KKU Res. J. 2013; 18(2): 221-239
http : //resjournal.kku.ac.th

ความมั่นคงของเทคโนโลยีการประมวลผลกลุ่มเมฆ
Security of Cloud Computing Technology

สุชาติ คุ้มมะณี[1]
Suchart Khummanee[1]

[1] *สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม*
Correspondent author: suchart.k@msu.ac.th

บทคัดย่อ

บทความนี้กล่าวถึง ปัญหา และแนวทางการแก้ไขปัญหาด้านความมั่นคงของเทคโนโลยีการประมวลผลกลุ่มเมฆ ซึ่งเป็นระบบคอมพิวเตอร์ที่มีสมรรถนะสูง และกำลังได้รับความสนใจเป็นอย่างมากในปัจจุบัน วัตถุประสงค์ของเทคโนโลยีดังกล่าวเพื่อตอบสนองต่อการประมวลผลข้อมูลที่มีปริมาณมาก ซับซ้อน ยืดหยุ่นต่อการใช้งาน และลดต้นทุนของการประมวลผลลง ปัจจุบันเทคโนโลยีดังกล่าวยังอยู่ในช่วงเริ่มต้นการใช้งานจริง ด้วยเหตุนี้ปัญหาด้านความมั่นคงยังคงเป็นประเด็นปัญหาที่สำคัญและน่าสนใจเป็นอย่างยิ่งในปัจจุบัน

Abstract

This article is explained problems and solutions to solve security problems of cloud computing technology which is the high-performance computer system. It is a very interesting topic at present. The aims of this technology are for respond processing of large amounts of data, complexity, flexibilities for applications and reduce the cost of processing. Currently this technology is still at its beginning stage of practical use. Thus, the security problems are still important and interesting problem at present.

คำสำคัญ: การประมวลผลกลุ่มเมฆ ความมั่นคง ความเสี่ยง การลดต้นทุน
Keywords: Cloud computing, security, risk, reducing cost

1. บทนำ

กิจกรรมต่างๆ ในปัจจุบันมีความจำเป็นต้องอาศัยระบบคอมพิวเตอร์เพื่อช่วยในการประมวลผลเกือบทั้งสิ้น เนื่องจากมีจุดเด่นหลายประการ เช่น สามารถแก้โจทย์ปัญหาที่ซับซ้อน รวดเร็ว ถูกต้อง แม่นยำ ประมวลผลข้อมูลได้จำนวนมาก ประหยัดค่าใช้จ่าย เป็นต้น ในอดีตที่ผ่านมา เมื่อต้องการระบบคอมพิวเตอร์มาสนับสนุนการทำงาน จำเป็นต้องลงทุนสูง โดยประกอบไปด้วยพื้นที่เหมาะสมในการติดตั้ง อุณหภูมิ ระบบไฟฟ้าสำรอง คอมพิวเตอร์แม่ข่าย คอมพิวเตอร์ส่วนบุคคล ระบบเครือข่าย เป็นต้น ซึ่งต้นทุนจะสูงหรือต่ำขึ้นอยู่กับปริมาณข้อมูลและภาระของงานที่ต้องการประมวลผล

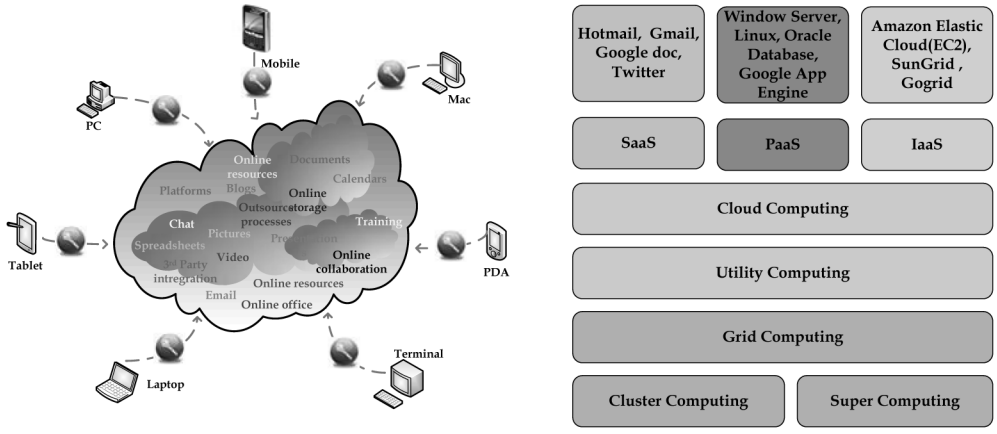
การเช่าเทคโนโลยีแทนการจัดซื้อช่วยลดต้นทุนได้มาก ผู้ให้บริการจะจัดหาทรัพยากรต่างๆ ให้ครบถ้วนพร้อมบริการเมื่อเกิดปัญหา เรียกว่า Service provider (SP) หากผู้ใช้ที่มีงบประมาณจำกัด สามารถใช้บริการแบบฟรีได้ โดยผ่านกลุ่มผู้ใช้ที่แบ่งปันทรัพยากรร่วมกันผ่านเครือข่ายอินเทอร์เน็ตโดยไม่หวังผลกำไร (Non-profit computing group) แต่มีจุดอ่อนด้านเสถียรภาพ ปัญหาที่พบจากการเช่าระบบคือ บริการไม่ตรงกับความต้องการ เสียค่าใช้จ่ายสูง ติดตั้งซอฟต์แวร์ที่จำเพาะงานไม่ได้ บริการอาจล่าช้า ไม่รับประกันความเร็วในการประมวลผล ความมั่นคงจะตกเป็นภาระของผู้ใช้งาน เป็นต้น ปัจจุบันจึงมีการคิดระบบคอมพิวเตอร์ที่สามารถตอบสนองต่อความต้องการ และแก้ปัญหาดังกล่าวข้างต้นได้ เรียกว่า การประมวลผลกลุ่มเมฆ (Cloud computing) ซึ่งกำลังได้รับความนิยมเป็นอย่างสูง และมีแนวโน้มที่จะมาทดแทนระบบคอมพิวเตอร์ปัจจุบัน จุดเด่นคือ มีประสิทธิภาพการประมวลผลที่สูง แต่มีต้นทุนต่ำ

ข้อได้เปรียบอื่นๆ ของเทคโนโลยีนี้ คือ ใช้ทรัพยากรคุ้มค่า บริการขึ้นอยู่กับผู้ใช้ ลดการใช้พลังงาน ประหยัดต้นทุนด้านลิขสิทธิ์ซอฟต์แวร์ สามารถขยายตัวได้ดี เป็นต้น สำหรับจุดอ่อนของเทคโนโลยีดังกล่าวในปัจจุบัน คือ "***ความมั่นคง***" ซึ่งกำลังดำเนินการวิจัยอย่างต่อเนื่องในปัจจุบัน ในบทความนี้จะนำเสนอความความเสี่ยงและความไม่มั่นคงของการประมวลผลกลุ่มเมฆ รวมถึงวิธีการป้องกัน เพื่อเป็นแนวทางสำหรับผู้ให้บริการเทคโนโลยีดังกล่าว ผู้ที่กำลังใช้งาน และผู้ที่กำลังจะใช้งานในอนาคต ได้มีองค์ความรู้เพื่อการใช้งานที่ถูกต้องต่อไป

2. โครงสร้างการประมวลผลกลุ่มเมฆ

โครงสร้างการประมวลผลกลุ่มเมฆเกิดจากการผสมผสานระหว่างระบบการประมวลผลคลัสเตอร์ (Cluster computing) (1) และการประมวลผลแบบกริด (Grid computing) (2, 3) หรืออาจกล่าวได้ว่า Cloud computing = Cluster computing + Grid computing การประมวลผลคลัสเตอร์ คือ การเชื่อมต่อของกลุ่มระบบคอมพิวเตอร์เดียวกันภายใต้ระบบเครือข่ายจำกัด ที่มีประสิทธิภาพและมีความเร็วสูง สามารถกระจายงานไปประมวลผลยังสมาชิกภายในกลุ่มได้ การประมวลผลกริด คือระบบคอมพิวเตอร์ที่รวมเอาคอมพิวเตอร์ที่อยู่ในสถานที่ต่างกัน เชื่อมต่อกันด้วยเทคนิคการประมวลผลแบบกระจาย งานขนาดใหญ่จะถูกแบ่งย่อยและกระจายไปทำงานในคอมพิวเตอร์หลายๆ เครื่องที่ได้เชื่อมต่อกันไว้แล้ว เสมือนเป็นระบบคอมพิวเตอร์ขนาดใหญ่เพียงระบบเดียว

การประมวลผลกลุ่มเมฆ (Cloud Computing) (4, 5) คือ การนำเครื่องคอมพิวเตอร์จำนวนมากเชื่อมต่อเข้าด้วยกัน คอมพิวเตอร์ในกลุ่มไม่จำเป็นต้องติดตั้งอยู่ในสถานที่เดียวกันก็ได้ คอมพิวเตอร์ทั้งหมดจะเชื่อมต่อกันผ่านเครือข่ายความเร็วสูง โดยไม่จำเป็นต้องมีฮาร์ดแวร์และระบบปฏิบัติการที่เหมือนกันก็ได้ ผู้ใช้ไม่จำเป็นต้องมีคอมพิวเตอร์ที่มีประสิทธิภาพสูงในการประมวลผล หรือต้องติดตั้งซอฟต์แวร์เป็นจำนวนมากๆ และไม่จำเป็นต้องรับรู้ถึงความซับซ้อนของการทำงานภายในของระบบ ผู้ใช้บริการรับแต่เพียงผลลัพธ์ที่ได้จากการประมวลผลเท่านั้น ที่เครื่องคอมพิวเตอร์ของผู้ใช้ทำหน้าที่เพียงติดต่อกับส่วนของผู้ใช้ (User Interface) เพื่อแสดงผล รับคำสั่งและสื่อสารไปยังบริการต่าง ๆ บนกลุ่มเมฆคอมพิวเตอร์ ดังรูปที่ 1 (a)



(a) บริการต่างๆ บน Cloud (b) โครงสร้างของ Cloud (6)

รูปที่ 1. บริการและโครงสร้างของการประมวลผลกลุ่มเมฆ

จากรูปที่ 1 (b) แสดงโครงสร้างการประมวลผลกลุ่มเมฆ ซึ่งประกอบไปด้วยส่วนต่างๆ ดังต่อไปนี้

1. Cluster Computing, Super Computing และ Grid Computing เป็นการรวบรวมทรัพยากรในการประมวลผล คือ ฮาร์ดแวร์และซอฟต์แวร์มาทำงานร่วมกันเป็นระบบคอมพิวเตอร์ขนาดใหญ่ที่มีประสิทธิภาพในการประมวลผลสูง

2. Utility Computing (7) ทำหน้าที่วัดปริมาณการทำงานของระบบออกมาเป็นหน่วยของการใช้บริการ เช่น วัดปริมาณการใช้งานซีพียู พื้นที่จัดเก็บข้อมูล ปริมาณแบนด์วิดท์ เป็นต้น

3. Cloud Computing (5, 8) จัดเตรียมบริการต่างๆ ที่ผู้ใช้ต้องการ เปลี่ยนรูปแบบการประมวล ผลแบบเดิม (ประมวลผลภายใต้เครื่องเซิร์ฟเวอร์เดียว) ไปเป็นการประมวลผลบนเครือข่ายความเร็วสูง ผ่านกลุ่มของเซิร์ฟเวอร์จำนวนมากที่ทำงานร่วมกัน วิธีการประมวลผลจะอ้างอิงกับความต้องการของผู้ใช้เป็นหลัก เมื่อผู้ใช้ร้องขอบริการ ซอฟต์แวร์บนกลุ่มเมฆจะจัดสรรทรัพยากรและบริการให้ตรงกับความต้องการของผู้ใช้ ระบบสามารถเพิ่มหรือลดจำนวนของทรัพยากร รวมถึงเสนอบริการที่เหมาะสมให้กับผู้ใช้ได้ตลอดเวลา บริการหลักๆ ประกอบด้วย

***3.1 SaaS**: Software-as-a-Service* (5) คือ การให้บริการซอฟต์แวร์หรือแอพพลิเคชั่น แก่ผู้ใช้งานในรูปแบบของบริการผ่านทางเว็บบราวเซอร์ โดยที่ผู้ใช้ไม่ต้องติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ของตัวเอง เช่น Hotmail, Gmail, Google doc เป็นต้น

***3.2 PaaS**: Platform-as-a-Service* คือ การให้บริการแพลตฟอร์มที่รองรับการทำงานของแอพพลิเคชันโดยผู้ใช้บริการสามารถปรับใช้และจัดการได้เอง PaaS นั้นประกอบด้วยระบบปฏิบัติการ ระบบฐานข้อมูล และ Middleware Systems เช่น Window Server, Linux, Database และ Google App Engine เป็นต้น

***3.3 IaaS**: Infrastructure-as-a-Service* (9) คือ การให้บริการโครงสร้างพื้นฐานสำหรับประมวลผลและการจัดเก็บข้อมูล เช่น ความเร็ว หน่วยความจำ ฮาร์ดดิสก์ ในรูปแบบเสมือน ทำให้สามารถจัดสรรทรัพยากรคอมพิวเตอร์ได้ยืดหยุ่น เช่น Amazon Elastic Cloud (EC2), SunGrid และ Gogrid เป็นต้น จากรูปที่ 2 (a) IaaS (Network architects) เป็นผู้จัดเตรียมทรัพยากรสำหรับประมวลผล และสนับสนุนการทำงานทั้ง PaaS และ SaaS, สำหรับ PaaS (Application developers) เป็นผู้จัดเตรียมเครื่องมือในการพัฒนาระบบให้กับ SaaS (End users)

3. ชนิดของการประมวลผลกลุ่มเมฆ

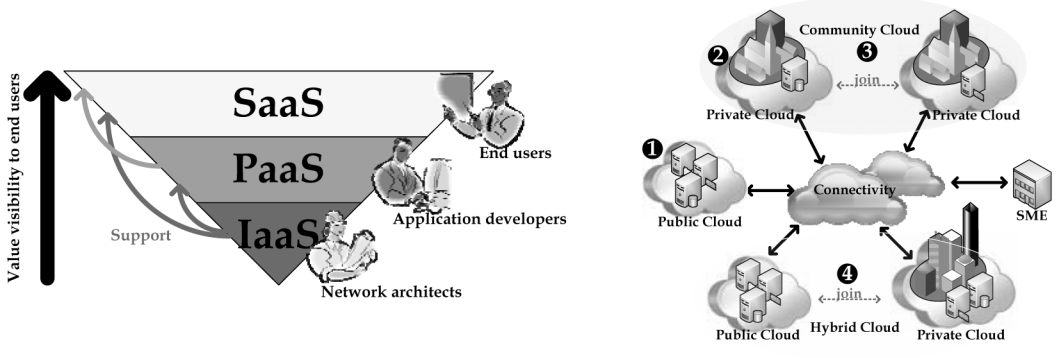
แบ่งเป็น 4 ชนิดหลักๆ คือ Public, Private, Community และ Hybrid ซึ่งแสดงในรูปที่ 2 (b)

1. Public cloud/External cloud (4, 10-12) มีทรัพยากรเป็นสาธารณะ สามารถเปิดเผยข้อมูลออกสู่สาธารณะได้ ผู้ให้บริการเป็นผู้ดูแลระบบ ให้บริการการแบ่งปันทรัพยากรและยูทีลิตี้ขั้นพื้นฐานผ่านทางเครือข่ายอินเทอร์เน็ต เว็บแอพพลิเคชัน หรือเว็บเซอร์วิสซ์ เหมาะสำหรับผู้ใช้งานทั่วๆไป

2. Private cloud/Internal ผู้ใช้บริหารจัดการระบบเอง โดยจำลองกลุ่มเมฆขึ้นมาใช้งานในเน็ตเวิร์คส่วนตัว ไม่เปิดเผยข้อมูลออกสู่สาธารณะ ข้อมูลมีความมั่นคงและเชื่อถือได้ในระดับหนึ่ง นิยมใช้ในภาครัฐ และองค์กรที่ไม่ต้องการเปิดเผยข้อมูล

3. Community Cloud เกิดขึ้นจากความร่วมมือกันระหว่างองค์กรหรือบริษัท โดยตกลงแบ่งปันทรัพยากรบางส่วนร่วมกัน เช่น ฮาร์ดแวร์ ซอฟต์แวร์ มาตรการความมั่นคง สิทธิต่างๆ ค่าใช้จ่ายสูงกว่าแบบ Public เล็กน้อย แต่ต่ำกว่าแบบ Private มาก

4. Hybrid Cloud เกิดขึ้นระหว่างผู้ให้บริการแบบ Public และ Private สามารถเปิดเผยข้อมูลบางส่วนได้ ผู้ใช้งานส่วนใหญ่เป็นบริษัทเอกชน



(a) ประเภทของบริการ (b) ชนิดของ Cloud

รูปที่ 2. ประเภทของการบริการและชนิดของการประมวลผลกลุ่มเมฆ

4. ความเสี่ยงของการประมวลผลกลุ่มเมฆ

จากงานวิจัยของ Mariana และคณะ (4) พบว่าความเสี่ยงที่เกิดขึ้นกับเทคโนโลยีกลุ่มเมฆอันดับ 1 คือ ความเสี่ยงที่เกิดจากความมั่นคง (Security) อันดับ 2 คือ การใช้งานแอพพลิเคชันจากบุคคลที่สาม (Third-party) อันดับ 3 คือ มาตรฐานการบริหารจัดการและการควบคุม ตามลำดับ ผลวิจัยสรุปว่าปัจจัยที่ส่งผลให้เกิดความเสี่ยงสูงสุดคือ *ข้อมูลและทรัพยากรสำหรับประมวลผลอยู่บนโครงสร้างของกลุ่มเมฆที่แบ่งปันกันใช้งาน* ถ้าผู้ให้บริการมีมาตรการควบคุมการรักษาความมั่นคงที่ไม่รัดกุมเพียงพอ จะเสี่ยงต่อการเกิดรูรั่วหรือช่องโหว่ในระบบขึ้นได้ง่าย ส่งผลให้เกิดความไม่ปลอดภัยอื่นๆ ตามมา เช่น สูญเสียความเป็นส่วนตัว ไม่สามารถระบุเอกลักษณ์ตัวบุคคลได้ การยืนยันตัวบุคคลล้มเหลว เป็นต้น นอกจากที่กล่าวมาแล้วยังมีความเสี่ยงด้านอื่นๆ ที่เกี่ยวข้องทางอ้อม เช่น ข้อตกลงทางด้านบริการ (Service Level Agreement: SLA) ที่ไม่ชัดเจน และการใช้งานแอพพลิเคชัน Third-party ซึ่งทั้งสองหัวข้อจะส่งผลตามมา เช่น การล็อกอินเข้าสู่ระบบอย่างไม่ถูกต้อง ประสิทธิภาพในการให้บริการ (Quality of Service) ลดลง เป็นต้น จากตารางที่ 1 แสดงลำดับความเสี่ยงบนเทคโนโลยีกลุ่มเมฆ

ตารางที่ 1. แสดงลำดับความเสี่ยงของเทคโนโลยีการประมวลผลกลุ่มเมฆ (4)

หัวข้อความเสี่ยง	เสี่ยงที่สุด	เสี่ยงปานกลาง	เสี่ยงน้อยที่สุด
ความมั่นคงของข้อมูล (Information security)	91.7%	8.3%	0.0%
การบริหารจัดการขั้นตอนการดำเนินงาน (Operations management)	41.7%	58.3%	0.0%
การบริหารความเปลี่ยนแปลง (Change management)	41.7%	50.0%	8.3%
การวางแผนรับมือภัยพิบัติและการกู้คืนระบบ (Disaster recovery/ business continuity planning)	66.7%	33.3%	0.0%
การบริหารจัดการ Third-party และการจัดลำดับการให้บริการ (Third-party/service level management)	41.7%	14.7%	16.7%
การบริหารจัดการส่วนเชื่อมต่อ (Interface management)	8.3%	50.0%	41.7%
ระเบียบและกฎหมาย (Regulations and legislation)	33.3%	41.7%	25.0%

จากตารางที่ 1 แบ่งความเสี่ยงออกเป็น 3 ระดับ คือ เสี่ยงสูงสุด เสี่ยงปานกลาง และเสี่ยงน้อยสุด โดยความเสี่ยงสูงสุดหมายถึง ระบบไม่ปลอดภัยอย่างยิ่ง ความเสี่ยงปานกลางหมายถึง ระบบจะไม่ปลอดภัย และความเสี่ยงน้อยที่สุดหมายถึง ระบบจะไม่ปลอดภัย แต่มีผลกระทบเพียงเล็กน้อยเท่านั้น จากตัวอย่างในตาราง ความมั่นคงของข้อมูล (Information security) ปรากฏว่ามีระดับความเสี่ยงสูงสุด 91.7% ความเสี่ยงปานกลาง 8.3% และเสี่ยงน้อยสุด 0.0% แสดงให้เห็นว่า ถ้าผู้ให้บริการละเลยความมั่นคงจะทำให้ระบบไม่มีความน่าเชื่อถือเลย เช่นเดียวกับการวางแผนรับมือภัยพิบัติและการกู้คืนระบบ ข้อมูลอาจจะเสียหายแบบถาวรได้ ประเด็นที่น่าสนใจคือ ความเสี่ยงจากการบริหารจัดการ Third-party และการจัดลำดับการให้บริการวัดความเสี่ยงได้ 41.7%(เสี่ยงสูงสุด) 14.7% และ 16.7% ตามลำดับ แสดงให้เห็นว่าถ้าผู้ให้บริการพึ่งแอพพลิเคชันของบุคคลที่สามมากเกินไปจะส่งผลให้ระบบขาดความน่าเชื่อถือ ข้อมูลในตาราง 1 จะช่วยให้ผู้ให้บริการวางแผนในการรับมือกับความมั่นคงที่จะเกิดขึ้นจากความเสี่ยงเหล่านี้ได้อย่างถูกต้องและทันเวลา

5. การจัดกลุ่มความเสี่ยงบนการประมวลผลกลุ่มเมฆ

สามารถจัดกลุ่มความเสี่ยงได้ทั้งหมด 11 กลุ่ม ดังต่อไปนี้ (13)

ความเสี่ยงกลุ่มที่ 1: *ความเสี่ยงทางด้านกายภาพ* (13) โครงสร้างการเชื่อมต่อทางกายภาพของกลุ่มเมฆต้องแบ่งปันกัน โดยใช้ฮาร์ดแวร์ร่วมกับบริษัทอื่นๆ ซึ่งจะเกิดความเสี่ยงมากถ้าผู้ใช้รายอื่นๆ สั่งประมวลผลซอฟต์แวร์ที่เป็นอันตราย ซึ่งจะส่งผลกระทบกับระบบโดยรวม

ความเสี่ยงกลุ่มที่ 2: *ความสูญเสียหรือการเสี่ยงต่อการเปิดเผยของข้อมูลของผู้ใช้* การละเมิดลิขสิทธิ์หรือทำผิดกฎหมายของผู้ใช้รายอื่นๆ เจ้าหน้าที่ของรัฐจำเป็นต้องยึดของกลางไว้ทั้งหมด ผู้ใช้รายอื่นๆ อาจจะถูกตรวจค้นข้อมูลไปด้วย ถ้าไม่มีกฎหมายเกี่ยวกับการสร้างมโนภาพ (Visualization) มารองรับ

ความเสี่ยงกลุ่มที่ 3: *ความเสี่ยงจากการสูญเสียข้อมูลเนื่องจากการเข้ากันไม่ได้ระหว่างหน่วยจัดเก็บข้อมูลที่ต่างกัน* หน่วยเก็บข้อมูลจากผู้ผลิตที่ต่างกันไม่สามารถทำงานร่วมกันได้ ยกตัวอย่างเช่น ข้อมูลจาก Microsoft Cloud ไม่สามารถโอนย้ายไปจัดเก็บกับ Google

Cloud ได้ (14)

ความเสี่ยงกลุ่มที่ 4: *ความเสี่ยงด้านระบบการเข้ารหัสและถอดรหัสข้อมูล* โดยปกติการทำธุรกรรมอิเล็กทรอนิกส์อย่างปลอดภัย จำเป็นต้องมีการเข้ารหัสข้อมูล การควบคุมการเข้ารหัสและถอดรหัสจะอยู่บนกลุ่มเมฆ ซึ่งเสี่ยงต่อการถูกขโมย (ควรจะเป็นหน้าที่ของผู้ใช้บริการในการเข้าและถอดรหัส)

ความเสี่ยงกลุ่มที่ 5: *ความเสี่ยงที่เกิดจากการรับส่งข้อมูล* การประมวลผลข้อมูลบนกลุ่มเมฆ จำเป็นต้องอาศัยการส่ง/รับข้อมูลผ่านเน็ตเวิร์คทั้งหมด ดังนั้นกลุ่มเมฆแบบ Public จะมีความเสี่ยงมากต่อการถูกดักจับ ปัจจุบันยังคงใช้มาตรการรักษาความมั่นคงผ่านเว็บบราวเซอร์เป็นหลัก

ความเสี่ยงกลุ่มที่ 6: *ความเสี่ยงจากการสูญเสียทรัพย์* ธุรกรรมบางจำพวกที่ต้องเกี่ยวข้องกับการเงิน เช่น บัตรเครดิต หรือ PCI DSS ผู้ให้บริการต้องดำเนินการให้ถูกต้องตามกฎหมาย มิเช่นนั้นจะทำให้ผู้ใช้บริการเสียทรัพย์ได้

ความเสี่ยงกลุ่มที่ 7: *ความเสี่ยงจากการปรับปรุงระบบ* ระบบที่ถูกปรับปรุงแล้วจะส่งผลกระทบกับแอพพลิเคชันที่เคยทำงานอยู่หรือไม่ บางบริการต้องปรับปรุงให้ทันสมัยอยู่เสมอ เช่น ฐานข้อมูลไวรัส ถ้าไม่ปรับปรุงก็จะเกิดผลเสียเช่นกัน และบางครั้งซอฟต์แวร์ป้องกันไวรัสก็ทำลายข้อมูลได้เหมือนกัน

ความเสี่ยงกลุ่มที่ 8: *ความเสี่ยงเนื่องจากนโยบายของรัฐ* บางประเทศมีกฎหมายบังคับในการจัดเก็บข้อมูล เช่น ข้อมูลด้านการเงินต้องเก็บไว้เป็นความลับ ถ้าข้อมูลดังกล่าวปรากฏอยู่บนกลุ่มเมฆ อาจจะผิดต่อกฎหมาย หรือบางธนาคารออกกฎว่าข้อมูลลูกค้าต้องเก็บในประเทศที่ตนเองอาศัยอยู่เท่านั้น

ความเสี่ยงกลุ่มที่ 9: *ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของเครื่องจักรเสมือน (Virtual Machine: VM)* การประมวลผลกลุ่มเมฆต้องใช้ VM จำลองฮาร์ดแวร์ที่มีอยู่จริงไปเป็นฮาร์ดแวร์เสมือน เพื่อต้องการความไม่ขึ้นต่อฮาร์ดแวร์ใดๆ เมื่อมีการปรับปรุง VM อาจส่งผลกระทบให้ข้อมูลเดิมเปลี่ยนสภาพ สูญเสียความมั่นคง และยากต่อการตรวจสอบภายหลัง

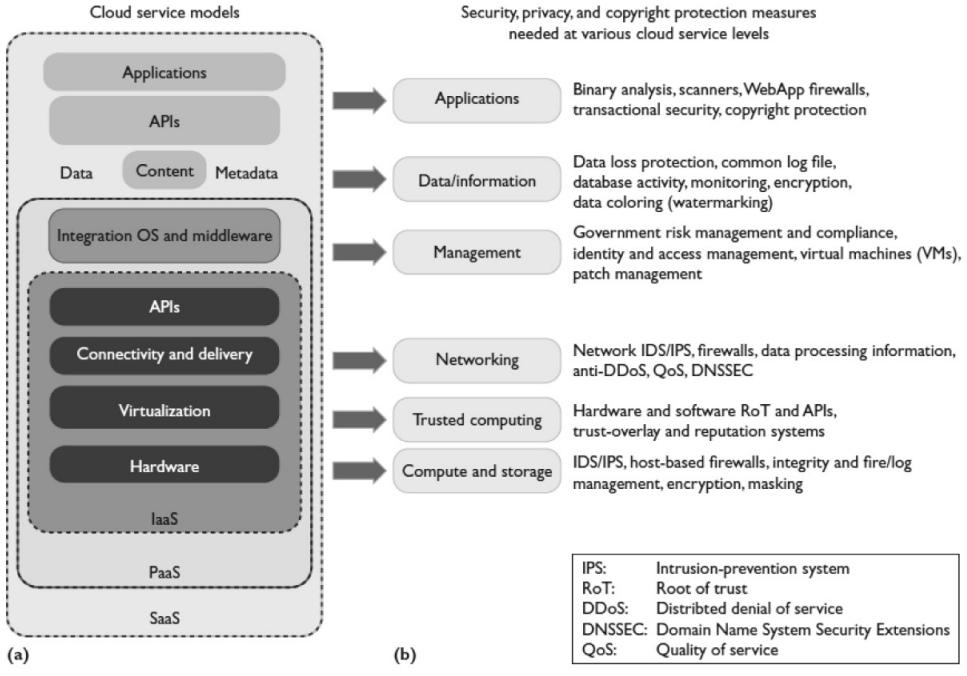
ความเสี่ยงกลุ่มที่ 10: *ความเสี่ยงจากการถูกเปิดเผยข้อมูลส่วนบุคคล* แม้ว่าปัจจุบันมีกฎหมายรองรับเรื่องความมั่นคงของข้อมูลผู้ใช้แล้ว แต่ก็มีบางกรณีที่ผู้ใช้เกิดความไม่มั่นใจว่าข้อมูลของตนที่ถูกประมวลผลบนกลุ่มเมฆ จะไม่ถูกนำไปใช้ หรือส่งต่อไปให้ผู้อื่น เนื่องจากข้อมูลถูกดูแลจากผู้ให้บริการ สำหรับข้อมูลที่ถือว่าเป็นข้อมูลสิทธิส่วนบุคคล เช่น ชื่อ ที่อยู่ วันเกิด จังหวัด ประเทศ ศาสนา สัญชาติ สุขภาพ เพศ สถานภาพการทำงาน ข้อมูลทางการเงิน ข้อมูลทางด้านการแพทย์ ข้อมูลที่เก็บบันทึกในเครื่องคอมพิวเตอร์ มือถือ คอมพิวเตอร์พกพา หมายเลขไอพี เป็นต้น

ความเสี่ยงกลุ่มที่ 11: *ความเสี่ยงของการสร้างมโนภาพ (Visualization)* จากงานวิจัยของ Mariana (15) และคณะ พบว่าความเสี่ยงที่เกิดจาก Visualization มีผลกระทบกับกลุ่มเมฆหลายประเด็น รายละเอียดเกี่ยวกับมาตรการลดความเสี่ยงของ Visualization สามารถดูได้จากตารางที่ 2 (j)

6. กรอบการรักษาความมั่นคงบนการประมวลผลกลุ่มเมฆ

หัวข้อนี้จะกล่าวถึงกรอบการรักษาความมั่นคงบนกลุ่มเมฆ เพื่อให้เห็นภาพรวมของการรักษาความมั่นคงก่อนที่จะเจาะลึกลงในรายละเอียดในทางปฏิบัติต่อไป จากรูปที่ 3 (16) แสดงมาตรการรักษาความมั่นคงในระดับต่างๆ ของเทคโนโลยีกลุ่มเมฆ ด้านซ้าย (a) แสดงประเภทของบริการต่างๆบนกลุ่มเมฆ ประกอบด้วย 3 ส่วนหลักๆ คือ IaaS, PaaS และ SaaS (17) ส่วนทางด้านขวามือ (b) แสดงมาตรการรักษาความมั่นคงในแต่ละบริการ จากรูปแบ่งออกเป็น 3 ระดับคือ ระดับนอกสุดเป็นส่วนของ SaaS ซึ่งประกอบไปด้วย Applications, APIs, Data, Content, Metadata สำหรับ Applications, APIs และ Content ซึ่งเรียกรวมกันว่า Applications จะใช้เทคนิคในการป้องกันด้านความมั่นคงหลายชนิด เช่น ใช้ซอฟต์แวร์ค้นหาความผิดปกติของโปรแกรมในระดับบิตข้อมูล ซอฟต์แวร์ค้นหาช่องโหว่ ไฟล์วอลล์ที่ทำงานระดับแอพพลิเคชัน ซอฟต์แวร์ตรวจสอบการ

เชื่อมต่อ และควบคุมลิขสิทธิ์ซอฟต์แวร์ เป็นต้น ส่วน Data และ Metadata รวมเรียกว่า Data หรือ Information จะมีมาตรการป้องกันข้อมูลสูญหาย การเก็บรักษาไฟล์บันทึกการทำงาน การเฝ้าระวังกิจกรรมต่างๆ บนฐานข้อมูล การเฝ้าระวังระบบ การเข้ารหัสข้อมูล และการทำลายน้ำข้อมูล (Watermarking) เป็นต้น ระดับที่ 2 คือ PaaS มีหน้าที่เตรียมสภาพแวดล้อมและทรัพยากรที่เหมาะสมสำหรับให้ผู้ใช้สร้างแอพพลิเคชันของตนเอง เช่น Java, Python หรือ .Net เป็นต้น มาตรการการดูแลเรียกว่า Management ซึ่งเตรียมมาตรการเรื่องความเสี่ยงและมาตรฐานต่างๆ ที่จำเป็นบนกลุ่มเมฆ กำหนดสิทธิ์การเข้าใช้งาน รวมถึงการอุดรอยรั่วของระบบด้วยการแพตช์ (Patch) ระดับสุดท้ายคือ IaaS มีหน้าที่ดูแลโครงสร้างทางกายภาพ ระบบปฏิบัติการ เครื่องจักรเสมือน และการเชื่อมต่อของกลุ่มเมฆ ป้องกันระบบเครือข่าย เช่น การติดตั้ง IDS/IPS ไฟล์วอลล์ การป้องกันการโจมตีในรูปแบบต่างๆ เช่น DDos และดูแลคุณภาพการรับส่งข้อมูลในเครือข่าย (QoS) เป็นต้น รวมไปถึงการเตรียมการสำรองข้อมูล แกะรอยและป้องกันการโจมตี ตรวจสอบความถูกต้องของข้อมูล ตรวจสอบและวิเคราะห์ log file เข้ารหัสและถอดรหัสข้อมูล เป็นต้น



รูปที่ 3. มาตรการรักษาความมั่นคงในระดับต่างๆ ของเทคโนโลยีกลุ่มเมฆ

7. มาตรฐานการรักษาความมั่นคงสากล

ในส่วนนี้จะกล่าวถึงมาตรฐานความมั่นคงสากล ที่ใช้กับเทคโนโลยีกลุ่มเมฆ (13)

1. ITIL-process Security Management จะอธิบายเกี่ยวกับการจัดการโครงสร้างในการรักษาความมั่นคงที่เหมาะสมสำหรับองค์กร

2. ISO IEC 27001/27002 ใช้เป็นเกณฑ์ในการตรวจรับรองความมีมาตรฐานของระบบบริหารความมั่นคงของข้อมูล

3. Open Virtualization Format (OVF) เป็นมาตรฐานสำหรับการสร้างเครื่องจักรเสมือน (VM) ให้สามารถข้ามแพล็ตฟอร์ม (Platform)ได้

8. โมเดลการจัดการความมั่นคงบนเทคโนโลยีกลุ่มเมฆ

ในหัวข้อนี้จะอธิบายถึงโมเดลการจัดการความมั่นคงที่ผู้ให้บริการ (Cloud Service Provider: CSP) ต้องพิจารณาและจัดเตรียม ในทางกลับกันผู้ใช้ที่ต้องการใช้งานก็สามารถสำรวจได้ว่ามีมาตรการต่างๆ เหล่านี้มีอยู่บนกลุ่มเมฆหรือไม่ เพื่อสร้างความมั่นใจด้วยกันทั้งสองฝ่าย ซึ่งมีหัวข้อดังต่อไปนี้

1. SaaS security ก่อนผู้ใช้จะตกลงเช่าและรับบริการซอฟต์แวร์หรือแอพพลิเคชั่นบนกลุ่มเมฆ Gartner (18) แนะนำว่าผู้ใช้จำเป็นต้องตรวจสอบความเสี่ยงทั้ง 7 ข้อนี้ก่อนเสมอ ดังนี้

1.1 สิทธิในการเข้าถึงข้อมูล สอบถามผู้ให้บริการถึงสิทธิการเข้าถึงข้อมูล มาตรการในการบริหารจัดการข้อมูล (หรือดูจากประกาศของผู้ให้บริการ เรียกว่า SLA) เป็นต้น

1.2 ปฏิบัติตามกฎการรักษาความมั่นคงอย่างเคร่งครัด สำหรับผู้ใช้ต้องตระหนักถึงหน้าที่ในการดูแลรักษาความมั่นคงข้อมูลของตนเอง สำหรับผู้ให้บริการต้องผ่านการตรวจสอบความมั่นคงจากหน่วยงานที่ทำหน้าที่ตรวจสอบ เช่น external audit และควรได้รับการรับรองมาตรฐาน ต้องไม่ปฏิเสธความรับผิดชอบเมื่อข้อมูลผู้ใช้เสียหาย

1.3 ตำแหน่งที่ตั้งการจัดเก็บข้อมูล ตามหลักการของกลุ่มเมฆ ผู้ใช้ไม่จำเป็นต้องรู้ที่ตั้งของระบบกลุ่มเมฆ แต่ในความเป็นจริงผู้ใช้ควรสอบถามผู้ให้บริการว่า ที่ตั้งที่สามารถอ้างอิงได้อยู่ที่จุดใด เนื่องจากกฎหมายอาจระบุให้เก็บข้อมูลในเมืองที่ตนเองอาศัยอยู่เท่านั้น

1.4 คัดแยกข้อมูล ต้องมีมาตรการรองรับการคัดแยกข้อมูลของผู้ใช้แต่ละรายอย่างชัดเจน เพื่อสร้างความมั่นใจให้ผู้ใช้ว่าข้อมูลต่างๆ ที่อยู่บนกลุ่มเมฆจะไม่ถูกละเมิด หรือประมวลผลโดยผู้ที่ไม่ใช่เจ้าของ รวมถึงมีมาตรการเข้ารหัสที่มีประสิทธิภาพรองรับด้วย

1.5 การกู้คืน การล้มเหลวจากเหตุการณ์ดังต่อไปนี้ เช่น แผ่นดินไหว น้ำท่วม การก่อการร้าย เป็นต้น เป็นสาเหตุให้ระบบกลุ่มเมฆไม่สามารถทำงานต่อได้ ดังนั้นผู้ใช้จะต้องสอบถามผู้ให้บริการว่า เมื่อระบบล่มข้อมูลเหมือนเดิมหรือไม่ และต้องใช้เวลาเท่าไหร่ในการกู้คืน

1.6 สนับสนุนการสืบสวน ถ้ามีการกระทำความผิดกฎหมายบนระบบกลุ่มเมฆ ผู้ให้บริการต้องสามารถตรวจสอบร่องรอยผู้ที่กระทำความผิดได้ แต่ในความเป็นจริงนั้นค่อนข้างทำได้ลำบากเนื่องจากการแกะรอย จะตรวจสอบจาก log file ซึ่งในกลุ่มเมฆ ผู้ใช้มีจำนวนมากทำให้ log file ใหญ่ แยกแยะลำบาก และอาจจะเก็บ log ข้ามไซต์

1.7 อายุในการใช้งาน มีโอกาสเป็นไปได้เมื่อบริษัทขนาดเล็กหรือมีผลกำไรน้อยจะไม่สามารถดำเนินธุรกิจต่อไปได้ จะถูกบริษัทขนาดใหญ่กว่าถือครองบริษัทแทน (Take over) หรือร่วมหุ้น ข้อมูลของผู้ใช้จะต้องคงอยู่ โดยไม่หายไปกับผู้ให้บริการรายเดิม

2. การจัดการความมั่นคง ต้องมีแผนการบริหารจัดการด้านความมั่นคงที่ชัดเจน และสอดคล้องกับกลยุทธ์ขององค์กร เพื่อป้องกันการสับสนเกี่ยวกับหน้าที่ของบุคลากร

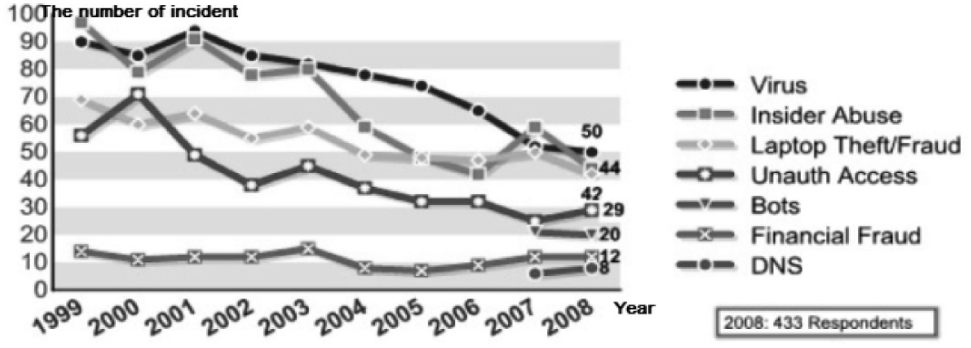
3. การกำกับดูแลการรักษาความมั่นคง ควรจัดตั้งคณะกรรมการทำงานด้านการรักษาความมั่นคง เพื่อวางนโยบายด้านไอที ความเสี่ยง กำหนดบทบาทหน้าที่ และคอยกำกับดูแลการดำเนินงานด้านความมั่นคงให้สอดคล้องกับแผนขององค์กรที่กำหนดไว้

4. การบริหารความเสี่ยง ดูแล ตรวจสอบ และควบคุมความเสี่ยงที่สัมพันธ์กับกิจกรรม หน้าที่และกระบวนการทำงาน เพื่อให้องค์กรลดความเสียหายจากความเสี่ยงมากที่สุด อันเนื่องมาจากภัยที่องค์กรต้องเผชิญในช่วงเวลาใดเวลาหนึ่งหรือเรียกว่า อุบัติภัย (Accident)

5. การประเมินความเสี่ยง การวิเคราะห์ช่องโหว่ ตรวจสอบและทดสอบความมั่นคงของระบบ ช่องโหว่ที่เกิดขึ้นในระบบสารสนเทศ ป้องกันการขโมย แก้ไขหรือทำลายข้อมูลอันมีค่าขององค์กร และลดโอกาสการเกิดความเสียหายแก่ระบบไอทีภายในองค์กร

6. การตระหนักถึงความมั่นคง คือ องค์ความรู้ และทัศนคติของสมาชิกทุกคนในองค์กรที่พึงมี เกี่ยวกับการป้องกันรักษาความมั่นคงทางเทคโนโลยีของ

องค์กร โดยเฉพาะอย่างยิ่งคือทรัพย์สินทางด้านข้อมูลขององค์กร เช่น การถูกดักจับข้อมูล ไวรัสคอมพิวเตอร์ การเจาะระบบ การไม่ยืนยันตัวตน เป็นต้น จากการรายงานอาชญากรรมทางด้านอินเทอร์เน็ตปี 2008 (19) มีการร้องเรียนเกี่ยวกับกระทำผิดกฎหมายทางอินเตอร์เน็ตรวม 2006,884 ราย พบว่าภัยคุกคามที่สูงสุดคือ อันดับที่ 1 คือ ไวรัส การละเมิดสิทธิ์ภายในองค์ ทรัพย์สินและการยักยอก ตามลำดับดังรูปที่ 4



รูปที่ 4. สถิติการกระทำผิดทางอาชญากรรมอินเตอร์เน็ต (สำรวจปี 2008)

7. การให้ความรู้และการอบรม มีโปรแกรมการจัดอบรมให้ความรู้เกี่ยวกับการรักษาความมั่นคงเกี่ยวกับไอทีให้กับบุคลากรทุกคนได้รู้และตระหนักเกี่ยวกับเรื่องดังกล่าว ซึ่งหัวข้อที่เป็นพื้นฐานในการอบรมควรเกี่ยวข้องกับเรื่องต่างๆ ดังนี้ เช่น ความรู้พื้นฐานด้านความมั่นคง ความเสี่ยงที่จะเกิดขึ้นกับไอที และแนวทางแก้ไขปัญหาเบื้องต้น เป็นต้น

8. นโยบายและการวางมาตรฐานความมั่นคง วางกฎและระเบียบด้านความมั่นคงตั้งแต่ต้นก่อนจะพัฒนาระบบใดๆ ขึ้นมาใช้งาน สำหรับกลุ่มเมฆนั้น ผู้ให้บริการจะต้องแสดงเอกสารเกี่ยวกับความมั่นคงของซอฟต์แวร์ที่ใช้ ขั้นตอนการพัฒนาหรือใช้งานซอฟต์แวร์บนกลุ่มเมฆ ข้อแนะนำในการใช้งาน กฎเกณฑ์ต่างๆ ที่จำเป็น

9. การบริหารความเสี่ยง Third party เมื่อผู้ให้บริการจำเป็นต้องใช้ Third party ควรต้องศึกษาถึงข้อกำหนด ความสามารถ และข้อจำกัดเกี่ยวกับผลิตภัณฑ์ให้ดีเสียก่อนใช้งาน

10. การสำรวจช่องโหว่ของระบบ หมายถึง การบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากช่องโหว่ต่างๆ ของระบบสารสนเทศ ควรดำเนินการอยู่ตลอดเวลา หรือบ่อยที่สุดเท่าที่จะทำได้

11. การทดสอบความมั่นคงของอิมเมจ เทคโนโลยีกลุ่มเมฆ จำเป็นต้องใช้เครื่องจักรเสมือน ซึ่งมีความสามารถจำลองโครงสร้างฮาร์ดแวร์ใหม่ได้ไม่จำกัด โดยเก็บไว้ในรูปของอิมเมจ (Image) เมื่อจำเป็นต้องปรับแต่งระบบ เช่น การปรับปรุงซอฟต์แวร์โดยการแพตช์ (Patch software) สามารถกระทำผ่านอิมเมจได้โดยตรง เมื่อปรับแต่งเสร็จควรทดสอบความมั่นคงก่อนการใช้งานจริง

12. การธรรมาภิบาลทางข้อมูล คือระเบียบปฏิบัติในการควบคุมคุณภาพของวิธีการจัดการข้อมูล การใช้ข้อมูล การปรับปรุงข้อมูลให้ดีขึ้น รวมถึงการปกป้องข้อมูลขององค์กร โดยอาศัยทั้งบุคคล กระบวนการ และเทคโนโลยีเข้ามาช่วยเพื่อเปลี่ยนแปลงวิธีจัดการข้อมูลขององค์กรให้มีระเบียบชัดเจน ตรวจสอบได้ คำนึงถึงความมั่นคง และความเป็นส่วนตัว

13. ความมั่นคงของข้อมูล เป็นการป้องกันผู้ไม่มีสิทธิ์เข้าใช้หรือแก้ไขข้อมูล การควบคุมการเรียกใช้ข้อมูลเดียวกันในเวลาพร้อมๆ กัน รวมถึงการรักษาความถูกต้องครบถ้วนสมบูรณ์ของข้อมูล โดยมีวัตถุประสงค์เพื่อ รักษาความลับของข้อมูล ข้อมูลมีความถูกต้องสมบูรณ์ มีข้อมูลพร้อมใช้งานเสมอ และลดความเสี่ยง

14. ความมั่นคงของแอพพลิเคชัน เป็นการป้องกันจุดอ่อนที่เกิดจากความรู้เท่าไม่ถึงการณ์ของผู้

พัฒนาซอฟต์แวร์ ทำให้ซอฟต์แวร์มีช่องช่องโหว่ต่าง ๆ เกิดขึ้น ที่พบบ่อยในเว็บแอพพลิเคชั่น เช่น SQL Injection, Cross-Site Scripting (XSS), Unvalidated Input เป็นต้น

15. ความมั่นคงเครื่องจักรเสมือน รายละเอียดสามารถดูได้จากตารางที่ 2 (j)

16. การจัดการการเข้าถึงข้อมูลเฉพาะตัว เป็นมาตรการความมั่นคงที่สร้างความมั่นใจให้กับผู้ใช้ บริการ โดยผู้ใช้ควรได้รับสิทธิ์เท่าที่มี ในเวลาที่เหมาะสมเท่านั้น

17. การบริหารการเปลี่ยนแปลง หมายถึง การขับเคลื่อนองค์กรในระยะเปลี่ยนผ่านไปสู่ขีดความสามารถที่จำเป็นต่อการรับมือกับสถานการณ์ที่แตกต่างจากอดีต

18. การรักษาความมั่นคงทางกายภาพ หมายถึง มาตรการที่ใช้ในการปกป้องทรัพยากรจากภัยคุกคามทางกายภาพทั้งโดยเจตนาและไม่เจตนา ซึ่งเป็นหนึ่งในวิธีที่ช่วยลดความเสี่ยงด้านความมั่นคง โดยการจำกัดให้เฉพาะผู้ที่จำเป็นต้องใช้งานเท่านั้น เช่น มาตรการในการเข้าห้องเครือข่ายจำเป็น ต้องมีการแสกนลายนิ้วมือ การติดกล้องวงจรปิด เป็นต้น

19. การเตรียมแผนงานในการกู้ระบบและข้อมูลจากภัยพิบัติ ต้องมีกระบวนการสำรองและกู้คืนระบบได้อย่างรวดเร็ว ทำให้องค์กรยังสามารถปฏิบัติงานต่อไปได้ โดยมีผลกระทบน้อยที่สุด

20. การรักษาความเป็นส่วนตัว มีนโยบายการคุ้มครองข้อมูลส่วนบุคคล เพื่อสร้างความมั่นใจให้กับผู้ใช้บริการในการทำพาณิชย์อิเล็กทรอนิกส์หรือธุรกรรมทางอิเล็กทรอนิกส์

9. แนวทางการรับมือความเสี่ยงและความไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆในทางปฏิบัติ

ในส่วนนี้จะกล่าวถึงเทคนิควิธีในการรับมือความเสี่ยงและความไม่ปลอดภัยทั้งหมดที่อาจจะเกิดขึ้นบนเทคโนโลยีกลุ่มเมฆ ซึ่งสามารถจำแนกออกเป็น 5 กลุ่มใหญ่ๆ คือ

1. การรับมือกับความเสี่ยงด้านการรักษาความมั่นคงของข้อมูล การบริหาร และการควบคุม ควรปฏิบัติตามคำแนะนำตามตารางที่ 2 (a) สำหรับการสูญเสียการควบคุมข้อมูลและแอพพลิเคชันที่อยู่บนกลุ่มเมฆให้ปฏิบัติตามคำแนะนำ (b) ความพร้อมของข้อมูลและบริการ ปฏิบัติตามคำแนะนำ (c) ความเสี่ยงด้านความไม่สมบูรณ์ของข้อมูล ปฏิบัติตามคำแนะนำ (d) การขาดประสิทธิภาพในการโอนถ่ายข้อมูลเนื่องจากขบวนการเข้ารหัสไม่ดีพอ ปฏิบัติตามคำแนะนำ (e)

2. การรับมือกับความเสี่ยงด้านการเข้าถึงตามหลักตรรกวิทยา (Logical access) ควรปฏิบัติตามคำแนะนำ ตารางที่ 2 (f)

3. การรับมือกับความเสี่ยงด้านระบบเครือข่าย (Network security) ควรปฏิบัติตามตารางที่ 2 (g)

4. การรับมือกับความเสี่ยงด้านกายภาพ (Physical security) ควรปฏิบัติตามตารางที่ 2 (h)

5. การรับมือกับความเสี่ยงด้านการยอมรับมาตรฐานความมั่นคง (Compliance) ควรปฏิบัติตามตารางที่ 2 (i)

6. การรับมือกับความเสี่ยงด้านโครงสร้างเสมือน (Virtualization) (15) ควรปฏิบัติตามตารางที่ 2 (j)

ตารางที่ 2. มาตรการรับมือจากความเสี่ยงและไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆ

(a) ข้อมูลส่วนบุคคล (Data Privacy) (4)
ความเสี่ยง 1: โครงสร้างของเทคโนโลยีกลุ่มเมฆมีการแบ่งปันทรัพยากรทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์ร่วมกัน ดังนั้นจึงเป็นสาเหตุให้เสี่ยงต่อการเปิดเผยและสูญเสียความเป็นส่วนตัวได้ง่ายขึ้น การเจาะระบบจึงคุ้มค่ามากกว่าเนื่องจากสามารถเข้าถึงข้อมูลของผู้ใช้รายอื่นๆ ด้วย และเนื่องจากโครงสร้างภายใต้กลุ่มเมฆ อาจจะมีการเก็บข้อมูลที่กระจายตัวอยู่ที่ใดก็ได้ ดังนั้นโอกาสที่จะกู้ข้อมูลคืน การโอนย้ายข้อมูลอาจจะเกิดขึ้นผิดพลาดได้ง่ายว่าการเก็บข้อมูลอยู่ในจุดใดจุดหนึ่ง บางส่วนของกลุ่มเมฆ จำเป็นต้องใช้ซอฟต์แวร์ Third-party ช่วยทำงาน ซึ่งอาจจะมีช่องโหว่ได้ง่าย ☑ **การรับมือ:** ผู้ให้บริการจะต้องยืนยันและสร้างความเชื่อมั่นให้กับผู้ใช้โดยการประกาศมาตรการการรักษาความมั่นคงของข้อมูลที่ถูกเก็บอยู่บนกลุ่มเมฆ อย่างชัดเจนว่าบริหารจัดการอย่างไร เป็นไปตามมาตรฐานสากลหรือไม่ ระบุชัดถึงเงื่อนไข และระเบียบการใช้ เช่น วิธีการเข้าถึงข้อมูล เครื่องมือที่ใช้งานบนกลุ่มเมฆ อย่างปลอดภัย เป็นต้น รวมถึงมีทีมงานที่มีความชำนาญ และดำเนินงานตามแผนความมั่นคงที่ตั้งไว้อย่างเคร่งครัด
(b) การควบคุมข้อมูล (Data control)
ความเสี่ยง 1: เทคโนโลยีกลุ่มเมฆจะประสบปัญหาเรื่องการป้องกันข้อมูล ความเป็นส่วนตัว การโจรกรรมข้อมูล และการบังคับใช้กฎการรักษาความมั่นคงต่างๆ เนื่องจากติดเงื่อนไขการแบ่งปันทรัพยากรระหว่างผู้ใช้บนกลุ่มเมฆ และผู้ใช้บริการก็ไม่สามารถควบคุมความมั่นคงของข้อมูลของตนเองได้เต็มที่ด้วย เมื่อมีการกระทำความผิดทางอาชญากรรมบนกลุ่มเมฆ ตามกฎหมายแล้ว ผู้ใช้รายอื่นๆ อาจจะถูกตรวจสอบข้อมูลด้วย ☑ **การรับมือ:** ผู้ให้บริการจะต้องสร้างความมั่นใจกับผู้ใช้บริการ โดยการจัดให้มีผู้เชี่ยวชาญด้านความมั่นคงจากภายนอก (External audit/Third party) มาตรวจสอบขั้นตอนและวิธีการรักษาความมั่นคงของกลุ่มเมฆเป็นระยะๆ พร้อมกับแจ้งให้ผู้ใช้ทราบถึงมาตรการดังกล่าวอย่างต่อเนื่อง
(c) ความพร้อมของข้อมูลและการบริการ (Availability of data and services)
ความเสี่ยง 1: แผนและขั้นตอนในการทดสอบการกู้คืนระบบในกรณีที่เกิดภัยพิบัติเป็นสิ่งที่มีความจำเป็นอย่างยิ่ง เพื่อให้ผู้ใช้มั่นใจว่าข้อมูลของพวกเขาจะไม่สูญหายและสามารถใช้งานได้ตลอดเวลาเมื่อต้องการ ความเสี่ยงอื่นๆ อาจเกิดจากผู้ใช้เผลอลบข้อมูล ข้อมูลถูกโจรกรรม หรือแก้ไข การกู้คืนจึงเป็นสิ่งจำเป็น และในกรณีที่ฉุกเฉินมากๆ การกู้คืนอาจจะจำเป็นต้องมีการกู้คืนตามลำดับความสำคัญของลูกค้าด้วย ☑ **การรับมือ:** ผู้ให้บริการจะต้องมีแผนและขั้นตอนการดำเนินงานในการกู้คืนระบบอย่างเป็นรูปธรรม เพื่อป้องกันข้อมูลสูญหาย การเผลอเลอ ข้อมูลถูกทำลาย การดำเนินงานจะต้องทำอย่างสม่ำเสมอ ทุกขั้นตอนจะต้องได้รับการพิสูจน์ว่าทำงานได้จริง และครบถ้วน ตามเวลาที่กำหนดไว้ ความถี่ของการสำรองข้อมูลขึ้นอยู่กับความสำคัญของข้อมูล **ความเสี่ยง** 2: ปัญหาที่สำคัญประการหนึ่งของผู้ให้บริการกลุ่มเมฆ คือ กิจการอาจจะประสบกับการขาดทุนและจำเป็นต้องล้มเลิกกิจการไปในที่สุด ดังนั้นจึงเกิดความเสี่ยงกับข้อมูลของผู้ใช้บริการ ซึ่งอาจจะจำเป็นต้องย้ายที่เก็บข้อมูลใหม่ ในบางครั้งจะพบปัญหาว่าไม่สามารถย้ายข้อมูลข้ามไปยังผู้ให้บริการรายใหม่ได้ ☑ **การรับมือ:** ผู้ให้บริการจะต้องมีเอกสารแสดงความสามารถและการเข้ากันได้ระหว่างระบบที่มีความแตกต่างกัน เพื่อใช้ในกรณีที่ผู้ใช้บริการต้องการเปลี่ยนจากผู้ให้บริการรายเดิมเป็นรายใหม่ และควรเสนอคุณสมบัติเพิ่มเติมในเรื่องของการสำรองข้อมูล (duplicate) ข้ามไซต์ เพื่อสร้างความมั่นใจให้ผู้ใช้ด้วย

ตารางที่ 2. มาตรการรับมือจากความเสี่ยงและไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆ (ต่อ)

ความเสี่ยง 3: เทคโนโลยีกลุ่มเมฆ จำเป็นอย่างยิ่งที่ต้องประมวลผลผ่านระบบเครือข่ายที่มีความเร็วสูง (ต้องการแบนด์วิดท์มาก) ซึ่งจะส่งผลกับความเร็วของผู้ใช้โดยตรง ถ้าระบบเครือข่ายเกิดความคับคั่ง หรือหนาแน่น ☑ **การรับมือ:** ผู้ใช้ควรพิจารณาเรื่องการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตและขนาดของแบนด์วิดท์ที่สามารถใช้งานได้ก่อนตกลงใช้งานระบบกลุ่มเมฆ พร้อมกับเลือกผู้ให้บริการที่น่าเชื่อถือและเหมาะสมที่สามารถบริหารจัดการด้านระบบเครือข่าย แบนด์วิดท์ การควบคุมความคับคั่ง การยืนยันคุณภาพการบริการ มาตรการเฝ้าระวังเครือข่ายที่มีคุณภาพ และการกระจายโหลดการทำงานที่ดี
(d) ความสมบูรณ์ของข้อมูล (Data integrity)
ความเสี่ยง 1: การเข้าถึงกลุ่มเมฆ ได้จากทุกๆ ที่ ที่เชื่อมต่ออินเทอร์เน็ตได้ เป็นสิ่งที่ดีและสะดวกสำหรับผู้ใช้งาน แต่ในทางกลับกันมันจะนำมาซึ่งความเสี่ยงในการถูกเจาะระบบการทำงานของเครือข่าย แอพพลิเคชัน ฐานข้อมูล และซอฟต์แวร์ ถ้าระบบกลุ่มเมฆ ไม่สามารถปรับแก้ข้อบกพร่อง (patch) ได้ทันเวลา ☑ **การรับมือ:** เป็นหน้าที่หลักอีกหน้าที่หนึ่งของผู้ให้บริการที่จำเป็นต้องมีแผนและวิธีการดำเนินงานเกี่ยวกับการอุดรอยรั่วของระบบให้ทันเวลาก่อนที่จะถูกเจาะระบบ หรือวางแผนในการแก้ไขข้อบกพร่องโดยใช้ซอฟต์แวร์การปรับปรุงแบบอัตโนมัติก็ได้ **ความเสี่ยง** 2: ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงสภาพแวดล้อมหรือโครงสร้างของกลุ่มเมฆ และจำเป็นต้องเปลี่ยนสิทธิ์ในการเข้าถึงข้อมูลและประมวลผลของผู้ดูแลระบบ ซึ่งอาจจะทำให้เกิดผลกระทบต่อความถูกต้องและความสมบูรณ์ของข้อมูลบนกลุ่มเมฆ ☑ **การรับมือ:** เมื่อผู้ให้บริการต้องการปรับปรุงอะไรก็ตามบนกลุ่มเมฆ สิ่งที่ต้องพิจารณาให้รอบครอบคือ เมื่อปรับเปลี่ยนแล้วผลกระทบที่ตามมาจะเกิดอะไรขึ้นบ้าง เช่น การทำงานของระบบจะหยุดชะงักหรือไม่ สิทธิ์ในการประมวลผลและเข้าถึงข้อมูลเปลี่ยนแปลงหรือไม่ เกิดข้อผิดพลาดกับการทำงานของแอพพลิเคชันที่ทำงานหรือไม่ เป็นต้น แนวทางในการปฏิบัติที่ดีที่สุดคือควรจะแยกระบบที่ทำงานจริงออกจากระบบที่ใช้ทดสอบหรือพัฒนาเมื่อระบบที่ใช้สำหรับทดสอบถูกทดสอบการทำงานและแก้ไขจุดปรกพร่องทุกด้านแล้ว จึงค่อยแก้ไขกับระบบจริง **ความเสี่ยง** 3: ระบบกลุ่มเมฆ ที่มีโครงสร้างการทำงานที่ซับซ้อนมากๆ จะมีผลกระทบกับความสมบูรณ์ของข้อมูล ถ้าระบบกลุ่มเมฆ ไม่สามารถจำแนกกลุ่มของผู้ใช้บริการได้ ☑ **การรับมือ:** การคัดแยกประเภทของผู้ใช้บริการเป็นสิ่งที่จำเป็นอันดับต้นๆ สำหรับผู้ให้บริการกลุ่มเมฆ เนื่องจากผู้ใช้แต่ละกลุ่มจะมีสิทธิ์ในการประมวลผลและใช้ข้อมูลที่แตกต่างกัน ซึ่งผู้ให้บริการต้องกำหนดกฎการสร้างรายชื่อผู้ใช้อย่างเหมาะสมและให้ผู้ดูแลระบบปฏิบัติตามกฎอย่างเคร่งครัด สำหรับในทางปฏิบัติสามารถกำหนดได้บน virtual machine หรือ hypervisors
(e) การเข้ารหัสข้อมูล (Data encryption)
ความเสี่ยง 1: ปัญหาหลักอีกประการของกลุ่มเมฆ คือการบริหารจัดการเรื่องการเข้ารหัสข้อมูลและการจัดการกับคีย์ (key) ที่ใช้สำหรับเข้ารหัสไม่ดีพอ เนื่องจากระบบ กลุ่มเมฆ ในสถานการณ์จริงจะมีจำนวนของผู้เช่าจำนวนมาก ทำให้ความเสี่ยงในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งอาจจะส่งผลกระทบกับคีย์ด้วย รวมถึงความเสี่ยงที่อาจจะเกิดจากผู้เจาะระบบ และข้อมูลอาจรั่วไหลเมื่อมีข้อมูลจำนวนมากส่งเข้ามาประมวลผลในกลุ่มเมฆ ผ่านทางเครือข่ายอินเทอร์เน็ต

ตารางที่ 2. มาตรการรับมือจากความเสี่ยงและไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆ (ต่อ)

☑ **การรับมือ:** ผู้ให้บริการต้องจัดเตรียมและควบคุมกระบวนการเข้ารหัสและถอดรหัสตามกฎการรักษาความมั่นคงมาตรฐานสากล เมื่อผู้ใช้ส่งและรับข้อมูลผ่านเครือข่ายอินเทอร์เน็ต คีย์ (public and private key) สำหรับใช้ในการเข้ารหัสจำเป็นต้องใช้จากผู้ผลิตที่เชื่อถือได้ และจำเป็นต้องมีกระบวนการจัดการคีย์ที่มีประสิทธิภาพ เช่น กำหนดที่เก็บของคีย์อย่างปลอดภัย การจัดส่งคีย์ กำหนดสิทธิ์ในการเข้าถึงคีย์เฉพาะบุคคลที่ได้รับสิทธิ์ กำหนดการสำรองคีย์เพื่อป้องกันการสูญหายของคีย์ **ความเสี่ยง** 2: การเลือกเทคนิคการเข้ารหัสที่ล้าหลัง หรือไม่ทันสมัยเพียงพอ จะส่งผลให้ข้อมูลรั่วไหลได้ ☑ **การรับมือ:** ผู้ให้บริการต้องติดตามความเปลี่ยนแปลงและวิวัฒนาการของวิทยาการเข้ารหัสอย่างสม่ำเสมอ และเลือกการเข้ารหัสที่น่าเชื่อถือ และใหม่ที่สุดเท่าที่จะสามารถจัดหาได้มาใช้งาน
(f) การเข้าถึงตามหลักตรรกวิทยา (Logical Access)
ความเสี่ยง 1: จะต้องมีมาตรการเฉพาะสำหรับผู้ดูแลระบบกลุ่มเมฆ เมื่อทำงานผ่านเข้ามาทางเครือข่ายสาธารณะ เพราะเกี่ยวข้องกับสิทธิ์ที่ผู้ดูแลระบบได้รับโดยตรง บนกลุ่มเมฆที่มีลักษณะแบบการบริการด้วยตนเอง (on-demand self-service) จะมีอินเทอร์เฟสให้ผู้ใช้ บริการสามารถบริหารจัดการระบบของตนเองได้เต็มที่ ผู้เจาะระบบสามารถใช้ช่องทางดังกล่าวยึดครองและควบคุมระบบได้ ☑**การรับมือ:** ผู้ให้บริการต้องแสดงให้ผู้ใช้บริการเห็นว่ามาตรการการรักษาความมั่นคงของระบบมีประสิทธิภาพ ป้องกันผู้ที่ไม่มีสิทธิ์ในข้อมูล การเปลี่ยนแปลงข้อมูล และป้องกันข้อมูลถูกทำลาย มีการสอบทวนกฎความมั่นคงอยู่เสมอ เฝ้าระวังการใช้งานและสิทธิ์การเข้าถึง แยกแยะประเภทของผู้ดูแลระบบและสิทธิ์การใช้งานอย่างชัดเจน มีการบันทึก log ในการเข้าระบบ อยู่ในระบบ และออกจากระบบ วางระบบการป้องกันการเจาะระบบ สำหรับการเข้าถึงกลุ่มเมฆ โดยผ่านเครือข่ายสาธารณะต้องใช้เครื่องมือที่ทันสมัยและได้มาตรฐาน เช่น VPN, IPSEC เป็นต้น สำหรับระบบกลุ่มเมฆที่เป็นแบบ on-demand self-service ต้องออกแบบให้ส่วนติดต่อกับผู้ใช้งานมีความมั่นคง โดยการเข้ารหัสข้อมูลตลอดกระบวนการระหว่างอยู่ในระบบ ระบบกลุ่มเมฆ ที่ดีควรเปิดโอกาสให้ผู้ใช้สามารถประเมินการให้บริการทั้งในส่วนของความสะดวกสบายในการบริการ ความใส่ใจของเจ้าหน้าที่ดูแลระบบ นโยบายด้านความมั่นคง และสมรรถนะการทำงานของกลุ่มเมฆ เป็นต้น ผู้ให้บริการต้องมีการบันทึกการเปลี่ยนแปลงทั้งหมดที่เกิดขึ้นบนระบบเช่น การเปลี่ยน เพิ่ม ลด สิทธิ์ การทำงานของระบบทั้งที่ทำงานในสภาวะปกติ และล้มเหลว การอนุมัติการเปลี่ยนแปลงใดๆ ในระบบจะต้องบันทึกหลักฐานเป็นรายลักษณ์อักษร สามารถตรวจสอบได้ในภายหลัง การเข้าถึงกลุ่มเมฆ ของผู้ดูแลระบบจะต้องมีมาตรการพิเศษ เช่น มีการใช้รหัสแบบครั้งเดียว (One time password) หรือต้องมีการพิสูจน์ตัวตนมากกว่า 1 มาตรการ ก่อนเข้าระบบ (multi-factor authentication) **ความเสี่ยง** 2: กลไกในการยืนยันตัวตนที่ไม่มีประสิทธิภาพ (Weak authentication mechanisms) เป็นปัจจัยที่สร้างความเสี่ยงให้กับระบบกลุ่มเมฆเป็นอย่างมาก เนื่องจากผู้ใช้สามารถเข้าถึงกลุ่มเมฆ จากจุดใดก็ได้ที่เชื่อมต่อกับอินเทอร์เน็ต ความเสี่ยงได้เพิ่มขึ้นอีกเพราะระบบมีการแบ่งปันทรัพยากรร่วมกันด้วย การตั้งรหัสผ่านที่ไม่รอบคอบ ง่ายต่อการคาดเดา การขอรหัสใหม่โดยไม่จำเป็น หรือไม่ใส่ใจในการจดจำรหัสผู้ใช้และรหัสผ่าน เหล่านี้ล้วนแต่สร้างความเสี่ยงทั้งสิ้น

ตารางที่ 2. มาตรการรับมือจากความเสี่ยงและไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆ (ต่อ)

☑ **การรับมือ:** ผู้ให้บริการต้องจัดหาผู้เชี่ยวชาญด้านการรักษาความมั่นคงจากภายนอก (external audit) มาทำการประเมินระบบเพื่อให้แน่ใจว่าการรักษาความมั่นคง เช่น ระบบการยืนยันตัวตนอยู่ในมาตรฐานสากล ปฏิบัติตามมาตรการการรักษาความมั่นคงที่สากลยอมรับอย่างเคร่งครัด ตรวจสอบช่องโหว่และรูรั่วของเว็บบราวเซอร์ เนื่องจากเป็นเครื่องมือที่สำคัญในการใช้งานร่วมกับกลุ่มเมฆ ต้องมั่นใจว่ากรอบการทำงาน (framework) ของการรักษาความมั่นคงแบบ server-side มีความความน่าเชื่อถือและเป็นที่ยอมรับ บริการต่างๆ บนกลุ่มเมฆ ต้องสอดรับกับสัญญาการให้บริการ (Service level agreement: SLA) ที่ได้กำหนดไว้อย่างครบถ้วน
(g) ความมั่นคงเครือข่าย (Network Security)
ความเสี่ยง 1: มีความเสี่ยงเพิ่มขึ้นจากการลักลอบเจาะระบบบนเทคโนโลยีกลุ่มเมฆ โดยอาศัยเทคนิคต่างๆ ผ่านเว็บแอพพลิเคชัน เช่น การจู่โจมโดยแทรกรหัสที่เป็นอันตรายเข้าไปประมวลผล (injection vulnerabilities exploited) การโจมตีโดยผ่านภาษา SQL injection หรือ cross-site scripting เป็นต้น รวมถึงการโจมตีในระดับเครือข่าย เช่น man-in-the-middle, authentication attacks, side channel attacks, social networking attacks, denial of service (DoS) ☑ **การรับมือ:** วางมาตรการในการควบคุมการใช้งานเครือข่าย เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่มีสิทธิ์ ป้องกันอุปกรณ์เครือข่ายโดยติดตั้งไฟล์วอลล์ รายการควบคุมบนอุปกรณ์ (access control list : ACL) มีระบบยืนยันตัวตนที่ได้มาตรฐาน ป้องกันการเปิดเผยข้อมูล ข้อมูลเสียหายและสูญหาย รวมถึงมาตรการในการตรวจสอบการจราจรบนเครือข่ายเพื่อเฝ้าระวังการใช้เครือข่ายที่ผิดปกติ รวมถึงติดตั้งอุปกรณ์ประเภทตรวจจับผู้บุกรุก (Intrusion detection) และเว็บสแกนเนอร์สำหรับหาช่องโหว่ด้วย (web scanner for vulnerability)
ความเสี่ยง 2: มาตรการในการจัดโซนของระบบเครือข่ายเป็นสิ่งที่ควรกระทำ โดยอาศัยอุปกรณ์ที่เรียกว่าไฟล์วอลล์เป็นอุปกรณ์ที่ทำหน้าที่ดังกล่าว แต่พบว่ายังมีปัญหาในส่วนของความมั่นคงใน virtual machine ที่ยังไม่มีมาตรการการรักษาความมั่นคงที่ชัดเจนมารองรับ ☑ **การรับมือ:** ผู้ให้บริการต้องจัดโซนที่ปลอดภัยให้กับ virtual machine โดยสร้างเครือข่ายส่วนตัว (private network) พร้อมกับติดตั้งไฟล์วอลล์บนเครือข่ายดังกล่าวเพิ่มเติม **ความเสี่ยง** 3: ปัจจุบันผู้ให้บริการเปิดให้มีบริการผ่านเครือข่ายมือถือหรืออุปกรณ์เคลื่อนที่ ซึ่งจะนำความเสี่ยงมายังระบบเพิ่มขึ้น ☑ **การรับมือ:** ผู้ให้บริการจัดเตรียมกลไกที่รองรับการใช้งานจากเครือข่ายเคลื่อนที่อย่างปลอดภัย (ในหัวข้อดังกล่าวยังเป็นส่วนที่กำลังอยู่ในช่วงวิจัย)
(h) การเข้าถึงทางกายภาพ (Physical Access)
ความเสี่ยง 1: ข้อมูลจำนวนมากจะถูกวางไว้ในกลุ่มเมฆ ซึ่งมักจะอยู่ที่ใดที่หนึ่ง เมื่อสามารถเข้าสู่ที่ตั้งของกลุ่มเมฆได้ ก็เท่ากับว่าสามารถเข้าถึงข้อมูลได้ทั้งหมดไปด้วย ☑ **การรับมือ:** ผู้ให้บริการต้องปฏิบัติตามหัวข้อ การควบคุมการเข้าถึงระบบเครือข่าย (Network Security) ตามที่ได้กล่าวมาแล้ว และปฏิบัติตามมาตรการยืนยันตัวตนการเข้าถึงทางกายภาพอย่างเคร่งครัด

ตารางที่ 2. มาตรการรับมือจากความเสี่ยงและไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆ (ต่อ)

(i) ยอมรับมาตรฐาน (Compliance)
ความเสี่ยง 1: ผู้ให้บริการจำต้องปฏิบัติตามมาตรฐานและกฎหมายที่วางไว้ มาตรฐานที่จำเป็นต้องมี เช่น ความมั่นคงของข้อมูล ด้านการเงินและบัญชี ข้อจำกัดที่ถูกบังคับในการจัดส่งและจัดเก็บข้อมูล การปกป้องนักลงทุนจากการตกแต่งบัญชีของบริษัท (Sarbanes Oxley Act) อนุญาตให้ทำธุรกรรมข้ามเขตได้เสรี (Gramm-Leach-Bliley Act) มาตรฐานในการปกป้องข้อมูลทางการแพทย์และข้อมูลด้านสาธารณสุข (Health Insurance Portability and Accountability Act) มาตรฐานอื่นๆ เช่น SAS70 และ ISO เป็นต้น ☑ **การรับมือ:** ผู้ให้บริการต้องศึกษาว่าองค์กรของตนเปิดบริการอะไรให้กับลูกค้าบ้าง แล้วเลือกมาตรฐานต่างๆ ดังที่กล่าวมาแล้ว ให้เหมาะสมกับบริการของตนเอง
(j) ความมั่นคงด้าน Virtualization (15)
ความเสี่ยง 1: การย้ายเครื่องจักรเสมือน (VM) ระหว่างโฮสต์ จะเสี่ยงต่อกระบวนการควบคุมการเปลี่ยนแปลง ยากต่อการติดตามร่องรอยการเปลี่ยนแปลงของ VM เสี่ยงต่อการถูกเปิดเผยข้อมูลของ VM อาจมีปัญหาเรื่องของลิขสิทธิ์ในการใช้ซอฟต์แวร์ และอาจเกิดข้อผิดพลาดจากค่าคอนฟิกที่เคยปรับแต่งไว้ (misconfiguration) ☑ **การรับมือ:** จัดกลุ่มของระบบคอมพิวเตอร์ที่มีมาตรฐานการรักษาความมั่นคงที่ใกล้เคียงกัน หรือเหมือนกัน เพื่อที่จะสามารถย้าย VM ข้ามระหว่างกันได้ และติดตั้งเครื่องมือที่ใช้สำหรับเฝ้าระวังการทำงานของ VM พร้อมกับตรวจสอบความถูกต้องของ configuration ที่ถูกปรับแต่งไว้ด้วยเสมอ **ความเสี่ยง** 2: VM ที่ถูกสร้างขึ้นโดยการคัดลอก (copy) หรือการโคลนนิ่งจากตัวแบบ (template) ไปเรื่อยๆ จะส่งผลกระทบกับความเสี่ยงด้วย เช่น จุดอ่อนที่มีอยู่ใน VM เดิมจะถูกถ่ายทอดติดไปด้วย ค่าคอนฟิก (config) เดิมที่ไม่ได้ถูกปรับแต่งให้เหมาะสมจะถูกใช้อัตโนมัติ VM อาจจะถูกละเลยการดูแลเนื่องจากคิดว่าปลอดภัยแล้ว ☑ **การรับมือ:** VM ที่จะถูกนำไปใช้เป็นแม่แบบสำหรับคัดลอกหรือโคลนนิ่ง จะต้องผ่านการทดสอบความถูกต้องในการทำงานและความมั่นคงเสียก่อน เช่น สิทธิต่างๆ ที่อนุญาตให้เข้าถึง รูรั่วที่ได้รับการ patch เรียบร้อยแล้ว ข้อมูลที่สำคัญจะไม่ถูกเปิดเผย และที่สำคัญคือ เมื่อมีการปรับแต่งใดๆ บน VM แล้วจะต้องทำการจดบันทึกลง log file ด้วยเสมอ **ความเสี่ยง** 3: VMs จะติดตั้งอยู่บนระบบคอมพิวเตอร์อีกชั้นหนึ่ง ถ้ามีการจู่โจมโดยตรงที่ระบบคอมพิวเตอร์ (single target for attack) หรือระบบฮาร์ดแวร์ล้มเหลว (failure) จะส่งผลต่อ VM ทั้งหมดโดยอัตโนมัติ
☑ การรับมือ: วางมาตรการป้องกันการโจมตีต่อระบบคอมพิวเตอร์ โดยดำเนินการตามมาตรฐานสากล, กำหนดกลุ่มของคอมพิวเตอร์ทดแทนเพื่อทำหน้าที่แทนกรณีที่ระบบหลักประสบปัญหา พร้อมกับวางมาตรการสำรองและกู้คืนระบบ ความเสี่ยง 4: การปรับแต่ง VM บางระบบ ต้องใช้ทักษะของผู้ดูแลระบบและปรับแต่งเป็นลักษณะแบบ manual มากเกินไป ทำให้เกิดความเสี่ยง และยากต่อการพัฒนาระบบในอนาคต รวมถึงเครื่องมือต่างๆ ที่ช่วยในการดูแลรักษา VM มีไม่เพียงพอหรือไม่ทันสมัย ใช้งานยุ่งยาก ☑ การรับมือ: เลือก VM ที่เหมาะสม โดยพิจารณาถึงซอฟต์แวร์เสริมที่มาพร้อมกับ VM เพื่อช่วยในการบริหารจัดการที่ง่ายและครอบคลุมการรักษาความมั่นคงตามที่ต้องการ ความเสี่ยง 5: ความแตกต่างและซับซ้อนของ Visualization ของผู้ผลิตแต่ละราย, ความต่างกันของ platform จะสร้างความเสี่ยงให้กับระบบ และจะประสบปัญหาเรื่องการเฝ้าติดตามความเปลี่ยนแปลง เช่น asset หรือ version เป็นต้น

ตารางที่ 2. มาตรการรับมือจากความเสี่ยงและไม่ปลอดภัยบนเทคโนโลยีกลุ่มเมฆ (ต่อ)

☑ การรับมือ: ผู้ให้บริการต้องตรวจสอบ VM แต่ละผู้ผลิตว่าเป็นไปตามข้อกำหนดพื้นฐาน (Service level agreement: SLA) หรือไม่ และต้องมีระบบบันทึกการเปลี่ยนแปลงของ VM
ความเสี่ยง 6: เมื่อเครื่องมือในการบริหารจัดการและการเฝ้าระวังบน VM ไม่มีประสิทธิภาพที่ดีเพียงพอ จำเป็นต้องอาศัย audit/event logging เข้ามาช่วย เพื่อลดความเสี่ยงและการสร้างสภาพแวดล้อมเสมือนที่ซับซ้อนเกินไปจนยากกับการตรวจสอบ
☑ การรับมือ: Audit/event logging จะช่วยบันทึกเหตุการณ์ต่างๆ ดังต่อไปนี้บน VM เช่น พฤติกรรมการใช้งาน การเข้า/ออกระบบ ความพยายามเปลี่ยนแปลงแก้ไขสิทธิ เข้าสู่ระบบโดยไม่ถูกต้อง เป็นต้น แล้วรายงานเหตุการณ์ต่างๆ ที่อาจจะเป็นสาเหตุของปัญหาให้กับผู้ดูระบบทราบ
ความเสี่ยง 7: การนำเอาฮาร์ดแวร์หลายๆ เครื่องรวมเป็น single virtual server เพียงตัวเดียว จากนั้นสร้าง VMs หลายๆ ตัวบน single virtual ดังกล่าวจะนำไปสู่ความเสี่ยง เนื่องจากระบบป้องกันบนเครือข่าย เช่น ไฟล์วอลล์ IDS และเครื่องมือป้องกันเครือข่ายต่างๆ จะไม่สามารถทำงานได้บน virtual เพราะอุปกรณ์เหล่านี้จะทำงานบนเครือข่ายที่เชื่อมต่อทางกายภาพจริงๆ ส่งผลให้เกิดการแพร่กระจายของไวรัส ซอฟต์แวร์ที่เป็นอันตรายขึ้นภายใน VM หรือ VLAN เดียวกัน
☑ การรับมือ: จัดวางระบบเครือข่ายให้อยู่ในสภาพแวดล้อมที่ที่มีความมั่นคง สามารถป้องกันผู้ไม่ได้รับสิทธิ ข้อมูลมีความมั่นคง ข้อมูลไม่เสียหายหรือถูกแก้ไข และต้องติดตั้งซอฟต์แวร์ที่ตรวจจับปริมาณการใช้งานในแต่ละ VM เพื่อตรวจสอบไวรัส หรือซอฟต์แวร์อันตราย
ความเสี่ยง 8: การจัดวางหรือการแบ่งโซนทางกายภาพของศูนย์กลางข้อมูล (data center) จะไม่สามารถใช้งานได้กับสภาพแวดล้อมเสมือน ส่งผลให้นักเจาะระบบหันมาเจาะ VMs แทน เนื่องจากสามารถเจาะระบบจากจุดใดๆ ก็ได้ที่เชื่อมต่อเน็ตเวิร์ค
☑ การรับมือ: ต้องอาศัยมาตรการรักษาความมั่นคงในระดับเครือข่าย และควรจำลองการสื่อสารระหว่าง VM ให้แยกออกจากกันโดยใช้ซอฟต์แวร์ที่มากับ VM เข้าช่วย เช่น vShield จากค่าย VMware เป็นต้น
ความเสี่ยง 9: การปรับปรุง firmware จะส่งผลกระทบกับ VM ทั้งหมดที่ทำงานอยู่ เนื่องมาจากทำงานอยู่ในฮาร์ดแวร์ตัวเดียวกัน ความเสี่ยงก็จะสูงขึ้นเพราะ VM ที่ทำงานอยู่จะจำลองฮาร์ดแวร์เดิมไว้ แต่เมื่อเกิดการปรับปรุง firmware ใหม่ อาจจะเกิดรอยรั่วขึ้น เมื่อสั่งให้ระบบทำงาน เนื่องจาก VM ใหม่ยังคงทำงานกับฮาร์ดแวร์เดิม
☑ การรับมือ: เมื่อจำเป็นต้องมีการปรับปรุง firmware ควรจะต้องทำการทดสอบกับระบบที่ไม่ได้ทำงานจริงๆ ก่อน เมื่อไม่มีข้อผิดพลาดใดๆ จึงนำมาทดแทนระบบจริงภายหลัง แต่ถ้าไม่มีระบบที่ใช้ทดสอบ เมื่อปรับปรุงเสร็จแล้วจะต้องอาศัยซอฟต์แวร์ประเภท audit/event log เข้ามาช่วยในการเฝ้าระวังระบบ เพื่อให้แน่ใจว่าระบบที่ปรับปรุงแล้วจะทำงานไม่ผิดพลาด

10. บทสรุป

จากตารางที่ 3 แสดงถึงบทสรุป สถานะ และทิศทางของงานวิจัยด้านความมั่นคงบนเทคโนโลยีกลุ่มเมฆในปัจจุบัน ว่ามีแนวโน้มเป็นอย่างไร (20) มีทั้งหมด 11 หัวข้อ สามารถแบ่งกลุ่มได้ 2 กลุ่ม คือ กลุ่มแรก ผู้ทำวิจัยทั่วโลกได้เสนอ รูปแบบ เครื่องมือ และแนวทางการแก้ไขปัญหาด้านความมั่นคงไว้แล้ว ซึ่งประกอบด้วยหัวข้อที่ 1, 2, 4, 5, 6, 8, 9 และ 10 กลุ่มที่สอง ยังอยู่ในช่วงที่นักวิจัยกำลังดำเนินการวิจัยอยู่ โดยยังอยู่ในช่วงการเสนอแนวทางในการแก้ไขออกมาเผยแพร่ ประกอบไปด้วยหัวข้อที่ 3 และ 7 กล่าวโดยสรุปแล้ว ความมั่นคงของการประมวลผลกลุ่มเมฆในปัจจุบัน ยังไม่สมบูรณ์ 2 ส่วน คือ ความชัดเจนของการพัฒนาและการวิจัยระบบ Cloud

ที่เป็นรูปธรรมจริงๆ ในทางปฏิบัติ (Implementation and research issues in cloud computing) และความชัดเจนในมาตรการรักษาความมั่นคงและความเป็นส่วนตัวของระบบ (Security & privacy in cloud computing) เมื่อคำนวณความเสี่ยง 2 หัวข้อ จาก 11 หัวข้อ คิดเป็นความเสี่ยงประมาณ 18.18% ซึ่งแสดงให้เห็นว่าผู้ที่กำลังตัดสินใจจะใช้งานระบบการประมวลผลกลุ่มเมฆสามารถมั่นใจระบบนี้ได้ แต่ให้ตรวจสอบมาตรการรักษาความมั่นคงและการรักษาข้อมูลโดยละเอียดจากผู้ให้บริการอีกครั้งก่อนการตัดใจ โดยการคาดการณ์ อีกประมาณ 1 – 2 ปีข้างหน้าเทคโนโลยีการประมวลผลกลุ่มเมฆจะถูกแก้ไขปัญหาการรักษาความมั่นคงครบทั้งหมดทุกหัวข้อ ผู้เขียนมีความเห็นว่าเทคโนโลยีแบบกลุ่มเมฆจะต้องเข้ามาทดแทนเทคโนโลยีการประมวลผลแบบเดิม (Client-Server) อย่างแน่นอน ซึ่งปัจจุบันหน่วยงานราชการของประเทศไทยหลายหน่วยงาน เช่น กระทรวงไอซีทีได้เปิดตัว The Government Cloud Service นำร่องเป็นที่เรียบร้อยแล้ว ดังนั้นเพื่อเป็นการเตรียมความพร้อมกับการรับเอาเทคโนโลยีดังกล่าวมาใช้งาน ผู้ใช้จำเป็นต้องทราบถึงความเสี่ยงที่อาจจะเกิดขึ้นกับเทคโนโลยีดังกล่าวในอนาคต เพื่อที่จะวางแผนในการรับมือ ก่อนที่จะเกิดความสูญเสียกับข้อมูลของตนเอง บทความนี้จึงถูกเขียนขึ้นเพื่อเปิดเผยข้อเท็จจริงที่กำลังเกิดขึ้นเกี่ยวกับเทคโนโลยีดังกล่าวในปัจจุบัน

ตารางที่ 3. แสดงบทสรุปของงานวิจัยด้านความมั่นคงของการประมวลผลกลุ่มเมฆในปัจจุบัน

กลุ่มที่	บริบทของงานวิจัย	มีโมเดล/เครื่องมือ/แนวทาง
1	Secure provenance in cloud computing	✓
2	Trusted cloud computing	✓
3	Implementation and research issues in cloud computing	✘
4	Data- centric cloud security	✓
5	Security audit in public infrastructure clouds	✓
6	Transparent cloud Security	✓
7	Security & privacy in cloud computing	✘
8	Security management of virtual machines	✓
9	Privacy manager for cloud computing	✓
10	Addressing security issues in cloud computing	✓
11	Data protection models for service provisioning in the cloud	✓

11. เอกสารอ้างอิง

(1) Buyya R. High Performance Cluster Computing: Architectures and Systems. New York USA: Prentice Hall; 1999. p. 94-104.

(2) Rajkumar Buyya, Bubendorfer K. Market-Oriented Grid and Utility Computing. New York USA: John Wiley & Sons, Inc.,; November 2009. p. 123-187.

(3) Barbara P. Heath, Vetter RJ. Fostering Undergraduate Research Partnerships through a Graphical User Environment for the North Carolina Computing Grid final report: The University of North Carolina WilmingtonMay; 2007.

(4) Mariana Carroll, Merwe Avd, editors. Secure Cloud Computing Benefits, Risks and Controls Information Security South Africa (ISSA); 2011 Aug 15-17; Johannesburg; South Africa: IEEE; 2011.

(5) Bhaskar Prasad Rimal, Choi E, editors. A Taxonomy and Survey of Cloud Computing Systems. 2009 Fifth International Joint Conference on INC IMS and IDC (2009); 2009 Aug 25- 27; Seoul, Korea: IEEE; 2009.

(6) Gerlach G. Defining Cloud Computing from the scratch [Internet]. 2009 [updated 2011 April 9; cited 2012 April 3]. Available from: http://www.gunthergerlach.com/tag/amazon-web-services

(7) FlexiScale. Utility computing on demand [Internet]. 2009 [updated 2010 Jan; cited 2012 April 30]. Available from: http://flexiscale.com/

(8) Radu Prodan, Ostermann S, editors. A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers. 10th IEEE/ACM International Conference on Grid Computing; 2009 Oct 13-15; Banff, AB: IEEE; 2009.

(9) Kai Hwang, Kulkarni S, editors. Cloud Security with Virtualized Defense and Reputation-based Trust Management. 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing; 2009 Dec 12-14; Chengdu: IEEE; 2009.

(10) B. Sotomayor ea, editor. Virtual Infrastructure Management in Private and Hybrid Clouds. Internet Computing, IEEE; 2009 Sept 09; New York: IEEE; 2009.

(11) Kai Hwang, Li D, editors. Trusted Cloud Computing with Secure Resources and Data Coloring. IEEE INTERNET COMPUTING; 2010 Sept 02; New York: IEEE; 2010.

(12) P. Mell, Grance T. The NIST Definition of Cloud Computing: National Institute of Standards and Technology, U.S. Department of Commerce; 2011 Sept. 7 p.

(13) Popovic, Kresimir, editors. Cloud computing security issues and challenges. MIPRO, 2010 Proceedings of the 33rd International Convention; 2010 May 24-28; Opatija, Croatia: IEEE; 2010.

(14) M. Casassa-Mont, Bramhall SPaP, editors. Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services; 2003 Sept 1-5; UK. New York: IEEE; 2003.

(15) M. Carroll ea, editor. Secure Virtualization: Benefits, Risks and Controls. The 1st International Conference on Cloud Computing and Services Science; 2011 May 7-9; Noordwijkerhout, The Netherlands: SciTePress; 2011.

(16) Kai Hwang, Li D, editors. Trusted Cloud Computing with Secure Resources and Data Coloring. IEEE INTERNET COMPUTING; 2010 Sept 02; UK. New York: IEEE; 2010.

(17) Buyya R, Ranjan R, Calheiros RN, editors. Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities. Cluster Computing and the Grid, CCGRID '09 9th; 2009 May 18-21; Shanghai: IEEE; 2009.

(18) Gartner. Seven cloud-computing security risks [Internet]. 2008 [updated 2010 July 2; cited 2012 April 3]. Available from: http://www.networkworld.com/news/2008/070208-cloud.html

(19) Robert Richardson. 2008 CSI Computer Crime and Security Survey [Internet]. 2008 [updated 2008 May 12; cited 2012 April 15]. Available from: http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

(20) Farhan Bashir Shaikh, Haider S, editors. Security Threats in Cloud Computing. 6th International Conference on Internet Technology and Secured Transactions; 2011 Dec 11-14; Abu Dhabi, United: IEEE; 2011.