Social Computing and Networking

ทศพร จันทรสุกรี, ชัชวาลย์ มุ่งแสง, หทัยรัตน์ วงศ์สุพรรณ, อรพรรณ อภิรักษ์กานต์, เอมวิการ์ คงนาวัง, ปิยธิดา เพ็ชรแสน,
ธวัชชัย เรืองธนานุรักษ์, ภัทฉิกานต์ ลิมปีนิศากร, ศิธศักดิ์ สมพร, อธิบดี มาลีหวล , IEEE

บทคัดย่อ *– ในอดีตซอฟต์แวร์ในองค์กรจะมีเฉพาะในส่วนที่รองรับการทำงาน (Functional) อย่างเดียว เป็นการทำงานในรูปแบบเฉพาะส่วนภายในองค์กร (Internal) ไม่มีการปฏิสัมพันธ์หรือการเข้าถึงข้อมูลกับภายนอกองค์กร ซึ่งการพัฒนาองค์กรในปัจจุบันจำเป็นต้องมีส่วนร่วมกับสังคมให้มากขึ้น ทำให้มีการพัฒนาเครื่องมือที่ใช้เป็นตัวกลางในการสื่อสารระหว่างผู้ใช้งานกับผู้อื่นบนโลกอินเตอร์เนต (Social Software) ขึ้นมาเพื่อให้เกิดการสื่อสารภายในชุมชน (Community) ระหว่างภายในกับภายนอกองค์กร จนทำให้เกิดระบบประมวลผลทางสังคม (Social Computing) ที่ทำงานอยู่บนเครือข่ายสังคมออนไลน์ (Social Network) โดยที่เว็บไซต์เครือข่ายสังคมออนไลน์ (Social Network Website) ในแต่ละรูปแบบ เช่น เฟสบุ๊ค (Facebook), ยูทูป (YouTube) ฯลฯ กำลังได้รับความนิยมอย่างมากทั้งในฐานะผู้ใช้ทั่วไปและองค์กรธุรกิจ เพราะเป็นสังคมออนไลน์ที่เปิดโอกาสให้เข้าไปใช้เผยแพร่ข้อมูลส่วนตัว บทความ รูปภาพ ผลงาน พบปะแสดงความคิดเห็นแลกเปลี่ยนประสบการณ์ ความสนใจร่วมกันและกิจกรรมอื่น ๆ รวมไปถึงเป็นแหล่งข้อมูลจำนวนมหาศาลที่ผู้ใช้สามารถช่วยกันสร้างเนื้อหาขึ้นได้ตามความสนใจของแต่ละบุคคล ช่วยก่อให้เกิดประโยชน์ต่อผู้ใช้งานมากมายและยังทำให้เกิดรูปแบบใหม่ของการติดต่อสื่อสาร โดยในอนาคตจะมีการนำ Social Network มาใช้ในรูปแบบของ Mobile มากขึ้น ซึ่งนอกจากการสื่อสารประเภทนี้จะมีประโยชน์แล้ว แต่หากไม่มีระบบการป้องกันที่ดี ก็สามารถมีโทษอย่างมากต่อตัวผู้ใช้งานหรือองค์กรเองก็เป็นได้ ดังนั้นส่วนที่ต้องให้ความสำคัญต่อก็คือ ความปลอดภัย (Security) และความเป็นส่วนตัว (Privacy) ของผู้ใช้งาน ผู้วิจัยได้สำรวจงานวิจัยเกี่ยวกับ การรักษาความปลอดภัยเมื่อมีผู้เข้ามาโจมตีระบบ การรักษาความเป็นส่วนตัวของข้อมูล ของผู้ใช้งานเครือข่ายสังคมออนไลน์ รวมไปถึงสำรวจงานวิจัยเกี่ยวกับการประยุกต์ใช้งานเครือข่ายสังคมออนไลน์บนโทรศัพท์เคลื่อนที่ (Mobile Social Network)*

Index Key: *Social Computing and Networking, Social Network, Botnet, Privacy Management, Mobile Social Network*

I . บทนำ

ในยุคที่เทคโนโลยีการสื่อสารผ่านอินเทอร์เน็ต กำลังเป็นที่นิยมและมีผลกระทบในทุกๆด้านในปัจจุบัน ทำให้ทุกคนทุกสังคมต้องมีการปรับตัว และพัฒนาให้ทันต่อการเปลี่ยนเปลี่ยนแปลงในโลกของการ สื่อสาร และการพัฒนาของโลกเวิลด์ไวด์เว็บ (World Wide Web; WWW) จากยุคแรก คือ Web 1.0 ซึ่งมีลักษณะเป็น Static Web คือมีการนำเสนอข้อมูลทางเดียว (one-way communication) ด้วยการแปลงข้อมูลข่าวสารที่มีอยู่รอบตัวเราให้อยู่ในรูปของดิจิตอล (Digital) เช่น หนังสือพิมพ์นิตยสาร หรือการโฆษณาตามหน้าเว็บไซต์ โดยผู้ใช้สามารถอ่านได้แต่ไม่สามารถเข้าร่วมในการสร้างข้อมูลได้

แต่เมื่อก้าวเข้าสู่ยุคที่ 2 ของเทคโนโลยีคือ WWW หรือ Web 2.0 เป็นยุคที่ทำให้อินเทอร์เน็ตมี ศักยภาพในการใช้งานมากขึ้น เน้นให้ผู้ใช้มีส่วนร่วมในการสร้างสรรค์ (Co- Creation) ลงบนเว็บไซต์ร่วมกัน และสามารถโต้ตอบกับข้อมูลที่อยู่บนเว็บไซต์ได้ (Interactivity) มีลักษณะเป็น Dynamic Web ที่ผู้ใช้สามารถ สร้างเนื้อหา (Content) แลกเปลี่ยน และกระจายข้อมูลข่าวสารเพื่อแบ่งปันถึงกันได้ทั้งในระดับบุคคล กลุ่ม และองค์กร จะเห็นได้ว่าWeb 2.0 เป็นยุคของการสื่อสารสองทาง (Two-way Communication) ซึ่งไม่ใช่แค่เพียงการรับส่งอีเมล์ (E-mail) รูปภาพ หรือการดาวน์โหลดข้อมูลผ่าน Search Engine หรือใช้เว็บบอร์ด (Web board) ในการแลกเปลี่ยนความคิดเห็นกันเท่านั้น Web 2.0 ยังช่วยสร้างความสัมพันธ์ (Relationship) ระหว่างผู้ใช้ในกลุ่มต่างๆ จนเกิดเป็นเครือข่ายทางสังคม (Social Network) บนโลกออนไลน์ที่สามารถเชื่อมโยงถึงกันได้อย่างไม่มีที่สิ้นสุด กลายเป็นสังคมเสมือนจริง (Virtual Communities) ซึ่งเป็นสังคมหนึ่งในโลกของอินเทอร์เน็ต ที่ปัจจุบันยังคงผูกพันและซับซ้อนกับการดำเนินชีวิตของผู้คนในโลกของความเป็นจริง

จุดกำเนิดของ Web 2.0 และการพัฒนาก้าวผ่านเข้าสู่ยุคWeb 3.0 หรือ Semantic Web ทำให้กระแสความนิยมขอ Social Network มีการเติบโตอย่างไม่หยุดยั้งเป็นไปตามผลการสำรวจของประเทศสหรัฐอเมริกาที่พบว่า มีผู้เข้าใช้บริการ Social Network เพิ่มสูงขึ้นอย่างต่อเนื่องทุกปี และมีแนวโน้มของผู้ใช้บริการทั่วโลกมากกว่า 1,200 ล้านคน ปัจจุบัน Social Network Website ต่าง ๆ ก็มีการพัฒนา และเปิดโอกาสให้ผู้ใช้ได้เข้าไปมีส่วนร่วมในการใช้ประโยชน์เชิงสังคมกันมากขึ้น ทั้งเว็บไซต์ในตระกูลของ Wiki, YouTube, Hi5, Myspace Face book และอีกมากมาย ซึ่งในแต่เว็บไซต์จะมีลักษณะเฉพาะสำหรับการใช้งานแตกต่างกันออกไปโดยเว็บไซต์ที่มีจำนวนผู้เข้าชมสูงสุดทั่วโลกในขณะนี้คือ Myspace รองลงมา คือ Facebook และ Orkut แต่ถ้าดูจากจำนวนสมาชิกในเว็บไซต์ ผลการสืบค้นข้อมูลในปี 2008 จะเห็นว่า Facebook เป็นเว็บที่มีจำนวนสมาชิกสูงสุดถึง 90 ล้านคน รองลงมาคือ Hi5 80 ล้านคน Friendster 75ล้านคน Myspace 72 ล้านคน และ LinkedIn 5 ล้านคน

ประวัติความเป็นมาของเครื่อข่ายสังคมออนไลน์ (Social Network)

Social Network มีจุดเริ่มต้นจากเว็บไซต์ Classmates.com (1995) และเว็บไซต์ SixDegrees.com (1997) ซึ่งเป็นเว็บที่จำกัดการใช้งานเฉพาะนักเรียนที่เรียนในโรงเรียนเดียวกันเพื่อสร้างประวัติ ข้อมูลติดต่อสื่อสาร ส่งข้อความ และแลกเปลี่ยนข้อมูลที่สนใจร่วมกันระหว่างเพื่อนในลิสต์เท่านั้น ต่อมาเว็บไซต์ Epinions.com (1999) ซึ่งเกิดขึ้นจากการพัฒนาของ Jonathan Bishop โดยได้เพิ่มในส่วนของการที่ผู้ใช้สามารถควบคุมเนื้อหาและติดต่อถึงกันได้ไม่เพียงแต่เพื่อนในลิสต์เท่านั้น นับได้ว่าเป็นจุดเริ่มต้นของ Social Networking ทั้งหลายที่ก่อกำเนิดต่อมาในยุคปัจจุบัน เช่น MySpace, Google, Facebook เป็นต้น

การประมวลผลทางสังคม (Social Computting) เป็นระบบที่สนับสนุนการเก็บรวบรวมข้อมูลเพื่อการนำเสนอ การประมวลผล การใช้งาน

และการเผยแพร่ โดยอาศัยพฤติกรรมต่างๆ ของผู้ใช้งาน Social Network ภายใต้การทำงานบน Social Software และ Social Media หลากหลายรูปแบบ [53]

Social Network คือ เครือข่ายบุคคลที่เกิดขึ้นในระบบสังคมออนไลน์ เป็นสังคมที่อยู่บนการติดต่อสื่อสารผ่านอินเตอร์เน็ต อาจเรียกอีกอย่างหนึ่งว่า Virtual Community โดยสมาชิกในกลุ่มไม่จำเป็นต้องมีความสัมพันธ์อย่างแน่นแฟ้น แต่มีหัวข้อความสนใจร่วมกัน มีบทสนทนาที่แสดงถึงแนวทางความคิดในเรื่องใดเรื่องหนึ่งร่วมกัน ตัวอย่างเช่น กระทู้ตามเว็บบอร์ดต่างๆ นั่นถือเป็น Community ที่สมาชิกอาจไม่รู้จักกันจริงๆ อยู่ในสถานะของคนแปลกหน้าต่อกัน [53]

Social Software คือ เครื่องมือที่ใช้เป็นตัวกลางในการสื่อสารระหว่างผู้ใช้งานกับผู้อื่นบนโลก Internet เช่น Instant Messenger ต่างๆ ได้แก่ MSN, Google Talk, Skype เป็นต้น นอกจากนี้ยังมีเครื่องมืออื่นๆ ที่ทำงานในลักษณะ Web-based ด้วย ได้แก่ Face book, Twitter, Blogger, Wikipedia, Drop box, YouTube, Picasa เป็นต้น [53]

Social Media จึงหมายถึงสังคมออนไลน์ที่มีผู้ใช้เป็นผู้สื่อสาร หรือเขียนเล่า เนื้อหา เรื่องราว ประสบการณ์ บทความ รูปภาพ และวิดีโอ ที่ผู้ใช้เขียนขึ้นเอง ทำขึ้นเอง หรือพบเจอจากสื่ออื่นๆ แล้วนำมาแบ่งปันให้กับผู้อื่นที่อยู่ในเครือข่ายของตน ผ่านทางเว็บไซต์ Social Network ที่ให้บริการบนโลกออนไลน์ปัจจุบัน การสื่อสารแบบนี้ จะทำผ่านทาง Internet และโทรศัพท์มือถือเท่านั้น เนื้อหาของ Social Media โดยทั่วไปเปรียบได้หลายรูปแบบ ทั้ง กระดานความคิดเห็น (Discussion boards), Blog, Wiki, Podcasts, รูปภาพ และวิดีโอ ส่วนเทคโนโลยีที่รองรับเนื้อหาเหล่านี้ก็รวมถึง Blogs, เว็บไซต์แชร์รูปภาพ, เว็บไซต์แชร์วิดีโอ, เว็บบอร์ด, อีเมล์, เว็บไซต์แชร์เพลง, Instant Messaging, Tool ที่ให้บริการ Voice over IP เป็นต้น[53]

ในโลกแห่งความเป็นจริงในอินเทอร์เน็ตนั้น การบุกรุก ก่อกวน ลักลอบใช้ และทำลายระบบเป็นเรื่องที่พบเห็นได้ในชีวิตประจำวันของสังคมเครือข่าย และหลายต่อหลายครั้งที่เป็นกรณีใหญ่ที่สร้างความเสียหายเข้าขั้นอาชญากรรมทางเครือข่าย ไม่มีใครทราบอย่างแน่ชัดว่ามีผู้ใช้อินเทอร์เน็ตทั่วโลกเป็นจำนวนเท่าใด นอกจากจะคาดประมาณไว้ว่าน่าจะมีผู้ใช้อินเทอร์เน็ตอยู่ราว 100 ล้านคน ใช้งานโฮลต์ที่ต่อเชื่อมอยู่ราว 10 ล้านเครื่องในเครือข่ายที่เชื่อมโยงกันนับแสนเครือข่าย สังคมซึ่งเป็นที่รวมของผู้คนจำนวนมากเช่นอินเทอร์เน็ตนี้ย่อมมีผู้คนส่วนหนึ่งที่เป็นนักสร้างปัญหาและก่อกวนสร้างความเสียหายให้ระบบ นับตั้งแต่มือสมัครเล่นที่ทำเพื่อความสนุกไปจนกระทั่งถึงระดับอาชญากรมืออาชีพ [54] ดังนั้นการรักษาความปลอดภัยของข้อมูลของการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) เป็นเรื่องจำเป็น ผู้วิจัยจึงได้นำเสนอการสำรวจงานวิจัยเกี่ยวกับ (II.)การรักษาความปลอดภัยเมื่อมีผู้เข้ามาโจมตีระบบ (III.) การรักษาความเป็นส่วนตัวของข้อมูล ของผู้ใช้งานเครือข่ายสังคมออนไลน์ รวมไปถึงสำรวจงานวิจัยเกี่ยวกับ (IV.) การประยุกต์ใช้งานเครือข่ายสังคมออนไลน์บนโทรศัพท์เคลื่อนที่ (Mobile Social Network) และ (V.) กล่าวถึงสรุปข้อเสนอแนะและงานในอนาคต

II. SECURITY

ความปลอดภัยของคอมพิวเตอร์และเครือข่ายสังคมออนไลน์

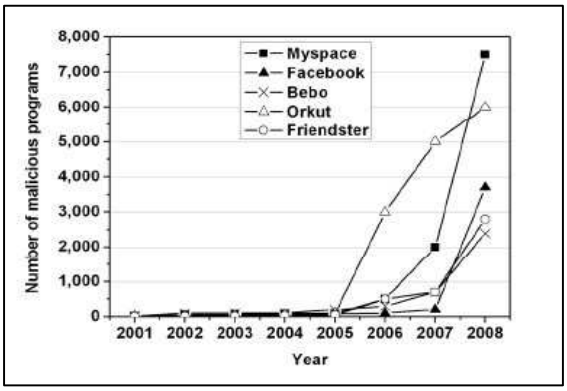
เครือข่ายทางสังคมออนไลน์ (Social Networks) เป็นเครือข่ายพื้นฐานที่สำคัญในการเปลี่ยนแปลงการดำเนินชีวิตของมนุษย์ ทั้งด้านการทำงาน ความบันเทิง การแลกเปลี่ยนข้อมูล และการติดต่อสื่อสารระหว่างกัน ทั้งนี้เพราะว่าผู้ใช้มักจะเป็นผู้นำเทคโนโลยีเครือข่ายทางสังคมออนไลน์ไปใช้เป็นกลุ่มแรกๆ ซึ่งจะมีผลต่อองค์กรธุรกิจต่างๆ ที่มักจะประสบปัญหาในการควบคุมการใช้งานเทคโนโลยีของพนักงาน และด้วยในปัจจุบันจำนวนเทคโนโลยีความปลอดภัยใหม่ๆ ที่เพิ่มมากขึ้น ทำให้ผู้ใช้สามารถที่จะรับมือกับภัยคุกคามที่มาจากการใช้งานเครือข่ายทางสังคม และด้วยเทคโนโลยีใหม่ๆ นี้จะเป็นการช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยจากการใช้งานผ่านเครือข่ายทางสังคมออนไลน์ได้

ในเครือข่ายทางสังคมออนไลน์เราสามารถที่จะแยกความแตกต่างของภัยคุกคามออกเป็น 2 ส่วน คือ ผู้ใช้ และพฤติกรรมของผู้ใช้[1] ซึ่งมักจะมีผลกระทบต่อการดำเนินงานของเครือข่ายทางสังคม และเว็บไซต์เครือข่ายสังคมก็เป็นหนึ่งในโปรแกรมของเครือข่ายอินเตอร์เน็ต ซึ่งนอกเหนือจากมาตรการที่มีคุ้มครองความปลอดภัยเว็บไซต์แล้ว เว็บไซต์นั้นควรให้สนใจการทำงานของชั้นแอปพลิเคชั่น เพื่อช่วยในการป้องกันข้อมูลของผู้ใช้ ซึ่งทั้ง 2 ส่วนนี้จะมีผลกระทบต่อความปลอดภัยของเครือข่ายสังคมออนไลน์

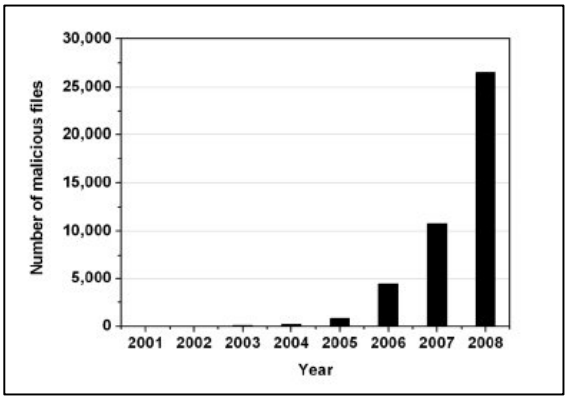
ปัจจัยสำคัญของการเกิดภัยคุกคามบนเครือข่ายสังคมออนไลน์

- การเพิ่มขึ้นของสแปมที่มีรูปแบบหลากหลายขึ้น ซึ่งเว็บไซต์เครือข่ายทางสังคมก็เป็นเป้าหมายหลักของอาชญากรรมออนไลน์ ที่จะใช้กลยุทธ์ในการโจมตีโดยการส่งข้อมูลสแปมด้วยวิธีที่หลากหลายรูปแบบเข้ามาเจาะระบบ
- มีการใช้งานเว็บไซต์เครือข่ายทางสังคมมากขึ้น เช่น เฟสบุ๊ค (Facebook) กลุ่มคนที่เล่นเฟสบุ๊ค เพื่อประโยชน์ทางด้านการแลกเปลี่ยนข้อมูล ความบันเทิง จะพบว่าเริ่มมีภัยคุกคามด้านความปลอดภัย โดยอาชญากรออนไลน์กำลังพัฒนาหนทางในการส่งมัลแวร์ผ่านเกมส์ต่างๆ เหล่านี้
- ช่องว่างของเชื่อมต่อการเข้าถึงเครือข่ายทางสังคม โดยอาชญากรรมทางคอมพิวเตอร์จะอาศัยช่วงเวลาที่เราไม่สามารถนำเทคโนโลยีการเชื่อมต่อที่ทันสมัยมาใช้ในองค์กร เพื่อป้องกันเครือข่ายให้ทันต่อความก้าวหน้าของภัยคุกคามที่มีการเพิ่มขึ้นอย่างรวดเร็ว
- การเติบโตของสแปม ที่มีอัตราการเติบโตของภัยคุกคามที่เพิ่มมากขึ้นซึ่งประเทศที่พบว่ามีจำนวนสแปมมากที่สุด คือ สหรัฐอเมริกาเครือข่ายสังคมออนไลน์จะยังคงเติบโตและมีความก้าวหน้าขึ้นไปอีก และในขณะเดียวกันภัยคุกคามที่เกี่ยวข้องกับความปลอดภัยในเครือข่ายทางสังคมก็เพิ่มมากขึ้นดังกราฟที่ 1 และ 2 ที่แสดงให้เห็นถึงจำนวนภัยคุกคามใน เครือข่ายทางสังคม ดังนั้นควรตระหนักและให้ความสำคัญกับเรื่องความปลอดภัยบนเครือข่ายสังคมออนไลน์

แผนภูมิที่ 1 แสดงให้เห็นถึงจำนวนไฟล์อันตรายในระบบเครือข่ายแยกตามปี [1]



แผนภูมิที่ 2 แสดงให้เห็นถึงจำนวนโปรแกรมอันตรายในบริการเครือข่ายสังคม [1]



ส่วนเป้าหมายของการโจมตีทางด้านออนไลน์นั้น มีหลายๆ วัตถุประสงค์[1] ตามแต่ละรูปแบบของการโจมตี โดยอาจสรุปเป้าหมายของการโจมตีได้ดังนี้

- สร้างชื่อเสียง : ผู้โจมตีบางคนโจมตีผู้ใช้คนอื่น เพียงแค่จะสร้างชื่อเสียงให้กับตัวเองหรือแค่ตอบสนองความรู้สึกส่วนตัว การโจมตีลักษณะนี้มักจะไม่ก่อให้เกิดความเสียหายมากนัก อาจจะเพียงแค่ทำให้การจราจรบนเครือข่ายหนาแน่นขึ้นเท่านั้น
- การควบคุมการเข้าถึง : การโจมตีลักษณะนี้ ผู้โจมตีจะโจมตีเพื่อที่จะเข้าควบคุมเครื่องคอมพิวเตอร์เป้าหมาย ให้ทำงานตามที่ตนเองต้องการ ที่รุนแรงคือการโจมตีในลักษณะ Botnet ซึ่งเครื่องที่ถูกโจมตีอาจจะเป็นเครื่องมือที่ใช้ในการโจมตีเครือข่ายแบบ DDoS ซึ่งจะกล่าวถึงรายละเอียดของการโจมตีแบบ Botnet ในส่วนถัดไป
- ข้อมูลส่วนตัว : ดังที่ได้กล่าวในช่วงที่แล้วว่า ข้อมูลส่วนบุคคลที่สำคัญๆ นั้น เป็นเป้าหมายสำคัญสำหรับการโจมตีเป็นอย่างมาก ข้อมูลอย่างเช่น รหัสผ่านบัญชีธนาคาร หรือหมายเลขประกันสังคม (สำหรับในประเทศสหรัฐอเมริกาหมายเลขประกันสังคมมีความสำคัญและถือเป็นข้อมูลส่วนบุคคล) ซึ่งเมื่อได้ข้อมูลส่วนนี้ จะเป็นสิ่งที่นำไปสู่การโจรกรรมทรัพย์สินของผู้เสียหาย
- ข้อมูลบริษัท : ในเวบไซต์เครือข่ายสังคมในทางธุรกิจ เช่น LinkedIn (www.linkedin.com) ผู้ใช้ส่วนมากจะเป็นเป็นภาคธุรกิจซึ่งสำหรับผู้ประสงค์ร้ายแล้ว ถือว่าเป็นอู่ข้าวอู่น้ำที่ยิ่งใหญ่สำหรับเขา การโจมจีผ่านระบบเครือข่ายภายในบริษัทนั้นมีความเป็นไปได้ยากกว่า อันเนื่องมาจากมาตรการด้านความปลอดภัยของบริษัทเหล้านี้มักจะเข้มงวดอยู่แล้ว ในทางตรงข้ามการโจมตีนี้จะทำได้ง่ายกว่าหากได้รับความไว้วางใจผ่านเครือข่ายทางสังคม ซึ่งก็จะได้ข้อมูลส่วนบุคคลของเป้าหมาย เพื่อจะนำไปเป็นกุญแจที่จะเข้าสู่บริษัทและความลับทางการเงินของบริษัทต่อไป
- เงิน : เป็นเป้าหมายใหญ่ของการโจมตี ที่มีมากขึ้นและเป็นแรงผลักดันให้มีการโจมตีในรูปแบบต่างๆ

จะเห็นว่าเป้าหมายในการโจมตีนั้นมีหลากหลายมาก โดยสามารถแบ่งรูปแบบการโจมตีคร่าวๆดังนี้

- Spam : การแพร่กระจายของอีเมลขยะที่จะเกิดความเสียหายอย่างมากสำหรับเครือข่าย สแปมแบบดั้งเดิมนั้นแพร่กระจายผ่านทาง e - mail แต่ตอนนี้พวกเขาเริ่มที่จะใช้เครือข่ายทางสังคม สแปมรวมถึงการโฆษณาหรือโปรแกรมที่เป็นอันตรายที่สามารถแพร่กระจายอย่างรวดเร็วผ่านทางรายชื่อเพื่อนในเครือข่ายทางสังคม
- ข้อบกพร่องของโปรแกรม : เครือข่ายทางสังคมเช่น Facebook เปิดโอกาสในการที่จะให้โปรแกรมเมอร์สร้างโปรแกรมเสริมเข้ามาในระบบได้ ซึ่งเพื่อที่จะดึงดูดผู้ใช้ และเมื่อมีการใช้งานผู้ใช้เพิ่มมากขึ้น อาจจะพบข้อบกพร่องของตัวโปรแกรมเอง ซึ่งจะนำไปสู่การเกิดอันตรายมากขึ้น
- Worm : หนอนที่สามารถกระจายตัวและการแพร่กระจายโดยอัตโนมัติ หนอนจะขโมยข้อมูลส่วนตัวเช่นรหัสผ่านและหมายเลขบัญชีธนาคาร ข้อมูลเหล่านี้จะถูกขายในตลาดมืด เพื่อใช้ในการขโมยข้อมูลบัตรเครดิตและธนาคารของผู้ใช้
- XSS : XSS สามารถสร้างขึ้นลงในโค้ดของหน้าเว็บและก่อให้เกิดภัยคุกคามที่ดีให้กับผู้ใช้ ผู้บุกรุกสามารถใช้ช่องโหว่ XSS เพื่อขโมยคุกกี้ เรียก FLASH, ในการดาวน์โหลดมัลแวร์และอื่น ๆ มีปฏิสัมพันธ์ระหว่างผู้ใช้หลายคนในเครือข่ายทางสังคม ข้อมูลจำนวนมากรวมทั้ง URL ที่มีบาง XSS ดึงดูดผู้ใช้จำนวนมาก เมื่อผู้ใช้คลิกที่ URL ที่เป็นเป้าหมายการโจมตีจะได้รับการนำไปสู่เป้าหมายนั้น
- Plug - in : โปรแกรมเสริมบางอย่างเช่น Flash และ Silverlight ได้รับอนุญาตให้ทำงานในเบราว์เซอร์ นอกจากนี้ยังนำเป็นภัยคุกคามใหม่เครือข่ายทางสังคม เมื่อเร็ว ๆ นี้ข้อบกพร่องของ Flash ได้รับการค้นพบ ซึ่งเป็นรูปแบบการโจมตีที่เกี่ยวข้องกับเครือข่ายทางสังคม
- Phishing : เครือข่ายทางสังคมในการโจมตีสามารถปลอมตัวเป็นผู้ใช้ที่ถูกต้อง และใช้วิศวกรรมทางสังคมเพื่อดึงดูดผู้ใช้อื่น ๆ คลิกที่ URL ที่ได้รับการออกแบบ ผู้ใช้ในเครือข่ายทางสังคมยินดีที่จะยอมรับคำเชิญของคนแปลกหน้าและสื่อสารกับพวกเขา ซึ่งจะนำไปสู่การโจมตีฟิชชิ่ง ซึ่งจะกล่าวถึงในส่วนต่อไป

ตัวอย่างการโจมตีและการป้องกัน (Security)

BOTNET

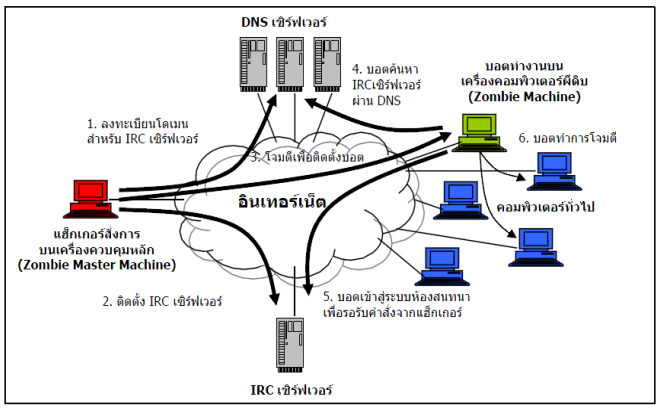
บอตเน็ต[2] (BOTNET) หรือ roBOT NETwork เป็นภัยคุกคามต่อผู้ใช้งานอินเทอร์เน็ตรูปแบบใหม่ ซึ่งแฮ็กเกอร์เขียนโปรแกรมบอตเน็ตโดยใช้เทคนิคการโจมตีเครือข่ายอินเทอร์เน็ตด้วยโปรแกรมประสงค์ร้าย (Malware) ที่ซับซ้อนและมีรูปแบบที่หลากหลายกว่าไวรัสคอมพิวเตอร์หรือหนอนอินเทอร์เน็ตทั่วไป บอตเน็ตที่ถูกสร้างขึ้นนี้อาจเป็นเครื่องมือที่ใช้ส่งสแปมเมล์ (Spam Mail) และ Phishing ซึ่งเป็นวิธีการสร้างความเสียหายให้กับระบบเครือข่ายอินเทอร์เน็ตได้ นอกจากนี้พบว่ามีการนำบอตเน็ตไปใช้เป็นเครื่องมือประกอบอาชญากรรมทางคอมพิวเตอร์อื่น ๆ อีกด้วย

BOTNET คืออะไร

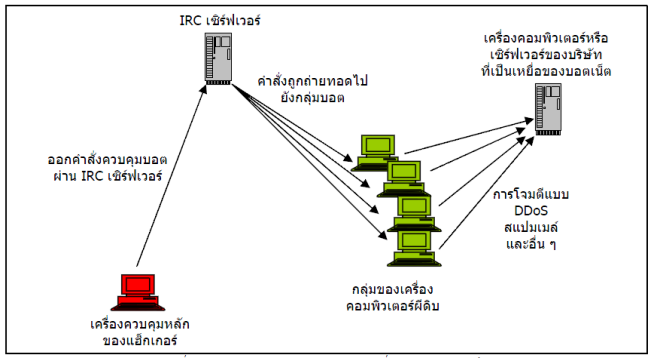
หลายคนคงเคยรู้จักกับคำว่า บอต (Bot) ซึ่งเป็นหุ่นยนต์ทางซอฟต์แวร์ที่มักจะถูกติดตั้งบนเครื่องไคลเอ็นต์ให้คอมพิวเตอร์สามารถทำงานตามคำสั่งที่กำหนดไว้ล่วงหน้าได้โดยอัตโนมัติ ตัวอย่างเช่นบอตของห้องสนทนา IRC (Internet Relay Chat) หรือบอตของเกมส์ออนไลน์ต่าง ๆ เป็นต้น ส่วนบอตที่ถูกใช้โดยโปรแกรมประสงค์ร้ายใน “บอตเน็ต” จะแตกต่างจากบอตธรรมดาตรงที่มันเป็นสมาชิกในเครือข่ายของบอตที่ถูกควบคุมจากระยะไกลโดยแฮ็กเกอร์ที่ใช้เครื่องควบคุมหลักหรือที่เรียกว่า Zombie Master Machine เป็นตัวสั่งการ ผลจากการวิเคราะห์ของผู้เชี่ยวชาญพบว่า บอตของบอตเน็ตมีวิวัฒนาการมาจากบอตของ IRC ที่ใช้ในการควบคุมห้องสนทนา IRC นั่นเอง

การทำงานของ BOTNET

ลักษณะที่สำคัญของบอตเน็ตก็คือจะมีศูนย์กลางควบคุมและสั่งการโดยแฮ็กเกอร์อยู่ที่ใดที่หนึ่งบนอินเทอร์เน็ต กลไกการทำงานของบอตเน็ตถูกออกแบบให้มีการแพร่กระจายตัวเพื่อหาเครื่องใหม่ให้เข้ามาอยู่ในกลุ่มและมีความสามารถในการแก้ไขโปรแกรมของบอตที่ฝังตัวอยู่บนเครื่องคอมพิวเตอร์ผีดิบเพื่อเปลี่ยนแปลงรูปแบบการบุกรุก ลักลอบใช้งานและสั่งการผ่านศูนย์ควบคุม ซึ่งองค์ประกอบหลักของบอตเน็ตได้แก่เครื่องคอมพิวเตอร์สั่งการระยะไกลของแฮ็กเกอร์ เครื่องเซิร์ฟเวอร์ของห้องสนทนา IRC ที่เป็นจุดนัดพบระหว่างกลุ่มของบอตและแฮ็กเกอร์เพื่อรอรับคำสั่ง กลุ่มของ DNS เซิร์ฟเวอร์ซึ่งเป็นทางผ่านเพื่อทำให้บอตสามารถหาเครื่อง เซิร์ฟเวอร์ของห้องสนทนา IRC เจอได้ นอกจากนี้ยังมีกลุ่มของเครื่องคอมพิวเตอร์ต่าง ๆ บนเครือข่ายอินเทอร์เน็ตที่เป็นเป้าหมายของบอตเน็ตและกลุ่มที่ได้กลายเป็นส่วนหนึ่งของบอตเน็ตไปแล้ว



รูป 2 แสดงลักษณะของผลกระทบที่เกิดจากบอทเน็ต



รูป 1แสดงขั้นตอนการทำงานของบอตเน็ต

กระบวนการทำงานของบอตเน็ตมีขั้นตอนดังรูปที่ 1 เริ่มจากแฮ็กเกอร์ที่เป็นเจ้าของบอตเน็ตจะสร้างบอตเน็ตด้วยการติดตั้งเซิร์ฟเวอร์ห้องสนทนา IRC เตรียมไว้ ณ ที่ใดที่หนึ่งบนเครือข่ายอินเทอร์เน็ต โดยอาจเป็นเซิร์ฟเวอร์ที่ถูกต้องตามกฎหมายหรือเป็นเครื่องที่ถูกบุกรุกเพื่อนำมาใช้เป็นเซิร์ฟเวอร์ห้องสนทนา IRC ก็ตามหลังจากนั้นแฮ็กเกอร์ก็จะทำการลงทะเบียนชื่อโดเมนและหมายเลข IP ของเซิร์ฟเวอร์ห้องสนทนา IRC ไว้กับบริการ DNS บนอินเทอร์เน็ตเพื่อให้บอตสามารถค้นหาเซิร์ฟเวอร์ของห้องสนทนาอื่น ๆ ที่แฮ็กเกอร์ผู้นั้นได้ติดตั้งบอตไว้ก่อนแล้ว

เมื่อโครงสร้างหลักข้างต้นพร้อมแล้ว แฮ็กเกอร์ก็จะเริ่มทำการโจมตีเครื่องคอมพิวเตอร์เครื่องอื่น ๆ บนอินเตอร์เน็ตเพื่อค้นหาเหยื่อสำหรับติดตั้งบอตและทำให้เครื่องคอมพิวเตอร์เหล่านั้นกลายเป็นเครื่องคอมพิวเตอร์ผีดิบ โปรแกรมโจมตีของบอตส่วนใหญ่ที่นิยมมักจะอยู่ในรูปแบบของหนอนอินเทอร์เน็ตหรือโปรแกรมโจมตีคอมพิวเตอร์ที่ฝังตัวอยู่ในโปรแกรมประยุกต์ต่าง ๆ เช่นการโจมตีโดยอาศัยข้อมูลทางเว็บไซต์ที่แฮ็กเกอร์อาจจะทำการฝังโปรแกรมประสงค์ร้ายต่าง ๆ ไว้บนเว็บเซิร์ฟเวอร์ก่อนอยู่แล้ว หรือการซ่อนโปรแกรมประสงค์ร้ายผ่านทางการแชร์ไฟล์ในแบบ peer-to-peer เพื่อที่จะลักลอบเข้าไปติดตั้งโปรแกรมโทรจันสำหรับบอตเน็ตในเครื่องคอมพิวเตอร์ของเหยื่อผู้เคราะห์ร้าย เป็นต้น

เมื่อบอตสามารถทำงานบนเครื่องคอมพิวเตอร์ผีดิบได้แล้ว บอตก็จะทำการติดต่อกับ DNS เซิร์ฟเวอร์โดยอัตโนมัติเพื่อค้นหาเซิร์ฟเวอร์ห้องสนทนา IRC ที่แฮ็กเกอร์ติดตั้งรอไว้ เมื่อพบเซิร์ฟเวอร์แล้วบอตก็จะทำการล็อกอินเข้าไปเพื่อรอรับคำสั่งจากแฮ็กเกอร์ เมื่อถึงเวลาที่ต้องการและมีจำนวนบอตมากเพียงพอแฮ็กเกอร์ก็จะล็อกอินผ่านเครื่องควบคุมบอตเน็ตหลัก (zombie master machine) เข้าสู่ระบบ IRC เซิร์ฟเวอร์นั้นเพื่อทำการออกคำสั่งต่าง ๆ เช่นให้ทำการโจมตีแบบ DDoS (Distributed Denial of Service) ไปยังเครื่องคอมพิวเตอร์เป้าหมายต่าง ๆ บนระบบเครือข่ายอินเทอร์เน็ต หรือทำการส่งสแปมเมล์สร้างความรำคาญให้กับผู้ใช้อินเทอร์เน็ตทั่วไปได้ นอกจากนี้แฮ็กเกอร์ยังสามารถที่จะสั่งการให้เกิดการแพร่กระจายและจู่โจมด้วยไวรัสคอมพิวเตอร์โดยอาศัยเครื่องคอมพิวเตอร์ผีดิบได้อีกด้วย ซึ่งจะส่งผลให้มีการติดตั้งบอตเพิ่มขึ้นบนเครื่องคอมพิวเตอร์อื่น ๆ อีกนับพันเครื่องในระบบเครือข่ายอินเทอร์เน็ตต่อไป นอกจากนี้เทคนิคที่เครื่องคอมพิวเตอร์ผีดิบนิยมใช้โจมตีเครื่องคอมพิวเตอร์อื่น

ๆ ก็คือการโจมตีโดยอาศัยโปรโตคอลปกติทั่วไป เช่นโปรโตคอลของเว็บ เป็นต้น ประกอบกับเทคนิคการปลอมแปลงหมายเลข IP ของผู้ส่งหรือที่เรียกว่าเทคนิค IP Spoofing ส่งผลให้การค้นหาต้นกำเนิดของบอตเน็ตที่แท้จริงนั้นทำได้ยากมากยิ่งขึ้น ดังนั้นจึงไม่น่าแปลกใจเลยว่าในปัจจุบันจำนวนเครื่องคอมพิวเตอร์ผีดิบที่ถูกควบคุมโดยเครื่องควบคุมบอตเน็ตหลักนั้นมีจำนวนมากและมีแนวโน้มว่าจะเพิ่มสูงขึ้นเรื่อย ๆ อีกด้วย

นอกจากนี้การโจมตีของเครื่องคอมพิวเตอร์ผีดิบมีความซับซ้อนมากยิ่งขึ้น มีการโจมตีแบบผสมผสานกล่าวคือในการโจมตีครั้งหนึ่งอาจจะใช้ทั้งไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต และม้าโทรจัน ประกอบกันตัวอย่างวิธีการโจมตีที่พบเห็นล่าสุดมีการแบ่งเป็นขั้นตอนดังนี้ เริ่มด้วยการใช้ไวรัสคอมพิวเตอร์โจมตีพร้อมทั้งติดตั้งม้าโทรจันซึ่งจะทำการเปิดประตูลับ (Backdoor) บนเครื่องคอมพิวเตอร์ของเหยื่อ หลังจากนั้นก็ทำการปลดการควบคุมการใช้งานของเครื่องเหล่านั้นพร้อมทั้งหยุดการทำงานของโปรแกรมป้องกันไวรัสต่าง ๆ และตามด้วยการโจมตีที่รุนแรงยิ่งขึ้นต่อไป เนื่องจากบอตนั้นถูกสั่งการจากศูนย์ควบคุมบอตหลักที่ถูกติดตั้งบนเซิร์ฟเวอร์ของห้องสนทนา IRC จึงไม่ใช่เรื่องยากที่แฮกเกอร์จะสามารถเปลี่ยนแปลงการทำงานของบอต รวมทั้งสามารถอัพเดตตัวเองได้ ล่าสุดเมื่อไม่นานมานี้บอตเน็ตเริ่มมีการประยุกต์ใช้เทคนิคที่สามารถแก้ไขข้อมูลในระดับเคอร์เนล(Kernel) และในระดับแอพพลิเคชัน (Application) ของระบบปฏิบัติการที่เรียกว่าเทคนิค Root Kits เพื่อทำการซ่อนการทำงานของโปรแกรมของบอตเน็ต บอตเน็ตประเภทนี้ได้แก่บอตเน็ตสายพันธุ์ “Rbot” เป็นต้น ดังนั้นจะเห็นว่าบอตเน็ตชนิดใหม่ที่ถูกพัฒนาและถูกปล่อยออกมาอาละวาดในโลกอินเทอร์เน็ตในปัจจุบันนั้นมีความสามารถและรูปแบบที่มีความรุนแรงสูงขึ้นจนทำให้การป้องกันก็ทำได้ยากยิ่งขึ้นด้วย

ผลกระทบของภัยคุกคามจาก BOTNET

จากความซับซ้อนและรูปแบบของการโจมตีต่าง ๆ ของบอตเน็ตดังที่อธิบายแล้วในข้างต้น จะเห็นได้ว่าบอตเน็ตสามารถทำให้เกิดผลกระทบในวงกว้างต่อองค์กรและผู้ใช้อินเทอร์เน็ตทั่วไปได้ มีการคาดการณ์ว่าบอตเน็ตอาจเป็นภัยรูปแบบใหม่ที่มีระดับความรุนแรงสูงสุดเท่าที่เคยมีมาบนเครือข่ายอินเทอร์เน็ต ตัวอย่างที่เห็นได้ชัดก็คือเหตุการณ์ที่เกิดขึ้นในเดือนมิถุนายน พ.ศ. 2547 ซึ่งมีการค้นพบสาเหตุของความขัดข้องของเครือข่ายของเว็บไซต์ชื่อดังอย่างเช่น Google และ Yahoo! ว่ามาจากการโจมตีแบบ DDoS (Distributed Denial of Service) ของบอตเน็ต ทำให้ผู้ใช้อินเทอร์เน็ตทั่วไปไม่สามารถเข้าไปขอใช้บริการเว็บไซต์ดังกล่าวได้เป็นเวลาประมาณสองชั่วโมง จากเหตุการณ์ดังกล่าวทำให้เจ้าหน้าที่รักษาความปลอดภัยของข้อมูลทางคอมพิวเตอร์และบริษัทที่พัฒนาโปรแกรมป้องกันไวรัสทั้งหลายเริ่มหันเหความสนใจจากปัญหาของไวรัสคอมพิวเตอร์และหนอนอินเทอร์เน็ตธรรมดามาสู่ภัยคุกคามรูปแบบใหม่ของบอตเน็ตมากขึ้น

เนื่องจากปริมาณข้อมูลที่ถูกสร้างขึ้นโดยบอตเน็ตอาจมีปริมาณมหาศาลหากจำนวนบอตมีจำนวนมากนับแสนเครื่อง ผู้ที่ได้รับผลกระทบเป็นอันดับแรกก็คือผู้ให้บริการเครือข่ายอินเทอร์เน็ต (Internet Service Providerหรือ ISP) เนื่องจากปริมาณข้อมูลจำนวนมากอาจทำให้ระบบโครงสร้างหลักของอินเทอร์เน็ตไม่สามารถให้บริการต่อไปได้ เช่นบริการของเซิร์ฟเวอร์ DNS อุปกรณ์เครือข่ายเราเตอร์ สวิตช์ ต้องทำงานหนักจนเกินไป และสายส่งข้อมูลอาจขัดข้องได้ เป็นต้น

อันดับที่สองก็คือผู้ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตทั่วไปซึ่งเป็นอาจตกเป็นเหยื่อ โดยถูกใช้เครื่องคอมพิวเตอร์ในการทำบอตเน็ต อาจถูกขโมยข้อมูลส่วนตัวที่สำคัญเช่น รหัสผ่านและข้อมูลทางการเงินจำพวกบัตรเครดิตหรือหมายเลขบัญชีธนาคาร เป็นต้น เพื่อนำไปขายหรือหาประโยชน์ บอตเน็ตบางประเภทสามารถที่จะขโมย CD keys ของโปรแกรมต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ส่วนบุคคลได้ นอกจากนี้บางครั้งเครื่องคอมพิวเตอร์อาจถูกใช้เป็นฐานในการโจมตีระบบเครือข่ายอื่น ๆ ต่อไปอีกด้วย

ผู้เสียหายที่ได้รับผลกระทบอันดับสุดท้ายคือผู้ที่ถูกโจมตีจากเครื่องคอมพิวเตอร์ผีดิบซึ่งถูกควบคุมโดยแฮกเกอร์ ตัวอย่างที่อาจเกิดขึ้นได้แก่ แฮกเกอร์สั่งการให้เครื่องคอมพิวเตอร์ผีดิบทำการโจมตีแบบ DDoS ไปยังเครื่องเซิร์ฟเวอร์อื่น ส่งผลทำให้เซิร์ฟเวอร์เหล่านั้นไม่สามารถให้บริการได้ตามปกติ ทั้งนี้เนื่องจากมีข้อมูลขยะจำนวนมาก บางครั้งผู้เสียหายบางกลุ่มอาจถูกขู่กรรโชกทรัพย์ หากไม่ยอมจ่ายเงินให้กับกลุ่มแฮกเกอร์ที่ควบคุมบอตเน็ต ก็อาจจะถูกโจมตีโดยบอตเน็ตได้ จากเหตุการณ์นี้แสดงให้เห็นว่าบอตเน็ตได้กลายเป็นเครื่องมือของการก่ออาชญากรรมบนอินเทอร์เน็ตไปแล้ว

การตรวจหา BOTNET

วิธีการตรวจหาบอตเน็ตจะใช้ทั้งหมด 4 เทคนิคด้วยกันคือ

- Signature-based Detection

เป็นระบบการตรวจหา botnet โดยอาศัยการตรวจหาลายเซ็นประจำตัวหรือพฤติกรรมประจำตัวของ botnet นั้นๆ จึงเป็นที่มาของอีกชื่อหนึ่งนั่นคือ signature based หรือ knowledge based detection ความรู้ในเรื่องของลายเซ็นประจำตัวหรือพฤติกรรมประจำตัวของ botnet มีประโยชน์ในการตรวจหา botnet คือ หากเราทราบถึงพฤติกรรมประจำตัวหรือกลไกการทำงานของ botnet เราจะสามารถตรวจจับได้ว่ามีการรัน botnet นั้นๆอยู่

ตัวอย่างเช่น Snort[3] ซึ่งเป็น open source ระบบตรวจจับการบุกรุก (IDS) ซึ่งตรวจสอบ network traffic เพื่อหาสัญญาณของการบุกรุก Snort มีการกำหนดค่าของกฎหรือลายเซ็นเพื่อล็อค traffic ที่ถือว่าน่าสงสัย[3] อย่างไรก็ตามเทคนิคการตรวจหาแบบ signature-based detection สามารถใช้สำหรับการตรวจหา บอตเน็ตที่รู้จักเท่านั้น ดังนั้นการแก้ปัญหานี้ยังไม่เป็นประโยชน์สำหรับบอตที่ไม่รู้จัก

- Anomaly-based Detection

การทำงานของระบบนี้จะเป็นการตรวจสอบ pattern ของข้อมูลหรือจะเรียกว่าพฤติกรรมต่างของ ข้อมูลที่วิ่งอยู่ในระบบเพื่อเรียน รู้ว่าอะไรคือสิ่งปกติและผิดปกติภายในระบบโดยที่ระบบจะมีกระบวนการเรียนรู้ ด้วยตัวเอง เหมือนดังเช่นกับระบบ spam filter โดยปกติแล้วระบบนี้จะถูกตั้งค่าโดยผู้ดูแลระบบเครือข่ายโดยที่ผู้ดูแล อาจจะกำหนดเส้นแบ่งว่าพฤติกรรมไหนถือว่าเป็นพฤติกรรมที่ปกติโดยอาจจะพิจรณา จาก traffic, พฤติกรรม, protocol หรือขนาดของข้อมูลเป็นต้น ดังนั้นจะทราบได้ทันทีว่าพฤติกรรมไหนเป็นพฤติกรรมที่เข้าข่ายการโจมตีระบบ นั่นเองเนื่องจากระบบ Anomaly Based นั้นสามารถที่จะ

เรียนรู้ได้ด้วยตนเอง ดังนั้นระบบดังกล่าวนี้ก็จะสามารถเรียนรู้วิธีหรือพฤติกรรมใหม่ๆ ที่ใช้ในการโจมตีระบบได้นั่นเองแต่ก็อาจจะทำงานผิดผลาดได้นั่นหมายถึงไม่มี การส่งสัญญาณเตือนเมื่อมีการโจมตีเพราะเข้าใจว่าเป็นพฤติกรรมที่ปกติในระบบ เครือข่าย ตัวอย่างเช่น Botsniffer [4]

- DNS-based Detection

เป็นการตรวจสอบหา botnet โดยอาศัยข้อมูลจาก DNS ที่สร้างโดย botnet นั้น เป็นวิธีการที่คล้ายกับ Anomaly-based Detection (การตรวจจับโดยอาศัยการตรวจความผิดปกติของ pattern ของข้อมูล) โดยจะเน้นที่การตรวจสอบความผิดปกติของสภาวะที่มีการคับคั่งของ DNS มากเกินไป คือเนื่องจากกลไกการทำงานของ bot เริ่มต้นการเชื่อมต่อโดยการเชื่อมต่อกับ C&C Server เพื่อรับเอาคำสั่ง เพื่อที่จะเข้าถึงกับ C&C Server bot จะต้องแสดง DNS quries เพื่อหาตำแหน่งที่ตั้งของ C&C Server ดังนั้นจึงสามารถตรวจหาความผิดปกติของสภาวะที่มีการคับคั่งของ DNS มากเกินไป โดยการเฝ้าสังเกตการคับคั่งของ DNS

ตัวอย่างเช่น Dagon [7] และ Kristoff [6] ใช้กลไกในการตรวจหา botnet โดยตรวจสอบโดเมนเนมที่มีมากกว่าปกติ หรือ โดเมนเนมที่มี query rate บน DDNS มากเกินไป อย่างไรก็ตาม กลไกนี้ยังมีจุดอ่อนคือ หากใช้ DNS ปลอมจะไม่สามารถตรวจสอบได้

ในปี 2007, Choi et al, [11] นำเสนอวิธี anomaly-based โดยการตรวจสอบกิจกรรมกลุ่ม Botnet ในการจราจรใน DNS ซึ่งรูปแบบกิจกรรมกลุ่มใน DNS มีการส่งคำสั่งพร้อมกันโดย Bot กระจาย พวกเขามีการกำหนดคุณลักษณะเฉพาะของการเข้าชม DNS เป็นกิจกรรมกลุ่มที่จะแยกแบบสอบถาม DNS botnet จากการสอบถาม DNS ถูกต้องตามกฎหมาย เนื่องจากการจราจร DNS จะปรากฏในหลายขั้นตอนของ Botnet วงจรชีวิตก็เป็นไปได้ในการตรวจสอบบ็อตเน็ตโดยใช้คุณสมบัติกิจกรรมกลุ่มของการเข้าชม DNS Botnet พวกเขายังได้พัฒนากลไกที่ช่วยให้การตรวจสอบการโยกย้ายเซิร์ฟเวอร์ C & C นี้ วิธี anomaly-based มีประสิทธิภาพมากขึ้นกว่าวิธีก่อนหน้านี้และสามารถตรวจสอบ botnet ไม่คำนึงถึงชนิดของ bot และ botnet โดยดูที่กิจกรรมกลุ่มของพวกเขาในการจราจร DNS นอกจากนี้ยังสามารถตรวจสอบ botnets ที่มีการเข้ารหัสเนื่องจากมันจะใช้ข้อมูลที่ส่วนหัวของ IP อย่างไรก็ตามข้อเสียของวิธีนี้คือการใช้เวลาการประมวลผลสูง สำหรับการตรวจสอบเครือข่ายขนาดใหญ่

- Mining-based Detection

เป็นวิธีการตรวจสอบโดยอาศัยการบ่งชี้ความคับคั่งของ botnet C&C เป็นการตรวจจับที่ค่อนข้างยากเนื่องจากการสื่อสารแบบ C&C เป็นโปรโตคอลปกติที่ botnet ใช้ ซึ่งการสื่อสารแบบนี้จะทำให้ความคับคั่งของระบบเป็นปกติ คือ ไม่เกิดสภาวะที่เครือข่ายใช้เวลาแฝงมากเกินปกติ (high latency network), ไม่เกิดสภาวะที่มีการคับคั่งของเครือข่ายมากเกินไป จึงทำให้วิธีที่ 2 ไม่สามารถตรวจจับความคับคั่งของ C&C ได้

ตัวอย่างเช่น Rishi [7] คิดค้นโดย Geobl and Holz เป็นการเฝ้าระวังตรวจหาความผิดปกติของ IRC nicknames, IRC servers, และ server ports ที่ไม่ปกติ ซึ่ง Rishi นี้มีจุดอ่อนคือจะไม่สามารถตรวจหา botnet ประเภท non-IRC ได้

ตารางที่ 1 เปรียบเทียบเทคนิคการตรวจสอบ Botnet ด้วยเทคนิคแบบต่างๆ

วิธีการตรวจสอบ		ตรวจสอบ Bot ที่ไม่รู้จัก	โปรโตคอลและโครงสร้างที่เป็นอิสระ	ตรวจสอบ Bot ที่เข้ารหัส	ตรวจสอบแบบเรียลไทม์	ความผิดพลาดจากการตรวจสอบต่ำ
Signature-based	[3]	×	×	×	×	×
Anomaly-based	[4]	✓	×	×	×	×
	[5]	✓	×	✓	×	✓
	[6]	✓	×	✓	×	✓
DNS-based	[7]	✓	×	✓	×	×
	[8]	✓	×	✓	×	×
	[9]	✓	×	✓	×	✓
	[10]	✓	×	✓	✓	×
	[11]	✓	✓	✓	×	✓
Mining-based	[12]	✓	×	×	×	×
	[13]	✓	×	×	×	×
	[14]	✓	✓	✓	×	✓
	[15]	✓	✓	✓	×	✓

จากการศึกษาเทคนิคการตรวจสอบ 4 เทคนิคด้วยกันคือ Signature-based, Anomaly-based, DNS-based และ Mining-based พบว่าเทคนิค Mining – based มีประสิทธิภาพมากที่สุด คือมีการวิเคราะห์หา botnet ที่แม่นยำกว่าเทคนิคอื่นๆเมื่อเปรียบเทียบกัน และจากค่าความผิดพลาดจากการตรวจสอบเทคนิคแบบ Mining-based มีค่าผิดพลาดต่ำที่สุด

III . Privacy

ความปลอดภัยหรือความเป็นส่วนตัว (Privacy) ของข้อมูลที่ผู้ใช้งานเผยแพร่บนเครือข่ายสังคมออนไลน์เป็นสิ่งที่ควรตระหนักถึงในการใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์ เนื่องจากผู้ใช้งานบางคนอาจมีวุฒิภาวะไม่เพียงพอที่จะใส่ใจในความปลอดภัยของตนเอง หรือรู้เท่าไม่ถึงการณ์ว่าข้อมูลบางประเภทนั้นสามารถเป็นประโยชน์ต่อมิจฉาชีพได้ หรือกรณีอื่นๆคือข้อมูลผู้ใช้งานเหล่านี้มีประโยชน์อย่างมากในทางการตลาด ส่วนหนึ่งของการปกป้องตัวเองนั้น ผู้ใช้งานจะต้องมีวิจารณญาณก่อนที่จะให้ข้อมูลต่างๆของตนลงบนเว็บไซต์ฯ และตัวเว็บไซต์ฯเองควรจะมีกลไกในการรักษาความปลอดภัยของข้อมูลให้แก่ผู้ใช้งานเพื่อป้องกันการรั่วไหลของข้อมูลผู้ใช้งาน จากงานวิจัยที่มีการสอบถามผู้ใช้งานเว็บไซต์ฯระดับนักเรียน [31] พบว่าผู้ใช้งานบางส่วนไม่มีความรู้ในด้านการใช้เครื่องมือในการป้องกันความเป็นส่วนตัวของข้อมูล

เว็บไซต์เครือข่ายสังคมออนไลน์ส่วนใหญ่นั้นจะมีฟังก์ชันในการป้องกันความเป็นส่วนตัวให้ผู้ใช้งานได้ตั้งค่ารวมถึงความสามารถในการจำกัดสิทธิ์ผู้ใช้งานอื่นในการเข้าถึงข้อมูล แต่ยังไม่เพียงพอต่อการป้องกันความเป็นส่วนตัวของข้อมูล เช่นการเข้าถึงข้อมูลจากบริการหรือแอพลิเคชันต่างๆ ผู้ใช้งานไม่สามารถจำกัดระดับของข้อมูลที่เปิดเผยแก่บริการนั้นๆได้ หรืออำนาจความเป็นเจ้าของข้อมูลของผู้ใช้งานเอง เว็บไซต์เครือข่ายสังคมออนไลน์ส่วนใหญ่แล้วมีระบบการทำงานแบบ client-server ทำให้ข้อมูลของผู้ใช้งานไปรวมศูนย์กลางที่ เครื่องแม่ข่าย (Server) ของเว็บไซต์ฯนั้นๆ และพบว่าเว็บไซต์ฯนำ

ข้อมูลเหล่านั้นไปใช้เป็นเครื่องมือทางการตลาด การพัฒนากลไกการป้องกันความเป็นส่วนตัวของการใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์ เป็นสิ่งจำเป็น เนื่องจากปัจจุบันผู้ใช้งานเว็บไซต์เครือข่ายสังคมออนไลน์มีจำนวนเพิ่มขึ้นมาก และมีหลากหลายระดับอายุ ซึ่งการติดต่อสื่อสารผ่านทางเว็บไซต์ฯเหล่านี้จะเป็นอันตรายต่อตัวผู้ใช้งานที่รู้เท่าไม่ถึงการณ์ ดังมีบทความวิจัยหลากหลายบทความที่ได้พัฒนากลไกการป้องกันความเป็นส่วนตัวบนเว็บไซต์เครือข่ายสังคมออนไลน์ ยกตัวอย่างเช่น Facecloak[22]

นอกจาก FaceCloak แล้วผู้วิจัยยังได้ศึกษาเพื่อเปรียบเทียบกลไกการทำงานของระบบป้องกันความเป็นส่วนตัวอีกหลายๆระบบ โดยอาศัยเทคนิคต่างๆของการป้องกันความเป็นส่วนตัวซึ่งอ้างอิงจาก [30]

การป้องกันความเป็นส่วนตัวบนเว็บไซต์เครือข่ายสังคมออนไลน์ คือ การควบคุมการเปิดเผยข้อมูลและจำกัดสิทธิในการเข้าถึงข้อมูลของบุคคลอื่น ซึ่งกลไกต่างๆเหล่านี้จะทำเพิ่มความสามารถในการป้องกันหรือขัดขวางการเปิดเผยข้อมูลบนเว็บไซต์ฯ มีเทคนิคต่างๆมากมายที่ผู้ทำวิจัยในเรื่องนี้นำมาใช้เป็นแนวคิดในการสร้างกลไกขึ้นมา จุดประสงค์เพื่อลดความเสี่ยงในอันตรายของตัวผู้ใช้งาน ซึ่งความเสี่ยง (risk) เหล่านี้มีได้สามประการคือ ความเสี่ยงด้านความปลอดภัย ความเสี่ยงด้านชื่อเสียงและความน่าเชื่อถือของบุคคล ความเสี่ยงด้านรายละเอียดของข้อมูลส่วนตัว เทคนิคต่างๆสามารถให้คำจำกัดความได้ดังนี้ [30]

- **การจัดการสิทธิในการเข้าถึงและนโยบายความเป็นส่วนตัว (Access Rights and Policy Management)**

เป็นการกำหนดสิทธิการเข้าถึงและการจัดการนโยบาย ซึ่งเกี่ยวข้องการบริหารจัดการสิทธิการเข้าถึงที่เป็นส่วนสำคัญในการป้องกันการเข้าถึงข้อมูลส่วนตัวจากบุคคลภายนอก อีกทั้งยังเป็นการควบคุมการเข้าถึงข้อมูลที่เป็นความลับ ดังนั้นจึงต้องมีการตรวจสอบนโยบายความเป็นส่วนตัวของผู้ใช้ เพื่อหลีกเลี่ยงการรั่วไหลของข้อมูลในขณะที่มีการแบ่งปันทรัพยากรและข้อมูลต่างๆ

- **การจำแนกประเภทข้อมูล (Classification of Resources)**

เป็นการจำแนกประเภทของทรัพยากรข้อมูลที่มีความหลากหลาย เพื่อให้มั่นใจว่าผู้ใช้ที่จะใช้ทรัพยากรร่วมกัน สามารถที่จะป้องกันการรั่วไหลของข้อมูลที่เป็นความลับและจะต้องมีการกำหนดการเข้ารหัสของนโยบายความเป็นส่วนตัว เพื่อให้กลไกการในการจำแนกแหล่งข้อมูลทั้งหมดสามารถใช้ในการจัดหมวดหมู่ทรัพยากรลงในกลุ่มที่แตกต่างกันเช่นภาพ วิดีโอหรือข้อความ

- **การควบคุมการคงอยู่ของข้อมูล (Data Persistence Control)**

การควบคุมการคงอยู่ของข้อมูล คือ ข้อมูลที่ถูกจัดเก็บโดยอัตโนมัติ และข้อมูลนั้นจะถูกเก็บไว้ได้นานในช่วงระยะเวลาหนึ่ง ข้อมูลส่วนบุคคลเป็นข้อมูลที่เป็นความลับ และต้องมีการป้องกันไม่ให้มีการเปิดเผยข้อมูลโดยไม่ได้รับการอนุญาต แต่โดยปกติแล้วข้อมูลอาจจะถูกจัดเก็บในหลายๆ ระบบ โดยแต่ระบบจะมีการทำงานที่เหมือนกัน คือ มีการควบคุมการเผยแพร่ของข้อมูล และมีการควบคุมความคงอยู่ของข้อมูล ซึ่งข้อมูลที่ถูกจัดเก็บไว้นั้นจะมีข้อจำกัดด้านเวลา และมีการกำหนดสิทธิในการเข้าถึง

- **การจำกัดและการอนุญาต (Constraints and Permissions)**

การจำกัดและการอนุญาต เป็นวิธีการที่ใช้ในการควบคุมการเข้าถึงทรัพยากรและการบริการ ผู้ใช้จะส่วนในการกำหนดสิทธิหรือบทบาทในการเข้าถึงข้อมูล โดยการกำหนดพื้นที่ของข้อมูลในการเข้าถึงข้อมูลของแต่ละบุคคลเพื่อป้องกันการรั่วไหลของข้อมูลและป้องกันไม่ให้ผู้ไม่มีสิทธิในข้อมูลนั้นเข้ามาละเมิดความเป็นส่วนตัว

- **การขัดขวางการไหลของข้อมูล (Information Flow Obfuscation)**

การขัดขวางการไหลของข้อมูล เป็นการกำหนดขอบเขตของข้อมูลที่จะสามารถไหลผ่านไปยังระบบหนึ่ง ซึ่งการขัดขวางการไหลของข้อมูลก็เป็นเทคนิคหนึ่งที่ใช้สำหรับป้องกันข้อมูลส่วนบุคคล และข้อมูลที่จะไหลผ่านระบบควรจะมีข้อจำกัดในการเปิดเผยข้อมูล อาจจะใช้กลยุทธ์การเข้ารหัสมาช่วยในการควบคุมการไหลของข้อมูล

- **การเป็นเจ้าของข้อมูล (Ownership of Context Information)**การเป็นเจ้าของของข้อมูล เป็นคุณสมบัติที่ช่วยให้ผู้ใช้ที่เป็นเจ้าของข้อมูลสามารถทำเครื่องหมายในการเปิดใช้งานหรือการเผยแพร่ข้อมูล มีลักษณะที่ช่วยให้เกิดความสัมพันธ์กับพฤติกรรมการเผยแพร่กับบุคคล และช่วยให้ระบบมีความสามารถในการปกป้องข้อมูลโดยการใช้กฎระเบียบที่อยู่บนพื้นฐานของการกำหนดนโยบายของข้อมูลส่วนบุคคล ซึ่งสามารถใช้เป็นรายละเอียดเพิ่มเติมที่ได้รับการพิจารณาในข้อจำกัดเกี่ยวกับสิทธิในการเข้าถึง

- **การป้องกันการเข้าถึงบริการ (Service Access Protection)**

การป้องกันการเข้าถึงบริการ เป็นวิธีการในการควบคุมการรั่วไหลของข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลส่วนตัวในการหลีกเลี่ยงการเปิดเผยข้อมูลด้านการบริการสำหรับผู้ใช้ การป้องกันการเข้าถึงบริการจะใช้ ID ของข้อมูลที่ถูกนำมาให้ในการกำหนดหมายเลยในการป้องกันการเข้าถึงบริการ

- **การป้องกันการเปิดเผยข้อมูล (Information Disclosure Protection)**

เป็นการป้องกันการเปิดเผยข้อมูล โดยมีการกำหนดกลไกที่เป็นนโยบายในการเข้าถึงและการควบคุมข้อมูล เพื่อรักษาและป้องกันการเปิดเผยข้อมูลของผู้ใช้ต่อบุคคลที่ไม่มีสิทธิในการเข้าถึงข้อมูล โดยผู้ที่สามารถเข้าถึงข้อมูลได้จะต้องถูกระบุในการกำหนดสิทธิในการเข้าถึงเท่านั้น

- **การป้องกันการใช้ข้อมูล (Protection of information usage)**

การป้องกันการใช้ข้อมูล คือ ความสามรถในการควบคุมการเผยแพร่ข้อมูล ซึ่งข้อมูลเหล่านี้จะถูกจัดเก็บโดยอัตโนมัติ ผู้ให้บริการจะเป็นเก็บข้อมูลส่วนบุคคล และทำการประมวลผลในการคุ้มครองการเข้าถึงจากบุคคลภายนอกและการใช้ข้อมูลจากผู้ที่ไม่พึงประสงค์

หากขาดเครื่องมือในการป้องกัน ความเป็นส่วนตัวของข้อมูล จะทำให้ข้อมูลเป็นจำนวนมาก เช่น รูปภาพ วีดีโอ ข้อความต่างๆของผู้ใช้งานมีความเสี่ยงที่จะถูกเปิดเผยซึ่งอาจตกอยู่ในมือของผู้ไม่ประสงค์ดี และเป็นอันตรายต่อชีวิตและทรัพย์สินของตัวผู้ใช้งานได้ หลากหลายบทความ [16],[17],[18],[19],[20],[21],[22],[23], [24],[25],[26],[27],[28],[29] ได้เสนอกลไกการทำงานของเครื่องมือป้องกันความเป็นส่วนตัวขึ้นมา ซึ่งมีเทคนิคการทำงานแตกต่างกันไปตามแนวความคิดของผู้ทำการวิจัย ซึ่งสามารถเปรียบเทียบได้ดังตารางที่ 2 และตารางที่ 3 แสดงให้เห็นถึงกลไกการทำงานของการป้องกันความเป็นส่วนตัวของกลไกแต่ละประเภทพร้อมกับจุดเด่นและข้อจำกัดของกลไกแต่ละประเภทนั้น

ตาราง 2 ตารางแสดงการเปรียบเทียบกลไกการป้องกันความเป็นส่วนตัวรูปแบบต่างๆที่มีผู้ศึกษาวิจัยขึ้นมา ตามหัวข้อของคำนิยามเทคนิคการป้องกันความเป็นส่วนตัว

เทคนิค / เปเปอร์	Access rights management (การจัดการสิทธิ์ในการเข้าถึง)	Access policy management (การจัดการนโยบายในการเข้าถึง)	Classification of resources (การจำแนกประเภทข้อมูล)	Data persistence control (การควบคุมการคงอยู่ของข้อมูล)	Constraints and permissions (การจำกัดและการอนุญาต)	Ownership of context (การเป็นเจ้าของข้อมูล)	Obscured information flow (การขัดขวางการไหลของข้อมูล)	Service access protection (การป้องกันการเข้าถึงบริการ)	Information disclosure protection (การป้องกันการเปิดเผยข้อมูล)	Protection of information usage (การป้องกันการใช้ข้อมูล)
UPP: User Privacy Policy for Social Networking Sites[16]	✓	✓	✓		✓	✓	✓			✓
PSNS: Privacy-enhanced Social Networking Site[17]	✓	✓	✓		✓	✓	✓	✓	✓	✓
BBN-Based Privacy Management System[18]			✓		✓		✓	✓	✓	✓
Private Relationships in Social Networks[19]	✓	✓			✓	✓		✓	✓	✓
Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on Social Network Sites[20]					✓	✓	✓		✓	
An Adaptive Privacy Management System for Data Repositories[21]	✓	✓			✓	✓		✓	✓	
FaceCloak: An Architecture for User Privacy on Social Networking Sites[22]	✓	✓			✓		✓	✓	✓	✓
A Collaborative Framework for Privacy Protection in Online Social Networks[23]	✓	✓	✓		✓	✓		✓	✓	✓
Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust[24]	✓	✓			✓			✓	✓	
Privacy Management for Facebook[25]	✓		✓			✓				
FoX: Protecting Users from Malicious Facebook Applications[26]	✓	✓			✓	✓			✓	
PRIMO - Towards Privacy Aware Image Sharing[27]	✓	✓			✓	✓	✓	✓		✓
Privacy preserving social networking through decentralization[28]	✓	✓		✓	✓	✓		✓	✓	
A gossip-based distributed social networking system[29]						✓		✓	✓	✓

จากตารางแสดงการเปรียบเทียบเทคนิคการป้องกันความเป็นส่วนตัวของกลไต่างๆดังกล่าว สามารถอธิบายลักษณะการทำงานของกลไกแต่ละปรเภทได้ดังแสดงใน

ตาราง 3 ตารางแสดงกลไกการทำงานของกลไกการป้องกันความเป็นส่วนตัวแต่ละประเภท

บทความ	กลไกการทำงาน	จุดเด่น	ข้อจำกัด
[16]	กลไกการทำงานของ UPP จะมีการสร้าง policy element ซึ่งเป็นข้อตกลงความเป็นส่วนตัวระหว่างผู้ใช้งานกับผู้ใช้งานอื่น โดยข้อตกลงนี้จะเป็นข้อกำหนดสิทธิ์ในการเข้าถึงข้อมูลส่วนตัว และเป็นข้อตกลงที่ทำระหว่างผู้ใช้งานต่อเพื่อน 1 คน หรือต่อกลุ่ม 1 กลุ่มเท่านั้น	เป็นการตั้งค่าความเป็นส่วนตัวที่ชัดเจนสำหรับเพื่อนแต่ละคน หรือแต่ละกลุ่ม	หากต้องการความเป็นส่วนตัวสูงจะต้องตั้งค่า policy element หลายครั้ง
[17]	กลไกการทำงานของ PSNS ได้ดังนี้ กลไกการทำงนแบ่งได้เป็นสามส่วนคือ Client Privacy manager (CPM), Social Network Site Server Provider (SNS Server), Mail Server 1. SNS Server ส่วน SNS Server Database คือส่วนที่เก็บ ข้อมูลต่างๆที่ส่งมาจาก CPM ของฝั่งผู้ใช้งาน ข้อมูลนั้นอาจเป็นข้อมูลปกติที่ไม่มีการเข้ารหัส หรือข้อมูลที่มีการเข้ารหัส และ Privacy Preference ต่างๆ คือ ฐานข้อมูลการตั้งค่าความเป็นส่วนตัวของข้อมูลนั้นๆ เช่นข้อมูลการตั้งค่าความเป็นส่วนตัวระหว่างเพื่อนร่วมงาน เป็นต้น 2. SNS Server ส่วน SNS Service **คือ**บริการต่างๆที่ เว็บไซต์ เครือข่ายสังคมออนไลน์ให้บริการแก่ผู้ใช้งาน เช่น การค้นหาเพื่อน การเพิ่ม/แก้ไขข้อมูล 3. Server Access Controller เป็นโมดูลที่ผู้วิจัยเพิ่มเติมเข้ามา เพื่อควบคุมการเข้าถึงข้อมูลของ SNS Server จะช่วยจัดการเกี่ยวกับการเข้าถึงข้อมูลของผู้ใช้งานโดยบุคคลอื่น โดย Server access controller จะเก็บการตั้งค่าความเป็นส่วนตัวของข้อมูลที่ผู้ใช้งานตั้งค่าไว้ และจัดการการเข้าถึงข้อมูลให้เป็นไปตามนั้น 4. Client Privacy Manager คือส่วนของปลั๊กอินที่ติดตั้งเพิ่มลงไปในเบราเซอร์ของผู้ใช้งาน แบ่งเป็นส่วนย่อยคือ Encryption/Decryption เป็นส่วนที่ควบคุมการเข้ารหัส และถอดรหัสข้อมูลที่ผู้ใช้งานต้องการให้มีส่วนของการป้องกันความเป็นส่วนตัว ซึ่งข้อมูลที่มีการเข้ารหัสเหล่านี้เมื่อถูกส่งไปเก็บที่ SNS Server จะทำให้ Server ไม่สามารถมองเห็นข้อมูลและนำข้อมูลเหล่านั้นไปใช้งานต่อได้ 5. Client Access Controller เป็นโมดูลที่ช่วยจัดการเกี่ยวกับ ข้อมูลที่ผู้ใช้งานป้อนเข้ามาสู่ SNS ทั้งส่วนของข้อมูลที่ถูกเข้ารหัสและข้อมูลที่ไม่ได้เข้ารหัส โดย Client Access Controller จะแบ่งเป็นสองส่วน คือ Key manager ทำหน้าที่สร้างและจัดเก็บกุญแจที่ใช้สำหรับเข้ารหัสและถอดรหัสข้อมูล รวมถึงจัดส่งกุญแจนั้นไปที่ e-mail address ของบุคคลอื่นๆที่ผู้ใช้งานให้สิทธิในการเข้าดูข้อมูลนั้นๆ จึงโยงไปถึงความข้องเกี่ยวกับ Mail Server (6.) ซึ่งหลักสำคัญคือต้องเป็นอิสระต่อ SNS Server และ Privacy advisor เป็นส่วนที่ช่วยให้คำแนะนำเกี่ยวกับการตั้งค่าระดับความปลอดภัยของข้อมูลให้แก่ผู้ใช้งาน	มีกลไกการควบคุมการเข้าถึงข้อมูลทางฝั่ง server ด้วย คือถึงแม้ข้อมูลจะเก็บที่ server ศูนย์กลางแต่ server ก็ไม่สามารถนำข้อมูลไปใช้ได้เนื่องจากมีการเข้ารหัสข้อมูล	ต้องมีการเข้ารหัสเพื่อดูข้อมูลโดยนำคีย์มาจาก e- mail address ทำให้มีความยุ่งยากของขั้นตอนการเข้าดูข้อมูล และ Mail server กับ Social network site server จะต้องเป็นอิสระต่อกันโดยสิ้นเชิง คือไม่มีการรู้เห็นกัน เนื่องจากกลไกจะมีการฝากคีย์ไว้ที่ Mail server

ตาราง 3 (ต่อ)

บทความ	กลไกการทำงาน	จุดเด่น	ข้อจำกัด
[18]	กลไกการทำงานคือ มีส่วนของ privacy manager : PM เป็นตัวควบคุมสิทธิ์ในการเข้าถึงข้อมูลโดย PM จะพิจารณาจาก Profile Information ที่เข้ามา แล้วจึงจัดการ Profile Zone ซึ่งก็คือสิทธิ์การเข้าถึงข้อมูล โดย PM จะทำงานโดยอาศัยหลักการของ Bayesian Belief Network (BBN)	กำหนดสิทธิ์ในการเข้าถึงข้อมูลโดยใช้ชนิดของข้อมูลเป็นหลัก PI (Profile information)	ชนิดของข้อมูลที่มีมากเกินไปทำให้การกำหนดสิทธิ์มีความสับสนวุ่นวายได้
[19]	เป็นการกำหนดความเป็นส่วนตัวโดยการเข้ารหัส และการถอดรหัส โดยหากผู้ใดต้องการเข้าถึงข้อมูลจะต้องมีใบรับรองความสัมพันธ์ เพื่อขออนุญาตเข้าถึงข้อมูลตามกฎของ AR ซึ่งลักษณะการทำงานคือ ผู้ร้องขอจะส่งคำร้องขอไปยังโหนดกลางเพื่อตรวจสอบว่าใบรับรองความสัมพันธ์สอดคล้องกับการเข้ารหัสหรือไม่ จากนั้นจะมีการคำนวณระดับความน่าเชื่อถือของพวกเขา เมื่อตรวจสอบแล้วว่า ใบรับรองความสัมพันธ์สอดคล้องกับการเข้ารหัสก็จะทำการยืนยันหลักฐานตามกฎของ AR ไปเจ้าของข้อมูล	การเข้ารหัสและการถอดรหัส เพื่อยืนยันการระบุตัวตนในการเข้าถึงข้อมูล ซึ่งเป็นกลไกในการป้องกันการเข้าถึงข้อมูล ประโยชน์หลักของกลไกการนี้คือการบังคับใช้ให้มีการกระจายอำนาจในแง่ของการขยายขีดความสามารถและประสิทธิภาพของการเข้าถึง การควบคุมกลไกในการปกป้องข้อมูลส่วนบุคคลในเครือข่ายทางสังคมโดยใช้วิธีการไม่เปิดเผย	ไม่สามารถเข้าถึงข้อมูลได้ทุกคน ซึ่งประเภทความสัมพันธ์อาจไม่จำเป็นต้องได้รับความคุ้มครองในการเข้าถึงข้อมูล เช่น เพื่อน เพื่อนร่วมงาน โดยในสถานการณ์อื่นๆ เพื่อนอาจจะทำให้เข้าถึงข้อมูลได้ทุกส่วน อาจนำไปสู่การกระจายของข้อมูลส่วนตัวที่ไม่เหมาะสม
[20]	กลไกในการกำหนดการควบคุมการเข้าถึง ในหน้าอินเตอร์เฟซ โดยพยายามที่จะเพิ่มการป้องกันการเข้าถึงและตระหนักถึงความสำคัญของข้อมูลที่ใช้ร่วมกัน โดยการใช้ตัวอย่างที่เป็นรูปธรรม ของการขอข้อมูลการสมัครและการเลือกเพื่อนแบบสุ่ม เพื่อที่จะแสดงให้เห็นว่าข้อมูลของพวกเขาจะยังสามารถเข้าถึงต้นแบบของเรา และช่วยให้ผู้ใช้ จำกัด ข้อมูลที่ไม่ได้ให้ใช้ร่วมกันภายในบริบทของโปรแกรม	ทำให้ผู้ใช้หรือเจ้าของข้อมูลเข้าใจกลไกนี้ได้ง่าย เนื่องจากเป็นการกำหนดและการความคุมการเข้าถึงข้อมูลจากหน้าอินเตอร์เฟซ เพื่อใช้ในการควบคุมและจำกัดการไหลของข้อมูล	กลไกนี้เป็นการกำหนดและควบคุมการเข้าถึง ในหน้าอินเตอร์เฟซ อาจจะทำให้การทำงานยังไม่มีความซับซ้อนมากนัก
[21]	กลไกในการควบคุมการเข้าถึงได้โดยนิติบุคคลมีการกำหนดจุดกำหนดเวลาในกระบวนการของการเปิดเผยคีย์ถอดรหัสจะถูกปรับขึ้นอยู่กับข้อมูลประจำตัวของผู้ร้องขอ สิทธิการเข้าถึงข้อมูลการจัดการข้อมูลส่วนบุคคลบริการเปิดเผยกุญแจถอดรหัสเพื่อร้องขอคีย์การถอดรหัส สามารถเรียกดูโดยผู้ใช้งาน ในกรณีนี้หากข้อมูลที่ไม่สามารถถอดรหัสได้ จะสามารถส่งไปยังหน่วยงานอื่น ๆ ที่อาจมีความสามารถในการเข้าถึงการจัดการบริการส่วนบุคคลที่สามารถให้บริการโดยองค์กร เมื่อมีการติดต่อกับนิติบุคคล จะมีการแจ้งให้ทาง e - mail ทุกครั้งที่คุณใช้บางส่วนของข้อมูลส่วนตัว จะสังเกตเห็นว่านโยบายเหล่านี้ไม่เพียง แต่กำหนดด้านการควบคุมการเข้าถึง แต่นอกจากนี้ยังมีการกระทำในช่วงเวลาการเปิดเผยข้อมูลเช่น การแจ้งเตือนหรือขออนุมัติก่อนการเข้าถึงข้อมูล	ลดความจำเป็นสำหรับคำจำกัดความของตนเพื่อรองรับหลายมุมมองที่แตกต่างกันขึ้นอยู่กับความสามารถใน การเข้าถึงและข้อจำกัด ความเป็นส่วนตัวที่เกี่ยวข้องกับข้อมูลและกำหนดสิ่งที่สามารถเห็นได้ที่ในจุดกำหนดเวลา	ปัญหาที่พบบ่อยสำหรับระบบที่จะต้องบังคับให้ใช้ข้อมูลส่วนบุคคลและในเวลาเดียวกันจะต้อง เปิดเผยข้อมูลที่เป็นความลับ อย่างน้อยจนกว่าจะมีการเปิดเผยข้อมูลครั้งแรกที่เกิดขึ้น จึงอาจจะทำให้การควบคุมการเปิดเผยข้อมูลเป็นไปด้วยความยุ่งยาก และเกี่ยวข้องกับการตรวจสอบในการเปิดเผยข้อมูลการเกิดขึ้นและเพิ่มความรับผิดชอบให้มากขึ้น

ตาราง 3(ต่อ)

บทความ	กลไกการทำงาน	จุดเด่น	ข้อจำกัด
[22]	เป็นกลไกในการป้องกันความเป็นส่วนตัว กล่าวคือ เป็นขั้นตอนการเข้ารหัสและขั้นตอนการถอดรหัสลับ ก่อนที่จะเข้าไปถึงข้อมูลส่วนตัว FaceCloak จะสร้างคีย์หลาย ๆ ชนิดและจัดส่งส่วนย่อยของคีย์เหล่านี้ไปให้เพื่อนของผู้ใช้ในการเข้ารหัสส่วนบุคคลข้อมูล ซึ่ง FaceCloak จะทำการจำลองข้อมูลเสมือนจริงเพื่อตรวจสอบก่อนที่จะมีการเข้าถึงข้อมูลจริง	FaceCloak จะทำการจำลองข้อมูลเพื่อช่วยปกป้องในการเข้าถึงข้อมูล โดยเริ่มต้นด้วยการลงทะเบียนบัญชีเพื่อให้ผู้ใช้ได้รับประโยชน์และสร้างความมั่นใจว่ามีการป้องกันความเป็นส่วนตัวของข้อมูลที่เก็บไว้ในรายละเอียด เช่น ชื่อจริง วันเกิดและออฟไลน์ จะแสดงได้ก็ขึ้นอยู่กับการกำหนดสิทธิในการเข้าถึงของผู้ใช้	FaceCloak ในขณะนี้ได้มีการสนับสนุนเฉพาะการเพิ่มการปกป้องข้อมูลที่เป็นข้อความ ในอนาคตต่อไปจะต้องมีการสำรวจความต้องการในการป้องกันความเป็นส่วนตัวของภาพและวิดีโอ ซึ่งต้องมีการศึกษาเพิ่มเติม
[23]	การป้องกันข้อมูลจากการให้บริการเว็บในการเข้าถึงข้อมูล โดยจะมีการสร้างรูปแบบการทำงานที่มุ่งเน้นในการเข้ารหัสแบบ Group - oriented convergence cryptosystem (GCC) ซึ่งจะมีการดำเนินการตรวจสอบเกี่ยวกับการเข้ารหัส ในการเข้ารหัสแบบจีซีซี ผู้ใช้แต่ละคนในเครือข่ายสังคมออนไลน์จะสร้างคีย์ของผู้ใช้ส่วนตัวและจะมีการลงทะเบียนสาธารณะภายในเครือข่ายสังคมออนไลน์ เพื่อที่จะสร้างเครือข่ายการสร้างคีย์เครือข่ายที่มีลักษณะของการทำงานร่วมมือ คีย์ส่วนตัวของผู้สร้างทั้งหมดเป็นสิ่งที่ถูกต้องและสำคัญในเครือข่ายนี้ สำหรับเพื่อนหรือบุคคลภายนอก ผู้ใช้สามารถสร้างคีย์เอพีเคเพื่อที่จะใช้ในการกำหนดสิทธิ์ในการเข้าถึงข้อมูล การใช้คีย์ส่วนตัวและคีย์ของเครือข่ายของ ผู้ใช้สามารถถอดรหัสหรือสามารถที่จะเข้าถึงข้อมูลที่ใช้ร่วมกันได้ แต่ไม่มีการเข้ารหัส หรือ) ข้อมูลสู่เครือข่าย การดำเ (ไม่มีการเผยแพร่นินการเข้ารหัสที่ไม่สามารถดำเนินการได้ ยกเว้นในกรณีที่ผู้ใช้มีคีย์เครือข่าย	เป็นวิธีการบริหารจัดการในการเข้าถึงข้อมูล โดยที่ไม่ต้องมีผู้คอยจัดการระบบในการกำหนดสิทธิ์ เพื่อป้องกันกลุ่มของผู้ใช้ที่ไม่มีความน่าเชื่อถือ ผู้ใช้จะทำงานร่วมกัน เพื่อจัดการและบำรุงรักษาเครือข่ายส่วนตัว นอกจากนี้ การเข้ารหัสยังสามารถที่จะนำมาใช้ในการแลกเปลี่ยนของกลุ่มคีย์ เพื่อที่สืบทอดการใช้ข้อมูลร่วมกันได้	ผู้ใช้คีย์สาธารณะทุกคนในเครือข่ายที่มีการบริหารจัดการและมีการตรวจสอบด้วยการจัดการเซิร์ฟเวอร์แบบศูนย์กลาง และโมเดลนี้จะมีการใช้งานหลายรูปแบบ ทำให้เกิดปัญหา เช่น ผู้ใช้จะต้องเก็บคีย์เครือข่ายจำนวนมาก ถ้าผู้ใช้นั้นอยู่ในหลายๆ เครือข่าย ไม่มีวิธีที่มีประสิทธิภาพในการเพิกถอนการเป็นสมาชิกแบบชั่วคราวหรือถาวร ไม่มีวิธีการที่มีประสิทธิภาพในการตรวจสอบการระบุชื่อกับมุมมองของการติดตามพฤติกรรมของผู้ใช้
[24]	แบบจำลอง Safebook จะเป็นการจำลองเครือข่ายในการกระจายเครือข่ายในการใช้ข้อมูลร่วมกัน เพื่อป้องกันการละเมิดความเป็นส่วนตัวที่อาจจะเกิดขึ้นกับเซิร์ฟเวอร์ศูนย์กลาง วิธีการการควบคุมการเข้าถึงของ Safebook นี้จะมีอยู่ 3 ส่วน คือ รูปแบบของเครือข่ายสังคมที่มีหลายรูปแบบ มีการวิเคราะห์ความปลอดภัยของภัยคุกคาม และการโจมตีในเครือข่ายสังคมออนไลน์	แนวคิดแบบ Safebook จะมีกลไกต่างๆ เพื่อความเป็นส่วนตัวและมีการรักษาความปลอดภัยความเป็นส่วนตัวรวมอยู่ในแนวคิดนี้ด้วย ซึ่งจะเป็นประโยชน์ในการบริการและการจัดการข้อมูล และฟังก์ชั่นการเก็บรักษาข้อมูลนี้เป็นการออกแบบมาเพื่อคำนึงถึงความเป็นส่วนตัวและประสิทธิภาพในการทำงาน	การออกแบบเครือข่ายนี้ จะมีการเน้นการเชื่อมต่อสื่อสารแบบไม่ระบุชื่อในการเข้ารหัส ซึ่งแนวคิด Safebook นี้ จะมีข้อจำกัดในเรื่องของความล่าช้าในการเข้ารหัสเพื่อที่จะเข้าสู่เครือข่ายสังคมออนไลน์

ตาราง 3 (ต่อ)

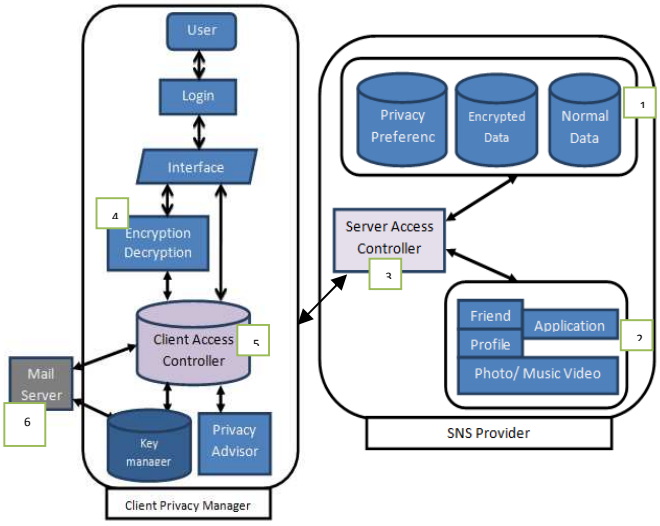
บทความ	กลไกการทำงาน	จุดเด่น	ข้อจำกัด
[25]	กลไกนี้จะใช้วิธีการทางคณิตศาสตร์ในการวิเคราะห์การเปิดเผยข้อมูลของผู้ใช้ ที่พฤติกรรมในการเข้าใช้งานเว็บไซต์เครือข่ายสังคม ซึ่งมีรูปแบบเบื้องต้น คือ การพัฒนาเพื่ออำนวยความสะดวกในกลไกการคุ้มครองข้อมูลส่วนบุคคล ผู้ใช้เฟคบุ๊คจะกำหนดค่าข้อมูลอะไรได้บ้าง ที่สามารถใช้แพลตฟอร์มมาช่วยในการแก้ไข ผู้ใช้สามารถเข้าถึงข้อมูลได้ต้องระบุและกำหนดสิทธิ์ในการเข้าถึงได้ ซึ่งรูปแบบของการป้องกันข้อมูลในการจัดเก็บ โดยจะพัฒนาระบบการป้องกันความเป็นส่วนตัวแบบพีเอสเอส)PSS(ที่จะกำหนดค่าของผู้ใช้โดยการตั้งค่าข้อมูลส่วนตัวบนพื้นฐานของข้อมูลในรายละเอียดของผู้ใช้ จากรูปภาพด้านล่างเป็นรูปแบบของระบบในการจัดการข้อมูลส่วนตัว ระบบจะประกอบไปด้วย ๓ ส่วน คือ ข้อมูลส่วนตัว (PI), ผู้จัดการส่วนตัว)PM) และการแบ่งขอบเขตของโปรไฟล์ (PZ) ข้อมูลส่วนตัว จะประกอบไปด้วยข้อมูล ๒ ชนิด คือ ข้อมูลส่วนบุคคลและสังคม เราจะเลือกข้อมูลส่วนบุคคลเป็นคุณสมบัติหลักของเราที่สามารถแสดงลักษณะของบุคลิกภาพของผู้ใช้และสามารถรับได้ง่ายจากข้อมูลรายละเอียด ในรายละเอียดของการแบ่งขอบเขตของโปรไฟล์จะมีการแบ่งข้อมูลส่วนตัวของผู้ใช้ออกเป็น ๒ ส่วน คือ โซนการดำเนินการอย่างใดอย่างหนึ่งที่สามารถเข้าถึงข้อมูลได้โดยแพลตฟอร์มอื่นๆ ที่โซนพาข้อมูล ซึ่งจะไม่สามารถเข้าถึงข้อมูลได้ โดยการประยุกต์ใช้แพลตฟอร์ม การกำหนดค่าส่วนบุคคลจะเกิดขึ้นในการจัดการความเป็นส่วนตัว	ระบบการจัดการความเป็นส่วนตัวบนเว็บไซต์เครือข่ายสังคม โดยระบบนี้จะทำการแก้ไขปัญหาการเปิดเผยข้อมูลของผู้ใช้ ระบบจะทำการจำกัดการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้ จากการทดลองแสดงให้เห็นว่าวิธีการนี้สามารถป้องกันข้อมูลได้ถึง 75%	รูปแบบของการเก็บข้อมูลส่วนบุคคล ในกรณีที่ผู้ใช้รายใหม่เข้ามาใช้งานในระบบและมีการประยุกต์แพลตฟอร์มเกี่ยวกับข้อมูลรายละเอียดทั้งหมดให้สามารถเข้าถึงได้ทั้งหมดเป็นค่าเริ่มต้นในการเยี่ยมชม โดยที่เขาไม่สามารถรู้ได้เลยว่าข้อมูลส่วนตัวของเขานั้นกำลังถูกโจมตี
[26]	จะมีการเชื่อมต่อการสื่อสารโดยตรงจากเซิร์ฟเวอร์ของ FB เมื่อมีการร้องขอการใช้งานภายในเครือข่าย ซึ่งการเข้าใช้งานนี้จะมีข้อจำกัดในการเข้าถึงข้อมูลของผู้ใช้ที่จะคอยควบคุมการทำงาน โดยจะมีการอ้างอิงค่าการตรวจสอบ คือ ค่าพร็อกซี่ ที่จะแสดงตำแหน่งอยู่ระหว่างโปรแกรมและเซิร์ฟเวอร์ การอ้างอิงค่าพร็อกซี่ในการตรวจสอบนี้จะได้รับความน่าเชื่อถือจากผู้ใช้ และช่วยป้องกันการละเมิดความต้องการของบุคคลภายนอก	วิธีการนี้จะช่วยให้การเข้าถึงข้อมูลมีความชัดเจนมากขึ้น รายละเอียดของข้อมูลที่จะร้องขอผ่าน proxy – client จะช่วยในการควบคุมการเข้าถึงข้อมูลที่สามารถย้อนกลับและเข้ากันได้	
[27]	เป็นการสร้างแนวคิดเพื่อที่จะนำมาวิเคราะห์ความเป็นส่วนตัว ซึ่งในแบบจำลองนี้จะเป็นการออกแบบนโยบายความเป็นส่วนตัวเกี่ยวกับระบบภาพเชิงวัตถุ โดยใช้ PRIMO มาช่วยในการระบุความเป็นส่วนตัวของแต่ละบุคคล โดยจะมีการสร้างดัชนีของภาพที่มีการเข้ารหัสลายเซ็นของภาพ ผู้ใช้สามารถที่จะสร้างบัญชี เพื่อเข้าถึงข้อมูล และจะมีการระบุกฎความเป็นส่วนตัว เพื่อรับอีเมล์ถ้ามีบุคคลมาละเมิดความเป็นส่วนตัว โดย PRIMO จะทำการสแกนดัชนีภาพสำหรับลายเซ็นของรูปภาพนั้น รูปภาพที่ถูกอัพโหลด PRIMO จะทำการตรวจสอบภาพ ให้เป็นไปตามเกณฑ์ของกฎความเป็นส่วนตัวที่ได้กำหนดไว้	กลไกการทำงานแบบ PRIMO นี้จะเป็นกฎความเป็นส่วนตัวในการป้องกันการเปิดเผยข้อมูล โดยเข้ารหัสและเก็บลายเซ็นของภาพ เพื่อใช้ในการควบคุมการเข้าถึงข้อมูล	การแบ่งปันรูปภาพนั้น จะไม่มีการรับประกันในการค้นหารูปภาพที่สูญไปแล้ว

ตาราง 3 (ต่อ)

บทความ	กลไกการทำงาน	จุดเด่น	ข้อจำกัด
[28]	กลไกในการป้องกันการเข้าถึงข้อมูล โดยวิธีของการดักข้อมูลก่อนเข้าถึงข้อมูลจริง ระบบการกระจายอำนาจที่เป็นไปตามเทคนิค แบบ peer – to – peer ข้อความจะถูกส่งต่อโดยการตั้งค่าของเพื่อนคนอื่น ๆ ซึ่งอาจจะมีบางคนที่เป็นอันตราย สิ่งสำคัญที่จะเน้นเป็นพิเศษเกี่ยวกับการเลียนแบบการโจมตี ซึ่งข้อมูลจะถูกซ่อนไม่ให้เห็นจนกว่าจะมีการตรวจสอบควบคุมการเข้าถึง ซึ่งแต่ละบัญชีของสมาชิก SN จะมีการจัดการข้อมูลที่อยู่บนพื้นฐานของความน่าเชื่อถือของบุคคลที่ร้องขอการเข้าถึง	อำนวยความสะดวกในการรักษาความลับของข้อมูลและความเป็นส่วนตัวโดยการกระจายอำนาจ โดยการจำลองข้อมูลของผู้ใช้และความสัมพันธ์ระหว่างเพื่อนและคนรู้จักเพื่อตรวจสอบสิทธิ์ก่อนที่จะเข้าถึงข้อมูล	ให้ทำงานของแบบจำลองข้อมูลและการการเลียนแบบการโจมตี จะมีความยุ่งยากมากขึ้น ถ้าการทำงานแบบนี้มีการใช้งานและการได้รับคำแนะนำถึงช่องโว่ของแบบจำลองข้อมูลในอนาคต ซึ่งระบบนี้ยังไม่สามารถประเมินความสมบูรณ์ของระบบได้
[29]	กลไกในการป้องกันการเข้าถึงข้อมูลโดยอาศัยสถาปัตยกรรมแบบ peer to peer ป้องกันการเข้าถึงข้อมูลจาก social network server โดยการรัน Social Network Site บน peer แทน ป้องกันการรวมข้อมูลต่างๆไว้ที่ server ศูนย์กลาง	ป้องกันการเข้าถึงข้อมูลจาก social network server	ยังไม่มีการกล่าวถึงการป้องกันความเป็นส่วนตัวระหว่างโหนด

จากการศึกษาเทคนิคกลไกการป้องกันความเป็นส่วนตัวแบบต่างๆ พบว่ากลไกแบบ PSNS (PRIVACY ENHANCED SOCIAL NETWORK SITE) มีประสิทธิภาพการป้องกันความเป็นส่วนตัวผู้ใช้งานมากที่สุด และสามารถอธิบายกลไกการป้องกันความเป็นส่วนตัว แบบ PSNS ได้ดังแผนภาพที่ 3 นี้

แผนภาพที่ 3 แสดงสถาปัตยกรรมของกลไกการป้องกันความเป็นส่วนตัวแบบ PSNS [17]

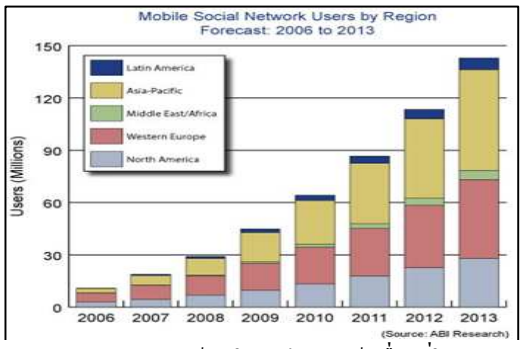


อธิบายกลไกการทำงานของ PSNS ได้ดังนี้ กลไกการทำงนแบ่งได้เป็นสามส่วน คือ Client Privacy manager (CPM), Social Network Site Server Provider (SNS Server), Mail Server

1. SNS Server ส่วน SNS Server Database คือส่วนที่เก็บข้อมูลต่างๆที่ส่งมาจาก CPM ของฝั่งผู้ใช้งาน ข้อมูลนั้นอาจเป็นข้อมูลปกติที่ไม่มีการเข้ารหัส หรือข้อมูลที่มีการเข้ารหัส และ Privacy Preference ต่างๆ คือ ฐานข้อมูลการตั้งค่าความเป็นส่วนตัวของข้อมูลนั้นๆ เช่นข้อมูลการตั้งค่าความเป็นส่วนตัวระหว่างเพื่อนร่วมงาน เป็นต้น
2. SNS Server ส่วน SNS Service **คือ**บริการต่างๆที่ เว็บไซต์เครือข่ายสังคมออนไลน์ให้บริการแก่ผู้ใช้งาน เช่น การค้นหาเพื่อน การเพิ่ม/แก้ไขข้อมูล
3. Server Access Controller เป็นโมดูลที่ผู้วิจัยเพิ่มเติมเข้ามาเพื่อควบคุมการเข้าถึงข้อมูลของ SNS Server จะช่วยจัดการเกี่ยวกับการเข้าถึงข้อมูลของผู้ใช้งานโดยบุคคลอื่น โดย Server access controller จะเก็บการตั้งค่าความเป็นส่วนตัวของข้อมูลที่ผู้ใช้งานตั้งค่าไว้ (Appendix1) และจัดการการเข้าถึงข้อมูลให้เป็นไปตามนั้น
4. Client Privacy Manager คือส่วนของปลั๊กอินที่ติดตั้งเพิ่มลงไปในเบราเซอร์ของผู้ใช้งาน แบ่งเป็นส่วนย่อยคือ Encryption/Decryption เป็นส่วนที่ควบคุมการเข้ารหัส และถอดรหัสข้อมูลที่ผู้ใช้งานต้องการให้มีส่วนของการป้องกันความเป็นส่วนตัว ซึ่งข้อมูลที่มีการเข้ารหัสเหล่านี้เมื่อถูกส่งไปเก็บที่ SNS Server จะทำให้ Server ไม่สามารถมองเห็นข้อมูลและนำข้อมูลเหล่านั้นไปใช้งานต่อได้
5. Client Access Controller เป็นโมดูลที่ช่วยจัดการเกี่ยวกับข้อมูลที่ผู้ใช้งานป้อนเข้ามาสู่ SNS ทั้งส่วนของข้อมูลที่ถูกเข้ารหัสและข้อมูลที่ไม่ได้เข้ารหัส โดย Client Access Controller จะแบ่งเป็นสองส่วนคือ Key manager ทำหน้าที่สร้างและจัดเก็บกุญแจที่ใช้สำหรับเข้ารหัสและถอดรหัสข้อมูล รวมถึงจัดส่งกุญแจนั้นไปที่ e-mail address ของบุคคลอื่นๆที่ผู้ใช้งานให้สิทธิในการเข้าดูข้อมูลนั้นๆ จึงโยงไปถึงความข้องเกี่ยวกับ Mail Server (6.) ซึ่งหลักสำคัญคือต้องเป็นอิสระต่อ SNS Server และ Privacy advisor เป็นส่วนที่ช่วยให้คำแนะนำเกี่ยวกับการตั้งค่าระดับความปลอดภัยของข้อมูลให้แก่ผู้ใช้งาน

IV. MOBILE SOCIAL NETWORK

ในช่วงเวลา 2-5 ปีที่กำลังมาถึงนี้ ถือว่าเป็นจุดเปลี่ยน ของอุตสาหกรรมโทรคมนาคมที่สำคัญยิ่ง ทั้งนี้เนื่องจากระบบโทรศัพท์เคลื่อนที่และเครือข่ายอินเทอร์เน็ตมีการหลอมรวมกัน (Convergence) อย่างเห็นได้ชัดเจนขึ้นเป็นลำดับ โดยมีการคาดการณ์ว่า ในอนาคตโทรศัพท์เคลื่อนที่จะเติบโตควบคู่ไปกับการใช้บริการ Content บนอินเทอร์เน็ต โดยเฉพาะเทคโนโลยีของ Web3.0 และพฤติกรรมการใช้งานของผู้บริโภคในยุค Net Generation จะทำให้เป็นแรงผลักดันให้อุตสาหกรรมโทรศัพท์เคลื่อนที่ สร้างอุปกรณ์ที่สามารถสนับสนุนการใช้งานในด้าน Mobile Social Network มากขึ้น ประกอบทั้งการขับเคลื่อนของแนวคิด Ubiquitous network ของอุตสาหกรรมโทรคมนาคม ก็ยิ่งทำให้ทิศทางของอุตสาหกรรมโทรศัพท์เคลื่อนที่มุ่งสู่การสร้าง Application ที่เกี่ยวข้องกับ Mobile Social Network อย่างหลีกเลี่ยงไม่ได้ และมีการคาดการณ์จากกลุ่มวิจัย ABI Research[32] ว่า กลุ่มผู้ใช้โทรศัพท์เคลื่อนที่ในอนาคตจะมีการใช้งานโทรศัพท์เคลื่อนที่ ที่มีลักษณะ Global, Interactive และ Dynamic มากขึ้น จนอาจทำให้ตัวแบบธุรกิจในอุตสาหกรรมอื่นที่เชื่อมโยงกับธุรกิจโทรศัพท์เคลื่อนที่เปลี่ยนไปอย่างรวดเร็ว (รูปต่อไปแสดงการพยากรณ์การใช้งานโทรศัพท์เคลื่อนที่ในลักษณะเครือข่ายสังคม (Mobile Social Network) ในช่วงปี 2008-2013 ของกลุ่มวิจัย ABI Research)



รูป 3 แสดง การพยากรณ์การใช้งานโทรศัพท์เคลื่อนที่ในลักษณะเครือข่ายสังคม (Mobile Social network) ในช่วงปี 2008-2013 [33]

จากการเชื่อมโยงผู้คนทั่วโลกในลักษณะเครือข่ายสังคมบนโลกอินเทอร์เน็ต จึงทำให้การพัฒนาเทคโนโลยี IP Multimedia Subsystem (IMS) และ Voice-over-IP เป็นไปด้วยความรวดเร็ว เพื่อรองรับการให้บริการโทรศัพท์เคลื่อนที่ทุกรูปแบบผ่านเครือข่ายอินเทอร์เน็ต เพื่อรองรับการเชื่อมต่อระหว่างเครือข่ายโทรศัพท์เคลื่อนที่และเครือข่ายอินเทอร์เน็ตความเร็วสูง ซึ่งสามารถให้บริการ Multimedia ต่างๆได้จากโทรศัพท์เคลื่อนที่ โดยอยู่บนพื้นฐานของการส่งข้อมูลบนเครือข่ายบนมาตรฐาน Internet Protocol (IP) ที่สามารถใช้บริการการเชื่อมโยงผู้คนทั่วโลกด้วยค่าบริการราคาถูกที่เท่ากับการใช้บริการการสื่อสารบนอินเทอร์เน็ต

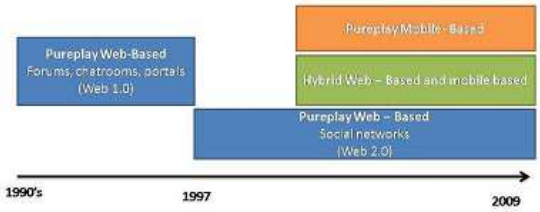
เทคโนโลยี IMS จะทำให้การให้บริการโทรศัพท์เคลื่อนที่ในอนาคตมีบริการที่หลากหลายและทรงพลัง เช่น บริการ Face-to-Face Communication (Presence), บริการระบุสถานที่ตั้งต่างๆ (Location Based Services) และ บริการเครือข่ายสังคมแบบเคลื่อนที่ (Mobile Social Network) เป็นต้น ซึ่งเป็นการให้บริการแบบ Real time ส่วนบุคคล เป็นการสร้างความพึงพอใจให้กับผู้ใช้บริการมากขึ้น และช่วยยกระดับคุณภาพชีวิตของผู้ใช้บริการ ตัวอย่างเช่น บริการแสดงภาพเคลื่อนไหวขณะใช้งาน (Presence) ทำให้เราสามารถมองเห็นเพื่อนหรือกลุ่มคนที่เราต้องการจะติดต่อ ไม่ว่าจะอยู่ในส่วนใดของโลก จุดพลิกผันที่สำคัญในอนาคตคือการให้บริการของโทรศัพท์เคลื่อนที่ที่สามารถให้บริการ การประชุมทางโทรศัพท์แบบเห็นหน้า (Video conference) จากจุดต่อจุด (point to point) ไปสู่การให้บริการหลายๆจุด (Multipoint) โดยการประชุมทางโทรศัพท์ดังกล่าว จำเป็นต้องใช้บริการสะพานเชื่อมต่อของ IMS เพื่อที่จะเชื่อมต่อการทำ Video call จากหลายจุดเข้าด้วยกัน โดยการเชื่อมต่อการประชุมนั้น จะไม่มีอุปสรรคในด้านความแตกต่างของโครงข่ายและอุปกรณ์ที่ใช้ในการเชื่อมต่อ (Client device) อีกต่อไป และการเชื่อมต่อดังกล่าวก็จะทำการส่งผ่านโครงข่าย IP ดังนั้น ผู้ใช้บริการสามารถใช้บริการ Video conference ได้จากหลายเทคโนโลยีที่สามารถเชื่อมต่อกับอินเทอร์เน็ต โดยเฉพาะอย่างยิ่ง Mobile Broadband Internet นั่นเอง

ซึ่งโดยความหมายของเว็บไซต์เครือข่ายสังคมขึ้นอยู่กับ [35] ประการแรกเป็นบริการ webbased ที่ช่วยให้บุคคลที่จะสร้างรายละเอียดสาธารณะหรือ semipublic ภายในระบบ ประการที่สองเป็นที่จัดการกับรายชื่อของผู้อื่นที่การเชื่อมโยงร่วมกัน และประการที่สามเป็นไปได้เพื่อดูและสำรวจรายการของการเชื่อมต่อ

เครือข่ายทางสังคมให้ความหลากหลายของกลไกสำหรับให้ผู้ใช้แบ่งปันข้อมูลกับผู้อื่น ยังมีความสามารถในการค้นหาสำหรับผู้ใช้ที่มีความสนใจคล้ายกันและการสร้างการรักษาสื่อสารระหว่างพวกผู้ใช้ [34] เครือข่ายสังคมออนไลน์ได้กลายเป็นที่นิยมมากในช่วงในไม่กี่ปีนี้ล่าสุด ตัวอย่างเช่น Facebook ได้กว่า 150 ล้านคนในเดือนกุมภาพันธ์ 2009 [37]

ต้นกำเนิดของเครือข่ายทางสังคมอยู่ในช่วงต้นปี 1990 วิธีง่ายๆในการติดต่อสื่อสารระหว่างผู้คนผ่านทางอินเทอร์เน็ตเช่น กระทู้สนทนา, สมาคมวิชาชีพหรือสถานที่อื่น ๆ ที่ผู้คนสามารถแลกเปลี่ยนความคิด เทคโนโลยีอินเทอร์เน็ตร่วมกับการพัฒนาซอฟต์แวร์เพื่อสังคม เกิดมีการใช้เนื้อหาร่วมกันเป็นชุมชนอินเทอร์เน็ต การให้ที่จุดเริ่มต้นที่เว็บไซต์เครือข่ายสังคมแรกที่เปิดตัวในปี 1997 คือ SixDegrees.com [35]

เครือข่ายทางสังคมเป็นส่วนหนึ่งของกระบวนการพัฒนาเว็บ 2.0 ของอินเทอร์เน็ต ซึ่งเกิดการระดมความคิดการประชุมนานาชาติ ระหว่าง O'Reilly และ MediaLive พวกเขาตั้งข้อสังเกตว่าเป็นเว็บที่สำคัญมากกว่าที่เคยและมีจำนวนมากโปรแกรมใหม่ ๆ และเว็บไซต์ที่จะปรากฏทุกวัน แนวคิดกลางที่อยู่เบื้องหลัง Web 2.0 คือ การแก้ปัญหาร่วมร่วมกัน ใช้ข้อมูลร่วมกัน [40]



รูปที่ 4 วิวัฒนาการของพื้นฐานเครือข่ายสังคม [42]

เทคโนโลยีที่ยังคงพัฒนาและความพร้อมของซอฟต์แวร์เพื่อสังคม โดยปัจจุบันโทรศัพท์เคลื่อนที่หรืออุปกรณ์เคลื่อนที่อื่น ๆ เป็นสิ่งนิยมใช้มากที่สุด และส่วนใหญ่ทั้งหมดโทรศัพท์เคลื่อนที่ใหม่ที่มีความสามารถเชื่อมต่ออินเทอร์เน็ต

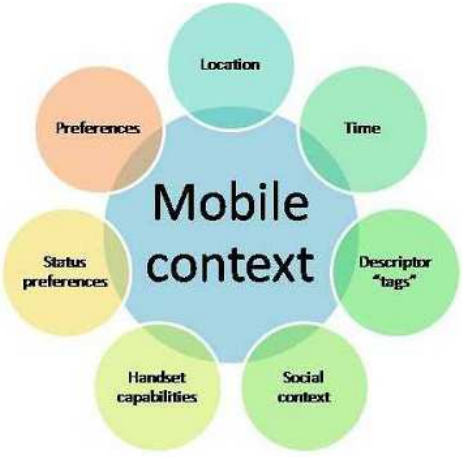
Mobile 2.0 เป็นชื่อที่กำหนดในการถ่ายโอนทั้งหมด แนวโน้มในปัจจุบันของ Web 2.0 อุปกรณ์เคลื่อนที่ [38] มีความคล่องตัวมากขึ้น ปัจจุบันมีผู้ใช้มากขึ้นกว่าโทรศัพท์เคลื่อนที่ผู้ใช้อินเทอร์เน็ต นอกจากนี้โทรศัพท์เคลื่อนที่เป็นอุปกรณ์ส่วนบุคคลที่จะไปที่ใดก็ตามที่เป็นเจ้าของไป เป็นผลให้ความสามารถการให้ข้อมูลจำนวนมากเกี่ยวกับสภาพแวดล้อมของผู้ใช้ ตัวอย่างเช่น เพลงที่ฟัง, ภาพที่ถ่าย ฯลฯ

ปัจจุบันส่วนใหญ่ของแนวทางการเครือข่ายสังคมเคลื่อนที่จะขยายส่วนติดต่อผู้ใช้เพื่อให้พวกเขาสามารถที่จะทำงานในอุปกรณ์ แต่การเปลี่ยนแปลงที่เป็นพื้นฐานที่จะขยายซอฟแวร์ที่ใช้ข้อมูลทั้งหมดที่โทรศัพท์เคลื่อนที่ให้ คุณสมบัติเหล่านี้ให้มากของรายละเอียดของเนื้อหาที่ใช้ร่วมกันผู้ใช้ในเครือข่ายทางสังคม ตัวอย่างเช่นผู้ใช้สามารถอัพโหลดภาพและระบบอัตโนมัติที่ภาพในแผนที่ [38]

จุดมุ่งหมายของหลายงานวิจัยนี้คือเพื่อให้การแนะนำเกี่ยวกับเครือข่ายสังคมเคลื่อนที่คุณสมบัติที่พวกเขาร่วมกับเครื่องคอมพิวเตอร์ทั่วไป ตามเครือข่ายทางสังคมและความแตกต่างอุปกรณ์ที่ใช้ในการสื่อสาร นอกจากนี้ในบทความที่ได้ศึกษาสถาปัตยกรรมบางแนวคิดเกี่ยวกับความเป็นส่วนตัวและการรักษาความปลอดภัย

คุณสมบัติที่เกี่ยวข้องของเครือข่ายสังคมโทรศัพท์เคลื่อนที่

โดยทั่วไปเครือข่ายสังคมโทรศัพท์เคลื่อนที่ จะแตกต่างจากเครือข่ายทางสังคมออนไลน์ที่ใช้ผ่านทางเครื่องคอมพิวเตอร์ทั่วไป เพราะคุณสมบัติเพิ่มเติมบางอย่างเช่น เนื้อหาของข้อมูลเชิงบริบท



รูปที่ 5 พื้นฐานบริบทของโทรศัพท์เคลื่อนที่ [38]

ดังแสดงในรูปที่ 2 บริบทของโทรศัพท์เคลื่อนที่สามารถสร้างขึ้นโดยวิธีการให้ของข้อมูล เช่น สถานที่ตั้งของอุปกรณ์โทรศัพท์เคลื่อนที่, เวลา, แท็ก (Tag) ที่อธิบายสภาพแวดล้อมที่ข้อมูลจากอุปกรณ์อื่น ๆ ซึ่งมีความสามารถบางอย่างที่โทรศัพท์เคลื่อนที่ สามารถตั้งค่าบางอย่างโดยผู้ใช้งาน

1) การให้ตำแหน่ง

การทราบถึงตำแหน่งของผู้ใช้สถานที่ ตามคุณลักษณะการวางตำแหน่งซึ่งเป็นหนึ่งในความแตกต่างระหว่างเครื่องคอมพิวเตอร์ทั่วไปและโทรศัพท์เคลื่อนที่ซึ่งแตกต่างกับความสามารถของโทรศัพท์เคลื่อนที่ในอดีต

ตัวอย่างเช่น [38] ชี้ให้เห็นว่าเป็นไปได้ที่จะทำให้รายการของสถานที่เข้าชมมากที่สุดหรือสถานที่ที่ชื่นชอบ ข้อมูลนี้สามารถรวบรวมได้จากโทรศัพท์เคลื่อนที่สถานที่เข้าชมมากที่สุดที่สามารถยกตัวอย่าง เช่น ร้านกาแฟที่ผู้ใช้ที่มักจะเข้าชมในตอนเช้าที่โรงเรียนหรือทำงาน ผับที่ไปเมื่อวันหยุดสุดสัปดาห์ อีกตัวอย่างหนึ่งคือการแปลโดยอัตโนมัติจากภาพถ่าย ดังนั้นผู้ใช้จะใช้เวลาถ่ายภาพด้วยโทรศัพท์เคลื่อนที่ของเขาและโดย เมื่อถ่ายภาพโปรแกรมบนโทรศัพท์จะกำกับแท็ก สถานที่ของภาพถ่ายบนแผนที่ โดยทราบว่าตำแหน่งที่แน่นอนของผู้ใช้เครือข่ายสังคมเคลื่อนที่สามารถให้บริการจำนวนมากคุณลักษณะที่น่าสนใจ

2) เพื่อนค้นหาเพื่อน

เพื่อนค้นหาเพื่อน เป็นอีกหนึ่งคุณลักษณะที่น่าสนใจที่ [38] ซึ่งในบทความนี้กล่าถึงการหาคุณลักษณะของเพื่อน นอกจากนี้ยังเป็นวิธีการที่คล้ายกันคือการอธิบายไว้ใน [34] และ [39] แนวคิดของแต่ละบทความทั้งหมดที่มีความสามารถหาเพื่อนที่อยู่ในสถานที่เดียวกันกับที่ผู้ใช้ ซึ่งเป็นการจำลองสถานการณ์เช่นนี้ ถ้าผู้ใช้อยู่ในที่สามารถเชื่อมต่อกับเครือข่ายสังคมเคลื่อนที่โดยความหมายของเทคโนโลยีเคลื่อนที่เช่น Bluetooth, ผ่านการที่เขาสามารถเรียกดูข้อมูลของทุกคนในสถานที่เชื่อมต่อไปยัง เครือข่ายทางสังคมเช่นเดียวกัน เป็นผลให้เขาถ้าเขาต้องการให้พวกเขาสามารถส่งข้อความหรือตรวจสอบรายละเอียดของใครบางคน คุณลักษณะนี้อาจเป็นที่น่าสนใจมากเพราะความสามารถในการรู้ว่าทุกคนที่อยู่ในสถานที่เดียวกันเป็นที่ดึงดูดจริงๆสำหรับผู้ใช้

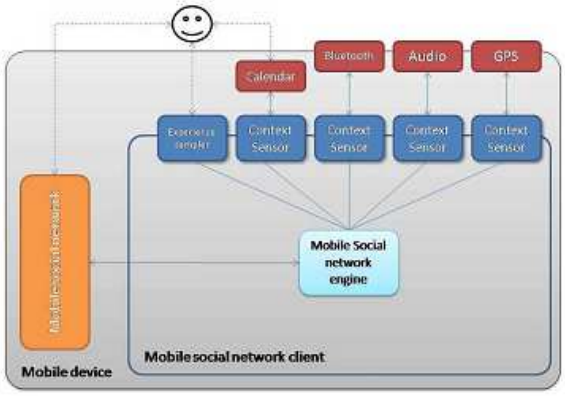
3) การจับภาพและสื่อแท็ก

คุณลักษณะนี้คือการใช้ข้อมูลตามบริบทเพื่อให้แท็กที่กำหนดไว้ล่วงหน้า / ที่ใช้กันทั่วไปตามสถานที่ตั้งและความใกล้ชิดกับผู้ใช้อื่นหรือสถานที่
ตัวอย่างเช่น ลักษณะภาพที่ใกล้เคียงกันจากผู้ใช้คนอื่นๆ จะนำมาแสดงที่ตำแหน่งหรือสถานที่ใกล้เคียงกัน โดยโทรศัพท์เคลื่อนที่ที่แท็กโดยอัตโนมัติเพื่อนในภาพและตั้งอยู่ใน [38] แผนที่

4) สถานะ การปรับปรุงส่วนบุคคล
แนวคิดสำคัญที่อยู่เบื้องหลังคุณลักษณะสถานะ การปรับปรุงส่วนบุคคลที่สถานะส่วนบุคคลสามารถได้รับการปรับปรุงโดยอัตโนมัติด้วยข้อมูลตามบริบท [38] ตัวอย่างเช่นที่ผู้ใช้คือสิ่งที่เขาเป็นเพลงที่ฟังสถานะของอุปกรณ์เคลื่อนที่ (ตัวอย่างเช่นในการประชุมรัฐ) ฯลฯ ข้อมูลเหล่านี้ทั้งหมดรวมกันให้ข้อมูลจำนวนมากที่ช่วยให้ซอฟต์แวร์ระบบเครือข่ายเคลื่อนที่ปรับปรุงโดยอัตโนมัติสถานะของ [38] ผู้ใช้

5) ดำเนินการส่งแบบไม่ประสานเวลา
ปฏิสัมพันธ์ไม่ตรงกันเกี่ยวกับการคุณสมบัติอื่น ๆ ของโทรศัพท์เคลื่อนที่เช่นความสามารถในการส่ง SMS หรืออีเมล คุณลักษณะนี้ช่วยให้ผู้ใช้สามารถส่งชนิดอื่น ๆ ของข้อความไปยังคนที่เชื่อมต่อกับ [38] เครือข่าย

6) การโฆษณา
อุปกรณ์เคลื่อนที่ที่มีศักยภาพในการโฆษณามหาศาล นอกจากเป็นที่นิยมอย่างมาก สามารถใช้งานได้ตลอดเวลาซึ่งช่วยให้การโฆษณาต่อบุคคล [36] มีการผลิตสื่อเฉพาะบุคคล ในการติดต่อสื่อสาร แม้ข้อดีของโทรศัพท์เคลื่อนที่มีหลายอย่าง แต่ยังมีข้อจำกัดของสื่อโฆษณา เช่น สแปม, ข้อจำกัดของอินเทอร์เฟสโทรศัพท์เคลื่อนที่, การละเมิดสิทธิส่วนบุคคลและค่าใช้จ่ายที่เกิดขึ้นจากสื่อมัลติมีเดีย



รูปที่ 6 ตัวอย่างโครงสร้างสถาปัตยกรรมที่เป็นไปได้ [38]

สถาปัตยกรรมบางส่วนของเครือข่ายสังคมเคลื่อนที่

การออกแบบสถาปัตยกรรมที่อยู่เบื้องหลังความต้องการของลูกค้าที่ใช้เครือข่ายโทรศัพท์เคลื่อนที่ทางสังคมกับการทำงาน ซึ่งมีเว็บเบราเซอร์เป็นส่วนประกอบที่สามารถจัดการกับข้อมูลทั้งหมดที่บริบทเป็นสิ่งจำเป็น
รายละเอียดในรูปที่ 3 เป็นหนึ่งในการออกแบบที่เป็นไปได้ของสถาปัตยกรรมสำหรับอุปกรณ์สำหรับเครือข่ายสังคม มีองค์ประกอบบางประการที่เป็น บลูทู ธ, เสียง, GPS, ฯลฯ ที่เป็นส่วนของอุปกรณ์เคลื่อนที่ และการติดต่อกับสภาพแวดล้อมของผู้ใช้ มีโปรแกรมอื่น ๆ เพิ่มเติม เช่น ปฏิทินช่วยในการวางแผนกิจกรรมในวันต่าง โดยข้อมูลทั้งหมดที่รวบรวมและประมวลผลโดยเครื่องมือเครือข่ายโทรศัพท์เคลื่อนที่ทางสังคมที่อยู่ในโทรศัพท์เคลื่อนที่ [38]

1) ไฮบริดหรือโทรศัพท์เคลื่อนที่ได้อย่างหมดจด
ความเป็นไปได้สำหรับเครือข่ายสังคมเคลื่อนที่ เป็นเครือข่ายสังคมเคลื่อนที่ได้อย่างหมดจดจะเป็นผู้ที่ได้รับการออกแบบจากช่วงเวลาก่อนที่จะใช้ในโทรศัพท์เคลื่อนที่ โดยที่เป็นหนึ่งในไฮบริดเป็นสิ่งหนึ่งที่แรกที่ถูกออกแบบมาเพื่อทำงานในแพลตฟอร์ม webbased แล้วคุณสมบัติของพวกเขาย้ายไปยังแพลตฟอร์มโทรศัพท์เคลื่อนที่ [41]

2) ซอฟท์แวร์ไคล้เอ็นท์หรือ www ของโทรศัพท์เคลื่อนที่
เป็นลักษณะสำคัญของเครือข่ายสังคมเคลื่อนที่เป็นวิธีที่จะได้รับการออกแบบ มีสองวิธีแตกต่างกันคือ webbased และซอฟต์แวร์ในลูกค้าที่มีและผลที่ได้รับจะแตกต่างกันมาก หากมีซอฟต์แวร์ที่ติดตั้งในโทรศัพท์เคลื่อนที่บางเครือข่ายสังคมเคลื่อนที่จะสามารถได้รับข้อมูลตามบริบทมากขึ้นจากโทรศัพท์เคลื่อนที่กว่าจะเครือข่ายสังคมที่เพียงแค่ webbased แต่วิธีนี้ยังสิ้นเปลืองทรัพยากรมากขึ้นและลูกค้าจะต้องมีการพัฒนามากของแพลตฟอร์มโทรศัพท์เคลื่อนที่ที่แตกต่างกัน

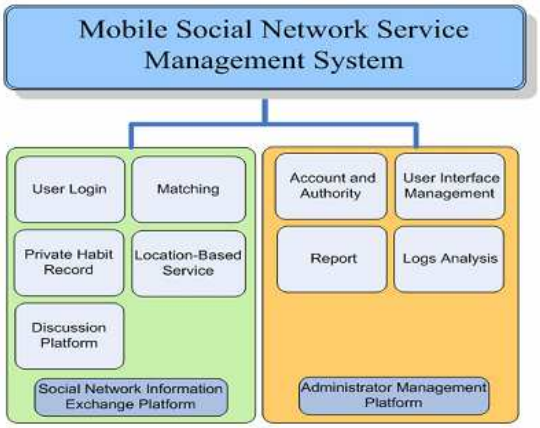
3) ข้อจำกัด
ปัจจุบันมีข้อจำกัดบางอย่างบนโทรศัพท์เคลื่อนที่และแพลตฟอร์ม ข้อจำกัดด้านอุปกรณ์ที่อยู่กับเครื่องโทรศัพท์ที่ยังไม่อำนวยความสะดวกในการสื่อสาร ซึ่งในอนาคตอันใกล้มากที่สุดของโทรศัพท์เคลื่อนที่จะมีกล้อง, GPS และอุปกรณ์อื่น ๆ และการประยุกต์ใช้ที่จะช่วยให้การป้อนข้อมูลความตระหนักในบริบทของเครือข่ายสังคมโทรศัพท์เคลื่อนที่
ข้อจำกัด อีกประการหนึ่งที่สำคัญของโทรศัพท์เคลื่อนที่คือการใช้ทรัพยากรเช่นแบนด์วิดธ์เวลาการประมวลผลหน่วยความจำและพลังงาน ทรัพยากรเหล่านี้จำกัดมากขึ้น ในสภาพแวดล้อมที่โทรศัพท์เคลื่อนที่กว่าในเครื่องคอมพิวเตอร์อย่างใดอย่างหนึ่ง ดังนั้นจึงเป็นสิ่งสำคัญในการออกแบบสถาปัตยกรรมที่มีวัตถุประสงค์ในการที่จะช่วยให้ประสิทธิภาพของการใช้ทรัพยากรเหล่านี้

4) ข้อมูลส่วนบุคคลและการรักษาความปลอดภัย
นโยบายความเป็นส่วนตัวและความปลอดภัยเป็นสองแนวคิดที่สำคัญในเครือข่ายทางสังคม ทุกอย่างต้องทำด้วยการยอมรับของผู้ใช้ซึ่งข้อมูลที่ควรจะภาครัฐและเอกชนที่ ในความเป็นส่วนตัวของระบบเครือข่ายโทรศัพท์เคลื่อนที่สังคมและการรักษาความปลอดภัยส่วนประกอบที่สำคัญของการสมัครเป็นเนื่องจากข้อมูลตามบริบทสามารถค้นพบข้อมูลเวลาจริงของผู้ใช้นี้สามารถสร้างข้อมูลที่ผู้ใช้อาจคิดว่าเป็นล่วงล้ำหรือไม่ถูกต้อง ตัวอย่างเช่นตำแหน่งของผู้ใช้

เป็นสิ่งที่ควรจะแสดงที่มีจำนวนมากของความเป็นส่วนตัวคือไม่สำหรับทุกคนที่ดู [38]

บทความและทฤษฎีที่เกี่ยวข้อง

1 Mobile Social Network Services for Families With Children With Developmental Disabilities [43] โดยในบทความนี้กล่าวถึงการออกแบบเทคโนโลยีเพื่อนำการสื่อสารโทรศัพท์เคลื่อนที่แบบไร้สายไปใช้ประโยชน์ด้านการให้บริการ location services และ เทคโนโลยีการค้นหาที่พยายามค้นหาความสัมพันธ์ของครอบครัวที่เกี่ยวข้องกันอย่างมีประสิทธิภาพ บนพื้นฐานการควบคุมการสืบค้นจากผู้แนะนำ ในบทความนี้ได้อธิบายถึง platform สำหรับการติดต่อสื่อสารที่ราบรื่นระหว่างผู้เชี่ยวชาญด้านการติดต่อสื่อสารและครอบครัวของเด็กที่มีความพิการ children with developmental disabilities (CDD) [43] โดยในบทความนี้มีผลกระทบกับการสื่อสารการบริการเครือข่ายสังคมบนโทรศัพท์เคลื่อนที่ mobile social network services (MSNS) และการฝึกอบรมของการดำเนินการเหล่านี้ เพื่อเป็นโอกาสในการสร้างปฏิสัมพันธ์กับครัวครัว CCD เหล่านี้ โดยหลักเกณฑ์ การจัดการการให้บริการเครือข่ายสังคมโทรศัพท์เคลื่อน Mobile social network service management (MSNSM) [43] ในการพัฒนาและจัดการบนพื้นฐานโครงสร้างสถาปัตยกรรมเครือข่ายเครือข่าย



รูปที่ 7 หลักเกณฑ์ของระบบ MSNSM [43]

โดยลักษณะการทำงานของระบบ CCD มีดังนี้

1) จับคู่อาสาสมัคร: โดยมีรายการของตารางอาสาสมัครและหมวดหมู่การบริการมีให้สำหรับผู้ปกครองที่มี CDD เพื่อเลือกเวลาที่เหมาะและรูปแบบของการบริการ

2) สร้างฐานข้อมูลเก็บลักษณะพฤติกรรมของ CDD : โดยใช้ข้อมูลจากรายงานของอาสาสมัครที่ดูแล CCD

3) ความไว้วางใจและความเชื่อมั่น: ระบบจะมีการติดตั้งโปรโตคอล AAA, และฝึกอบรมอาสาสมัครโดยผู้เชี่ยวชาญ

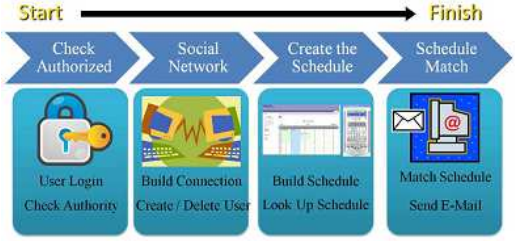
4) การร้องขอให้ดูแลเด็กอย่างประจำสม่ำเสมอ โดยผู้ปกครองสามารถขอร้องให้อาสาสมัครดูบริการดูแลเด็กและทำงานผ่านระบบ CDD นี้

5) การค้นหาและการจับคู่ของงาน: ครอบครัวที่มี CDD พึ่งพาระบบนี้ในการหางานเป็นเจ้าหน้าที่ของมูลนิธิ

6) ปรึกษาแพลตฟอร์ม: ผู้ใช้งานระบบนี้จะแลกเปลี่ยนข้อมูลดังกล่าวเป็นการให้คำปรึกษาเช่น ยา, กฎหมาย, การศึกษาและจิตวิทยาหรือ, กับแต่ละอื่น ๆ

7) สถานที่ทำงานจะช่วยให้เป็นส่วนหนึ่งกับ CDD ในการหาอาสาสมัครที่ใกล้ที่สุดหรือการสูญเสียเด็ก

8) หลักการการวางแผนของระบบการจัดการในเบื้องหลังระบบ: หน้าที่การบริหารจะต้องมีอินเตอร์เฟซผู้ใช้แบบกราฟิก, การจัดการและรับรองความถูกต้องของบัญชีรายชื่อ, การรักษาความปลอดภัยเครือข่ายและระบบการบันทึกเหตุการณ์



รูปที่ 8 หลักเกณฑ์หาความสัมพันธ์ (matching) [43]

หลักการทำงานของระบบ MSNSM ดังรูปที่ 7 มีการทำงานดังต่อไปนี้

1) โมดูลเข้าสู่ระบบผู้ใช้ : ผู้ใช้จะต้องลงทะเบียนในระบบเป็นอาสาสมัคร CDD, หรือผู้ปกครองที่มี CDD ตามรายละเอียดของผู้ใช้แต่ละ ผู้ใช้ที่มีการกำหนดให้เหมาะสมกับกลุ่มเฉพาะ ประวัติผู้ใช้จะถูกบันทึกไว้ในฐานข้อมูลเพื่อความสะดวกของผู้ดูแลระบบ ตัวอย่างเช่นเมื่อผู้ดูแลระบบจะส่งข้อความกระจายไปยังกลุ่ม

2) การจับคู่โมดูล : โมดูลนี้ถูกออกแบบมาเพื่อให้ตรงกับขึ้นอาสาสมัครและผู้ปกครองกับ CDD อาสาสมัครเหล่านี้จะได้รับการรับรองโดย AHFSWF ที่มีการตรวจสอบคุณสมบัติและบริการฝึกอบรม ทั้งพ่อและแม่กับ CDD และอาสาสมัครสามารถที่จะกรอกตารางเวลาของพวกเขาและเลือกการจับคู่ที่เหมาะอย่างยิ่งสำหรับสถานการณ์ของพวกเขา

ผู้ดูแลระบบสามารถจัดการประวัติของการจับคู่และผู้ใช้ในโมดูลนี้ ดังรูปที่ 8 ที่ได้อธิบายถึงการดำเนินการของขั้นตอนของโมดูลที่ตรงกันแต่ละครั้งรวมถึงเข้าสู่ระบบในผู้ใช้, การตรวจสอบของผู้มีอำนาจอนุญาตของผู้ใช้ของกลุ่มเครือข่ายทางสังคม, การตั้งเวลาการจับคู่

3) ลักษณะการบันทึก : อาสาสมัครจะเป็นผู้ช่วย CDD สามารถที่จะบันทึกพฤติกรรมใด ๆ ที่เป็นนิสัยของเด็กที่ไม่ดี เพื่อช่วยให้อาสาสมัครที่พบลักษณะนิสัยเดียวกัน สมารถนำข้อมูลส่วนนี้มาใช้ได้

4) การปรึกษาบนแพลตฟอร์ม : แพลตฟอร์มนี้จะแสดงในรูปแบบของกระดานสนทนาซึ่งสามารถเข้าถึงได้ภายใต้การอนุมัติ การจัดเรียงเพื่อให้มั่นใจว่าเรื่องของการสนทนาจะเพิ่มขึ้นเฉพาะหลังจากที่ได้รับความยินยอมจากผู้ใช้ทั้งหมดได้รับอนุญาตจากผู้ดูแลระบบ

5) สถานที่ตั้งอยู่ในโมดูลบริการ : ผู้ดูแลสามารถสถานที่ตั้งของผู้ใช้โดยใช้โมดูลบริการตามสถานที่ที่จะหาคนที่หายไปถ้าคนที่ขาดหายไปดำเนินการเปิดการใช้งานจีพีเอสอุปกรณ์ไร้สายและอัพโหลดสถานที่ของพวกเขาไปยังระบบโดยมีการติดตามคนหายไปยังสถานที่ต่างๆ โดยใช้ GPS และมีการอัพโหลดสถานที่ที่เขาไป เนื่องจากครอบครัวที่มี CDD และอาสาสมัครต้องทำงานของระบบและการตัดสินใจมี PDA ติดตัวไปทุกแห่ง แม้ว่าเด็กจะหายไป พ่อแม่ยังสามารถสอบถามดูแลจากผู้ดูแลระบบเพื่อค้นหาเด็กที่หายไป ซึ่ง ข้อมูลสถานที่ตั้งยังสามารถช่วยหาให้ตรงกับของระบบ MSNSM ตัวอย่างเช่นอาสาสมัครสามารถที่จะหาผู้ปกครองด้วย CDD ที่ต้องการความช่วยเหลือเร่งด่วนผ่านโมดูลนี้

6) บัญชีและผู้เข้าถึง : โมดูลนี้ช่วยให้ผู้ดูแลเพื่อการตรวจสอบสิทธิ์หน้าที่ของผู้ใช้และการบำรุงรักษาและจัดการบัญชีผู้ใช้

7) การใช้งานอินเตอร์เฟซ : ผู้ดูแลระบบสามารถจัดการโมดูลทั้งหมดของ frontend เครือข่ายสังคมแพลตฟอร์มการให้บริการโดยใช้โมดูลนี้

8) ลักษณะการรายงานและวิเคราะห์ : การจัดการเครือข่ายและการวิเคราะห์เหตุการณ์ที่เกิดขึ้นบนพื้นฐานเว็บไซต์ที่ช่วยอำนวยความสะดวก Web-based mode for convenience [44] การนำ logfile ที่ถูกบันทึกลงในระบบมาทำการวิเคราะห์หาผลลัพธ์และสร้างรายงาน[45] โดย Router Traffic Grapher (MRTG) เป็นซอฟแวร์ที่ช่วยในการวิเคราะห์การส่งผ่านของการเชื่อมต่อเครือข่ายและการมองเห็นประสิทธิภาพของระบบ ดังนั้นผู้ดูและระบบสามารถตรวจสอบภาพรวมการทำงานของระบบ

การจัดการเครือข่ายระบบนี้ PHP Protocol (SNMP) เป็นตัวแทนให้การตั้งค่าจะได้รับและการตั้งค่าฐานข้อมูลการบริหารจัดการ (MIB) ค่าบนพีดีเอ นี้จะช่วยให้ผู้ดูแลระบบตรวจสอบระบบในระหว่างการเดินทาง metadata นอกจากนี้ระบบนี้ได้บูรณการของ XML ที่มี e - mail ดังนั้นการส่งข้อมูลจะถูกกำหนดลักษณะการส่งคล้ายการส่งคล้าย e-mail v.3, SMTP, HTTP, และ / หรือการเข้าถึงข้อความอินเทอร์เน็ต Protocol (IMAP) ซึ่งระบบวิเคราะห์ XML อัตโนมัติเพื่อประสานงานการจัดการเครือข่ายของ SNMP

เมื่อบูรณาการการกำหนดค่าของ XML ที่มี e - mail, ระบบมีการรันโปรแกรมเป็นระยะ ๆ โดยอัตโนมัติ การวิเคราะห์หัวของ e - mail ที่มาถึง ถ้าการวินิจฉัยว่าเป็นข้อมูลการกำหนดค่าระบบโปรแกรมจะวิเคราะห์เนื้อหาของ e - mail ต่อไป ถ้าทั้ง XML การกำหนดค่าและอำนาจหน้าที่ของผู้ใช้อย่างถูกต้องและถูกต้องตามกฎหมายจากนั้นระบบจะเปลี่ยนการตั้งค่าระบบให้เป็นไปตามเนื้อหาของ e - mail ผู้ใช้พร้อมกันจะได้รับการยืนยัน e - mail

ในบทความได้สร้างการสนับสนุนการให้บริการติดต่อสื่อสารเครือข่ายสังคมบนโทรศัพท์เคลื่อนที่และเทคโนโลยีการใช้ข้อมูลเช่น database , เทคโนโลยีการค้นหาและการเทคโนโลยีโทรคมนาคม โดยได้ศึกษาความเป็นไปได้จากการสัมภาษณ์แบบเจาะลึกและการมุงเน้นไปยังกลุ่มที่ถูกสัมภาษณ์จากแบบสอบถามและการวิเคราะห์ระบบ framework และการออกแบบที่เหมาะสมกับครอบครัว CDD บนพื้นฐานงานวิจัยนี้ได้สร้างระบบการจัดการบริการสำหรับเครือข่ายสังคมโทรศัพท์เคลื่อนที่

ซึ่งระบบมีการรูปแบบการจัดการที่มีการพบปะกับผู้ปกครองกลุ่ม CDD โดยที่มีการให้ความช่วยเหลือให้ทันเวลาของอาสาสมัครและในเวลาเดียวกันเป็นแพลตฟอร์มการอภิปรายสำหรับการแลกเปลี่ยนข้อมูลระหว่างเคลื่อนที่ทุกกลุ่มเครือข่ายทางสังคม ด้วยความระมัดระวังการแปลการสื่อสาร ในการแก้ไขปัญหาในชีวิตจริงทางสังคมในองค์กรทางด้านเทคนิคของชุมชนเสมือนบทความนี้แสดงให้เห็นว่าเทคโนโลยีการคำนวณมีค่าในชีวิตของทุกครอบครัวที่มี CDD โดยบทความนี้ได้คาดหวังว่าเป็นจุดเริ่มต้นในการให้บริการทางสังคมสำหรับคนกลุ่มน้อยที่ด้อยโอกาสทั่วโลก โดยเฉพาะอย่างยิ่งกับครอบครัวที่มี CDD ซึ่งในอนาคตการพัฒนาและปรับปรุงในระบบนี้จะทำให้มีส่วนร่วมสำคัญในการทำงานทางสังคมและจะได้รับประโยชน์ของคนกลุ่มน้อยด้อยโอกาส

2 R-U-In? - Exploiting Rich Presence and Converged Communications for Next-Generation Activity-Oriented Social Networking [46]

ความนิยมในเครือข่ายสังคม ซึ่งทำให้ ISP (Internet Service Providers) และผู้ให้บริการด้าน โทรคมนาคมได้มีการเริ่มต้นการสำรวจโอกาสใหม่ๆที่ส่งเสริมรายได้ของพวกเขาจากเครือข่ายสังคม มีความพยายามอำนวยความสะดวกให้กับลูกค้าที่เชื่อมต่อแล้วบนเครือข่ายสังคมจากช่องทางของ ISP หรืออุปกรณ์โทรศัพท์เคลื่อนที่ โดยการใช้งานเทคโนโลยี Web 2.0 และการรวมการสื่อสารต่างๆ เข้าด้วยกัน เป็นสิ่งนำพาให้เกิดการใช้งานคู่กันของผู้ใช้ที่สร้างเนื้อหา และการให้ข้อมูลไปในตัวเอง เช่น ผู้ใช้อยู่ไหนในขณะนี้ , ความง่าย, ความสนใจต่างๆ และบ่งบอกสภาวะอารมณ์ ในการพัฒนาด้านภูมิศาสาตร์นี้ ซึ่งเครือข่ายสังคมนี้มีวามแปลกใหม่นี้ทำให้เป็นศูนย์กลางในการดึงดูดผู้ใช้เข้ามาก และรูปแบบทางด้านธุรกิจก็จะสร้างความร่ำรวยจากด้านสังคมมีเดีย โดยในบทความนี้จะแสดงถึง R-U-In , กิจกรรมเครือข่ายสังคมที่จัดวางโดยผู้ใช้ให้ความร่วมมือและเข้าร่วมกันในการทำกิจกกรมที่สนใจเหมือนกัน ซึ่งกิจกรรมสามารถเริ่มขึ้นและรายการีขึ้นอยู่กับความต้องการที่ไม่นานนักตามความสนใจของพวกเขา R-U-In จะขัดกับรูปแบบเนื้อหาและเหตุผลด้านเทคนิคที่สามารถค้นหาสังคม บนพื้นฐาน real time และการหาขีดจำกัดที่มีความสนใจที่เหมือนกันอนาคตต่อไปเทคนิคการติดต่อสื่อสาร ที่มีการจัดการเข้ากับชีวิตประจำวันของผู้ใช้แบบ Real Time ซึ่งเริ่มแรกในการสำรวจผลลัพธ์ บนพื้นฐานรูปแบบการสร้างของ R-U-In ได้พิสูจน์ความเชื่อของ กิจกกรม real time เครือข่ายสังคมที่มีการจัดวาง และการเปลี่ยนแปลงของประสบการณ์ของผู้ใช้

ความสามารถของเครือข่ายสังคม ผู้ใช้จะได้ติดต่อและเข้าร่วมกันกิจกรรมที่สนใจแบบ real time โดยผ่านผู้ให้บริการด้านเครือข่ายที่มีการขยายขอบเขตการใช้งานอย่างกว้างขวาง อย่างไรก็ตามประสบการณ์ในมิติต่างๆของเครือข่ายสังคม ในบทความนี้ได้วิเคราะห์ถึงความท้าทายในการกำหนดขอบเขตกิจกรรมที่ได้ทำบนเครือข่ายสังคมและการนำเสนอ R-U-In ที่ไม่มีวันหยุด การจัดการกิจกรรมที่สนใจในแบบ real time ซึ่ง R-U-In สามารถขยายไปได้ด้วยความนิยมบนเครือข่ายสังคมทุกวัน

การทำ R-U-In ให้เพิ่มขึ้นบนความแตกต่างของเส้นทาง - ซึ่งได้มีการรวมกราฟสังคมในการค้นประมวลผลการค้นหา การคำนวณหาความสัมพันธ์ที่ได้ตั้งไว้ และการรวมความเชื่อถือและเรื่องความส่วนบุคคล ซึ่งเครือข่ายสังคมยังมี

ผลกระทบกับกิจกรรมการทำงานแบบ real time และการวิเคราะห์พฤติกรรมของผู้ใช้ ที่มีอยู่ในหลายๆพื้นที่ที่ต้องแก้ไข

3 Designs of Privacy Protection in Location-Aware Mobile Social Networking Applications [47]

ในบทความนี้ได้มุงเน้นถึงความเป็นส่วนตัวในโทรศัพท์เคลื่อนที่ SNA ได้คำนึงถึงจากมุมมองต่างๆ โดยเฉพาะอย่างยิ่งผู้ปกครองของวัยรุ่นและเยาวชนที่ได้รับประโยชน์จากการใช้โทรศัพท์เคลื่อนที่ Social Network Application (SNAs) ได้ทราบสถานที่ต่างๆที่พวกเขาไป แต่ยังมีความเสียงหลายอย่าง เช่น การติดตามตรวจสอบโดยผู้อื่นๆ ที่อาจเป็นอันตรายต่อพวกเขาจากการเปิดเผยสถานที่อยู่ให้กับผู้อื่นได้ทราบ

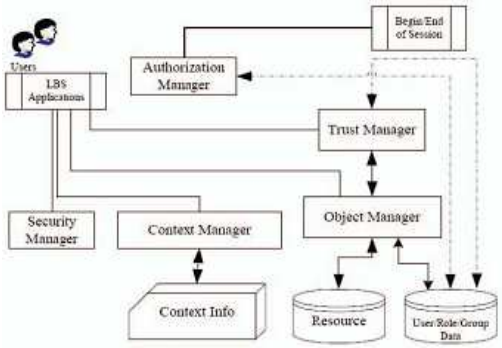
ในปัจจุบัน SNAs ได้ตระหนึกถึงความเรื่องของสถานที่อยู่ แต่กลไกลในการแก้ปัญหายังมีน้อย ในการปกป้องข้อมูลส่วนบุคคล จากการวิเคราะห์บทความควรกำหนดผู้หลักการประกาศการแสดงตัวหรือมีหลักการตรวจสอบและการปฏิเสธ โดยมีวิธีการป้องกันความเป็นส่วนตัว

โดยในบทความได้มีการสำรวจและการวิเคราะห์ปัญหาความเป็นส่วนตัวในปัจจุบัน ซึ่งได้มีการปรับปรุงออกแบบในการปกป้องข้อมูลส่วนบุคคลในระบบ LaMOC มีกลไกลตามหลักการที่ได้เปิดให้ผู้ใช้งานได้สะดวกและปลอดภัยจากการเปิดเผยข้อมูลที่ตั้ง และวิธีการคำนวณสามารถป้องกันไม่ให้ผู้ใช้ถูกทำร้ายในที่ๆเป็นอันตราย

ขั้นตอนต่อไป เป็นลักษณะการใช้งานที่แพร่หลายของอุปกรณ์โทรศัพท์เคลื่อนที่ ที่มีการปรับปรุงวิธีการคำนวณตรวจสอบสถานะความเป็นตัวมากขึ้น

- การออกแบบป้องกันความเป็นส่วนตัวใน LaMOC

LaMOC เป็นระบบแพลตฟอร์มการทำงานร่วมกันให้บริการตามพื้นที่ เช่นแบบสอบถามสมุดหน้าเหลือง, บริการให้คำแนะนำจุดที่น่าสนใจ, การบริการเส้นทางและบริการนำทาง [39] สำหรับผู้ใช้โทรศัพท์เคลื่อนที่ อย่างไรก็ดีการรวมกันของบริการได้มีการเพิ่มการติดต่อแบบเสมือนและการรวบรวมข้อเสนอแนะจุดต่างๆ แม้ว่า LaMOC ไม่ได้เป็น SNA จริงๆ, ซึ่งบริการส่วนใหญ่จะเป็นการแนะนำสถานที่ที่เกี่ยวข้องและไม่สามารถเลือกสถานที่อื่นๆ ดังนั้นจึงได้รับประโยชน์จากการวิเคราะห์บทความก่อนหน้าของเราในประเด็นความเป็นส่วนตัว, เป็นความสำคัญมากที่ออกแบบคุ้มครองความเป็นส่วนตัวในระบบโดยเฉพาะอย่างยิ่งกับสถานที่ที่เกี่ยวข้อง



รูปที่ 9 โครงสร้างสถาปัตยกรรมโปรแกรม LaMOC [47]

- หลักการกลไกลความเป็นส่วนตัว

1) LaMOC เมื่อเข้าสู่ระบบ ช่วยให้ผู้ใช้กำหนดรายชื่อเพื่อนที่สามารถเข้าถึงได้ในสิ่งที่พวกเขาให้บุคคลหรือกลุ่มสามารถทราบถึงสถานที่ของพวกเขา ซึ่งในกลไกลที่คล้ายกันจะถูกใช้โดย SNAs เคลื่อนที่

2) การนำเสนอของผู้ใช้ ได้ตระหนักถึงเป้าหมายที่ตั้ง SNAs โทรศัพท์เคลื่อนที่ในปัจจุบันมักจะใช้ GPS, Wi - Fi เครือข่ายโทรศัพท์เคลื่อนที่หรือการรวมกันเพื่อให้ได้ข้อมูลสถานที่และความถูกต้องแตกต่างกันไป ตามที่ระบุไว้ก่อนหน้านี้ LaMOC ใช้ GPS ในการรับข้อมูลสถานที่และช่วงที่พบความถูกต้องจากไปหลายสิบหลายร้อยเมตรขึ้นอยู่กับการเปิดกว้างกลางแจ้ง โดยทั่วไปแล้วการการันตรีที่ผู้ใช้สามารถได้รับสถานที่ความถูกต้องของเป้าหมายของพวกเขาอย่างไรก็ตามเนื่องจากกิจกรรมของผู้ใช้และข้อมูลส่วนบุคคลที่สามารถอ้างถึงโดยสถานที่ของตนโดยใช้เทคโนโลยีการทำเหมืองข้อมูล โดยผลในปรากฏในโอกาสในการเปิดเผยข้อมูลส่วนบุคคลที่ไม่พึงประสงค์ที่เกิดขึ้นเพิ่มขึ้นตามการเพิ่มขึ้นของความถูกต้องของสถานที่ ดังนั้นจึงเป็นเรื่องที่ดีที่จะให้ผู้ใช้มีทางเลือกมากขึ้นในการนำเสนอสถานที่ของพวกเขา โดยทั่วไปจะแสดงไอคอน LaMOC คนบนหน้าจอแผนที่ตามที่จะยืนสำหรับสถานที่ที่แท้จริงของผู้ใช้เป้าหมาย แต่จินตนาการสถานการณ์ที่ผู้ใช้จะไม่เต็มใจที่จะแบ่งปันสถานที่ของตนเองให้กับบางคนทราบ แต่เป็นไปได้ให้การปกป้อง โดยมีการประยุกต์ใช้อาจทำให้บุคคลบางคนเกิดความละอายในการต้องการทราบที่อยู่ของผู้ใช้ โดยมีวิธีการนำเสนอในภูมิภาคเช่นวงกลมรวมทั้งสถานที่จริงเป้าหมายของแทนตำแหน่งของตัวเองได้และเพื่อให้ผู้ใช้เพื่อระบุจุดสถานที่ที่เหมาะสมเช่น 1 กม. วิธีการนี้จะแสดงเป็นคำอธิบายที่แน่ชัดของสถานที่เป้าหมาย แต่ก็ถือว่าไม่ได้มีผลตั้งแต่ภูมิภาคยังคงปกคลุมเปิดเผยข้อมูลบางส่วน

เพื่อแก้ปัญหาภาวะลำบากใจ กลไกทั้งสองที่แตกต่างกันจะเปิดใน LaMOC สำหรับคุณภาพการหายไปของการนำเสนอข้อมูลสถานที่ : ความไม่ชัดเจนและความคลุมเครือ หมายความว่าเราได้นำเสนอวิธีการที่แน่นอนซึ่งใช้ลูกศรมุ่งหน้าไปยังสถานที่จริงเป้าหมายของ ขนาดของลูกศรที่เป็นแบบเดียวกันเสมอภายในขอบเขตของหน้าจอแม้ว่าสถานที่จริงของเป้าหมายที่อยู่นอกหน้าจอตามแผนที่

นอกจากความคลุมเครือซึ่งหมายความว่าประโยคภาษาตัวอย่างเช่นว่า" เป้าหมายที่อยู่ไกลจากคุณ"จะดำเนินการให้ความช่วยเหลือในการอธิบายถึงระยะห่างระหว่างผู้ใช้และเป้าหมาย (ดูรูปที่ 10) การรวมกันของลูกศรทิศทางกับแง่ภาษาศาสตร์ได้จัดให้มี

ข้อมูลที่เพียงพอสำหรับการค้นหาที่แท้จริงและสามารถปกป้องผู้ใช้จากผู้สังเกตการณ์ที่เป็นอันตราย ซึ่งในความเป็นจริงก็พยายามที่จะทำให้ผู้ใช้รู้สึกสะดวกสบายขึ้นและสนับสนุนให้สถานที่ของพวกเขาร่วมกันกับผู้อื่นได้โดยไม่ต้องวิตกกังวล

รูปที่ 10 ที่ลูกศรชี้ทิศทางและแง่ภาษาศาสตร์ระบุตำแหน่งของผู้ใช้เป้าหมายของ [47]

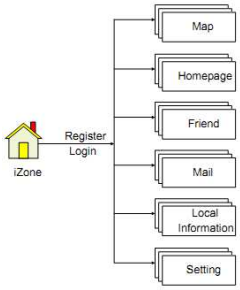
3) การตั้งค่าโหมดความเป็นส่วนตัวแม้จะมีความกังวลว่าผู้ใช้สามารถระบุรายชื่อเพื่อนที่สามารถเข้าถึงได้ว่าผู้ที่สถานที่ของพวกเขาที่มีอยู่มันไม่ได้มีประสิทธิภาพและประสิทธิผลในบางกรณี งานวิจัยก่อนหน้านี้ได้แสดงให้เห็นว่าผู้ใช้การตั้งค่าความเป็นส่วนตัวแตกต่างกันในกิจกรรมเงื่อนไขและการตรวจสอบ เมื่อเทียบกับการใช้งานคอมพิวเตอร์ที่มีความซับซ้อนและการดำเนินงานบ่อย ควรจะหลีกเลี่ยงเท่าที่จะทำได้ภายในสถานการณ์ที่โทรศัพท์เคลื่อนที่ นั่นคือมันไม่เหมาะสมที่จะขอให้ผู้ใช้เพื่อปรับการเข้าถึงรายการเพื่อนของพวกเขาบ่อย แต่น่าเสียดายที่แม้กระทั่งเมื่อเวลาของการละเลยอาจทำให้เกิดผลกระทบที่ไม่พึงประสงค์

ดังนั้น LaMOC มีกลไกที่รวดเร็วและสะดวกในการปรับนโยบายความเป็นส่วนตัวสถานที่ โดยการเลือกโหมดการเก็บข้อมูลส่วนบุคคลที่สี่ : บุคคลที่ใกล้ชิด, ปกติ, และโหมดที่มองไม่เห็น เหมือนทุกคนร่วมกันชื่อจริงของพวกเขาเพื่อให้เพื่อน ๆ กับแต่ละอื่น ๆ ในบุคคลที่สถานที่จริงของผู้ใช้ที่มีให้บริการแก่ประชาชนในโหมดของบุคคลที่แสดงไอคอนที่คนบนหน้าจอแผนที่ขึ้นอยู่กับพวกเขา ด้วยโหมดนี้ผู้ใช้จะสามารถที่จะทำให้เพื่อนใกล้เคียงและทำให้การส่งเสริมการปฏิสัมพันธ์ในท้องถิ่น ในโหมดความใกล้ชิด, สถานที่ที่เกิดขึ้นจริงจะมีให้กับเพื่อนของผู้ใช้เป็นไปตามรายชื่อเพื่อนที่สามารถเข้าถึงได้และ LaMOC จะให้ตอบปฏิเสธคลุมเครือเช่นล้มเหลวในการหาผู้ใช้เป้าหมายไปที่เพื่อนที่ถูกบล็อกจริงโดยผู้ใช้ในกรณีนี้เฉพาะ . โหมดปกติจะใช้วิธีนำเสนอโดยนัยที่อธิบายข้างต้นกลับเป็นลูกศรทิศทางและคำอธิบายที่คลุมเครือของระยะทางในการระบุตำแหน่งของเป้าหมายเมื่อแบบสอบถามเพื่อน / สถานที่ของตน ในโหมดที่มองไม่เห็นไม่มีใครสามารถเข้าถึงสถานที่ของผู้ใช้ การเปลี่ยนแปลงของเหล่าสี่โหมดเป็นเรื่องง่ายเหมือนกับการตั้งค่าสถานะในการใช้งานมากที่สุดข้อความโต้ตอบแบบทันที

4) การตรวจสอบการทำงาน LaMOC ช่วยให้ผู้ใช้เพื่อตรวจสอบการบันทึกแบบสอบถามที่สถานที่ของพวกเขาถูกร้องขอโดยคนในสิ่งที่เวลา ดังนั้นแม้ว่าผู้ใช้จะคิดถึงข้อความแจ้งเตือน, เขา / เธอยังคงสามารถรับข้อมูลนี้โดยการทำงานตรวจสอบการตรวจสอบความเสี่ยงที่อาจเกิดขึ้น

4 iZone: A Location-Based Mobile Social Networking System [48]

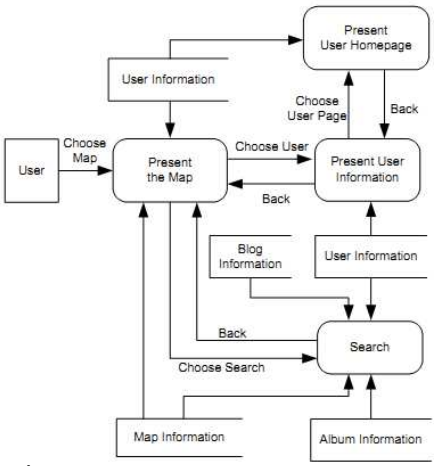
ในบทความนี้ได้นำเสนอการออกแบบและการดำเนินงานต้นแบบของระบบ iZone ซึ่งระบบจะขึ้นอยู่กับการรวมกันของเทคโนโลยีไร้สาย, J2ME, LBS และ GIS และสามารถหาผู้ใช้และส่งข้อมูลขึ้นอยู่กับสถานที่ของพวกเขา ระบบ iZone ที่มีประสิทธิภาพยังอยู่ภายใต้การดำเนินงาน เราเชื่อว่าการแพร่กระจายกว้างของโทรศัพท์เคลื่อนที่และเทคโนโลยีไร้สายจะนำไปสู่การพัฒนาอย่างกว้างขวางของการใช้งานตามพื้นที่



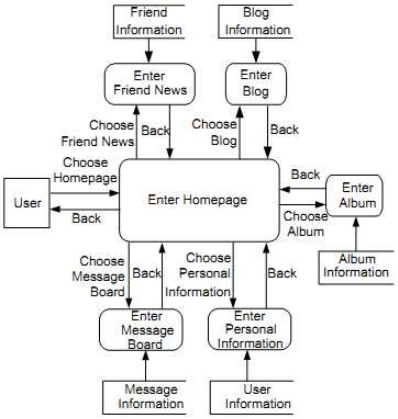
รูปที่ 11 โครงสร้างของระบบ iZone [48]

Map Subsystem : หลังจากที่เข้าสู่ระบบผู้ใช้สามารถดูระบบย่อยเริ่มต้นของระบบย่อยแผนที่ดังแสดงในรูปที่ 10 มันเป็นแกนของระบบตามสถานที่ ซึ่งประกอบด้วยการค้นหาในท้องถิ่นและ online ของโมดูลเพื่อน ในโมดูลการค้นหาในท้องถิ่น, ผู้ใช้สามารถค้นหาผู้ใช้ท้องถิ่น, ร้านอาหารท้องถิ่นและโรงพยาบาลในท้องถิ่นและอื่น ๆ ซึ่งเป็นคู่มือที่ช่วยสร้างความแปลกใหม่ให้กับผู้ใช้ และผู้ใช้ยังสามารถเลือกมุมมองปกติและมุมมองจากดาวเทียม ใน on line ของโมดูลเพื่อนที่ผู้ใช้สามารถดูผู้ใช้อื่น ๆ ที่ใกล้เคียงบนแผนที่ บางข้อมูลเพิ่มเติม (ชื่อเล่นเช่นเพศและสถานะ) ผู้ใช้บางคนแสดงตัวแทนของตัวเองและชี้ไปยังสถานที่ นอกจากนี้ยังมีแผนที่ที่มีการทำงานของขยายเข้าและออก ซึ่งเป็นเรื่องง่ายที่จะเปลี่ยนขนาดของแผนที่

Homepage Subsystem : เป็นส่วนแรกที่ผู้ใช้จะเข้าถึงและแสดงข่าวของเพื่อนๆในกลุ่ม, เส้นทาง, ข้อมูลส่วนบุคคลเมื่อเข้าสู่ระบบและในโมดูลที่แสดงในรูปที่ 13 มีข้อมูลข่าวของเพื่อนๆเป็นแบบไดนามิก สามารถปรากฏขึ้น ซึ่งในข่าวๆของเพื่อนเหล่านั้นจะแสดงตามจุดสถานที่ เวลา ที่สอดคล้องกับข้อมูลใหม่ ซึ่งผู้ใช้เองสามารถแสดงความคิดเห็นกับข่าวของเพื่อนๆ โดยโมดูลนี้เป็นประตูไปสู่โมดูลอื่นๆ ซึ่งในโมดูลนี้จะบันทึกติดตามผู้ใช้คนอื่นๆ ที่ได้เข้าชมและเพื่อนของผู้ใช้รายการ และมีข้อมูลส่วนบุคคลของผู้ใช้งาน สามารถจัดการกับฟังก์ชั่นต่างๆ เช่นการเผยแพร่บล็อก แก้ไข ลบ ความคิดเห็นต่างๆ



รูปที่ 12 Dataflow diagram ของ Map Subsystem [48]



รูปที่ 13 Dataflow diagram ของ Homepage Subsystem [48]

Friend Subsystem : ระบบย่อยในส่วนของเพื่อน เพื่อเป็นการสร้างความมั่นใจว่ามีการจัดการข้อมูลเกี่ยวกับเพื่อน โดยสามารถตั้งค่ากลุ่มที่แตกต่างกัน เพิ่ม แก้ไข กลุ่มผู้ใช้ หรือแม้แต่มุมอง และมีฟังก์ชั่นหนึ่งที่แนะนำเพื่อนที่มีความสนใจคล้ายกับผู้ใช้ คือ โมดูลการสื่อสารกับเพื่อน การสนทนา เช่น โปรแกรมโต้ตอบข้อความแบบทัน นอกจากนั้นผู้ใช้ยังสามารถถ่ายโอนไฟล์ รูปภาพได้

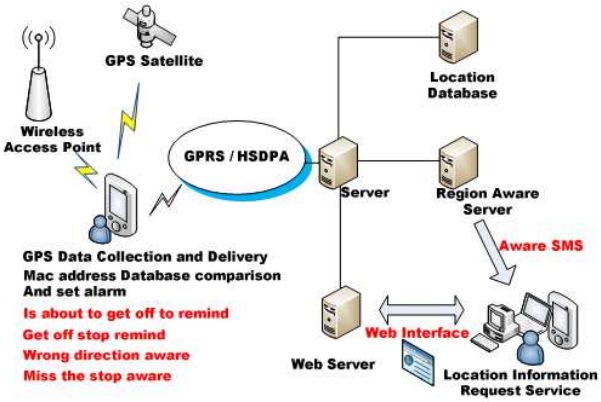
Mail Subsystem : เป็นระบบเดียวกับการทำงานของการจัดการกับจดหมาย ผู้ใช้สามารถเขียนส่ง ดู ลบและจัดการอีเมล มันคล้ายกับระบบอีเมลทั่วไป

Local Information Subsystem : ระบบย่อยข้อมูลท้องถิ่นสามารถให้ผู้ใช้เกี่ยวกับข่าวท้องถิ่น ซึ่งประกอบด้วยการรายงานสภาพอากาศท้องถิ่นข่าวท้องถิ่นและโมดูลฟอรั่มท้องถิ่น ในโมดูลรายงานสภาพอากาศในท้องถิ่นผู้ใช้จะได้รับการพยากรณ์อากาศ สามวันถัดไปรวมทั้งอุณหภูมิ, แสงแดด, ความชื้นและความเร็วลม นอกจากนี้ยังมีข้อเสนอแนะบางอย่างเช่นตามเป็นจำไว้ว่าให้นำร่มหรือใช้เสื้อผ้ามากขึ้น โมดูลข่าวสารท้องถิ่นบอกข่าวผู้ใช้ทุกวัน ผู้ใช้สามารถสมัครเป็นสมาชิกส่วนที่แตกต่างจากข่าวเช่นกีฬาสุขภาพหรือการเมืองโมดูลฟอรั่มอื่น ๆ ท้องถิ่นเป็นฟอรั่มสำหรับผู้ใช้ที่โพสต์ข้อความ

Setting Subsystem : ระบบย่อยคือระบบการตั้งค่าสำหรับผู้ใช้เพื่อกำหนดข้อมูลส่วนบุคคลและความเป็นส่วนตัว ประกอบด้วยโมดูลการตั้งค่าความเป็นส่วนตัวและโมดูลการตั้งค่าข้อมูล ในโมดูลการตั้งค่าความเป็นส่วนตัวของผู้ใช้สามารถตั้งค่าว่าคนอื่น ๆ ได้รับอนุญาตให้ดูข้อมูลของเขาเช่นหมายเลขโทรศัพท์เคลื่อนที่, เพศ, วันเกิด ฯลฯ ผู้ใช้สามารถตั้งค่านี้เป็นคนมีการอนุญาตให้มีเพียงเพื่อนที่จะได้รับอนุญาตหรือไม่มีคนอื่นจะได้รับอนุญาต ในการตั้งค่าข้อมูลผู้ใช้สามารถแก้ไขข้อมูลส่วนบุคคลของเขา / เธอ มันเป็นทางลัดของโมดูลข้อมูลส่วนบุคคลของระบบย่อยโฮมเพจ ผู้ใช้สามารถแก้ไขได้ที่นี่โดยไม่ต้องป้อนระบบย่อยโฮมเพจ

5 Mobile guiding and tracking services in public transit system for people with mental illness [49]

ในบทความนี้ได้สร้างระบบที่ใช้งานโทรศัพท์เคลื่อนที่ PDA ด้วยการเชื่อมต่อข้อมูลผู้ใช้ที่มีความเจ็บป่วยทางจิตที่จะเดินทางไปทำงาน โดยระบบจะสามารถแนะนำผู้ใช้ที่จะใช้ระบบรถไฟฟ้าใต้ดินรวมถึงการแจ้งให้ทราบถึงการแจ้งเตือนสถานีที่ผิดและการแจ้งเตือนผิดทิศทาง ซึ่งระบบได้ตระหนักถึงสถานที่ (ความสามารถตรวจจับที่ดีจะอยู่ในเมือง) ดังนั้นจึงสามารถที่จะนำทางผู้ใช้ในการติดต่อกับผู้ดูแลหรือผู้ให้บริการที่ตรงกับความต้องการเฉพาะของพวกเขา โดยผู้ให้บริการการยังมีอุปกรณ์โทรศัพท์เคลื่อนที่บอกสถานที่บอกให้ทราบ นอกจากนี้ระบบยังมีการประยุกต์ใช้เทคโนโลยีสำหรับการตรวจสอบการเคลื่อนไหวของผู้ใช้ตลอดเวลาเพื่อให้ผู้ดูแลสามารถแจ้งเตือนหากผู้ใช้หลงทางจากสถานที่ถูกต้องในระหว่างการเดินทางของพวกเขา ผลโดยรวมของการประเมินผลการศึกษาพบว่าระบบที่ถูกใช้งานแน่นอนและเป้าหมายของผู้ใช้ผู้ดูแล ใช้งานได้อย่างสะดวกเพราะมีความเข้าใจเกี่ยวกับระบบอย่างดี ซึ่งในหน้าจอควบคุมจะมีการรายงานแสดงภาพกราฟฟิค ที่ช่วยแสดงสัญลักษณ์ให้พวกเขาทราบถึงที่ตั้งและระบุสถานะการณ์ฉุกเฉิน การในช้อินเตอร์เฟซทั้งบนเว็บและข้อความ SMS บนโทรศัพท์เคลื่อนที่ได้รับการยอมรับ



รูปที่ 14 โครงสร้างสถาปัตยกรรมระบบ [49]

โครงสร้างสถาปัตยกรรมระบบ :

ในรูปที่ 14 นำเสนอโครงสร้างสถาปัตยกรรมระบบ ที่ประกอบด้วยองค์ประกอบหลักสี่องค์ประกอบ : อุปกรณ์ของไคล์เอ็นท์, การเข้าถึงเครือข่ายไร้สายอินเทอร์เน็ต, อินเทอร์เน็ตและโฮส และฝั่งเซิร์ฟเวอร์ที่รองรับเซิร์ฟเวอร์ฐานข้อมูลและเว็บ โดยสถานีที่ติดตั้งอุปกรณ์ของไคล์เอ็นท์ โดยโมดูลนี้จะจัดการกับอุปกรณ์ฮาร์ดแวร์และมีผลตอบกลับเมื่อมีการร้องขอข้อมูลจากผู้ใช้ที่ไปยังสถานที่ตามโปรแกรม โดยในสถานที่รถไฟฟ้าใต้ดิน ,WiFi จะถูกติดตั้งเพื่อใช้ประเมินตำแหน่งปัจจุบันของผู้ใช้งาน (สัญญาณ WiFi ครอบคลุมประมาณ 50 เมตรในสภาพแวดล้อมในร่ม) มีสัญญาณแบบ AP เท่านั้นที่สามารถตรวจพบได้จากที่ในหนึ่งในสถานี ดังนั้นขั้นตอนวิธีการวางตำแหน่งสำหรับผู้ใช้ตรวจสอบที่สถานีรถไฟฟ้าใต้ดินจะกลายเป็นเรื่องง่าย โดยการใช้เทคโนโลยีการบริการเว็บโมดูลสถานที่ที่สามารถสอบถามได้โดยโปรแกรมประยุกต์บนเว็บใด ๆ ที่จะได้รับตำแหน่งเคลื่อนที่ของโดยไม่ต้องมีการติดตั้งซอฟต์แวร์ใด ๆ ของบุคคลที่สามเกี่ยวกับอุปกรณ์ของไคล์เอ็นท์ เมื่อมีการสอบถามโดยใช้โปรแกรมประยุกต์เว็บโมดูลสถานที่ที่จะส่งตำแหน่งของเคลื่อนที่ไปยังเว็บเซิร์ฟเวอร์ที่ริเริ่มการร้องขอ การเข้าถึงเครือข่ายไร้สายทำหน้าที่ท่อส่งแบบ TCP/IP มากกว่า

โครงสร้างพื้นฐาน ตัวอย่างเช่นเครือข่ายผู้ให้บริการสามารถใช้ HSPDA, GPRS หรือ WiFi เพื่ออำนวยความสะดวกในการจราจรของข้อมูล สถาปัตยกรรมที่นำเสนอเครือข่ายผู้ให้บริการที่ง่ายโดยการเอาตำแหน่งผู้ให้บริการให้ความช่วยเหลือตามที่เสนอในการลดการเปลี่ยนแปลงที่ทำกับแกนเครือข่ายโทรศัพท์เคลื่อนที่ ในการนี้ทดสอบ HSDPA จะใช้ตามวัตถุประสงค์ PDA โทรศัพท์เคลื่อนที่ทั่วไปมีการนำมาใช้เป็นอุปกรณ์ของไคล์เอ็นท์และฟังก์ชันที่จำเป็นต้องใช้เป็นโปรแกรมโทรศัพท์เคลื่อนที่ ซึ่งมีข้อดีสองอย่างคือ : อย่างแรกคือ เป็นอุปกรณ์ที่มีราคาถูกและเป็นอุปกรณ์เฉพาะ อย่างที่สอง ผู้ใช้สามารถเลือกประเภทของโทรศัพท์เคลื่อนที่และใช้บริการโปรแกรมโทรศัพท์เคลื่อนที่ที่ทันสมัยเช่น รองรับ MP3 และแฟลชเกม โดยจะไม่มีการติดฉลากมีผลเมื่อผู้ป่วยทางจิตใช้อุปกรณ์เหล่านั้น จากการสัมภาษณ์ผู้ดูแลผู้ป่วยและผู้ที่มี ความเจ็บป่วยทางจิตพบว่าสิ่งที่ไม่ชอบที่สุดคืออุปกรณ์ที่เปิดเผยตัวตนว่าตนเองเป็นผู้ป่วย ซึ่งเป็นเหตุผลที่สำคัญที่การอำนวยความสะดวกบางโปรแกรมล้มเหลว

ผลการทดลองและข้อเสนอแนะ : โดยงานวิจัยนี้ได้รับความร่วมมือจากห้าโรงพยาบาลในไทเป ประเทศไตหวัน มีผู้ช่วยให้การสนับสนุนผู้ป่วยหกท่าน ในการทดลองภาคสนาม ประกอบได้เพศชายและหญิงช่วงอายุระหว่าง 21-44 ปี ซึ่งทั้งหมดเป็นผู้ป่วยทางติด สามคนได้รับบาดเจ็บที่หัวและอีกสามคนพิการทางปัญญา สามคนใช้โทรศัพท์เคลื่อนที่ในชีวิตประจำวันและอีกสามคนไม่ได้ใช้ มีสองคนใช้บริการรถประจำทางและรถไฟฟ้าใต้ดิน และสามคนจะใช้บริการรถไฟฟ้าใต้ดินนานๆครั้ง อีกหนึ่งคนนานๆ ถึงใช้รถไฟฟ้าใต้ดินและรถประจำทาง

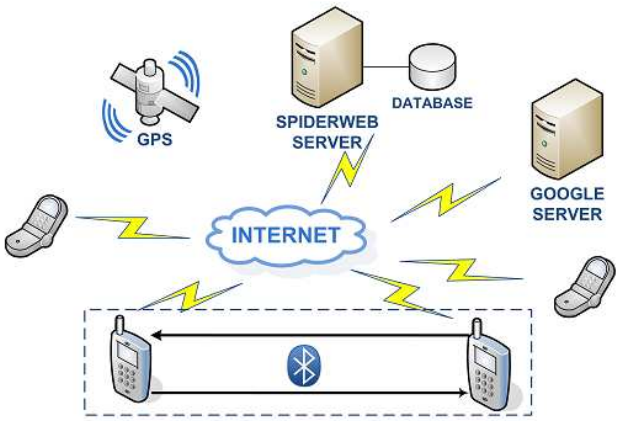
การทดลองดำเนินการในสาย Bannan ในรถไฟใต้ดินไทเป มีผู้ช่วยเรื่องดังต่อไปนี้เพื่อความปลอดภัยผู้ทำการทดลอง โดยจะไม่มีการบอกข้อความใด ๆ ระหว่างการทดสอบภาคสนาม การทดลองถูกแบ่งออกเป็นสามส่วน (1) คำสั่งในการดำเนินงานโทรศัพท์เคลื่อนที่ (2) การทดสอบหลัก (3) ข้อเสนอแนะเรื่องเพราะเป็นครั้งแรกในการทดสอบได้ใช้เวลาห้านาทีในการสอนผู้ทดสอบวิธีการใช้งาน

หลังจากการทดสอบได้รับผลตอบรับจากเรื่องที่ทำ คะแนะแต่ละคนที่ทำทั้งห้าจุดและการถามเรื่องความรู้สึกก่อนและหลังทำการทดสอบ พบกว่ามีการใช้งานได้จริงมีประโยชน์ในการเดินทางของผู้ป่วย และได้พบอีกว่าการใช้งานระบบสั่นสะเทือนของโทรศัพท์จะได้ผลดีกว่าการใช้งานเสียงสำหรับผู้ป่วยด้านจิต

6 Spiderweb: A Social Mobile Network [50]

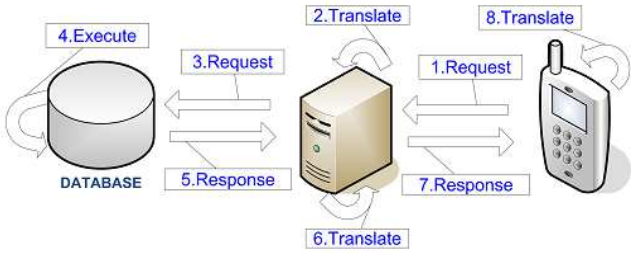
เป็นโปรแกรมเคลื่อนที่ซึ่งจะช่วยให้ผู้ให้บริการของเครือข่ายทางสังคมช่วยการดำเนินการประสบความสำเร็จ โดยต้นแบบนี้มีชุดของการบริการเครือข่ายสังคมเสริม แต่ขึ้นอยู่กับเทคโนโลยีแบบของโทรศัพท์เคลื่อนที่ (เช่น GPS, กล้อง) และนอกจากนี้ยังช่วยการจัดตั้งเครือข่าย Spiderweb ทำงานร่วมกันได้ดีกับเทคโนโลยีบลูทู ธ ไร้สาย โดยโปรแกรมได้สร้างแบบจำลองเสมือนเป็นตัวแทนของผู้ใช้ ที่มีส่วนร่วมในเครือข่ายทางสังคมในท้องถิ่น ซึ่ง Spiderweb แสดงให้ความสามารถระดับสูงที่สามารถนำไปต่อยอดในเชิงพาณิชย์ได้ แต่ยังมีข้อจำกัดบางอย่างความเร็วในการรับส่งบลูทูธต่ำและการค้นหาบลูทูธยังต่ำอยู่

ซึ่งข้อจำกัดการออกแบบของโทรศัพท์คือคีย์บอร์ดที่มีขนาดและเล็กหน้าจอที่ไม่สามารถขยายได้น้อย และการขยายสัญญาณได้น้อย



รูปที่ 15 โครงสร้างสถาปัตยกรรม Spiderweb [50]

โครงสร้างสถาปัตยกรรม Spiderweb บนพื้นฐานไคล์เอ็นท์/เซริฟเวอร์ ซึ่งบนเซิร์ฟเวอร์ใช้ฐานข้อมูล MySQL โดยเก็บข้อมูลเกี่ยวกับผู้ใช้ทั้งหมดของโปรแกรม การสื่อสารระหว่างเซิร์ฟเวอร์และใช้ Java Database Connectivity (JDBC) , ดาวเทียม GPS เพื่อให้โอกาสสำหรับผู้ใช้ที่มีการอัพโหลดตำแหน่งปัจจุบันไปยังฐานข้อมูล และการเรียกคืนตำแหน่งของเพื่อนของผู้ใช้บริการแผนที่ Google ให้โดยเซิร์ฟเวอร์ของ Google และองค์ประกอบอื่น ๆ ของรูปที่ 15 แสดงการแบ่งประเภทของไคล์เอ็นท์



รูปที่ 16 การสื่อสาระหว่างอินเทอร์เน็ต [50]

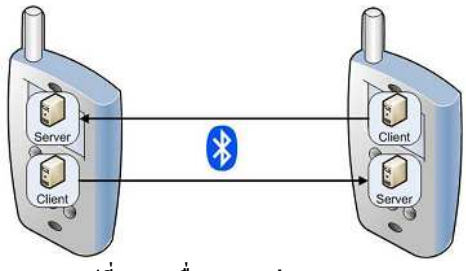
1) *การเชื่อมต่ออินเทอร์เน็ต* : การทำงานร่วมกันระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ Spiderweb จะปรากฏในรูปที่ 14 ไคลเอ็นต์จะเริ่มต้นการสื่อสารกับเซิร์ฟเวอร์ (ผ่านทาง IP) และส่งคำขอ (1) หากเซิร์ฟเวอร์ยอมรับการเชื่อมต่อกับไคลเอ็นต์ที่จะประมวลผลการร้องขอ โดยเชื่อมต่อกับฐานข้อมูล (2) และจากนั้นก็จะคำร้องที่ถูกแปลไปยังฐานข้อมูล (3) ของ ฐานข้อมูลดำเนินการตามคำร้อง (4) และให้การตอบสนองกลับไปยังเซิร์ฟเวอร์ (5) เซิร์ฟเวอร์สร้างกระบวนการเพื่อนจะตอบไปไคลเอ็นต์ (6) สุดท้ายเมื่อเซิร์ฟเวอร์แปลความที่จะส่งการตอบสนองกลับไปยังไคลเอ็นต์ (7) เมื่อไคลเอ็นต์ที่ร้องขอได้รับการตอบกลับจากเซิร์ฟเวอร์แปลผ่านทางโปรแกรมประยุกต์ (8)

รูปที่ 17 การรับตำแหน่ง GPS ของผู้ใช้ [50]

2) *GPS* : การอัพโหลดตำแหน่งปัจจุบันของผู้ใช้ลงในฐานข้อมูลโปรแกรมจะดำเนินการสองขั้นตอนที่ :

- ได้รับละติจูดและลองจิจูดจากดาวเทียมจีพีเอ
- ภาพที่ส่งพิกัดปัจจุบันของผู้ใช้ฐานข้อมูลโดยใช้การเชื่อมต่ออินเทอร์เน็ต

ในการดึงข้อมูลตำแหน่ง GPS ของผู้ใช้โปรแกรมประยุกต์ที่มีลักษณะการทำงานดังแสดงในรูปที่ 15 ไคลเอ็นต์จะเริ่มต้นการสื่อสารกับเซิร์ฟเวอร์ (1) ซึ่งกระบวนการการร้องขอโดยจะส่งไปยังฐานข้อมูล (2) จากนั้นเซิร์ฟเวอร์จะส่งกลับการตอบสนองให้กับไคลเอ็นต์ (3) ที่ส่งต่อการตอบสนองต่อเซิร์ฟเวอร์ของ Google (4) นี้ เซิร์ฟเวอร์ Google กระบวนการขอ (5) และส่งกลับมาเพื่อตอบสนองไคลเอ็นต์ (6) การตอบสนองนี้ถูกแปลโดยไคลเอ็นต์และการมองเห็นเป็นภาพซึ่งบ่งชี้ที่ตำแหน่ง GPS เพื่อปรับปรุงของผู้ใช้ที่จำเป็น (7) การใช้งานของเซิร์ฟเวอร์ของ Google อาจจะมีการ จำกัด ส่งคำร้อง 1000 ไม่ซ้ำกัน (ที่แตกต่างกัน) การร้องขอต่อภาพของผู้ชมต่อวัน [51] ด้วยเหตุนี้การเชื่อมต่อระหว่างไคลเอ็นต์ Spiderweb และเซิร์ฟเวอร์ของ Google เป็นที่ต้องการอย่างใดอย่างหนึ่งระหว่างเซิร์ฟเวอร์ Spiderweb และเซิร์ฟเวอร์ของ Google



รูปที่ 18 การสื่อสารระหว่างบลูทูธ [50]

3) การเชื่อมต่อบลูทูธ : ดังรูปที่ 18 เป็นการขยายตัวของรูปสี่เหลี่ยมที่อยู่ในด้านล่างของรูปที่ 13 โหนดของเครือข่าย P2P ที่สามารถทำหน้าที่ไปพร้อมกันสองบทบาทที่แตกต่างกันของเซิร์ฟเวอร์และไคลเอนต์ ในความเป็นจริงที่แสดงใน รูปที่ 16 ในโทรศัพท์เคลื่อนที่เป็นทั้งเซิร์ฟเวอร์และไคลเอนต์กำลังทำงานอยู่ในเวลาเดียวกัน หน้าที่ของเซิร์ฟเวอร์คือการเผยแพร่บริการและการยอมรับการเชื่อมต่อพร้อมกันในขณะที่งานของไคลเอนต์ค้นหาและเชื่อมต่อกับบริการ [52] ซึ่งเป็นครั้งแรกที่ไคลเอนต์ดำเนินการค้นพบอุปกรณ์ซึ่งประกอบด้วยในการค้นหาของทุกอุปกรณ์บลูทูธ โดยกรองบางที่ทำให้ถูกจำกัดการค้นหาไปยังอุปกรณ์ที่ตรงกับเงื่อนไข โดยเฉพาะอย่างยิ่งเนื่องจากข้อเท็จจริงที่ว่า Spiderweb จะทำงานได้เฉพาะบนโทรศัพท์เคลื่อนที่ที่มีบลูทูธ โดยไม่ยอมรับบูลธูทจากอุปกรณ์ประเภทอื่น ๆ เพราะทำให้เกิดการเสียเวลาและพลังงาน เนื่องจากอุปกรณ์ที่พบจะต้องมีการวิเคราะห์ แต่หากอุปกรณ์เหล่านั้นมีการติดตั้งโปรแกรม Spiderweb ดังนั้นการค้นพบการบริการเป็นสิ่งจำเป็น การค้นพบแต่ละสืบค้นบริการโทรศัพท์เคลื่อนที่ที่ผ่านการกรองจากการค้นพบอุปกรณ์ หากอุปกรณ์บางอย่างตรงตามเงื่อนไข ของทั้งสองอุปกรณ์ (โดยอุปกรณ์ที่หนึ่งจะดำเนินการสอบถามรายละเอียดเพิ่มเติมและอีกหนึ่งค้นพบ) จะสามารถที่จะสื่อสารและแลกเปลี่ยนข้อมูลกันได้

เปรียบเทียบบทความที่เกี่ยวข้อง

ตารางที่ 4 เปรียบเทียบบทความที่เกี่ยวข้อง Mobile Social Network

บทความ	[43]	[47]	[48]	[49]	[50]
ติดตามจุดต่างๆ	✓	✓	✓	✓	✓
WiFi	×	✓	✓	✓	✓
GPS	✓	×		✓	✓
เครือข่ายโทรศัพท์	✓	✓	✓	×	✓
ความปลอดภัยในการตรวจสอบสถานที่อยู่	✓	✓	✓	×	✓
ความปลอดภัยเรื่องความเป็นส่วนบุคคล	✓	✓	✓	×	✓
สถาปัตยกรรม client/server	✓	×	✓	✓	✓
มีเก็บข้อมูลในฐานข้อมูล	✓	✓	✓	✓	✓
ความพึงพอใจของผู้ทดสอบมากกว่า 50%	×	×		✓	✓
เชิงพาณิชย์	×	✓		×	✓

V. สรุป/ข้อเสนอแนะและงานในอนาคต

การประมวลผลและการสร้างเครือข่ายสังคมออนไลน์ (Social Computing and Networking) เป็นวิวัฒนาการของการติดต่อสื่อสารแบบก้าวกระโดด ที่ทำให้ผู้คนมากมายที่อยู่ห่างไกลกันต่างมีส่วนร่วม ในการทำกิจกรรม (Activity) ต่างๆผ่านเครือข่ายอินเตอร์เน็ต โดยการสร้างกลุ่มสังคม (Community) เพื่อวัตถุประสงค์หนึ่งๆขึ้นมา โดยใช้โปรแกรมและเทคโนโลยีในด้าน Social Computing ที่ทำงานอยู่บน Social Network ที่มีอยู่หลายรูปแบบ เช่น Identity Network (เผยแพร่ตัวตน) Creative Network (เผยแพร่ผลงาน) Interested Network (ความสนใจตรงกัน) Collaboration Network (การทำงานร่วมกัน) Gaming/Virtual Reality (โลกเสมือน) Peer to Peer (P2P) เป็นต้น โดยที่กลุ่มสังคมนั้นๆสามารถได้รับประโยชน์จากเทคโนโลยีเหล่านี้อย่างมหาศาล ปัญหาต่างๆในการสื่อสารที่เกิดขึ้น เป็นจุดกำเนิดของ Social Computing ซึ่งถูก

พัฒนาขึ้นเพื่ออำนวยความสะดวกให้กับผู้ใช้ พร้อมทั้งใช้แก้ปัญหาเหล่านั้นให้หมดไป

แต่ขณะเดียวกันการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลที่สื่อสารกันผ่าน Social Network เป็นเรื่องสำคัญที่มีผู้ศึกษาวิจัยเกี่ยวกับเรื่องเหล่านี้มากมาย ดังที่ได้ทำการสำรวจ (survey) มาแล้วนี้ จากการศึกษาดังกล่าวทั้ง 3 ส่วน คือ ส่วนของ Security , Privacy และ Mobile Community โดย Security จะประกอบด้วยการตรวจสอบสิ่งที่ก่อให้เกิดความผิดพลาดแก่ Social Computing and Network เช่น BotNet, Spam, Pishing, Phishing, Malware ซึ่งจากการศึกษาได้ใช้เทคนิคการตรวจสอบทั้งหมด 4 เทคนิคด้วยกัน คือ Signature-based, Anomaly-based, DNS-based และ Mining-based โดยจากการศึกษาการตรวจสอบจากเทคนิคดังกล่าวปรากฏว่า เทคนิค Minig-based จะได้ประสิทธิภาพมากที่สุด ส่วนสองคือ Privacy จะเป็นการศึกษาความเป็นส่วนตัวใน Social Computing and Network กลไกและเทคนิคต่างๆที่มีผู้คิดค้นขึ้นเพื่อป้องกันรักษาความเป็นส่วนตัวของผู้ใช้งาน และผลการสำรวจพบว่ากลไกการป้องกันความเป็นส่วนตัวแบบ PSNS[17] จะมีเทคนิคในการป้องกันความเป็นส่วนตัวที่มีประสิทธิภาพกว่าเมื่อเปรียบเทียบกับกลไกอื่นๆ และส่วนที่สาม การประยุกต์นำเอา Social Network ไปใช้ในงานเกี่ยวกับโทรศัพท์เคลื่อนที่ยุคใหม่: Mobile Social Network เป็นอีกทางเลือกหนึ่งในการประยุกต์ใช้งาน Social Network และได้มีผู้ทำการศึกษาวิจัยในเรื่องนี้อย่างมากมายเช่นกัน

งานในอนาคตที่สนใจศึกษาต่อไปคือการนำเทคนิค Security และ Privacy ไปประยุกต์ใน Mobile Social Network ซึ่งเป็นสิ่งที่ต้องศึกษาให้ลึกซึ้งอีกครั้งหนึ่ง

เอกสารอ้างอิง

[1] Weimin L. Jingbo L. Jing L.Chengyu F., “An Analysis of Security in Social Networks,” in Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on , 2009 , PP. 648 – 651

[2] ดร.กมล เขมะรังษี และ กิติศักดิ์ จิรวรรณกูล, “บอตเน็ต ภัยรูปแบบใหม่บนอินเทอร์เน็ต,” 10 สิงหาคม 2548.

[3] Snort IDS web page. http://www.snort.org, March 2006.

[4] J.R. Binkley and S.Singh, “An algorithm for anomaly-based botnet detection,” in Proc. USENIX Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI’06), , 2006, pp 43–48.

[5] A. Karasaridis, B. Rexroad, and D. Hoeflin, “Wide-scale botnet detection and characterization,” in Proc. 1st Workshop on Hot Topics in Understanding Botnets, 2007.

[6] G. Gu, J. Zhang, and W. Lee, “Botsniffer: Detecting botnet command and control channels in network traffic,” in Proc. 15th Annual Network and distributed System Security Symposium (NDSS’08), 2008.

[7] D. Dagon, “Botnet Detection and Response, The Network is the Infection,” in OARC Workshop, 2005.

[8] J. Kristoff, “Botnets,” in 32nd Meeting of the North American Network Operators Group, 2004.

[9] A. Schonewille and D.J. van Helmond. “The Domain Name Service as an IDS,” Master’s Project, University of Amsterdam, Netherlands, Feb 2006, http://staff.science.uva.nl/~delaat/snb-2005-2006/p12/report.pdf

[10] N. F. A. Ramachandran and D. Dagon, “Revealing botnet membership using dnsbl counter-intelligence,” in Proc. 2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI ’06), 2006.

[11] H. Choi, H. Lee, H. Lee, and H. Kim, “Botnet Detection by Monitoring Group Activities in DNS Traffic,” in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007, pp.715-720.

[12] J. Goebel and T. Holz, “Rishi: Identify bot contaminated hosts by irc nickname evaluation,” in Proc. 1st Workshop on Hot Topics in Understanding Botnets, 2007.

[13] W. Strayer, D. Lapsley, B. Walsh, and C. Livadas, Botnet Detection Based on Network Behavior, ser. Advances in Information Security. Springer, 2008, PP. 1-24.

[14] M. M. Masud, T. Al-khateeb, L. Khan, B. Thuraisingham, K. W. Hamlen, “ Flow-based identification of botnet traffic by mining multiple log file,” in Proc. International Conference on Distributed Frameworks & Applications (DFMA), Penang, Malaysia, 2008.

[15] G. Gu, R. Perdisci, J. Zhang, and W. Lee, “Botminer: Clustering analysis of network traffic for protocol- and structure independent botnet detection,” in Proc. 17th USENIX Security Symposium, 2008

[16] E. Aïmeur, S. Gambs and Ai Ho,”UPP: User Privacy Policy for Social Networking Sites”, *2009 Fourth International Conference on Internet and Web Applications and Services*,2009.

[17] E. Aimeur, S. Gambs, and A. Ho. Towards a privacyenhanced social networking site. In *Availability, Reliability, and Security, 2010. ARES ’10 International*

Conference on, pages 172 –179, 2010.

[18] E. Baatarjav, R. Dantu, Y. Tang and J. Cangussu,” BBN-Based Privacy Management Sytem for Facebook”, *Proceeding ISI'09 Proceedings of the 2009 IEEE international conference on Intelligence and security informatics* ,2009.

[19] Carminati, B., Ferrari, E., Perego, A . 2007. “Private Relationships in Social Networks”. *Data Engineering Workshop, 2007 IEEE 23rd International Conference on*, p.*163-171.*

[20] Lipford, H., Hull, G., Latulipe, C., Besmer, A.,Watson, J. 2009 . “Visible Flows: Contextual Integrity and the Design of Privacy Mechanisms on

Social Network Sites". *Computational Science and Engineering, 2009. CSE '09. International Conference on* ,Vol.*4*, p. 985-989.

[21] Mont, M., Pearson, S., Bramhall, P. 2004. "An Adaptive Privacy Management System for Data Repositories". *System*, p.236-245.

[22] Luo, W., Xie, Q., & Hengartner, U. 2009. "FaceCloak: An Architecture for User Privacy on Social Networking Sites". *Computational Science and Engineering, 2009. CSE '09. International Conference on*, Vol.*3*, p.26-33.

[23] Z. Yan, H. Zexing, W. Huaixi, H. Hongxin and A. G. Joon. "A Collaborative Framework for Privacy Protection in Online Social Networks," in *Proc. SEFCOM*, 2010, pp. 1-15.

[24] L.A. Cutillo, R. Molva and T. Strufe. "Safebook: A privacy-preserving online social network leveraging on real-life trust." *IEEE Communications Magazine*, vol. 47, pp. 94 – 101, Dec. 2009

[25] B. E. Amgalan, D. Ram and P. Santi. "Privacy Management for Facebook," *Conf. Department of Computer Science and Engineering*, University of North Texas, Denton, Texas, USA, 2008

[26] M. Egele, A. Moser, C. Kruegel and E. Kirda, "PoX: Protecting users from malicious Facebook applications," 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011, pp 288 - 294

[27] T. Burghardt, A. Walter, E. Buchmann and K. Bohm, "PRIMO - Towards Privacy Aware Image Sharing," IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT), 2008, pp 21 - 24

[28] Cutillo, L.A., Molva, R , Strufe, T. 2009. "Privacy preserving social networking through decentralization". *Sixth International Conference on Wireless OnDemand Network Systems and Services*, *2*, pp. 145-152.

[29] S.M.A. Abbas, J.A. Pouwelse, D.H.J. Epema, and H.J. Sips," A gossip-based distributed social networking system", *2009 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprise*s,2009.

[30] Kurkovsky, O Rivera, J Bhalodi, "Classification of Privacy Management Techniques in Pervasive Computing," *International Journal of u- and e-Service, Science and Technology*, Vol.11, No.1, pp.55-71, 2007.

[31] Lawler, J.P. and Molluzzo, J.C. (2010) "A Study of the perceptions of students on privacy and security on Social Networking Sites (SNS) on the internet", *Journal of Information Systems Applied Research,* Vol. 3, No.12

[32] Huaqing Liang; Min Geng; Lei Wu; Hongdong Yin; , "Research on methods of ABI and PWV measurement," Image and Signal Processing (CISP), 2010 3rd International Congress on , vol.9, pp.4130-4134, 16-18 Oct. 2010.

[33] พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ. 2554. โทรศัพท์เคลื่อนที่กับการเชื่อมโลกด้วยเทคโนโลยี VoIP และ IMS. (ออนไลน์). แหล่งที่มา : http://www.vcharkarn.com/varticle/40613. 28 สิงหาคม 2554.

[34] A. Beach, M. Gartell, S. Akkala, J. Elston, J. Kel-ley, K. Nishimoto, B. Ray, S. Razgulin, K. Sundaresan,

[35] D. M. Boyd and N. B. Ellison. Social network sites:Definition, history and scholarship. Journal of computer- medited communication, 2007.

[36] R. Bulander, M. Decker, G. Schiefer, and B. Kolmel.Comparison of Different Approaches for mobile Adver-tising. University of Karlsruhe, 2005.

[37] Facebook. Facebook statistics. http://www.facebook.com/press/info.php?statistics/press/info.php?statistics,08/02/2009.

[38] F. Johansson. Extending mobile social software with contextual information. Umeå University, Sweden, 2008.

[39] D. Melinger, K. Bonna, M. Sharon, and M. SantRam.Socialight: A Mobile Social Networking System. New York University, 2004.

[40] T. O'Reilly. Web 2.0. http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html, 08/02/2009.

[41] C. Tong. Analysis of some popular mobile social net-work system. Helsinki University of Technology, 2008.

[42] N. Ziv and B. Mullth. An exploration on mobile social networking: Dodgeball as case in point. Proceedings of the international conference on mobile business, 2006.

[43] C. Li-Der, L. Nien-Hwa, C. Yen-Wen, C. Yao-Jen, Y. Jyun-Yan, H. Lien-Fu, C. Wen-Ling , C. Hung-Yi and S. Haw-Yun, "Mobile Social Network Services for Families With Children With Developmental Disabilities," Information Technology in Biomedicine, IEEE Transactions on., Oct. 2011, pp. 585–593.

[44] J.-W. Choi and K.-H. Lee, "A web-based management system for network monitoring," in Proc. 2002 IEEE Workshop IP Oper. Manage., Oct. 2002, pp. 98–102.

[45] Y.-W. Chen and S.-H. Hu, "Study of the traffic scheduler by using correlation heuristics," IEICE Trans. Commun., vol. E87-B, no. 8, pp. 2273–2280, Aug. 2004.

[46] N. Banerjee, D. Chakraborty, K. Dasgupta, S. Mittal, S. Nagar and Saguna, "R-U-In? - Exploiting Rich Presence and Converged Communications for Next-Generation Activity-Oriented Social Networking,"Mobile Data Management: Systems, Services and

Middleware, 2009. MDM '09. Tenth International Conference on, p.222-231, year.2009.

[47] Rong Tan, Junzhong Gu, Jing Yang and Peng Chen, “Designs of privacy protection in location-aware mobile social networking applications,” Pervasive Computing and Applications (ICPCA), 2010 5th International Conference on., 2011, pp.62-68.

[48] Rui Cheng, Zhuo Yang and Feng Xia, "iZone: A Location-Based Mobile Social Networking System," Parallel Architectures, Algorithms and Programming (PAAP), 2010 Third International Symposium on., 2010, pp.33-38.

[49] L. Hung-Huan, C. Yung-Ju, C. Yu-Jen and C. Wei-Hsun, "Mobile guiding and tracking services in public transit system for people with mental illness," TENCON 2009 - 2009 IEEE Region 10 Conference., 2009, pp.1-4.

[50] A. Sapuppo, "Spiderweb: A social mobile network," Wireless Conference (EW), 2010 European., 2010, pp.475-481.

[51] Google, Static Maps API Developer’s Guide, http://code.google.com/apis/maps/documentation/staticmaps, 2009.

[52] Martin de Jode, Programming Java 2 Micro Edition on Symbian OS , pp. 208-225, WILEY, 2004.

[53] saengsith.blogspot. /social-computing http://saengsith.blogspot.com/2011/07/social-computing.html,26/09/2011.

[54] ku.ac.th. Network safety. http://web.ku.ac.th/schoolnet/snet1/network/safety.htm