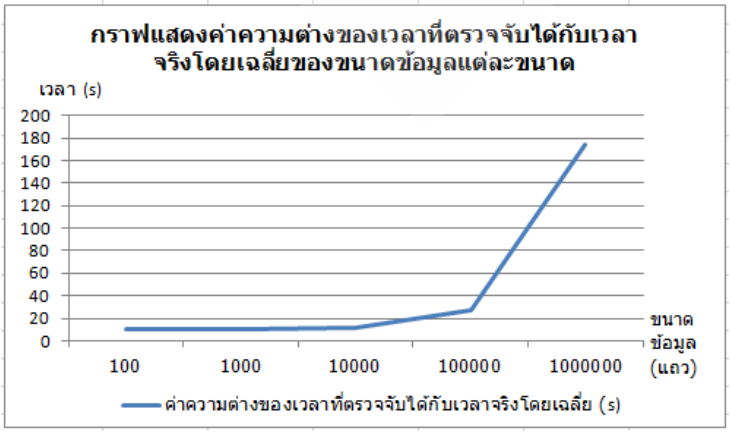
ภาพที่ 4.3 รายละเอียดตัวอย่างการลักลอบโทรไปกลุ่มเดิมซ้ำๆหลากหลาย

4.2 การทดลองตรวจจับตามเงื่อนไขที่กำหนด

ในการทดลองได้ทำการทดสอบประสิทธิภาพทางเวลาในการตรวจจับจะทำการสร้างกลุ่มข้อมูลเป็น 5 กลุ่ม ซึ่งมีขนาดจำนวน 100 1,000 10,000 100,000 1,000,000 แถวตามลำดับ โดยข้อมูลแต่ละขนาดจะมีข้อมูลที่คาดว่าจะเกิดการลักลอบใช้งานอยู่ด้วย 2 กรณีคือ การเรียกออกไปยังประเทศกลุ่มเป้าหมายและการมีพฤติกรรมการโทรผิดปกติ ในการทดสอบจะทำการเทียบเวลาที่มีการโทรที่ถูกบันทึกในชุมสายเทียบกับเวลาที่ตรวจจับได้ โดยผลการทดสอบดังในตาราง 4.1 และกราฟแนวโน้มเวลาการประมวลผลเมื่อมีปริมาณข้อมูลเพิ่มขึ้นดังภาพที่ 4.4

ตารางที่ 4.1 ผลการทดสอบของระบบตรวจจับการลักลอบใช้งานในปริมาณข้อมูลที่แตกต่างกัน

จำนวนข้อมูล (แถว)	ค่าความต่างของเวลาที่ระบบตรวจจับได้กับเวลาจริงที่เริ่มมีการโทร (วินาที)
100	10.00
1,000	10.00
10,000	11.71
100,000	27.00
1,000,000	174.91



ภาพที่ 4.4 กราฟแสดงค่าความต่างของเวลาที่ตรวจจับได้กับเวลาจริงโดยเฉลี่ยของข้อมูลแต่ละขนาด

ในการทดสอบด้านความถูกต้องในการตรวจจับ ได้ทำการสร้างตัวอย่างข้อมูลการใช้งานใน 1 ปีในปี ค.ศ. 2012 โดยมีจำนวนเลขหมายที่สุ่มทดสอบจำนวน 540 เลขหมาย มีข้อมูลจำนวน 17,550 แถว โดยกรณีการใช้งานเป็นเวลานานจนเกิดผิดสังเกตได้ทำการกำหนดค่า Threshold ไว้ที่ 30 นาที กรณีการใช้งานเกินมาตรฐานที่ทางชุมสายกำหนดได้กำหนดวงเงินการเรียกออกไว้ที่ 500 บาทต่อชั่วโมง และกำหนดปริมาณการเรียกออกไม่เกิน 60 ครั้งต่อชั่วโมง และสุดท้ายในกรณีการมีพฤติกรรมการโทรแปลกๆโดยมีการเข้ามาลักษณะตรวจสอบโครงข่ายแล้วกระหน่ำโทรจะทำการตั้งจำนวนครั้งในการโทรที่ 20 ครั้งต่อนาที โดยผลการทดลองดังในตาราง 4.2

ตารางที่ 4.2 ผลการทดสอบความถูกต้องของระบบตรวจจับการลักลอบใช้งาน

กรณีการตรวจจับ	% การตรวจจับได้	% การเกิดการลักลอบใช้บริการจริง	% ไม่เป็นการลักลอบใช้บริการ
(1)	100	0	100
(2)	100	4.44	95.56
(3)	100	1.11	98.89
(4)	100	0.06	99.94

หมายเหตุ. (1) การใช้งานเป็นเวลานานจนเกิดผิดสังเกต

(2) การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง

(3) การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด

(4) การมีพฤติกรรมการโทรแปลกๆโดยมีการเข้ามาลักษณะตรวจสอบโครงข่ายแล้วกระหน่ำโทร

จากผลการทดสอบจะเห็นได้ว่าหากปริมาณข้อมูลมีมากขึ้นจะส่งผลทำให้การประมวลผลในการตรวจจับใช้เวลาเพิ่มขึ้นดังแสดงเป็นกราฟได้ดังภาพที่ 4.1 ซึ่งเหตุที่ทำการทดสอบในปริมาณข้อมูลที่น้อยไปจนถึงปริมาณข้อมูลที่มากเพราะในความเป็นจริงแล้วข้อมูลการโทรในชุมสายในแต่ละช่วงเวลาอาจมากน้อยแตกต่างกัน หากมีข้อมูลการโทรในปริมาณมาก ระบบ

ตรวจจับการลักลอบใช้งานก็จะใช้เวลาการประมวลผลเพิ่มขึ้น ส่งผลทำให้การตรวจจับได้ช้าลง นอกจากนี้แล้วยังมีค่าสภาวะแวดล้อมอื่นๆ เช่น เวลาในการที่ต้องรอในการดึงข้อมูลจากเครื่องแม่ข่าย เวลาที่ทำการหน่วงเวลาในการแสดงผลบนเว็บบราวเซอร์ เป็นต้น

ในส่วนของการทดสอบความถูกต้องของระบบ พบว่าสามารถตรวจจับได้ 100% โดยเมื่อทำการแยกว่าเป็นการลักลอบใช้งานจริงหรือไม่ พบว่าการเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยงมีมากที่สุด และในกรณีการใช้งานเป็นเวลานานจนเกิดผิดสังเกตจะน้อยที่สุด ซึ่งในความเป็นจริงแล้วการให้บริการโทรศัพท์ระหว่างประเทศ ผู้ใช้งานส่วนมากจะมีการเรียกออกไปยังต่างประเทศมากกว่าการเรียกใช้ภายในประเทศ ดังนั้นโอกาสที่จะมีการลักลอบใช้โดยการเรียกออกไปยังประเทศที่เป็นกลุ่มเสี่ยงย่อมมีโอกาสเกิดได้มากกว่า

4.3 การทดลองตรวจจับโดยตัวแบบที่ได้ทำการออกแบบและพัฒนา

ในส่วนของการทดลองประกอบไปด้วย การทดลองด้วยตัวแบบนาอีฟย์เบย์เซียน (NB: Naïve Bayesian) การทดลองด้วยตัวแบบโครงข่ายประสาทเทียม (ANN: Artificial Neural Network) การทดลองด้วยการประยุกต์ตัวแบบนาอีฟย์เบย์เซียนและโครงข่ายประสาทเทียมรวมถึงการนำไวท์ลิสต์มาประยุกต์ (NB-ANN with White list) โดยผลการทดสอบในการคำนวณเปอร์เซ็นต์ความถูกต้องของการตรวจจับสามารถคำนวณได้ดังนี้

$$\%Correct = \frac{N_{fraud}}{N_{found}}\ x\ 100 \quad \text{เมื่อ} \quad N_{found} \text{ ไม่เท่ากับ } 0 \tag{4.1}$$

$$\%\text{Correct} = 100 \text{ เมื่อ } N_{found} = N_{fraud} = 0 \tag{4.2}$$

โดย

%Correct แทนค่าเปอร์เซ็นต์ความถูกต้องในการตรวจจับได้

N_{found} แทนจำนวนครั้งของการลักลอบใช้ที่ตรวจจับได้ โดย $N_{found} \geq N_{fraud}$ เสมอ เนื่องจากในส่วนของการตรวจจับได้อ้างอิงกับตัวแบบที่ได้ทำการออกแบบระยะแรก นั่นคือ การใช้งานเป็นเวลานานจนเกิดผิดสังเกต การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด การมีพฤติกรรมการโทรแปลกๆโดยมีการเข้ามาลักษณะตรวจสอบโครงข่ายแล้วกระหน่ำโทร โดยทั้ง 4 กรณีได้ครอบคลุมการตรวจจับได้ 100% ดังนั้นในขั้นตอนของการตรวจจับจึงอาจตรวจจับได้เท่ากับหรือมากกว่าความเป็นจริงที่เกิดจากการลักลอบใช้งานจริง ซึ่งในอนาคตหากมีรูปแบบของตัวแบบที่

เปลี่ยนไปที่เกิดจากขั้นตอนของการเรียนรู้ใหม่ จำเป็นที่ต้องทำการปรับปรุงข้อมูลในส่วนการตัดสินใจนี้เพิ่มเติม

N_{fraud} แทนจำนวนครั้งที่เกิดการลักลอบใช้งานจริง

โดยในการทดลองมีรายละเอียดดังนี้

4.3.1 การทดลองด้วยตัวแบบนาอีฟย์เบย์เซียน

ในการทดลองด้วยตัวแบบนาอีฟย์เบย์เซียนจะใช้กลุ่มข้อมูลนำเข้าปี ค.ศ. 2013 ถึง มิถุนายน ค.ศ. 2016 โดยได้ทำการแบ่งข้อมูลออกเป็น 10 ชุด ทำการใช้ฝึกหัดจำนวน 9 ชุดและใช้ทดสอบจำนวน 1 ชุด โดยทำการสลับข้อมูลการฝึกหัดและการทดสอบจำนวน 10 ครั้ง โดยมีรายละเอียดผลการทดลองดังตารางที่ 4.3

ตารางที่ 4.3 ผลการทดลองโดยใช้ตัวแบบนาอีฟย์เบย์เซียน

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ				
1	05/2013 – 06/ 2016	01– 04/2013	74,451	4	98	4.081633
2	01 – 04/ 2013 และ 09/2013 – 06/2016	05 – 08/2013	104,965	7	105	6.666667
3	01 – 08/ 2013 และ 01/2014 – 06/2016	09 – 12/2013	128,993	4	78	5.128205
4	01 – 12/ 2013 และ 05/2014 – 06/2016	01 – 04/2014	152,106	0	57	0

ตารางที่ 4.3 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ				
5	01/2013 – 04/2014 และ 09/2014 – 06/2016	05 – 08/2014	187,110	0	49	0
6	01/2013 – 08/2014 และ 01/2015 – 06/2016	09 – 12/2014	223,794	39	533	7.317073
7	01/2013 – 12/2014 และ 05/2015 – 06/2016	01 – 04/2015	251,238	48	746	6.434316
8	01/2013 – 04/2015 และ 09/2015 – 06/2016	05 – 08/2015	288,457	4	132	3.030303
9	01/2013 – 08/2015 และ 01/2016 – 06/2016	09 – 12/2015	328,440	1	22	4.545455
10	01/2013 – 12/2015	01 – 06/2016	562,345	1	31	3.225806

จากผลการทดลองข้างต้นพบว่าจำนวนข้อมูลที่เกิดการลักลอบใช้จริงมีจำนวน 108 แถว พบว่ามีการตรวจจับได้จากการใช้ตัวแบบนาอีฟย์เบย์เซียนจำนวน 1,851 แถว ดังนั้นจะมีความถูกต้องในการตรวจจับโดยเฉลี่ยอยู่ที่ 5.83 %

4.3.2 การทดลองด้วยตัวแบบโครงข่ายประสาทเทียม

ในการทดลองด้วยตัวแบบโครงข่ายประสาทเทียมจะใช้กลุ่มข้อมูลนำเข้าปี ค.ศ. 2013 ถึง มิถุนายน ค.ศ. 2016 โดยได้ทำการแบ่งข้อมูลออกเป็น 10 ชุด ทำการใช้ฝึกหัดจำนวน 9 ชุดและใช้ทดสอบจำนวน 1 ชุด โดยทำการสลับข้อมูลการฝึกหัดและการทดสอบจำนวน 10 ครั้ง โดยมีรายละเอียดผลการทดลองดังตารางที่ 4.4

ตารางที่ 4.4 ผลการทดลองโดยใช้ตัวแบบโครงข่ายประสาทเทียม

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
1	05/2013 – 06/ 2016	01– 04/2013	74,451	4	1	205	1.951219512
					2	89	4.494382022
					3	76	5.263157895
					4	75	5.333333333
					5	75	5.333333333
					6	76	5.263157895
					7	77	5.194805195
					8	80	5
					9	81	4.938271605
					10	78	5.128205128

ตารางที่ 4.4 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
2	01 – 04/2013 และ 09/2013 – 06/2016	05 – 08/2013	104,965	7	1	472	1.483051
					2	186	3.763441
					3	143	4.895105
					4	146	4.794521
					5	138	5.072464
					6	142	4.929577
					7	137	5.109489
					8	137	5.109489
					9	137	5.109489
					10	137	5.109489
3	01 – 08/2013 และ 01/2014 – 06/2016	09 – 12/2013	128,993	4	1	212	1.886792
					2	117	3.418803
					3	73	5.479452
					4	75	5.333333
					5	75	5.333333
					6	73	5.479452
					7	75	5.333333
					8	72	5.555556
					9	72	5.555556
					10	72	5.555556

ตารางที่ 4.4 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
4	01 – 12/ 2013 และ 05/2014 – 06/2016	01 – 04/2014	152,106	0	1	103	0
					2	78	0
					3	65	0
					4	65	0
					5	78	0
					6	72	0
					7	78	0
					8	78	0
					9	78	0
					10	78	0
5	01/2013 – 04/2014 และ 09/2014 – 06/2016	05 – 08/2014	187,110	0	1	137	0
					2	114	0
					3	108	0
					4	97	0
					5	94	0
					6	105	0
					7	105	0
					8	105	0
					9	105	0
					10	105	0

ตารางที่ 4.4 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
6	01/2013 – 08/2014 และ 01/2015 – 06/2016	09 – 12/2014	223,794	39	1	2127	1.833568
					2	742	5.256065
					3	494	7.894737
					4	494	7.894737
					5	502	7.768924
					6	502	7.768924
					7	502	7.768924
					8	511	7.632094
					9	511	7.632094
					10	511	7.632094
7	01/2013 – 12/2014 และ 05/2015 – 06/2016	01 – 04/2015	251,238	48	1	3224	1.488834
					2	1047	4.584527
					3	742	6.469003
					4	759	6.324111
					5	807	5.947955
					6	807	5.947955
					7	805	5.962733
					8	807	5.947955
					9	812	5.91133
					10	812	5.91133

ตารางที่ 4.4 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
8	01/2013 – 04/2015 และ 09/2015 – 06/2016	05 – 08/2015	288,457	4	1	257	1.55642
					2	98	4.081633
					3	76	5.263158
					4	76	5.263158
					5	82	4.878049
					6	81	4.938272
					7	81	4.938272
					8	77	5.194805
					9	77	5.194805
					10	77	5.194805
9	01/2013 – 08/2015 และ 01/2016 – 06/2016	09 – 12/2015	328,440	1	1	112	0.892857
					2	94	1.06383
					3	73	1.369863
					4	73	1.369863
					5	86	1.162791
					6	83	1.204819
					7	83	1.204819
					8	83	1.204819
					9	85	1.176471
					10	85	1.176471

ตารางที่ 4.4 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
10	01/2013 – 12/2015	01 – 06/2016	562,345	1	1	96	1.041667
					2	75	1.333333
					3	72	1.388889
					4	72	1.388889
					5	76	1.315789
					6	82	1.219512
					7	82	1.219512
					8	82	1.219512
					9	85	1.176471
					10	85	1.176471

จากผลการทดลองข้างต้นจะได้ค่าเฉลี่ยความถูกต้องในการตรวจจับแยกตามจำนวนโหนดซ่อน ดังตารางที่ 4.5

ตารางที่ 4.5 ค่าเฉลี่ยความถูกต้องในการตรวจจับแยกตามจำนวนโหนดซ่อน

จำนวนโหนด	ค่าเฉลี่ย % ความถูกต้อง
1	1.555076
2	4.090909
3	5.619147
4	5.590062
5	5.365127
6	5.338606
7	5.333333
8	5.314961
9	5.286344
10	5.294118

4.3.3 การทดลองด้วยการประยุกต์ตัวแบบนาอีฟย์เบย์เซียนและโครงข่ายประสาทเทียมรวมถึงการนำไวท์ลิสต์มาประยุกต์

ในการทดลองด้วยตัวแบบโครงข่ายประสาทเทียมจะใช้กลุ่มข้อมูลนำเข้าปี ค.ศ. 2013 ถึง มิถุนายน ค.ศ. 2016 โดยได้ทำการแบ่งข้อมูลออกเป็น 10 ชุด ทำการใช้ฝึกหัดจำนวน 9 ชุดและใช้ทดสอบจำนวน 1 ชุด โดยทำการสลับข้อมูลการฝึกหัดและการทดสอบจำนวน 10 ครั้ง รวมถึงการทดสอบที่จำนวนโหนดซ่อนที่แตกต่างกันโดยเริ่มตั้งแต่จำนวนโหนดซ่อนเท่ากับ 1 โหนดจนถึง 10 โหนด โดยมีรายละเอียดผลการทดลองดังตารางที่ 4.5

ตารางที่ 4.6 ผลการทดลองโดยประยุกต์ตัวแบบนาอีฟย์เบย์เซียนและโครงข่ายประสาทเทียมรวมถึงการนำไวท์ลิสต์มาประยุกต์

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
1	05/2013 – 06/ 2016	01– 04/2013	74,451	4	1	37	10.81081
					2	28	14.28571
					3	11	36.36364
					4	5	80
					5	6	66.66667
					6	14	28.57143
					7	15	26.66667
					8	12	33.33333
					9	12	33.33333
					10	12	33.33333
2	01 – 04/ 2013 และ 09/2013 – 06/2016	05 – 08/2013	104,965	7	1	52	13.46154
					2	37	18.91892
					3	20	35
					4	8	87.5
					5	11	63.63636
					6	26	26.92308
					7	27	25.92593
					8	24	29.16667
					9	24	29.16667
					10	23	30.43478

ตารางที่ 4.6 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
3	01 – 08/ 2013 และ 01/2014 – 06/2016	09 – 12/2013			1	27	14.81481
					2	22	18.18182
					3	14	28.57143
					4	4	100
					5	4	100
					6	12	33.33333
					7	12	33.33333
					8	11	36.36364
					9	10	40
			128,993	4	10	11	36.36364
4	01 – 12/ 2013 และ 05/2014 – 06/2016	01 – 04/2014			1	2	0
					2	3	0
					3	2	0
					4	0	100
					5	0	100
			152,106	0	6	1	0
					7	1	0
					8	2	0
					9	2	0
					10	2	0

ตารางที่ 4.6 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
					7	1	0
					8	2	0
					9	2	0
					10	2	0
5	01/2013 – 04/2014 และ 09/2014 – 06/2016	05 – 08/2014	187,110	0	1	4	0
					2	2	0
					3	2	0
					4	0	100
					5	1	0
					6	2	0
					7	3	0
					8	2	0
					9	2	0
					10	2	0
6	01/2013 – 08/2014 และ 01/2015 – 06/2016	09 – 12/2014	223,794	39	1	305	12.78689
					2	278	14.02878
					3	86	45.34884
					4	41	95.12195
					5	53	73.58491

ตารางที่ 4.6 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
					6	107	36.4486
					7	96	40.625
					8	102	38.23529
					9	114	34.21053
					10	118	33.05085
7	01/2013 – 12/2014 และ 05/2015 – 06/2016	01 – 04/2015	251,238	48	1	417	11.51079
					2	342	14.03509
					3	156	30.76923
					4	51	94.11765
					5	63	76.19048
					6	152	31.57895
					7	156	30.76923
					8	137	35.0365
					9	141	34.04255
					10	134	35.8209

ตารางที่ 4.6 (ต่อ)

ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
8	01/2013 – 04/2015 และ 09/2015 – 06/2016	05 – 08/2015	288,457	4	1	32	12.5
					2	28	14.28571
					3	15	26.66667
					4	5	80
					5	7	57.14286
					6	22	18.18182
					7	21	19.04762
					8	13	30.76923
					9	14	28.57143
					10	14	28.57143
9	01/2013 – 08/2015 และ 01/2016 – 06/2016	09 – 12/2015	328,440	1	1	9	11.11111
					2	7	14.28571
					3	2	50
					4	1	100
					5	1	100
					6	3	33.33333
					7	3	33.33333
					8	5	20
					9	5	20

ตารางที่ 4.6 (ต่อ)

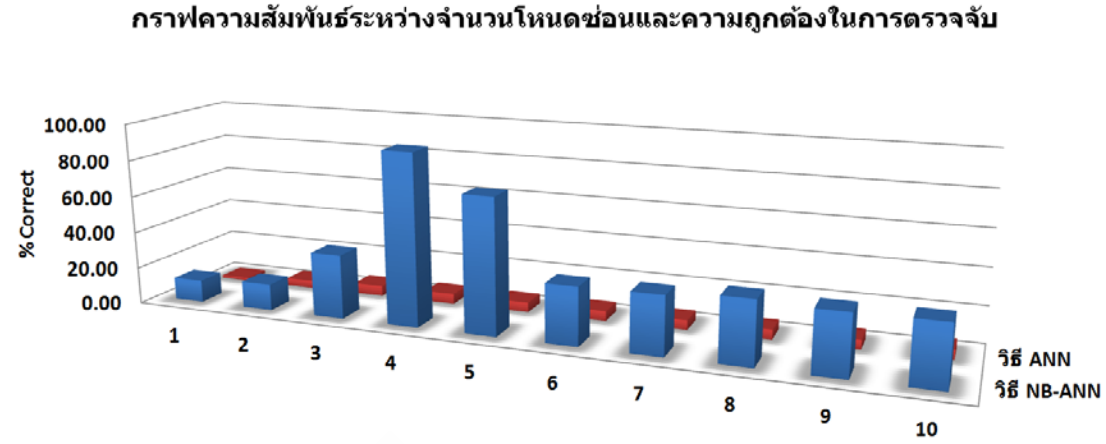
ครั้งที่	ช่วงเวลาของข้อมูล		จำนวนข้อมูล (Records)	จำนวนการลักลอบจริง (Records)	จำนวนโหนดซ่อน	จำนวนการตรวจจับได้ (Records)	% ความถูกต้องในการตรวจจับได้
	ฝึกหัด	ทดสอบ					
					10	5	20
10	01/2013 – 12/2015	01 – 06/2016			1	7	14.28571
					2	6	16.66667
					3	2	50
					4	1	100
					5	1	100
					6	4	25
					7	5	20
					8	5	20
					9	4	25
			562,345	1	10	4	25

จากผลการทดลองข้างต้นจะได้ค่าเฉลี่ยความถูกต้องในการตรวจจับแยกตามจำนวนโหนดซ่อน ดังตารางที่ 4.7

ตารางที่ 4.7 ค่าเฉลี่ยความถูกต้องในการตรวจจับแยกตามจำนวนโหนดซ่อน

จำนวนโหนด	ค่าเฉลี่ย % ความถูกต้อง
1	12.10762
2	14.34263
3	34.83871
4	93.10345
5	73.46939
6	31.48688
7	31.85841
8	34.50479
9	32.92683
10	33.23077

ในการทดสอบพบว่าในกรณีการใช้ตัวแบบนาอีฟย์เบย์เซียน (วิธี NB) พบว่าสามารถตรวจจับได้ถูกต้องโดยเฉลี่ย 5.83% ในกรณีการใช้เฉพาะตัวแบบการตรวจจับด้วยโครงข่ายประสาทเทียม (วิธี ANN) จำนวนโหนดซ่อนที่เหมาะสมคือ 3 โหนด มีความถูกต้องอยู่ที่ 5.62% ในกรณีของการใช้ตัวแบบการตรวจจับด้วยนาอีฟเบย์เซียนและโครงข่ายประสาทเทียม (วิธี NB-ANN with Whitelist) พบว่าจำนวนโหนดซ่อนที่เหมาะสมอยู่ที่ 4 โหนด ความถูกต้องอยู่ที่ 93.10% โดยผลการทดลองดังภาพที่ 4.5



	1	2	3	4	5	6	7	8	9	10
วิธี NB-ANN	12.11	14.34	34.84	93.10	73.47	31.49	31.86	34.50	32.93	33.23
วิธี ANN	1.56	4.09	5.62	5.59	5.35	5.34	5.33	5.31	5.29	5.29

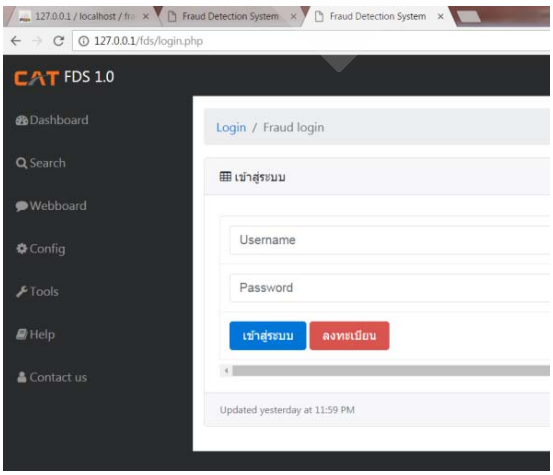
ภาพที่ 4.5 กราฟความสัมพันธ์ระหว่างจำนวนโหนดซ่อนและ % ความถูกต้องของแต่ละวิธี

4.4 การทดสอบระบบที่ทำการพัฒนาเพื่อใช้ตรวจจับการลักลอบ

ในขั้นตอนของการทดสอบระบบที่ทำการพัฒนาเพื่อใช้ในการตรวจจับการลักลอบใช้สามารถเข้าไปยังระบบผ่านเว็บบราวน์เซอร์ โดยมีรายละเอียดดังนี้

4.4.1 การเข้าสู่ระบบ

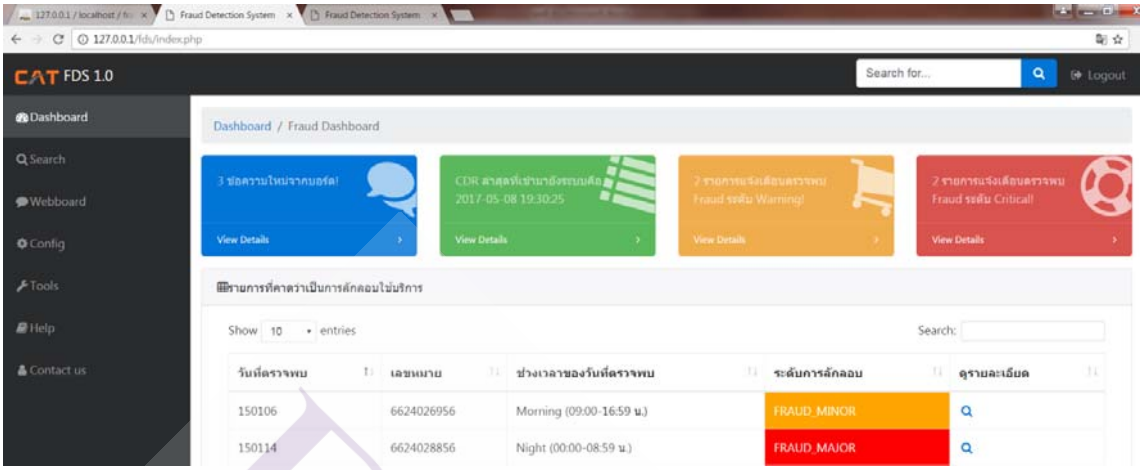
ในขั้นตอนของการเข้าสู่ระบบในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/login.php ดังภาพที่ 4.6



ภาพที่ 4.6 การเข้าสู่ระบบ (1)

4.4.2 การเข้าดูรายการการแจ้งเตือนผ่านหน้า Dashboard

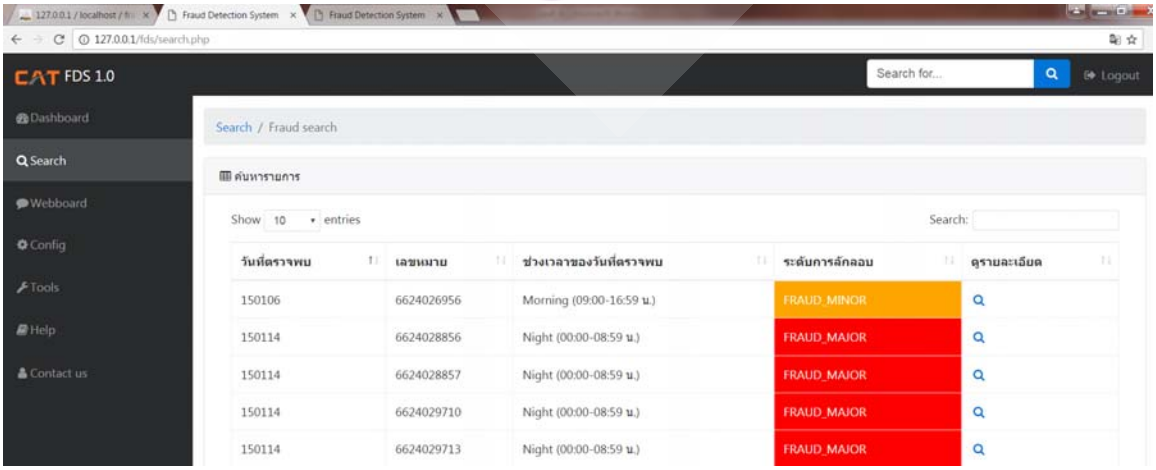
ในขั้นตอนของการดูรายงานการแจ้งเตือนในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/index.php ดังภาพที่ 4.7



ภาพที่ 4.7 การเข้าสู่ระบบ (2)

4.4.3 การค้นหาข้อมูลการเกิดการลักลอบ

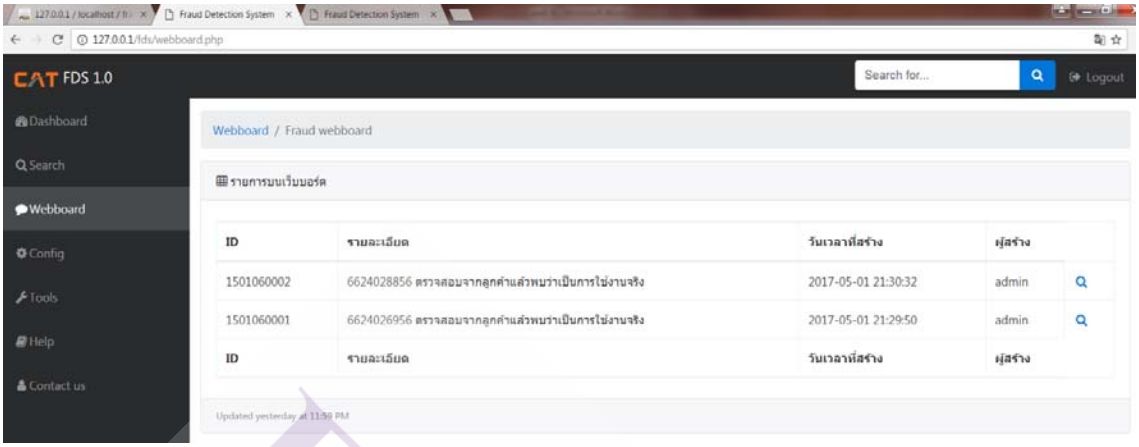
ในขั้นตอนของการค้นหาข้อมูลการเกิดการลักลอบ ในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/search.php ดังภาพที่ 4.8



ภาพที่ 4.8 การค้นหาข้อมูลการเกิดการลักลอบ

4.4.4 การเข้าดูรายการข้อมูลบน Webboard

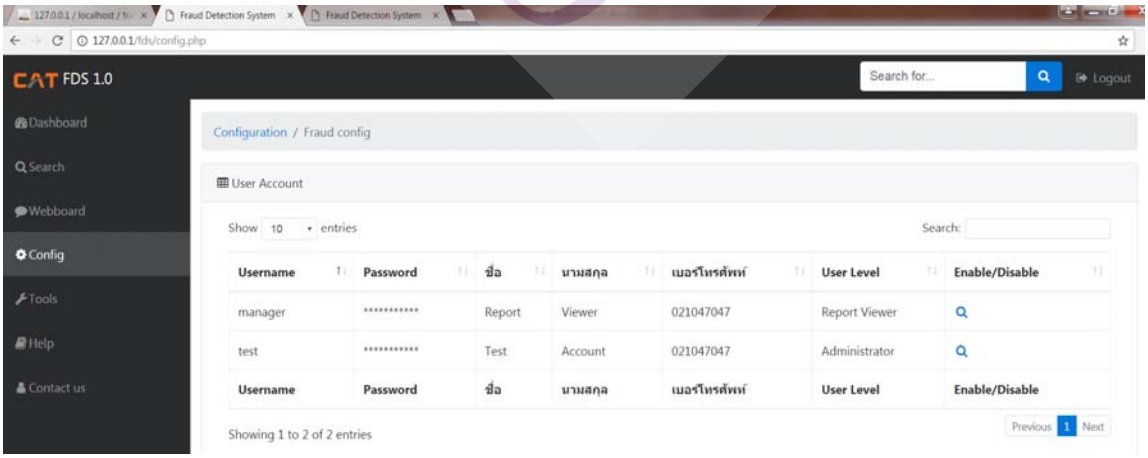
ในขั้นตอนของเข้าดูรายการข้อมูลบน Webboard ในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/webboard.php ดังภาพที่ 4.9



ภาพที่ 4.9 การเข้าดูรายการข้อมูลบน Webboard

4.4.5 การเข้าปรับแต่งข้อมูล Config

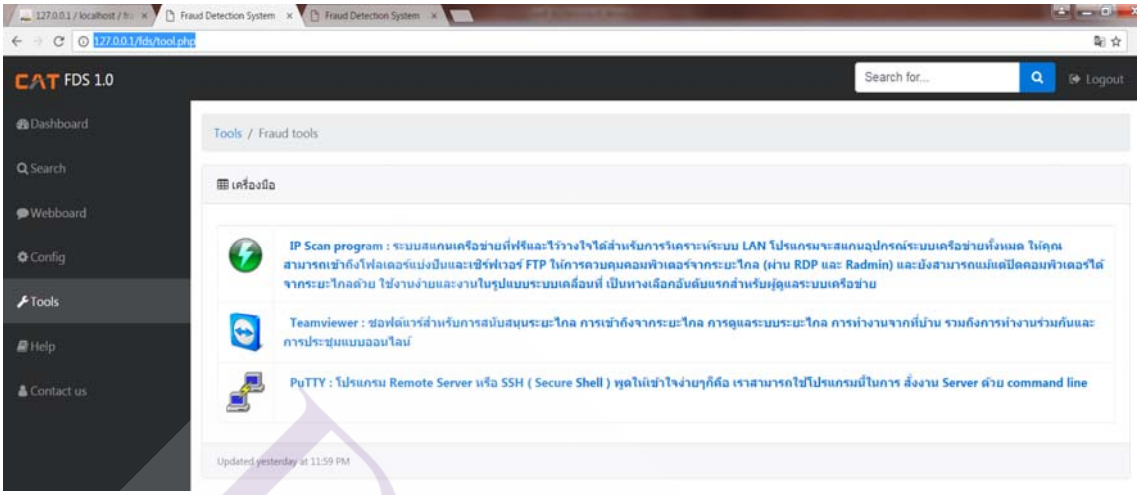
ในขั้นตอนของเข้าปรับแต่งข้อมูล Config ในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/config.php ดังภาพที่ 4.10



ภาพที่ 4.10 การเข้าปรับแต่งข้อมูล Config

4.4.6 การเข้าดูรายการข้อมูลเครื่องมือ

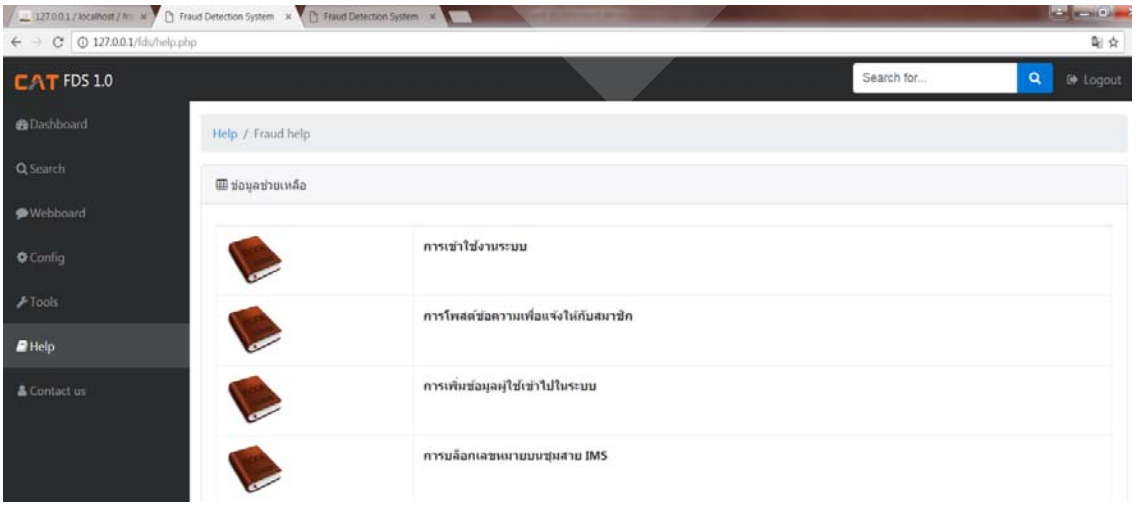
ในขั้นตอนของเข้าดูรายการข้อมูลเครื่องมือ (Tools) ในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/tool.php ดังภาพที่ 4.11



ภาพที่ 4.11 การเข้าดูรายการข้อมูลเครื่องมือ

4.4.7 การเข้าดูรายการข้อมูลช่วยเหลือ

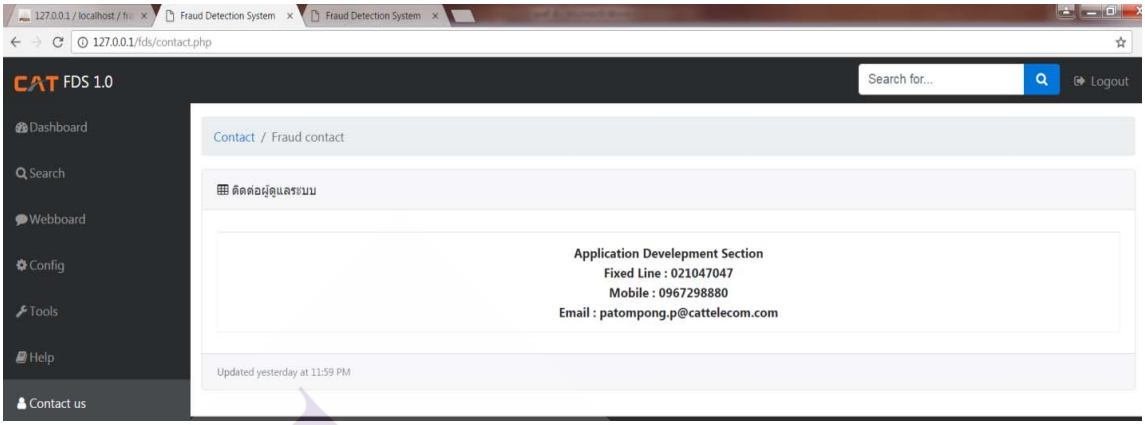
ในขั้นตอนของเข้าดูรายการข้อมูลช่วยเหลือ (Help) ในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/help.php ดังภาพที่ 4.12



ภาพที่ 4.12 การเข้าดูรายการข้อมูลช่วยเหลือ

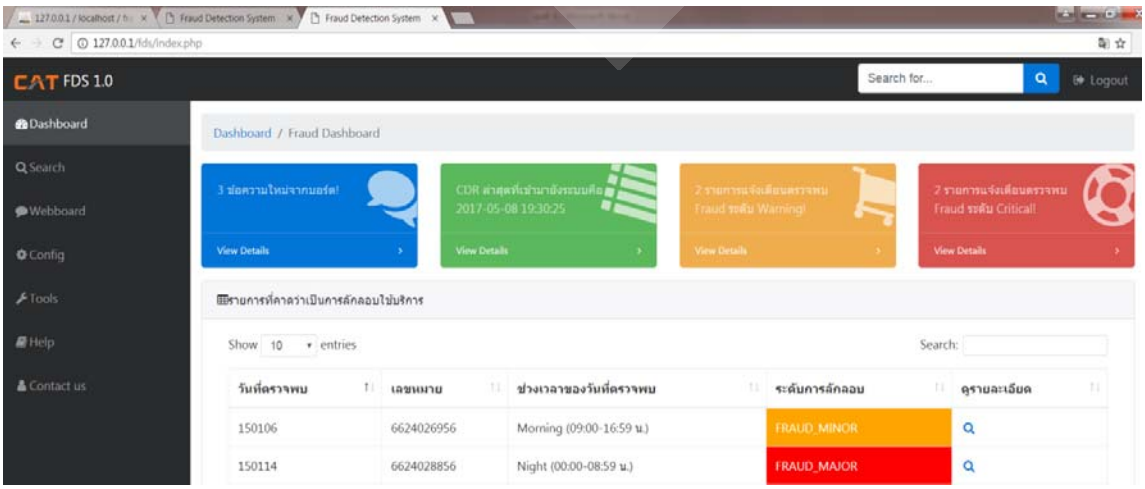
4.4.8 การเข้าดูรายการติดต่อผู้ดูแลระบบ

ในขั้นตอนของเข้าดูรายการติดต่อผู้ดูแลระบบ (Contact) ในการทดลองจะใช้ผ่าน Localhost โดยผ่าน URL : http://127.0.0.1/fds/contact.php ดังภาพที่ 4.13

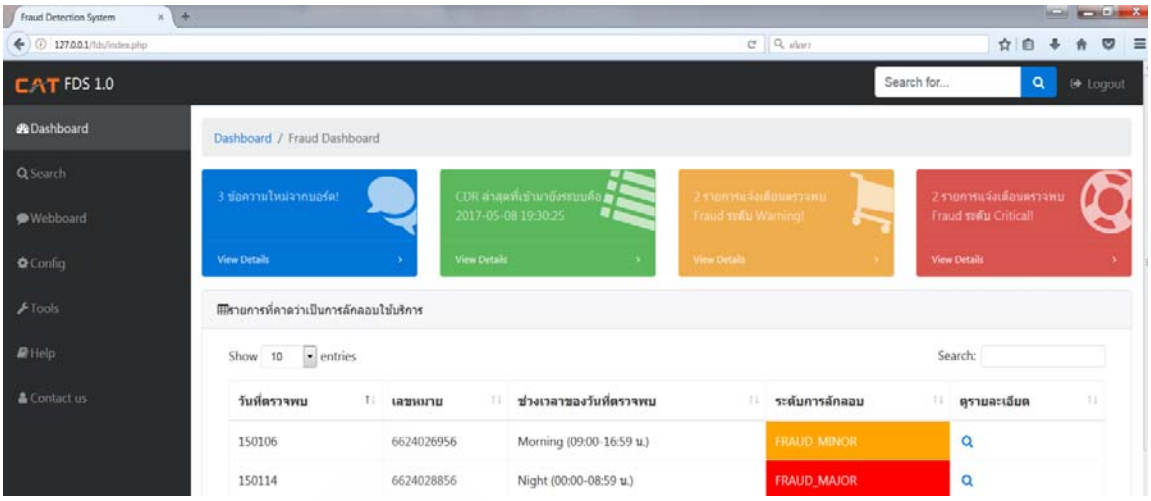


ภาพที่ 4.13 การเข้าดูรายการติดต่อผู้ดูแลระบบ

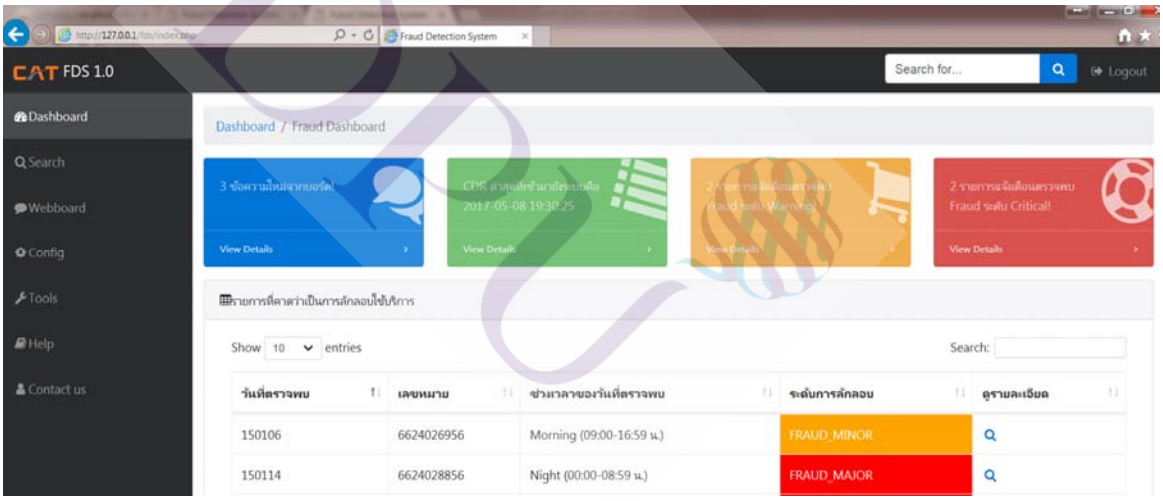
โดยจากการทดลองพบว่าสามารถดึงข้อมูลที่ถูกจัดเก็บไว้บนฐานข้อมูลได้อย่างถูกต้อง และสามารถปรับปรุงข้อมูล แก้ไขข้อมูล เพิ่มข้อมูลได้ และสามารถรองรับกับเว็บบราวน์เซอร์ได้หลากหลาย อาทิ Google Chrome, Mozilla Firefox, Internet Explorer, Zafari และสามารถทำงานรับกับอุปกรณ์สมาร์ทโฟน แท็บเล็ต เนื่องจากการออกแบบหน้าเว็บให้ตอบสนองต่ออุปกรณ์อย่างหลากหลาย (Responsive Design) โดยตัวอย่างการทดสอบดังภาพที่ 4.14 ถึง 4.17



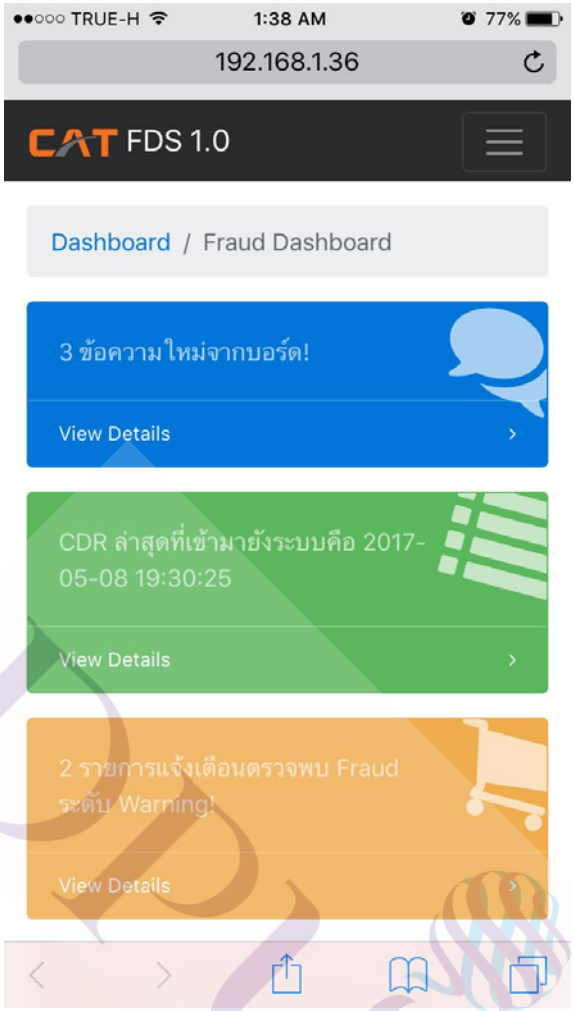
ภาพที่ 4.14 การทดสอบการเข้าใช้งานผ่าน Google Chrome



ภาพที่ 4.15 การทดสอบการเข้าใช้งานผ่าน Mozilla Firefox



ภาพที่ 4.16 การทดสอบการเข้าใช้งานผ่าน Internet Explorer



ภาพที่ 4.17 การทดสอบการเข้าใช้งานผ่าน Smart Phone ด้วย Safari

สรุป

จากการทดลองที่ได้แบ่งออกเป็น 3 ส่วน คือ การทดสอบตามเงื่อนไขการตรวจจับที่ได้กำหนดไว้ พบว่ามีความถูกต้องเพียงประมาณ 5% เมื่อเทียบกับกรณีที่เป็นการลักลอบใช้ที่เกิดขึ้นจริง และส่วนต่อมาคือการทดสอบตามตัวแบบที่ได้ทำการออกแบบและพัฒนาพบว่ามีความถูกต้องสูงสุดถึง 93% เมื่อเทียบกับกรณีที่เป็นการลักลอบใช้ที่เกิดขึ้นจริง ส่วนสุดท้ายคือการทดสอบระบบที่ทำการพัฒนาเพื่อใช้ตรวจจับการลักลอบสามารถแสดงผลข้อมูลที่ตรวจจับได้อย่างถูกต้อง รวมถึงการรองรับการทำงานกับหลากหลายเว็บบราวน์เซอร์ ซึ่งเป็นไปตามวัตถุประสงค์ของงานวิจัยนี้ ในบทต่อไปจะกล่าวถึงบทสรุปและการวิเคราะห์ผลการทดลอง รวมถึงงานวิจัยที่สามารถนำไปต่อยอดในอนาคตได้

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้ได้แบ่งการทดสอบออกเป็น 3 ส่วน คือ การทดสอบตามเงื่อนไขการตรวจจับที่ได้กำหนดไว้ การทดสอบตามตัวแบบที่ได้ทำการออกแบบและพัฒนา และการทดสอบระบบที่ทำการพัฒนาเพื่อใช้ตรวจจับการลักลอบ โดยบทสรุปและข้อเสนอแนะมีรายละเอียดดังนี้

5.1 วิเคราะห์ผลการทดลอง

ในส่วนของการทดลองแรกเป็นการทดลองโดยใช้ปริมาณข้อมูลที่แตกต่างกันรวมถึงการใช้เงื่อนไขในการตรวจจับทั้ง 4 เงื่อนไข ได้แก่ การใช้งานเป็นเวลานานจนเกิดผิดสังเกต การเรียกออกไปยังประเทศกลุ่มเป้าหมายที่ทางชุมสายกำหนดว่าเป็นประเทศกลุ่มเสี่ยง การใช้งานเกินมาตรฐานที่ทางชุมสายกำหนด สุดท้ายคือการมีพฤติกรรมตรวจสอบโครงข่ายแล้วกระหน่ำโทร โดยพบว่าตัวแบบตรวจจับมีความถูกต้องเพียง 5% เมื่อเทียบกับการลักลอบใช้งานที่เกิดขึ้นจริง เหตุผลเนื่องจากโดยส่วนใหญ่แล้วพบว่าเป็นพฤติกรรมการ ใช้งานของลูกค้าในชีวิตประจำวัน เช่น ลูกค้าบางรายชอบโทรเป็นเวลานาน หรือบางรายมีการโทรไปประเทศกลุ่มเสี่ยงแต่เป็นการใช้งานจริงจากลูกค้า เป็นต้น ส่งผลให้การคาดการณ์จากเงื่อนไขการตรวจจับดังกล่าวมีความถูกต้องหรือตรวจพบว่าเป็นการถูกลักลอบใช้งานน้อยมาก กอปรกับทั้งไม่มีการตรวจสอบจากข้อมูลในอดีตว่าเคยมีลักษณะการโทรแบบดังกล่าวหรือไม่

ในส่วนของการทดลองที่สองเป็นการพัฒนาตัวแบบโดยการประยุกต์ระหว่างตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียม พบว่าสามารถตรวจจับได้ถูกต้องถึงประมาณ 93% เมื่อเทียบกับการลักลอบใช้งานที่เกิดขึ้นจริง เหตุผลเนื่องจากการนำตัวแบบทั้งสองมาประยุกต์โดยอาศัยข้อมูลที่ได้จากตัวแบบนาอีฟเบย์เซียนซึ่งเป็นข้อมูลนำเข้าให้กับตัวแบบโครงข่ายประสาทเทียม รวมถึงการนำข้อมูลในอดีตของลูกค้าว่าเคยเกิดลักษณะการโทรดังกล่าวหรือไม่ ซึ่งถ้าหากเคยซึ่งถือเป็นเหตุการณ์ปกติของลูกค้ารายนั้น ก็จะถูกแจ้งเตือนในระดับเฝ้าระวัง ส่งผลให้ภาพรวมการตรวจจับมีความถูกต้องมากยิ่งขึ้น

ในส่วนของการทดลองระบบที่ได้ทำการออกแบบและพัฒนา สามารถแสดงผลข้อมูลได้ถูกต้อง และยังสามารถรองรับอุปกรณ์ได้อย่างหลากหลาย เนื่องจากมีการออกแบบให้รองรับกับอุปกรณ์หลากหลาย (Responsive Design) รวมถึงการแยกการทำงานกันชัดเจนระหว่างส่วน

ประมวลผลเบื้องหลัง (Background Process) และส่วนแสดงผล ทำให้มีความรวดเร็วในการค้นหาข้อมูล ไม่ดึงทรัพยากรระหว่างกัน

5.2 สรุปผลการทดลอง

5.2.1 สรุปผลการวิจัยตามการบรรลุวัตถุประสงค์

5.2.1.1 เพื่อศึกษาและพัฒนาขั้นตอนวิธีในการตรวจจับการลักลอบใช้งานบนโครงข่ายเอ็นจีเอ็น

ผู้วิจัยได้ทำการศึกษาเงื่อนไขในการตรวจจับเบื้องต้น รวมถึงการพัฒนาตัวแบบที่เป็นการประยุกต์ระหว่างตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียม

5.2.1. 2 เพื่อพัฒนาระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น

ผู้วิจัยได้ทำการพัฒนาระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็น โดยได้พัฒนาแบ่งออกเป็นสองส่วนหลักได้แก่ ส่วนของการประมวลผลพื้นหลัง (Background Process) และส่วนของการแสดงผลโดยอยู่ในรูปแบบของเว็บแอพพลิเคชัน ซึ่งสามารถรองรับกับอุปกรณ์และเว็บบราวน์เซอร์ได้หลากหลาย

5.2.2 สรุปผลการวิจัยตามขอบเขต

สรุปผลการวิจัยตามขอบเขตของงานวิจัยที่ได้กำหนดไว้ จากการทดสอบตามขอบเขตสามารถทำงานได้ตามขอบเขตที่กำหนดไว้ทุกข้อ โดยมีผลการทดสอบตามขอบเขตสรุปได้ตามตารางที่ 5.1

ตารางที่ 5.1 สรุปผลการทดสอบตามขอบเขตของงานวิจัย

ลำดับ	ความสามารถของระบบ	ผลการทดลอง	
		ทำได้	ทำไม่ได้
1	สามารถตรวจจับในลักษณะแบบ Real Time	✓	
2	สามารถพยากรณ์ได้ว่าอาจมีการเกิดการลักลอบใช้งาน	✓	
3	สามารถแสดงผลการตรวจจับได้ในรูปแบบของเว็บแอพพลิเคชัน	✓	
4	สามารถเชื่อมต่อเข้ากับระบบโครงข่ายโดยผ่านอุปกรณ์จัดเก็บข้อมูลการโทร	✓	
5	สามารถประมวลผลข้อมูลการโทรแบบคู่ขนาน (Parallel)	✓	
6	สามารถแสดงผลรายงานออกมาเป็นกราฟและตาราง	✓	
7	สามารถแจ้งเตือนกรณีการเกิดการลักลอบใช้ผ่านทาง E-mail ของผู้ดูแลระบบ	✓	
8	สามารถเชื่อมต่อเพื่อใช้ตรวจจับการลักลอบใช้กับโครงข่ายอื่น	✓	

5.3 ข้อจำกัดของระบบ

5.3.1 ข้อมูลการโทรที่ได้จะช้ากว่าเวลาปัจจุบันประมาณ 30 นาที – 1 ชั่วโมง เนื่องจากที่ชุมสายมีการคลายข้อมูล CDR ทุกๆ 30 นาที และทำการประมวลผลรวมถึงการจัดเก็บลงบนฐานข้อมูล ซึ่งใช้เวลาพอสมควร

5.3.2 ในกระบวนการฝึกหัด ระบบยังไม่สามารถกำหนดให้เรียนรู้ได้เองอย่างอัตโนมัติ จำเป็นต้องทำการป้อนข้อมูลความรู้ใหม่และทำการฝึกหัดใหม่

5.4 ข้อเสนอแนะ

5.4.1 จากผลการศึกษาพบว่ามีกรณีที่เป็นการลักลอบใช้อย่างหลากหลายรูปแบบ ทั้งนี้จำเป็นอย่างยิ่งที่จะต้องหามาตรการในการป้องกันและการหาช่องโหว่ที่จะส่งผลกระทบต่อการให้บริการ

5.4.2 ในเชิงนโยบายการรักษาความปลอดภัยของโครงข่าย กรณีที่เป็นลูกค้ารายใหญ่จำเป็นที่จะต้องกำหนดช่องทางการใช้งานที่เหมาะสม เช่น การระบุ IP Address ที่เข้ามายังโครงข่าย การยืนยันตัวตน หรืออื่นๆ เพื่อลดความสูญเสียที่จะเกิดขึ้น

5.4.3 ในการป้องกันการโดนยึดครองอุปกรณ์เพื่อให้ได้มาซึ่งการเข้าถึงโครงข่าย จำเป็นต้องป้องกันเบื้องต้น เช่น การหมั่นเปลี่ยนรหัสผ่านของอุปกรณ์ การไม่ต่ออุปกรณ์ Voice Gateway โดยตรงกับ Public IP หากเป็นไปได้ให้ทำการต่อหลังผ่านการทำ NAT

5.5 สรุป

ระบบตรวจจับการลักลอบใช้บริการบนโครงข่ายเอ็นจีเอ็นสามารถตรวจจับการลักลอบใช้งานได้ตามเงื่อนไขที่กำหนดไว้ แต่ยังพบปัญหาคือกรณีที่มีปริมาณข้อมูลมาก จะมีความสามารถในการตรวจจับได้ช้าลง เป็นผลเนื่องมาจากค่าสภาวะแวดล้อมต่างๆ รวมถึงในการตรวจสอบจำเป็นต้องทำการประมวลผลทุกๆแถวของข้อมูลโดยเข้าไปตรวจสอบเงื่อนไขทุกเงื่อนไข นอกจากนี้แล้วปัจจัยในการตรวจจับแล้วบอกได้ว่าเป็นการลักลอบใช้หรือไม่นั้นเป็นเรื่องที่คาดเดาได้ยาก เนื่องจากลูกค้าอาจมีการใช้งานจริง ทั้งนี้จำเป็นต้องมีข้อมูลทางสถิติมาช่วยในการตัดสินใจในระบบด้วย รวมถึงมีวิธีการพยากรณ์จากข้อมูลที่ดี ดังนั้นจึงได้ทำการออกแบบและพัฒนาตัวแบบในการตรวจจับโดยประยุกต์ระหว่างตัวแบบนาอีฟเบย์เซียนและตัวแบบโครงข่ายประสาทเทียม รวมถึงการนำข้อมูลในอดีตในการใช้งานของลูกค้ามาทำการวิเคราะห์ประกอบ จากการทดลองจะพบว่าการประยุกต์ตัวแบบการตรวจจับด้วยการประยุกต์ตัวแบบนาอีฟเบย์เซียนและโครงข่ายประสาทเทียมรวมทั้งมีการใช้ข้อมูลเลขหมายที่มีการใช้งานจริงจากเจ้าของเลขหมายกรณีที่เคยตรวจจับได้ (วิธี NB-ANN with Whitelist) สามารถตรวจจับได้แม่นยำถึง 93% แตกต่างจากการใช้ตัวแบบโครงข่ายประสาทเทียมเพียงอย่างเดียว ซึ่งสามารถตรวจจับได้แม่นยำเพียง 5% จากการประยุกต์ตัวแบบดังกล่าวกับงานนั้นพบว่าการเพิ่มการตรวจสอบข้อมูลการใช้งานของเจ้าของเลขหมายในอดีต ส่งผลต่อการพยากรณ์ได้แม่นยำขึ้นเป็นอย่างยิ่ง

สำหรับงานในอนาคตอาจมีการใช้ข้อมูลที่เกี่ยวข้องกับลูกค้า เช่น ข้อมูลประวัติการชำระเงิน ระดับความน่าเชื่อถือ รวมถึงการจัดกลุ่มลูกค้า เพื่อนำมาวิเคราะห์แนวโน้มที่จะเกิดการลักลอบใช้งานโทรศัพท์บนโครงข่ายเอ็นจีเอ็นเพิ่มเติม

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

กิตติพงษ์ สุวรรณราช. (2553). *ออกแบบและติดตั้งระบบโทรศัพท์ IP-PBX ด้วย Asterisk*. กรุงเทพฯ: ออฟเซ็ทเพรส.

ฝ่ายเลขานุการคณะกรรมการเฉพาะกิจจัดมาตรฐานทางเทคนิคสำหรับ Next Generation Network (NGN). (2550). *รายงานสรุปผลการดำเนินงานคณะอนุกรรมการเฉพาะกิจจัดทำมาตรฐานทางเทคนิคสำหรับ Next Generation Network* (NGN). สืบค้นจาก www.ntc.or.th

ศิรมณ์ เสถียรรัมย์. (2553). *ความมั่นคงปลอดภัยกับเทคโนโลยี VoIP*. สืบค้นจาก http://innotech4all.blogspot.com/2010/02/voip.html

ภาษาต่างประเทศ

A. Abdallah, M. Maarof, A. Zainal. (2016). *Fraud detection system.* Journal of Network and Computer Applications,

D. Hoffstadt, S.Monhof, E. Rathgeb. (2011). *"SIP Trace Recorder: Monitor and Analysis Tool for Threats in SIP-based networks."* IEEE.

G. Lun-feng. (2011). *"The Application of Naïve Bayesian Classification in Anti-fraud System of Telecommunications."* Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).

M. Ghosh. (2010). *"Telecoms fraud0"* Computer Fraud & Security.

M. Yelland, *"Fraud in mobile networks."* Computer Fraud & Security, 2013.

M. Ghosh, *"Mobile ID fraud: the downside of mobile growth."* Computer Fraud & Security, 2010.

M. Sahin et al., *"SoK: Fraud in Telephony Networks."*IEEE European Symposium on Security and Privacy, 2017.

S. Qayyum et al., *"Fraudulent Call Detection For Mobile Networks."* Information and Emerging Technologies (ICIET), June 14-16, 2010.

S. Zabkowski, W. Szczesny. (2012). *"Insolvency modeling in the cellular telecommunication industry."* Expert Systems with Applications.

S. Hilas, (2009). *"Designing an expert system for fraud detection in private telecommunications networks."* Expert Systems with Applications.

Y. Rebahi et al., "*On the Use of Unsupervised Techniques for Fraud Detection in VoIP Networks."* Emerging Trends in ICT Security, 2014.

ประวัติผู้เขียน

ชื่อ-นามสกุล	ปฐมพงศ์ ประไพย์
ประวัติการศึกษา	วิทยาศาสตรบัณฑิต (เกียรตินิยมอันดับ 2) สาขาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเชียงใหม่
ตำแหน่งและสถานที่ทำงานปัจจุบัน	โปรแกรมเมอร์ ระดับ 6 หัวหน้าแผนกพัฒนาโปรแกรมส่วนชุมสาย TANDEM และ VoIP นนทบุรี ฝ่ายชุมสายโทรศัพท์ บริษัท กสท โทรคมนาคม จำกัด (มหาชน)

ประสบการณ์ ผลงานทางวิชาการ รางวัลหรือทุนการศึกษาเฉพาะที่สำคัญ

- อดีตนักเรียนทุนเพชรทองกวาว ทุนเรียนดี มหาวิทยาลัยเชียงใหม่
- Assessor Course for ISO/IEC17025 รุ่นที่ 19 สอบผ่านเป็นผู้ประเมินห้อง LAB ทดสอบงานด้านวิศวกรรมคอมพิวเตอร์และโทรคมนาคม, สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม, 2555
- กรรมการวิชาการด้านมาตรฐานผลิตภัณฑ์อุตสาหกรรม หัวข้อ “อุปกรณ์จัดเส้นทางที่ทำหน้าที่เป็น SIP Server” ตามความร่วมมือระหว่างศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) และบริษัท กสท โทรคมนาคม จำกัด (มหาชน), 2555
- Certificate of Fundamental Information Technology Engineers Examination (FE), ITPEC, 2557