บทที่ 5

สรุปผลการวิจัย อภิปรายผล และข้อเสนอแนะ

การศึกษาและวิจัยเรื่อง “ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ” เป็นการวิจัยที่ใช้รูปแบบการวิจัยผสมผสานระหว่างการวิจัยด้วยเทคนิคเหมืองข้อมูล และโครงสร้างกราฟ เพื่อศึกษาและวิเคราะห์ถึง (1) ความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์ (2) รูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (3) พัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟสำหรับรองรับการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริง และ (4) พัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

ทั้งนี้ผู้วิจัยได้นำผลการวิจัยที่ได้มาประยุกต์ใช้ในการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ

สรุปผลการวิจัย

จากวัตถุประสงค์ของการวิจัยเรื่อง “ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ” ซึ่งประกอบด้วยวัตถุประสงค์ 4 ข้อดังนี้

1. เพื่อทำการวิเคราะห์หาความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์

2. เพื่อศึกษารูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

3. เพื่อพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟสำหรับรองรับการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริง

4. เพื่อพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

ผลจากการวิจัยค้นพบ มีดังนี้

1. สามารถพบความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) โดยสามารถนำเสนอความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์

โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบความผิดปกติและโอกาสการถูกโจมตีสูงสุดด้วยการทำให้ระบบสื่อสารขัดข้องสูงถึง 16.10% รองลงมาเป็นความผิดปกติของ HTTP 12.85% และ การถูกเปิดเผยข้อมูลโดยผู้บุกรุกที่ใช้เส้นทางในการเข้าถึงข้อมูลข่าวสารผ่านทางระบบที่ตกเป็นเหยื่อ 12.30%

2. สามารถค้นหาลักษณะการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) โดยสามารถนำเสนอความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ และแสดงภาพการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm

โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือ หากโหนดหมายเลข 129, 87, 3, 90 และ 224 ซึ่งเป็นโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ หรือโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร คือโหนดหมายเลข 234, 90, 217, 229 และ 216 กระจายข้อมูลข่าวสารหรือกระจายความผิดปกติและการถูกโจมตีใน

เครือข่ายสังคมออนไลน์ จะมีโอกาสมาจากโหนดที่ใกล้ชิด คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้โหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์

3. สามารถค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังการวิเคราะห์หาวิธีการสืบค้นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Degree Centrality, Betweenness Centrality, Closeness Centrality โดยสามารถแสดงภาพผู้มีอิทธิพล (Influencing Node) หรือผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ และพัฒนาตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm

โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ด้วยโหนดศูนย์กลางการรับข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือโหนดหมายเลข 129, 87, 3, 90 และ 224 ส่วนโหนดศูนย์กลางการกระจายข้อมูลข่าวสาร หรือกระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือโหนดหมายเลข 234, 90, 217, 229 และ 216

4. สามารถทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังการวิเคราะห์หาวิธีการหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ในหลักการของ Data Mining (Supervised Learning, Classification Analysis, oneR Algorithm) โดยสามารถแสดงภาพเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ และพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ในหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm

โดยตัวอย่างชุดข้อมูลประเทศไทยเดือนเมษายน 2556 พบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าด้วยโหนดศูนย์กลางการกระจายข้อมูลข่าวสารหรือกระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ คือโหนดหมายเลข 234, 90, 217, 229 และ 216 มีโอกาสส่งไปยังโหนดที่ใกล้ชิด คือโหนดหมายเลข 119, 217, 216, 171 และ 234 ทำให้โหนดใกล้ชิดดังกล่าวเป็นโหนดที่ได้รับผลกระทบของการรับหรือกระจายข้อมูลข่าวสารหรือพบความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ หรือเป็นโหนดเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า

5. สามารถสรุปรวมแนวคิดทั้งหมดตามกรอบการวิจัยเป็น ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ที่มีความละเอียดถูกต้อง (Accuracy) อย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

อภิปรายผล

1. ผู้วิจัยได้ใช้หลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) ทำการวิเคราะห์ถึงความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 ของประเทศไทยและประเทศที่ร่วมทดสอบเพื่อเชื่อมโยงไปยังความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ พร้อมนำเสนอภาพความผิดปกติและโอกาสการถูกโจมตีเฉลี่ยเมื่อใช้เครือข่ายสังคมออนไลน์

ความผิดปกติและโอกาสการถูกโจมตีเฉลี่ย เมื่อใช้เครือข่ายสังคมออนไลน์จากชุดข้อมูลของประเทศไทยสูงสุด 5 อันดับแรกได้ดังนี้

(1) Unauthorized access to the server ด้วยอัตรา 16.07%

(2) Unexpected network communication ด้วยอัตรา 14.36%

(3) Information disclosure: attackers gain full path information of the document root on the victim system ด้วยอัตรา 11.25%

(4) Anomaly with HTTP ด้วยอัตรา 10.16%

(5) Denial of service: memory corruption ด้วยอัตรา 8.77%

ความผิดปกติและโอกาสการถูกโจมตีเฉลี่ย เมื่อใช้เครือข่ายสังคมออนไลน์จากชุดข้อมูลของประเทศที่ร่วมทดสอบสูงสุด 5 อันดับแรกได้ดังนี้

(1) Anomaly with HTTP ด้วยอัตรา 16.43%

(2) Unauthorized access to the server. ด้วยอัตรา 14.50%

(3) Stack overflow in the http header ด้วยอัตรา 14.29%

(4) Unexpected network communication ด้วยอัตรา 10.00%

(5) Denial of service: memory corruption. ด้วยอัตรา 9.77%

2. ผู้วิจัยได้ใช้หลักการของ Data Mining (Unsupervised Learning, Cluster Analysis, Distance Measure, K-means Algorithm) เพื่อค้นหาลักษณะการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ พร้อมนำเสนอความผิดปกติและโอกาสการถูกโจมตีเมื่อใช้เครือข่ายสังคมออนไลน์ และแสดงภาพการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm

3. ผู้วิจัยได้ใช้หลักการของ Social Network Analysis (SNA) ด้วยหลักการ Degree Centrality, Betweenness Centrality, Closeness Centrality เพื่อค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555 เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังการวิเคราะห์หาวิธีการสืบค้นผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ และแสดงภาพผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์หรือผู้มีอิทธิพล (Influencing Node) และพัฒนาตัวแบบการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงเมื่อใช้เครือข่ายสังคมออนไลน์ด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm

4. ผู้วิจัยได้ใช้หลักการของ Data Mining (Supervised Learning, Classification Analysis, oneR Algorithm) เพื่อทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ในฐานข้อมูล 4 ชุดในเดือนธันวาคม 2554 เดือนเมษายน 2555

เดือนธันวาคม 2555 และเดือนเมษายน 2556 เพื่อเชื่อมโยงไปยังการวิเคราะห์หาวิธีการหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ และแสดงภาพเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ และพัฒนาตัวแบบการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ด้วยหลักการของ Social Network Analysis (SNA) ด้วย Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm

5. ตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟ มีความถูกต้อง (Accuracy) อย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 %

ปัญหาและอุปสรรคในการทำวิจัย

1. เนื่องจากงานวิจัยชิ้นนี้ใช้หลักการเทคนิคเหมืองข้อมูลและโครงสร้างกราฟ ดังนั้นความรู้ในการวิจัยจะต้องครอบคลุมทั้งเทคนิคเหมืองข้อมูลซึ่งมีหลักการอยู่หลายแนวคิด จึงต้องวางแผนการทดลองเพื่อคัดเลือกเทคนิคเหมืองข้อมูลที่เหมาะสมกับวัตถุประสงค์การวิจัยที่มีความถูกต้อง (Accuracy) อย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % อีกทั้งการผนวกนำความรู้ด้านโครงสร้างกราฟมาทำให้เห็นภาพของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์ในประเด็นตามวัตถุประสงค์ได้อย่างชัดเจน จึงเป็นงานวิจัยที่บูรณาการความรู้ทางด้านสถิติและวิทยาการคอมพิวเตอร์ทำให้เกิด Research Contribute ที่น่าสนใจ ซึ่งต้องทำการค้นคว้างานวิจัยที่เกี่ยวข้องและความรู้หลากหลายสาขา

2. เนื่องจากเป็นงานวิจัยที่บูรณาการความรู้ทางด้านสถิติและวิทยาการคอมพิวเตอร์นอกเหนือจากที่ต้องอาศัยความชำนาญในการพัฒนาโปรแกรมการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟแล้ว ผู้พัฒนาโปรแกรมการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟจะต้องมีความรู้อย่างลึกซึ้งทางด้านสถิติและวิทยาการคอมพิวเตอร์เพื่อสร้างอัลกอริทึมที่ถูกต้องตามหลักวิชาการ ผู้วิจัยจึงได้เสนอแนวคิดในการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟในลักษณะ Prototype

ข้อเสนอแนะ

1. ข้อเสนอแนะสำหรับการนำผลการวิจัยไปใช้งาน

1.1 เทคนิคของการวิจัยเป็นการผนวกเทคนิคด้านการรวมกลุ่ม (Cluster Algorithm) เทคนิคทางทฤษฎีกราฟ (Graph-based Structure) และการพยากรณ์และการจำแนก ณ เวลาอนาคต (Classification for Prediction) เพื่อรองรับวัตถุประสงค์ของการวิจัยที่กำหนดเท่านั้นที่มีความถูกต้อง (Accuracy) อย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % ในกรณีที่มีการกำหนดเพิ่มหรือปรับวัตถุประสงค์ หรือกำหนดระดับความเชื่อมั่นที่สูงขึ้น ควรทบทวนกรอบการวิจัยเนื่องจากกลุ่มเทคนิคที่ใช้อาจไม่เหมาะสม

1.2 ผลการวิจัยที่ได้มาจากการนำเทคนิคของการวิจัยเป็นการผนวกเทคนิคด้านการรวมกลุ่ม (Cluster Algorithm, Distance Measure, K-means Algorithm) เทคนิคทางทฤษฎีกราฟ (Graph-based Structure ด้วย Degree Centrality, Betweenness Centrality, Closeness Centrality, Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm) และการพยากรณ์และการจำแนก ณ เวลาอนาคต (Classification for Prediction ด้วย oneR Algorithm) เท่านั้น

1.3 สำหรับองค์กรที่มีการใช้ Online Social Networks ในการประชาสัมพันธ์กิจกรรมขององค์กร ควบคู่ไปกับการใช้งานระบบสารสนเทศหลักขององค์กรด้วยนั้น นับว่าองค์กรมีความเสี่ยงต่อข้อมูลและระบบสารสนเทศขององค์กรเป็นอย่างยิ่ง และเนื่องจากงานวิจัยชิ้นนี้มีจุดเด่นใน (1) การวิเคราะห์หาความผิดปกติและโอกาสการถูกโจมตีจากการใช้เครือข่ายสังคมออนไลน์ (2) การแสดงภาพรูปแบบการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ (3) การสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงในเครือข่ายสังคมออนไลน์ (4) การทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้า ซึ่งเป็นคุณลักษณะที่สามารถตอบสนองการใช้งานของทุกองค์กร จึงสามารถประยุกต์งานวิจัยนี้เพื่อใช้งานในองค์กรได้หลายประเภทธุรกิจ ส่งผลให้องค์กรได้รับความเชื่อถือไว้วางใจจากหน่วยงานอื่นๆ ด้านความมั่นคงปลอดภัย

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

2.1 ในการสร้างผลการวิเคราะห์เพื่อรองรับวัตถุประสงค์ของการวิจัยนั้น เป็นลักษณะงานแบบ Loop คือลักษณะวนซ้ำเพื่อนำข้อมูลใหม่ที่เกิดขึ้นเข้าประมวลผลเพื่อแสดงผลของการวิจัยล่าสุดที่มีความถูกต้อง (Accuracy) อย่างมีนัยสำคัญภายใต้ระดับความเชื่อมั่น 95 % ซึ่งในการ

ประมวลผลทุกครั้งจะได้ความรู้เกิดขึ้นเสมอ ดังนั้นการประมวลผลงานวิจัยชิ้นนี้สามารถขยายผลในรูปแบบของการจัดการองค์ความรู้ด้านการรักษาความมั่นคงปลอดภัย (Security Knowledge Management) ต่อได้

2.2 งานวิจัยชิ้นนี้รองรับวัตถุประสงค์งานวิจัยจากคำนิยามของความผิดปกติและการจู่โจมในเครือข่ายสังคมออนไลน์ (Anomaly and Attack Patterns in Online Social Networks) คือการที่ผู้ใช้ได้รับสิ่งต่างๆที่เกิดจากการใช้งานเครือข่ายสังคมออนไลน์ที่ Firewall สามารถดักจับและแปลผลออกมาว่าเป็นความผิดปกติ ได้แก่ ภัยมัลแวร์ และ เทคนิควิศวกรรมสังคม (Malware with Social Engineering Technique Attack) ภัยสแปมเมล์ (Spam Mail Attack) ภัยจากการใช้โปรแกรมประเภท IM และ P2P โดยไม่ระวังอย่างเพียงพอ (IM and P2P Attack) ภัยกับดักหลอกลวงผ่านทางอิเล็คโทรนิกส์เมล์ และ การโจมตีผู้เล่นเกมส์ออนไลน์ (Phishing, Pharming และ Gold Farming Attack) ภัยการโจมตีระบบด้วยวิธี DoS หรือ DDoS (Denial of Services and Distributed Denial of Services Attack) ภัยการโจมตี Web Server และ Web Application (Web Server and Web Application Attack) และภัยเครือข่ายหุ่นยนต์ (Botnets Attack) โดยผู้วิจัยท่านอื่นสามารถขยายผลในการนำ Content ความผิดปกติและการจู่โจมในเครือข่ายสังคมออนไลน์ดังกล่าวเพื่อเรียนรู้รูปแบบของความผิดปกติและการจู่โจมในเครือข่ายสังคมออนไลน์ที่แท้จริงต่อไป (Information Retrieval)

2.3 เนื่องจากเทคนิคของการวิจัยเป็นการผนวกเทคนิคด้านการรวมกลุ่ม (Cluster Algorithm, Distance Measure, K-means Algorithm) เทคนิคทางทฤษฎีกราฟ (Graph-based Structure ด้วย Degree Centrality, Betweenness Centrality, Closeness Centrality, Minimum Spanning Tree ของ Prim's Algorithm และ All-Pair Shortest Path ของ Floyd-Warshall Algorithm) และการพยากรณ์และการจำแนก ณ เวลาอนาคต (Classification for Prediction ด้วย oneR Algorithm) ดังนั้นถ้าผู้วิจัยท่านอื่นเปลี่ยนอัลกอริทึมใด เช่น จาก Minimum Spanning Tree ของ Prim's Algorithm เป็น Kruskal's Algorithm จะส่งผลให้การแสดงภาพของการแพร่กระจายความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์ ภาพของการสืบค้นหาผู้กระทำผิดปกติและมีพฤติกรรมการโจมตีที่แท้จริงจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์ และภาพของการทำนายหาเป้าหมายในเครือข่ายสังคมออนไลน์ที่อาจจะได้รับผลกระทบจากความผิดปกติและการถูกโจมตีในเครือข่ายสังคมออนไลน์เพื่อทำการแจ้งเตือนล่วงหน้าจากความเชื่อมโยงในเครือข่ายสังคมออนไลน์แตกต่างไป

2.4 เนื่องจากความผิดปกติและการจู่โจมในเครือข่ายสังคมออนไลน์ (Anomaly and Attack Patterns in Online Social Networks) คือการที่ผู้ใช้ได้รับสิ่งต่างๆที่เกิดจากการใช้งาน

เครือข่ายสังคมออนไลน์ที่ Firewall สามารถดักจับและแปลผลออกมาว่าเป็นความผิดปกติ ได้แก่ ภัยมัลแวร์ และ เทคนิควิศวกรรมสังคม (Malware with Social Engineering Technique Attack) ภัยสแปมเมล์ (Spam Mail Attack) ภัยจากการใช้โปรแกรมประเภท IM และ P2P โดยไม่ระวังอย่างเพียงพอ (IM and P2P Attack) ภัยกับดักหลอกลวงผ่านทางอิเล็คโทรนิกส์เมล์ และ การโจมตีผู้เล่นเกมส์ออนไลน์ (Phishing, Pharming และ Gold Farming Attack) ภัยการโจมตีระบบด้วยวิธี DoS หรือ DDoS (Denial of Services and Distributed Denial of Services Attack) ภัยการโจมตี Web Server และ Web Application (Web Server and Web Application Attack) และภัยเครือข่ายหุ่นยนต์ (Botnets Attack) ซึ่งผู้วิจัยท่านอื่นสามารถพัฒนาการเรียนรู้ความผิดปกติและการจู่โจมในเครือข่ายสังคมออนไลน์ (Anomaly and Attack Patterns in Online Social Networks) อย่างอัตโนมัติด้วยตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟด้วยหลักการ Artificial Intelligent ก็สามารถต่อยอดงานวิจัยชิ้นนี้

2.5 ตามที่กล่าวในปัญหาและอุปสรรคในงานวิจัยเนื่องจากตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟซึ่งมีคุณลักษณะเด่นของงานวิจัยในงานวิจัยด้วยการใช้เทคนิคเหมืองข้อมูล (Data Mining) โครงสร้างกราฟ (Graph-based Structure Technique) การทำให้เห็นภาพ (Visualization) การทดสอบทางสถิติ (Statistic) และการพัฒนาตัวแบบการวิเคราะห์ความมั่นคงปลอดภัยและวิชวลไลเซชันของความมั่นคงปลอดภัยในเครือข่ายสังคมออนไลน์โดยใช้เทคนิคเหมืองข้อมูลและโครงสร้างกราฟให้เห็นเป็นรูปธรรมโดยการพัฒนาโปรแกรมตามหลักการของงานวิจัยชิ้นนี้ ทำให้ผู้วิจัยจะต้องมีความรู้และความสามารถในทักษะเฉพาะหลายด้านตามที่กล่าวข้างต้น