

ระบบการสร้างรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟ

รุ่งรัตน์ กุลมาศ¹, สุริยา จันทะระ² ณรงค์ฤทธิ์ วังศิริ³ และณณกร คววรรณติกุล⁴

^{1,2,3,4} สาขาวิชาระบบสารสนเทศ คณะเทคโนโลยีสังคม มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก วิทยาเขตจันทบุรี

Emails: rungrat170837@gmail.com, suriya035@gmail.com, mui_kmutnb@hotmail.com, aof.kawattikul@gmail.com

บทคัดย่อ

งานวิจัยนี้ช่วยในการสร้างรหัสผ่านเพื่อให้แต่ละบุคคลได้รับรหัสผ่านที่มีความปลอดภัยและมีความแข็งแกร่งเหมาะสมกับการใช้งาน ยากต่อการโจรกรรมรหัสผ่านหรือข้อมูล โดยระบบได้มีการประมวลผลตามเงื่อนไขเพื่อนำมาจัดกลุ่มความเข้มงวดแบบอัตโนมัติ เพื่อนำมาสร้างรหัสผ่านตามเงื่อนไข มีการทดสอบระบบจากผู้ใช้ 100 คน และนำผลที่ได้มานำเสนอในรูปแบบกราฟ โดยใช้โปรแกรม Cytoscape

โดยระบบมีการประเมินระบบจากผู้เชี่ยวชาญทั้ง 5 ท่าน มีการประเมินทั้งหมด 3 ด้าน โดยมีด้านความปลอดภัยของรหัสผ่าน, ด้านประสิทธิภาพของระบบและด้านความเหมาะสมของรหัสผ่าน โดยด้านที่มีการประเมินมากที่สุด คือ ด้านความปลอดภัยของรหัสผ่านมีค่าเฉลี่ยเท่ากับ 4.27 ด้านความเหมาะสมของรหัสผ่านมีค่าเฉลี่ยเท่ากับ 3.93 และด้านประสิทธิภาพของระบบมีค่าเฉลี่ยเท่ากับ 3.60 โดยภาพรวมของระบบนั้นอยู่ในระดับดี มีค่าเฉลี่ยเท่ากับ 3.93

คำสำคัญ— รหัสผ่าน; กราฟเทคนิค; พฤติกรรม

Abstract

This research to created password so that each person got password that was security and there was a strong fit for use. Difficult to steal passwords or data. The system had a processed by created an online questionnaire and are processed accord to the group austerly automated in order to created passwords based on criteria are tested by 100 users, and results obtained. Presented in graph form using Cytoscape

The system had assessment a system from expert 5 persons. Had assessment the security of the password, The performance of system and appropriate password. It had assessment that by most was security of password had an average of 4.27, The system's performance had an average of 3.93 and the appropriate password. had an average of 3.60 The overall system is at a good level with an average of 3.93.

Keywords— Password; Graph Technique; Behavior

1. บทนำ

ปัจจุบันเป็นยุคที่เข้าถึงข้อมูลข่าวสารออนไลน์ได้อย่างรวดเร็ว ซึ่งข้อมูลโดยส่วนใหญ่มีความสำคัญ จึงทำให้เกิดการโจรกรรมข้อมูลเพื่อขโมยรหัสผ่านหรือข้อมูลใด ๆ ซึ่งถือเป็นปัญหาพื้นฐานและเป็นปัญหาสำคัญที่อาจก่อให้เกิดความเสียหายแก่หน่วยงานหรือตัวบุคคล ในการเข้าใช้งานระบบหรือการเข้าถึงข้อมูล ให้เกิดความสะดวกและมีความปลอดภัยนั้นมีหลากหลายวิธี แต่วิธีการที่นิยมที่สุด ได้แก่ การสร้างความปลอดภัยด้วยวิธีการที่ใช้ในการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ต (Authentication) ซึ่งการ Authentication โดยข้อความนั้นไม่จำเป็นที่จะต้องใช้อุปกรณ์ใด ๆ แต่ในปัจจุบันรหัสผ่านยังไม่มีความปลอดภัยเท่าที่ควร รหัสที่ใช้โดยส่วนใหญ่มักจะกำหนดเป็นคำง่าย ๆ หรือตัวเลขที่คาดเดาได้ง่าย เพื่อให้สะดวกในการจำจด จึงทำให้รหัสผ่านไม่ปลอดภัยและเกิดเป็นสาเหตุหนึ่งที่ทำให้ต้องมีการเปลี่ยนแปลงรหัสผ่านบ่อยขึ้นหรือทำให้รหัสผ่านต้องมีหลายระดับ

งานวิจัยพัฒนาระบบการสร้างรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟ ในการจัดทำระบบนั้น มุ่งให้ความ

สนใจในกลุ่มของนักศึกษาเป็นหลัก เพราะจากการศึกษาผลการสำรวจการใช้อินเทอร์เน็ตของคนไทยปี 2559 มีการสำรวจโดย ETDA พบว่า กลุ่ม Gen Y เป็นกลุ่มที่มีการใช้อินเทอร์เน็ตโดยเฉลี่ยสูงที่สุด 53.2 ชั่วโมงต่อสัปดาห์ โดยที่จะมีการใช้งานมากที่สุดในส่วนของสังคมออนไลน์, YouTube, รับส่งอีเมลและการค้นหาข้อมูล [1] อีกทั้งกลุ่มนักศึกษายังเป็นกลุ่มคนที่จัดว่ามีความรู้ทางด้านเทคโนโลยีมากที่สุด แต่ทั้งนี้ความตระหนักเรื่องปัญหาความปลอดภัยของข้อมูลส่วนบุคคล ยังมีความใส่ใจน้อยเกินไป พฤติกรรมส่วนใหญ่ในเรื่องการสร้างรหัสผ่านของแต่ละบุคคลนั้นจะมีความคล้ายคลึงกันในบุคคลที่ไม่มีความรู้ในเรื่องความปลอดภัยของข้อมูล และจะมีการสร้างรหัสผ่านที่แตกต่างกันในผู้ที่มีความรู้ ระบบการสร้างรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟ จึงสร้างมาเพื่อช่วยในการวิเคราะห์ความแข็งแกร่งและจัดกลุ่มความแข็งแกร่งของรหัสผ่านของผู้ใช้งานระบบ ให้ตรงตามมาตรฐาน ISO/IEC 27001 [2] ว่าด้วยเรื่องของจัดการการความมั่นคงปลอดภัยของสารสนเทศเพื่อช่วยให้มีองค์ประกอบในความมั่นคงของข้อมูลสารสนเทศอย่างครบถ้วน

2. ทฤษฎีที่เกี่ยวข้อง

2.1. ทฤษฎีพฤติกรรม

พฤติกรรม (Behavior) เป็นการแสดงออกและกิริยาท่าทางซึ่งสิ่งมีชีวิต ระบบหรือลักษณะประติสัที่เกิตร่วมกันกับสิ่งแวดล้อม ซึ่งรวมระบบอื่นหรือสิ่งมีชีวิตโดยรวม เช่นเดียวกับสิ่งแวดล้อมทางกายภาพ พฤติกรรมเป็นการตอบสนองของระบบหรือสิ่งมีชีวิตต่อสิ่งเร้าหรือการรับเข้าทั้งหลาย ไม่ว่าจะเป็นภายในหรือภายนอก มีสติหรือไม่มีสติระลึก ชัดเจนหรือแอบแฝง และโดยตั้งใจหรือไม่ตั้งใจ [3]

2.2. มาตรฐาน ISO/IEC 27001

มาตรฐาน ISO/IEC 27001:2005 เป็นมาตรฐานการจัดการข้อมูลที่มีความสำคัญเพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่องซึ่งข้อกำหนดต่าง ๆ กำหนดขึ้นโดยองค์กรที่มีชื่อเสียงและมีความน่าเชื่อถือระหว่างประเทศ

มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กร และใช้เป็น

มาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรอย่างแพร่หลาย สำหรับมาตรฐาน ISO/IEC 17799-2005 ว่าด้วยเรื่องของวิธีปฏิบัติที่จะนำไปสู่ระบบบริหาร จัดการความมั่นคงปลอดภัยที่องค์กรได้จัดทำขึ้น ซึ่งจะต้องเป็นไปตามข้อกำหนดในมาตรฐาน ISO/IEC 27001 รายละเอียดของมาตรฐานนี้จะบอกถึงวิธีปฏิบัติในการลดความเสี่ยงที่เกิดจากจุดอ่อนของระบบโดยแบ่งเป็นหัวข้อหลักที่เกี่ยวข้องกับระบบและให้แนวทางว่าผู้จัดทำควรปฏิบัติอย่างไร ซึ่งผู้ใช้งานสามารถเพิ่มเติมมาตรการหรือใช้วิธีการที่มีความมั่นคงปลอดภัยเพียงพอหรือเหมาะสมตามที่ต้องการได้ประเมินไว้ โดยในเรื่องของนโยบายความมั่นคงปลอดภัยขององค์กร (Security policy) และการควบคุมการเข้าถึง (Access Control) [2]

2.3. นโยบายความปลอดภัย

2.3.1. เกณฑ์การตั้งรหัสผ่าน (Password)

2.3.1.1. Password ต้องมีความยาว 8 ตัว อักขรขึ้นไป

2.3.1.2. ห้ามตั้ง Password เป็นตัวอักษร หรือตัวเลขทั้งหมด

2.3.1.3. Password ต้องประกอบด้วยการผสมกันระหว่างตัวอักษรกับตัวเลข โดยมีตัวเลขตั้งแต่ 2 ตัวขึ้นไปหรือตัวอักษรกับอักขระพิเศษ โดยมีอักขระพิเศษตั้งแต่ตัวขึ้นไป หรือตัวอักษรกับตัวเลขและอักขระพิเศษ โดยมีตัวเลขและอักขระพิเศษรวมกันตั้งแต่ 2 ตัวขึ้นไป

2.3.2. รหัสผ่าน (Password) ที่ควรใช้

2.3.2.1. เป็นคำที่ตั้งขึ้นเองโดยไม่ปรากฏในพจนานุกรม

2.3.2.2. ใช้คำที่ยากต่อการคาดเดา แต่จำง่าย

2.3.2.3. ควรเปลี่ยน Password ให้บ่อยที่สุด เช่นอย่างน้อย 3 เดือนต่อครั้ง

2.3.2.4. ต้องเลือกเปลี่ยน Password ให้แตกต่างกันในแต่ละครั้ง ไม่ควรใช้ซ้ำ อย่าใช้รหัสผ่านเดียวกันทุก Account

2.3.3. ข้อควรหลีกเลี่ยงสำหรับการตั้งรหัสผ่าน (Password)

2.3.3.1. อย่าให้เหมือนกับ Username เพราะจะเป็นการง่ายต่อการคาดเดา ไม่ควรสะกดชื่อกลับหลัง

2.3.3.2. อย่าใช้ชื่อของสามี/ภรรยา แฟนและ/หรือลูก หลาน

2.3.3.3. อย่าใช้ชื่อของสัตว์เลี้ยงของท่าน เช่น สุนัข

2.3.3.4. อย่าใช้ชื่อบุคคลที่ท่านนับถือซึ่งรวมไปถึงชื่อทีมกีฬาที่โปรดปราน ชื่อภาพยนตร์ เพลง ฯลฯ

2.3.3.5. อย่าใช้ชื่อเมือง ประเทศ

2.3.3.6. อย่าใช้หมายเลข ประกันสังคม หมายเลขโทรศัพท์ วันเกิด ฯลฯ

2.3.3.7. อย่าใช้คำซึ่งสามารถหาความหมายได้จากพจนานุกรมทั่วไป

2.3.3.8. อย่าใช้ชื่อหรือนามสกุลเป็นภาษาไทย โดยพิมพ์ในโหมดแป้นพิมพ์ภาษาอังกฤษ เช่น ชื่อ พรชัย ใช้ Password เป็น ri=yp เป็นต้น [4]

2.4. ทฤษฎี Complex Network

เครือข่ายซับซ้อน (Complex Network) มีอยู่มากมายทุกหนทุกแห่งทั้งในธรรมชาติและมนุษย์สร้างขึ้น เครือข่ายในโลกแห่งความเป็นจริงนั้นมีความซับซ้อนและมีพลวัตของพฤติกรรมต่าง ๆ ซึ่งอาจทำให้เครือข่ายนั้นเติบโตหรือล่มสลายได้ โดย Complex Network มีลักษณะการเชื่อมต่อเครือข่ายที่ไม่มีรูปแบบที่แน่นอน เนื่องจาก Complex Network มีการเพิ่มจำนวนหรือลดจำนวนของโหนดและเส้นเชื่อมต่อกันอยู่ตลอดเวลา มักเป็นเครือข่ายที่มีขนาดใหญ่ ซับซ้อน ลักษณะการเชื่อมต่อเลียนแบบพฤติกรรมเครือข่ายในธรรมชาติ โครงสร้างของ Complex Network ได้แก่ โหนด (Node) และเส้นเชื่อมโยง (Edge) เชื่อมต่อเข้าด้วยกันก่อให้เกิดเครือข่ายที่มีขนาดใหญ่และซับซ้อน ในการค้นพบในการเชื่อมต้อมี 3 แบบได้แก่ Random Network Model เป็นการเชื่อมต่อกันระหว่างโหนดจากการเพิ่มโหนดที่เป็นสมาชิกของเครือข่ายเพื่อเชื่อมต่อด้วยวิธีการสุ่ม Small-World Network Model เกิดจากกลุ่มเครือข่าย (Cluster) หลายกลุ่มเครือข่ายเชื่อมต่อเข้าด้วยกัน ลักษณะความสัมพันธ์ของการเชื่อมโยงมองถึงโหนดที่เชื่อมอยู่ใกล้กันจะมีความสัมพันธ์กันมากกว่าโหนดที่อยู่ไกลกันและ Scale-Free Network Model รูปแบบการเชื่อมต่อใช้กฎการกระจายตัวแบบ Power Law Degree Distribution [5-6]

2.5. โปรแกรม Cytoscape

Cytoscape เป็นโอเพนซอร์สชีวสารสนเทศซอฟต์แวร์ แพลตฟอร์มสำหรับการแสดงผลเครือข่ายการทำงานร่วมกันในระดับโมเลกุลและการบูรณาการกับการแสดงออกของยีนและข้อมูลอื่นของรัฐคุณสมบัติเพิ่มเติมมีอยู่เป็นปลั๊กอิน ปลั๊กอินที่มีอยู่สำหรับ

เครือข่ายและการวิเคราะห์โมเลกุลรูปแบบใหม่ มีการสนับสนุนรูปแบบไฟล์เพิ่มเติมและการเชื่อมต่อกับฐานข้อมูลและการค้นหาข้อมูลในเครือข่ายขนาดใหญ่

Cytoscape เป็นที่นิยมใช้มากที่สุดสำหรับการใช้งานการวิจัยทางชีววิทยา การใช้งาน Cytoscape สามารถนำมาใช้เพื่อให้มองเห็นและวิเคราะห์กราฟเครือข่ายใด ๆ ที่เกี่ยวข้องกับโหนด [7]

2.6. งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้อง จึงได้มีการแบ่งกลุ่มงานวิจัยตามเกณฑ์ดังนี้

งานวิจัยแบ่งตามการยืนยันตัวตน ซึ่งเป็นรูปแบบในการตรวจสอบการยืนยันตัวตนเพื่อความปลอดภัยตนเอง โดยงานวิจัยที่ได้ทำการศึกษาได้แก่เรื่อง การยืนยันตัวตนด้วยรหัสผ่านแบบครั้งเดียวโดยใช้การแก้ปัญหาของตัวเลขแบบสุ่ม และการคำนวณอย่างง่าย เป็นงานวิจัยที่เสนอแนวคิดในการแก้ปัญหาในการยืนยันตัวตนด้วยรหัสผ่านแบบครั้งเดียว จะมีการสุ่มตัวเลขซึ่งเปลี่ยนแปลงทุกครั้งที่ทำการยืนยันตนร่วมกับตัวการดำเนินงานมาสร้างเป็นสูตร โดยคำตอบบนนี้ก็คือ รหัสผ่านที่เป็นการยืนยันตัวตนในแต่ละครั้ง นอกจากยังมีงานวิจัยในเรื่องการพิสูจน์ตัวตนแบบสองปัจจัยโดยใช้รหัสผ่านและภาพ เป็นงานวิจัยที่สร้างขึ้นเพื่อให้ได้ขั้นตอนวิธีการพิสูจน์ตัวตนด้วยภาพที่มีประสิทธิภาพ โดยได้กำหนดพื้นที่ในการใส่รหัสภาพให้มีพื้นที่ที่จำกัดได้ง่าย เมื่อผู้ใช้ทำการใส่รหัสภาพ แล้วจึงแปลงข้อมูลให้อยู่ในรูปแบบของ Byte of Array เพื่อนำมาแปลงค่าในรูปแบบของข้อความ เพื่อให้มีความปลอดภัยและง่ายต่อการจัดเก็บลงในฐานข้อมูล ใช้คำสั่ง Filestream ในการเรียกข้อมูลภาพที่แปลงค่าให้อยู่ในรูปของ Byte เพื่อทำการเปรียบเทียบรูปภาพต้นฉบับกับฐานข้อมูล [8-9]

งานวิจัยแบ่งตามการสร้างรหัสผ่าน ซึ่งเป็นรูปแบบของระบบช่วยสร้างรหัสผ่าน โดยงานวิจัยที่ได้ทำการศึกษา ได้แก่ เรื่อง การวิจัยการสร้างรหัสผ่าน หลัก โดยใช้แนวคิดและ 10 ทฤษฎีบทในเรื่องสมภาค เป็นงานวิจัยเพื่อแก้ปัญหาในเรื่องของบุคคลภายนอกเข้าไปใช้ระบบของนักศึกษา โดยที่นักศึกษาไม่ทราบและการเกิดความเสี่ยงในการเข้าถึงข้อมูลจึงเกิดการสร้างรหัสผ่าน 10 หลัก โดยใช้แนวคิดและทฤษฎีบทในเรื่องสมภาค มีการสร้างสูตรในรูปของสมการเชิงเส้นและพิสูจน์สูตรดังกล่าวเพื่อแสดงถึงความแตกต่างของรหัสผ่านในนักศึกษาแต่ละคน นอกจากงานวิจัยนี้แล้วยังมีงานวิจัยในเรื่อง การศึกษาปัจจัยที่มี

อิทธิพลต่อการใช้งานได้และความปลอดภัยของรหัสผ่านแบบการคูณ เป็นงานวิจัยที่ทำการทดลองเพื่อประสิทธิภาพในการสร้างรหัสผ่านที่มีความปลอดภัยโดยใช้รูปภาพเป็นตัวช่วยในการสร้างรหัสผ่าน ซึ่งรูปภาพที่นำมาใช้เป็นตัวการคูณจาก Walt Disney ทั้งหมด 100 ตัว ซึ่งตัวการคูณเป็นที่รู้จักและจดจำได้ง่าย โดยมีการเลือกตัวการคูณ 6 ตัว จาก 100 ตัวจัดเรียงกัน โดยแบ่งกลุ่มตัวอย่างเป็น 2 ส่วน การมีตารางกริดและไม่มีตารางกริด โดยภายหลังจากการเลือกรูปภาพ แล้วจะเกิดระบบสุ่มรหัสผ่านและกลุ่มตัวอย่างจะต้องจำรหัสผ่านที่ได้มา [10-11]

3. วิธีดำเนินการศึกษา

3.1. ศึกษาและรวบรวมข้อมูลที่เกี่ยวข้องกับโครงการ

คณะผู้จัดทำได้มีการศึกษาพฤติกรรมในการสร้างรหัสผ่านของผู้ใช้งาน โดยแบ่งกลุ่มผู้ใช้งานออกเป็น 3 กลุ่มเพื่อให้เหมาะสมกับการสร้างรหัสผ่านให้กับผู้ใช้งานตามลักษณะการใช้งานอินเทอร์เน็ต จากนั้นได้ทำการศึกษาทำความเข้าใจเกี่ยวกับทฤษฎีและกระบวนการในการสร้างรหัสผ่านเพื่อให้มีความเหมาะสมและมีความปลอดภัยที่มากขึ้น

3.2. วิเคราะห์สภาพปัญหา

รหัสผ่านโดยส่วนใหญ่ที่ผู้ใช้งานสร้างขึ้นมาเพื่อที่จะใช้ในการยืนยันตัวตนนั้น มักเป็นรหัสผ่านที่เป็นข้อมูลส่วนตัวของผู้ใช้งาน เช่น วันเดือนปีเกิด เบอร์โทรศัพท์ เลขท้ายบัตรประจำตัวประชาชน เป็นต้น ทั้งนี้ล้วนเป็นรหัสผ่านที่มีการคาดเดาได้ง่าย ทำให้เกิดความเสี่ยงต่อข้อมูลที่จะถูกโจรกรรมข้อมูล

3.3. แนวทางในการแก้ไขปัญหา

คณะผู้จัดทำได้มีการวางแผนแนวทางในการแก้ปัญหาดังนี้

- 3.3.1. ทำการศึกษาพฤติกรรมในการใช้งานอินเทอร์เน็ตของผู้ใช้งาน
- 3.3.2. แบ่งกลุ่มผู้ใช้งานออกเป็น 3 กลุ่ม
- 3.3.3. วิเคราะห์ถึงความเหมาะสมของรหัสผ่านของแต่ละกลุ่มผู้ใช้งาน
- 3.3.4. สร้างแบบสอบถามออนไลน์เพื่อแบ่งกลุ่มผู้ใช้งานตามที่กำหนดไว้
- 3.3.5. สร้างกระบวนการในการสร้างรหัสผ่านให้แก่ผู้ใช้งาน

3.3.6. สร้างรหัสผ่านที่เหมาะสมให้กับผู้ใช้งาน

3.4. ออกแบบขั้นตอนในการแก้ไขปัญหา

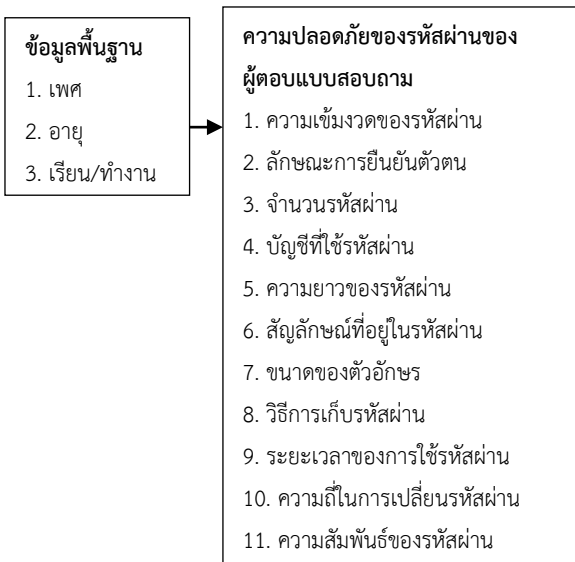
3.4.1. ออกแบบแบบสอบถาม

ตัวแปรอิสระ

ตัวแปรตาม

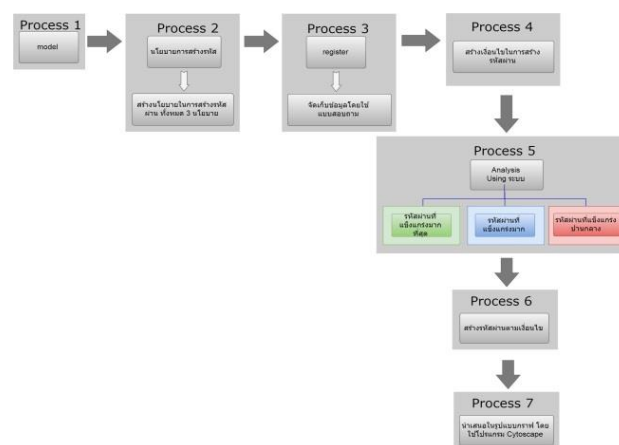
(Independent Variables)

(Dependent variables)



รูปที่ 1. กรอบแนวคิดแบบสอบถามออนไลน์

3.4.2. กรอบแนวคิด



รูปที่ 2. กรอบแนวคิดในการศึกษา

Process 1 : นำ Model จัดทำนโยบายในการสร้างรหัสผ่านตามมาตรฐาน ISO/IEC 27001

Process 2 : จัดทำนโยบายในการสร้างรหัสผ่านตามเงื่อนไขที่ได้และมีการจัดกลุ่มตามเงื่อนไขที่กำหนดไว้ โดยมีการแบ่งไว้ทั้งหมด 3 กลุ่ม และมีการจัดเก็บนโยบายไว้ในฐานข้อมูล

Process 3 : ได้มีการจัดเก็บข้อมูลเพื่อทำการทดสอบ model โดยในการจัดเก็บข้อมูลได้ใช้เครื่องมือเป็นแบบสอบถามออนไลน์

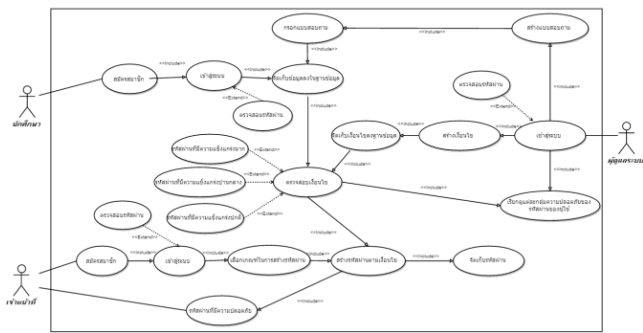
Process 4 : สร้างเงื่อนไขในการสร้างรหัสผ่านที่มีความปลอดภัย โดยแบ่งสาขาวิชาที่ความปลอดภัยของรหัสผ่านที่ใกล้เคียงไว้ แบ่งเป็น 3 กลุ่ม เพื่อสร้างรหัสผ่านที่เหมาะสม

Process 5 : วิเคราะห์ข้อมูลโดยระบบ โดยนำข้อมูลของผู้ใช้งานที่ได้จากการตอบแบบสอบถามมาตรวจสอบเงื่อนไขในการสร้างและจัดกลุ่มที่เหมาะสม

Process 6 : สร้างรหัสผ่านที่ตรงตามเงื่อนไขให้กับผู้ใช้งานในแต่ละเกณฑ์

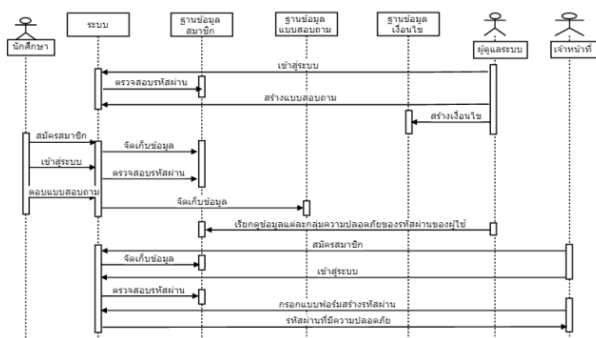
Process 7 : นำผลที่ได้จากการประมวลผลมานำเสนอในรูปแบบกราฟ โดยใช้โปรแกรม Cytoscape

3.4.3. Use Case Diagram



รูป 3. Use Case Diagram

3.4.4. Sequence Diagram



รูป 4. Sequence Diagram

กระบวนการทำงานของระบบในส่วนของ Use Case Diagram และ Sequence Diagram

ผู้ดูแลระบบ ทำการเข้าสู่ระบบและทำการตรวจสอบรหัสผ่าน หากไม่ถูกต้องจะต้องทำการเข้าสู่ระบบใหม่อีกครั้ง จากนั้นผู้ดูแลระบบจะสามารถสร้างแบบสอบถามและสร้าง

เงื่อนไขในการสร้างรหัสผ่าน ทั้งสามารถเรียกดูแต่ละกลุ่มความปลอดภัยของรหัสผ่านของผู้ใช้ได้

นักศึกษา จะต้องทำการสมัครสมาชิกและทำการตรวจสอบรหัสผ่าน หากไม่ถูกต้องจะต้องทำการเข้าสู่ระบบใหม่อีกครั้ง จากนั้นจึงจะทำการตอบแบบสอบถามและมีการตรวจสอบว่านักศึกษาตรงกับเงื่อนไขใดและอยู่ในกลุ่มใด

เจ้าหน้าที่ต้องทำการสมัครสมาชิกและทำการตรวจสอบรหัสผ่าน หากไม่ถูกต้องจะต้องทำการเข้าสู่ระบบใหม่อีกครั้ง จากนั้นจึงจะสามารถทำการเลือกเกณฑ์ในการสร้างรหัสผ่านเพื่อให้มีการสร้างรหัสผ่านที่ตรงตามเงื่อนไข และมีการจัดเก็บรหัสผ่านไว้ในฐานข้อมูล และแสดงรายงานรหัสผ่านที่มีความปลอดภัยให้กับเจ้าหน้าที่

3.5. เครื่องมือที่ใช้ในการพัฒนาระบบ

Cytoscape โปรแกรมที่ช่วยในการวิเคราะห์การจัดกลุ่มนักศึกษาที่มีระดับความปลอดภัยที่อยู่ในกลุ่มเดียวกัน เพื่อให้สามารถสร้างรหัสผ่านที่เหมาะสมกับแต่ละกลุ่ม และช่วยในการนำเสนอเพื่อให้ดูแนวโน้มและการทำงานของงานการจัดกลุ่ม เพื่อให้สะดวกและเข้าใจได้ง่ายขึ้นภายใต้รูปภาพของกราฟ

3.6. ทดสอบระบบโดยผู้เชี่ยวชาญ

ระบบการสร้างรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟนั้น มีการทดสอบระบบมีผู้เชี่ยวชาญทั้งหมด 5 ท่านและมีการสร้างแบบประเมินระบบขึ้นมาโดยแบ่งแบบประเมินทั้งหมด 3 ด้าน ได้แก่ ด้านความปลอดภัยของรหัสผ่าน, ด้านความเหมาะสมของรหัสผ่าน และด้านประสิทธิภาพของระบบ

3.7. เครื่องมือที่ใช้ในการวิจัย

การประเมินความพึงพอใจของระบบการสร้างรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟ ซึ่งจะประเมินความพึงพอใจระบบหลังจากการที่ได้ทดลองใช้ระบบ โดยใช้เครื่องมือในการวิจัยเป็นแบบสอบถาม (Questionnaire) ซึ่งมีประเด็นการประเมินทั้งหมด 3 ด้าน คือ

3.7.1. ด้านความปลอดภัยของรหัสผ่าน

3.7.2. ด้านความเหมาะสมของรหัสผ่าน

3.7.3. ด้านประสิทธิภาพของระบบ

โดยเกณฑ์ในการแปลความหมายของความพึงพอใจของระบบการสร้งรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟดังต่อไปนี้

คะแนนเฉลี่ย ด้านความปลอดภัยของรหัสผ่าน ด้านความเหมาะสมของรหัสผ่านและด้านประสิทธิภาพของระบบ

4.50 – 5.00	ความพึงพอใจมากที่สุด
3.50 – 4.49	ความพึงพอใจมาก
2.50 – 3.49	ความพึงพอใจปานกลาง
1.50 – 2.49	ความพึงพอใจน้อย
1.00 – 1.49	ความพึงพอใจน้อยที่สุด

และเกณฑ์ยอมรับต้องมีคะแนนเฉลี่ยระหว่าง 3.50 ขึ้นไปในแต่ละด้านอยู่ระดับมากขึ้นไป และคะแนนเฉลี่ยของแบบประเมินทั้งฉบับต้องมีคะแนนเฉลี่ยระหว่าง 3.50 ขึ้นไป จึงยอมรับว่ามีคุณภาพดี และสามารถนำไปใช้งานได้

4. ผลการดำเนินงาน

ระบบการสร้งรหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟ มีการพัฒนาระบบขึ้นมา โดยมีหน้าตาของระบบเป็นแบบออนไลน์เพื่อการประยุกต์ระบบในการสร้งรหัสผ่านและมีผลการประเมินระบบจากผู้เชี่ยวชาญทั้ง 5 ท่าน

4.1. ผลการพัฒนาระบบ

รูป 5. หน้าสมัครสมาชิก

รูป 5. หน้าสมัครสมาชิก ผู้ใช้งานจะต้องทำการกรอก username และ password เพื่อใช้ในการเข้าสู่ระบบ รวมทั้งกรอกข้อมูลทั่วไปของผู้ใช้งาน

รูป 6. หน้าแบบสอบถาม

รูป 6. หน้าแบบสอบถาม ภายหลังจากผู้ใช้งานทั่วไปเข้าสู่ระบบแล้ว จะสามารถเข้าสู่หน้าการตอบแบบสอบถามเพื่อเก็บข้อมูลไปใช้ในการประมวลผล

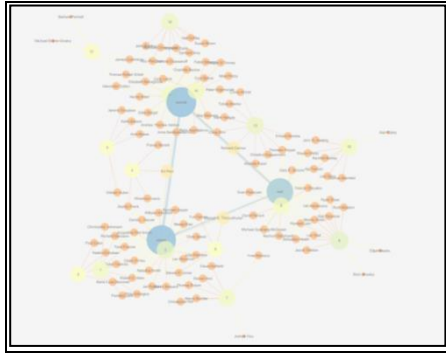
รูป 7. หน้าแบบสอบถาม

รูป 7. หน้าแบบสอบถาม เป็นหน้าที่เก็บข้อมูลเกี่ยวกับรายละเอียดของรหัสผ่านที่ผู้ใช้มีอยู่

รายงานรหัสผ่านแต่ละรายบุคคล	
รหัสประจำตัว	รหัสผ่าน
0358-40221001	bcCOC8rmM
0358-40221002	@YMUFXHN
0358-40221003	lveVjY
0358-40221004	Z5ubmbw1
0358-40221005	pCPZV67
0358-40221006	8FQA'6
0358-40221007	uJXCT2
0358-40221008	0YHZVXSJVG
0358-40221009	GAGQY6KQ
0358-40221010	6SYIYI0ETNS

รูป 8. หน้ารายงานรหัสผ่านของแต่ละบุคคล

รูป 8. หน้ารายงานรหัสผ่านของแต่ละบุคคล เป็นหน้าการทำงานในส่วนของผู้ใช้ที่ทำการสร้างรหัสผ่านเพื่อแสดงรายงานการสร้างรหัสผ่านของแต่ละบุคคลที่ได้เข้ามาตอบแบบสอบถาม



รูป 9. หน้าผลการวิเคราะห์การจัดกลุ่ม

รูป 9. หน้าผลการวิเคราะห์การจัดกลุ่ม โดยโปรแกรม Cytoscape ได้ผลการวิเคราะห์ว่าสาขาวิทยาการคอมพิวเตอร์อยู่ในกลุ่มที่มีรหัสผ่านที่แข็งแกร่งมากที่สุด โดยส่วนใหญ่จะอยู่ในกลุ่มเดียวกัน

4.2. ผลการประเมิน

ตาราง 1. ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของความพึงพอใจ ด้านความปลอดภัยของรหัสผ่าน

รายการประเมิน	ผลประเมิน		
	\bar{X}	S.D.	ผล
รหัสผ่านมีส่วนผสมของตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ อักขระ และตัวเลข	4.60	0.548	ดี มาก
รหัสผ่านตรงตามมาตรฐาน ISO/IEC 27001	4.40	0.548	ดี
รหัสผ่านมีความคาดเดาได้ยาก	3.80	0.837	ดี
รวม	4.27	0.644	ดี

จากตาราง 1. พบว่า โดยภาพรวมอยู่ในระดับดี มีค่าเฉลี่ยเท่ากับ 4.27 และเมื่อพิจารณารายข้อพบว่า ข้อที่มีการประเมินมากที่สุด คือ รหัสผ่านมีส่วนผสมของตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ อักขระ และตัวเลข มีค่าเฉลี่ยเท่ากับ 4.60 รหัสผ่านตรงตามมาตรฐาน ISO/IEC 27001 มีค่าเฉลี่ยเท่ากับ 4.40 และรหัสผ่านมีความคาดเดาได้ยากมีค่าเฉลี่ยเท่ากับ 3.80

ตาราง 2. ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของความพึงพอใจ ด้านความเหมาะสมของรหัสผ่าน

รายการประเมิน	ผลประเมิน		
	\bar{X}	S.D.	ผล
รหัสผ่านมีขนาดที่เหมาะสม	3.20	0.447	ปานกลาง
รหัสผ่านมีความเหมาะสมกับผู้ใช้	3.80	0.837	ดี
รหัสผ่านสามารถจดจำได้ง่าย	4.80	0.447	ดีมาก
รวม	3.93	0.577	ดี

จากตาราง 2. พบว่า โดยภาพรวมอยู่ในระดับดี มีค่าเฉลี่ยเท่ากับ 3.93 และเมื่อพิจารณารายข้อพบว่า ข้อที่มีการประเมินมากที่สุด รหัสผ่านสามารถจดจำได้ง่ายมีค่าเฉลี่ยเท่ากับ 4.80 รหัสผ่านมีความเหมาะสมกับผู้ใช้มีค่าเฉลี่ยเท่ากับ 3.80 และรหัสผ่านมีขนาดที่เหมาะสมมีค่าเฉลี่ยเท่ากับ 3.20

ตาราง 3. ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของความพึงพอใจ ด้านประสิทธิภาพของระบบ

รายการประเมิน	ผลประเมิน		
	\bar{X}	S.D.	ผล
ระบบมีความสวยงาม	3.40	0.548	ปานกลาง
ความง่ายต่อการใช้งานของระบบ	3.80	0.837	ดี
รวม	3.6	0.692	ดี

จากตาราง 3. พบว่า โดยภาพรวมอยู่ในระดับดี มีค่าเฉลี่ยเท่ากับ 3.6 และเมื่อพิจารณารายข้อพบว่า ข้อที่มีการประเมินมากที่สุด ความง่ายต่อการใช้งานของระบบมีค่าเฉลี่ยเท่ากับ 3.80 และระบบมีความสวยงามมีค่าเฉลี่ยเท่ากับ 3.40

ตาราง 4. ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของความพึงพอใจ ภาพรวมทั้งหมด

รายการประเมิน	ผลประเมิน		
	\bar{X}	S.D.	ผล
รวมด้านความปลอดภัยของรหัสผ่าน	4.27	0.644	ดี
รวมด้านความเหมาะสมของรหัสผ่าน	3.93	0.577	ดี
รวมด้านประสิทธิภาพของระบบ	3.6	0.692	ดี
รวม	3.93	0.637	ดี

จากตาราง 4. พบว่า โดยภาพรวมอยู่ในระดับดี มีค่าเฉลี่ยเท่ากับ 3.93 และเมื่อพิจารณารายด้านพบว่า ด้านที่มีการประเมินมากที่สุด คือ ด้านความปลอดภัยของรหัสผ่านมีค่าเฉลี่ยเท่ากับ 4.27 ด้านความเหมาะสมของรหัสผ่านมีค่าเฉลี่ยเท่ากับ 3.93 และด้านประสิทธิภาพของระบบมีค่าเฉลี่ยเท่ากับ 3.60

5. สรุปผลการศึกษาและข้อเสนอแนะ

ระบบการเข้ารหัสผ่านตามนโยบายอัจฉริยะด้วยเทคนิคกราฟระบบสามารถจัดกลุ่มความปลอดภัยของการเข้ารหัสผ่านให้กับผู้ใช้งานได้อย่างเหมาะสมและยังสามารถที่จะแสดงการวิเคราะห์และนำเสนอการจัดกลุ่มให้เข้าใจได้ง่ายมากขึ้น ระบบยังสามารถทำให้ได้รหัสผ่านที่มีความปลอดภัยของแต่ละคน นอกจากนี้ระบบยังสามารถประยุกต์ใช้งานได้หลากหลาย ทั้งแบบเรียลไทม์, การยืนยันตัวตนด้วยรหัสผ่านเพียงครั้งเดียว (OTP) ฯลฯ

จากการประเมินระบบโดยผู้เชี่ยวชาญทั้ง 5 ท่านพบว่า ในแต่ละด้านของการประเมิน ด้านที่มีการประเมินมากที่สุด คือ ด้านที่มีการประเมินมากที่สุด คือ ด้านความปลอดภัยของรหัสผ่านมีค่าเฉลี่ยเท่ากับ 4.27 ด้านความเหมาะสมของรหัสผ่านมีค่าเฉลี่ยเท่ากับ 3.93 และด้านประสิทธิภาพของระบบมีค่าเฉลี่ยเท่ากับ 3.6 โดยสรุปแล้วระบบมีค่าเฉลี่ยเท่ากับ 3.93 อยู่ในระดับดี

5.1. ข้อเสนอแนะ

5.1.1. ควรเพิ่มเติมในส่วนของการประเมินประสิทธิภาพของเครื่องมือ มากกว่าการประเมินความพึงพอใจจากผู้ใช้ และผู้เชี่ยวชาญ

5.1.2. เครื่องมือการวิจัย แบบประเมินหรือแบบสอบถาม - ควรมีการหาค่า IOC

6. เอกสารอ้างอิง

- [1] ETDA. ETDA เผยพฤติกรรมผู้ใช้เน็ตปี 59 ชี้เทรนด์ใหม่มาแรงของรัฐ - เอกชน จับตา 3G/4G ยังต้องปรับปรุงออนไลน์. 2550. จาก : <https://www.etda.or.th/content/thailand-internet-user-profile-2016-conference.html/> (23 ตุลาคม 2559).
- [2] Admin. มาตรฐาน ISO27001 ข้อมูลของท่านมีความปลอดภัยเพียงใด. ออนไลน์. 2550. จาก : <http://positioningmag.com/34131> (23 ตุลาคม 2559)
- [3] Super User. วิธีการกำหนดรหัสผ่านที่มีความปลอดภัย (Security Password). ออนไลน์. 2559. จาก : <http://agri.pnu.ac.th/index.php/2014-10-29-09-36-45/2016-01-13-04-08-25/337-password> (23 ตุลาคม 2559)

- [4] NovaBizz. พฤติกรรมมนุษย์. ออนไลน์. 2556. จาก : [http://www.novabizz.com/NovaAce/Behavior/\(23 ตุลาคม 2559\)](http://www.novabizz.com/NovaAce/Behavior/(23%20ตุลาคม%202559)).
- [5] รุจเรชา วิทยาจุฑามกุล. ความรู้เบื้องต้นเกี่ยวกับ small – world, scale-free. ออนไลน์. 2558. จาก : <https://www.gotoknow.org/posts/498766> (23 ตุลาคม 2559).
- [6] สุภาพร เกิดกิจ, ล้วนกร สร้อยมาตและสุนันทา สดสี. การวิเคราะห์การเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์โดยทฤษฎีกราฟ กรณีศึกษาวิทยาลัยพัฒนวิชาการธนบุรี. ออนไลน์. 2550. จาก : www.panitthon.ac.th:443/tccmodle/Project/supaporn/2015.pdf (23 พฤศจิกายน 2559)
- [7] Wikipedia. Cytoscape. ออนไลน์. 2550. จาก : <https://en.wikipedia.org/wiki/Cytoscape> (23 พฤศจิกายน 2559)
- [8] ณัฏพล อัครวิพัฒน์, เกียรติศักดิ์ โยชนะนัง และศิริปฐข บัญครอง. 2554. การยืนยันตัวตนด้วยรหัสผ่านแบบครั้งเดียวโดยไขการแก้ปัญหาของตัวเลขแบบสุ่มและการคำนวณอย่างง่าย. ภาควิชาเทคโนโลยีสารสนเทศ. คณะเทคโนโลยีสารสนเทศ. มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
- [9] สุภกิจ มหิทธิบุรินทร์. 2557. การพิสูจน์ตัวตนแบบสอปปัจจัยโดยใช้รหัสผ่านและภาพ. ปริญญาโท. ภาควิชาเทคโนโลยีสารสนเทศ. คณะเทคโนโลยีสารสนเทศ. มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.
- [10] นัตพร สรสง. 2556. รายงานการวิจัยการสร้างรหัสผ่าน 10 หลัก โดยใช้แนวคิดและทฤษฎีบทในเรื่องสมภาค. ปริญญาตรี. ภาควิชาคณิตศาสตร์. คณะวิทยาศาสตร์. มหาวิทยาลัยราชภัฏจันทรเกษม.
- [11] วชิรินทร์ มธูรสงพงศ์พันธ์และณัฐธนนท์ หงส์วริทธิ์ธร. “การศึกษาปัจจัยที่มีอิทธิพลต่อการใช้งานได้และความปลอดภัยของรหัสผ่านแบบการคูณ”. วารสารเทคโนโลยีสารสนเทศ ปีที่ 9, ฉบับที่ (1 มกราคม - มิถุนายน 2556). หน้า 24-33.