การวัดประสิทธิภาพตัวต้นแบบระบบตรวจสอบการบุกรุกบนเครือข่ายเฉพาะบริเวณ

The Intrusion Detection System Network Model of Performance Measurement on Local Area Network

จิรวิญญ์ ดีเจริญชิตพงศ์[1] ธีรภัทร ประวัติรุ่งเรือง[2]
มหาวิทยาลัยนอร์ทกรุงเทพ, มหาวิทยาลัยนอร์ทกรุงเทพ
สาขาวิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ
มหาวิทยาลัยนอร์ทกรุงเทพ

บทคัดย่อ

ในบทความนี้เป็นการนำเสนอการลดคุณลักษณะของชุดข้อมูลเอ็นเอสแอล-เคดีดี (NSL-KDD) เพื่อใช้สำหรับพัฒนาตัวต้นแบบระบบตรวจสอบการบุกรุกบนเครือข่ายเฉพาะบริเวณ โดยมีวัตถุประสงค์เพื่อลดคุณลักษณะ (Attribute) สำหรับใช้ในการจำแนกการบุกรุก และหาประสิทธิภาพความแม่นยำ การดำเนินการวิจัยครั้งนี้ มีการใช้ข้อมูลจากชุดข้อมูลมาตรฐาน NSL-KDD ในการวิเคราะห์รูปแบบการบุกรุก จำนวน 41 คุณลักษณะ 62,984 ระเบียน โดยงานวิจัยจะเลือกใช้วิธีลดคุณลักษณะ 5 วิธี คือ Gain Ratio, Information Gain, RelieF, Symmetrical Uncertainty และ Filtered เพื่อคัดเลือกคุณลักษณะที่ใช้เป็นตัวแทนข้อมูลในการทดสอบไม่น้อยกว่าร้อยละ 80 ขึ้นไปของระเบียนข้อมูล แล้วนำคุณลักษณะที่ได้มาจัดอันดับ (Rang) แล้วทำโหวตหาคุณลักษณะที่เหมาะสมเพื่อใช้สำหรับจำแนกการบุกรุก 4 ประเภท ด้วยกันคือ การโจมตีแบบ Denial-of-Service (DOS), Remote to Local (R2L), User to Root (U2R) และ Probing ผลการโหวตจะได้ 17 คุณลักษณะ ที่สามารถนำมาในการจำแนกการโจมตี และจากการวิจัยพบว่าประสิทธิภาพความแม่นยำในการแยกการโจมตีแบบ DOS เท่ากับ 99.1% การโจมตีแบบ Probe 99.5% การโจมตีแบบ R2L 98.5% และการโจมตีแบบ U2R 99.7% สามารถสรุปได้ว่าการลดคุณลักษณะของข้อมูลส่งผลต่อประสิทธิภาพ โดยให้ค่าสูงประสิทธิภาพสูงกว่าการเลือกคุณลักษณะโดยใช้วิธีการใดวิธีการหนึ่งเพียงอย่างเดียว

คำสำคัญ: การตรวจสอบการบุกรุก, เครือข่ายเฉพาะบริเวณ

Abstract

This article is a demonstration of NSL-KDD feature selection for developing an intrusion detection system model on a local area network. The purpose is to reduce the attribute for use in the classification of Intrusion and find the precision performance. This research data came from the NSL-KDD dataset that were used to analyze the 41 attribute of 62,984 records. The research used five methods to reduce Gain Ratio, Information Gain, Relief, Symmetrical Uncertainty and Filtered for using as a test data substitution for at least 80 percent of data records. Then evaluate attribute ranking and then vote for the appropriate attribute to identify four types of intrusions Denial-of-Service (DOS), Remote to Local (R2L), User to Root (U2R) and Probing. The result of the vote will generate 17 attributes that can be taken in the classification of attacks. 99.1 % DOS attack probability, 99.5% Probe attack probability, 98.5% R2L attack and 99.2% U2R attack.

In summary, the result indicated that reduction of attributes impact higher performance value than feature selection using one of the methods alone.

Keywords: Intrusion Detection System, Local Area Network

[1]อาจารย์ประจำหลักสูตรคอมพิวเตอร์ธุรกิจ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยนอร์ทกรุงเทพ E-mail: jirawin.de@northbkk.ac.th

[2]อาจารย์ประจำหลักสูตรเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยนอร์ทกรุงเทพ

E-mail: theerapath.pr@northbkk.ac.th

คำนำ

เทคโนโลยีการสื่อสารในปัจจุบันมีการใช้งานผ่านเครือข่ายอินเทอร์เน็ตมากขึ้น จะเห็นได้จากจำนวนผู้ใช้โทรศัพท์สมาร์ทโฟน ที่ทำการเชื่อมต่ออินเทอร์เน็ตมากขึ้นทุกวัน แต่สิ่งสำคัญก็คือ การใช้งานอินเทอร์เน็ตจะต้องใช้งานอย่างไรให้มีความปลอดภัยในเรื่องของข้อมูลส่วนตัว การส่งข้อมูลบนระบบเครือข่ายโดยปกติผู้ใช้ไม่ได้มีการเฝ้าระวังดูแลหากไม่เกิดปัญหาขึ้นก่อนก็จะไม่มีการระมัดระวัง การรักษาความปลอดภัยให้กับระบบเครือข่ายที่ดีนั้น จะช่วยป้องกันการบุกรุกที่อาจเกิดขึ้นภายนอกและภายในระบบเครือข่าย จากกลุ่มคนที่ไม่หวังดีที่ไม่ประสงค์ดีที่เจาะข้อมูลหรือขโมยข้อมูล หรือแม้แต่จะทำลายข้อมูล ทำให้องค์กรหรือหน่วยงานต่าง ๆ ต้องให้ความสำคัญในเรื่องนี้ การบุกรุกเข้ามาในเครือข่ายอาจมีหลายรูปแบบทั้งที่เป็น virus worm และการบุกรุกโจมตีในรูปแบบอื่น ๆ ซึ่งการบุกรุกหรือทำลายข้อมูลบางรูปแบบที่ยังไม่เคยเจอจะไม่สามารถรักษาความปลอดภัยและตรวจสอบได้ครบถ้วน จึงเป็นเหตุผลที่สำคัญที่จะต้องมีมาตรการรักษาความปลอดภัย โดยการใช้ระบบการตรวจจับการบุกรุกมาช่วยเพิ่มประสิทธิภาพในการดูแลรักษาความปลอดภัยในเครือข่าย

ในการป้องกันโดยใช้ไฟร์วอลล์ (Firewall) จะช่วยป้องกันอันตรายต่าง ๆ จากผู้ใช้งานภายนอกเครือข่ายที่เข้ามาใช้งานทรัพยากรระบบภายในเครือข่าย แต่การป้องกันโดยใช้ไฟร์วอลล์ ไม่ถึงกับป้องกันได้สมบูรณ์ แต่ช่วยลดความเสียหายให้แก่องค์กรเพียงบางส่วน จึงจำเป็นอย่างยิ่งที่จะต้องหาวิธีการป้องกันและรักษาความปลอดภัยภายในองค์กร ซึ่งระบบตรวจสอบการบุกรุก (Intrusion Detection System) เป็นเทคโนโลยีในการรักษาความปลอดภัยที่ได้รับความสนใจ ที่ได้ทำการศึกษาค้นคว้าและทำการวิจัย เนื่องจากระบบสามารถติดตามตรวจสอบพฤติกรรมของเหตุการณ์ที่มีความผิดปกติจากผู้ไม่หวังดีทำการโจมตีระบบเครือข่ายและข้อมูล

งานวิจัยนี้จึงให้ความสำคัญในเรื่องของการวัดประสิทธิภาพของตัวต้นแบบระบบตรวจจับการบุกรุกโดยใช้วิธีการลดคุณลักษณะที่เหมาะสม เพิ่มประสิทธิภาพในการตรวจจับการบุกรุกโดยการสร้างตัวจำแนกที่อาศัยวิธีการลดคุณลักษณะที่เหมาะสมร่วมกันจำแนกข้อมูล โดยจะนำข้อดีของแต่ละวิธีการมาทำการโหวตหาคุณลักษณะที่เหมาะสม และเลือกใช้วิธีการจำแนกข้อมูลที่เหมาะสมเพื่อนำไปสร้างโมเดลสำหรับการตรวจจับการบุกรุกที่มีประสิทธิภาพ และทำการวัดประสิทธิภาพของระบบตรวจจับการบุกรุก ด้วยค่าความถูกต้อง (Accuracy) และ ค่า F-measure

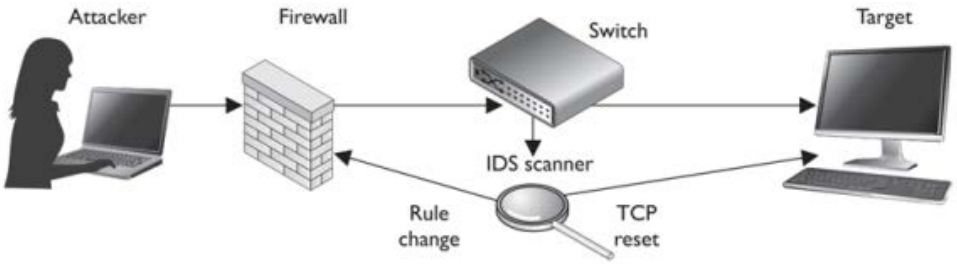
วัตถุประสงค์

1. เพื่อทำการลดคุณลักษณะ (Attribute) เพื่อใช้ในการจำแนกการบุกรุกที่เหมาะสมโดยใช้ชุดข้อมูล NSL-KDD

2. เพื่อหาประสิทธิภาพของของตัวต้นแบบระบบตรวจจับการบุกรุก ด้วยค่าความแม่นยำ และค่าความถูกต้อง

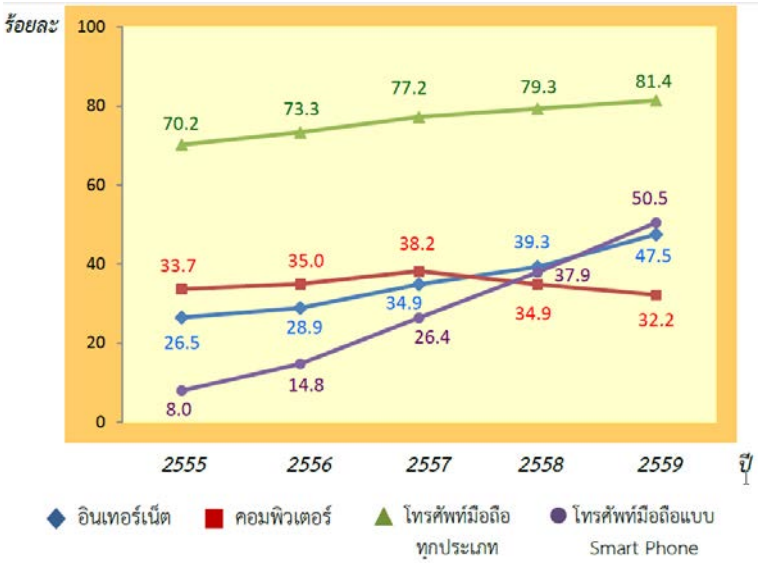
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ระบบตรวจสอบการบุกรุก (Intrusion Detection System) คือระบบที่ใช้สำหรับการเฝ้าระวังหรือตรวจสอบเหตุการณ์ต่าง ๆ ที่เกิดขึ้นในระบบคอมพิวเตอร์หรือมีการบุกรุกในระบบเครือข่ายแล้วนำมาทำการวิเคราะห์เพื่อหาร่องรอยของการบุกรุก ซึ่งหมายถึงการพยายามที่จะทำลายความลับ (Confidentially) ความคงสภาพ (integrity) และความพร้อมใช้งาน (availability) ของข้อมูลหรือการหลีกเลี่ยงระบบรักษาความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่าย การบุกรุกเกิดจากการที่ผู้บุกรุกเข้าถึงระบบจากอินเทอร์เน็ต หรือการที่ผู้ใช้ภายในที่พยายามจะทำในสิ่งที่ไม่ควรจะทำหรือไม่ได้รับอนุญาตหรือไม่มีสิทธิ์หรือการที่ผู้ใช้พยายามที่จะใช้สิทธิพิเศษของตนเอง ในทางที่ผิดระบบตรวจจับการบุกรุก (IDS) จะทำหน้าที่ในการตรวจจับสิ่งผิดปกติเหล่านี้ แล้วรายงานให้ทราบพร้อมทั้งหยุดการบุกรุกได้ทันท่วงที

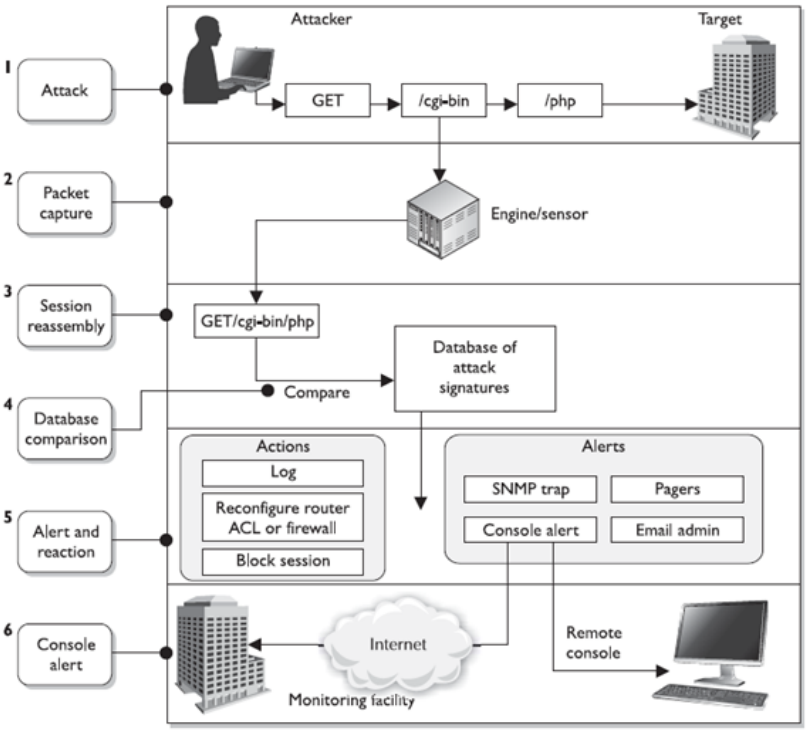


ภาพที่ 1 แสดงสถาปัตยกรรมระบบตรวจสอบการบุกรุก (IDS)

จากข้อมูลสำนักสถิติเศรษฐกิจและสังคม สำนักงานสถิติแห่งชาติในปี พ.ศ. 2559 จะเห็นได้ว่าปริมาณผู้ใช้งานโทรศัพท์เพิ่มขึ้นมากกว่าร้อยละ 80 โดยคาดคะเนว่าปริมาณการใช้งานโทรศัพท์มือถือจะเพิ่มขึ้นมากว่าร้อยละ 90 ในเวลาไม่เกิน 10 ปี ดังนั้นจะเห็นได้ว่า ผู้ใช้งานโทรศัพท์มือถือจะมีความเสี่ยงในการที่จะมีผู้บุกรุกหรือผู้ไม่หวังดี มากขึ้นด้วย จากข้อมูลดังกล่าวจะเห็นได้ว่าการใช้งานอินเทอร์เน็ตผ่านโทรศัพท์มือถือก็เพิ่มขึ้นมากขึ้นด้วยเช่นกัน



ภาพที่ 2 แสดงปริมาณการใช้งานคอมพิวเตอร์ อินเทอร์เน็ต และโทรศัพท์มือถือ



ภาพที่ 3 แสดงสถาปัตยกรรมระบบตรวจสอบการบุกรุกแบบพื้นฐานของ (NIDS)

ความสำคัญของระบบตรวจจับการบุกรุก เป็นสิ่งสำคัญอย่างยิ่งในการรักษาความปลอดภัยบนเครื่องคอมพิวเตอร์ การใช้งานคอมพิวเตอร์ของผู้ใช้โดยทั่วไป การทำงานและในชีวิตประจำวัน อาจจะไม่สามารถทราบได้ว่าการใช้งานคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์มีความปลอดภัยมากน้อยเพียงใด เนื่องจากความปลอดภัยของคอมพิวเตอร์เป็นสิ่งที่มองเห็นยากและยากต่อการวัด อย่างไรก็ตามหากเปรียบเทียบความปลอดภัยของคอมพิวเตอร์กับการรักษาความปลอดภัยสถานที่หรืออาคารต่าง ๆ จะสามารถจัดการเรื่องของการรักษาความปลอดภัยของสถานที่นั้นได้ง่าย เนื่องจากสามารถที่จะล้อมรั้วรอบขอบชิดได้ง่าย เพราะจะใช้กุญแจล็อกประตูหรือทางเข้าออก ซึ่งสามารถควบคุมดูได้ง่าย สามารถจัดให้มีบุคคลหรืออุปกรณ์ที่คอยตรวจสอบการละเมิดต่ออุปกรณ์และเครื่องกีดขวางเพื่อเพิ่มความปลอดภัยได้ ทั้งนี้เนื่องจากอาจมีผู้ไม่หวังดีพยายามบุกรุกโดยทำลายอุปกรณ์หรือเครื่องกีดขวางดังกล่าว ดังนั้นควรต้องอาศัยระบบที่ใช้ตรวจสอบเมื่อมีการทำลายหรือล่วงล้ำต่ออุปกรณ์หรือเครื่องกีดขวางที่ได้ติดตั้งไว้อีกชั้นหนึ่ง ตัวอย่างอุปกรณ์ที่ใช้ตรวจสอบเช่น ระบบสัญญาณเตือนขโมยที่ใช้ควบคู่กับรั้วที่แข็งแรง

ระบบเครือข่ายคอมพิวเตอร์ก็เช่นเดียวกัน บุคคลทั่วไปที่ทำงานอยู่อาจจะคิดว่าหน่วยงานมีระบบรักษาความปลอดภัยและมีระบบไฟร์วอลล์ (Firewall) ที่ติดตั้งไว้เพื่อความปลอดภัยอยู่แล้ว แต่อย่างไรก็ตาม การติดตั้งไฟร์วอลล์ ให้กับระบบเครือข่ายคอมพิวเตอร์ก็เปรียบเสมือนการสร้างรั้วหรือกำแพงเพื่อตรวจสอบบุคคลที่จะเข้า

มาในสถานที่ที่จะรักษาความปลอดภัยแต่หากมีบุคคลที่ไม่หวังดีสามารถปีนรั้วเข้ามาได้การรักษาความปลอดภัยโดยใช้รั้วก็หมดความหมาย ดั้งนั้นในการเพิ่มความปลอดภัยอีกประการหนึ่งคือการใช้ระบบตรวจจับการบุกรุกซึ่งมีคุณลักษณะที่กล่าวมาในตอนต้น

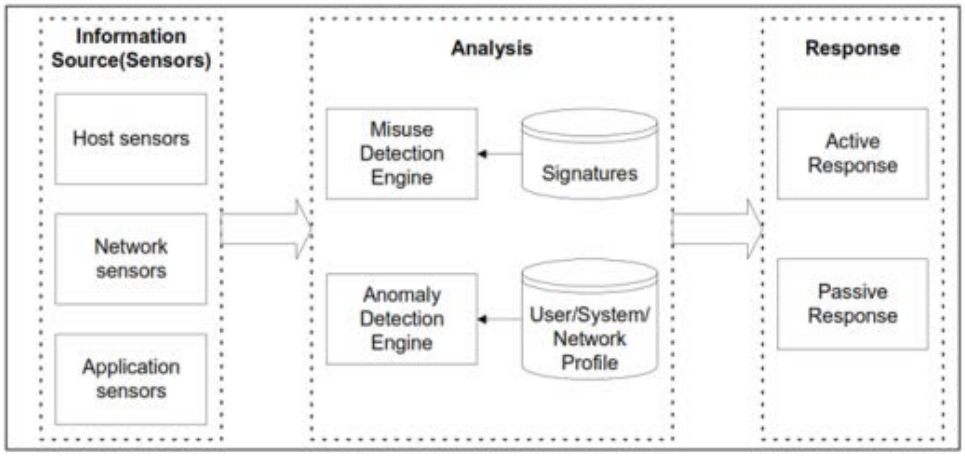
1. องค์ประกอบสำหรับระบบตรวจจับการบุกรุก

ปัจจุบันระบบตรวจจับการบุกรุกจะมีหลากหลายประเภท แต่ละประเภทมีลักษณะการทำงานและแนวทางในการวิเคราะห์เพื่อตรวจจับการบุกรุกที่แตกต่างกัน แต่ระบบตรวจจับการบุกรุกส่วนใหญ่จะมีองค์ประกอบและกระบวนการในการทำงานทั่วไปเหมือนกันคือ ประกอบด้วย 3 องค์ประกอบพื้นฐานดังนี้

1.1 Information Source (Sensor) ข้อมูลเหตุการณ์และข้อมูลการทำงานจากแหล่งข้อมูลต่าง ๆ จะถูกนำมาใช้ในการวิเคราะห์เพื่อตัดสินว่าเมื่อใดที่มีการบุกรุกเกิดขึ้นโดยแหล่งข้อมูลเหล่านี้จะนำมาจากข้อมูลในระดับต่าง ๆ ของระบบ เช่น ข้อมูลในระดับเครือข่าย ระดับเครื่องคอมพิวเตอร์ และโปรแกรมประยุกต์ที่มีการใช้งานอยู่ในระบบ

1.2 Analysis เป็นส่วนที่ทำหน้าที่ในการจัดการและวิเคราะห์ข้อมูลที่ได้รับจากแหล่งข้อมูลต่างๆ แล้วตัดสินว่าเหตุการณ์หรือการกระทำใดที่บ่งชี้ว่ากำลังมีการบุกรุกเกิดขึ้นหรือได้มีการบุกรุกเกิดขึ้นแล้วในระบบ โดยแนวทางที่ใช้ในการวิเคราะห์มีสองรูปแบบ คือ Anomaly Detection และ Misuse Detection

1.3 Response เป็นชุดของการกระทำเมื่อระบบตรวจจับการบุกรุกจับได้ว่ามีการบุกรุกเกิดขึ้น โดยการกระทำเหล่านี้สามารถจัดกลุ่มได้เป็นการกระทำแบบ active และ passive โดยการกระทำแบบ active จะก่อให้มีการกระทำอื่น ๆ ที่จะตอบสนองต่อเหตุการณ์การบุกรุกนั้นโดยอัตโนมัติ เช่น การปรับค่าของเราเตอร์หรือโปรโตคอลในการบุกรุก เป็นต้น ส่วนการกระทำแบบ passive จะเป็นการรายงานหรือแจ้งเตือนการบุกรุกไปยังบุคคลที่รับผิดชอบเพื่อแก้ไขปัญหา โดยอาศัยข้อมูลที่ได้รับรายงาน



ภาพที่ 4 แสดงองค์ประกอบระบบตรวจจับการบุกรุก

วิธีการดำเนินการวิจัย

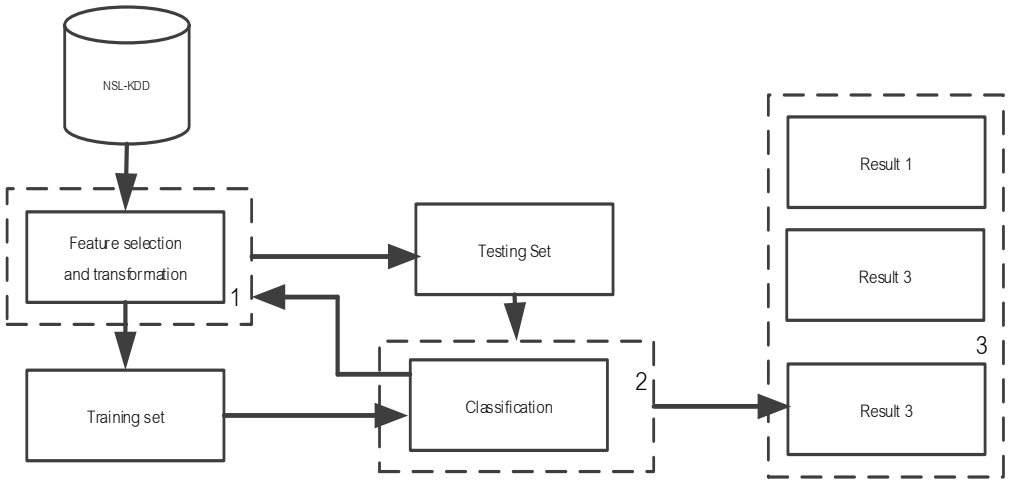
การวิจัยนี้เป็นการนำเสนอวิธีการวัดประสิทธิภาพตัวต้นแบบตรวจสอบการบุกรุกโดยใช้การลดคุณลักษณะ (Feature Selection) จากนั้นจะนำการลดคุณลักษณะมาใช้ในการจำแนกเพื่อเพิ่มประสิทธิภาพในด้านการจำแนกการบุกรุก ได้ถูกต้อง โดยการประเมินประสิทธิภาพ ค่าของความถูกต้อง (Accuracy) ค่าความแม่นยำ (Precision) จากนั้นนำผลลัพธ์ที่ได้มาทดสอบทางด้านสถิติ ดังมีรายละเอียดเนื้อหาประกอบด้วยหัวข้อย่อย ดังนี้

1. การวิเคราะห์และจัดเตรียมข้อมูลเบื้องต้นเป็นขั้นตอนที่จะทำการจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่สามารถนำไปวิเคราะห์ข้อมูลได้ตรงตามชนิดของข้อมูล

2. การลดคุณลักษณะจะทำการลดคุณลักษณะ (Attribute) เพื่อใช้คุณลักษณะที่สำคัญในการนำไปใช้ในการฝึกสอนและทดสอบต่อไป

3. การฝึกสอนและทดสอบ เป็นการนำเอาข้อมูลมาทำการแบ่งออก 2 ส่วนคือ ในการฝึกสอน และหาประสิทธิภาพ คือ 60 และ 40 เปอร์เซ็นต์

4. การวัดประสิทธิภาพ ในการวัดประสิทธิภาพต่อไปนี้จะเป็นการนำเสนอเกี่ยวกับข้อมูลที่นำมาใช้ในการทดลองประสิทธิภาพของโมเดลซึ่งผู้วิจัยได้ใช้ข้อมูลทดสอบ (Datasets) เป็นข้อมูลที่นำมาใช้เพื่อวัดผลอัลกอริทึมที่คิดค้นขึ้นมา หรือดัดแปลงใช้งาน รวมทั้งการฝึกสอน ดังภาพที่ 5 เป็นกรอบแนวคิดในการพัฒนาตัวแบบ



ภาพที่ 5 แสดงกรอบแนวคิดในการพัฒนา

ในการลดคุณลักษณะ (Attribute) โดยใช้เครื่องมือที่เป็นแอพพลิเคชั่นทางด้าน Data Mining มาช่วย ในการลดคุณลักษณะ โดยจะมีข้อมูลที่ใช้ทดสอบทั้งหมด 62,984 เรคคอร์ด ประกอบด้วย 41แอทริบิว 22 คลาส ซึ่ง

เป็น Dataset ของ NSL-KDD โดยเป็นฐานข้อมูลที่ใช้ในวิจัยทางด้านการโจมตีของระบบเครือข่ายที่มีความน่าเชื่อถือ โดยจะมีรูปแบบการโจมตี 4 รูปแบบหลักด้วยกัน ดังตารางที่ 1

ตารางที่ 1 แสดงลักษณะโดยรวมของการบุกรุกแต่ละรูปแบบ

รูปแบบการบุกรุก	**ลักษณะโดยรวมของการบุกรุกแต่ละรูปแบบ**
Denial-of-Service (DOS)	เป็นการโจมตีที่มีการเรียกใช้งานหรือส่งแพ็กเกต (Packet) จำนวนมากไปยังเป้าหมาย ทำให้คิว (Queue) ของการให้บริการของเครื่องเป้าหมายเต็มจึงไม่สามารถให้ บริการได้ตามปกติ รูปแบบการโจมตีที่นิยมใช้กัน ตัวอย่างเช่น SYN flood UDP Flood และ Smurf เป็นต้น
Remote to Local (R2L)	เป็นลักษณะการพยายามเข้าถึงระบบงานของเป้าหมาย ที่ไม่ได้รับอนุญาตในการเข้าถึงเพื่อทำลายระบบงานของเป้าหมาย หรือเจาะระบบข้อมูล โดยรูปแบบการโจมตีที่นิยมใช้กัน เช่น การทายพาสเวิร์ดเป็นต้น
User to Root (U2R)	เป็นลักษณะที่ผู้ใช้พยายามใช้งานสิ่งที่ไม่ได้รับอนุญาตในการเข้าถึงสิทธิ์สำหรับ Local Supper-User (Root) เช่น การโจมตี Buffer Overflow เป็นต้น
Probing	เป็นลักษณะการตรวจสอบและการตรวจเช็คข้อมูลบนเครือข่าย โดยจะทำการ สแกนหาจุดอ่อนหรือช่องโหว่ของเป้าหมาย เพื่อจำและนำมาเป็นข้อมูลในการโจมตี โดยรูปแบบการโจมตีที่นิยมใช้กัน เช่น Port Scanning

ตารางที่ 2 แสดงการกระจายประเภทการโจมตีแบบต่างๆ ในชุดข้อมูลที่ทดสอบ

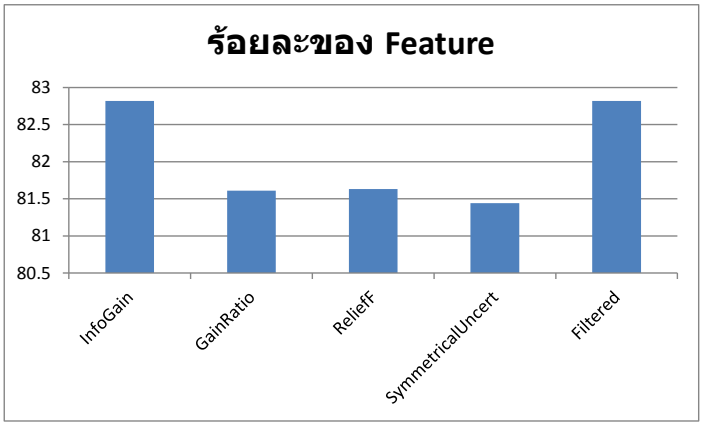
ประเภทการโจมตี	จำนวนเรคคอร์ดในชุดฝึกสอน	จำนวนเรคคอร์ดในชุดทดสอบ
Normal	13,449	9,711
Dos	9,234	5,741
Probe	209	2,199
R2L	2,289	1,106
U2R	11	37
Total	25,192	18,794

2. การลดคุณลักษณะ (Feature Selection)

เนื่องจากจำนวนคุณลักษณะ (Attribute) ที่นำมาใช้ในการจำแนกประเภทการบุกรุกมีจำนวนมาก วิธีการลดคุณลักษณะจึงเป็นสิ่งสำคัญในงานวิจัยนี้ โดยได้ใช้เทคนิควิธีการคัดเลือกคุณลักษณะ feature selection จาก Dataset ของ NSL-KDD โดยสามารถคัดเลือกและแบ่งคุณลักษณะออกได้เป็น จำนวน 41 คุณลักษณะ โดยผู้วิจัยจะทำการเลือกเฉพาะคุณลักษณะที่สำคัญมาใช้งาน โดยมีขั้นตอนและวิธีการคัดเลือกคุณลักษณะที่จะส่งให้ผลสำหรับประสิทธิภาพการตรวจจับการบุกรุกที่ดีมากยิ่งขึ้น โดยเริ่มต้นจากการนำชุดข้อมูล NSL-KDD มาทำการทดสอบ ด้วยการใช้วิธีการลดคุณลักษณะ ซึ่งการลดคุณลักษณะนี้จะมีการหาค่า Gain โดยมีการจัดเรียงอันดับจาก Feature ที่มีค่า Rank สูงสุด เรียงลงมาไปยังค่า Rank ที่มีค่าต่ำสุด ผลที่ได้จะนำค่าของ Feature ที่มีค่าไม่น้อยกว่าร้อยละ 80 ของค่า Rank อาทิเช่น การคำนวณจากการเลือกของ Information Gain อันดับที่ 1-17 แล้วนำค่า Rank มารวมกันจะได้เท่ากับ 13.21 นำมาหารด้วยค่ารวม ผลลัพธ์ที่ได้เท่ากับ 82.82 % ในการวิจัยจะมีการใช้คุณลักษณะ ดังนี้ Gain Ratio, Information Gain, RelieF, Symmetrical Uncertainty และ Filtered และในขั้นตอนต่อไปผู้วิจัยได้ทำการนำข้อมูลที่ได้ จากการลดคุณลักษณะที่ได้ทั้ง 5 วิธี นำไปทำการหาผลโหวตกับวิธีการเลือกคุณลักษณะทั้งที่เหมาะสมต่อ โดยผลของการเลือก feature selection แต่ละวิธีได้ผลลัพธ์ทั้ง 5 คุณลักษณะ มีดังนี้

ผลจากการลดคุณลักษณะของแต่ละวิธีจะให้ผลไม่เหมือนกันเพื่อป้องกันไม่ให้มีการโน้มเอียงไปทางวิธีใดวิธีหนึ่ง จากภาพที่ 6 จะเห็นว่า Feature ที่ได้ทำการเลือกมาจาก 5 วิธีจะให้ผลลัพธ์ของคะแนนที่ได้จากการเลือก Feature มากกว่า 80% ขึ้นไป

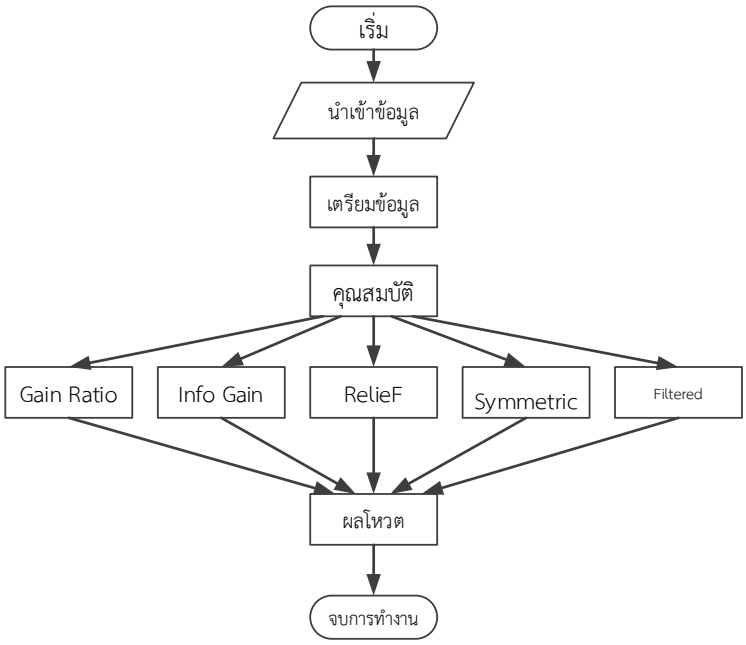
จากภาพที่ 6 แสดงร้อยละของแต่ละ Feature ซึ่งผลที่ได้ของ Info Gain ร้อยละ 82.82 Gain Ratio ร้อยละ 81.61 ReliefF ร้อยละ 81.63 Symmetrical Uncert ร้อยละ 81.84 และ Filtered อยู่ที่ 82.82 ซึ่งเท่ากับ Info Gain สามารถสรุปได้ว่า Feature ที่เลือกสามารถเป็นตัวแทนของ Feature ได้ไม่น้อยกว่าร้อยละ 80



ภาพที่ 6 แสดงค่าผลร้อยละของแต่ Feature

ดังนั้นการที่จะเลือกใช้ Feature หรือ Attribute ใดมาใช้งานนั้น ควรมีการเลือกคุณลักษณะที่เหมาะสมที่จะสามารถใช้เป็นตัวแทนของ Feature ได้ดีและเหมาะสม ดังนั้นเพื่อให้ได้ข้อสรุป Feature ที่จะทำการเลือกนั้นเหมาะสมทางผู้วิจัยได้มีการกำหนดเกณฑ์การให้คะแนนของคุณลักษณะที่ต้องการ โดยใช้วิธีการโหวตให้คะแนน

ของคุณลักษณะ โดยการคิดคะแนน โดยจะทำการเลือกคุณลักษณะที่มีคะแนนรวมในการโหวตมากกว่า 3 คะแนนขึ้นไป ดังภาพที่ 7 และ ภาพที่ 8

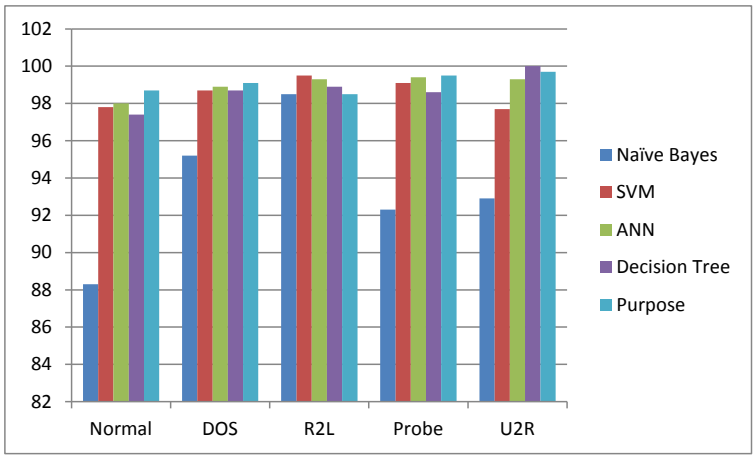


ภาพที่ 7 แสดงขั้นตอนการโหวตเลือก Feature

ในการเลือกคุณลักษณะที่เหมาะสมจะใช้วิธีการโหวตเพื่อหาคุณลักษณะที่จะสามารถนำไปใช้ในการตรวจจับการบุกรุก ได้และมีความถูกต้องไม่น้อยกว่าร้อยละ 80 ขึ้นไป

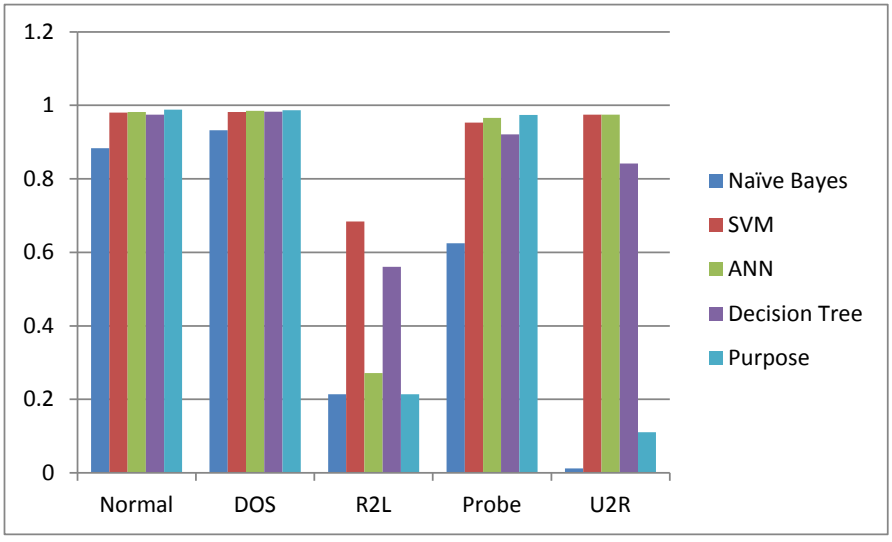
ภาพที่ 8 แสดงการโหวตเลือก Feature ที่จะนำมาใช้

จากผลการทดสอบประสิทธิภาพหลังจากที่หาคุณลักษณะที่เหมาะสม มาเรียบร้อยแล้วก็จะนำมาหาค่าความถูกต้อง (Accuracy) ซึ่งผลที่ได้การหาประสิทธิภาพ โดยทำการเปรียบเทียบกับเทคนิควิธีการแบบอื่น ๆ เพื่อหาการบุกรุกทั้ง 4 รูปแบบ ผลลัพธ์ที่ได้จะเห็นว่าหลังจากการเลือกคุณลักษณะที่เหมาะสม จะสามารถตรวจจับการบุกหรือการโจมตีแบบ DOS และ Probe ได้สูงกว่าวิธีการโจมตีแบบ R2L และ U2R จึงทำให้การเลือกคุณลักษณะที่เหมาะสมส่งผลต่อการตรวจจับการบุกรุกได้ ดังแสงในภาพที่ 9



ภาพที่ 9 สรุปผลค่า Accuracy แต่ละประเภทการโจมตี

หลังจากที่ได้ค่า ความถูกต้อง (Accuracy) มาแล้ว ต่อมาทำการหาประสิทธิภาพของค่า F-Measure ซึ่งผลลัพธ์ที่ได้ มีการแสดงในภาพที่ 10 โดยเป็นการแสดงผลสรุปค่าของ F-Measure ซึ่งจะเห็นได้ว่าการเลือกคุณลักษณะที่เหมาะสมจะสามารถจะระบุการโจมตี แบบ DOS และ Probe และมีค่า F-Measure สูงกว่าวิธีการอื่น ๆ ส่งผลให้ประสิทธิภาพของตัวต้นแบบที่ได้ศึกษาสามารถตรวจจับการบุกรุกแบบ DOS และ Probe ได้ดีกว่า โดยผลที่ได้จากการศึกษานี้สามารถนำไปใช้เป็นต้นแบบในการพัฒนาการใช้งานจริงต่อไปได้



ภาพที่ 10 สรุปผลค่า F-Measure แต่ละประเภทการโจมตี

สรุปผลการวิจัย

จากงานวิจัยเป็นการศึกษาหากคุณลักษณะที่เหมาะสม (Feature Selection) เพื่อนำมาใช้สำหรับการเลือกคุณลักษณะ (Attribute) ที่เหมาะสมที่จะนำมาใช้ในการตรวจสอบการบุกรุกแบบต่าง ๆ โดยการบุกรกแบ่ง

ออกได้เป็น 4 รูปประเภทคือ DOS, R2L, Probe และ U2R การเลือกคุณลักษณะที่เหมาะสมจะส่งผลให้ประสิทธิภาพการตรวจจับการบุกรุกมีประสิทธิภาพที่สูงขึ้นกว่าวิธีการอื่น ๆ ดังนั้น การใช้งานคุณลักษณะใดลักษณะหนึ่ง หรือวิธีการเดียว จะทำให้ผลการคัดเลือกคุณลักษณะ ไม่ถูกต้อง ในงานวิจัยนี้จึงได้มีการเลือกคุณลักษณะที่เหมาะสมที่จะนำมาใช้ในการตรวจสอบการบุกรุกประเภทต่าง ๆ ได้อย่างถูกต้อง จึงได้อาศัยวิธีการโหวตเพื่อหาคุณลักษณะที่เหมาะสมเพื่อนำมาใช้งานในการตรวจสอบการบุกรุก

ข้อเสนอแนะ

ในการการทดสอบประสิทธิภาพนี้ เป็นการใช้ข้อมูลที่เป็น Data Set ในการทดสอบ จึงไม่ได้ข้อสรุปได้อย่างชัดเจนแน่ชัด ที่อาจจะนำไปใช้ทดสอบกับการโจมตีที่เกิดขึ้นบนเครือข่ายในปัจจุบัน เนื่องจากการทดสอบเป็นการทดสอบประสิทธิภาพในเรื่องของความถูกต้องเพียงทางเดียวจึงไม่สามารถได้ข้อสรุปได้ชัดเจนว่ามีประสิทธิภาพที่แท้จริงครบถ้วนทุกด้าน ดังนั้นเพื่อให้งานวิจัยนี้สมบูรณ์ขึ้นจะต้องมีการทดสอบในเรื่องประสิทธิภาพของความเร็ว และการตรวจสอบการบุกรุกรูปแบบใหม่ ๆ ที่อาจเกิดขึ้นต่อไปในอนาคต

กิตติกรรมประกาศ

งานวิจัยฉบับนี้สำเร็จลุล่วงลงได้ ด้วยความร่วมมือจากบุคลากรที่เกี่ยวข้องกับงานวิจัยของมหาวิทยาลัยนอร์ทกรุงเทพที่ได้รับความร่วมมือในการเก็บข้อมูลเป็นอย่างดียิ่ง รวมถึงผู้เชี่ยวชาญในการตรวจสอบคุณภาพของเครื่องมือซึ่งผู้วิจัยต้องขอขอบคุณมา ณ โอกาสนี้ และท้ายสุดนี้ต้องขอขอบคุณมหาวิทยาลัยนอร์ทกรุงเทพที่ได้ให้ทุนสนับสนุนในการทำวิจัยครั้งนี้

เอกสารอ้างอิง

ธีรสุต ไพรินทราภา. (2555). *ระบบการจัดการกฎของระบบตรวจจับการบุกรุก.*สารนิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิศวกรรมเครือข่าย คณะวิทยาการและเทคโนโลยีสารสนเทศ, มหาวิทยาลัยเทคโนโลยีมหานคร.

พลอยพรรณ สอนสุวิทย์. (2552).*การพัฒนาขั้นตอนวิธีสำหรับการตรวจจับสิ่งผิดปกติบนการจราจรระบบเครือข่าย.* วิทยานิพนธ์วิศวกรรมศาสตรมหาบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์, มหาวิทยาลัยเชียงใหม่.

มารุต คำภักดี.(2555).*การสำรวจระบบตรวจจับการบุกรุกที่อยู่บนพื้นฐานของ Snort.* สาขาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์, มหาวิทยาลัยขอนแก่น.

ศุภโชค สุขเกษม. (2548). *การวิเคราะห์ข้อมูลกิจกรรมของระบบเพื่อตรวจจับการบุกรุก.* วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์.

สำนักสถิติเศรษฐกิจและสังคม สำนักงานสถิติแห่งชาติ. (2559). *สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ.* 2559. กรุงเทพมหานคร: ค้นเมื่อ 25 มีนาคม 2560 จาก http://www.nso.go.th

Abdulla Amin Aburomman and Mamun Bin Ibne Reaz.(2016). *Survey of learning methods in intrusion Detection system.* International Conference on Advances in Electrical, Electronic and System Engineering. Putrajaya, Malaysia.

Bisyron Wahayudi Masduki and Kalamullah Ramli.(2016). *Improving Intrusion Detection System Detection Accuracy and Reducing Learning Time by Combining Selected Features Selection and Parameters Optimization.* IEEE International Conference on Control System, Computing and Engineering. Penang, Malaysia.

Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Hiren Patel, Avi Patel, and Muttukrishnan Rajarajan. (2012). *A survey of intrusion detection techniques in Cloud.* Journal of Network and Computer Applications.

Hung-Jen Liao a, Chun-Hung Richard Lin a,n, Ying-Chih Lin a,b, and Kuang-Yuan Tung. (2012). *Intrusion detection system: A comprehensive review.* Journal of Network and Computer Applications.

Mohamed Anbar, Rosmi Abdullah, Iznan H. Hasbullah, Yung-Wey Chong and Omar E.Elejla. (2016). *Comparative performance analysis of classification algorithms for intrusion detection system.* IEEE Privacy, Security and Trust (PST), 2016 14th Annual Conference on Privacy, Security and Trust (PST).

S. Harris. (2008). *CISSP All-in-One Exam Guide.*Fourth Edition. The McGraw-Hill Companies.