สำรวจคลาวด์คอมพิวเตอร์บนอุปกรณ์พกพา

เกษมสันต์ จันทร์ศรี, ภาณุพันธุ์ สังขพัฒน์, นัฏฐา พุทธาวันดี, สุภัทรชัย มีพร

ภาควิชา วิทยาการคอมพิวเตอร์ มหาวิทยาลัยขอนแก่น

บทคัดย่อ แนวคิดของ Mobile Cloud Computing (MCC) ทำให้ผู้ใช้สามารถใช้โทรศัพท์มือถือบนเครือข่าย Cloud Computing แต่จะให้ฟังก์ชันการทำงานเพิ่มเติมไปยัง “cloud” สำหรับ MCC จะช่วยในการเอาชนะข้อจำกัดของโทรศัพท์มือถือโดยเฉพาะอย่างยิ่งในการประมวลผลพลังงานและการจัดเก็บข้อมูล นอกจากนี้ยังช่วยยืดอายุการใช้แบตเตอรี่ โดยการย้ายการดำเนินการของโปรแกรมไปยัง cloud เพื่อลดปัญหาต่าง ๆ เช่น ด้านความปลอดภัย ด้านการประหยัดพลังงาน และด้านสถาปัตยกรรมต่างๆเป็นต้น โดยงานที่นำเสนอนี้จะทำการสรุปและจัดกลุ่มดังต่อไปนี้ 1) ด้านพลังงาน 2) ด้านสถาปัตยกรรม 3) ด้านการเชื่อมต่อ Cloud 4) ด้านความปลอดภัย

คำสำคัญ-*โมบายคลาวด์คอมพิวเตอร์ คลาวด์คอมพิวเตอร์ ประยุกต์ใช้โมบายคลาวด์คอมพิวเตอร์ สถาปัตยกรรมโมบายคลาวด์คอมพิวเตอร์ ความปลอดภัย*

I. บทนำ

Cloud Computing คือ บริการทางอินเตอร์เน็ตที่เป็นแบบการรวบรวมทรัพยากรต่างๆที่จำเป็นมาเชื่อมโยงไว้ด้วยกัน โดยมีการทำงานสอดประสานกันแบบรวมศูนย์ โดยผู้จัดสรรทรัพยากรนั้นเรียกว่า third-party Provider หรือผู้ให้บริการบุคคลที่ 3 มีหน้าที่รวบรวมพื้นฐานต่างๆที่จำเป็นเข้าไว้ด้วยกัน

Cloud Computing จะทำงานโดยเมื่อผู้ขอใช้บริการต้องการใช้สิ่งใดก็ส่งร้องขอไปยังซอฟแวร์ระบบ แล้วซอฟแวร์ระบบก็จะร้องขอไประบบเพื่อจัดสรรทรัพยากรและบริการให้ตรงกับความต้องการของผู้ขอใช้บริการต่อไป โดยผู้ขอใช้บริการมีหน้าที่เสียค่าใช้บริการเพื่อความสามารถในการทำงานตามต้องการโดยไม่ต้องทราบหรือเข้าใจหลักการทำงานเบื้องหลังซึ่งหลักการทำงานนั้น จะแบ่งออกเป็น 2 ส่วน คือ Client กับ Server ซึ่งจะเห็นได้ว่าทางฝั่งของ Client จะมีแค่คอมพิวเตอร์ คือ Client แค่มี Web browser เพื่อเปิดเรียกใช้การทำงานก็เพียงพอแล้ว ส่วน Server ก็ทำหน้าที่ประมวลผลต่างๆให้ผู้ขอใช้บริการ

จุดเด่นของ Cloud Computing

1) Agility : มีความรวดเร็วในการใช้งาน
2) Cost : ค่าใช้จ่ายน้อย หรืออาจไม่เสียค่าใช้จ่ายสำหรับ Client
3) Device and Location Independence : สามารถเข้าถึงระบบจากที่ใดก็ได้และสามารถใช้อุปกรณ์ได้หลายรูปแบบ
4) Multi-Tenancy : แบ่งการใช้ทรัพยากรให้ผู้ใช้จำนวนมากได้
5) Reliability : มีความน่าเชื่อถือ
6) Scalability : มีความยืดหยุ่น
7) Security : มีความปลอดภัย
8) Sustainability : มีความมั่นคง

ข้อดีของ Cloud Computing

1) ลดต้นทุน
2) ลดความเสี่ยงการเริ่มต้น หรือการทดลองโครงการ
3) สามารถลดหรือขยายได้ตามความต้องการ
4) ประสิทธิภาพสูง
5) อยู่ภายใต้การดูแลของผู้เชี่ยวชาญ

ข้อเสียของ Cloud Computing

1) จากการที่มีทรัพยากรที่มาจากหลายแห่ง จึงอาจเกิดปัญหาด้านความต่อเนื่องและความรวดเร็ว
2) ยังไม่มีการรับประกันในการทำงานและความปลอดภัย
3) แพลทฟอร์มยังไม่ได้มาตรฐาน

Mobile Cloud Computing

ปัจจุบัน Mobile Computing กับ Mobile Internet Device (MID) เช่น iPhone และ Android กลายเป็น คอมพิวเตอร์ส่วนบุคคลที่เป็นทางเลือกในการอำนวยความสะดวก โดย การรวมการเคลื่อนที่ การติดต่อสื่อสาร software ในการทำงาน และ ความบันเทิง เนื่องจากข้อจำกัดของทรัพยากรของ MID ของ cloud services กลายเป็นทางเลือกที่เหมาะสำหรับการติดตั้ง software บน MID โดยจะเข้ามาช่วยในการเอาชนะข้อจำกัดของโทรศัพท์มือถือโดยเฉพาะอย่างยิ่งในการประมวลผล พลังงานและการจัดเก็บข้อมูล นอกจากนี้ยังอาจช่วยยืดอายุการใช้แบตเตอรี่ โดยการย้ายการดำเนินการโปรแกรมจากข้อจำกัดของ Mobile เรื่องความเร็วในการประมวลผล ขนาดของหน่วยความจำ และพลังงานแบตเตอรี่ จึงมีการนำเทคโนยี Cloud computing มาช่วยลดปัญหาในด้านต่างๆ โดยอาจจะไม่ต้องคำถึงถึงข้อจำกัดของ Mobile อีกต่อไป เช่นโปรแกรมทางฝั่ง Client ที่นำมาติดตั้งลงใน Mobile จะมีขนาดเล็กจะทำหน้าที่ในการติดต่อกับผู้ให้บริการ Cloud โดยจะโอนเรื่องการประมวลผลให้กับทางฝั่งผู้ให้บริการรับผิดชอบ ทำให้ทางฝั่ง Client นั้นไม่จำเป็นต้องมีการประมวลที่สูงก็ได้ และจากการที่มีการประมวลผลต่ำนั้นจะส่งผลต่อพลังงานในแบตเตอรี่โดยตรงนั่นคือจะช่วยลดการใช้พลังงานในการประมวลผล ทำให้สามารถใช้งานได้นานมากขึ้น จากข้อดีของ Cloud Computing บน Mobile ก่อให้เกิดการประยุกต์และพัฒนาการให้บริการด้านต่างๆอย่างรวดเร็ว ไม่ว่าจะเป็นการใช้ Cloud Computing บน Mobile ในเรื่องของการค้า การศึกษา การค้นหาข้อมูล และอื่นๆ ทำให้ Mobile Cloud Computing เป็นเทคโนโลยีที่กำลังเติบโตอย่างรวดเร็ว เพราะสามารถตอบโจทย์ในเรื่องที่ว่า สามารถเข้าถึงการบริการได้ทุกที่ทุกเวลา ในส่วนถัดไปจะเป็นการวิพากษ์บทความต่างๆที่ได้ทำการศึกษามาโดยจะ

แบ่งเป็นหัวข้อที่พิจารณา 4 กลุ่ม คือ กลุ่มพลังงาน กลุ่มสถาปัตยกรรม กลุ่มการเข้าถึง cloud ด้วย mobile และกลุ่มความปลอดภัย

II. ด้านพลังงาน

เนื่องจากข้อจำกัดของ Mobile ที่มีพลังงานแบตเตอรี่ที่จำกัดทำให้การใช้งาน Mobile มีระยะเวลาที่สั้น ด้วยเหตุนี้จึงเกิดการศึกษาการลดการใช้พลังงานเพื่อให้แบตเตอรี่อยู่ได้นานและสามารถนำอุปกรณ์ไปใช้ในงานตามที่ต้องการได้อย่างเหมาะสมด้วยเหตุนี้จึงมีการนำ Cloud Computing มาช่วยในการแก้ปัญหาในด้านนี้ดังนี้

Virtualized In-Cloud Security Services for Mobile Devices [3]

เป็นการนำเสนอการให้บริการเครือข่ายเสมือนจริงในการรักษาความปลอดภัยใน Cloud สำหรับอุปกรณ์บนมือถือ เป็นการนำเสนอแนวคิดในการทำงานป้องกันไวรัสบนมือถือในรูปแบบใหม่ต่างๆ โดยการย้ายอุปกรณ์และการให้บริการทางด้านเครือข่าย โดยใช้เครื่องมือตรวจหามัลแวร์ต่าง ๆ ซึ่งจะมีความเป็นไปได้ในเรื่องของการลดแบนด์วิด ลดอุปกรณ์ทางด้าน ซีพียู หน่วยความจำและอุปกรณ์ตัวอื่น ๆ ทางด้านการตรวจจับของซอฟต์แวร์นั้นเมื่อทำงาน การประเมินผลการทำงานจะมีส่วนที่แตกต่างคือไฟล์หรือวิธีการนั้นจะใช้เครื่องมือในการตรวจสอบภายในเครือข่ายการให้บริการ อุปกรณ์มือถือที่มีความสามารถในการป้องกันนั้นจะลดการใช้ทรัพยากรอุปกรณ์ โดยการโอนไฟล์ไปยังเครือข่ายบริการใน Cloud ซึ่งมีวิธีการ 2 วิธีคือ 1. ส่งข้อมูลที่อยู่บนมือถือไปยังเครือข่ายสำหรับการวิเคราะห์และการบริการ เครือข่ายก็จะได้รับไฟล์จากอุปกรณ์และระบุเนื้อหาว่าเป็นอันตรายหรือไม่ 2.สามารถป้องกันไวรัสคอมพิวเตอร์เวลาคอมพิวเตอร์หรืออุปกรณ์รับเอกสารใหม่หรือโปรแกรมแต่ละรายการที่ตรวจพบโดยอัตโนมัติและส่งไปยัง Cloud เพื่อป้องกันไวรัสและนำไปวิเคราะห์ ระบบ CloudAV เพื่อทำการตรวจสอบและเช็คว่าคอมพิวเตอร์มีรายการที่มีความปลอดภัยหรือไม่ ระบบ CloudAV จะเป็นการให้บริการ Cloud ในตรวจหามัลแวร์ซึ่งประกอบด้วย host agent และ Network service-components ซึ่ง Host Agent มีลักษณะเช่นเดียวกับซอฟต์แวร์ป้องกันไวรัสจากค่ายต่าง ๆ คือกระบวนการของซอฟแวร์จะมีน้ำหนักค่อนข้างเบาตอนรันบนอุปกรณ์แต่ละตัว และได้ทำการตรวจไฟล์กิจกรรมต่างๆ ในระบบและทำการเข้าถึงแต่ละไฟล์โดยจะโอนไปจัดการ ส่วน Network Service นั้นองค์ประกอบสำคัญของสถาปัตยกรรมเครือข่ายเป็นการวิเคราะห์การใช้บริการเครือข่ายเพื่อตรวจสอบว่าเป็นไฟล์ไหนที่เป็นอันตรายหรือที่ไม่พึงประสงค์ ซึ่งแตกต่างจากที่มีอยู่ในซอฟต์แวร์ป้องกันไวรัสที่สามารถรวมกลไกต่าง ๆ เพื่อตรวจสอบและคุ้มครอง ผลการทดสอบโปรแกรมแสกนไวรัส

ประเภทของสแกนไวรัส	การตรวจจับ	การคุ้มครอง
CM	229 / 469	4882%
SM CM	290/469	6183%
MA CM SM	358/469	7633%
CM SM MA BD	417/469	8891%
CM SM MA BD FS	430/469	9168%

ตารางที่ 1 ตัวอย่างของการตรวจจับไวรัสประเภทมัลแวร์ต่าง ๆ เมื่อใช้เครื่องมือหลาย ๆ ตัวในแบบคู่ขนาน ClamAV (CM) Symantec (SM) McAfee (MA) BitDefender (BD) and F-Secure (FS)

หลังจากที่แฟ้มข้อมูลได้รับการวิเคราะห์ผลสามารถเก็บไว้ในหน่วยความจำและแชร์ข้อมูลหน่วยความจำเพื่อใช้ร่วมกันในการให้บริการนอกจากนี้สามารถเข้าถึงแฟ้มข้อมูลและสามารถเข้าถึงอุปกรณ์อื่น ๆ ที่ใช้ร่วมกันโดยผ่านทางไกล ซึ่งหน่วยความจำที่ตั้งอยู่ในบริการเครือข่ายไม่จำเป็นต้องส่งไฟล์สำหรับการวิเคราะห์ ซึ่งจะเก็บไว้ในเครือข่ายในการให้บริการแล้วซึ่งก่อให้เกิดความรวดเร็วในการเข้าใช้งานในอนาคต CloudAV ขยายไปยัง Mobile ขยายผลประโยชน์ของแพลตฟอร์ม ที่จะใช้งานบนแพลตฟอร์ม โดยแพลตฟอร์มจะถูกกระตุ้นได้ง่าย เมื่ออุปกรณ์หรือมีปรับเปลี่ยนพื้นฐานของสถาปัตยกรรม ซึ่งจะมีความจำเป็นในการพัฒนาและสนับสนุนตัวแทนจำหน่ายโทรศัพท์มือถือซึ่งจะมีความแตกต่างระหว่างตัวแทนโฮสต์แบบเดิมและตัวแทนจำหน่ายมือถือ ที่พัฒนาขึ้นใหม่พฤติกรรมกลไกต่าง ๆ บนมือถือ วิธีการใช้ทรัพยากรบนมือถือมีมากขึ้นทำให้ต้องมีการตรวจสอบว่ามีกิจกรรมไหนที่เป็นอันตรายต่อมือถือ โดยมีแพลตฟอร์มให้สามารถจัดลำดับความแตกต่างของการให้บริการการรักษาความปลอดภัย SMS Spam Filtering-SMS เป็นฟังก์ชั่นการกรองข้อมูลในลักษณะของ SMS ที่ส่งมากับโทรศัพท์มือถือ เป็นการป้องกันเมล์ขยะหรือไวรัสต่าง ๆ ซึ่งจะดำเนินการขณะที่อยู่ในลักษณะการโฆษณา โดยผลิตภัณฑ์แอนตี้ไวรัสนั้นบางมือถือมีความสามารถมาก ซึ่งรูปแบบการใช้งานเครือข่ายจะเป็นศูนย์กลางผ่านการรวมตัวของข้อมูลจากคลังข้อมูลขนาดใหญ่ของผู้ใช้งาน Phishing Detection ตรวจจับฟิชชิ่ง เป็นการรวบรวมสำรวจเว็บที่มีส่วนช่วยพัฒนา Google ให้มีความแข็งแรงโดยมีเครื่องมือป้องกันฟิชชิ่ง ซึ่งจะรวบรวมความสามารถในการจัดหาการบริการที่จะช่วยให้สามารถควบคุมดักจับและป้องกันฟิชชิ่ง จากการโจมตีแบบฟิชชิ่งกับลูกค้า Centralized Blacklists เป็นการรวบรวมข้อมูลที่ควรหลีกเลี่ยง ซึ่งจากการติดต่อสื่อสารที่แอดเดรสหรือบลูทูธ และไอพีต่าง ๆ ทำให้มีผลเวลาอุปกรณ์การให้บริการความปลอดภัยไม่ทำงาน การประเมินผลสำหรับการประเมินผลจะดำเนินการตามมาตรฐานของอุปกรณ์โทรศัพท์มือถือโนเกียจะวัดได้จากการใช้ทรัพยากรการใช้พลังงานของอุปกรณ์เหล่านี้โดยเปรียบเทียบมือถือกับตัวแทนที่มีผลิตภัณฑ์แอนตี้ไวรัสที่มีอยู่ในเชิงพาณิชย์ สำหรับแต่ละการทดสอบจะมีผลสำหรับตัวแทนมือถือ

ตัวแทนจำหน่าย	เวลาเริ่มต้น	หน่วยความจำเฉลี่ย	หน่วยความจำสูงสุด	ผู้ใช้	รวม
ClamAV	57 sec	25967 KB	39556 KB	13349	15684
MA-CL+CR	02 sec	1502 KB	2154 KB	1502	2185
MA-CL+WR	02 sec	1486 KB	2124 KB	1486	1854
MA-WL+WR	02 sec	1189 KB	1812 KB	1189	1714

ตารางที่ 2 การเปรียบเทียบของตัวแทนมือถือกับ ClamAV ในผู้ใช้หน่วยความจำและซีพียูในโนเกีย N800

การเปรียบเทียบตัวแทนผู้จัดจำหน่ายความปลอดภัย

ตัวแทนผู้จัดจำหน่ายความปลอดภัย	ค่าเฉลี่ย/ช่วงเวลา/รวมพลังงาน
MA - WR + CL (EDGE)	122 / 213 / 1269 W
MA - WR + CL (WiFi)	092 / 183 / 745 W
MA - WR + WL	082 / 120 / 599 W

ตารางที่ 3 การเปรียบเทียบของตัวแทนผู้จัดจำหน่ายความปลอดภัยกับ Kaspersky ความปลอดภัยโทรศัพท์บน Nokia N95

การเปรียบเทียบตัวแทนผู้จัดจำหน่ายความปลอดภัย

กลไกในการตรวจจับ	ลายเซ็นขนาดฐานข้อมูลการตรวจสอบ
Symantec Mobile	27 signatures
Kaspersky Mobile	284 signatures
ClamAV	262289 signatures
Mobile Agent	> 5 ล้าน +พฤติกรรม

ตารางที่ 4 จำนวนของภัยคุกคามที่ส่งในลายเซ็นฐานข้อมูลของเครื่องมือตรวจหาการจัดการความกังวลที่เพิ่มขึ้นของภัยคุกคามอุปกรณ์เคลื่อนที่

วิธีตรวจสอบค้นหามัลแวร์แบบใหม่บนโทรศัพท์มือถือโดยการย้ายความสามารถในการตรวจสอบไปยังเครือข่ายให้บริการ ซึ่งเกิดประโยชน์มากรวมทั้งการตรวจสอบที่ครอบคลุมมากยิ่งขึ้นทำให้ซอฟแวร์มีความซับซ้อนน้อยลงและการใช้ทรัพยากรลดลง

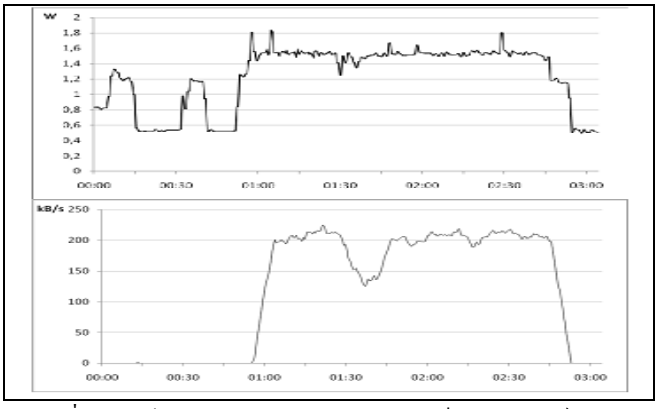
CloudTorrent - Energy-Efficient BitTorrent Content Sharing for Mobile Devices via Cloud Services [17] เสนอการใช้ BitTorrent ประหยัดพลังงานร่วมกันสำหรับอุปกรณ์มือถือผ่านบริการ CloudTorrent

รูปแบบของ CloudTorrent ส่วนประกอบการประยุกต์ใช้โทรศัพท์ติดต่อสื่อสารที่มีกลุ่มและเซิร์ฟเวอร์โฮสติ้งของลูกค้า BitTorrent ระยะไกล การประยุกต์ใช้โทรศัพท์เป็นส่วนขยายของ SymTorrent ลูกค้าเปิดแหล่ง BitTorrent สำหรับอุปกรณ์ S60 Symbian ซึ่งสามารถควบคุมจากระยะไกลเซิร์ฟเวอร์ BitTorrent โดยระบุความคืบหน้าการดาวน์โหลดและการถ่ายโอนไฟล์ที่ดาวน์โหลดจากเซิร์ฟเวอร์ไปยังโทรศัพท์มือถือ การสื่อสารกับเซิร์ฟเวอร์ทั้งหมดจะดำเนินการผ่านการเชื่อมต่อโปรโตคอลเดียวกันในฝั่งเซิร์ฟเวอร์จะใช้ uTorrent ซึ่งเป็นที่นิยมของลูกค้า PC ฟรี โดยใช้ฟังก์ชั่นผ่านทาง HTTP - based API ตั้งแต่ uTorrent API จะไม่สนับสนุนไฟล์ดาวน์โหลดแล้วยังเรียกใช้เว็บเซิร์ฟเวอร์ที่แยกต่างหากที่ใช้ในการถ่ายโอนไฟล์ที่ดาวน์โหลดไปยังโทรศัพท์มือถือ ขณะนี้การดาวน์โหลดข้อมูล CloudTorrent เกิดขึ้นในสองขั้นตอน ด้านเซิร์ฟเวอร์ใช้โปรโตคอล BitTorrent ดาวน์โหลดข้อมูลไปยังเซิร์ฟเวอร์ CloudTorrent ข้อมูลเมื่อดาวน์โหลดเสร็จสมบูรณ์แล้วดาวน์โหลด HTTP โอนข้อมูลไปยังโทรศัพท์

การวัดและผลในการประเมินผลการแก้ปัญหาเมื่อเทียบกับประสิทธิภาพของ SymTorrent ดำเนินการถ่ายโอนพลังงานและการวัดความเร็วด้วย Nokia N82 เชื่อมต่อกับอินเทอร์เน็ตผ่าน 3G โฮสติ้งเซิร์ฟเวอร์และไคลเอนต์ BitTorrent เว็บเซิร์ฟเวอร์คือ Amazon EC2 ความเร็วในการดาวน์โหลดโดยเฉลี่ยในมือถือมุ่งเน้นเฉพาะประสบการณ์ความเร็วจากโทรศัพท์มือถือในกรณี CloudTorrent HTTP การถ่ายโอนไฟล์จากเซิร์ฟเวอร์มาที่มือถือและในกรณีที่ SymTorrent ดาวน์โหลด รวมความเร็วจากสิ่งที่แตกต่างกัน CloudTorrent SymTorrent ทำได้ดีกว่าทั้งในการใช้พลังงานและเวลาในการดาวน์โหลด ความแตกต่างในการใช้พลังงานส่วนใหญ่จะนำมาประกอบกับความแตกต่างด้านความเร็วในการดาวน์โหลด CloudTorrent ก็สามารถมีความเร็วในการโอนสูงกว่า SymTorrent ซึ่งสอดคล้องกับข้อสังเกตก่อนหน้านี้ที่สูงกว่าอัตราบิตต่ำ ค่าใช้จ่ายพลังงานต่อบิต ในกรณี CloudTorrent เซิร์ฟเวอร์ที่แยกลูกค้าโทรศัพท์มือถือจากข้อจำกัด และความแปรปรวนของการดาวน์โหลดข้อมูลให้รวดเร็วและทุ่มเทเพื่อการเชื่อมต่อโทรศัพท์มือถือ SymTorrent บนมืออื่น ๆ ที่ได้รับข้อมูลจากคนอื่น และประสบโดยตรงจากข้อจำกัดแบนด์วิดของในรุ่นเดียวกัน การส่งอินเตอร์เน็ตที่เป็นปัญหาและการแข่งขันระหว่างการดาวน์โหลดทั้งหลาย นอกจากนี้ตั้งแต่ลูกค้า BitTorrent ในกลุ่มจะสามารถให้บริการด้วยความเร็วในการอัพโหลดสูง กลไกการเพิ่มความเร็วในการดาวน์โหลดของข้อมูล จะเปรียบเทียบเวลาในการดาวน์โหลดข้อมูลเท่านั้นและไม่รวมเวลาในการถ่ายโอนไฟล์จากเซิร์ฟเวอร์ไปยังโทรศัพท์มือถือโดยแจ้งให้ทราบล่วงหน้าที่เซิร์ฟเวอร์ CloudTorrent ก็สามารถดาวน์โหลดข้อมูล 88% เร็วกว่า SymTorrent

ในกรณีของ CloudTorrent ช่วงการโอนข้อมูลเริ่มต้นจะเริ่มด้วยระยะต่ำมีบาง spikes ที่มีกำลังสูง ในช่วงเวลานี้เซิร์ฟเวอร์จะทำการดาวน์โหลดข้อมูลและโทรศัพท์ไม่ได้ใช้งานรอข้อมูลมีความพร้อม ความคมชัดที่ 30 วินาที เกิดขึ้นเพราะสำรวจมือถือสถานะของเซิร์ฟเวอร์ผ่านทางแบบสอบถาม HTTP ซึ่งมีเพียงไม่กี่ไบต์การถ่ายโอนข้อมูลซึ่งไม่ได้มองเห็นได้ในกราฟ แต่การใช้พลังงานยังคงอยู่ในระดับสูงประมาณ 10 วินาที สมมติฐานคือการที่ล่าช้าเกิดจากการตั้งค่าตัวจับเวลา 3G ที่ควบคุมการเปิดใช้งานโหมดประหยัดพลังงานในเครือข่าย

3G นี้ คือการแสดงให้เห็นว่าการจัดการมีความคืบหน้าอย่างมากในความฉลาดทางด้านโทรศัพท์ ทำให้มีประสิทธิภาพในการทำงานมากขึ้น สำหรับข้อมูลนั้นจะมีขนาดใหญ่มากเช่น หนังก็ไม่ได้ทำให้รู้สึกถึงการสำรวจความคืบหน้าของข้อมูลบ่อยเกินไปเป็นแบบสำรวจความคิดเห็นทำให้สิ้นเปลืองพลังงานบางอย่าง อย่างไรก็ตามในกรณีของข้อมูลที่มีขนาดเล็กนั้น เวลาในการดาวน์โหลดจะสั้น แต่ผู้ใช้อาจมีความต้องการที่จะติดตามความคืบหน้า ของกลไกในการปรับตัวขึ้นอยู่กับขนาดของข้อมูลอาจเป็นทางออกที่เหมาะสม

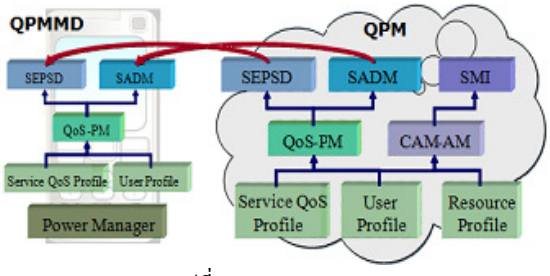


รูปที่ 1 การใช้พลังงาน CloudTorrent และความเร็วในการดาวน์โหลด

จากภาพจะแสดงให้เห็นว่าข้อมูลจะถูกย้ายไปเป็นแฟ้มไปยังอุปกรณ์มือถือเพื่อการใช้งานในภายหลัง ซึ่งทางเลือกอื่น ๆ นอกจากนี้ยังเป็นไปได้ที่ผู้ใช้จะสามารถส่งข้อมูลไปยังโทรศัพท์มือถือจากเซิร์ฟเวอร์ แสดงให้เห็นว่าการย้ายการทำงานของลูกค้าไปยังกลุ่มข้อมูล ทำให้ง่ายสำหรับอุปกรณ์มือถือ การใช้พลังงานจะลดลง การส่งข้อมูลจะลดลง และการเข้าถึงข้อมูลบนกลุ่มเซิร์ฟเวอร์จึงเป็นไปได้ในหลายวิธีการดังกล่าว เป็น HTTP หรือสตรีมมิ่งได้อย่างรวดเร็วก่อนใช้เซิร์ฟเวอร์เพื่อดาวน์โหลดเนื้อหาที่ข้อมูลเป็นประโยชน์สำหรับผู้ใช้โทรศัพท์มือถือที่มีแนวโน้ม แต่ความเป็นไปได้ในกลุ่มเซิร์ฟเวอร์จะต้องตรวจสอบต่อไปทั้งจากรูปแบบเครือข่ายและด้านธุรกิจ

A Framework for QoS and Power Management in a Service Cloud Environment with Mobile Devices [12] เน้นไปที่การจัดการการใช้พลังงานประมวลผล และพลังงานในการติดต่อสื่อสารให้มีความสมดุลกันออกแบบกรอบงานของ Qos และการจัดการพลังงาน QPM ในการใช้บริการ Cloud บนอุปกรณ์พกพา System Model การบริการที่มีการจัดการการใช้การกระจายตารางแฮช DHT การบริการและแบบจำลอง

ข้อจำกัดโดยทั่วไปของอุปกรณ์พกพา คือการคำนวณ และการเก็บข้อมูล โดยจะขึ้นอยู่กับพลังงานแบตเตอรี่ในการใช้งาน การแสดงผลการบริการนั้นจะขึ้นอยู่กับส่วนประกอบในอุปกรณ์พกพาที่สามารถใช้งานได้ ถ้าสามารถตอบสนองความต้องการทรัพยากรสามารถเข้าถึงการให้บริการ cloud ผ่านสถานีฐาน ยังมีในการแสดงข้อมูล DHT ให้ทำการแทน สำหรับลูกค้าเพื่อให้สามารถเรียกใช้บริการได้ ส่วน QPM Framework นั้นจะอำนวยความสะดวก QoS และการจัดการพลังงานบนโทรศัพท์มือถือในสภาพแวดล้อมที่ให้บริการ Cloud ได้เสนอกรอบงาน QPM ที่พยายามที่จะลดการใช้พลังงานในโทรศัพท์มือถือในขณะที่คุณภาพความต้องการ QoS ผ่านการประสานงานของโทรศัพท์มือถือ และการให้บริการ cloud กรอบงาน QPM แสดงอยู่ในรูปที่ 2 มีสองคู่ QPM บน service cloud (ขนาดเต็มรูปแบบ QPM) และ QPM บนโทรศัพท์มือถือ (QPMMD)



รูปที่ 2 QPM framework

การบริการโปรไฟล์ QoS ให้บริการ QoS และข้อมูลพฤติกรรมพลังงานการให้บริการภายใต้การกำหนดค่าที่แตกต่างกัน นอกจากนี้กำหนดข้อมูลส่วนตัวของผู้ใช้รูปแบบการใช้บริการ cloud ซึ่งรวมถึงโปรไฟล์สำหรับทุกบริการ และผู้ใช้โทรศัพท์มือถือช่วยให้แบบจำลองบางส่วนง่ายและ QoS - PM (QoS โมดูลคาดการณ์) ใช้ข้อมูลในประวัติที่ระบุไว้ในโปรไฟล์ของผู้ใช้ไปคาดการณ์รูปแบบการบริการที่มีศักยภาพ การใช้งานของผู้ใช้บางประการขึ้นอยู่กับรูปแบบการใช้งาน QoS - PM ในการให้บริการ cloud ประมาณพฤติกรรม QoS ที่อาจเกิดขึ้น สำหรับผู้ใช้เฉพาะการเรียกบริการที่เจาะจง QoS - PM ในโทรศัพท์มือถือ ในทางกลับกันการประมาณการการรวมตัวของพฤติกรรม QoS สำหรับทำงานหลาย ๆ บริการ ทั้งการให้บริการ cloud และโทรศัพท์มือถือ มีการจัดสรรบริการโมดูลการตัดสินใจ SADM ซึ่งทำให้การตัดสินใจ สำหรับการจำลองแบบบริการบนโทรศัพท์มือถือ SADM ใน service cloud หากดำเนินการให้บริการบนโทรศัพท์มือถือ สามารถปรับปรุง latency อย่างมาก (การสื่อสารไม่มี latency) จากนั้นบริการยังสามารถติดตั้งบนโทรศัพท์มือถือ สำหรับบริการที่เกี่ยวข้องกับฐานข้อมูลที่เกี่ยวกับการทำซ้ำข้อมูลจะได้รับการพิจารณา SADM ทำให้การจัดสรรคำแนะนำตามข้อมูล บนโทรศัพท์มือถือในการตัดสินใจขั้นสุดท้ายพิจารณาคำแนะนำการติดตั้งรวมทั้งการตั้งค่าของผู้ใช้และสภาพแวดล้อมในการทำงานของอุปกรณ์ที่อาจเกิดขึ้นในอนาคต เช่น หากผู้ใช้ต้องการจะใช้บริการบางอย่างในโหมด standalone การบริการควรจะติดตั้งบนโทรศัพท์มือถือทั้งการให้บริการ cloud และโทรศัพท์มือถือให้แพลตฟอร์มการดำเนินการบริการตัดสินใจเลือก (SEPSD) ซึ่งทำให้การตัดสินใจว่าจะใช้การบริการในท้องถิ่นบนโทรศัพท์มือถือหรือสามารถเรียกใช้บริการจากระยะไกลใน cloud เช่นหากเวลาในการคำนวณการบริการสั้นและข้อจำกัดเรียลไทม์ก็อาจจำเป็นต้องเรียกใช้การบริการในท้องถิ่นเพื่อให้เกิด latency ต่ำ เมื่อข้อจำกัดเรียลไทม์ของงานที่สร้างความพึงพอใจ ซึ่งการบริการจากระยะไกลจะช่วยประหยัดพลังงานในโทรศัพท์มือถือโมดูล SEPSD ในการให้บริการ cloud และโมดูล SEPSD บนโทรศัพท์มือถือสำหรับการตัดสินใจระยะยาวและระยะสั้นจะต้องตามลำดับ SEPSD ในการให้บริการ cloud จะดำเนินการวิเคราะห์ที่ครอบคลุมและการตัดสินใจ สำหรับเงื่อนไขการดำเนินต่างๆโมดูล SEPSD บนโทรศัพท์มือถือจะใช้ผลการวิเคราะห์จากการ

ให้บริการและใช้เพื่อให้เกิดการตัดสินใจเลือกใช้แพลตฟอร์ม ผู้ใช้สามารถประกอบเป็นการบริการเพื่อให้ได้งานที่ต้องการ ในบางครั้งการบริการที่ต้องการอาจจะใช้แพลตฟอร์มที่อยู่ห่างไกลออกไปจากไคลเอนต์หรือแพลทฟอร์มการบริการส่งผลให้ latency การสื่อสารสูง ดังนั้นกรอบการให้บริการโครงสร้างพื้นฐานด้านการโยกย้ายการบริการ SMI ให้การบริการการโอนย้ายให้ลด latency การสื่อสาร SMI ดูแลโปรไฟล์ของทรัพยากรซึ่งจะเจาะจงให้สามารถใช้ได้การทุกแพลตฟอร์มที่อาจจะถูกใช้สำหรับการย้ายการบริการ SMI วิเคราะห์โปรไฟล์ของการบริการและโปรไฟล์ผู้ใช้ให้เฉพาะที่พบบ่อยเป็นผู้ที่เข้าใช้การบริการสำหรับการตัดสินใจการโยกย้าย CAM - PM การสื่อสารการเข้าถึงและการโยกย้ายโมดูลคาดการณ์ ค่าใช้จ่ายได้รับการประมาณการในค่าใช้จ่ายในการสื่อสาร ในกรณีของการโยกย้ายวิเคราะห์ค่าใช้จ่ายในการโยกย้ายรวมทั้งค่าใช้จ่ายที่อาจเกิดขึ้นสำหรับเข้าใช้งานย้อนกลับไปยังแหล่งข้อมูลเพื่อให้แน่ใจว่า การโยกย้ายเป็นประโยชน์ พิจารณาค่าใช้จ่ายทั้งหมดจากข้อมูลที่ให้ SMI กำหนดว่าให้ย้ายการบริการที่ใช้บ่อย โดยผู้ใช้ ให้แพลตฟอร์มใน service cloud ที่ใกล้เคียงกับการตัดสินใจ ไม่เพียงแต่ขึ้นอยู่กับข้อมูลที่เกี่ยวข้องกับผู้ใช้ แต่ยังขึ้นอยู่กับบทบาทของผู้ใช้ในการบริการ ที่ประกอบด้วยบนอุปกรณ์มือถือพลังงานระดับต่ำเพื่อจัดการใช้เทคนิคการจัดการพลังงานที่มีอยู่ให้ควบคุมการตั้งค่า สำหรับส่วนประกอบในโทรศัพท์มือถือดังตารางที่ 5

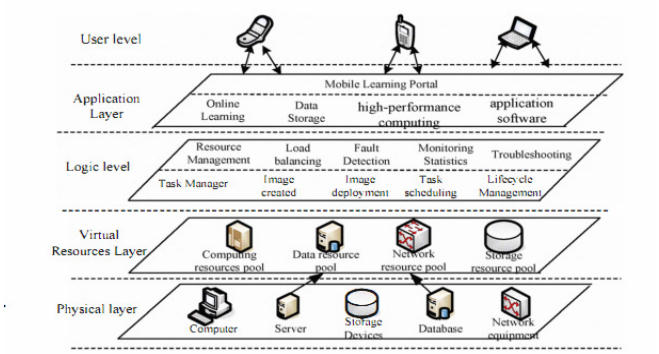
ตารางเปรียบเทียบด้านพลังงาน

	CloudAV	CloudTorrent	QOS
หน่วยความจำ	-มีการปรับปรุงลายเซ็นของโปรแกรมจะทำได้รวดเร็วขึ้นและใช้ CPU น้อย -หน่วยความจำโดยรวมลดลงมีการเก็บลายเซนในศูนย์ข้อมูลไม่ได้อยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้	-เมื่อมีการโหลดข้อมูลมากจะจัดเก็บในเครื่องจะทำให้เปลืองเนื้อที่ในหน่วยความจำ	-มีการจัดการประมวลผลให้สมดุลกับการออกแบบQOS และ QPM
ทรัพยากร	-แต่ละไฟล์ใช้ทรัพยากรน้อยกว่าการใช้ลายเซ็นฐานข้อมูลท้องถิ่น	-ถ้าข้อมูลมีขนาดเล็กเวลา Download จะสั้นขึ้นอยู่กับขนาดข้อมูล	-สามารถตอบสนองความต้องการของทรัพยากรและเข้าถึงการใช้บริการ Cloud ผ่านสถานีฐาน
บริการ	-มีการโอนไฟล์ไปยังเครือข่ายเพื่อทำการวิเคราะห์ -ต้องไปดึงโปรแกรมมาจาก Server ผู้ผลิต ถ้าเป็นเวอร์ชั่นฟรีคนใช้เยอะ Server อาจล่มได้	-ผู้ใช้สามารถส่งข้อมูลจากมือถือไปยัง Server ทำให้การย้ายการทำงานของลูกค้าไปยังกลุ่มทำได้ง่าย การใช้พลังงานลดลง การส่งลดลง	-ขึ้นอยู่กับส่วนประกอบ ของอุปกรณ์พกพาที่ใช้งาน และรูปแบบการใช้งาน QOS
ติดต่อสื่อสาร	-สูง สามารถเข้าถึงอุปกรณ์อื่น ๆ ที่ใช้ผ่านทางไกล	-การสื่อสารกับServerทั้งหมดจะดำเนินการผ่านการเชื่อมต่อ HTTP	-มีการจัดสรรการบริการโดยใช้โมดูลSADM เพื่อให้การสื่อสารไม่มี latency
ความปลอดภัย	-เนื่องจากCloudAV จัดเก็บข้อมูลของไฟล์ที่ปลอดภัยและเป็นไวรัสทำให้ Cloud Antivirus แสกนเร็วขึ้นเหมือนมี Whitelist ในตัว	- สูง เนื่องจากมีการตรวจสอบและควบคุมการทำงานของ Software และทรัพยากร	- เป็นการรักษาความปลอดภัยที่ดีที่สุดสำหรับการโจมตีแบบปฏิเสธในการให้บริการ
หลักทำงาน/การให้บริการ	-เป็นแบบ Automatic ใช้งานง่ายเพราะระบบจะเช็คว่าไฟล์ไหนเป็นไวรัส สามารถตัดสินใจได้ด้วยตนเองไม่ต้องถามผู้ใช้ -ทำงานคล้าย P2P ดังนั้นต้องส่ง/รับข้อมูลตลอดเวลา	-สามารถควบคุมจากระยะไกลจาก Server โดยระบุความคืบหน้าการ Download และการถ่ายโอนไฟล์ที่Download ไปยังโทรศัพท์	- หากต้องการใช้โหมด standalone การบริการจะติดตั้งที่อุปกรณ์พกพาทั้งในบริการ cloud และอุปกรณ์พกพาโดยให้แพลตฟอร์มช่วยตัดสินใจเลือก ว่าจะใช้บริการแบบ local บนมือถือหรือจะใช้บริการจาก cloud ระยะไกล

ตารางที่ 5 เปรียบเทียบด้านพลังงาน

III. ด้านสถาปัตยกรรม

มีการนำเสนอสถาปัตยกรรมในการประยุกต์ใช้ Cloud เพื่อช่วยในการทำงานด้านต่างๆโดยการออกแบบกรอบงานสำหรับการใช้ cloud computing บน mobileในระบบต่าง โดยในเรื่อง **System Design of Cloud Computing Based on Mobile Learning** [2] ได้นำเสนอรูปแบบสถาปัตยกรรมของโทรศัพท์มือถือสำหรับการเรียนรู้ ซึ่งเดิมนั้นจะมีปัญหาในเรื่องของการคำนวณ และพื้นที่เก็บข้อมูลในโทรศัพท์มือถือที่มีขนาดเล็ก ทำให้เป็นอุปสรรคต่อการส่งเสริมการเรียนรู้ในอนาคตของโทรศัพท์มือถือ เพื่อแก้ปัญหาปัญหาจึงได้นำแนวคิดของ Cloud Computing ในการพัฒนาแบบกระจายข้อมูลแบบขนานและแบบ Grid เพื่อก่อให้เกิดแนวทางที่เหมาะสม ซึ่งหลักการพื้นฐานของ Cloud Computing คือรวมจำนวนข้อมูลสำหรับเก็บไว้กระจาย และทรัพยากรในการประมวลผล สำหรับการทำงานร่วมกัน ดังนั้นจึงช่วยให้ผู้ใช้ สามารถเข้าถึงข้อมูลที่ต้องการได้อย่างรวดเร็ว Hadoop เป็นการดำเนินงานที่มาเปิดการให้บริการ ซึ่งเป็นกรอบการทำงานและระบบแฟ้มแบบกระจาย (HDFS, Hadoop Distributed File System) จากการที่กรอบการทำงานแต่ละโหนด Hadoop จะดำเนินงานโดยมีความสามารถทำหน้าที่เกี่ยวกับ HDFS และ MapReduce ซึ่งประเภทโหนด Hadoop คือเป็นการดำเนินงานที่มาเปิดการให้บริการ theMapReduce ซึ่งเป็นกรอบการทำงานและระบบแฟ้มแบบกระจาย จากการที่แต่ละโหนด Hadoop จะดำเนินงานทำหน้าที่เกี่ยวกับ HDFS และ MapReduce ซึ่ง Hadoop ในการแนะนำรูปแบบของโทรศัพท์มือถือการเรียนรู้ตาม hadoop และโมดูลการทำงานคือ วิเคราะห์กระบวนการทำงานตามรูปแบบของการใช้เทคโนโลยี Hadoop และสถาปัตยกรรมซึ่งแบ่งออกเป็น 5 ชั้นดังแสดงในรูปที่ 3



รูปที่ 3 การเรียนรู้บนมือถือตามแบบ hadoop

ระดับผู้ใช้ (User Layer) : การเรียนรู้ของโทรศัพท์มือถือความต้องการของลูกค้า โดยผู้ใช้จะต้องสามารถเข้าสู่ระบบเว็บบราวเซอร์ที่สามารถแสดงความหลากหลายของบริการประยุกต์ใช้ในหน้า (Portal) ของสถาปัตยกรรม

ระดับแอพพลิเคชั่น (Application Layer) : ประกอบด้วยโทรศัพท์มือถือการเรียนรู้แบบ Portal และการให้บริการของโปรแกรมประยุกต์ซึ่งมีคุณสมบัติของการตรวจสอบสำหรับผู้ใช้ที่แตกต่างกันและสะดวกสบายเพื่อการบริการที่แตกต่างกันสำหรับผู้เรียนแต่ละคน โดยผู้ใช้สามารถเพลิดเพลินกับการเรียนรู้ Portal ออนไลน์มาก หน่วยเก็บข้อมูลคอมพิวเตอร์ที่มีประสิทธิภาพสูง การประยุกต์ใช้ซอฟแวร์และบริการอื่น ๆ ในการออกแบบซึ่งรูปแบบการใช้และคุณสมบัติที่แข็งแกร่งของแพลตฟอร์ม Cloud Computing จะมี API สำหรับการเข้าถึงพอร์ตอื่น ๆ cloud server สามารถเข้าถึง cloud server อื่น ๆ เพื่อให้บริการอื่น ๆ ตามที่ระบุสถานการณ์หรือสามารถนำไปใช้ในการเข้าถึงทรัพยากร เพื่อขจัดปัญหาที่มาจากการกระจายไม่เท่ากันของทรัพยากรและตระหนักถึงใช้งานร่วมกันแบบเต็มของทรัพยากร

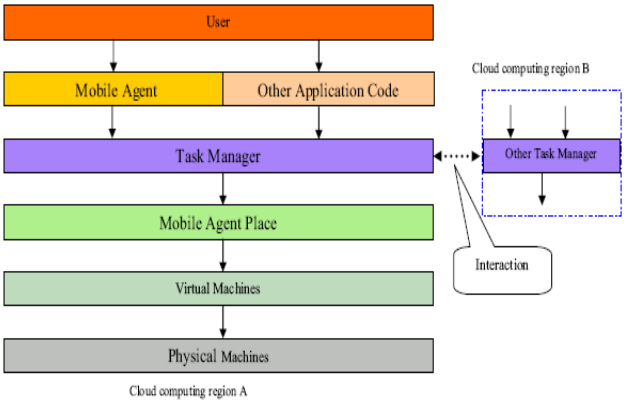
ระดับลอจิก (Logic level) : ชั้นตรรกะและทรัพยากรเสมือนเป็นชั้นการจัดการหลักของ Cloud Computing โครงสร้างพื้นฐาน ตั้งอยู่ระหว่างการให้บริการและตรรกะบริการกลุ่มที่อยู่ในค่าใช้จ่ายของทรัพยากรการบริหารจัดการการเรียนรู้แบบมือถือและกำหนดการต่าง ๆ ของผู้ใช้โปรแกรมประยุกต์เพื่อให้แจ้งให้ทรัพยากรที่สามารถให้บริการที่มีประสิทธิภาพและปลอดภัยเป็นความรับผิดชอบสำหรับการจัดการทรัพยากรโดยใช้โหนดทั้งหมด รูปแบบตรวจจับความล้มเหลวของโหนดและความพยายามที่จะเรียกคืน และการตรวจสอบสถิติการใช้งานทรัพยากรเพื่อการใช้งานหลักของแต่ละโหนด

Virtual Resources Layer: virtualization เป็นพื้นฐานเทคโนโลยีการออกแบบที่ใช้กับโครงสร้าง Cloud ทั้งหมดใน Cloud Computing ซึ่งส่วนใหญ่หมายถึงบทบาทในรูปแบบนามธรรมของในทรัพยากรทางไอที มาจากคนของทรัพยากร การใช้งานและการประยุกต์ใช้ ซึ่งใช้เทคโนโลยีเสมือนจริง ฮาร์ดแวร์ ซอฟต์แวร์และบริการ

ชั้นกายภาพ (Physical layer): จะใช้ในการสนับสนุนเครือข่ายขั้นพื้นฐาน สภาพแวดล้อมรวมทั้งเครื่องคอมพิวเตอร์ที่เก็บสินค้า โดยเครือข่ายจะเชื่อมต่อระหว่างอุปกรณ์ ฐานข้อมูลทรัพยากรและความหลากหลายของการเรียนรู้ฐานข้อมูลทรัพยากรในเครือข่าย ผ่านทางเทคโนโลยีเครือข่ายที่มีอยู่และเทคโนโลยีกระจายเทคโนโลยีการทำงานแบบเสมือนคอมพิวเตอร์จะได้รับการกระจายผนวกเข้ากับความสามารถที่เหนือกว่าจะใช้สำหรับ Cloud การดำเนินการคำนวณ เช่นการคำนวณและการเก็บรักษา

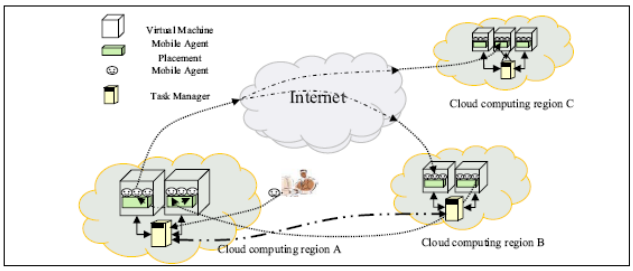
Realization of Open Cloud Computing Federation Based on Mobile Agent [4] เสนอสถาปัตยกรรมองค์ประกอบของ MABOCCF และการทำงานร่วมกันระหว่างแพลตฟอร์มที่แตกต่างกันบน Cloud Computing ถึงแม้ว่า Cloud Computing นั้นจะได้รับการยอมรับโดยทั่วไปว่าเป็นเทคโนโลยีที่จะมีบทบาทในอนาคต Cloud Computing นั้นได้มีการนำเสนอในหลายแพลตฟอร์มที่จะแตกต่างกัน ซึ่งจะต้องตระหนักถึงการทำงานร่วมกันด้วย เพื่อเป็นจุดเริ่มต้นของการนำเสนอ Cloud Computing ที่จะกลายมาเป็นส่วนหนึ่งในอนาคตของ Cloud Computing และจะเป็นแรงจูงใจสำหรับการรวมกันของตัวแทนมือถือและ Cloud Computing เพื่อให้มีประสิทธิภาพการทำงาน ซึ่ง API ของ Cloud ที่จะแตกต่างกัน แพลตฟอร์มของคอมพิวเตอร์ CCSP แต่ละอันจะมีขนาดใหญ่ทำให้ Cloud Computing ไม่สามารถละทิ้งแพลตฟอร์มในปัจจุบันและนำมาตรฐาน Cloud อันใหม่มาใช้เป็น IBM และ Microsoft สำหรับมาตรฐาน Cloud Computing การบริการ Cloud Computing ที่แตกต่างกัน CCSP ไม่

สามารถโยกย้าย และทำงานร่วมระหว่างกัน แนวคิด OCCF และแบบจำลอง มีจุดมุ่งหมายเพื่อสนับสนุนการพัฒนาระบบและเทคโนโลยีการบริการที่จะ เป็นโครงสร้างพื้นฐานสำหรับ Cloud Computing ข้อเสนอรูปแบบและสถาปัตยกรรมนั้น พยายามที่จะใช้อินเตอร์เฟซและตารางโปรโตคอลเพื่อตระหนักถึงการทำงานร่วมกันระหว่าง Cloud หรือ ผู้ให้บริการโครงสร้างพื้นฐาน ซึ่งเทคโนโลยี Cloud Computing จะให้โอกาสสำหรับตัวแทนมือถือในการแสดงความสามารถของ Cloud สำหรับแพลตฟอร์มของตัวแทนจำหน่ายโทรศัพท์มือถือมีความเป็นไปได้เพราะระบบตัวแทนมือถือจะขึ้นอยู่กับการสนับสนุนจาวา เช่น Aglets และ D'Agen ใน Cloud Computing หลายแพลตฟอร์ม ปัจจุบันนี้เครื่องแต่ละเครื่องจะต้องสนับสนุน OS ที่แตกต่างกันในระบบปฏิบัติการ เช่น ลินุกซ์และ Windows เนื่องจาก Java สามารถเขียนครั้งเดียวทำงานได้ทุกที่ดังนั้น ตัวแทนมือถือสามารถทำงานใน JVMs (Java Virtual Machine) ซึ่งติดตั้งบน OSs เหล่านี้ ข้อเสนอที่เรียกกลไกใหม่ MABOCCF (Mobile Agent Based Open Cloud Computing Federation) ซึ่งจะรวมตัวแทนมือถือกับ Cloud Computing เพื่อสร้าง Cloud Computing กลไกที่สามารถพกพาและตระหนักถึงการทำงานร่วมกันระหว่างแพลตฟอร์มที่แตกต่างกันใน Cloud Computing สถาปัตยกรรมและองค์ประกอบของ MABOCCF นั้นจะเสนอความเข้ากันได้นั้นกลไกของผู้ใช้งาน โทรศัพท์มือถือแต่ละตัวแทนมือถือทำงานบนแผนที่ (Mobile Agent Place) เสมือนเป็นเครื่องที่สามารถมีได้มากกว่าหนึ่งแผนที่เมื่อเครื่องที่ให้บริการโดย CCSPs สามารถย้ายข้อมูลให้ตระหนักถึงความง่ายในหมู่ CCSPs ถึงแม้ว่าพวกจะไม่เหมือนกัน ในขณะเดียวกันการทำงานร่วมกันโดยการเจรจาต่อรองและการทำงานร่วมกันระหว่างตัวแทนตามมาตรฐานในการทำงานร่วมกับตัวแทน เช่น MASIF และ FIPA เพราะการตะหนักถึงการพกพาและการทำงานร่วมกันทำให้มีความเป็นไปได้สำหรับ implemention ของสถาปัตยกรรมของ MABOCCF ที่แสดงในรูปที่ 4 JVM (Java Virtual Machine) และแผนที่ (Mobile Agent Place) มีการติดตั้งในเครื่องเสมือนทุกเครื่องใน CCR และ CCSP หรือผู้ดูแลระบบในโดเมนกระบวนการนี้สามารถทำได้โดยอัตโนมัติ เสมือนเครื่องกายภาพเลือกที่จะทำหน้าที่เป็น TS จะเป็นจุดเชื่อมภูมิภาคของ CCR ในการผลิต



.รูปที่ 4 สถาปัตยกรรมของตัวแทนจากมือถือนำเสนอ Cloud Computing

กลไกการ MABOCCF จะปรากฏในรูปที่ 5 ผู้ใช้ส่งตัวแทนมือถือเพื่อ TS อ่านหัวของโทรศัพท์มือถือตัวแทนในการตัดสินว่าเป็นตัวแทนมือถือหรือชนิดข้อมูลอื่น ๆ แพคเกจ TS แล้วตรงกับความต้องการทรัพยากรของดัชนีการตัดสินใจที่แผนที่ตัวแทนมือถือ ควรจะส่งไป หรือกำหนดให้เครื่องเสมือนใหม่ที่มีแผนที่สำหรับโทรศัพท์มือถือนี้ ตัวแทนจำหน่าย เมื่อแผนที่ได้รับตัวแทนมือถือก็เปิดใช้งาน ตัวแทนมือถือและดำเนินงานรวมทั้งในตัวแทนมือถือการกำหนดเริ่มดำเนินการในเครื่องเสมือน ตัวแทนมือถือจะตรวจสอบการทำงานของงาน และสถานการณ์ของทรัพยากรในแผนที่ให้ตัดสินใจว่าจะออกจากแผนที่หรือตัวแทนมือถือ และส่งให้แผนที่อื่น ๆ (ใน CCSP เดียวกันหรือในที่แตกต่างกัน CCSP) เพื่อบรรลุผลงาน ตัวแทนจำหน่ายโทรศัพท์มือถือสามารถดำเนินงานและย้ายไปมาระหว่างแผนที่ใน CCR หรือแผนที่ที่กระจายกว่า CCRs ที่แตกต่างกัน ซึ่งต้องตระหนักถึงคอมพิวเตอร์พกพา ตัวแทนมือถือสามารถต่อรองได้ และทำงานร่วมกันผ่านการสื่อสารเพื่อ ตระหนักถึงการทำงานร่วมกันระหว่าง CCSPs ที่แตกต่างกัน TS สามารถทรัพยากร CCRs อื่น ๆ แผนที่ (ซอฟแวร์ ฮาร์ดแวร์ และข้อมูล) เพื่อ CCR ของตามกฎระเบียบบริหารท้องถิ่นหากพวกเป็นทรัพยากรท้องถิ่น หรือส่งตัวแทนมือถือเพื่อ CCR อื่น ๆ เมื่อทรัพยากรของ CCR ท้องถิ่นหายาก ดังนั้นกลไกนี้ สำหรับผู้ใช้ที่ตระหนักถึงความยืดหยุ่นสูง ของทรัพยากรในการคำนวณ Cloud ในกรณีที่เรียบง่ายของผู้ใช้งานจะถูกกำหนดให้ตัวแทนจำหน่ายอุปกรณ์มือถือ การโต้ตอบกันระหว่างการทำงานของงาน TS ตัวแทนจำหน่ายโทรศัพท์มือถือและส่งไปยังแผนที่เพื่อปฏิบัติการตัวแทนจำหน่ายโทรศัพท์มือถือสามารถโยกย้ายจากที่หนึ่งไปยังอีกแผนที่ในช่วงหนึ่งและจะถูกส่งกลับโดยตรงไปยังผู้ใช้หรือ ส่งมอบให้กับผู้ใช้โดย TS



รูปที่ 5 Mobile Agent Based ในการนำเสนอ Cloud Computing

กรณีที่ซับซ้อนมากขึ้นก็คืองานถูกกำหนดให้กับหลายตัวแทนมือถือและตัวแทนจำหน่ายโทรศัพท์มือถือ ร่วมมือกับการควบคุมการทำงานให้สำเร็จสามารถย้ายตัวแทนมือถือ ในแผนที่แตกต่างกัน ในขณะที่ให้ความร่วมมือ กรณีที่ซับซ้อนมากที่สุดก็คืองานจำนวนมากถูกกำหนดให้กับ ตัวแทนจำหน่ายโทรศัพท์มือถือ ทำงานร่วมกันและได้แข่งขันเพื่อตอบสนองความต้องการ ตัวอย่างเช่นในกรณีของ e - business ของตัวแทนมือถืออาจจะใช้งาน ตัวแทนมือถือถูกบังคับให้ย้ายไปยังแผนที่อื่นหรือมีความผิดปกติ

การวิเคราะห์ผลการดำเนินงานของ MABOCCF

MABOCCF เป็นกลไกการก่อให้เกิดการนำเสนอ Cloud จึงมีคุณสมบัติข้อดี และข้อได้เปรียบที่ไม่ซ้ำกันมาโดยการรวมกันของ

โทรศัพท์มือถือ ตัวแทนและ Cloud Computing มีความยืดหยุ่นของการใช้ทรัพยากรในการคำนวณซึ่งมีความสามารถในการปรับแต่งการโยกย้ายงานโดยผู้ใช้หรือบุคคลที่สามจะช่วยลดภาระเครือข่ายและประสิทธิภาพการทำงานในการคำนวณแบบฉลาดมากขึ้น เปรียบเทียบกับ Cloud Computing MABOCCF ปัจจุบัน กลไกไม่สนับสนุนการพกพาระหว่าง CCSPs ที่แตกต่างกัน เนื่องจากการทำงานร่วมกันโดยเฉพาะที่เกี่ยวข้องกับการใช้งาน จะสร้าง MABOCCF 1.0 ต้นแบบ MABOCCF ในคอมพิวเตอร์เครื่องเดียวแล้วจะจำลองการปฏิบัติงาน 10 CCSPs (Cloud Computing ผู้ให้บริการ) สำหรับ MABOCCF และ NMBOCCF (กลไกการคำนวณ ที่ไม่สนับสนุนระหว่าง CCSPs ที่แตกต่างกัน) การทดลองเป็นครั้ง 3000 หน่วยเวลาเป็นการดำเนินการขั้นตอนที่กำหนดโดยโปรแกรม เช่นสมมติว่ามีงานถูกส่งไปยัง CCSP ที่เวลาเป็นแบบสุ่ม ค่าระหว่าง 0 ~ 100 งานทั้งหมดมาถึงที่เวลาที่เหมือนกัน เวลารันอีกทีมีค่าสุ่มอยู่ระหว่าง 1 ~ 10 คือ Wit = Nit * ETt มาถึงภาระงานของ CCSP ที่เวลา และ CCSPs ทั้งหมดมีความสามารถในการดำเนินการเดียวกัน EC EC ถูกตั้งค่าเป็น 275 เวลาภาระงานหน่วยงานมาถึงแต่ละ CCSP ได้ตลอดเวลาจะเหมือนกัน สำหรับ MBOCCF และ NMBOCCF และงานจัดการค่าใช้จ่ายปัจจัย TF ถูกตั้งค่าเป็น 0.03 USM (เฉลี่ยความพึงพอใจของผู้ใช้) และ URM (เฉลี่ยอัตราส่วนการใช้ประโยชน์) คอมพิวเตอร์และ OCCF เป็นการยากที่จะตระหนักถึงข้อเสนอของใน Mobile Agent Based การนำเสนอ Cloud Computing นี้กลไกมีวัตถุประสงค์เพื่อตระหนักถึงความง่ายและการทำงานร่วมกันระหว่างแพลตฟอร์มที่แตกต่างกัน Cloud Computing มีผลงานที่ดีในความพึงพอใจของผู้ใช้และสิ่งอำนวยความสะดวก อัตราส่วนการใช้ประโยชน์ในระบบ Cloud Computing ในอนาคตจะมีการใช้งานหลายล้านคนประกอบด้วยโมดูลเหล่านี้ตอบสนองการใช้งานสำหรับผู้ใช้จำนวนมากและความต้องการของผู้ใช้เป็นแบบไดนามิก

SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment [6] ได้นำเสนอสถาปัตยกรรมของระบบ Cloud-Computing ซึ่งแยกเป็น DaaS SaaS และ Haas ในการนำ SaaAS มาใช้บนมือถือในการให้บริการ Cloud Computing บนอินเทอร์เน็ต นำเสนอโทรศัพท์มือถือที่ได้มีการจัดจำหน่ายซอฟต์แวร์และการบริการข้อมูลสำหรับผู้ใช้ ทางอินเทอร์เน็ตโดยการใช้ระบบ Cloud Computing ในการปรับตัวในการทำงานทางอินเทอร์เน็ต ซึ่งจะประกอบไปด้วย 3 ส่วน

(1) แนะนำมือถือไปยังการให้บริการ Cloud Computing

(2) นำเสนอตัวที่กระทำกับcodeและข้อมูลในการให้บริการพร้อมทั้งกลไกการโหลดข้อมูลที่ได้รับบริการ SaaAS จากโทรศัพท์มือถือ

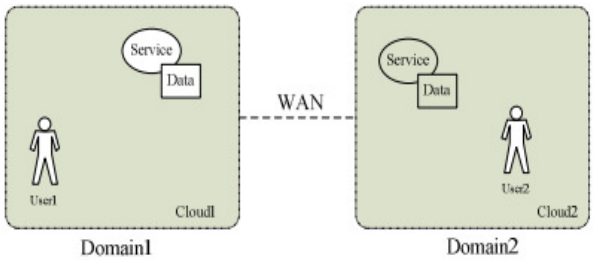
(3) นำเสนอข้อมูลที่มีวิธีการเชื่อมโยงกับ SaaAS โดยมีการแบ่ง Cloud และวิธีการกลไกต่าง ๆ (DCCM)

มือถือบนเครือข่ายอินเทอร์เน็ตหรือ WAN จะมีลักษณะอิสระต่อกัน มีการติดต่อ สื่อสารที่มีประสิทธิภาพสูงและป้องกันความผิดพลาด จุดประสงค์หลักระบบ Cloud Computing เพื่อใช้งานให้มีการกระจายเครือข่ายในลักษณะพื้นที่กว้าง เพราะสามารถประหยัดค่าใช้จ่ายการสื่อสารโดยการย้าย ทรัพยากรและบริการให้กับสภาพแวดล้อมที่กำหนดเป้าหมายระยะไกลเพื่อให้เหมาะสมกับผู้ใช้มือถือจึงได้นำเสนอการใช้มือถือแทนที่จะใช้ RPC / RMI เป็นต้นแบบที่จะใช้ในการย้ายการข้อมูลการเชื่อมโยงกันของไดเรคทอรี่ โดยการให้รับบริการ SaaAS ซึ่งมีความเหมาะสมที่จะทำงานในอินเทอร์เน็ต ซึ่งจะนำเสนอ Code และการโหลดข้อมูลในการให้บริการมือถือตามกลไกและมี Cloud เป็นตัวแบ่งกลไกการเชื่อมโยงกันซึ่งสุดท้ายก็จะมาบรรจบกัน SaaAS ซึ่งสามารถลดค่าใช้จ่ายในการสื่อสารได้อย่างมีประสิทธิภาพ ในอินเตอร์เน็ต SaaAS ถูกแบ่งออกเป็นจำนวนโดเมน ทำหน้าที่เป็นโดเมนหลักและรับผิดชอบในทุกโดเมนของผู้อื่น โดเมนทุกคนมีเซิร์ฟเวอร์ที่เรียกว่าโดเมน Server (DS) ที่วิ่งบนเครือข่ายสำหรับโทรศัพท์มือถือโดยใช้ SaaAS ซึ่งมี DS จำนวนมากโดยทำงานบนแพลตฟอร์มสำหรับโทรศัพท์มือถือ

SaaS และ DaaS มี 2 แนวคิด ได้แก่

1) ทางด้านซอฟแวร์ จะใช้การบริการ (SaaS) ซอฟท์แวร์จะถูกจัดเป็นการบริการและให้ไว้กับลูกค้าผ่านอินเตอร์เน็ต โหมดนี้จะช่วยลดความจำเป็นในการติดตั้งและเรียกใช้โปรแกรมประยุกต์ของลูกค้าในเครื่องข่ายคอมพิวเตอร์

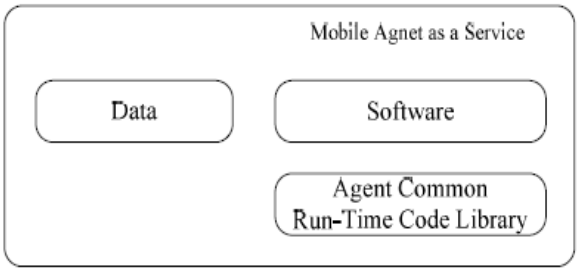
2) ข้อมูลการให้บริการ (DaaS) ซึ่งข้อมูลจะมีหลายรูปแบบและจากหลายแหล่งอาจจะเข้าถึงได้ผ่านทางผู้ใช้บริการในเครือข่าย เช่น จัดการข้อมูลระยะไกลเช่นเดียวกับการทำงานบนดิสก์หรือการเข้าถึงข้อมูลในอินเตอร์เน็ต



รูปที่ 6 SaaAS Cloud Computing ในระบบอินเตอร์เน็ต

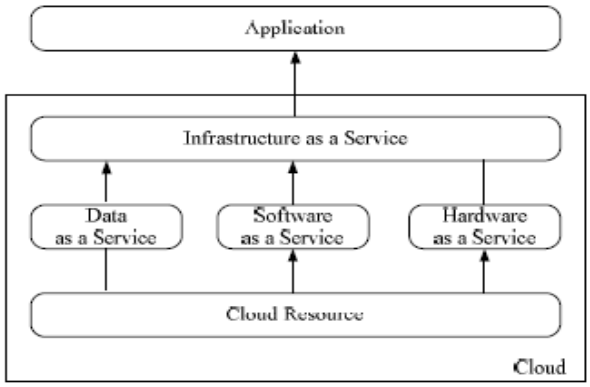
รูปที่ 6 แสดง User 1 ใน cloud 1 ที่ต้องการเข้าถึงข้อมูลที่จะเข้าถึงโดยตรงเรียกดูได้จาก cloud 1 จากนั้น cloud 1 เป็นผู้รับผิดชอบสำหรับการรวบรวมข้อมูลจากทั้งสอง cloud 1 และ cloud 2 และส่งกลับข้อมูลที่รวบรวมได้ให้กับผู้ใช้ซึ่ง cloud มีจัดหาตำแหน่งของแอปพลิเคชั่นเพื่อการใช้งาน

จากสถานการณ์นี้ cloud จะจัดเก็บข้อมูลและการเข้าถึงข้อมูล ซึ่งการสื่อสารระหว่าง cloud นั้นสามารถสื่อสาร ข้าม cloud ได้ข้อมูล cloud ไม่เพียงแต่จะต้องเข้าใช้งานในวง LAN เท่านั้นแต่ยังสามารถโยกย้ายใน WAN ได้แต่ในความเป็นจริง Cloud Computing เป็นซอฟแวร์และข้อมูลที่จะถูกแยกออกจากกันเสมอซึ่งจะขึ้นอยู่กับการดำเนินงานของผู้ใช้

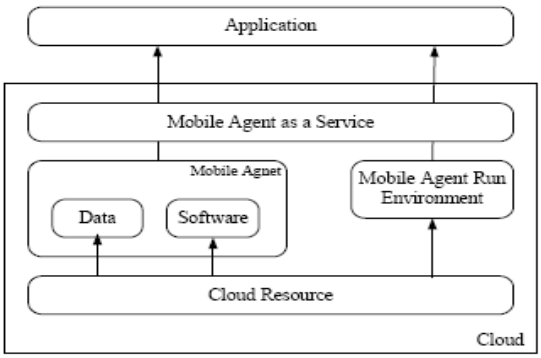


รูปที่ 7 แสดง Componet ของ WA ใน SaaAS

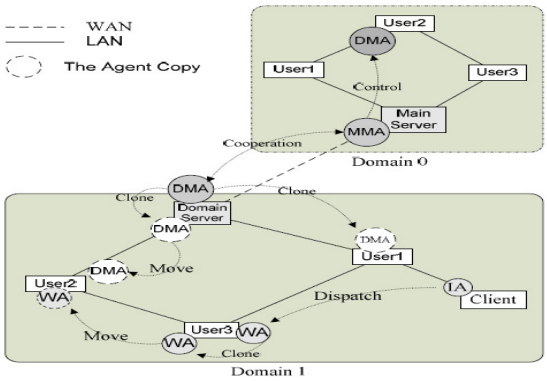
โทรศัพท์มือถือจะมีความยืดหยุ่นในการปรับตัวที่ดีถ้ามีการใช้งานที่มีความเหมาะสมในการทำงานในอินเทอร์เน็ต ร่วมกับ ซอฟแวร์ SaaAS และข้อมูลรวมกัน ดังรูปที่ 8 ที่แสดงมือถือใน SaaAS ซึ่งประกอบด้วย 3 ส่วนคือ ข้อมูล ซอฟแวร์และ Run-Time Code ที่รันอยู่ในไบนารี่



รูปที่ 8 สถาปัตยกรรมของระบบ Cloud Computing



รูปที่ 9 สถาปัตยกรรมของโทรศัพท์มือถือในระบบ Cloud Computing



รูปที่ 10 แสดงการแบ่งการทำงานและการร่วมมือการทำงานใน SaaAS

รูปที่ 10 ที่แสดงอยู่ใน SaaAS ทั้งหมดสามารถจัดอยู่ในประเภทดังต่อไปนี้

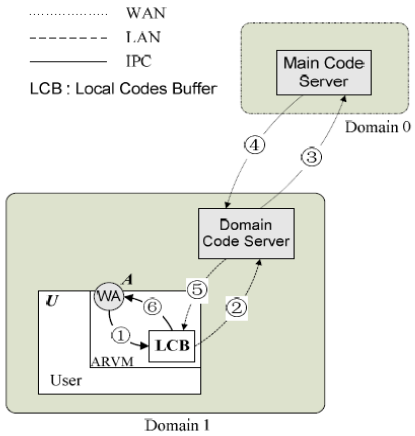
(1) IA (Interface Agent) IA ทำงานบนผู้ใช้และโต้ตอบกับผู้ใช้ จากนั้นจะทำการประมวลผลกับคอมพิวเตอร์แล้ว IA จะทำการควบคุมหรือการประสานงานกับตัวแทนอื่น ๆ

(2) WA (Working Agent) WA ยอมรับวิธีการจาก IA ของชุดซอฟแวร์และข้อมูลไปยังเซิร์ฟเวอร์โดเมนเป้าหมายเพื่อทำการรันข้อมูลแล้วส่งผลกลับมา

(3) DMA (Domain Manage Agent) DMA มีหน้าที่ในการจัดการโดเมน DMA จะเป็นแบบจำลองสามารถทำซ้ำด้วยตัวเองและสามารถย้ายไปยังกลุ่มเป้าหมาย ในเซิร์ฟเวอร์เพื่อที่จะได้ใกล้เคียงกับข้อมูลที่ต้องการเพื่อจะได้รับการประมวลผลและประสิทธิภาพที่สูงขึ้น

4) MMA (Main Management Agent) MMA จะรับผิดชอบในการบริหารจัดการและการประสานงานของ DMAs ทั้งหมดใน SaaAS ซึ่ง MMA และ DMA สามารถร่วมมือกันเพื่อจัดการใน SaaAS

SaaAS เป็นวิธีการจัดการซอฟแวร์และข้อมูลโดยการย้ายรหัสข้อมูลของมือถือ โดยจะทำการวิเคราะห์ประสิทธิภาพการทำงานของแพลตฟอร์มมือถือ 3 แพลตฟอร์มและหาที่โหลดข้อมูลซึ่งจะมีความสัมพันธ์ใกล้เคียงกันกับการโหลด Runtime Code และกลไกต่าง ๆ และถ้าหาก Runtime Code มีส่วนร่วมในมือถือก็จะโหลดอยู่ในระดับต่ำมาก แต่การสื่อสารเครือข่ายนั้นค่าใช้จ่ายจะสูงหากเพียงส่วนหนึ่งของ Runtime Code มีส่วนร่วมในมือถือนั้นต้องโหลดรหัสและ Runtime Code เซิร์ฟเวอร์ทำให้ศักยภาพการโหลดสูงเกินไป แต่ค่าใช้จ่ายในเครือข่ายการติดต่อสื่อสารจะอยู่ในระดับต่ำ ซึ่งจะมีกลไกการวางเซิร์ฟเวอร์ Code มือถือร่วมกันในทุกโดเมนรหัส (Code) และข้อมูลในการให้บริการตามกลไกต่าง ๆ



รูปที่ 11 Runtime Code ในการโหลดกลไกต่าง ๆ

รูปที่ 11 รหัสไม่ได้อยู่ในเครือข่ายท้องถิ่นทั้งโฮสต์และ DCS ดังนั้นจะต้องโหลดรหัสมาจาก MCS ให้ตัวแทนผู้ใช้งานทำการโหลดรหัสในขั้นตอนนี้ ซึ่งมี 6 ขั้นตอนดังต่อไปนี้

1) ตรวจสอบรหัสบัฟเฟอร์ของผู้ใช้ที่มีรหัสรันไทม์

2) User ขอรหัสเพื่อ DCS

3) DCS ขอรหัสเพื่อ MCS

4) MCS จะส่งค่ารหัสกลับไประหว่าง DCS

5) DCS จะส่งค่ารหัสกลับไปยังผู้ใช้

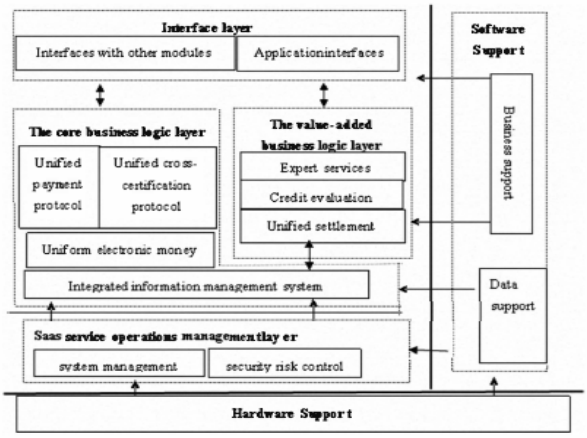
6) ผู้ใช้จะส่งค่ารหัส กลับไปยัง W A

ขั้นตอนนี้จะอธิบายไว้ข้างต้นขั้นตอน 3 และ 4 จะดำเนินการใน WAN ส่วนขั้นตอน 2 และทำงาน 5 จะดำเนินการใน LAN ส่วนขั้นตอน 1 และ 6 จะดำเนินการใน User โดย IPC (Inter-Process Communication) เพราะรหัสที่ต้องการจะถูกเก็บไว้ในบัฟเฟอร์ใน Client และ DCS เพื่อนำมาใช้ใหม่ การแบ่ง Cloudและกลไกการเชื่อมโยงกัน

SaaAS ได้ถูกออกแบบมาโดยมีเป้าหมายเพื่อที่จะช่วยลดการจราจรในเครือข่ายและสนับสนุนระบบปฏิบัติการ UNIX เมื่อมีการเข้าถึงข้อมูลในระบบ Cloud Computing ก็จะทำการแจกแจง Cloud และเชื่อมโยงกลไกต่าง ๆ (DCCM) แล้วจะนำเสนอใน SaaAS ซึ่ง DCCM สามารถลดการสื่อสารใน WAN โดยใช้การการเคลื่อนที่ ความยืดหยุ่น และ การโต้ตอบ ของโทรศัพท์มือถือ

Cloud แบ่งกลไกการเชื่อมโยงกันสุดท้ายก็มารวมกันใน SaaAS ไม่เพียงแต่มีข้อได้เปรียบแต่ยังใช้โทรศัพท์มือถือเพื่อปรับปรุงประสิทธิภาพ

The Framework of the Fourth Party Mobile Integrated Payment Platform Based on Cloud Computing [5]ได้นำเสนอสถาปัตยกรรมระบบบนพื้นฐานของทฤษฎี ในการชำระเงินมือถือ ตามแพลตฟอร์ม Cloud Computing แพลตฟอร์ม กรอบการทำงานบนมือถือแบ่งออกเป็น 4 ส่วนในการนำเทคนิคการชำระเงินมาใช้บน Cloud Computing เป็นที่วิเคราะห์ปัญหาของการชำระเงินมือถือรวมทั้งลักษณะของ Cloud Computing รวมกับการชำระเงินที่เกี่ยวข้อง กรอบการทำงานที่สมบูรณ์ของสี่แพลตฟอร์มบนมือถือ การชำระเงินตาม Cloud Computing และฟังก์ชั่น การชำระเงินจะเกี่ยวข้องกับผู้ประกอบการมือถือสถาบันการเงิน ระบบภาษี บริการเสริมอื่น ๆ ซึ่งผู้ให้บริการการชำระเงินธุรกิจและอื่น ๆ เกี่ยวกับการเก็บรักษาและการดำเนินงานของข้อมูลที่ต้องใช้ฮาร์ดแวร์และซอฟแวร์เพื่อประหยัดค่าใช้จ่ายซึ่งจะมีประสิทธิภาพและการใช้งานนั้นต้องเผชิญกับความต้องการ ซึ่งจะมีทางเลือกสามชนิดคือโหมดการทำงานของ CLOUD COMPUTING: Saas (Software เป็น Service) ซอฟต์แวร์และการให้บริการบริการ CLOUD COMPUTING ของผู้ประกอบการคอมพิวเตอร์ในรูปแบบของ ditect ในการให้บริการซอฟแวร์ Paas Platform แพลตฟอร์มและการให้บริการ CLOUD COMPUTING ผู้ประกอบการให้การพัฒนาของตนเอง และ plalform เพื่อปรับใช้งานในการพัฒนาบนพื้นฐานดังกล่าวจะมีการพัฒนาซอฟต์แวร์ของตนเองและบริการที่มีแก่ผู้ใช้ laas โครงสร้างพื้นฐานเกี่ยวกับบริการ CLOUD COMPUTING จะไม่ดำเนินการจัดการโครงสร้างพื้นฐานให้ซึ่งนักพัฒนาซอฟต์แวร์จะเป็นคนจัดและให้บริการไปยังหน่วยงาน เพื่อปรับใช้และจัดการ การรวมแพลตฟอร์มในการชำระเงินตาม CLOUD COMPUTING นั้นผู้ใช้และผู้ให้บริการของ CLOUD ในการคำนวณแพลตฟอร์มนี้จะสร้างขึ้นบนแพลตฟอร์มของ Cloud Computing Paas ผู้ประกอบการ Paas ให้ฮาร์ดแวร์และซอฟต์แวร์จัดการแพลตฟอร์มในการชำระเงินแบบบูรณาการ ในโหมดการใช้งานจะมีความยืดหยุ่น ดังนั้นสี่แพลตฟอร์มในการชำระเงินรวมกลายเป็นที่ให้ความสนใจใกล้เคียงกับเทคโนโลยีและบริการ ซึ่งสี่แพลตฟอร์มมือถือแบบบูรณาการในการชำระเงินมีหลายชนิด ในการเข้าใช้แพลตฟอร์มไม่จำเป็นต้องใช้บริการทั้งหมด เมื่อมี CLOUD แล้วจะให้บริการคำนวณ Saas ซึ่งจะแสดงข้อได้เปรียบของโทรศัพท์มือถือที่สี่แพลตฟอร์มแบบบูรณาการชำระเงินให้บริการ CLOUD เพื่อเข้าใช้งาน และการเข้าถึงจะสามารถเลือกบริการที่ต้องการและยังสามารถให้คำปรึกษาและโซลูชั่นที่เหมาะสมโดยเจ้าหน้าที่ผู้เชี่ยวชาญของแพลตฟอร์ม สำหรับผู้ใช้ไม่จำเป็นต้องไปสนใจกับซอฟแวร์และฮาร์ดแวร์และอื่น ๆ เพียงแค่กังวลเกี่ยวกับการบริการและการดำเนินงานที่มีประสิทธิภาพของธุรกิจ



รูปที่ 12 แผนภาพกรอบแพลตฟอร์ม การบูรณาการของการชำระเงินมือถือ

1) Cloud Computing Infrastructure Layer เป็นการให้บริการสนับสนุนฮาร์ดแวร์ในการใช้ CLOUD COMPUTING เป็นแพลตฟอร์มในการ

บริการตามความต้องการฮาร์ดแวร์ที่จำเป็น วิธีนี้เป็นระบบใช้เป็นช่องทางเพื่อให้การสนับสนุน และยังประหยัดค่าใช้จ่าย สนับสนุนซอฟท์แวร์รวมถึงการสนับสนุนข้อมูลและธุรกิจ

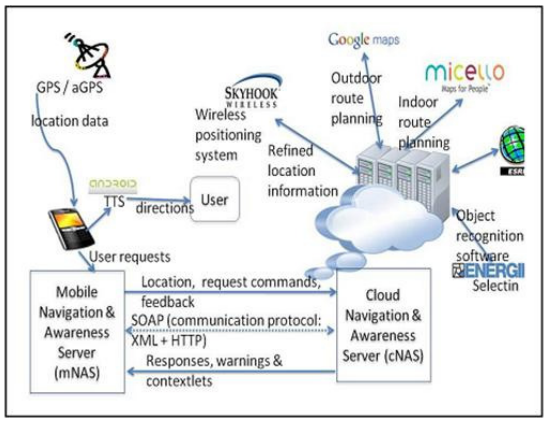
2) การบริการด้านการดำเนินงานการจัดการ Saas Layer ให้ดำเนินการระบบและการจัดการการดำเนินงาน โดยควบคุมให้มีประสิทธิภาพทำงานได้อย่างราบรื่นรวมทั้งการบริการระบบรักษาความปลอดภัยและการควบคุมความเสี่ยง หลักคือการจัดการทรัพยากรการประยุกต์ การจัดกลุ่มลูกค้า การจัดการการดำเนินงาน การจัดการบริการ ควบคุมความเสี่ยงด้านความปลอดภัย

3) Core Business Logic Layer กับการพัฒนาอย่างรวดเร็ว ในการชำระเงินมือถือค่อนข้างมีวิธีการชำระเงินที่หลากหลายและมีการพัฒนาอย่างจริงจังทางด้านอิเล็กทรอนิกส์และโปรโตคอลในการชำระเงินแบบครบวงจร ของรูปแบบการชำระเงินที่โพรโตคอลแสดงในการกำหนดรูปแบบการชำระเงินทั่วไป บนพื้นฐานของการพิจารณาความหลากหลายของการชำระเงินมือถือ โปรโตคอลที่รองรับมักจะดำเนินการรับรองตัวตนผู้ใช้ระหว่างโปรโตคอลการตรวจสอบ โดยเฉพาะอย่างยิ่ง การชำระเงินแต่ละคนและธนาคารที่แตกต่างกันจากหน่วยงานที่แตกต่างกันการซื้อขายในเวลาเดียวกัน

4) มูลค่าเพิ่มของ Business Logic Layer ในการประเมินเครดิต การดำเนินการครบวงจร การประเมินมีความน่าเชื่อถือทั้งผู้ซื้อและผู้ขายในการทำธุรกรรมและการชำระเงินของบุคคลที่สาม ในสี่โหมดการชำระเงินแพลตฟอร์มชำระเงินจะต้องสร้างเครดิตแบบครบวงจร เพื่อเป็นตัวบ่งชี้การประเมินผลการประเมินจากแพลตฟอร์มหรือ ข้อกำหนดของอินเตอร์เฟซ การประเมินเครดิตเฉพาะ หน่วยงานการในการให้คะแนนการประเมินการทำงานผ่านอินเตอร์เฟซไม่ว่าการชำระเงินของบุคคลที่สามหรือ เครือข่ายสามารถติดตั้งรวมเป็นหนึ่งเดียวในสี่แพลตฟอร์มการชำระเงินมือถือแบบบูรณาการและแพลตฟอร์ม ซึ่งแพลตฟอร์มยังสามารถให้ติดตั้งรวมเป็นหนึ่งเดียว อินเตอร์เฟซติดตั้งแบบครบวงจรโดยเฉพาะสถาบันการศึกษา ผ่านอินเตอร์เฟซนี้เพื่อให้เกิดการบริการ อย่างครบวงจร ซึ่งแพลตฟอร์มการชำระเงินจะต้องมีทีมงานผู้เชี่ยวชาญที่มีความสามารถที่ดีเยี่ยมสามารถ แก้ปัญหาการชำระเงินสำหรับการเข้าใช้แพลตฟอร์ม หรือให้คำแนะนำอย่างมืออาชีพ ซึ่งจำเป็นต้องใช้การเข้าถึง

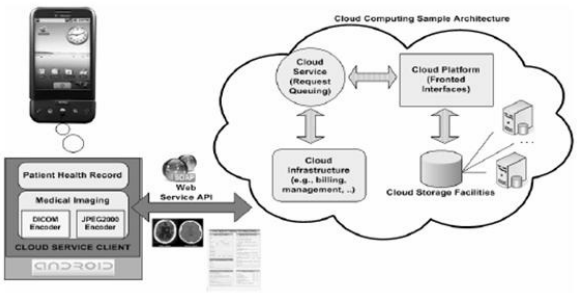
5) Layer Interface ใน Application การเชื่อมต่อ E - commerce ในอินเตอร์เฟซเพื่อเข้าถึงระบบธุรกิจแบบครบวงจร ซึ่งสี่แพลตฟอร์มของมือถือในการชำระเงิน เพื่อพัฒนาโปรโตคอลเข้าเป็นอันเดียวกันเป็นปฏิสัมพันธ์โปรโตคอลระหว่างระบบการค้าและบุคคลที่สาม ในการชำระเงินภายใต้โปรโตคอลเพื่อการเข้าถึงไปยังธุรกิจ ระบบอินเตอร์เฟซ นั้นมูลค่าเพิ่มของอินเตอร์เฟซในการเข้าถึงบริการแบบครบวงจรนี้ จะมีอินเตอร์เฟซให้บริการที่มีมูลค่าเพิ่มในการให้บริการ เพื่อให้มั่นใจว่าระเบียบและความสม่ำเสมอ ของอินเตอร์เฟซการชำระเงินเพื่อให้การชำระเงินแบบครบวงจร อินเตอร์เฟซธนาคารแต่ละแห่งโดยมีโปรโตคอลในการชำระเงิน ซึ่งทั้งสี่แพลตฟอร์มในการชำระเงิน รวมไปถึงโปรโตคอลกับธนาคารบนพื้นฐานของการรวมกันของโปรโตคอลในการชำระเงินแล้ว ให้ชำระเงินแบบครบวงจร อินเตอร์เฟซนั้นจะต้องติดต่อธนาคารเพื่อจัดให้มีระบบการธนาคารในการติดต่ออย่างครบวงจร

A Mobile-Cloud Collaborative Traffic Lights Detector for Blind Navigation [15] ได้นำเสนอสถาปัตยกรรมของการทำงานร่วมกันระหว่าง mobile กับ Cloud Computing ในการตรวจจับสัญญาณไฟจราจรสำหรับอำนวยความสะดวกให้แก่ผู้ที่ตาบอดหรือมีอาการผิดปกติทางสายตา โดยเสนอสถาปัตยกรรมของระบบนำทางที่มีการรับรู้บริบท เป็นสองระดับที่เห็นในภาพ 13 สองส่วนประกอบหลักคือ “Mobile Navigation and Awareness-Server” (mNAS) ซึ่งอาจเป็น smart phone ใด ๆ ในตลาดและ “Cloud-Navigation and Awareness Server” (cNAS) ซึ่งจะเป็นพื้นฐาน Web Services-Platform จะใช้เพื่อสนับสนุนความหลากหลายของฟังก์ชัน context-awareness mNAS จะรวมกับเครื่องรับจีพีเอส จะรับผิดชอบสำหรับการนำทางในการตรวจหาสิ่งกีดขวางและหลีกเลี่ยงรวมทั้งการโต้ตอบกับผู้ใช้ ทางด้าน cloud จะรับผิดชอบสำหรับจัดหาข้อมูลสถานที่ตั้งไปยัง cNAS ซึ่งจะดำเนินการที่ตำแหน่งที่ต้องการโดยเฉพาะฟังก์ชั่น และการสื่อสารข้อมูลที่ต้องการตลอดจนบริบทที่เกี่ยวข้อง (contextlets) และคำเตือนของอันตรายที่อาจเกิดในบริบทกลับไปยัง mNAS



รูปที่ 13 แสดงสถาปัตยกรรมของระบบตรวจจับสัญญาณไฟจราจร

Mobile Healthcare Information Management utilizing Cloud [8] ได้นำเสนอสถาปัตยกรรมในการ พัฒนาระบบ E-health ซึ่งจะมีการใช้ประโยชน์จาก Cloud Computing เป็นส่วนประกอบหลักของการพัฒนาระบบ ซึ่งจะใช้ทั้งช่วยในการประมวลผลและช่วยในการแสดงผลในการติดต่อกับผู้ใช้และจัดการข้อมูลให้สามารถดูผ่านเว็บหรือโปรแกรม ให้สะดวกมากยิ่งขึ้น

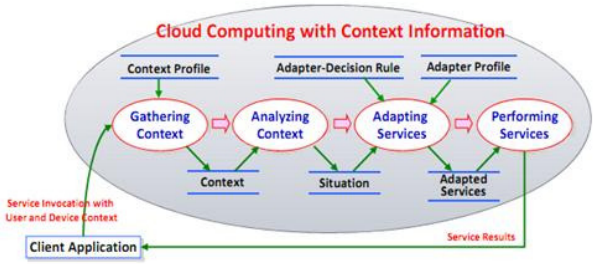


รูปที่ 14 แสดงสถาปัตยกรรมของระบบ E-Health

จากภาพข้างบนนี้จะเป็นการแสดงถึงลักษณะของการใช้งานโปรแกรม (a) จะเป็นการแสดงสุขภาพของผู้ช่วย โดยจะแสดงรหัส ชื่อ การเข้ารักษา (b) จะเป็นการแสดงข้อมูลภาพที่ได้มีการถ่ายไว้ (c) จะเป็นการแสดงภาพที่ได้มีการ CT scan วิเคราะห์โรค (d) จะเป็น CT scan ผลลัทธ์ที่ได้ออกมา (e) เป็นส่วนการติดต่อกับผู้ใช้โปรแกรม (f) เป็นการ upload ภาพขึ้นไปประมวลผลที่ Cloud Computing

ภาพนี้จะเป็นการให้บริการ Cloud เป็นโทรศัพท์มือถือ รันผ่าน Android OS การทำงานนั้นจะใช้ web service ในการติดต่อระหว่าง Cloud-service client กับ Cloud Computing ที่ทำงานอยู่บน server

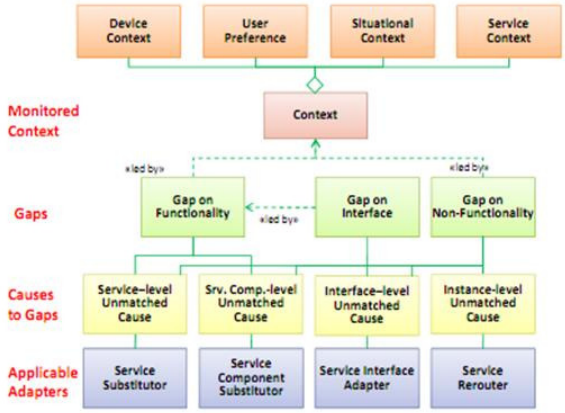
Context-aware Mobile Cloud Services [16] เสนอแนวคิดในการออกแบบการบริการที่เป็นไดนามิคโดยจัดเตรียมการบริการที่เหมาะสมกับซึ่งมีวิธีการคือหลังจากได้รับการเรียกใช้บริการ ถ้าไม่มีข้อมูลบริบท การบริการจะยึดติดกับฝั่งผู้ให้บริการ ในอีกทางนึง ถ้าใน Cloud computer มีข้อมูลบริบทและมีข้อมูลบริบทถูกส่งมาพร้อมกับคำร้องขอใช้บริการ จะมีกระบวนการวิเคราะห์สถานการณ์ปัจจุบันของฝั่งผู้บริโภค จากนั้นการบริการที่เหมาะสมจะถูกเลือกมาปรับใช้ในการบริการ ดังรูปที่ 15 แสดงภาพรวมของขั้นตอนแบบจำลอง



รูปที่ 15 แสดงแบบจำลองของ Context –Aware Cloud Service

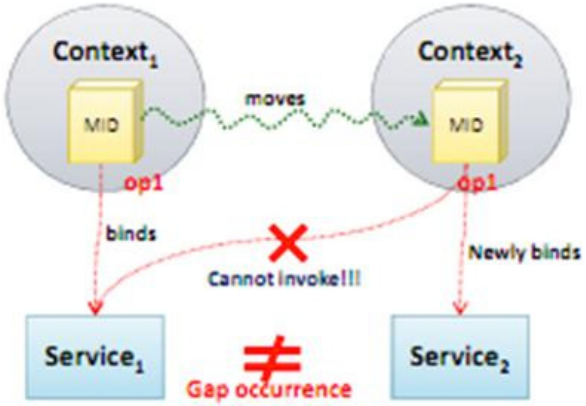
ประเภทของ CONTEXT-BASED SERVICE ADAPTER

เป็นการปรับเปลี่ยนการบริการแบบไดนามิคจะต้องมีการวิเคราะห์ข้อมูลต่างๆ ดังรูปที่ 16 แสดงลำดับชั้น Context-Concernd Hierarchy



รูปที่ 16 แสดง Context-Concernd Hierarchy

เลเยอร์บนสุดประกอบด้วย Device Context เป็นการตั้งค่าและการกำหนดค่าอุปกรณ์ของผู้ใช้ User Preference ใช้ระบุการตั้งค่าที่ผู้ใช้กำหนดโดยเฉพาะอย่างยิ่งเกี่ยวข้องกับการเลือกบริการและการร้องขอการบริการ Situational Context คือกลุ่มของการติดตามข้อมูล และข้อมูลเกี่ยวข้องกับตำแหน่งของผู้ใช้ เวลา และตั้งค่าในปัจจุบันอื่น ๆ ที่เกี่ยวข้องกับผู้ใช้ Service-Context จับสถานะปัจจุบันของการให้บริการ เช่นมูลค่าการติดตามของคุณสมบัติ QoS ในการจัดเตรียม context-aware service เป้าหมายของการบริการควรจะเหมาะสมกับบริบทที่ได้รับ มักจะมีช่องว่างระหว่างการบริการที่สามารถใช้ได้และการบริการที่จำเป็น เลเยอร์ลำดับที่สอง ในรูป ใช้สำหรับ Types of-Gaps ซึ่งจะระบุสามประเภทที่แตกต่างกันของช่องว่างที่อาจเกิดขึ้น เมื่อผู้ใช้ย้ายสถานที่ด้วย Mobile Internet Device (MID) บริบทของผู้ใช้สามารถเปลี่ยนแปลงได้จาก $Context_1$ ไป $Context_2$ การบริการที่ผูกติดสามารถเปลี่ยนแปลงได้เมื่อรูปแบบการให้บริการไม่ตรงกับบริบทใหม่ ดังนั้นจึงมีช่องว่างระหว่าง Service 1 และ Service2



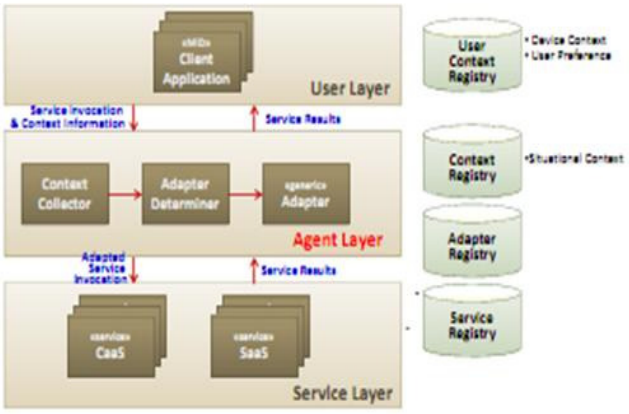
รูปที่ 17 แสดงระดับต่าง ๆ ของ Service Realization

ช่องว่างบน functional จะแตกต่างกันเล็กน้อยระหว่าง การให้บริการที่สามารถใช้ได้และการให้บริการที่เป็นที่ต้องการใช้งาน เช่นหากผู้บริโภคต้องการฟังก์ชั่น การหาเส้นทางที่สั้นที่สุดเพื่อไปยังปลายทาง ฟังก์ชั่นควรจะเป็นแบบเฉพาะและเหมาะตามประเภทของแต่ละการขนส่งเช่นรถบัสซึ่งช่องว่างบน non-functional เป็นความแตกต่างระหว่างการวัดค่า QoS ในปัจจุบัน และค่าก่อนหน้า ซึ่งโดยปกติจะเกิดขึ้นเมื่อผู้บริโภคใช้บริการในการเดินทาง หรือบริบทของแพลตฟอร์มที่ให้บริการได้รับการเปลี่ยนแปลง ช่องว่างบน functional อาจทำให้เกิดช่องว่างใน Interface เลเยอร์ที่สามในรูป 16 แสดงรายการสี่สาเหตุที่เป็นไปได้ซึ่งอาจส่งผลให้เกิดช่องว่าง ช่องว่างในผลลัพธ์ของ functional จะก่อให้เกิดการให้บริการที่แตกต่างกันซึ่งเป็นของ Service-level-Unmatched Cause และ Service Component-level Unmatched Cause โดยถ้า Service-level Unmatched Cause เกิดขึ้นความแตกต่างใน Interface ที่ให้บริการ (เช่นช่องว่างใน Interface) อาจเกิดขึ้น ในอีกทางหนึ่งมาจาก Service Interface-level Unmatched Cause ช่องว่างบน Non-functionality บางอย่างนั้นบ่งบอกว่า QoS ของ Cloud services มีการลดคุณภาพลงหรือเกิดความผิดพลาดในระหว่างการใช้บริการนี้ซึ่งมีการแสดงด้วย Service Instance-level Unmatched Cause ในเลเยอร์ที่สี่กำหนดสี่ชนิดของอแด็ปเตอร์ Service Substitutor เป็นการผูกมัดการบริการที่แตกต่าง สำหรับฟังก์ชั่นที่ต้องการ Service Interface Adapter เป็น

การปรับเปลี่ยนส่วนติดต่อการใช้บริการสำหรับการให้บริการที่จะเรียกใช้ฟังก์ชั่นที่แตกต่างกันนำไปสู่การกำหนด Interface ที่แตกต่างกัน ตั้งแต่อธิบาย Interface ว่าฟังก์ชันการทำงานของการให้บริการคืออะไร Service Component-Substitutor เป็นการเรียกใช้องค์ประกอบหนึ่งของการให้บริการที่ใช้ Interface เดียวกัน Service Rerouter เป็นการเปลี่ยนตำแหน่งของ Component instances ที่จะเรียก

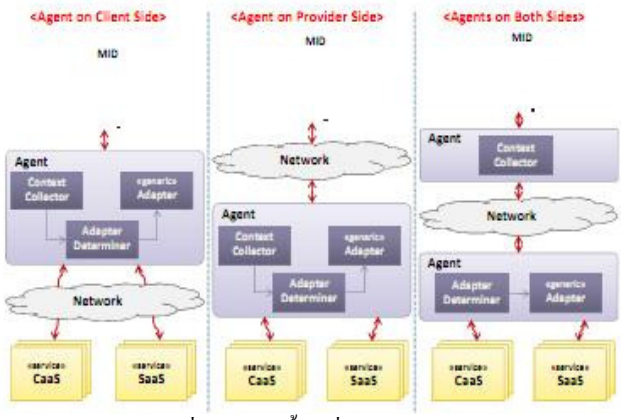
สถาปัตยกรรม CONTEXT-AWARE

บนพื้นฐานของ Computing model กำหนดสถาปัตยกรรมของกรอบการทำงานการเตรียม Context-aware service ดังที่แสดงในรูป 18 สถาปัตยกรรมประกอบด้วยสามเลเยอร์ คือ User Layer Agent Layer และ Service Layer แต่ละเลเยอร์ มีส่วนประกอบและชุดข้อมูลที่เกี่ยวข้องกันอยู่คือ User layer ประกอบด้วยหลาย ๆ MID และโปรแกรมฝั่งไคลเอ็นต์จะมีใช้งานใน MID Agent Layer มีบทบาทในการปรับการบริการโดยใช้ข้อมูลรวมทั้งการตั้งค่าของผู้ใช้ ซึ่งเลเยอร์ประกอบด้วยสามประเภทของส่วนประกอบคือ Context Collector Adapter Determiner และ Adapter Context Collector คือการรวบรวมข้อมูลบริบททั้งหมดจากผู้ใช้หรืออุปกรณ์ ด้วยการใช้ข้อมูลบริบท Adapter-Determiner คือการวิเคราะห์ข้อมูลบริบท ค้นหาบริการคู่แข่ง เลือก Context-aware service adapter ที่เหมาะสมที่สุดและเรียกใช้การปรับการให้บริการ Adapter คือการให้บริการส่วนบุคคลไปสู่การให้บริการผู้บริโภคที่หลากหลาย ซึ่งรูปแบบเฉพาะจะครอบคลุมในส่วน Service Layer เพื่อนำไปใช้กับการให้บริการที่หลากหลาย



รูปที่ 18 แสดงสถาปัตยกรรมของ Context-Aware Provisioning

สำหรับการแบ่งเลเยอร์ไปยังเครื่องไคลเอนต์นั้นทางด้านผู้ให้บริการจะกำหนดการตั้งค่าดังแสดงในรูปที่ 19 ซึ่งจะเห็นได้ว่ามีความแตกต่างแต่ละหลักในระหว่างการตั้งค่าคือ ตำแหน่งของ Agent Layer การตั้งค่าที่หนึ่งและที่สอง อยู่ที่ Agent Layer ตั้งอยู่บนฝั่งไคลเอ็นต์และด้านผู้ให้บริการตามลำดับ ในขณะตั้งค่าสุดท้ายคือที่ Agent Layer มีการกระจายไปยังลูกค้าและฝั่งผู้ให้บริการ โดยคำนึงถึงการกระจายฟังก์ชั่น



รูปที่ 19 แสดงตั้งค่าที่เป็นไปได้ 3วิธี

เมื่อผู้ใช้ทำการเรียกใช้การให้บริการบนอุปกรณ์ Context Collector จะทำหน้าที่รวบรวมข้อมูลที่เพิ่มเติมเกี่ยวกับการให้บริการและหลังจากนั้น Adapter Determiner จะทำการค้นหาการให้บริการที่คล้าย ๆ กันเมื่อพบฟังก์ชั่นที่ผู้บริโภคต้องการก็จะทำการปรับตัวตามสิ่งแวดล้อมที่ต้องการและกำหนดรูปแบบที่เหมาะสมสุดท้ายการปรับการให้บริการจะถูกเรียกใช้และส่งกลับผลลัพธ์ไปยังการใช้บริการของผู้ใช้

สรุปด้านสถาปัตยกรรมที่มีการนำ Cloud Computing มาประยุกต์

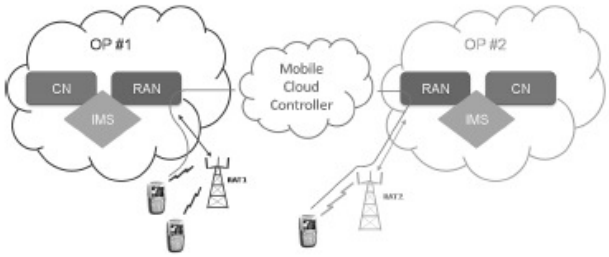
ในที่มีการเสนอด้านสถาปัตยกรรมในการประยุกต์ใช้ Cloud บนอุปกรณ์พกพานั้นพบว่าส่วนใหญ่การบริการจะเป็นรูปแบบที่เป็น Static คือมีการส่งข้อมูลที่คงที่ มีส่วนน้อยที่จะเป็นการบริการแบบ Dynamic ซึ่งจะมีการส่งข้อมูล สถานที่ตำแหน่งในปัจจุบันที่มีการเปลี่ยนแปลงตามการเดินทาง ในส่วน Protocal จะใช้ Http และ Soap ใน Web Service โดยในที่นำเสนอนั้นจะเป็นในรูปแบบของ Software As a Service

	Mobile Learning	**Mobile Payment**	**Traffic Lights**	**E-health**
Application Layer	ส่งข้อมูลผู้ใช้	ส่งข้อมูลผู้ใช้	ส่งสถานที่และรูปสัญญาณไฟจราจร	ส่งข้อมูลผู้ใช้และรูป CT scan
Logical Layer	จัดสรรทรัพยากรสำหรับการเรียนรู้	ประเมินความน่าเชื่อถือของผู้ใช้	ตรวจสอบสถานที่รูปสัญญาณไฟจราจร	ประมวลผลรูป CT scan และข้อมูลผู้ป่วย
Protocol	HTTP,WAP	HTTP	SOAP	SOAP
Type of Service	SaaS	SaaS	SaaS	SaaS
Dynamic service	ไม่	ไม่	ใช่	ไม่

ตารางที่ 6 เปรียบเทียบสถาปัตยกรรมในต่างๆ

IV. ด้านการเชื่อมต่อ Cloud

Access Schemes for Mobile Cloud Computing [13] นำเสนอโซลูชั่นที่ปรับใช้ Mobile Cloud Computing (MCC) ในสถานการณ์การเข้าถึงที่แตกต่างกัน เช่น GPRS WCDMA HSPA LTE WiMAX CDMA 2000 WLAN เช่นตำแหน่งสถานีและความสามารถของผู้ใช้โดยควบคุม mobile cloud เพื่อเพิ่มประสิทธิภาพการจัดการการเข้าถึงภายใน



รูปที่ 20 การใช้ mobile cloud ควบคุมตำแหน่งสถานีและความสามารถของผู้ใช้

ซึ่งจะพิจารณาว่าอัตราข้อมูลต่ำของสัญญาณ ในส่วนช่องทางควบคุม cloud สามารถใช้ได้ เช่นการใช้ GPRS ที่มีการปรับใช้ในหลายประเทศที่มีความคุ้มครองที่สูงมากและใช้งานอยู่แล้ว สำหรับพื้นหลังอัตราการส่งข้อมูลสื่อสารต่ำจาก เครื่องจักรไปยังเครื่องจักร พลังงานและค่าใช้จ่ายที่มีประสิทธิภาพ สามารถ ขอการเชื่อมต่อไร้สายสามารถปรับขนาดได้ ซึ่งจาก TCP / IP โมเดลดั้งเดิม สำหรับผู้ใช้โทรศัพท์เคลื่อนที่มีการแก้ไขพารามิเตอร์เพื่อแบบจำลองการจราจร mobile cloud มีวัตถุประสงค์เพื่ออธิบายถึงผู้บริโภคและ MCC เช่น ABIResearch คาดว่าส่วนใหญ่ผู้ใช้ mobile cloud จะอยู่ในกลุ่ม NETWORK-SELECTION AND HETEROGENEOUS ACCESS MANAGEMENT

สำหรับอัตราการส่งข้อมูลที่สูง หรือแม้กระทั่งความต้องการขยายขีดความสามารถในการส่งผ่านแบนด์วิดธ์ สำหรับสถานการณ์ MCC ความจำเป็นในการจัดการการเข้าถึงเครือข่ายที่มีประสิทธิภาพผ่านการเข้าถึงเทคโนโลยีวิทยุที่แตกต่างกัน (RATs) เรียกว่า การจัดการการเข้าถึงที่แตกต่าง ข้อจำกัดด้านโหนดเครือข่ายหรือจาก sensors ที่ใช้งานในสภาพแวดล้อมของผู้ใช้ จะถูกใช้ประโยชน์อย่างมากเพื่อลดความสูญเปล่าของทรัพยากรที่ขาดแคลน และมีประสิทธิภาพในการจัดการกับการเชื่อมต่อไร้สายผ่าน RATs ที่แตกต่างกัน ปัญหาของการเลือกเครือข่ายในสภาพแวดล้อมในการเชื่อมต่อไร้สายในปัจจุบัน HAM อธิบายถึงแนวคิดสำหรับการควบคุมการจัดสรรทรัพยากรวิทยุ และการใช้ประโยชน์ เช่น แบนด์วิดท์ พลังงานผ่าน RATs ต่าง ๆ ซึ่งเป้าหมายหลักคือเพื่อเพิ่มประสิทธิภาพการทำงานของระบบโดยรวมและเพื่อให้สามารถเคลื่อนที่อย่างราบรื่น HAM ตัดสินใจและการดำเนินการอาจได้รับผลจากนโยบายการให้บริการเครือข่าย สำหรับปรับเครือข่ายและการตัดสินใจ HAM ดังนั้นการปรับที่ไม่ได้ป้องกันอาจนำไปสู่การทำลายประสิทธิภาพ

4.1 Context Awareness เปรียบเสมือนกับเป็น Software ที่มีความสามารถเปลี่ยนแปลงหรือโต้ตอบกับผู้ใช้เมื่อมีการเปลี่ยนแปลงสิ่งแวดล้อม ซึ่งจะมีหลักการดังนี้

1) เข้าสู่เซนเซอร์โดยตรงของเซนเซอร์ที่ใช้งานใน Terminal เครือข่ายสามารถรวบรวมบริบทสิ่งแวดล้อม เช่น สถานที่หรืออุณหภูมิรวมทั้งข้อมูลบริบทของเครือข่าย

2) ตัวกลางโครงสร้างพื้นฐานการแนะนำของตัวกลางโครงสร้างพื้นฐานมีวัตถุประสงค์เพื่อแบ่งกระบวนการอย่างเคร่งครัดในการได้มาของบริบทและการจัดการบริบท การแยกดีขึ้นและการขยายระบบความสามารถนำกลับมาใช้ใหม่

3) ContextServer วิธีการนี้ Serverใช้เวลามากกว่างานของการบริหารข้อมูล ที่ได้รับจากแหล่งต่าง ๆ จะช่วยลดเซนเซอร์และ terminals จากการจัดการการร้องขอบริบทจากหน่วยงานอื่น ๆ ซึ่งกระบวนการการจัดการและการกระจายข้อมูลตามบริบทเพื่อความต้องการเฉพาะของโปรแกรมประยุกต์และบริการ

4.2 A CONCEPT FOR INTELLIGENT RADIO NETWORK-ACCESS FOR MCC ความเป็นไปได้ในการเชื่อมต่อไร้สาย

การเข้าใช้อย่างมีประสิทธิภาพและการจัดการทรัพยากร ที่แตกต่างกันการเลือกเครือข่ายและการตัดสินใจนั้นสำคัญอย่างมาก เช่น ภาระเครือข่ายและการคาดการณ์การเคลื่อนไหวของผู้ใช้สามารถใช้ได้ MCO จะไม่จำเป็นต้องมีการเข้าถึงข้อมูลทรัพยากรภายใน RAT ถือว่าข้อมูลที่เกี่ยวกับสถานะของเครือข่ายนี้จะใช้ได้เฉพาะโดย ข้อมูลนี้จะต้องอยู่ภายใต้การประมาณค่าข้อผิดพลาด และความล่าช้าในการส่งสัญญาณแน่นอน ดังนั้นจึงสร้างแบบจำลองของคุณภาพที่มีความเกี่ยวข้องกับเครือข่ายที่เข้าถึง ในการเข้าถึงจะช่วยลดเวลาการสแกน Terminal สำหรับการเข้าถึงเครือข่ายให้ผล Terminal การบริโภคพลังงานลดลง multicasting จะถูก rerouted อย่างมีประสิทธิภาพ และสามารถส่งความรู้ Terminal และจุดของสิ่งที่แนบมา กลไกของ RATs ไร้สายที่ทันสมัยเช่น การปรับเชื่อมโยง จะยังได้รับประโยชน์จากข้อมูล เช่น สภาพแวดล้อมของผู้ใช้และข้อมูล

4.3 A CONTEXT MANAGEMENT ARCHITECTURE FOR-IRNA-MCC PURPOSES ขึ้นอยู่กับการใช้ประโยชน์ตามวัตถุประสงค์เพื่อให้สอดคล้องกับความต้องการที่แตกต่างกัน สถาปัตยกรรมการจัดการ CMA ยึดตามแบบอย่างผู้ผลิตผู้บริโภค ที่สามารถพบได้บ่อยในพื้นที่ของจัดการ เช่น CMA ได้รับการออกแบบมาเพื่อจัดการและจัดจำหน่ายข้อมูลบริบทและการควบคุมคุณภาพ เพื่อวัตถุประสงค์ IRNA ฟังก์ชั่นนี้ต้องใช้องค์ประกอบทางสถาปัตยกรรมที่สำคัญดังต่อไปนี้

- Context Provider : ประเภทของข้อมูลการให้บริการสามารถจัดในข้อมูลแบบคงที่ และข้อมูลแบบไดนามิก ข้อมูลแบบคงที่ เช่นมีความสามารถ terminal การตั้งค่าของผู้ใช้หรือข้อมูลที่ผู้ใช้เรียกจากชุมชนสังคมบน สำหรับจุดประสงค์ของการจัดการ IRNA แบบไดนามิก เช่นตำแหน่งผู้ใช้และการเคลื่อนย้าย (เช่นความเร็วและทิศทาง) และเงื่อนไขที่เครือข่ายมีความเกี่ยวข้องสูงกว่า นอกจากนี้ CPS ใช้อัลกอริทึมการให้เหตุผลบนระดับต่ำข้อมูลบริบทสามารถที่จะเป็นนามธรรมและทำนายพฤติกรรมของผู้ใช้เช่น การเคลื่อนไหว

ของผู้ใช้การสื่อสารระหว่าง CPS และหน่วยงาน CMA อื่น ๆ เกิดขึ้นในโหมด synchronous

- Context Broker : ฟังก์ชั่นหลักของ CPS จะขึ้นอยู่กับรีจิสเตอร์ที่สามารถให้บริการการค้นหา CP ไปยังหน่วยงาน นอกจากนี้ CB สามารถให้ข้อมูล โดยการส่งต่อข้อมูลที่ได้รับจาก CPS สองโหมดการติดต่อสื่อสารที่แตกต่างกันมีอยู่ สำหรับการร้องขอหน่วยงาน ในโหมด asynchronous ถูกส่งต่อหากเงื่อนไขที่ระบุไว้ หรือเหตุการณ์จริงมา ในโหมด synchronous สามารถตอบได้ทันทีโดย CB เพื่อที่จะอนุญาตให้มีการส่งต่อ CB ตัวเองรักษาแคชซึ่งจะเก็บข้อมูลฐานข้อมูล

- Context Consumer : เป็นการอินพุตสำหรับการใช้งานจริงของการบริการเครือข่ายโปรแกรมสำหรับผู้ใช้ที่เปิดใช้งาน หรือตัวกระตุ้นในเซนเซอร์ไร้สายและเครือข่ายเป็นตัวกระตุ้นผู้บริโภคที่เป็นแบบอย่างข้อมูลมุ่งเน้นที่ประกอบด้วยขององค์ประกอบที่แตกต่างกันของกรอบงาน IRNA

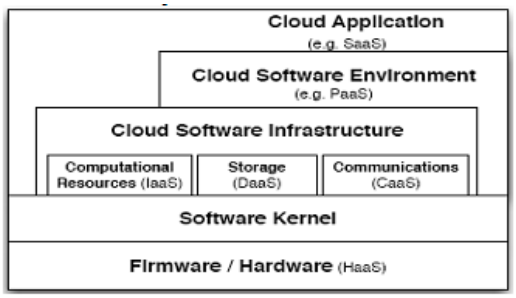
- Context Quality Enablern : ผู้ผลิตจำเป็นต้องดำเนินการหลากหลายของงานเพื่อเพิ่มประสิทธิภาพการใช้เครือข่ายในการตัดสินใจที่ถูกต้องในแง่ของการเลือกเครือข่ายการเชื่อมโยงการปรับตัว การทำนายพฤติกรรมของผู้ใช้และ multicasting โมดูล IRNA ต้องการข้อมูลที่มีคุณภาพสูงซึ่งจะ ปฏิบัติตามกับเกณฑ์คุณภาพที่ระบุไว้จะนำมาใช้สำหรับจัดการ IRNA ด้วยเหตุนี้ CPS เท่านั้นที่มีลักษณะที่สอดคล้องกัน สามารถส่งมอบข้อมูลที่เหมาะสมดังนั้น CQE ถูกแนบไปกับ CB เนื่องจากเป็นโบรกเกอร์ที่ disposes ของข้อมูลเกี่ยวกับความสามารถของCPและความพร้อมใช้ ดังนั้น เมื่อร้องขอข้อมูลบริบท HAM จะส่งความต้องการขั้นต่ำด้วยการไปถึงคุณภาพบริบท CQE ใช้ข้อมูลเหล่านี้ นอกจากนี้ CQE อาจระบุผู้ให้บริการเนื้อหาที่เป็นอันตรายหรือ terminals ที่มีเจตนาพยายามที่จะทำให้เสียการทำงานของระบบโดยใช้ข้อมูลของ terminals อื่น ๆ เป็นค่าอ้างอิงหรือการดำเนินการและนโยบายการลงโทษตามลำดับ ค่าอ้างอิง สามารถคำนวณโดยใช้ข้อมูลของ CPS

4.4 A CONTEXT-AWARE RADIO NETWORK SIMULATOR-(CORAS) เป็นการจำลองเครือข่ายในรูปแบบเนื้อหาแบบไดนามิกเพื่อจำลองอิทธิพลของคุณภาพใน HAM และจุดสิ้นสุดของผู้ใช้ ซึ่งการปฏิบัติงานให้มีประสิทธิภาพสำหรับการประเมินของ HAM จะต้องตัดสินใจเลือกเครือข่ายและการใช้ทรัพยากรมีการเดินสุ่มการปฏิบัติ การจำลองค่าใช้จ่ายในการส่งสัญญาณและความล่าช้าที่เกิดขึ้นส่งมอบเข้าบัญชี เครือข่ายการตัดสินใจคัดเลือก ขึ้นอยู่กับความแรงของสัญญาณบ่งชี้และการคาดการณ์การเคลื่อนไหวของผู้ใช้และการใช้ทรัพยากรมีการติดตามและ สำหรับการประเมินคุณภาพการเชื่อมโยงตัวอย่าง เช่นการผลิตปัจจุบันคือแบบจำลองเครือข่ายขึ้นอยู่กับความจุที่ผ่านมาและการประมาณความสามารถทันที สำหรับการปรับตัวเชื่อมโยงการวัดและรายงานโดยแต่ละสถานีจะช่วยทางด้านตัดสินใจ

An Optimized Solution for Mobile Environment Using Mobile Cloud Computing abstraction [14]

นำเสนอสถาปัตยกรรมโทรศัพท์มือถือที่ดีที่สุด เป็นโซลูชั่นไฮบริดเทคโนโลยี mobile agent รวมกับ mobile cloud computing สภาพแวดล้อมมือถือถูกแบ่งออกเป็นจำนวนมากในแต่ละเซลล์มี cloud หลายอันทำหน้าที่เป็นสถานีที่มีการรองรับโมบายให้สนับสนุนการให้บริการสำหรับผู้ใช้โทรศัพท์มือถือในพื้นที่นี้ หน่วย Cloud ในพื้นที่ทุกเซลล์และหน่วย Cloud ระยะไกลเชื่อมต่อกับเป็น cloud บนมือถือซึ่งสนับสนุนความสามารถในการคำนวณ และความสามารถในการจัดเก็บข้อมูล วิธีการในการให้บริการที่หลากหลาย mobile cloud จะบรรเทา mobile host จากการคำนวณที่ซับซ้อนและโฮสต์มือถือเพียงแค่มุ่งที่การโต้ตอบกับผู้ใช้ สำหรับการส่งผ่านมือถือระหว่างโฮสต์และ cloud units การนำบริการ Universal Mobile Cell ซึ่งทำหน้าที่เป็น abstraction ของ mobile agent ซึ่ง สถาปัตยกรรมนี้มี 3 ลักษณะสำคัญ mobile cloud ที่สนับสนุนบริการ Universal Mobile Service Cell ซึ่งทำหน้าที่เป็นตัวแทนให้บริการสำหรับผู้ใช้มือ

ประโยชน์จากการ cloud computing ถูกนำมาที่โทรศัพท์มือถือ mobile cloud ประกอบด้วยสองชนิด cloud units ในพื้นที่ทุกเซลล์และ cloud-units ระยะไกลมี cloud บางส่วนจากความแตกต่างอย่างเป็นทางการ ประการแรกในการคำนวณ cloud units ที่แตกต่างกัน เดิมมีจุดมุ่งหมายที่เกี่ยวข้องการร้องขอจากผู้ใช้โดยตรง หลังจะใช้หนึ่งในการจัดการการคำนวณที่สำคัญของให้บริการบางอย่าง cloud units ในพื้นที่เซลล์ส่งการร้องขอให้ cloud units ระยะไกลสำหรับให้บริการที่ซับซ้อนบางอย่าง mobile cloud แบ่งออกเป็น 5 ชั้นในมุมมองของ composability ของระบบ Cloud Application Layer, Cloud Software Environment Layer, Cloud Software Infrastructure Layer, Software Kernel, Hardware and Firmware



รูปที่ 21 โครงสร้างและความสัมพันธ์ข้ามระหว่างแต่ละชั้น

การเชื่อมต่อไร้สายให้มั่นคงและจะมีผลต่อคุณภาพและความมั่นคงของบริการของ mobile cloud เพื่อแก้ปัญหานี้ได้นำ Universal Mobile Service-Cell ที่ทำหน้าที่เป็นพร็อกซี่สำหรับการส่งผ่านระหว่าง mobile hosts และ mobile cloud เป็นโมดูลซอฟต์แวร์ที่ชาญฉลาดที่นำการร้องขอจากผู้ใช้และผู้อพยพใน mobile cloud ไปที่การค้นหาการตอบสนองคำขอ มีสองชนิดของเซลล์ผู้ใช้ Mobile Service Cell และ Cloud Mobile Service Cell รายละเอียดกระบวนการของการสื่อสารระหว่าง MH และ MC ขึ้นอยู่กับ Universal Mobile -Service Cell ประการแรกใน mobile host ตัวแทนที่เรียกว่า User Mobile-

Service Cell รวบรวมคำขอจากผู้ใช้ ประการที่สองตัวแทนอพยพไป cloud-units ที่สอดคล้องกันและก็เรียกว่า Cloud Mobile Service Cell ประการที่สาม Cloud Mobile Service Cell ย้ายไปในmobile cloud และค้นหา cloud units ซึ่งสามารถตอบสนองการร้องขอ จากนั้นที่จะนำผลลัพธ์และย้ายข้อมูล MH ที่สอดคล้อง

Universal Mobile Service Cell ไม่จำเป็นต้องใช้ในการส่งการร้องขอข้อความตอบกลับมีการเชื่อมต่อแบบไร้สายระหว่างแบนด์วิดธ์ต่ำ mobile cloud และ mobile host บริการตัวเองเป็นเซลล์ อพยพสามารถแก้ไขได้ด้วยการสื่อสารอย่างต่อเนื่องกับ mobile host จากนั้นความท้าทายที่มาจากการขาดการเชื่อมต่อเครือข่ายไร้สายอย่างฉับพลันและสถานการณ์ของ mobile host ปิดเพื่อประหยัดพลังงานมีความโปร่งใสให้กับ สิ่งที่ระบบนี้สามารถตอบสนองกับสถานการณ์เมื่อ mobile host ตัดการเชื่อมต่อในขณะที่ cloud service cell ต้องการผลลัพธ์คืนจากคำขอของผู้ใช้ให้ mobile host หรือเมื่อ mobile host ได้รับจากเซลล์พื้นที่นี้เข้าสู่พื้นที่เซลล์อื่นสำหรับปัญหาแรก cloud units ในพื้นที่บางเซลล์เก็บรายการของข้อมูลการเชื่อมต่อระหว่าง MH ทุกครั้ง MB เมื่อเสร็จสิ้น Cloud Mobile-Service Cell ซึ่ง cloud units ตรวจสอบรายชื่อที่จะตัดสินหากการเชื่อมต่อจะถูกเก็บไว้หากมีการเชื่อมต่อกระบวนการทำงานอย่างเป็นทางการเสร็จสิ้น ถ้าไม่ได้เชื่อมต่อ cloud units ใช้ระบบพร็อกซี่ เพื่อบันทึกบาง Cloud Mobile Service - Cell จนกว่าการเชื่อมต่อสามารถสร้างใหม่ สำหรับปัญหาที่สองที่ใช้สนับสนุนการเคลื่อนย้ายทรัพย์สินทางปัญญา cloud units ในพื้นที่บางเซลล์จะสามารถรู้การเปลี่ยนแปลงของ mobile host Cloud Mobile Service Cell ย้ายไปให้ cloud-units ที่สอดคล้องกันและซ้ำขั้นตอน ทำให้การเคลื่อนย้ายโปร่งใสให้กับผู้ใช้และยังช่วยลดผลกระทบที่ไม่ดีของเครือข่ายไร้สายไม่มั่นคง เหมือนสะพานอัจฉริยะเชื่อมต่อ MH ไป MB

Mobile Host

ประการแรกการแบ่งแยกระหว่าง CPU และหน่วยความจำ เมื่อเทียบกับจำนวนหน่วยความจำดังนั้นการปรับปรุงที่ดีในฮาร์ดแวร์สามารถปรับปรุงสถาปัตยกรรม ประการที่สองด้านอุปกรณ์พกพาไม่สามารถมีความสามารถในการใช้คอมพิวเตอร์ที่มีประสิทธิภาพและความสามารถในการเก็บรักษา cloud-computing ทำให้มีทรัพยากรไม่จำกัด สำหรับการจัดเก็บข้อมูลและความสามารถในการคำนวณสามารถรวม CPU และหน่วยความจำชื่อ CM นอกจากนี้ยังเป็นองค์ประกอบใหม่ที่สำคัญที่เรียกว่า Mobile Cloud ถูกแนบไปกับสถาปัตยกรรมใหม่

.

	Access Schemes for MCC	Solution for Mobile Environment
ด้านการเชื่อมต่อ	-การเชื่อมต่อไร้สายสามารถปรับขนาดได้ สังเกตได้จาก TCP / IP โมเดลดั้งเดิม -มีการเชื่อมต่อไร้สายผ่าน RATs ที่แตกต่างกัน	-เป็นการสื่อสารระหว่าง MH และ MC จะขึ้นอยู่กัน Universal Mobile service Cell ทำหน้าที่เป็นพร็อกซี่สำหรับการส่งผ่านระหว่าง Mobile Cloud และ Mobile Host -ข้อความตอบกลับจะมีการเชื่อมต่อแบบไร้สายระหว่างแบนด์วิดธ์ต่ำ
ด้านการติดต่อสื่อสาร	-มี 2 โหมด ได้แก่ asynchronous จะถูกส่งต่อเมื่อมีเงื่อนไขที่ระบุไว้ หรือเหตุการณ์จริงมา และ Synchronous สามารถตอบได้ทันที	-เป็นการสื่อสารระหว่าง MH และMC ขึ้นอยู่กับ Universal Mobile Service Cell -สามารถแก้ไขการติดต่อสื่อสารได้

ตารางที่ 7 แสดงการเปรียบเทียบด้านการเชื่อมต่อ Cloud

V. ด้านความปลอดภัย

ความปลอดภัยนับเป็นปัญหาที่เป็นความท้าทายของ Cloud-Computing เพราะมีการรวมข้อมูลต่างๆมาไว้ที่ส่วนกลางทำให้ความเป็นส่วนตัวน้อยลงไปซึ่งถ้าหากข้อมูลหรือการดูแลการเก็บรักษาไม่มีความปลอดภัยแล้วจะส่งผลให้ผู้ใช้บริการจะเกิดความไม่ใจในการใช้บริการได้ โดยได้ทำการศึกษางานต่างๆที่เกี่ยวข้องซึ่งมีการนำเสนอรูปแบบหรือวิธีการควบคุมความปลอดดังนี้

Distributed Intrusion Detection in Clouds Using Mobile Agents [10]

การตรวจหาการบุกรุกการแทรกกระจายในตัวแทนผู้ใช้ Mobile-cloud นำเสนอ Mobile Agent การรบกวนระบบการตรวจสอบตาม (IDS) ซึ่งสามารถนำมาใช้โดยลูกค้า Cloud และได้รับการปรับแต่งมากสำหรับสภาพแวดล้อม Cloud Computing เพื่อสนองต่อความต้องการการรักษาความปลอดภัยของผู้ใช้ ข้อดีของวิธีที่เสนอสำหรับ Cloud Computing รวมถึงการบรรลุความยืดหยุ่นสูงกว่าการป้องกันการแอบแฝงเครือข่ายลดภาระค่าใช้จ่ายเครือข่ายและส่งผลการดำเนินงานที่ต่ำกว่าการรัน asynchronously และ autonomously, adopting แบบไดนามิก การดำเนินงานในสภาพแวดล้อมที่ต่างกันของ cloud และมีลักษณะการทำงานมีประสิทธิภาพและป้องกันความ

ผิดพลาด โดยแสดงวิธีการ DIDMA จะเพิ่มองค์ประกอบใหม่และนำไปใช้กับ subnet ของแต่ละเครือข่ายในขณะที่รูปแบบ Peer to Peer จะใช้ในการเชื่อมต่อย่อยทั้งหมดเข้าด้วยกัน

Components ของระบบตรวจสอบการบุกรุกใน Subnet

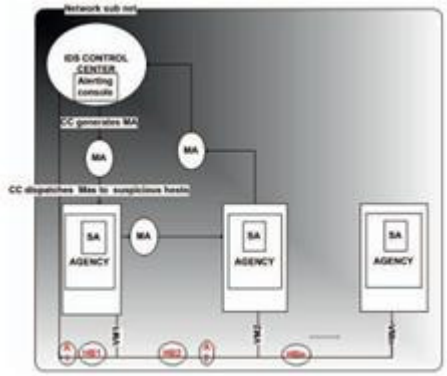
การออกแบบพื้นฐานแบบไฮบริดที่นำเสนอใน subnet เสมือนแต่ละเครื่องประกอบด้วยสี่องค์ประกอบหลัก ได้แก่ ศูนย์ควบคุม IDS (IDS CC)- Agency งานเฉพาะ StaticAgent ตรวจจับและสืบสวนเฉพาะกิจ Mobile Agent จากรูปที่ 22 Static Agents (SA) สร้างการแจ้งเตือนเมื่อใดก็ตามที่ตรวจสอบกิจกรรมที่น่าสงสัยแล้วบันทึกข้อมูลเหล่านั้นกิจกรรมในล็อกไฟล์และส่งหมายเลขการแจ้งเตือน (เช่น A1 ในรูปที่ 22) ไปยังศูนย์ควบคุม IDS จากนั้นศูนย์ควบคุม IDS จะส่งการตรวจสอบงานเฉพาะทุกตัวแทนมือถือให้กับหน่วยงานที่ส่งการแจ้งเตือนที่คล้ายกันในรูปที่ 22 MA จะเข้ามาและตรวจสอบ VMs ทุกอย่าง แต่เก็บข้อมูลความสัมพันธ์และในที่สุดก็ส่งผลหรือดำเนินการกลับไปยังศูนย์ควบคุม IDS ดังนั้นแจ้ง Console ในศูนย์ควบคุม IDS จะวิเคราะห์ข้อมูลที่มาและเปรียบเทียบและตรงกับรูปแบบการรบกวน ในฐานข้อมูล IDS CC

จากนั้นก็จะเพิ่มการเตือนภัยถ้าตรวจพบการรบกวน ศูนย์ควบคุม IDS บันทึกข้อมูลที่ได้รับจากการตรวจสอบ MA ลงในฐานข้อมูลของ ชื่อและการวินิจฉัยของการค้นพบที่อาจจะถูกรบกวน VM จะแสดงสีดำและส่งไปยัง VMs ทั้งหมดยกเว้น VMs ไว้สีดำ เมื่อผู้ดูแลค้นพบ VM ใหม่ในรายการสีดำ การดำเนินงานที่จำเป็นจะต้องดำเนินการ การกระทำเหล่านั้นจะแตกต่างกันมากเมื่อเทียบกับการกระทำต่อเครื่องที่ถูกรบกวนทางกายภาพ นั่นเพราะเสมือนเป็นเครื่องแบบไดนามิกและจะถูกสำเนาได้อย่างง่ายดายและย้ายได้อย่างลงตัวระหว่างเซิร์ฟเวอร์ทางกายภาพ นั่นคือเหตุผลที่ช่องโหว่สามารถแพร่กระจายโดยไม่รู้ตัว จึงเสมือนเครื่องที่มีข้อความที่ถูกรบกวนเช่นเดียวกับข้อแนะนำจากการถูกห้ามโยกย้ายที่โยกย้ายของ VMs ที่รบกวนอาจนำไปสู่การแพร่ระบาดของการรบกวน

ตามที่ปรากฏในรูปที่ 22 IDS ทุกหน่วยงานควรส่งข้อความ "HB" เพื่อแสดงว่ามีตัวตนอยู่ (ดังแสดงในรูปที่ 22) เพื่อ IDSCC เป็นระยะ ๆ เพื่อบ่งชี้ถึงสถานะ ในกรณีเมื่อมีข้อความเหล่านี้ จะไม่ได้รับการรบกวน

1) IDS Agency : ตัวแทนมือถือต้องการสภาพแวดล้อมที่มีตัวตนที่เรียกว่าเอเจนซี่ หน่วยงานมีหน้าที่ในการโฮสติ้งและตัวแทนในการรันแบบขนานและจัดให้มีสภาพแวดล้อมเพื่อให้สามารถเข้าถึงบริการสื่อสารกันและการโอนย้ายไปหน่วยงานอื่น ๆ หน่วยงานยังควบคุมการทำงานของตัวแทนและปกป้อง VMs ต้นแบบจากการเข้าถึงโดยไม่ได้รับอนุญาตจากตัวแทนที่เป็นอันตราย นอกจากนี้ตั้งแต่ สร้างระดับของการแยก virtualization เครื่องข้อมูลทางกายภาพได้รับความคุ้มครองโดยการสั่งตัวแทนใน VE ปัญหาของการปกป้องเครือข่ายตัวแทนมือถือจากอันตรายที่ได้รับการเป็นเวลานาน แต่พิสูจน์แล้วว่าเป็น ปัญหาอาจจะท้าทายโดยเทคโนโลยีเสมือนจริง

2) การประยุกต์ใช้ตรวจจับเฉพาะ Static Agent : Agent Static ตรวจจับการกระทำ (SAD) เช่นจอภาพ VM สร้างเหตุการณ์ ID ร่องรอยของการรบกวน เมื่อใดก็ตามที่มีการตรวจพบและเหตุการณ์เหล่านี้จะถูกส่งในรูปแบบของข้อความที่มีโครงสร้างเพื่อ IDS Control Center SAD คือความสามารถในการตรวจสอบ VM สำหรับชั้นเรียนที่แตกต่างกัน การรบกวน SAD เป็นผู้รับผิดชอบต่อการแยกวิเคราะห์แฟ้มบันทึกการตรวจสอบข้อมูลสำหรับรูปแบบการรบกวนที่เกี่ยวข้องในแฟ้มบันทึก การแยกข้อมูลที่เกี่ยวข้องกับการรบกวนจากส่วนที่เหลือของข้อมูลและการจัดรูปแบบข้อมูลตามที่ต้องการโดยการตรวจสอบ MA จากโครงสร้าง IDS อนุญาตให้ใช้องค์ประกอบของโครงการอื่น ๆ เป็นเซ็นเซอร์ตรวจจับการรบกวน



รูปที่ 22 สถาปัตกรรม IDS ใน Subnet

กรณีดังกล่าวจะทำการตรวจจับ Agent ที่ทำงานในด้านบนสุดของเซนเซอร์ ตัวอย่างเช่นการรบกวนเครือข่าย Snort ระบบการตรวจสอบและเซนเซอร์ที่สามารถใช้ในการทำแพ็คเก็ตการกรองและการมองหาการรบกวนในแพ็คเก็ตสัญลักษณ์ ที่จะกำหนดภาระของ CPU อย่างน้อยใน VM

3) ผู้เชี่ยวชาญสืบสวน Mobile Agent : ตัวแทนมือถือสืบสวน (IMA) มีความรับผิดชอบในการเก็บรวบรวมหลักฐานของการรบกวนจากทั้งหมด VM การวิเคราะห์การรบกวนและการตรวจสอบต่อไป แล้วรวมข้อมูลนั้นไปตรวจยังพบการรบกวนแบบกระจาย แต่ละ IMA เป็นเพียงความรับผิดชอบในการตรวจสอบประเภทการรบกวน ทำให้ง่ายขึ้นสำหรับการอัปเดตเมื่อพบรูปแบบการรบกวนใหม่หรือประเภทใหม่ ๆ ที่คิดค้นวิธีการตรวจสอบ นอกจากนี้ตัวแทนมือถือเก็บข้อมูลที่น้อยลงและรหัสที่ประหยัดแบนด์วิดธ์และส่งผลให้ลดค่าใช้จ่ายการดำเนินงาน การตรวจสอบรายชื่อ MA ใช้ของที่ถูกรบกวน Agency (LCA) เพื่อระบุรายละเอียดการเดินทางของโฮสต์สำหรับการเยี่ยมชม

4) ศูนย์ควบคุม ระบบตรวจสอบการบุกรุก : Intrusion Detection-System Control Center คือ (IDSCC) จุดกลางของ IDS การบริหารองค์ประกอบในแต่ละ subnet ซึ่งจะรวมถึงองค์ประกอบ VM ทั้งหมดที่ไม่ ปกติและส่วนประกอบต่อไปนี้

- ฐานข้อมูล ควรมีฐานข้อมูลของการรบกวนทุกรูปแบบที่สามารถนำมาใช้โดยแจ้ง Console เพื่อเพิ่มการเตือนภัยหากรูปแบบการจับคู่กับการตรวจพบกิจกรรมที่น่าสงสัย รหัสเหตุการณ์ทั้งหมดที่รายงานโดย SAD จะถูกเก็บไว้ในฐานข้อมูลอื่น นอกจากนี้ IDS ศูนย์ควบคุมควรจะเก็บสถานะใหม่ของ VMs VM ในระบบของจะมีสามสถานะเป็น : ปกติ รบกวน โยกย้าย

- แจ้ง Console ส่วนนี้จะเปรียบเทียบกิจกรรมที่น่าสงสัยกับฐานข้อมูลการรบกวนและเพิ่มเตือนหากถูกเปรียบเทียบได้

- เครื่องกำเนิดไฟฟ้า Agent สร้างงานเฉพาะตัวแทนในการตรวจสอบการรบกวน (SAD และ IMA) ได้สมาชิกใหม่ ๆ โดยใช้ความรู้ที่ถูกสร้างขึ้นโดยข้อมูลสรุปจากหลักเกณฑ์หรือจากประสบการณ์ที่ได้รับก่อนหน้านี้

- ผู้จัดส่ง Mobile Agent การดำเนินการตรวจสอบตัวแทน VMs มือถือตามหมายเลขประจำตัวของเหตุการณ์หรือกิจกรรมที่น่าสงสัยที่ได้รับจาก SADs นอกจากนี้จะกำหนดรายชื่อผู้ที่ถูกรบกวนหน่วยงาน (LCA) สำหรับ IMAs

- ข้อมูลตามหลักเกณฑ์ ใช้แบบเรียนรู้ที่จะอนุมานความรู้การตรวจสอบ การรบกวน ใหม่จากระบบฐานข้อมูลที่มีการรบกวนตรวจพบและระบบบันทึกและข้อมูลที่มาจาก SADs ในส่วนนี้ใช้ Java ตัวแทนสำหรับ Meta - Learning โครงการ (JAM) ที่ Columbia University NY ซึ่งจะใช้กับเรียนรู้ที่จะอนุมานข้อมูลแบบกระจาย

- ผู้จัดการระดับ Trust กำหนดระดับความไว้วางใจสำหรับทุกหน่วยงานใน subnet IDS ยิ่งกว่านั้นช่วยให้ระดับความไว้วางใจของอื่น ๆ IDS ศูนย์ควบคุมอยู่ในบริเวณเดียวกันของเครือข่าย มีระดับความไว้วางใจสามคือ 1 ปกติ 2 ที่น่าสงสัย 3 ความสำคัญ การเปลี่ยนแปลงระดับความน่าเชื่อถือขึ้นอยู่กับ SA และMA ผลการตรวจสอบระดับความน่าเชื่อถือของทุกหน่วยงานใน subnet IDS สามารถแก้ไขความน่าเชื่อถือได้โดยผู้จัดการระดับ ตัวอย่างเช่นตามที่กล่าวไว้ก่อนหน้านี้ในบทความนี้ในกรณีที่จังหวะข้อความที่ไม่ได้รับโดย IDSCC จาก IDS Agency ผู้จัดการจะลดระดับความเชื่อมั่นและความไว้วางใจของสำนักงาน เมื่อระดับความไว้วางใจจากหน่วยงานถึงเกณฑ์ที่คาดไว้นั้นจะถูกระบุว่าเป็นหน่วยงานที่ถูกรบกวน IDS

ตามที่จุดมุ่งหมาย VMs ทั้งหมดที่ผลิต ID เดียวกันกิจกรรมที่น่าสงสัยจะรวมอยู่ในรายการเดียวกันของหน่วยงานที่ถูกรบกวน (LCA) แต่เมื่อ VM ได้รับละเมิดซึ่งบริเวณใกล้เคียงก็มีความเสี่ยงสูงจึงต้องมีการตรวจสอบเช่นกัน วิธีการของสำหรับการกำหนด LCA คือการใช้รุ่นที่เรียบง่ายของระบบตรวจหาการรบกวนตามกราฟ (กริด) กริดสร้างรูปทรงที่แตกต่างกันของกราฟสำหรับระยะเวลาหนึ่งที่แสดงถึงการกระจายการรบกวนขนาดใหญ่ โหมดและการเชื่อมโยงของกราฟแสดงที่น่าสงสัย VMS และการเชื่อมต่อระหว่าง VMs ตามลำดับ การขยายผลต่อไปของการรบกวนเพื่อ VMs อื่น ๆ นำไปสู่ทางที่จะเจริญเติบโตของกราฟ แสดงกราฟนี้แล้วสรุปว่าจะให้ผลลัพธ์ที่มีการเปรียบเทียบกับค่าเกณฑ์สำหรับข้อบ่งชี้ของการรบกวน สรุปหมายความว่ากริดจะใช้วิธีการของกราฟรวมกันก็จะอ้างถึงและลดข้อมูลที่ต้องวิเคราะห์ได้ในระดับที่สูงขึ้น

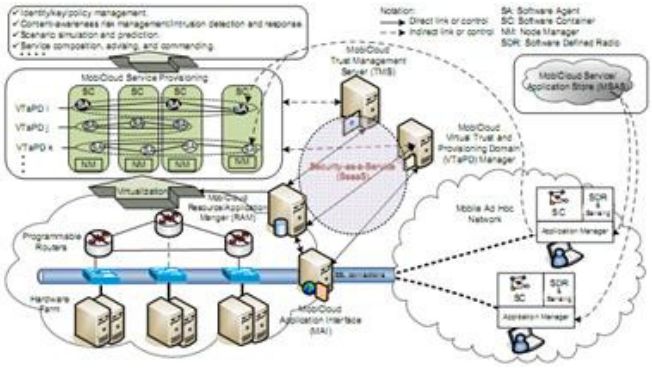
เพื่อที่จะใช้กลยุทธ์ที่ไปยังโปรแกรมประยุกต์ IDS ขั้นตอนแรกคือการสร้างพื้นที่ใกล้เคียงที่เสมือนศูนย์ควบคุมทั้งหมด IDS มีเพื่อนอยู่ในบริเวณเดียวกัน เมื่อใด ศูนย์ IDS ใหม่ควบคุมเข้าสู่ระบบ แต่ก็เป็นไปได้รับการกำหนดพื้นที่ใกล้เคียงเสมือน กำหนดค่าของระบบพื้นที่ใกล้เคียงนี้ไม่คงที่และสามารถเป็นแบบไดนามิก การกำหนดค่าเริ่มต้นของกราฟประกอบด้วยจุดและตำแหน่งในเครือข่ายกำหนดพื้นที่ใกล้เคียง เพื่อที่จะได้รับประสิทธิภาพการทำงานที่มีประสิทธิภาพจำนวนของบริเวณใกล้เคียงในละแวกใกล้เคียงกันไม่ควรเกินขอบเขตที่กำหนดไว้ล่วงหน้า ซึ่งประเด็นนี้จะกล่าวถึงต่อไปในส่วน ในวิธีการดูพื้นที่ใกล้เคียงทั้งหมด IDS CC จะถือเป็นเท่ากับทุก IDS CC จะดำเนินการตรวจสอบการรบกวนสำหรับอื่น ๆ IDS CC ในพื้นที่ใกล้เคียงของแต่ละศูนย์ควบคุมจัดเก็บข้อมูลเกี่ยวกับประเภทบริเวณใกล้เคียงส่วนใหญ่เป็นคำอธิบายของพฤติกรรมปกติของบริเวณใกล้เคียงและข้อมูลได้เช่น checksums ของไฟล์ระบบปฏิบัติการที่สำคัญ ตัวอย่างเช่นถ้า VM ตรวจพบการรบกวนในบริเวณใกล้เคียง B แล้วจะสื่อสารกับบริเวณใกล้เคียง B ก็ต่อเมื่อ VM ได้รับข้อตกลงร่วมแล้ว B จะถูกระบุว่าเป็นบริเวณใกล้เคียงที่ถูกรบกวน การออกแบบระบบตรวจสอบการบุกรุก IDS ที่แตกต่าง การรบกวนบน IDS CC มีการตรวจพบการใช้ peer-to-peer ดังนั้นจึงได้ทำวงแหวนการป้องกันสำเร็จในเครือข่ายนี้ นอกจากนี้จะมีการฝึกฝนจุดเดียวของปัญหาความล้มเหลวในรูปแบบ AAFID เพราะมีมากกว่าหนึ่ง IDS CC ในเครือข่าย นอกจากนี้เมื่อเทียบกับวิธี AFFID โหลดเครือข่ายมีการกระจายมากขึ้นสมมาตรระหว่างเครือข่าย นอกจากนี้ยังใช้ข้อมูลและความรู้เทคนิค การซื้อแบบของคือแม้มีความสามารถในการบรรลุความรู้ใหม่ ๆ เพื่อตรวจหารูปแบบใหม่ของการรบกวน scalability ดีเด่นเป็นอีกหนึ่งจุดแข็งของการออกแบบ เช่น VM ย้ายไปยังเครื่องนอกขอบเขตองค์กร (เช่นจาก cloud ส่วนตัวไป Cloud สาธารณะ เช่น Amazon EC2) ก็ยังคงเป็นไปได้ที่จะดำเนินการตรวจสอบการรบกวน IMA สามารถโยกย้ายเช่นเดียวกับ VMs และนี่คือความเป็นเอกลักษณ์ของการออกแบบที่จะให้ขยายระบบ IDS ที่ดีและมีความยืดหยุ่น

MobiCloud Building Secure Cloud Framework for Mobile Computing AndCommunication [11]

MobiCloud : กรอบการสร้าง Cloud ที่ปลอดภัยสำหรับคอมพิวเตอร์เคลื่อนที่และการสื่อสารวัตถุประสงค์คือการใช้วิธีการตรวจสอบระบบ Cloud คอมพิวเตอร์ทั้งสองและเทคโนโลยี โทรศัพท์มือถือเครือข่ายแอดฮ็อก (MANETs) เพื่อให้เข้าใจถึงความสามารถของ Cloud คอมพิวเตอร์สำหรับการใช้งาน Manet รักษาความปลอดภัย จะนำเสนอเป็นแนวทางเพื่อเลือกทิศทางการและการแก้ปัญหาที่เป็นไปได้ในการเพิ่มการรักษาความปลอดภัยคอมพิวเตอร์เคลื่อนที่โดยใช้ Cloud คอมพิวเตอร์ นำเสนอใหม่กรอบการสื่อสาร Manet ชื่อ MobiCloud ที่จะเปลี่ยนแปลงพื้นฐานการและพัฒนาเทคโนโลยีด้านการรักษาความปลอดภัย Manet นอกจากนี้จะระบุตัวเลขของปัญหาการเพื่อให้ให้คำแนะนำสำหรับ Cloud คอมพิวเตอร์และ Manet เพื่อพัฒนาโซลูชั่นใหม่สำหรับการรักษาความปลอดภัยระบบคอมพิวเตอร์เคลื่อนที่

MobiCloud แปลง MANETs แบบดั้งเดิมในรูปแบบการสื่อสารใหม่ที่มุ่งเน้นบริการ MobiCloud แปลงโหมดแต่ละมือถือจากโหมดการสื่อสารแบบดั้งเดิม layer structured อย่างเคร่งครัดในโหมดบริการ (SN) SN แต่ละคนสามารถนำมาใช้เป็นผู้ให้บริการหรือตัวแทนบริการตามความสามารถของสถานประกอบการ เช่น การคำนวณความสามารถในการสื่อสารที่มีอยู่และเพื่อสนับสนุนการบริการโดยเฉพาะ วิธีการนี้จะใช้ประโยชน์สูงสุดของมือถือแต่ละ

โหมดในระบบโดยใช้เทคโนโลยี Cloud คอมพิวเตอร์ เพื่อลดความไม่แน่นอนที่เกิดจากการเคลื่อนย้ายรวม SN เป็น MobiCloud ทุกองค์ประกอบเป็นแบบเสมือนจริง SN แต่ละหนึ่งหรือหลาย Extended Semi - Shadow ใน Cloud ถึงแอดแดรสของการสื่อสารและการคำนวณของโทรศัพท์มือถือ ESSI สามารถมีความแตกต่างจากภาพเสมือนในที่ ESSI สามารถโคลนแน่นอน โคลนบางส่วนหรือภาพเสมือนที่มีฟังก์ชั่นการขยายของอุปกรณ์ทางกายภาพ นอกจากนี้ ESSIs สร้าง Manet รูปแบบเสมือนและการสื่อสารในชั้นที่สามารถให้ความช่วยเหลือโหมดเคลื่อนที่ทางกายภาพ



รูปที่ 23 แสดงแบบจำลอง MobiCloud

สำหรับการเพิ่มความพร้อมของบริการ MobiCloud ให้แพร่หลายสำหรับผู้ใช้โทรศัพท์มือถือสามารถสรุปได้ดังต่อไปนี้

- สนับสนุนฟังก์ชั่น MobiCloud Manet การเผยแพร่ข้อมูลการกำหนด Rounter รองรับหลายภาษาและมีความเชื่อมั่น

- ผสมผสาน MobiCloud และเทคโนโลยี Cloud คอมพิวเตอร์ เพื่อสร้างสภาพแวดล้อมเสมือนจริงสำหรับการดำเนินงานใน Manet บริการจัดหาโดเมนหลายๆตามสถานะของบริการ Manet และข้อกำหนดด้านความปลอดภัยที่สอดคล้องกัน

- MobiCloud ให้ความเชื่อมั่นพื้นฐานรูปแบบรวมทั้งการจัดการ identity การจัดการคีย์และความปลอดภัยของข้อมูล การบังคับใช้นโยบายการใช้บริการที่สามารถใช้ในการพัฒนาโปรแกรมบนมือถือในอนาคต

- MobiCloud สนับสนุนการดำเนินการ Manet ผ่านงานเกี่ยวกับการประเมินความเสี่ยงหน้าที่ตระหนักถึงการใช้ ตัวชี้วัดการสื่อสารและประสิทธิภาพการทำงานของแต่ละโหมดมือถือภายใต้ข้อกำหนดด้านความปลอดภัยที่สอดคล้องกันนี้จะช่วยให้สามารถใช้ MobiCloud ที่จะตรวจสอบประสิทธิภาพการทำงานที่หลากหลายและปัญหาด้านความปลอดภัยของ Manet และสร้างข้อมูลที่มีประโยชน์

สำหรับสถาปัตยกรรม MobiCloud ในบริการรักษาความปลอดภัย

1) MobiCloud Architecture : รูปที่ 23 แสดงโครงสร้างพื้นฐานของแนวคิดใน MobiCloud เช่นเดียวกับที่มีอยู่ในการคำนวณและการเก็บรักษาเอาท์ซอร์ส cloudbased ฟาร์มฮาร์ดแวร์ สามารถใช้ประโยชน์จากโหมดมือถือบนกลุ่ม Cloud เพื่อเพิ่มความสามารถในการใช้คอมพิวเตอร์ นอกจากนี้ยังแนะนำรูปแบบใหม่ของบริการที่ชื่อ "การจัดเตรียมโดเมนเสมือนที่เชื่อถือได้ (VTaPD)" เพื่อแยกข้อมูลที่กระจายอยู่ในที่แตกต่างกัน โดยใช้เทคโนโลยีเตอร์ที่ตั้งโปรแกรมโดเมนของการรักษาความปลอดภัยได้ นอกจากนี้ยังให้การจัดการความเชื่อมั่นที่ละเอียดและข้อเสนอแนะความสามารถในคำสั่งไปยังผู้ใช้โทรศัพท์มือถือ โดยสรุป MobiCloud ได้รับการออกแบบเพื่อให้บริการ Cloud สำหรับ MANETs ต่อไปนี้:

- ให้บริการนโยบายการตัดสินใจที่สำคัญและการจัดการเข้าใช้ข้อมูลความปลอดภัย ให้ isolations รักษาความปลอดภัยเพื่อป้องกันข้อมูลที่ผู้ใช้มือถือ

- ตรวจสอบสถานะ Manet สำหรับการประเมินความเสี่ยงการตรวจจับการรบกวนและการตอบสนอง

- จำลองสถานการณ์และคาดการณ์สถานการณ์ Manet ในอนาคตเพื่อการตัดสินใจ

- ให้บริการและการประยุกต์ใช้องค์ประกอบสำหรับอุปกรณ์มือถือ

จะอธิบายการทำงานและคุณสมบัติขององค์ประกอบของรูปที่ 23 ตัวแทน MobiCloud ใช้ซอฟท์แวร์ (SAS) คือองค์ประกอบที่ใช้งาน เพื่อเชื่อมโยงบริการ Cloud และโทรศัพท์มือถือ SA เดียวกันสามารถทำงานได้ทั้งบนอุปกรณ์มือถือและแพลตฟอร์ม Cloud อุปกรณ์แต่ละตัวสามารถมีได้หลาย SAS สำหรับการบริการที่แตกต่างกันหรือ MANETS Cloud ซึ่งมีการจัดการโดยการจัดการประยุกต์ใช้อุปกรณ์ อุปกรณ์แต่ละตัวยังให้ข้อมูลเกี่ยวกับอุปกรณ์ตรวจจับตัวเอง เช่น ประเภทของการประมวลผลการใช้ประโยชน์ สถานะพลังงานและพื้นที่ด้วยการสนับสนุนจีพีเอส และ ที่อยู่ของผู้ใกล้เคียงที่มีคุณภาพเชื่อมโยงระยะเวลาใกล้เคียงและอื่นๆ ซึ่งมีการจัดการโดยมีผู้จัดการการตรวจจับ

ทางด้าน Cloud, MobiCloud Application Interface (MAI) บริการการส่งออกที่สามารถใช้งานโดยอุปกรณ์มือถือ นอกจากนี้เอ็มเอไอยังให้อินเตอร์เฟซเพื่อ VTaPD ผู้จัดการและอุปกรณ์และการประยุกต์ใช้ Manager-(RAM) จะต้องตอบอยู่บนพื้นฐานซอฟท์แวร์กลาง เมื่อส่วนประกอบ Cloud ไม่ได้ใช้อินเตอร์เฟซบนเว็บ หลายชิ้นส่วน Cloud ที่ไม่ซ้ำกันและโครงสร้างถูกเสนอ MobiCloud โดยแนะนำตั้งโปรแกรมเตอร์ที่สามารถใช้ในการสร้างหลาย VTaPDs VTaPDs ส่วนใหญ่จะถูกสร้างขึ้นสำหรับการแยกการกระจายของข้อมูลและการควบคุมการเข้าถึงโดยการสร้างโดเมนเสมือนหลาย ๆ มีสองเหตุผลหลักสำหรับโดเมนเสมือน คือ (1) การรักษาความปลอดภัยของอุปกรณ์ของผู้ใช้อาจเรียกใช้โปรแกรมหลายโดเมนที่มีการรักษาความปลอดภัยที่แตกต่างกันเช่นการสื่อสารในเวลาเดียวกันกับสองบุคคลที่มีจากโดเมนที่บริหาร (2) หน้าที่ context aware - อาจมีความจำเป็นต้องแยกบริการต่างหากสำหรับการตั้งค่าโลคอลและเครือข่ายที่แตกต่างกัน ตัวอย่าง เช่น MobiCloud สามารถจำลองการดำเนินงานของ MANETs ใช้พารามิเตอร์ของระบบที่แตกต่างกันหรือขั้นตอนวิธีการเลือกแนวทาง เพื่อเปรียบเทียบวิธีการที่แตกต่างกันสำหรับการใช้ Cloud คอมพิวเตอร์และอุปกรณ์การสื่อสาร วิธีการนี้จะช่วยให้เข้าใจถึงภาพรวมของการดำเนินงาน Manet และให้ข้อมูลกับโทรศัพท์มือถือแก่ผู้จัดการระบบเพื่อการตัดสินใจ

ในแต่ละ VTaPD หนึ่งหรือมากกว่า SAS จะใช้ในการ ESSI ทุก Node Manager (นาโนเมตร) มีหน้าที่จัดการโหลดและขน SAS ใน ESSI ESSI ยังมีความสามารถเพิ่มเติมนอกเหนือจากการทำงานของอุปกรณ์มือถือ ตัวอย่างเช่น Cloud จะสามารถเรียกใช้บริการที่ไม่สามารถใช้ได้ใน MANETs เช่น การค้นหา การทำข้อมูลให้เป็นประโยชน์การประมวลผลสื่อ ความเชื่อมั่น สถานประกอบการก่อน (เช่นการแลกเปลี่ยน credential และการสร้างกุญแจ รักษาความปลอดภัยในโค้ด) เป็นต้น MobiCloud อุปกรณ์และโปรแกรม ประยุกต์การจัดการ (RAM) โครงสร้าง VTaPDs เมื่อมีการกำกับการแสดงโดย ผู้จัดการ MobiCloud VTaPD และ MobiCloud Trust Manager Server (TMS) รูปแบบหลักการในการให้บริการ Security- as - a - Service (SeaaS) ด้วย SeaaS MobiCloud สามารถนำเสนอความสามารถในการประกอบบริการรักษาความ ปลอดภัยตามการร้องขอจากการใช้งานโทรศัพท์มือถือ ในรูปแบบการบริการ SeaaS ผู้จัดการ VTaPD มีตั้งแต่บทบาทเป็นศูนย์กลางการเก็บรวบรวมข้อมูล จาก Manet (เช่นค่าอุปกรณ์ตรวจจับสถานที่และสถานะอุปกรณ์ใกล้เคียง) และ ใช้สำหรับตรวจสอบการรบกวนและการบริหารความเสี่ยง TMS MobiCloud เป็น Authority Trust (TA) สำหรับ MobiCloud สามารถจัดการกับการกระจาย คีย์แอตทริบิวต์ที่ใช้และการเพิกถอน จะให้การค้นหาตัวตนและการบริการ สหพันธ์สำหรับอุปกรณ์มือถือของการบริหารหลายโดเมน นอกจากนี้ยัง ดำเนินการตรวจสอบนโยบายและการบังคับใช้ฟังก์ชั่นที่จะให้ความเชื่อมั่นต่อ ระบบการจัดการแบบครบวงจรสำหรับ MobiCloud

สุดท้าย MobiCloud บริการและ Application Store (MSAS) ทำ หน้าที่เป็นพื้นที่เก็บข้อมูลสำหรับ SAS และการประยุกต์ใช้ เมื่อองค์ประกอบ ของบริการเป็นสิ่งจำเป็น MSAS จะต้องติดตั้ง SAS หรือการใช้งานผ่านเอ็มเอไอ ตัวอย่าง เช่น เมื่อต้องการใช้โทรศัพท์มือถือสื่อสารกับอุปกรณ์ที่ใช้คลื่นความถี่ที่ แตกต่างกัน ซอฟแวร์ที่กำหนด Radio (SDR) ความต้องการในการติดตั้ง โปรแกรมควบคุมใหม่และโหมดความต้องการรูปแบบการตรวจสอบอื่น ใน สถานการณ์สำหรับไดรเวอร์ใหม่นี้ SAS และโมดูลการตรวจสอบจะถูกติดตั้ง การดำเนินการนี้ต้องการความร่วมมือระหว่าง TMS และ MSAS

2) การแยกรักษาความปลอดภัยผ่าน VTaPDs : VTaPDs ถูกจัดตั้ง ขึ้นเพื่อให้การควบคุมการเข้าถึงข้อมูลและการป้องกันข้อมูล จะต้องทราบว่า กรอบอาจไม่จำเป็นต้อง บ่งบอกถึงการแบ่งการบริหารของโดเมนเป็น VTaPDs ในส่วนย่อยต่อไปนี้จะอยู่แยกอุปกรณ์ Cloud และการแยกการรักษาความ ปลอดภัย

- การแยกอุปกรณ์ การบริหารงานที่เกิดขึ้นจริงจะถูกจัดการโดย ผู้จัดการ MobiCloud VTaPD โหมดที่เป็นของ VTaPD โดยเฉพาะทุกคนจะมี ข้อมูลเตอร์ที่สมบูรณ์เพื่อ VTaPD แต่ไม่สำหรับคนอื่นๆ แต่ละโหมดสามารถ อยู่ในระบบทางกายภาพที่แตกต่างกัน แต่ละโหมดจะต้องสนับสนุนกรอบการ สื่อสารของซึ่งรวมถึงกลุ่มสื่อสารที่ปลอดภัยเพื่อส่งข้อมูลไปยัง ESSIs ทั้งหมด ใน VTaPD เดียวกัน แบนด์วิดท์สำหรับการเชื่อมโยงการสื่อสารสามารถแบ่งได้ โดยใช้ cryption en แตกต่างกัน ถอดรหัสคีย์รับรองความถูกต้อง ประโยชน์จาก กรอบ MobiCloud ที่ให้การทำงานแบบเสมือนผ่านเครือข่ายหลาย VTaPDs คือ การจัดลำดับความสำคัญของการอำนวยความสะดวกที่สำคัญ บริการฉุกเฉินใน เครือข่าย ตัวอย่าง เช่น การใช้วิธีการทำงานแบบเสมือนเสนอจัดลำดับ ความสำคัญและชั้นบริการปกติสามารถกำหนดได้โดยใช้ VTaPDs ที่แตกต่าง กัน สามารถแบ่งปัน Manet ทางกายภาพเดียวกัน แต่จัดลำดับความสำคัญตาม VTaPD Manet การดำเนินงานและการสื่อสารสามารถโยกย้ายมา Cloud เมื่อ การสื่อสาร Peer - to - peer อยู่ภายใต้ความปั่นป่วนทั้งจากแบนด์วิดธ์ไม่เพียงพอ หรือการรบกวน

- การควบคุมการเข้าถึงข้อมูล นอกเหนือจากการแยกให้บริการ โดเมน VTaPD, MobiCloud ยังต้องการที่จะรวมการควบคุมการเข้าถึงข้อมูล และการแยกข้อมูลโดยใช้วิธีการเข้าตามรหัส นอกจากนี้ยังกังวลด้านความ ปลอดภัยแบบเดิม (ซึ่งก็คือการตรวจสอบ อนุมัติการตรวจสอบ ฯลฯ) ความ เสี่ยงด้านความปลอดภัยเพิ่มเติมได้ถูกนำเสนอโดยผู้ใช้โทรศัพท์มือถือที่ใช้ อุปกรณ์ร่วมกัน อุปกรณ์ที่เกี่ยวข้องใน Cloud นี้จะหมายถึงสภาพแวดล้อมที่เป็น ผู้เช่าหลายคน ผู้ใช้มือถือของแต่ละ ESSI ถือได้ว่าเป็น การครอบครองของตน ใน MobiCloud ในสภาพแวดล้อมแบบหลายผู้เช่า การควบคุมการเข้าถึงข้อมูล เป็นหนึ่งในปัญหาการรักษาความปลอดภัยที่จำเป็นที่สุดที่ต้องมี addressed ข้อมูลการแยกกลไกการป้องกันผู้ใช้จากการเข้าถึงแหล่งข้อมูลอื่น ๆ ที่เป็นของผู้ เช่า โดยทั่วไปจะมีสองชนิดของการเข้าถึงรูปแบบการแยกการควบคุมการ อนุญาตอย่างชัดแจ้งและ แนะนำวิธีการใช้ทั้งสองรูปแบบในรูปแบบข้อมูล multitenant

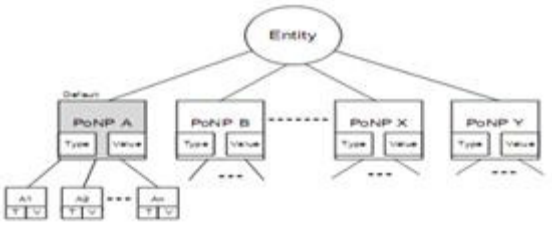
- การแยกจาก Access Control ในรูปแบบนี้เมื่อผู้ใช้ร้องขอเพื่อเข้าถึง อุปกรณ์ที่ใช้ร่วมกัน ระดับแพลตฟอร์มบัญชีทั่วไป (คือตัวตนที่สอดคล้องกัน ESSI กับ SA และการร้องขออุปกรณ์ Cloud) จะมอบหมายให้จัดการกับคำขอนี้ โดยได้รับมอบหมายเป็นผู้เช่าของบัญชีที่ใช้ร่วมกันและมีสิทธิ์ในการเข้าถึง อุปกรณ์ของผู้เช่าทั้งหมด แต่ที่สำคัญของกลไกนี้คือการประกอบเป็นผู้เช่าโดย atenant-oriented คือตัวกรองที่จะใช้ในการป้องกันไม่ให้ผู้ใช้คนหนึ่งใช้อุปกรณ์ ของผู้เช่าอื่น ๆ นี้สามารถทำได้โดยใช้วิธีการเข้ารหัสที่ใช้คือกลุ่มโซลูชั่นการ บริหารจัดการตามหลักเพื่อรักษาความปลอดภัยการกระจายของข้อมูลผ่าน VTaPDs โดยแตกต่างกันที่ระบบทางกายภาพเดียวกัน

- กำหนดการอนุญาตจากการควบคุมการเข้าถึงอย่างชัดเจน: ใน รูปแบบนี้ให้สิทธิ์การเข้าใช้อุปกรณ์ที่ได้รับอย่างชัดเจนก่อนกำหนดให้กับบัญชี ผู้เช่าที่สอดคล้องกันโดยใช้กลไกการควบคุมการเข้าถึงรายการ (ACL) ดังนั้นจึง ไม่จำเป็นต้องใช้ประโยชน์จากผู้เช่าที่ได้รับมอบหมายจากบัญชีเพิ่มเติมทั่วไป

การจัดการความเชื่อถือ MobiCloud

การจัดการความเชื่อมั่นใน Mobil Cloud ประกอบด้วยการเชื่อมโยง กันหลายองค์ประกอบซึ่งจะได้รับการรวมทั้งการจัดการ identity การจัดการคีย์มี ประสิทธิภาพการควบคุมการเข้าถึงข้อมูลและการประเมินความเสี่ยงของการ รักษาความปลอดภัยตระหนักถึงหน้าที่ที่ใช้ นอกจากนี้จะนำเสนอวิธีการในการ รวมเทคนิค Cloud คอมพิวเตอร์เพื่อพิจารณาแก้ไขปัญหาการหลายปัญหาที่ยาก มากสำหรับ MANETs

1) MobiCloud Identity Management : การบริหารจัดการตัวตนผู้ใช้เป็นศูนย์กลางซึ่งยังเรียกบ่อยครั้งเพื่อเป็น 2.0 identity ช่วยให้บุคคลที่จะระบุมีหลายตัว ตัวอย่าง เช่น ตัวระบุดำเนินการในบัตรประจำตัวประชาชนของชาติจะกลายเป็นเพียงหนึ่งในหลายของตัวระบุของแต่ละบุคคลซึ่งยังรวม ID หนังสือเดินทาง บัตรประจำตัวสโมสรทหาร ID ID อีเมลที่ไม่ซ้ำกัน MAC IP ฯลฯ มีงานหลายวิเคราะห์ว่าปัญหาอาจอยู่ในบริเวณนี้ วิธีการให้ความสะดวกปลอดภัย Single Sign - On ไปยังหน่วยงานที่แตกต่างกันหลาย วิธีการให้บุคคลควบคุมที่ละเอียดสำหรับ identities ส่วนบุคคลร่วมกันระหว่างหน่วยงานเฉพาะเมื่อมีการให้ประโยชน์ จะทราบได้ว่าข้อมูลใดที่จะแบ่งปันตัวตนเมื่อสองผู้ใช้ที่ตอบสนองอย่างไร จะนำเสนอเนื้อหา Attribute - Based Identity Management-(ABIDM)

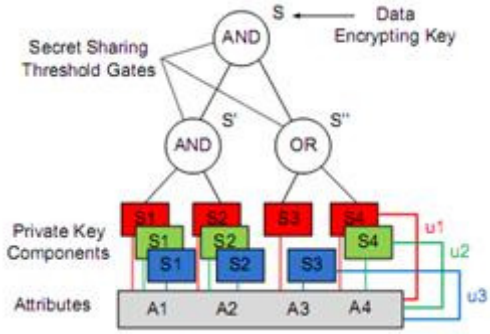


รูปที่ 24 แสดง Identity scheme

การแสดงตัวตนพื้นฐานของ ABIDM จะแสดงในรูปที่ 24 การใช้ ABIDM อันดับแรกจำเป็นต้องกำหนดจุดของการนำเสนอระบบเครือข่าย (PoNP) ความสัมพันธ์ของโหมดมือถือสามารถคิดเป็นเส้นแผ่จาก PoNP กับคู่ค้าต่างๆ แต่ละบรรทัดมีที่แตกต่างและติดแท็กที่มีคุณลักษณะที่ใช้โดยเฉพาะเป็นคู่โดยเฉพาะอย่างยิ่งกำหนดค่าเริ่มต้น PoNP สำหรับแต่ละบุคคล

PoNP เริ่มต้นได้ที่จะเชื่อมโยงโดยใช้ ID โลคอลที่ไม่ซ้ำกัน เอกลักษณ์ของ ID โลคอลทำได้ไม่อยาก แท้จริงแล้วผู้ใช้สามารถมีรหัสโลคอลที่ไม่ซ้ำกันโดยเพียงแค่คนใดคนหนึ่งของ hashing เธอตัวระบุที่ไม่ซ้ำกันเช่น ID ทหาร SSN ฯลฯ ไม่จำเป็นต้องใช้ตัวระบุจากการบริหารโดเมนเดียวกัน PoNP แต่ละคนมีสองคุณสมบัติ : ชนิดและมูลค่า PoNP แต่ละ บริษัท ร่วมกับแอตทริบิวต์หนึ่งหรือหลาย ๆ (A1. ..) และคุณลักษณะแต่ละชนิดมีคุณสมบัติและค่า

ประโยชน์ที่สำคัญของการใช้แทนตัวนี้เป็นมาตรฐานของการจัดการข้อมูล ในทางปฏิบัติสำหรับมือถือทุกโหมดตัวเลขของ PoNPs ไม่ควรมากสามารถกำหนดให้ผู้ใช้มือถือเป็นคุณลักษณะที่กำหนดไว้ล่วงหน้าว่าจะไม่มีการเปลี่ยนแปลงบ่อย เรียกลักษณะเหล่านี้เป็นแอตทริบิวต์แบบคงที่ เพื่อความแตกต่าง PoNPs สามารถที่จะลดตัวเลขของคุณลักษณะที่สามารถนำมาใช้เพื่อการติดต่อสื่อสารที่อาจมีความปลอดภัยในภายหลัง



รูปที่ 25 Attribute-based Encryption

2) การจัดการคีย์ที่มีประสิทธิภาพสำหรับการรักษาความปลอดภัยและการควบคุมการเข้าถึงข้อมูลส่วนตัว : ในรูปที่ 25 จะนำเสนอตัวอย่างเพื่อแสดงให้เห็นถึงการใช้ ABE สำหรับการเข้ารหัสข้อมูลและการถอดรหัส ในตัวอย่างนี้คุณลักษณะ A1 ถึง A4 ถูกจัดเป็นโหมดใบของโครงร่างต้นไม้คุณลักษณะ คุณลักษณะที่แต่ละคนสามารถมีหลายข้อมูลลับสำหรับผู้ใช้ที่แตกต่างกัน จะต้องทราบว่าผู้ใช้สามารถใช้แอททริบิว แต่อย่างไรก็ตามองค์ประกอบหลักที่สอดคล้องกันว่าภาคเอกชนสำหรับคุณลักษณะที่แตกต่างกันนี้จะแสดงเป็นสีที่แตกต่างกันของคีย์ ดังนั้น U1 มีองค์ประกอบหลักสำคัญ (สีแดง : S1; S2; S3; S4) U2 มีเอกชน สีเขียวมีองค์ประกอบสำคัญ : S1; S2; S4 และ U3 มีคีย์ส่วนสำคัญประกอบ สีน้ำเงิน : S1; S2; S3 โหมดภายในของโครงร่างต้นไม้คุณลักษณะเป็นตรรกะเช่น AND OR เรียบเรียงข้อมูลลับที่จะดำเนินการโดยใช้รูปแบบการใช้งานร่วมกันของข้อมูลลับสามารถจะได้มาจาก S'S " และการใช้รูปแบบการแบ่งปันความลับ ในระดับล่างการเข้ารหัสจะทำโดยใช้การก่อสร้างคล้ายกับการเข้ารหัส identity - based (IBE) ในระหว่างการเข้ารหัสเพื่อความพึงพอใจและทางเข้า Decrypter ต้องมีความลับทั้งหมดตามนั้นเพื่อสร้างความลับระดับสูงกว่าเพื่อตอบสนองความการเข้ารหัส จะต้องมีหนึ่งความลับเท่านั้น วิธีการเข้ารหัสลับของ ABE จะดำเนินการในลักษณะจากบนลงล่างโดยการสร้าง ciphertext ในคุณลักษณะระดับล่างของโครงร่างต้นไม้ขั้นตอนวิธีการถอดรหัสลับของ ABE จะดำเนินการในลักษณะล่างขึ้นโดยใช้ความลับก่อนการกระจายของผู้ใช้เพื่อสร้างความลับระดับที่สูงขึ้นจนกว่าจะถึงราก ในตัวอย่างนี้ขึ้นอยู่กับความลับก่อนกระจาย U1 U3 สามารถถอดรหัสความลับจึงสามารถเข้าถึงข้อมูลที่เข้ารหัสโดยใช้ DEK S โซลูชั่นการจัดการที่สำคัญที่มีอยู่มักจะพิจารณาการจัดการที่สำคัญและ Identity Management (IDM) เป็นที่แตกต่างกันของข้อมูล จะใช้โซลูชั่นการจัดการเนื้อหาสำคัญ ได้แก่ ABKM เพื่อบูรณาการการจัดการที่สำคัญและ IDM ใน ABKM ก็สามารถพิจารณาคุณลักษณะทั้งหมดเป็นของนิติบุคคลที่เป็นคีย์สาธารณะของคุณลักษณะที่แต่ละคนสามารถได้รับการพิจารณาเป็นองค์ประกอบสำคัญของ state และแต่ละคู่แอตทริบิวต์ยังมีองค์ประกอบสำคัญส่วนตัว คีย์ส่วนตัวซึ่งในทางกลับกันจะเกิดขึ้นจากองค์ประกอบสำคัญหลายภาคเอกชนมีการกระจายจาก TA จะต้องทราบว่า ABKM เป็นพื้นฐานรุ่นขยายตัวของการเข้ารหัสที่ใช้ซึ่ง

ในตัวตนได้รับการพิจารณาและหลายแอตทริบิวต์อธิบายคุณลักษณะสามารถนำมาใช้ในการแทนอธิบายผู้ประกอบการตรรกะเช่น "And" และ "Or" เมื่อเทียบกับแบบดั้งเดิม PKI โซลูชันการจัดการคีย์ที่คีย์ส่วนตัวของผู้ใช้เป็นที่รู้จักกันเฉพาะกับเจ้าของสาธารณะโดยใช้ ABKM TA จะสร้างองค์ประกอบหลักส่วนตัวสำหรับผู้ใช้แต่ละคนตามคุณลักษณะของตนสาธารณะ วิธีการนี้จะให้ประโยชน์ที่สำคัญในคีย์ส่วนตัวที่สามารถสร้างขึ้นสำหรับคำอธิบายหรือแทนการใช้เลขสุ่มขนาดใหญ่ (เช่น RSA) คำบรรยายสามารถใช้ในการกำหนดนโยบายการควบคุมการเข้าถึงข้อมูลที่มากที่มีประสิทธิภาพในแง่ของการจัดการนโยบายการรักษาความปลอดภัย ตัวอย่างเช่นข้อมูลการควบคุมแบบดั้งเดิมมักจะใช้วิธีการเข้าถึงโพรโทคอแลกเปลี่ยนที่สำคัญในการเผยแพร่ข้อมูลการเข้ารหัส Key (DEK) ให้กับผู้ใช้ในการถอดรหัส ciphertext อย่างไรก็ตามการใช้ ABKM โปรโตคอลการแลกเปลี่ยนที่สำคัญคือไม่จำเป็นต้องใช้ ผู้ส่งเพียงแค่สามารถเลือกแบบของคุณลักษณะตามนโยบายการรักษาความปลอดภัยที่จำเป็นในการสร้าง ciphertext คุณสมบัตินี้เป็นประโยชน์อย่างมากใน MANETs ทนความล่าช้าตั้งแต่แหล่งที่มามักจะไม่จำเป็นต้องพูดคุยกับปลายทางก่อนที่จะส่งข้อมูล นอกจากนี้ยังสามารถเข้าถึงข้อมูลได้อย่างมีความยืดหยุ่นโดยที่ผู้ส่งข้อมูลไม่จำเป็นต้องรู้ว่าตัวตนของผู้รับ ในความเป็นจริงวิธีการนี้มีประสิทธิภาพมากสำหรับการสื่อสารกลุ่มรักษาความปลอดภัยที่กลุ่มของเครื่องรับอาจตอบสนองนโยบายการเข้าใช้ข้อมูลที่ระบุ นอกจากนี้นโยบายโครงร่างต้นไม้สามารถนำมาใช้เพื่อการสื่อสารในกลุ่มรักษาความปลอดภัยตั้งแต่สามารถนำคุณสมบัติมาใช้เพื่อระบุกลุ่มของผู้ใช้ที่ทำให้น่าสนใจในการ ABKMระบบการสื่อสารขนาดใหญ่

3) Context - ตระหนักถึงการบริหารความเสี่ยงใน MobiCloud : การบริหารจัดการความเสี่ยงเรียกร้องให้มีการระบุการประเมินและจัดลำดับความสำคัญของความเสี่ยงด้วยการประสานงานและประหยัดการใช้งานเพื่อลดการตรวจสอบและการควบคุมความน่าจะเป็นและหรือผลกระทบของเหตุการณ์เพื่อเพิ่มความตระหนักในโอกาส วิธีการนิยามและเป้าหมายแตกต่างกันใน MANETs ไม่ว่าจะเป็นวิธีการจัดการความเสี่ยงในหน้าที่ของภารกิจที่สนับสนุนฟังก์ชั่นการดำเนินงานหรือการรักษาความปลอดภัย จะมุ่งเน้นไปที่สององค์ประกอบสำคัญของการบริหารความเสี่ยง : กรอบหน้าที่เตอร์และตรวจสอบการรบกวนตอบสนอง Context - Aware Routing : การรับรู้หน้าที่เป็นแนวคิดที่มีความหลากหลายของความหมายแท้จริงจะหมายถึงการคำนึงถึงหน้าที่ในขณะที่การตัดสินใจ แต่ความหมายของหน้าที่ที่แตกต่างกันไปขึ้นอยู่กับการใช้งาน การตัดสินใจใช้สภาพแวดล้อม ใน MANETs การรับรู้หน้าที่มักจะหมายถึงให้พิจารณาถึงค่าระบบของอุปกรณ์ (เช่นระดับแบตเตอรี่ไฟ CPU) พารามิเตอร์ของเครือข่าย (เช่นแบนด์วิดธ์ ความล่าช้าการเชื่อมต่อ) ปริมาณ (เช่นภารกิจที่ระบุเป้าหมาย) และการรักษาความปลอดภัย (เช่นความเป็นส่วนตัวของสถานที่การโจมตี) เมื่อใช้งานเครือข่าย ทั้งนี้เป็นเพราะสภาพแวดล้อมดังกล่าวมักจะมีลักษณะแบบไดนามิกสูงที่อาจมีผลต่อการใช้งานอย่างมีนัยสำคัญ เพื่อที่จะให้บริการอย่างต่อเนื่องในเช่นเครือข่ายแบบไดนามิกสูง หน้าที่ตระหนักถึงการย้ายจะต้องให้บริการเพื่อให้การใช้งานสามารถปรับตัวกับการหมดอายุ ตัวอย่างเช่นเมื่อโหมดการให้บริการบางอย่างหมดแบตเตอรี่ กรอบควรจะตระหนักถึงความเปลี่ยนแปลงหน้าที่ดังกล่าวและโอนย้ายบริการ (และหน้าที่การรันทั้งหมด) ไปยังอีกโหมดใช้ได้ เพื่อให้บรรลุถึงความสามารถในการรับรู้หน้าที่โหมดมือถือความต้องการในการเก็บรวบรวมข้อมูลหน้าที่ของทั่วไป (เช่นคุณสมบัติของอุปกรณ์ พารามิเตอร์การสื่อสารและการรักษาความปลอดภัย) และเป็นระยะส่งของ ESSI การประเมินความเสี่ยงที่ครอบคลุมสามารถทำงานใน MobiCloud ตั้งแต่สถานะของระบบทั้งหมด (เช่น end - to - end ความล่าช้าของการสื่อสาร สถานการณ์เชื่อมต่อไปยังปลายทาง สถานะการรักษาความปลอดภัยของโหมดแต่ละมือถือและอื่น ๆ) สามารถใช้ได้ ถ้าต้นทุน (คำนวณผ่านทางฟังก์ชันอรรถประโยชน์) ของการใช้การสื่อสารเฉพาะกิจสูงกว่าค่าใช้จ่ายในการส่งข้อมูลผ่าน Cloud การสื่อสาร Cloud เป็นที่ต้องการ คุณภาพฟังก์ชั่นจะต้องมีการออกแบบมาอย่างดีเพื่อดำเนินงานภายใต้สถานการณ์ต่าง ๆ ที่เป้าหมายพันธกิจของ MANETs ยุทธวิธีและสอดคล้องหน้าที่ที่เกี่ยวข้องกับการวัดความสามารถแตกต่างกันการใช้บริการCloud การเก็บรวบรวมข้อมูลและการประมวลผลจะได้รับการจัดการแบบรวมศูนย์ มีความซับซ้อนของการดำเนินงาน context-awareness มาก นอกจากนี้ยังสามารถดำเนินการจำลองบน MobiCloud ในการประเมินแบบต่างของการดำเนินการสำหรับ MANETs แล้วให้คำแนะนำที่ดีกว่า ในโหมดมือถือนี้จะลดความไม่แน่นอนของระบบโทรศัพท์มือถือและทำให้ปรับปรุงประสิทธิภาพของการสื่อสาร Manet โดยเฉพาะอย่างยิ่งการวางตำแหน่ง การบำรุงรักษาโครงสร้างเครือข่ายและฟังก์ชั่นการกำหนดเตอร์สามารถทำได้โดยการใช้บริการ Cloud แต่ละโหมดจะได้รับข้อมูลจาก Cloud นี้ด้วยวิธีนี้การเผยแพร่ข้อมูลในโหมดมือถือจะกลายเป็นแบบหนึ่งต่อหนึ่งการสื่อสารระหว่างอุปกรณ์ทางกายภาพและภาพเงาใน Cloud แทนการสื่อสารแบบหนึ่งต่อจำนวนมากใน MANETs แบบดั้งเดิมนี้จะช่วยลดค่าใช้จ่ายในการสื่อสารและการจัดการของโหมดโทรศัพท์มือถือ นอกจากหน้าที่ที่ใช้เตอร์ MobiCloud ยังต้องคำนึงถึงเนื้อหาของข้อความเมื่อมีการกำหนดเตอร์การตัดสินใจ ข้อมูลภารกิจ Manet มักจะอยู่ในเนื้อหาที่ส่ง ตัวอย่าง เช่น เนื้อหาดังต่อไปนี้จะมีผลต่อการตัดสินใจกำหนดเตอร์ : ต่ำสุดของช่วงเวลา จากผู้ส่งข้อความ เนื้อหาของเพรดิเคผู้ใกล้เคียง (เช่นบทบาทเพื่อนบ้านการประมวลผลข้อมูลที่ได้รับฟังก์ชั่นในระดับการกวาดล้างการรักษาความปลอดภัยและอื่น ๆ) และระยะเวลาที่แต่ละผู้ใกล้เคียงได้รับนอกเหนือจากปลายทาง

การบริหาร MobiCloud หลายโซลูชั่นมีความเสี่ยงด้านความปลอดภัย Manet ที่มีอยู่แล้วได้พยายามป้องกัน MANETs โดยใช้วิธีการป้องกันถึงแม้ว่าวิธีการป้องกันอย่างมีนัยสำคัญสามารถลดการโจมตีที่อาจเกิดขึ้นพวกเขาไม่สามารถนับบุคคลภายในที่เป็นอันตราย (จากการกำหนดค่าผิดพลาดหรือความผิดปกติโหมด) การทำงานก่อนนั้น มีการเสนอให้นับระบุโหมดมือถือเป็นอันตรายโดยการแยกโหมด uncooperative จากมุมมองของการจัดการความเสี่ยงและเป็นอุปสรรคที่สำคัญของวิธีการว่าไม่คำนึงถึงผลกระทบด้านลบของการแยก ในมาตรการบางกรณีการแทรก อาจก่อให้เกิดความเสียหายมากขึ้นกว่าการโจมตีที่เกิดขึ้นจริงที่ระบุ (เช่นโดยการแยกเครือข่ายทั้งหมด) เพื่อให้การประเมินความเสี่ยงที่ครอบคลุมการเก็บรวบรวมข้อมูลรวมศูนย์และการประมวลผลจะมี

ประสิทธิภาพมากขึ้น ในกรณีของเครือข่ายแบ่งพาร์ทิชันที่เป็นโหมดอันตราย การกระจายสูงจะประสบอัตราเชิงลบที่ผิดพลาดตั้งแต่ผู้โจมตีสามารถจัดการในการสร้างพาร์ทิชันที่แตกต่างกันภายใน MobiCloud สามารถระบุจุดที่เป็นอันตรายและทำให้การประเมินความเสี่ยงที่มีความรู้เต็มทั้งระบบการสื่อสาร Manet

VI. บทสรุป

โมบายคลาวด์คอมพิวติ้งเป็นเทคโนโลยีที่มีความน่าสนใจและเหมาะสมกับยุคที่โทรศัพท์มือถือหรืออุปกรณ์พกพาที่มีความสามารถในการเชื่อมต่อเข้ากับเครือข่ายอินเตอร์เน็ตในการติดต่อสื่อสารปัจจุบันและสามารถช่วยในการรับส่งข้อมูลต่าง ๆ โดยจะเป็นการนำเทคโนโลยีคลาวด์คอมพิวติ้งมาช่วยในการลดข้อจำกัดของอุปกรณ์พกพาในด้านพื้นที่ในการจัดเก็บข้อมูลหรือโปรแกรมต่าง ๆ ในด้านการช่วยประหยัดพลังงานทำให้ใช้งานได้ยาวนานขึ้น และในด้านการประมวลผลจะทำให้รวดเร็วขึ้น มีประสิทธิภาพมากยิ่งขึ้น ซึ่งสิ่งเหล่านี้จะทำให้มีการพัฒนาการในด้านต่าง ๆ เช่น ด้านธุรกิจไม่ว่าจะเป็นการทำธุรกรรมออนไลน์ ด้านการอำนวยความสะดวก เช่น การแจ้งสัญญาณไฟจราจรสำหรับผู้พิการทางการมองเห็น และอื่น ๆ โดยจะเห็นได้ว่ามีข้อดีอยู่มากมายแต่เทคโนโลยีนี้ก็มีจุดอ่อนอยู่ที่ต้องมีการเก็บข้อมูลไว้ที่ส่วนกลาง ทำให้ความปลอดภัยนับว่าเป็นเรื่องที่ต้องให้ความสำคัญ

สำหรับงานวิจัยที่ควรศึกษาในอนาคตควรจะเป็นเรื่องการรักษาความปลอดภัยในการใช้คลาวด์คอมเตอร์ทั้งในส่วนของที่ใช้ผ่านอุปกรณ์พกพาและใช้คอมพิวเตอร์แบบปกติ

VII.บรรณานุกรม

[1] Li. Li, Li. Xiong, Youxia. Sun, Wen. Liu, “Research on Mobile Multimedia Broadcasting Service Integration Based on Cloud Computing”, Multimedia Technology (ICMT), 2010 International Conference, pp. 1, Oct 2010

[2] Hongqing. Gao, Yanjie.Zhai, “System design of cloud computing based on Mobile Learning”, Knowledge Acquisition and Modeling (KAM), 2010 3rd International Symposium , pp. 239, Oct 2010

[3] Jon. Oberheide, Kaushik. Veeraraghavan, Evan. Cooke, Jason. Flinn, Farnam. Jahania, “Virtualized in cloud security services for mobile devices”, Virtualization in Mobile Computing (MobiVirt'08) Breckenridge, pp. 1, June 2008

[4] Zehua. Zhang, Xuejie. Zhang, “Realization of Open Cloud Computing Federation”, Intelligent Computing and Intelligent Systems, 2009. ICIS 2009. IEEE International Conference, pp. 642, Nov 2009

[5] Xu. Young, Hu. Qiqi, “The framework of the fourth party mobile integrated payment platform based on cloud computing“, Networking and Digital Society (ICNDS), 2010 2nd International Conference, pp. 496, May 2010

[6] Gaoyun. Chen, Jun. Lu, Jian. Huang, Zexu. Wu, “SaaAS The mobile agent based service for cloud computing in internet environment”, Natural Computation (ICNC), 2010 Sixth International Conference, pp. 2935, Aug 2010

[7] Xiaoyan. Yang, Tiejun. Pan, Jingjing. Shen, “On 3G mobile E-commerce platform based on Cloud Computing”, Ubi-media Computing (U-Media), 2010 3rd IEEE International Conference, pp. 198, July 2010

[8] Charalampos. Doukas, “Mobile Healthcare Information Management utilizing CloudComputing and Android OS”, Argentina, 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina,pp. 1037, August 2010

[9] VishnuS. Pendyala, JoAnne. Holliday, “Performing Intelligent Mobile Searches in the Cloud using Semantic Technologies”, Santa Clara University, Santa Clara, CA, USA, 2010 IEEE International Conference on Granular Computing, pp. 642, Nov 2009

[10] Dastjerdi, A. V, Bakar, K. A, Tabatabaei, S. G. H, "Distributed Intrusion Detection in Clouds Using Mobile Agents", Advanced Engineering Computing and Applications in Sciences, 2009. ADVCOMP '09. Third International Conference, pp. 175, Oct 2009

[11] Dijiang. Huang, Xinwen. Zhang, Myong. Kang, Jim. Luo, " MobiCloud: Building Secure Cloud Framework for Mobile Computing and Communication", Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium, pp. 27, June 2010

[12] Yunqi. Ye, Jain. N, Longsheng. Xia, Joshi. S, I-Ling. Yen, Bastani. F, Bowler. M.K, ”A Framework for QoS and Power Management in a Service Cloud Environment with Mobile Devices”, Service Oriented System Engineering (SOSE), 2010 Fifth IEEE International Symposium, pp. 236, June 2010

[13] Klei. Andreas, Mannweiler. Christian, Schneider, Joerg, Schotten, Hans. D, “Access Schemes for Mobile Cloud Computing ”, Mobile Data Management (MDM), 2010 Eleventh International Conference, pp. 387, May 2010

[14] Qingfeng. Liu, Xie. Jian, Jicheng. Hu, Hongchen. Zhao, Shanshan. Zhang, “An Optimized Solution for Mobile Environment Using Mobile Cloud Computing”, Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference, pp. 1, Sept 2009

[15] Angin, Pelin, Bharat, Helal, Sumi, “A Mobile-Cloud Collaborative Traffic Lights Detector for Blind Navigation ”, Mobile Data Management (MDM), 2010 Eleventh International Conference, pp. 396, May 2010

[16] HyunJung. La, SooDong. Kim, “A Conceptual Framework for Provisioning Context-aware Mobile Cloud Services ”, Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference, pp. 466, July 2010

[17] Kelenyi. I, Nurminen. J.K, “CloudTorrent - Energy - Efficient BitTorrent Content Sharing for Mobile Devices via Cloud Services ”, Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE , pp. 1, Jan 2010