A Survey of Mobile Cloud Computing Security

ณัชชารีย์ วิเชียรนิตย์, บุญญารินทร์ อ่อนนุ่ม, เยาวลักษณ์ พรมดี, สุทธิยา รัตนคุณศาสน์
อรปริญญ์ วนาพันธพรกุล, อ้อมใจ เขาทอง
ภาควิชา วิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยขอนแก่น

บทคัดย่อ- เทคโนโลยีของการประมวลผลบนคลาวด์เป็นที่ได้รับความแพร่หลายในปัจจุบัน โดยระบบการประมวลคลาวด์มีการใช้งานผ่านหลายแพลตฟอร์มรวมทั้งบนอุปกรณ์สมาร์ทโฟน ที่เป็นที่นิยมมาก โดยการใช้คลาวด์เข้ามาช่วยในการใช้งานมีทั้งองค์กรและส่วนบุคคลที่เลือกใช้งานบนคลาวด์ การใช้อุปกรณ์ในการเข้าถึงพื้นที่การจัดเก็บข้อมูลนั้นสิ่งที่จำเป็นต่อการเข้าถึง คือ ด้านการรักษาความปลอดภัยในการเข้าใช้บริการคลาวด์ อีกทั้งประสิทธิภาพในการรักษาความปลอดภัย ปัจจัยที่เกี่ยวข้องต่างๆ ซึ่งแบบสำรวจงานวิจัยนี้ได้ทำการสำรวจเก็บข้อมูลงานวิจัยด้านความปลอดภัยในการใช้งานคลาวด์คอมพิวติ้งบนอุปกรณ์โทรศัพท์สมาร์ทโฟน โดยได้ทำการสำรวจและจัดกลุ่มเนื้อหาออกเป็น 5 หัวข้อ แบ่งเป็นด้านต่างๆ ดังนี้ การบริการความปลอดภัย (Security Service), กรอบแนวคิดการรักษาความปลอดภัย (Security Framework), การบริการความปลอดภัยของการจัดเก็บ (Cloud Storage), การพิสูจน์ตัวตน (Authentication), การควบคุมการเข้าถึง (Access Control) เพื่อเป็นการสำรวจเปรียบเทียบของด้านความปลอดภัยในการใช้งานการประมวลผลแบบคลาวด์บนสมาร์ทโฟน

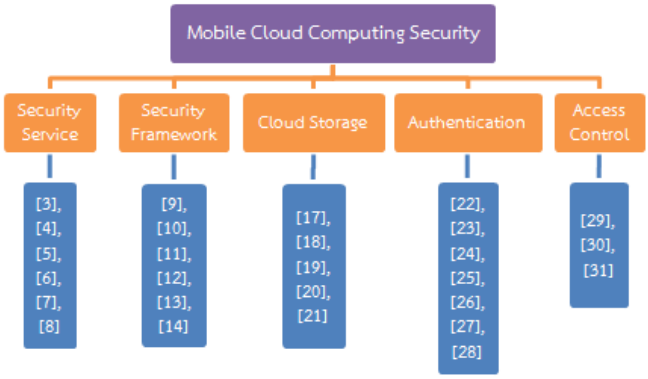
คำสำคัญ-- *Security Service, Security Framework, Cloud Storage, Authentication, Access Control*

I. บทนำ

Mobile Cloud Computing Security ก็คือ รูปแบบของความปลอดภัยในการประมวลที่มีความสามารถต่างๆ ที่เกี่ยวข้องกับข้อมูลสารสนเทศ ที่มีการจัดสรรในรูปแบบของบริการต่างๆ จากผู้ให้บริการผ่านการเข้าใช้งานโดยอุปกรณ์สมาร์ทโฟน ทำให้ผู้ใช้งานผ่านระบบเครือข่าย ผ่านอุปกรณ์สมาร์ทโฟนโทรศัพท์เคลื่อนที่เข้าถึงการใช้งานผ่านระบบอินเตอร์เน็ต ประโยชน์การใช้เทคโนโลยีจากคลาวด์คอมพิวติ้ง ในแง่ของด้านธุรกิจ ด้านการจัดสรรทรัพยากร ซึ่งสำหรับข้อมูลและทรัพยากรของระบบยังคงต้องมีการรักษาความปลอดภัยของส่วนความสามารถในการเข้าถึงข้อมูลและการบริการ ผ่านการใช้โทรศัพท์มือถือแบบสมาร์ทโฟนในการเข้าถึงการใช้บริการผ่านแอพพลิเคชั่นของคลาวด์

ในการสำรวจงานวิจัยที่เกี่ยวข้องทีมผู้วิจัยได้ศึกษาเรื่องของการรักษาความปลอดภัยของการใช้คลาวด์บนสมาร์ทโฟนหรือโทรศัพท์มือถืออัจฉริยะ โดยทำการศึกษาหัวข้อในการเปรียบเทียบผลงานวิจัย ลักษณะประสิทธิภาพ การเข้าถึง ความปลอดภัยในการจัดเก็บของคลาวด์ ซึ่งในส่วนของเนื้อหาภายในการสำรวจงานวิจัยนี้ประกอบด้วย (II) การบริการความปลอดภัย (Security Service) (III) กรอบแนวคิดการรักษาความปลอดภัย (Security Framework) (IV) การบริการความปลอดภัยของการจัดเก็บ (CloudStorage) (V) การพิสูจน์ตัวตน (Authentication) (VI) การควบคุมการเข้าถึง (Access Control) รวมทั้งกล่าวถึง (VII) ข้อสรุป และ (VIII) ข้อเสนอแนะงานวิจัยในอนาคต

ในการศึกษาแต่ละข้อหัวของด้านความปลอดภัยคลาวด์บนอุปกรณ์โทรศัพท์มือถือ จำพวกสมาร์ทโฟน ทำการศึกษางานวิจัยและมีการเปรียบเทียบผลงานของการวิจัยที่เกี่ยวข้องกับด้านการรักษาความปลอดภัยของข้อมูล ของการใช้งานโมบายคลาวด์หลากหลายงานวิจัย โดยจำแนกตามหัวข้อในการศึกษาเปรียบเทียบงานวิจัยดังนี้ Secutiy Service ได้ศึกษาจากงานวิจัยทั้งสิ้น 7 งานวิจัย Security Framework ศึกษางานวิจัยที่เกี่ยวข้องทั้งสิ้น 6 งานวิจัย Cloud Storage ศึกษางานวิจัยที่เกี่ยวข้องทั้งสิ้น 5 งานวิจัย Authentication ศึกษางานวิจัยทั้งสิ้น 5 งานวิจัย และหัวข้อสุดท้าย Access Control การเปรียบเทียบแบบจำลองการเข้าถึง ได้ทำการศึกษางานวิจัยที่สิ้น 4 งานวิจัย ดังรูปที่ 1

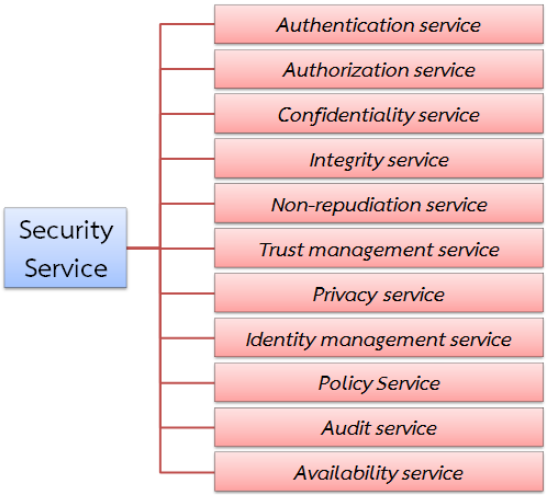


รูปที่ 1 แผนผังแสดงภาพรวมการสำรวจ Mobile Cloud Computing Security

II. Security Service

การบริการความปลอดภัย (Security Service) นับเป็นสิ่งสำคัญของการให้บริการความปลอดภัยแก่การประมวลผลแบบคลาวด์บนอุปกรณ์เคลื่อนที่อย่างเช่น โทรศัพท์มือถือ แท็บเล็ต หรืออุปกรณ์อื่นๆ ที่สามารถเชื่อมต่อเครือข่ายอินเตอร์เน็ตและใช้บริการข้อมูลบนคลาวด์ได้ เนื่องจากผู้ใช้ที่ใช้บริการคลาวด์ผ่านอุปกรณ์เคลื่อนที่จะต้องมีการทำกิจกรรมหรือทำธุรกรรมต่างๆ ผ่านแอพพลิเคชั่น อย่างเช่น การใช้บริการดาวน์โหลดแอพพลิเคชั่นผ่านแหล่งที่ให้บริการดาวน์โหลด มาติดตั้งในเครื่อง การใช้บริการที่ต้องกรอกข้อมูลเลขบัตรเครดิตให้กับบางแอพพลิเคชั่นที่มีการซื้อขายที่ไม่เคยติดต่อมาก่อน การลงทะเบียนเพื่อเข้าร่วมเป็นสมาชิกกับแอพพลิเคชั่นเชิง Social Network หรือการแบ่งปันข้อมูล รูปภาพ ข้อความต่างๆ ให้กับผู้ใช้งานอื่นๆ ผ่านบริการคลาวด์ เป็นต้น ซึ่งกิจกรรมเหล่านี้ผู้ใช้แต่ละคนมีความต้องการความเป็นส่วนตัวของข้อมูล การได้รับข้อมูลที่มีความถูกต้องครบถ้วนและ

แม่นยำ การมีสิทธิในการเข้าถึงข้อมูลของตนหรือข้อมูลของผู้ใช้อื่นที่อนุญาตและได้รับบริการที่มีประสิทธิภาพ มีความปลอดภัยจากเหตุการณ์อันตรายต่างๆ ดังนั้น ผู้ให้บริการคลาวด์จึงให้ความสำคัญกับการรักษาความปลอดภัย โดยมีการนำการบริการการรักษาความปลอดภัยรูปแบบต่างๆ มาช่วยเพิ่มประสิทธิภาพในการบริการคลาวด์ให้ปลอดภัยจากภัยคุกคามมากยิ่งขึ้น เราจึงได้นำรูปแบบต่างๆ สำหรับการบริการการรักษาความปลอดภัย [1] มาใช้ในการเปรียบเทียบกลไกการทำงานหรือโมเดลของแต่ละงานวิจัยที่ได้ค้นคว้าว่างานวิจัยนั้นได้นำบริการใดมาใช้ในการรักษาความปลอดภัยบ้าง ซึ่งรูปแบบการบริการความปลอดภัย แสดงแผนผังได้ดังรูปที่ 2 และอธิบายรายละเอียดความสำคัญของแต่ละบริการดังนี้



รูปที่ 2 แผนผังรูปแบบต่างๆ สำหรับบริการความปลอดภัย (Security Service)

- ***บริการการพิสูจน์ตัวตนของผู้ใช้ (Authentication service)***

การพิสูจน์ตัวตนของผู้ใช้ หมายถึง กระบวนการของการยืนยันหรือปฏิเสธการอ้างข้อมูลประจำตัวของผู้ใช้แต่ละคน เพื่อพิสูจน์ตัวตนว่าบุคคลที่ใช้งานระบบอยู่นั้นใช่บุคคลคนนั้นๆ จริงหรือไม่ เนื่องจากการใช้งานระบบต่างๆ จะเป็นการใช้งานระยะไกลไม่สามารถพิสูจน์ตัวตนได้ ไม่เห็นหน้า ไม่ทราบลักษณะของผู้ใช้ แต่จะเห็นเพียงข้อมูลที่ส่งผ่านไปมาเท่านั้น ซึ่งการใช้งานระบบต่างๆ จะเป็นแบบ Logical ทั้งสิ้น ดังนั้นการพิสูจน์ตัวตนของผู้ใช้ จึงเป็นกระบวนการที่ตรวจสอบว่า Logical ที่แทนบุคคลหรือระบบต่างๆ นั้นเป็นตัวแทนของบุคคลหรือระบบนั้นจริง กระบวนการใน**การ**พิสูจน์ตัวตนของผู้ใช้ ได้แก่ การพิสูจน์หลักฐานที่บุคคลนั้นๆ จะอ้างความเป็นตัวตนของบุคคลนั้นๆ จริงๆ เช่น Username และ Password การยืนยันตัวบุคคลด้วยใบรับรองอิเล็กทรอนิกส์ (certificates) เป็นต้น

- ***บริการการกำหนดสิทธิ์ในการใช้งานให้กับผู้ใช้ (Authorization service)***

การกำหนดสิทธิ์ในการใช้งานให้กับผู้ใช้ หมายถึง การพิสูจน์สิทธิว่าบุคคลที่ผ่านกระบวนการ Authentication นั้นมีสิทธิในการใช้งานระบบหรือทรัพยากรใดบ้าง จะเป็นกระบวนการที่เกี่ยวข้องกับการตรวจสอบและตั้งค่าสิทธิต่างๆ ของผู้ใช้งานในระบบ เพื่อให้การดำเนินการต่างๆ ถูกต้องตามนโยบายหรือกฎของระบบที่กำหนดไว้ล่วงหน้า โดยผู้ที่จะให้สิทธิ์แก่ผู้ใช้งานอื่นได้จะต้องเป็นผู้ใช้ที่มีอำนาจในการดำเนินงานภายในระบบนั้นๆ

- ***บริการการรักษาความลับของข้อมูล (Confidentiality service)***

การรักษาความลับของข้อมูล หมายถึง กระบวนการที่ช่วยให้แน่ใจว่าข้อมูลที่เป็นความลับนั้นจะสามารถเข้าถึงได้เฉพาะกับผู้ที่มีอำนาจหรือผู้ใช้ที่เป็นเจ้าของเท่านั้น บริการการรักษาความลับเพื่อป้องกันการดักฟังหรือลักลอบดูขอมูล เนื่องจากผู้บุกรุกที่ประสงค์ร้ายสามารถดักฟังการสื่อสารไร้สายและข้อมูลที่ตอบสนองกันได้ง่าย เช่น รหัสผ่าน การรักษาความลับสามารถทำได้โดยการสร้างเส้นทางแบบเข้ารหัส (Encryption) ระหว่างสถานีที่ใช้งานข้ามเครือข่ายกันและทางเข้าบนโครงสร้างพื้นฐานแบบมีสาย ซึ่งการรักษาความลับของข้อมูลจะจัดตั้งขึ้นโดยการใช้อัลกอริทึมการเข้ารหัสลับที่ให้ข้อมูลจำนวนหนึ่งมีการป้องกัน บริการรักษาความลับ จึงจะประกอบด้วยการปกป้องข้อมูลโดยใช้เทคนิคการเข้ารหัสและถอดการป้องกันด้วยเทคนิคการถอดรหัส อินเตอร์เฟสนี้จะกำหนดสองการดำเนินงาน: ซ่อนเพื่อปกป้องข้อมูลและเปิดเผยในการดึงข้อมูลจากข้อมูลที่มีการป้องกัน

- ***บริการการตรวจสอบความสมบูรณ์ของข้อมูล (Integrity service)***

การตรวจสอบความสมบูรณ์ของข้อมูล หมายถึง กระบวนการที่ช่วยให้แน่ใจว่าการสื่อสารของข้อความ (ข้อมูล) จะไม่เกิดความยุ่งยากในขณะที่มีการส่งหรือการจัดเก็บ (เช่น ในหน่วยความจำของอุปกรณ์) การสื่อสารที่ปลอดภัยจะต้องตรวจสอบความสมบูรณ์ของข้อความ(ข้อมูล) ที่ส่ง ซึ่งหมายความว่าจะสิ้นสุดการรับได้ต้องทราบก่อนว่าข้อความ (ข้อมูล) ที่ผู้รับกำลังได้รับนั้นเป็นข้อมูลเดียวกัน จึงจะถือว่าเป็นการสิ้นสุดการส่งข้อมูลที่ได้ส่งไป ความสมบูรณ์ (Integrity) มีเพื่อให้แน่ใจในความถูกต้องหรือความแม่นยำของข้อมูล และให้ข้อมูลที่ได้รับมีการป้องกันการเปลี่ยนแปลง แก้ไข การลบ การสร้าง และการทำสำเนาจากผู้ใช้ที่ไม่ได้รับอนุญาต

- ***บริการการป้องกันการปฏิเสธหรืออ้างความรับผิดชอบ (Non-repudiation service)***

การป้องกันการปฏิเสธหรืออ้างความรับผิดชอบ หมายถึง การป้องกันการปฏิเสธว่าไม่ได้มีการส่งหรือรับข้อมูลจากฝ่ายต่างๆ ที่เกี่ยวข้อง หรือการป้องกันการอ้างที่เป็นเท็จว่าได้รับหรือส่งข้อมูลแล้ว ซึ่งบริการนี้อาจมีการจัดกลไกต่างๆ ให้ใช้ เช่น ลายเซ็นดิจิตอล (Digital Signatures) การแปลงข้อมูลให้เป็นรหัส (Encipherment) การจดทะเบียนรับรอง (Notarization) และกลไกความสมบูรณ์ของข้อมูล (Data Integrity mechanisms) พร้อมการสนับสนุนจากการบริการอื่นๆ เช่น การประทับรับรองเวลาอิเล็กทรอนิกส์ (Time Stamping) ขั้นตอนวิธีการเข้ารหัสทั้งแบบสมมาตรและไม่สมมาตร (Symmetric and Asymmetric Cryptographic Algorithms) สามารถใช้สำหรับการป้องกันการปฏิเสธได้ โดยบริการนี้สามารถใช้รวมกับกลไกและการบริการเหล่านี้ได้ตามความเหมาะสม เพื่อเป็นการตอบสนองตามความต้องการด้านความปลอดภัยของแอพพลิเคชั่น

- ***บริการการจัดการความไว้วางใจ (Trust management service)***

ความไว้วางใจ (Trust) ถือเป็นสิ่งสำคัญอย่างหนึ่งกับการบริการการประมวลผลแบบคลาวด์บนอุปกรณ์เคลื่อนที่ โดยเฉพาะกับการใช้บริการที่ผู้ใช้งานรู้สึกว่าตนเองอาจจะตกอยู่ในภาวะที่เสี่ยงและอาจถูกหลอกลวง เช่น การใช้บริการที่ต้องมีการกรอกข้อมูลให้กับแอพพลิเคชั่นที่ไม่เคยใช้มาก่อน การใช้บริการที่ต้องมีการดาวน์โหลดโปรแกรมจากเครือข่ายอินเทอร์เน็ตมาติดตั้งในอุปกรณ์เคลื่อนที่ส่วนตัว และการใช้บริการที่ต้องกรอกข้อมูลเลขบัตรเครดิตให้กับบางแอพพลิเคชั่นที่มีการซื้อขายที่ไม่เคยติดต่อมาก่อน เป็นต้น

โดยการจัดการความไว้วางใจเป็นกระบวนการของการตัดสินใจเลือกสิ่งที่สามารถให้ความไว้วางใจในการกระทำนั้นได้ ซึ่งในสภาพแวดล้อมที่นโยบายการเข้าถึงได้อธิบายไว้ในแง่ของลักษณะของผู้ใช้หรือคุณลักษณะที่ต้องการ การจัดการความไว้วางใจประกอบด้วยการกำหนดแหล่งที่มาของผู้ที่มีอำนาจในการระบุตัวตนของผู้ใช้ การกำหนดคุณลักษณะ และการสร้างนโยบายที่เป็นไปได้ ในระบบที่ผู้ใช้จะได้รับยินยอมเครื่องแสดงการอนุญาต โดยระบบการอนุญาตสิทธิให้ทั้งหมดนั้นเรียกว่า การจัดการความไว้วางใจ ในระบบที่ผู้ใช้สามารถมอบหมายความถูกต้องบางส่วนหรือทั้งหมดของผู้ใช้ไปให้แก่ผู้ใช้อื่น โดยการควบคุมของการมอบหมายนั้นจะเป็นส่วนหนึ่งของการจัดการความไว้วางใจ

- ***บริการความเป็นส่วนตัวของผู้ใช้ (Privacy service)***

ความเป็นส่วนตัว (Privacy) ถือว่าเป็นความสามารถของผู้ใช้อุปกรณ์เคลื่อนที่เพื่อควบคุมการเปิดเผยของคุณลักษณะส่วนบุคคลให้กับคู่สนทนาของผู้ใช้ การปิดบังชื่อของผู้ใช้เป็นสิ่งจำเป็นสำหรับความเป็นส่วนตัว ความเป็นส่วนตัวส่งผลให้เอนทิตี้ที่ไม่อาจหลีกเลี่ยงได้ (เป็นปกติที่บุคคลจะทำหน้าที่ในนามของตัวเองเอง) สิทธิที่จะกำหนดระดับที่สิทธิจะโต้ตอบกับสภาพแวดล้อมของมัน รวมถึงระดับที่เอนทิตี้จะแบ่งปันข้อมูลเกี่ยวกับตัวเองให้กับผู้ใช้อื่นด้วยความสมัครใจ (การปิดบังชื่อ) บริการความเป็นส่วนตัวจะมุ่งประเด็นไปที่การจัดหมวดหมู่การขับเคลื่อนนโยบายของข้อมูลที่ระบุความเป็นส่วนบุคคล (Personally Identifiable Information (PII)) PII นั้นได้รวมถึงข้อมูล เช่น หมายเลขประกันสังคม, ที่อยู่, อายุ หรือความชอบในเครื่องดื่ม และข้อมูลนี้อาจมีความต้องการที่แตกต่างกันสำหรับการป้องกันความเป็นส่วนตัว ผู้ให้บริการและผู้ร้องขอบริการอาจเก็บข้อมูลส่วนบุคคลโดยใช้บริการความเป็นส่วนตัว บริการดังกล่าวสามารถนำมาใช้ในการสื่อสารและการบังคับใช้นโยบายความเป็นส่วนตัวขององค์กรแบบเสมือน (VO) นี่คือความสำเร็จโดยทั่วไปด้วยขั้นตอนวิธีการเข้ารหัส/ถอดรหัส

- ***บริการการจัดการการระบุตัวตน (Identity management service)***

การระบุตัวตน (Identity) เป็นขั้นตอนที่ผู้ใช้แสดงหลักฐานที่แสดงว่าตนเป็นบุคคลที่กล่าวอ้างจริง เช่น ชื่อผู้ใช้ (Username) ส่วนการจัดการการระบุตัวตนนั้นจะอธิบายถึงการจัดการระบุความเป็นตัวตนของผู้ใช้แต่ละคน การพิสูจน์ตัวตนของผู้ใช้ การกำหนดสิทธิ์การใช้งานของผู้ใช้ และสิทธิพิเศษหรือการออกใบอนุญาตเพื่อให้ผ่านเข้าไปในระบบได้ โดยการบริการนี้จะช่วยควบคุมการเข้าถึงข้อมูลและทรัพยากรในการประมวลผล ผู้ให้บริการคลาวด์บนอุปกรณ์เคลื่อนที่จะมีการรวมระบบการจัดการการระบุตัวตนอยู่ในโครงสร้างของพวกเขาด้วย เช่น การใช้ Federated Identity Management (FIdM) และ Single Sign-On (SSO)

- ***บริการนโยบายความปลอดภัย (Policy Service)***

ประเด็นสำคัญในการรักษาความปลอดภัยของอุปกรณ์เคลื่อนที่นั้นไม่ได้มีเพียงวิธีรักษาความปลอดภัยวิธีเดียวที่จะทำงานกำหนดลักษณะของสภาพแวดล้อมของอุปกรณ์เคลื่อนที่และการเสนอโครงสร้างพื้นฐานของการรักษาความปลอดภัยที่มีอยู่สำหรับอุปกรณ์เคลื่อนที่ไม่ได้เกี่ยวข้องกับการปฏิบัติ องค์กรจะต้องรักษาความปลอดภัยอุปกรณ์เคลื่อนที่อย่างเป็นอิสระและโดยเฉพาะนโยบายด้านความปลอดภัยการใช้งานโทรศัพท์มือถือจะต้องสร้างขึ้นและดำเนินการอย่างเป็นอิสระ การวิเคราะห์ความเสี่ยงอย่างครอบคลุมของการรักษาความปลอดภัยอันตรายที่เกี่ยวข้องกับการใช้อุปกรณ์เคลื่อนที่ที่อาจเกิดขึ้นได้ ควรเป็นขั้นตอนแรกคล้ายกับเส้นทางของการสร้างนโยบายการรักษาความปลอดภัยอุปกรณ์เคลื่อนที่ การสร้างนโยบายการรักษาความปลอดภัยที่มีเฉพาะในการใช้งานกับอุปกรณ์เคลื่อนที่นั้น ควรจะรวมถึงวิธีการลดผลกระทบการสูญหายของอุปกรณ์: อุปกรณ์ทั้งหมดควรจะป้องกันด้วยรหัสผ่าน เอกสารสำคัญที่เก็บไว้ในอุปกรณ์ควรจะเข้ารหัสและสคริปต์อัตโนมัติไม่ควรใช้ในการเข้าสู่ระบบ VPN รวมถึงลดการเข้าถึงแหล่งที่มาที่ถูกจำกัด โดยใช้ไฟร์วอล ดังนั้นขั้นตอนแรกคือการพัฒนานโยบายการรักษาความปลอดภัยที่เหมาะสมเพื่อควบคุมการใช้งานอุปกรณ์เคลื่อนที่ในเครือข่ายองค์กรควรมีนโยบายที่เฉพาะเจาะจงไปยังอุปกรณ์เคลื่อนที่ และไม่เพียงแค่พยายามที่จะใช้นโยบายด้านความปลอดภัยแบบทั่วไป แต่ยังเป็นสิ่งสำคัญที่องค์กรจะให้ความรู้แก่ผู้ใช้อุปกรณ์เคลื่อนที่ของตนในเรื่องเกี่ยวกับปัญหาด้านความปลอดภัย รวมทั้งการรักษาความปลอดภัยทางกายภาพ บางนโยบายการรักษาความปลอดภัยสามารถบังคับให้ทำเกี่ยวกับเทคโนโลยีได้ แต่นโยบายอื่นๆ จะขึ้นอยู่กับการปฏิบัติตามของผู้ใช้ ผู้ใช้อุปกรณ์เคลื่อนที่ฝั่งไคล์แอนต์ เช่น Smartphone, Tablet หรือ PDA ควรใช้มาตรการป้องกันในท้องถิ่น เช่น การควบคุมการเข้าถึง การพิสูจน์ตัวตนของผู้ใช้ (ลายนิ้วมือ) การป้องกันไวรัส ไฟร์วอลส่วนบุคคล การถูกจำกัดการเข้าถึงทรัพยากรฮาร์ดแวร์ (เช่น การเข้าถึง Memory cards ของโทรศัพท์มือถือ) และการเข้ารหัสข้อมูลท้องถิ่น

- ***บริการการตรวจสอบวัดประสิทธิภาพ (Audit service)***

บริการการตรวจสอบวัดประสิทธิภาพ เป็นตัวขับเคลื่อนนโยบายและความรับผิดชอบในการบันทึกเหตุการณ์การรักษาความปลอดภัยที่เกี่ยวข้อง บริการนี้โดยปกติจะใช้โดยผู้ดูแลระบบรักษาความปลอดภัยภายใน VO เพื่อตรวจสอบการปฏิบัติตามนโยบายการควบคุมการเข้าถึงและนโยบายการพิสูจน์ตัวตน การตรวจสอบนั้นต้องการเหตุการณ์ที่ถูกลงบันทึกไว้ในรูปแบบความปลอดภัยที่กำลังเป็นที่นิยม โดยบริการการบันทึกและความปลอดภัยในการเข้าถึงเพื่อลงบันทึกลงไว้ในการตั้งค่าแบบกระจาย ซึ่งเป็นปัญหาที่ซับซ้อนตั้งแต่ที่บันทึกอาจอยู่ในโดเมนการดูแลระบบที่แตกต่างกัน การลงบันทึก (Log) จะต้องได้รับความปลอดภัยและความยุ่งยากที่ผ่านการตรวจสอบแล้วและความสามารถในการสร้างความมั่นใจความสมบูรณ์ของข้อความท่ามกลางเหตุการณ์ที่ต้องการการตรวจสอบเหตุการณ์การรักษาความปลอดภัย ตัวอย่างเช่น การบุกรุก ซึ่งควรจะมีการจัดการด้วยบริการการรักษาความปลอดภัย

- ***บริการความพร้อมในการใช้งาน (Availability service)***

ความพร้อมในการใช้งาน (Availability) [2] เป็นการรักษาความพร้อมในการใช้งานของข้อมูล เช่น ข้อมูลบัญชีเงินฝากของลูกค้าธนาคาร หรือข้อมูลสำคัญต่าง ๆ ที่ต้องพร้อมใช้งานในเวลาที่ต้องการ ซึ่งในบางครั้งเป็นข้อมูลที่สามารถเปิดเผยให้สาธารณชนรับทราบได้ เพื่อประโยชน์ในการประชาสัมพันธ์ หรือการเผยแพร่ในวงกว้าง เช่น ข้อมูลการท่องเที่ยว การแบ่งปันข้อมูล หรือ การติดต่อแบบ Social Network เป็นต้น โดยใช้วิธีการ Back Up ต่าง ๆ ซึ่งการบริการนี้จะบริการการควบคุมระบบไม่ให้เกิดความล้มเหลว มีสมรรถภาพการทำงานต่อเนื่อง ไม่อนุญาตให้ผู้ที่ไม่มีสิทธิมาทำให้ระบบหยุดการทำงานได้ รวมทั้งมีการเตรียมที่ตั้งระบบสำรองในยามฉุกเฉิน

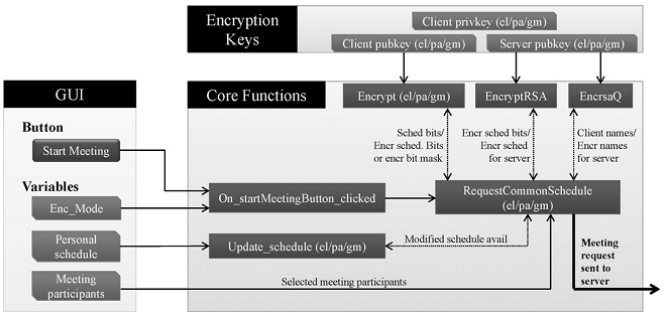
หากผู้ใช้อุปกรณ์เคลื่อนที่มีการใช้งานแอพพลิเคชั่นผ่านการประมวลผลบนคลาวด์แล้ว ผู้ให้บริการขาดการบริการความปลอดภัยดังที่กล่าวมาข้างต้น จะทำให้ข้อมูลที่มีอยู่เป็นจำนวนมาก เช่น ข้อความ รูปภาพ วิดีโอ ข้อมูลที่เป็นส่วนตัวต่างๆ ของผู้ใช้นั้น อาจถูกโจมตีจากผู้บุกรุกในสภาพแวดล้อมบนคลาวด์ ทำให้ขาดความเป็นส่วนตัวของข้อมูล อาจเป็นอันตรายต่อชีวิตและทรัพย์สินต่อผู้ใช้งาน และทำให้ผู้ใช้งานขาดความน่าเชื่อถือต่อผู้ให้บริการในการใช้บริการคลาวด์ เราจึงได้ศึกษางานวิจัยหลายๆบทความ [3], [4], [5], [6], [7], [8] ที่ได้เสนอโมเดลหรือกลไกการทำงานที่ให้บริการความปลอดภัยบนคลาวด์ ซึ่งมีเทคนิคและนำบริการความปลอดภัยรูปแบบต่างๆ มาใช้แตกต่างกันไป เราจึงขออธิบายรายละเอียดของแต่ละงานวิจัย และเปรียบเทียบได้ดังตารางที่ 1 แสดงให้เห็นถึงการบริการความปลอดภัยรูปแบบต่างๆ ที่แต่ละงานวิจัยได้นำมาใช้ และเปรียบเทียบข้อดีและข้อจำกัดของแต่ละกลไกนั้น ดังตารางที่ 2ก

A. *Meetings through the cloud: Privacy-preserving scheduling on mobile devices* [3]

งานวิจัยนี้ได้นำเสนอ 3 แนวคิดใหม่คือ ขั้นตอนวิธีการกำหนดเวลาของการรักษาความเป็นส่วนตัว (privacy-preserving scheduling) ซึ่งมีการใช้ประโยชน์จากคุณสมบัติ homomorphic ของระบบการเข้ารหัสลับแบบไม่สมมาตร (asymmetric cryptosystems) โดยมีอธิบายการทำงานของแต่ละกลไกได้ดังนี้ *1) SchedElG* เป็นแผนการจัดการเวลาแบบรวมศูนย์การรักษาความเป็นส่วนตัวที่อยู่บนพื้นฐานของระบบการเข้ารหัสลับ ElGamal โดยความปลอดภัยของการเข้ารหัส ElGamal ขึ้นอยู่กับปัญหาลอการิทึมที่ไม่ต่อเนื่อง (Discrete Logarithm Problem (DLP)) ที่ควบคุมและจัดการได้ยาก ซึ่งโปรโตคอล *SchedElG* ได้ใช้คุณสมบัติ Homomorphic ของการเข้ารหัสลับ ElGamal เพื่อให้เซิร์ฟเวอร์การจัดการเวลาทำการคำนวณผลรวมความพร้อมการใช้งานโดยการทำงานเฉพาะในแต่ละตารางเวลาการเข้ารหัส เช่น โปรโตคอลนี้สามารถตรวจสอบได้ว่าแบบแผน ElGamal นั้นตอบสนองความต้องการ *2) SchedPa algorithm* อยู่บนพื้นฐานของระบบการเข้ารหัสลับ Paillier โดยความปลอดภัยของการเข้ารหัส Paillier ขึ้นอยู่กับการตัดสินใจที่จัดการได้ยาก โปรโตคอลนี้ใช้คุณสมบัติ Homomorphic ของการเข้ารหัสลับ Paillier เพื่อคำนวณในการรักษาความเป็นส่วนตัวทำให้มีอยู่ในรูปสภาพพร้อมใช้งานของผู้ใช้ทุกคนที่เกี่ยวข้องกับกระบวนการการจัดการเวลา *3) SchedGM algorithm* อยู่บนพื้นฐานของระบบการเข้ารหัสลับ Goldwasser–Micali (GM) ซึ่งความปลอดภัยขึ้นอยู่กับการควบคุมได้ยากของปัญหา Quadratic residuosity

ในส่วนของการนำขั้นตอนวิธีการกำหนดเวลาของการรักษาความเป็นส่วนตัวทั้งสามรูปแบบไปทำงานกับระบบจริงบนแอพพลิเคชั่น ซึ่งจะวัดประสิทธิภาพทั้งฝั่งอุปกรณ์ไคลแอนต์และเซิร์ฟเวอร์ โดยแอพพลิเคชั่นฝั่งไคลแอนต์จะทำงานบนโทรศัพท์มือถือรุ่น Nokia N810 และมีส่วนของการโต้ตอบโดยการกรอกข้อมูลจากผู้ใช้ ส่วนฝั่งเซิร์ฟเวอร์จะทำงานบน Intel-based PC และจัดการผ่าน UNIX console

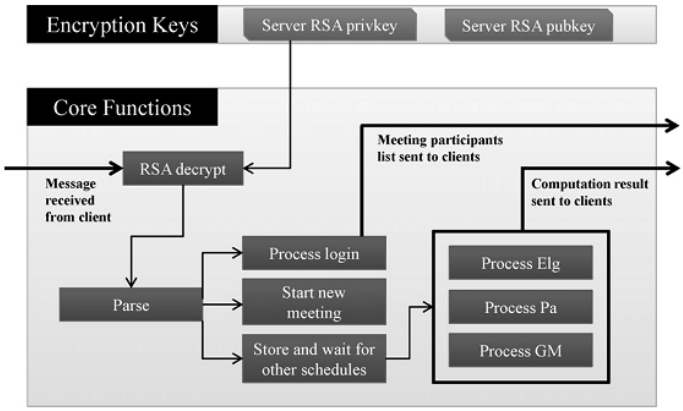
แอพพลิเคชั่นฝั่งไคลแอนต์จัดเก็บตารางเวลาของผู้ใช้และแสดงรายการของผู้เข้าร่วมการประชุมที่มีศักยภาพสำหรับผู้ใช้แต่ละคน โดยรายการนี้ได้รับการดู-แลและจัดการโดยผู้ใช้เองที่สามารถเลือกผู้เข้าร่วมการประชุมก่อนที่จะเริ่มขั้นตอนการตั้งเวลาการประชุม ผู้ใช้แต่ละคนสามารถใช้ GUI เพื่อกำหนดความพร้อมใช้งาน ส่งคำร้องขอกำหนดตารางการประชุม ตอบกลับการร้องขอการประชุมอย่างต่อเนื่อง หรือปฏิเสธที่จะมีส่วนร่วมในการร้องขอการประชุมที่ได้รับ โดยการส่งคำขอการจัดตารางเวลาการประชุม เริ่มแรกผู้ใช้จะต้องเลือกขั้นตอนวิธีการรักษาความเป็นส่วนตัวที่มีอยู่ (SchedElG, SchedPa หรือ SchedGM) และเลือกผู้เข้าร่วมการประชุม จากนั้นการดำเนินงานจะเริ่มโดยการคลิกที่ปุ่ม 'Start meeting' ดังรูปที่ 3 แสดงแผนผังของแอพพลิเคชั่นบนอุปกรณ์ไคลแอนต์ เมื่อผู้ใช้ร้องขอกำหนดตารางการประชุม



รูปที่ 3 แสดงแผนผังของแอพพลิเคชั่นบนอุปกรณ์ไคลแอนต์ เมื่อผู้ใช้ร้องขอกำหนดตารางการประชุม

ส่วนฝั่งเซิร์ฟเวอร์เป็นแอพพลิเคชั่นที่มี GUI น้อย โดยมีการโต้ตอบกับไคลแอนต์เพื่อจัดการคำร้องขอ เช่น การเข้าสู่ระบบ และการคำนวณของความพร้อมใช้งานทั่วไป เซิร์ฟเวอร์ระดับหลัก ScServer แล้วรับช่วงต่อจาก QTcpServer และใช้เป็นซ็อกเก็ตเซิร์ฟเวอร์ ดังรูปที่ 4 แสดงโครงสร้างโฟล์วชาร์ตฝั่งเซิร์ฟเวอร์ โดยโครงสร้างภายในของเซิร์ฟเวอร์จะให้บริการแก่สาธารณะร่วมกับซอร์สโค้ดภายใต้ใบอนุญาต GPL

จากการทดสอบประสิทธิภาพ SchedElG and SchedPa protocols มีประสิทธิภาพมากที่สุด ทั้งสองโปรโตคอลมีการสื่อสารอยู่ในรูปของ *O(m)* โดยที่ m = จำนวนของ time slots และ O(m) มีการคำนวณที่ซับซ้อน นอกจากนี้ทั้งสองขั้นตอนวิธีมีการให้หลักประกันความเป็นส่วนตัวที่น่าเชื่อถือ แต่ SchedGM กลับมีประสิทธิภาพน้อยกว่า เนื่องจากข้อความแลกเปลี่ยนที่มีจำนวนมากขึ้น (O(N·m) โดยที่ N คือ จำนวนของผู้เข้าร่วม) จากมุมมองของ



รูปที่ 4 แสดงโครงสร้างโฟล์วชาร์ตฝั่งเซิร์ฟเวอร์

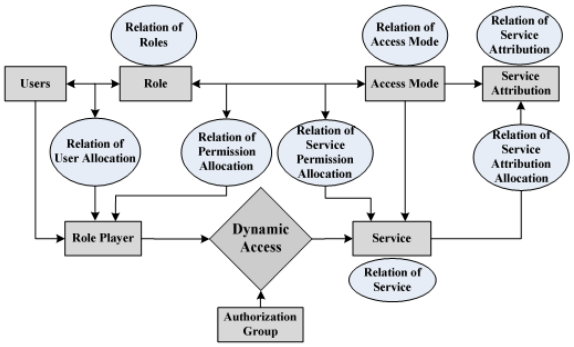
ความของเป็นส่วนตัว SchedGM แสดงให้เห็นถึงข้อมูลเพิ่มเติม คือ ผู้ใช้สามารถสรุปอัตราส่วนของผู้เข้าร่วมได้ว่าว่างหรือไม่ว่าง สำหรับแต่ละ time

slot โดยไม่มีการระบุผู้ที่ไม่ว่างและผู้ที่ว่างเพราะในแบบแผนทั้งหมดเซิร์ฟเวอร์จะดำเนินการเฉพาะข้อมูลที่เข้ารหัส จะไม่สามารถรับรู้ถึงข้อมูลใดๆ เกี่ยวกับตารางเวลาส่วนตัวของผู้ใช้ และเมื่อนำมาเปรียบเทียบกับวิธี Distributed และ Hybrid ผลที่ได้คือวิธี Distributed และ Hybrid มีประสิทธิภาพน้อยกว่าในมุมมองของการสื่อสาร แต่ก็มีประสิทธิภาพสูงกว่าในเรื่องของการคำนวณที่มีความซับซ้อน

B. Cloud Security Service Providing Schemes Based on Mobile Internet Framework [4]

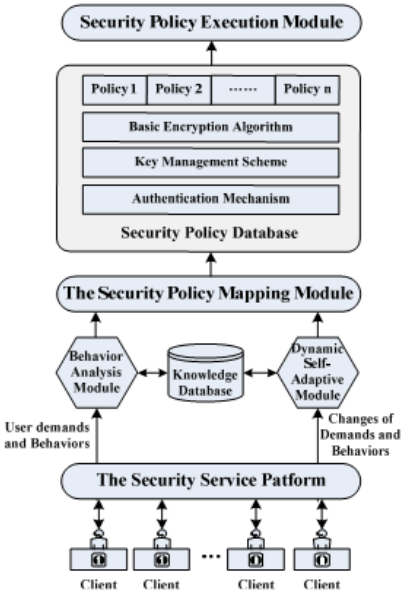
งานวิจัยนี้นำเสนอรูปแบบการให้บริการความปลอดภัย 3 รูปแบบด้วยกัน:

1) โมเดลการควบคุมการเข้าถึงการให้บริการของระบบคลาวด์ ที่สนับสนุนการเปลี่ยนแปลงของการอนุญาตแบบไดนามิก ดังรูปที่ 5 เพื่อป้องกันการเข้าถึงข้อมูลจากผู้ใช้ที่ไม่ได้รับอนุญาต เมื่อผู้ใช้เริ่มปฏิบัติงาน สถานะ พฤติกรรม และอายุการใช้งานของบทบาทที่มีชีวิตได้รับการควบคุมดูแลโดยผู้เล่นที่มีบทบาท นอกจากนี้โมเดลนี้ได้แยกการควบคุมการเข้าถึงออกเป็นสองระดับ คือ ระดับการบริการจะรับประกันเฉพาะผู้ใช้ที่ได้รับอนุญาตสามารถเรียกใช้บริการได้ และระดับความเป็นเจ้าของบริการและข้อมูลซึ่งจะถูกเข้าถึงได้เมื่อผู้ใช้ที่มีสิทธิ์ผ่านเข้ามาระดับการให้บริการได้สำเร็จแล้ว



รูปที่ 5 โมเดลควบคุมการเข้าถึงตามบทบาทระดับชั้นแบบไดนามิก

และ 2) กลไกการดัดแปลงความปลอดภัยด้วยตนเองสำหรับการให้บริการบนระบบคลาวด์ ดังรูปที่ 6 ซึ่งจะกำหนดปรับเปลี่ยนความปลอดภัยด้วยตนเองเป็นการรวมชุดของวิธีการรักษาความปลอดภัยแบบดั้งเดิม การตรวจหาช่องโหว่ และการตอบสนองการบุกรุกไว้ โดยโมเดลนี้จะตรวจสอบและวิเคราะห์พฤติกรรมการใช้งานของผู้ใช้และการเปลี่ยนแปลงความต้องการอย่างต่อเนื่องและจากนั้นจะใช้มาตรการการป้องกันที่เหมาะสม หลักการทำงานของโมเดลนี้ มีดังนี้ ประการแรกระบบบริการมีการโต้ตอบกับผู้ใช้ผ่านแพลตฟอร์มบริการความปลอดภัย ขณะเดียวกันก็ตรวจพบพฤติกรรมของผู้ใช้ในเวลาที่เหมาะสม พร้อมกับเก็บความต้องการของผู้ใช้และการเปลี่ยนแปลงของพฤติกรรมและพารามิเตอร์สภาพแวดล้อมอื่นๆ ประการที่สองข้อมูลข้างต้นจะถูกส่งไปโมดูลการวิเคราะห์พฤติกรรมหรือโมดูลการปรับด้วยตนเองแบบไดนามิกที่มีการอ้างอิงจากข้อมูลที่เกี่ยวข้องในฐานข้อมูล สองโมดูลนี้จะเริ่มกระทำการจับคู่คุณลักษณะ การประเมินรูปแบบ สถานะ ความต้องการความปลอดภัยของการให้บริการในปัจจุบันและการเปลี่ยนแปลงด้วยตนเอง แล้วพิจารณาอิทธิพลที่การร้องขอเซสชั่นที่มีต่อการทำงานของระบบตามด้วยการประเมินผลการปรับด้วยตนเองของระดับความปลอดภัยของระบบ ต่อไปโมดูลการแมพนโยบายความปลอดภัยจะให้ผลการประเมินและจากนั้นจะแมพผลเหล่านี้ไปยังนโยบายความปลอดภัยที่เฉพาะเจาะจง ซึ่งจะได้รับในฐานข้อมูลนโยบายความปลอดภัย หลังจากการรวมและการประเมินผลระบบได้รับการป้องกันความปลอดภัยที่ดีที่สุดให้สอดคล้องกับสถานะของบริการในปัจจุบัน ประการสุดท้ายโมดูลการดำเนินการนโยบายความปลอดภัยจะดำเนินมาตรการการป้องกันขึ้นอยู่กับความต้องการของนโยบาย การปรับการพิสูจน์ตัวตนด้วยตนเอง การกำหนดมาตรการการป้องกันตามความต้องการนโยบายของผู้ใช้ การตั้งคีย์ การเข้ารหัส และการกำหนดสิทธิในการเข้าถึงบริการ



รูปที่ 6 กลไกการดัดแปลงความปลอดภัยด้วยตนเองสำหรับการให้บริการบนระบบคลาวด์

C. Efficient audit service outsourcing for data integrity in clouds [5]

หน่วยจัดเก็บข้อมูลภายนอกอย่างคลาวด์ช่วยลดภาระของลูกค้าสำหรับการจัดการการจัดเก็บและการบำรุงรักษาโดยมีค่าใช้จ่ายที่ถูกและปรับขยายขนาดการจัดเก็บได้ และมีแพลตฟอร์มที่อิสระต่อกันกับสถานที่ เพื่อหลีกเลี่ยงความเสี่ยงของความปลอดภัย จึงให้ความสำคัญกับบริการการตรวจสอบเพื่อมั่นใจได้ว่าข้อมูลจากภายนอกมีความสมบูรณ์และมีสภาพพร้อมใช้งานและเพื่อให้บรรลุการพิสูจน์หลักฐานแบบดิจิตอลและความน่าเชื่อถือของการประมวลผลบนคลาวด์ การพิสูจน์ความเป็นเจ้าของของข้อมูล (Provable data possession (PDP)) ซึ่งเป็นเทคนิคการเข้ารหัสลับสำหรับการยืนยันความถูกต้องความสมบูรณ์ของข้อมูลที่ปราศจากการเรียกข้อมูลคืนมาที่เซิร์ฟเวอร์ที่ไม่น่าเชื่อถือและสามารถนำมาใช้ทำให้การบริการการตรวจสอบเป็นจริงได้

งานวิจัยนี้ได้สร้างรูปแบบการตรวจสอบซึ่งเกี่ยวข้องกับ 3 ขั้นตอนวิธี ดังในรูปที่ 7 คือ การสร้าง key (*KeyGen* (1^s)) การสร้าง tag (*TagGen (sk,F)*) และโปรโตคอลการตรวจสอบ (*Proof(CSP,TPA)*) ในขั้นตอนวิธีการสร้าง key ในแต่ละไคลแอนท์จะได้รับกุญแจลับ *sk* ที่สามารถใช้สร้าง tag ของไฟล์จำนวนมาก และกุญแจสาธารณะ *pk* สามารถนำไปใช้ตรวจสอบความสมบูรณ์ของไฟล์ที่จัดเก็บไว้ได้ โปรโตคอลการตรวจสอบมีโครงสร้าง 3 การแลกเปลี่ยน ดังรูปที่ 8 คือ ความรับผิดชอบ (commitment) การร้องขอ (challenge) และการตอบสนอง (response) โดยมีการนำคุณสมบัติของ zero-

knowledge proof system มาใช้ทำให้กระบวนการการตรวจสอบไม่มีการเปิดเผยข้อมูลอื่นนอกจากความถูกต้องของคำสั่งของความสมบูรณ์ของข้อมูลในคลาวด์ส่วนบุคคล

KeyGen(1^κ): Let $\mathbb{S} = (p, \mathbb{G}, \mathbb{G}_T, e)$ be a bilinear map group system with randomly selected generators $g, h \in_R \mathbb{G}$, where $\mathbb{G}$, $\mathbb{G}_T$ are two group of large prime order p, $|p| = O(\kappa)$. Generate a collision-resistant hash function $H_k(\cdot)$ and chooses a random $\alpha, \beta \in_R \mathbb{Z}_p$ and computes $H_1 = h^\alpha$ and $H_2 = h^\beta \in \mathbb{G}$. Thus, the secret key is $sk = (\alpha, \beta)$ and the public key is $pk = (g, h, H_1, H_2)$.

TagGen(sk, F): Splits the file F into $n \times s$ sectors $F = \{m_{i,j}\} \in \mathbb{Z}_p^{n \times s}$. Chooses s random $\tau_1, \cdots, \tau_s \in \mathbb{Z}_p$ as the secret of this file and computes $u_i = g^{\tau_i} \in \mathbb{G}$ for $i \in [1, s]$ and $\xi^{(1)} = H_\xi(\text{"}Fn\text{"})$, where $\xi = \sum_{i=1}^{s} \tau_i$ and Fn is the file name. Builds an index table $\chi = \{\chi_i\}_{i=1}^{n}$, then calculates its tag as

$$\sigma_i \leftarrow (\xi_i^{(2)})^\alpha \cdot g^{\sum_{j=1}^{s} \tau_j m_{i,j} \beta} \in \mathbb{G}.$$

where $\xi_i^{(2)} = H_{\xi^{(1)}}(\chi_i)$ and $i \in [1, n]$. Finally, sets $u = (\xi^{(1)}, u_1, \cdots, u_s)$ and outputs $\zeta = (\tau_1, \cdots, \tau_s)$, $\psi = (u, \chi)$ to TTP, and $\sigma = (\sigma_1, \cdots, \sigma_n)$ to CSP.

Proof(CSP, TPA): This is a 3-move protocol between CSP and TPA with the common input (pk, ψ), as follows:

- **Commitment**($CSP \rightarrow TPA$): CSP chooses a random $\gamma \in \mathbb{Z}_p$ and s random $\lambda_j \in_R \mathbb{Z}_p$ for $j \in [1, s]$, and sends its commitment $C = (H_1', \pi)$ to TPA, where $H_1' = H_1^\gamma$ and $\pi \leftarrow e(\prod_{j=1}^{s} u_j^{\lambda_j}, H_2)$;
- **Challenge**($CSP \leftarrow TPA$): TPA chooses a random challenge set I of t indexes along with t random coefficients $v_i \in \mathbb{Z}_p$. Let Q be the set $\{(i, v_i)\}_{i \in I}$ of challenge index coefficient pairs. TPA sends Q to CSP;
- **Response**($CSP \rightarrow TPA$): CSP calculates the response θ, μ as

$$\begin{cases} \sigma' \leftarrow \prod_{(i,v_i) \in Q} \sigma_i^{\gamma \cdot v_i}, \\ \mu_j \leftarrow \lambda_j + \gamma \cdot \sum_{(i,v_i) \in Q} v_i \cdot m_{i,j}, \end{cases}$$

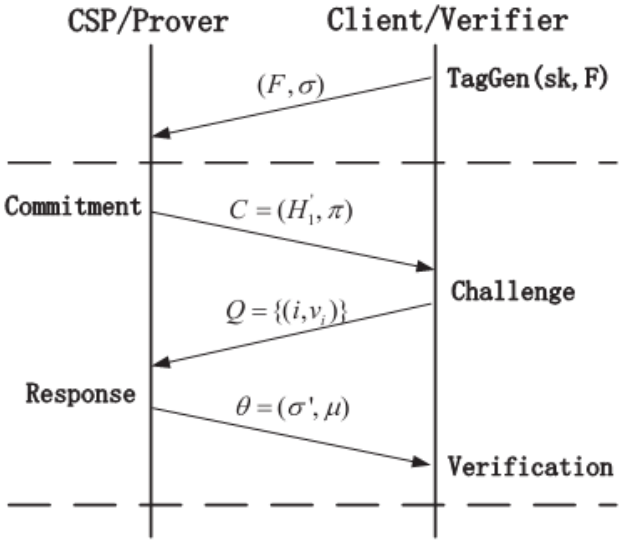
where $\mu = \{\mu_j\}_{j \in [1,s]}$. P sends $\theta = (\sigma', \mu)$ to V;

Verification: TPA can check that the response was correctly formed by checking that

$$\pi \cdot e(\sigma', h) \stackrel{?}{=} e(\prod_{(i,v_i) \in Q} (\xi_i^{(2)})^{v_i}, H_1') \cdot e(\prod_{j=1}^{s} u_j^{\mu_j}, H_2).$$

รูปที่ 7 แสดงโปรโตคอลตรวจสอบการโต้ตอบ

ได้สร้างบริการการตรวจสอบความสมบูรณ์ของข้อมูลบนคลาวด์ได้อย่างมีประสิทธิภาพ ได้ประโยชน์จากระบบพิสูจน์หลักฐานการโต้ตอบที่มีมาตรฐาน ซึ่งโปรโตคอลการตรวจสอบการโต้ตอบได้นำไปใช้บริการการตรวจสอบกับผู้ตรวจสอบของบุคคลที่สาม บริการนี้ผู้ตรวจสอบของบุคคลที่สามเป็นที่รู้จักกันดี ในฐานะที่เป็นตัวแทนของเจ้าของข้อมูล สามารถตรวจสอบเป็นระยะๆ เพื่อติดตามการเปลี่ยน แปลงของข้อมูลจากภายนอกโดยการให้ตารางที่ดีที่สุดเพื่อทำให้โมเดลการตรวจสอบใช้ได้จริงจะต้องมีการบำรุงรักษาความปลอดภัยให้กับผู้ตรวจสอบของบุคคลที่สามและปรับใช้ดีมอนเพื่อปฏิบัติการโปรโตคอลพิสูจน์ความจริง ดังนั้นเทคโนโลยีนี้สามารถนำมาใช้ในระบบการประมวลผลบนคลาวด์ได้อย่างสะดวกแทนที่วิธีแฮชตามแบบดั้งเดิม วิธีการนี้จะช่วยลดภาระในการทำงานบนเซิร์ฟเวอร์จัดเก็บข้อมูลได้ระยะเวลาหนึ่ง แม้ว่าจะสำเร็จในการตรวจพบพฤติกรรมที่ไม่เหมาะสมของเซิร์ฟเวอร์ซึ่งมีโอกาสที่จะเป็นไปได้สูง การทดสอบแสดงให้เห็นว่าวิธีการนี้สามารถลดการคำนวณและค่าใช้จ่ายในการติดต่อสื่อสารให้เหลือน้อยที่สุดได้



รูปที่ 8 กรอบแบบแผนตรวจสอบการโต้ตอบ

D. Improving the Capacity, Reliability & Life of Mobile Devices with Cloud Computing [6]

โมเดลที่เสนอมีจุดประสงค์ที่จะกล่าวถึง การคำนวณ (Computational) การจัดเก็บข้อมูล (Storage) และการรักษาความปลอดภัย (Security) สำหรับแอพพลิเคชั่นบนอุปกรณ์เคลื่อนที่ บางบริการของ CSS จะให้บริการด้วย Secure Multimedia Health Services (SMHS) ซึ่งอธิบายโดยสังเขปได้ดังนี้

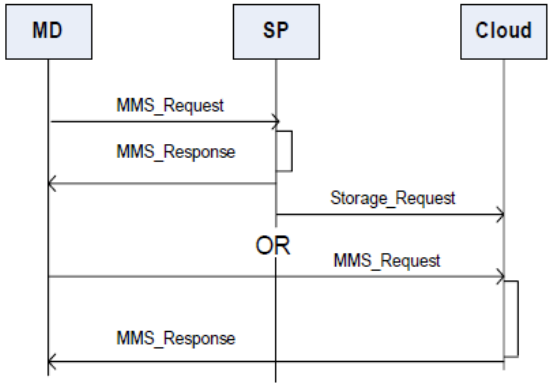
- *สภาพแวดล้อมการประมวลผลซอฟต์แวร์ที่ปลอดภัย*: การประมวลผลด้วยสัญญาณเซ็นเซอร์มัลติมีเดีย สำหรับการประมวลผลข้อมูลทางกายภาพอย่างถูกต้อง ในสภาพแวดล้อมการประมวลผลซอฟต์แวร์ที่ปลอดภัย
- *การสื่อสารข้อมูลที่ปลอดภัย*: ช่องทางการสื่อสารไร้สายจะต้องมีความเป็นส่วนตัว และข้อมูลที่สื่อสารต้องมั่นคงปลอดภัยจากการใช้แอพพลิเคชั่นบนอุปกรณ์เคลื่อนที่
- *การแสดงตัวผู้ใช้*: การตรวจสอบและป้องกันการเข้าถึงของผู้ใช้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูลและแอพพลิเคชั่นบนอุปกรณ์เคลื่อนที่
- *การเข้าถึงเครือข่ายที่ปลอดภัย*: เฉพาะสมาชิกที่ลงทะเบียนแล้วเพื่อรับบริการสุขภาพบนอุปกรณ์เคลื่อนที่จะสามารถเชื่อมต่อกับเครือข่ายสุขภาพและเข้าถึงบริการได้
- *การรักษาความปลอดภัยของเนื้อหา*: เนื้อหาจากอุปกรณ์เคลื่อนที่ต้องสามารถนำมาใช้เป็นเงื่อนไขที่กำหนดโดยผู้ให้บริการได้
- *การจัดเก็บที่ปลอดภัย*: เพื่อรับประกันความปลอดภัยและความเป็นส่วนตัวของข้อมูลด้านสุขภาพที่สำคัญ จึงต้องมีการการจัดเก็บอย่างปลอดภัยบนเซิร์ฟเวอร์ นอกจากนี้ เพื่อป้องกันการโจรกรรมและการสูญหายของข้อมูล

จึงต้องมีการให้บริการเก็บสำรองข้อมูลอย่างปลอดภัยโดยหน่วยจัดการบริการสุขภาพบนคลาวด์

แนวคิดพื้นฐานของรูปแบบบริการนี้คือ การประมวลผลสัญญาณมัลติมีเดียที่แรงและหนักจะต้องใช้พลังงานเพิ่มขึ้นเพื่อให้สามารถดำเนินการบนอุปกรณ์เคลื่อนที่ได้ เพื่อป้องกันพลังงานนี้ไหลออก วิธีการที่เสนอจะอัพโหลดอัลกอริทึมแบบที่ซับซ้อนกว่าเพื่อดำเนินการบนคลาวด์และผลลัพธ์สุดท้ายจะอัพโหลดกลับไปที่อุปกรณ์เคลื่อนที่ จึงแบ่งกลุ่มกลไกบริการที่จำเป็นเป็นแบบกลุ่มที่เป็นจุดแข็งและจุดอ่อน

ในส่วนนี้จะเป็นตัวอย่างการร้องขอบริการจากคลาวด์และแผนภาพเวลาในการตอบรับของบริการ เมื่อ Mobile Station (MS) ร้องขอบริการคลาวด์ กระบวนทัศน์ปัจจุบันของเครือข่ายไร้สายคือจะขอผ่านโหนดผู้ให้บริการ การตรวจสอบการรักษาความปลอดภัยจะต้องทำการตรวจสอบ MS สำหรับบริการที่ร้องขอมา สมมติว่าในกรณีนี้โทรศัพท์มือถือ MS ร้องขอการประมวลผลซอฟต์แวร์รักษาความปลอดภัยของสัญญาณเซ็นเซอร์มัลติมีเดีย ผู้ให้บริการจะดำเนินการการประเมินความต้องการแบนด์วิดธ์ และ QoS สัญญาณเซ็นเซอร์จะย้ายไปยังคลาวด์เพื่อการประมวลผลสัญญาณ ข้อมูลทางกายภาพที่แยกส่วนแล้วจะถูกส่งไปยังเซิร์ฟเวอร์แอพพลิเคชั่นของผู้บริการ เพื่อวิเคราะห์และตัดสินใจ สิ่งนี้จะช่วยเก็บพลังงานของ MS และขยายขีดความสามารถของอุปกรณ์เคลื่อนที่สำหรับแอพพลิเคชั่นที่สำคัญอื่นๆ ดังรูปที่ 9 แสดงการโต้ตอบและตารางเวลาของกระบวนการระหว่างกลุ่มที่ให้บริการการรักษาความปลอดภัยบนอุปกรณ์เคลื่อนที่ที่อยู่บนคลาวด์ องค์ประกอบคลาวด์ของรูปแบบการปฏิสัมพันธ์สามารถเป็นศูนย์กลางข้อมูลที่มีความสามารถในการคำนวณสูง

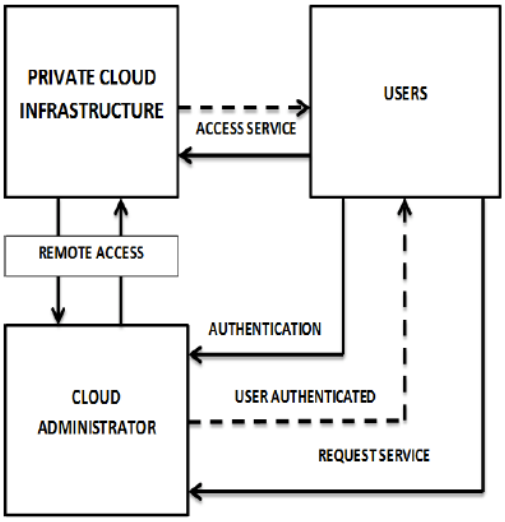
1) ผู้ใช้อุปกรณ์มือถือ (MD) เริ่มต้นการสื่อสารโดยการร้องขอบริการจากผู้ให้บริการ (SP)
2) SP ตรวจสอบสิทธิและส่งข้อความตอบรับไปยัง MD ด้วยค่า QoS ที่ใช้ได้ (แบนด์วิดธ์, บริการแบบเรียลไทม์หรือไม่เรียลไทม์)
3) ขึ้นอยู่กับ QoS ที่ใช้ได้ , MD ที่ขอบริการ มีสองวิธีคือ ทำสำเนาของ MD ในคลาวด์ หรือเชื่อมต่อกับคลาวด์เพื่อบริการออนไลน์
4) ขึ้นอยู่กับชนิดของการร้องขอบริการโดย MD, SP ร้องขอการเชื่อมโยงไปยังคลาวด์โดยตรงจาก MD, การประมวลผลที่ร้องขอแล้วจะส่งต่อไปยังคลาวด์เพื่อดำเนินการต่อไป



รูปที่ 9 ไดอะแกรมการจัดตารางเวลาของการบริการคลาวด์

วิธีที่แตกต่างสามารถดำเนินการระหว่าง Service Provider (SP) และ การร้องขอบริการอุปกรณ์เคลื่อนที่จาก MDs ได้ ตัวแบบระหว่าง SP และ CHMS cloud จะแลกเปลี่ยนกันเพื่อส่งเสริมหน่วยจัดเก็บสำรองที่ปลอดภัย และเหมืองข้อมูลและการวิเคราะห์ข้อมูลบนอุปกรณ์เคลื่อนที่สำหรับการโฆษณา

E. Secure Private Cloud Architecture for Mobile Infrastructure as a Service [7]



รูปที่ 10 สถาปัตยกรรมระดับสูงของระบบ

จากรูปที่ 10 แสดงสถาปัตยกรรมระดับสูงของระบบที่งานวิจัยนี้นำเสนอ ซึ่งประกอบด้วยผู้ใช้ โครงสร้างพื้นฐานของคลาวด์ และผู้ดูแลระบบคลาวด์ ผู้ดูแลระบบคลาวด์ หมายถึง บุคคลหรือกลุ่มบุคคลที่รับผิดชอบในการจัดการโครงสร้างพื้นฐานและให้บริการการร้องขอของผู้ใช้ ผู้ใช้ต้องตรวจสอบตัวตนเพื่อยืนยันกับผู้ดูแลระบบคลาวด์ โครงสร้างพื้นฐานคลาวด์หมายถึงชุดการตั้งค่าคอมพิวเตอร์ที่จะให้บริการคลาวด์แก่ผู้ใช้ตามข้อกำหนดต่างๆ เมื่อใดก็ตามที่มีการร้องขอทรัพยากร ผู้ดูแลระบบคลาวด์จะให้ระบบเสมือนขององค์ประกอบที่กำหนดผ่านทางโครงสร้างพื้นฐานคลาวด์ ระบบเสมือนทำงานในหนึ่งคอมพิวเตอร์ของโครงสร้างพื้นฐานคลาวด์ จากนั้นผู้ใช้สามารถเข้าถึงเครื่องเสมือนทั้งผ่านเดสก์ทอปและอุปกรณ์เคลื่อนที่

ส่วนแสดงผลสำหรับผู้เข้าชมจะทำหน้าที่เป็นผู้ดูแลระบบและเก็บข้อมูลบัญชีเกี่ยวกับเครื่องจักรเสมือนและการเข้าถึงเครื่องจักรเสมือนของผู้ใช้ มันจะเก็บไฟล์ติดตั้งที่จำเป็นซึ่งจะให้บริการกับกลุ่มโหนดผ่านทางการแชร์ไฟล์ กลุ่มคือคอมพิวเตอร์ซึ่งเป็นเครื่องจักรเสมือน ดังนั้นกลุ่มโหนดควรจะมีเทคนิคเสมือนต่างๆเปิดใช้งานอยู่ ภาพของระบบปฏิบัติการที่ถูกร้องขอโดยเครื่องจักรเสมือนจะถูกเก็บในพื้นที่เก็บข้อมูลภาพ กระบวนการทำงานของระบบของเราอธิบายในขั้นตอนต่อไปนี้

1) การพิสูจน์ตัวตน : ผู้ใช้ต้องพิสูจน์ตัวตนให้แก่ผู้ดูแลระบบคลาวด์
2) ร้องขอ : จากนั้นผู้ใช้ให้ข้อกำหนดในรูปแบบดังนี้ < Operating system, Memory, Hard Disk, Processor, Software >
3) เมื่อลูกข่ายส่งข้อกำหนดแล้ว ผู้ดูแลคลาวด์จะสร้างเทมเพลทสำหรับเครื่องเสมือน จากนั้นเครือข่ายเสมือนจะถูกสร้างขึ้น และผู้ดูแลคลาวด์ก็จะกระจายคำสั่งเครื่องเสมือนที่สร้างขึ้นนั้น
4) จากนั้นส่วนแสดงผลผู้ใช้จะรันอัลกอริทึมตารางงานและเลือกกลุ่มที่เหมาะสมที่สามารถทำหน้าที่เป็นเครื่องเสมือนของการตั้งค่าที่จำเป็นได้

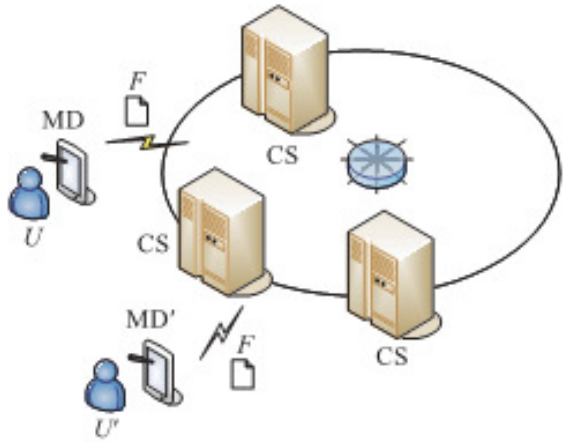
5) รูปแบบระบบปฏิบัติการที่ถูกร้องขอจะถูกเลือกจากแหล่งเก็บข้อมูลและคัดลอกไปยังกลุ่ม
6) จากนั้น hypervisor (ซอฟต์แวร์ที่ทำหน้าที่จัดสรรทรัพยากรให้เครื่องเสมือน : Virtual Machine Monitor) จะเสนอกลุ่มสัญญาณที่จะนำไปปรับใช้กับ VM
7) VM จะเข้าสู่สถานะการทำงานหลังจากเซตอัพตัวเชื่อมโยงเครือข่ายแล้ว เพื่อให้ NIC เสมือนกับ MAC เสมือน

F. Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing [8]

ในสถานการณ์ทั่วไปของ Mobile Cloud Computing (MCC) งานวิจัยนี้ระบุสามการดำเนินการดังนี้ (1) MD: Mobile Device (อุปกรณ์เคลื่อนที่) เป็นอุปกรณ์ที่ครบครันด้านความสามารถ เช่น การประมวลผล การจัดเก็บและการสื่อสารแบบไร้สาย ตัวอย่างเช่น สมาร์ทโฟน แท็บเล็ต PC หรือเซ็นเซอร์ไร้สาย (2) CS: Cloud Server (คลาวด์เซิร์ฟเวอร์) คือผู้ให้บริการในการประมวลผลคลาวด์ ซึ่งมักจะมีการจัดเก็บหรือบริการประมวลผล ในบทความนี้จะพิจารณาเฉพาะบริการจัดเก็บเท่านั้น สามารถแบ่งออกเป็นสองประเภท คือ เว็บไซต์ท่า CS และ เบื้องหลัง CS เมื่อก่อนมีการเข้าโดยตรงจาก MD ภายหลังมีการเข้าถึงโดยเว็บไซต์ท่า CS (3) U: ผู้ใช้ เป็นคนที่จัดการกับ MD ผู้ใช้หลายคนอาจจะมีคนที่ต้องการเข้าถึงไฟล์หรือข้อมูลเดียวกันใน CS วัตถุที่ดำเนินการคือไฟล์หรือข้อมูล แสดงด้วย F ซึ่งหมายถึงไฟล์ที่อัพโหลด (ดาวน์โหลด) ไปยัง CS สองรูปแบบการดำเนินการแบบพื้นฐานมีดังนี้

1) บริการในรูปการจัดเก็บ CS ทำงานเป็นผู้ให้บริการการจัดเก็บ F ถูกสร้างขึ้นและดำเนินการที่ MD U อัพโหลด F ไปยัง CS เมื่อกู้คืนไฟล์F U จะดาวน์โหลด F จาก CS U อาจจะแก้ไข F ภายในและอัพเดท F จากระยะไกลโดยการอัพโหลดเวอร์ชั่นแก้ไขไปยัง CS
2) บริการในรูปแบบการประมวลผล CS ทำงานเป็นแพลตฟอร์มประมวลผล F ถูกสร้างที่ CS และดำเนินการที่ CS

หลังจากที่กล่าวถึงรูปแบบการดำเนินการไปแล้ว ต่อไป CS จะต้องเชื่อถือได้อย่างเต็มที่ ดังนั้นปัญหาด้านการรักษาความปลอดภัยจึงเป็นปัญหาเล็กน้อย ดังรูปที่ 11 แสดงให้เห็นสิ่งที่เกี่ยวข้องใน MCC



รูปที่ 11 เอนทิตี้ในการประมวลผลแบบคลาวด์บนอุปกรณ์เคลื่อนที่

บทความนี้ถือว่าเป็น MD ที่เชื่อถือได้บางส่วน (เข้าถึงได้จากทั้งภายในและภายนอก) การประมวลผลใน MD เป็นที่เชื่อถือ ซึ่งมักจะเป็นการยากสำหรับการโจมตีเพื่อเปลี่ยนโค้ดการดำเนินการในฟังก์ชั่นที่ถูกติดตั้งไว้ ส่วนหน่วยจัดเก็บใน MD ยังไม่น่าไว้ใจ เนื่องจากผู้โจมตีอาจจะขโมยข้อมูลบางอย่างใน MD ด้วยการติดตั้งซอฟต์แวร์ที่เป็นอันตราย หรือ MD อาจจะหายไปโดยบังเอิญและสิ่งที่จัดเก็บทั้งหมดก็จะถูกเปิดเผย โดยสรุปแล้ว เราถือว่า MD นี้คุณสมบัติเป็นไปตามโครงสร้างที่เสนอ แต่ข้อมูลที่จัดเก็บอาจจะสูญหาย ซึ่งทำให้ความน่าเชื่อถือของ MD ลดน้อยลง CS มีการสันนิษฐานถึงความไม่ปลอดภัยโดยรูปแบบการโจมตีประกอบด้วยการสูญเสียข้อมูลทั้งหมด การผิดปกติในการประมวลผล การปรับเปลี่ยนข้อมูล และข้อมูลมีการรั่วไหล

การเชื่อมต่อระหว่าง MD และเว็บไซต์ท่า CS ประกอบด้วยหนึ่งฮอปหรือมากกว่า ช่องสัญญาณแบบมีสายหรือไร้สาย แต่อย่างไรก็ตาม การรักษาความปลอดภัยของการเชื่อมต่อเช่น ความเป็นส่วนตัวและความสมบูรณ์คือการให้บริการที่แท้จริงโดยโปรโตคอลชั้นการเข้าถึงสื่อ เช่น IEEE 802.11 หรือโปรโตคอลชั้น IP เช่น IPSec ดังนั้น จึงถือว่าการเชื่อมต่อมีความน่าเชื่อถือและพุ่งเป้าไปที่ประเด็นนั้นเป็นหลัก

ในขณะที่เรากำหนดรูปแบบความไว้วางใจอย่างชัดเจน เราสามารถเปรียบเทียบการรักษาความปลอดภัยของรูปแบบที่เสนอเมื่อเป้าหมายการรักษาความปลอดภัยเดียวกันประสบความสำเร็จ นั่นคือ รูปแบบที่เสนอจะต้องมีความปลอดภัยมากขึ้นถ้าสมมติฐานของรูปแบบความไว้วางใจพื้นฐานนั้นมีจุดอ่อน ความต้องการความปลอดภัยที่แท้จริง ในบทความนี้คือความลับของข้อมูลและความสมบูรณ์ข้อมูลของไฟล์ของผู้ใช้ใน MCC ตามรูปแบบความไว้วางใจแบบพื้นฐาน

มีการเสนอกลุ่มของรูปแบบที่จะป้องกันความลับและความสมบูรณ์ของการอัพโหลดไฟล์หรือข้อมูลในหน่วยจัดเก็บข้อมูลบนคลาวด์บนอุปกรณ์เคลื่อนที่ รูปแบบ EnS จะแก้ปัญหาสถานการณ์ที่มีเซิร์ฟเวอร์คลาวด์อยู่แล้วเท่านั้น ได้มีการทดสอบแล้วว่า จะรับประกันเป้าหมายการรักษาความปลอดภัยและเป็นเงื่อนไขที่จำเป็นสำหรับสถานการณ์นี้ รูปแบบ CoS สามารถหลีกเลี่ยงการประมวลผลของอัลกอริทึมเข้ารหัสในสถานการณ์ที่หลายๆ คลาวด์เซิร์ฟเวอร์จบการทำงาน โดยการเข้ารหัสแบบเส้นตรง รูปแบบ ShS สามารถลดค่าใช้จ่ายในการประมวลผลได้มากขึ้นโดยอาศัยการดำเนินการแบบ exclusive-or เท่านั้น รูปแบบที่เสนอทั้งหมดมีความยืดหยุ่นในการจัดเก็บบนอุปกรณ์เคลื่อนที่ และทั้งหมดก็ยอมรับว่าเซิร์ฟเวอร์คลาวด์ไม่น่าไว้วางใจ ดังนั้น จึงมีการให้การป้องกันมากขึ้นสำหรับสถานการณ์ทั่วไปและสถานการณ์จริงเปรียบเทียบกับงานเดิม

จากรูปแบบการบริการการรักษาความปลอดภัยข้างต้น เราจะทำการเปรียบเทียบงานวิจัยที่มีการนำบริการรักษาความปลอดภัยรูปแบบต่างๆ มาใช้ ดังแสดงในตารางที่ 1 และในตารางที่ 2ก, 2ข แสดงให้เห็นถึงเทคนิคที่งานวิจัยใช้ในแต่ละบริการรักษาความปลอดภัยรูปแบบต่างๆ

ตารางที่ 1 แสดงการเปรียบเทียบงานวิจัยที่มีการใช้บริการรักษาความปลอดภัยรูปแบบต่างๆ

Security service / Paper	Authentication service	Authorization service	Confidentiality service	Integrity service	Non-repudiation service	Trust management service	Privacy service	Identity management service	Policy service	Audit service	Availability service
[3]	✓		✓	✓	✓		✓				✓
[4]	✓	✓	✓	✓	✓		✓		✓		
[5]	✓			✓			✓			✓	✓
[6]	✓	✓		✓		✓	✓	✓			
[7]	✓		✓	✓		✓	✓		✓		✓
[8]	✓		✓	✓		✓	✓				

ตารางที่ 2ก แสดงเทคนิคที่งานวิจัยใช้ในแต่ละบริการรักษาความปลอดภัยรูปแบบต่างๆ

Security service	Authentication service	Authorization service	Confidentiality service	Integrity service	Non-repudiation service
[3]	เข้ารหัสด้วยครึ่งหลังของ public key		ความลับในการแชร์ข้อมูลระหว่างเซิร์ฟเวอร์กับผู้ใช้จะใช้เทคนิคขีดแบ่งการเข้ารหัส (Threshold Cryptography) เพื่อป้องกันการบุกรุก	ความสมบูรณ์ของตารางเวลาการเข้ารหัสผู้ใช้ที่อยู่ในระบบที่รู้ข้อมูลลับนั้นจะใช้ในการสร้างคีย์คู่ public key และ private key ดังนั้นผู้ใช้จะเป็นผู้ที่สามารถสร้างและตรวจสอบความสมบูรณ์ของข้อมูลที่เข้ารหัสได้	ใช้คุณสมบัติ homomorphic ของ Asymmetric Cryptosystems
[4]	Security Policy Database: authentication mechanism, เมื่อผู้ใช้ร้องขอใช้บริการคลาวด์ ระบบจะทำการตรวจสอบเป็นอันดับแรกและสอบถามถึงบทบาทของผู้ใช้	ลำดับชั้นแบบไดนามิกตามบทบาท Access control model สนับสนุนการเปลี่ยนแปลงการอนุญาต ช่วยในการกำหนดสิทธิ์ให้กับผู้ใช้และช่วยป้องกันบริการของตนเองและข้อมูลที่บริการ ผู้ใช้ไม่สามารถรับการอนุมัติได้เว้นแต่บทบาทคล้ายคลึงกันถูกเปิดใช้งาน	encryption (หรือ decryption) function	Hash signature function	Hash signature function
[5]	public-key authentication technology คล้ายกับ PDP และ CPOR schemes	-	ใช้ zero-knowledge proof system ทำให้กระบวนการการตรวจสอบไม่มีการเปิดเผยข้อมูลอื่น	Provable data possession (PDP) เป็นเทคนิคCryptographic สำหรับตรวจสอบความสมบูรณ์ของข้อมูล, ใช้ กุญแจสาธารณะ *pk* ตรวจสอบความสมบูรณ์ของไฟล์ที่จัดเก็บไว้	-
[6]	Next Generation Networks (NGN) อยู่บนพื้นฐานของมาตรฐาน IP multimedia subsystem (IMS), 3GPP Generic Authentication Architecture (GAA)	3GPP Generic Authentication Architecture (GAA)	-	Secure multimedia health services (SMHS) โดยใช้เทคนิคของ Secure Data Communication	Security verification ภายในคลาวด์
[7]	ผู้ใช้ต้องพิสูจน์ตัวตนให้แก่ผู้ดูแลระบบคลาวด์	-	ส่วนติดต่อกับผู้ใช้ควรมีการเข้าถึงที่สมบูรณ์ โดยไม่ควรทำให้จำรหัสผ่านของโหนดคลัสเตอร์ได้ในทันทีขณะที่มีการเชื่อมต่อผ่าน SSH	ป้องกันการบุกรุกจากภัยคุกคามอยู่ในรูป VM Hopping	-
[8]	Next generation networks (NGN) สนับสนุนการพิสูจน์ตัวตนบนพื้นฐานมาตรฐานระบบย่อยไอพีมัลติมีเดีย (IMS) ใน Encryption based Scheme (EnS)	-	Encryption based Scheme (EnS) Coding base d Scheme (CoS) จัดการความลับของไฟล์	Encryption based Scheme (EnS)	-

ตารางที่ 2ข แสดงเทคนิคที่งานวิจัยใช้ในแต่ละบริการรักษาความปลอดภัยในรูปแบบต่างๆ

Security service	Trust management service	Privacy service	Identity management service	Policy service	Audit service	Availability service
[3]	Semi-honest adversarial model	เสนอ 3 แนวคิดโปรโตคอลการรักษาความเป็นส่วนตัว SchedElG: ใช้ระบบการเข้ารหัส ElGamal ขึ้นอยู่กับปัญหาลอการิทึมที่ไม่ต่อเนื่อง (DLP) SchedPa: อยู่บนพื้นฐานของระบบการเข้ารหัสลับ Paillier และ SchedGM: อยู่บนพื้นฐานของระบบการเข้ารหัสลับ Goldwasser–Micali (GM)	-	-	-	ใช้การเข้ารหัสลับ ElGamal เพื่อให้เซิร์ฟเวอร์การจัดการเวลาทำการคำนวณผลรวมความพร้อมการใช้งาน, ใช้การเข้ารหัสลับ Paillier เพื่อคำนวณในการรักษาความเป็นส่วนตัว ทำให้มีอยู่ในรูปสภาพพร้อมใช้งานของผู้ใช้ทุกคนที่เกี่ยวข้องกับกระบวนการการจัดการเวลา
[4]	-	ใช้ฟังก์ชั่นEncryption (หรือ Decryption)	-	Security policy execution module ฟังก์ชั่นการจัดการคีย์เพื่อสร้างการรักษาเซสชั่นการเข้ารหัส/ถอดรหัสของคีย์, ตระหนักถึงการบริการความเป็นความลับ, ฟังก์ชั่นลายเซ็นแฮชเพื่อความเป็นintegrity และ non-repudiation	-	-
[5]	-	privacy-preserving public auditing protocol	-	-	เสนอโปรโตคอลตรวจสอบการโต้ตอบเพื่อจัดเตรียมบริการตรวจสอบขึ้นอยู่กับผู้ตรวจสอบบุคคลที่สาม	ใช้บริการการตรวจสอบเพื่อสร้างความมั่นใจในความพร้อมการใช้งานของข้อมูลจากภายนอก
[6]	CSS management model	secure multimedia health services (SMHS), CSS management model	SIM (subscriber identity module)	-	-	-
[7]	ผู้ใช้โต้ตอบด้วยกระบวนการ three-way เมื่อผู้ใช้ล็อกอินเข้าระบบจะสามารถใช้บริการที่จัดหาไว้ให้ได้	secure private cloud architecture for Mobile Infrastructure	-	การสื่อสารของเครือข่ายจะเข้ามาอยู่ในโครงสร้างของคลาวด์ มีการตรวจสอบโดยไฟร์วอลล์เครื่องเสมือนของบางโปรไฟล์จะถูกตั้งค่าให้เป็น VLAN ที่เหมาะสม โดยจะทำให้สะดวกขึ้นของการบังคับใช้นโยบายด้านความปลอดภัยที่สอดคล้องกับโปรไฟล์ของผู้ใช้ที่ต่างกัน สามารถทำได้โดยการติดแท็ก VLAN	-	สถาปัตยกรรมนี้มีสภาพพร้อมใช้งานเนื่องจากมีโครงสร้างพื้นฐานของความเป็นส่วนตัวคลาวด์ (private cloud)
[8]	สร้างโมเดลความไว้วางใจ (Trust model) ให้ระบบ, semi-trust	Media access layer protocol เช่น IEEE 802.11, หรือ IP layer protocols เช่น IPSec	-	-	-	-

ตารางที่ 3 แสดงสรุปข้อดีและข้อจำกัดของการบริการความปลอดภัยในการประมวลผลแบบคลาวด์บนอุปกรณ์เคลื่อนที่ของแต่ละงานวิจัย

งานวิจัย	ข้อดี	ข้อจำกัด
[3]	• มี 3 โปรโตคอลการรักษาความเป็นส่วนตัว (privacy-preserving protocols) ให้เลือกใช้กับแอพพลิเคชั่นมือถือ • ขั้นตอนวิธีการและสถาปัตยกรรมซอฟต์แวร์มีการบูรณาการอย่างต่อเนื่องกับขั้นตอนวิธีการรักษาความเป็นส่วนตัวในวิธีที่ไม่ขัดขวางผู้ใช้ • มีการประมวลผลที่รวดเร็วและมีประสิทธิภาพ อีกทั้งไม่เสียค่าใช้จ่าย • จากการใช้งานบนโทรศัพท์มือถือนั้น มีการหลักประกันความเป็นส่วนตัวที่น่าเชื่อถือและมีประสิทธิภาพในแง่ของการคำนวณและความซับซ้อนของการสื่อสาร • มีการควบคุมการเข้าถึงอย่างมีประสิทธิภาพและการเผยแพร่ข้อมูลส่วนบุคคลมีความแตกต่างอย่างมีนัยสำคัญสำหรับแอพพลิเคชั่นมือถือ	• เมื่อผู้ใช้จะร้องขอการกำหนดตารางการประชุมจะต้องเลือกขั้นตอนวิธีการรักษาความเป็นส่วนตัววิธีใดวิธีหนึ่ง (SchedElG, SchedPa หรือ SchedGM) ก่อนที่จะเริ่มการใช้งาน • เมื่อนำมาเปรียบเทียบกับวิธี Distributed และ Hybrid ผลที่ได้คือวิธี Distributed และ Hybrid มีประสิทธิภาพน้อยกว่าในมุมมองของการสื่อสาร แต่ก็มีประสิทธิภาพสูงกว่าในเรื่องของการคำนวณที่มีความซับซ้อน

งานวิจัย	ข้อดี	ข้อจำกัด
[4]	• โมเดลควบคุมการเข้าถึงจะสามารถเตรียมบริการรักษาความปลอดภัยให้ได้ขึ้นอยู่กับสิทธิ์ของผู้ใช้และปรับเปลี่ยนประเภทบริการตามการเปลี่ยนแปลงที่ได้รับอนุญาต • โมเดลควบคุมการเข้าถึงนั้นจะช่วยในการปกป้องบริการของตัวเองและข้อมูลบริการ ซึ่งจะส่งผลในการเพิ่มประสิทธิภาพของความยืดหยุ่นอย่างเป็นอิสระและช่วยในการขยายการควบคุมการเข้าถึงบริการคลาวด์ • กลไกการปรับตัวด้วยตนเองนั้นช่วยให้ระบบตอบสนองกับสภาพแวดล้อมของปัจจัยที่กำหนดโดยอัตโนมัติและมีการป้องกันที่สอดคล้องกัน ทำให้สามารถปรับปรุงนโยบายด้านความปลอดภัยได้ทันที พร้อมกับมาตรการการป้องกันแบบใหม่ โมเดลแบบไดนามิกนี้มีการปรับตัวด้วยตนเองได้หลากหลายและไม่สามารถคาดการณ์ได้ • ช่วยเพิ่มศักยภาพของระบบ ทำให้มีประสิทธิภาพในการให้บริการ	• โมเดลควบคุมการเข้าถึงนั้นจะสามารถเตรียมบริการรักษาความปลอดภัยให้ได้อย่างเหมาะสมขึ้นอยู่กับสิทธิ์ของผู้ใช้และปรับเปลี่ยนประเภทบริการตามการเปลี่ยนแปลงที่ได้รับอนุญาต • จะสามารถใช้งานได้จริงและสะดวกในการใช้งาน อุปกรณ์เคลื่อนที่จะต้องอยู่ในสภาพแวดล้อมที่มีอินเทอร์เน็ต ทำให้ระบบให้บริการด้วยความยืดหยุ่นและมีประสิทธิภาพ • จะดำเนินมาตรการการป้องกันขึ้นอยู่กับความต้องการของนโยบายการปรับการพิสูจน์ตัวตนด้วยตนเอง การกำหนดมาตรการการป้องกันตามความต้องการนโยบายของผู้ใช้ การตั้งคีย์ การเข้ารหัสและการกำหนดสิทธิในการเข้าถึงบริการ
[5]	• มีระบบพิสูจน์หลักฐานการโต้ตอบที่มีมาตรฐาน สามารถตรวจสอบเป็นระยะๆ เพื่อติดตามการเปลี่ยนแปลงของข้อมูลจากภายนอก • ลดภาระในการทำงานบนเซิร์ฟเวอร์จัดเก็บข้อมูลได้ระยะเวลาหนึ่ง • สามารถลดการคำนวณและค่าใช้จ่ายในการติดต่อสื่อสารให้เหลือน้อยที่สุดได้	• โมเดลนี้จะใช้ได้จริงต้องมีการบำรุงรักษาความปลอดภัยให้กับผู้ตรวจสอบของบุคคลที่สามและปรับใช้ดีมอนในการปฏิบัติการเกี่ยวกับโปรโตคอลพิสูจน์ความจริง
[6]	• ประมวลผลด้วยสัญญาณเซ็นเซอร์มัลติมีเดียและอยู่ในสภาพแวดล้อมที่ปลอดภัย • ช่องทางในการสื่อสารมีความเป็นส่วนตัว • มีการตรวจสอบและป้องกันการเข้าถึงจากผู้ใช้ที่ไม่ได้รับอนุญาตในการเข้าถึงข้อมูล • มีการรับประกันความปลอดภัยและความเป็นส่วนตัวของข้อมูล • มีการจัดเก็บอย่างปลอดภัยบนเซิร์ฟเวอร์ เพื่อป้องกันการโจรกรรมและการสูญหายของข้อมูล จึงต้องมีการให้บริการเก็บสำรองข้อมูลอย่างปลอดภัย • การทำงานช่วยขยายความจุ ความน่าเชื่อถือ และอายุการใช้งานของอุปกรณ์เคลื่อนที่ผ่านทางผู้ให้บริการทั่วไปได้ • ช่วยให้ผู้ใช้ที่ใช้โทรศัพท์มือถือราคาต่ำสามารถเข้าถึงบริการที่ประสิทธิภาพสูงได้	• เป็นการประมวลผลสัญญาณมัลติมีเดียที่แรงและหนักจะต้องใช้พลังงานเพิ่มขึ้นเพื่อให้สามารถดำเนินการบนอุปกรณ์เคลื่อนที่ได้ เพื่อป้องกันพลังงานนี้ไหลออก วิธีการที่เสนอจะอัพโหลดอัลกอริทึมแบบที่ซับซ้อนกว่าเพื่อดำเนินการบนคลาวด์และผลลัพธ์สุดท้ายจะอัพโหลดกลับไปที่อุปกรณ์เคลื่อนที่ จึงแบ่งกลุ่มกลไกบริการที่จำเป็นเป็นแบบกลุ่มที่เป็นจุดแข็งและจุดอ่อน
[7]	• มีผู้ดูแลระบบคลาวด์รับผิดชอบในการจัดการโครงสร้างพื้นฐานและให้บริการการร้องขอ • ระบบนี้ใช้การคำนวณแบบไดนามิกทำให้มีค่าใช้จ่ายน้อยมาก • สามารถรองรับจำนวนผู้ใช้ได้สองเท่าของระบบแบบเดิม เพราะมีการจัดสรรระบบเครื่องจักรเสมือนให้กับผู้ใช้ • สามารถใช้ประโยชน์จากทรัพยากรที่มีอยู่ในมือได้อย่างเต็มที่ • สามารถให้ผู้ใช้เข้าถึงคลาวด์ได้ง่ายจากที่ใดก็ได้ภายในที่มีทรัพยากรมาสนับสนุน	• ขาดบริการการกำหนดสิทธิ์ในการใช้งานให้กับผู้ใช้ บริการการป้องกันการปฏิเสธความรับผิดชอบ บริการการจัดการการระบุตัวตน และบริการการตรวจสอบวัดประสิทธิภาพให้ตรงตามนโยบายการเข้าถึงข้อมูล
[8]	• มีการป้องกันความปลอดภัยทั้งการปกป้องความลับและความสมบูรณ์ของข้อมูลหรือไฟล์ที่กำลังอัพโหลดในอุปกรณ์เคลื่อนที่ที่จัดเก็บข้อมูลบนคลาวด์ • รูปแบบ EnS จัดการแก้ปัญหาสถานการณ์ที่มีเซิร์ฟเวอร์คลาวด์เพียงเซิร์ฟเวอร์เดียว โดยจะรับประกันความปลอดภัยตามเป้าหมายและเงื่อนไขจำเป็นสำหรับเหตุการณ์นี้ • รูปแบบ CoS สามารถหลีกเลี่ยงการประมวลผลของขั้นตอนวิธีการเข้ารหัสในสถานการณ์ที่มีเซิร์ฟเวอร์คลาวด์อยู่มากมายโดยการเข้ารหัสแบบเส้นตรง • รูปแบบ ShS สามารถลดค่าใช้จ่ายในการคำนวณโดยใช้ exclusive-or operations	• ยังเป็นรูปแบบที่เชื่อถือได้บางส่วน (เนื่องจากเข้าถึงได้จากทั้งภายในและภายนอก) ส่วนหน่วยจัดเก็บในอุปกรณ์เคลื่อนที่ยังไม่น่าไว้ใจ เนื่องจากผู้โจมตีอาจจะขโมยข้อมูลบางอย่างด้วยการติดตั้งซอฟต์แวร์ที่เป็นอันตราย หรืออุปกรณ์เคลื่อนที่อาจจะหายไปโดยบังเอิญและสิ่งที่จัดเก็บทั้งหมดก็จะถูกเปิดเผย

จากการเปรียบเทียบเทคนิคการทำงานต่างๆที่ใช้ในแต่ละบริการความปลอดภัย ดังในตารางที่ 1, 2 และตารางที่ 3 แสดงข้อดีและข้อจำกัดของแต่ละงานวิจัยนั้น พบว่า [4] นำเสนอโมเดลการรักษาความปลอดภัยที่ใช้เทคนิคการทำงานที่ครอบคลุมและค่อนข้างที่จะปลอดภัยมากกว่ากลไกในงานวิจัยอื่นๆ เพราะสามารถเตรียมบริการรักษาความปลอดภัยได้ ขึ้นอยู่กับสิทธิ์ของผู้ใช้ ผู้ใช้ปรับเปลี่ยนประเภทบริการตามการเปลี่ยนแปลงที่ได้รับอนุญาต มีบริการการตรวจสอบสิทธิ์ของผู้ใช้ มีนโยบายรักษาความปลอดภัยที่ช่วยให้บริการคลาวด์มีความปลอดภัยมากขึ้น อีกทั้งนำไปประยุกต์ใช้กับการรักษาความปลอดภัยคลาวด์บนอุปกรณ์เคลื่อนที่ ทำให้ผู้ใช้อุปกรณ์เคลื่อนที่ผ่านบริการบนคลาวด์มีความปลอดภัยสูง ช่วยเพิ่มศักยภาพของระบบ ทำให้มีประสิทธิภาพสูงขึ้นในการให้บริการ และตอบสนองความต้องการของผู้ใช้ได้อย่างเต็มที่ แต่โมเดลข้อยังขาดบริการความไว้วางใจ บริการการจัดการระบุตัวตน บริการการตรวจสอบวัดประสิทธิภาพ และบริการความพร้อมใช้งานของบริการคลาวด์ควรที่จะพัฒนาในตรงส่วนนี้ให้บริการมีความปลอดภัยสมบูรณ์ยิ่งขึ้น

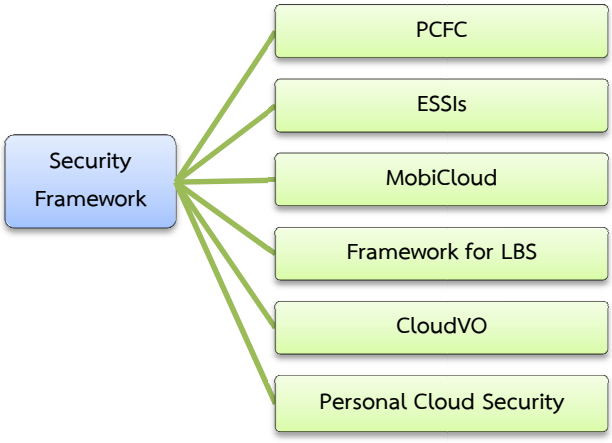
III. Security Framework

จากการศึกษางานที่ผ่านมา ข้อจำกัดของการรักษาความปลอดภัยคลาวด์บนอุปกรณ์เคลื่อนที่ที่พบคือ [10] อุปกรณ์ที่สนับสนุนการเชื่อมต่อและแบนด์วิธที่ยังไม่แพร่หลายมากนัก เนื่องจากถ้าผู้ใช้ไม่สามารถเชื่อมต่อกับเครือข่ายหรืออาจจะใช้อุปกรณ์เคลื่อนที่ที่ไม่สนับสนุนการเชื่อมต่อเครือข่ายได้ การรักษาความปลอดภัยคลาวด์บนอุปกรณ์เคลื่อนที่ก็ไม่มีประสิทธิภาพเท่าที่ควร

- การรักษาความปลอดภัยไม่สามารถการันตีได้ว่าไฟล์ที่มีการส่งออกจากอุปกรณ์เคลื่อนที่นั้นจะถูกเก็บเป็นความลับ โดยเฉพาะอย่างยิ่งในกรณีที่ระบบส่งไฟล์ในขณะที่กำลังประมวลผลอยู่ การรั่วไหลของข้อมูลอาจจะทำให้เกิดความเสียหายอย่างมาก
- ความหนาแน่นของข้อมูลในคลาวด์เซิร์ฟเวอร์จะเป็นภาระให้แก่เครือข่าย เนื่องจากแบนด์วิธมีจำกัด ทำให้การบริการปกติ เช่น การสนทนาด้วยเสียงผ่านอินเตอร์เน็ต อาจจะได้รับผลกระทบได้

ภาระทางเศรษฐกิจ ในเมืองใหญ่ๆ ผู้ใช้จะถูกเก็บค่าบริการในการใช้อินเตอร์เน็ต แม้ว่าบางคนจะเลือกการจ่ายแบบจ่ายเท่าที่ใช้ และการจ่ายแบบเป็นรายเดือนที่สามารถใช้ได้ไม่จำกัด เป็นไปตามหลักที่ว่า ใช้มากจ่ายมาก ด้วยเหตุนี้ บริการคลาวด์บนอุปกรณ์เคลื่อนที่จึงจะหักเงินจากบัญชีธนาคารของผู้ใช้สำหรับค่าใช้จ่ายเพิ่มเติมที่เกิดขึ้น

Framework คือกรอบการทำงานหรือโครงสร้างกึ่งสำเร็จรูปที่ผู้ใช้สามารถนำไปประยุกต์ใช้และเขียนเพิ่มเติม เพื่อใช้งานอย่างใดอย่างหนึ่ง ซึ่ง Framework จะมีโครงสร้างที่เป็นมาตรฐานและมีทรัพยากรอยู่เป็นจำนวนมาก ทำให้ประหยัดเวลาในการนำไปใช้เนื่องจากไม่ต้องสร้างระบบบางส่วนแบบเดิมซ้ำๆ ปัจจุบันนี้ เชื่อว่าปัจจุบันนี้ หลายหน่วยงานหรือองค์กรที่มีการให้บริการแอพพลิเคชั่นบนอุปกรณ์เคลื่อนที่และมีการประมวลผลบนคลาวด์นั้นต้องการสร้างความเชื่อมั่นในการรักษาความปลอดภัยและสามารถจัดการกับระบบได้อย่างมีประสิทธิภาพซึ่งหน่วยงานหรือองค์กรดังกล่าวน่าจะต้องการ Framework ที่มีประสิทธิภาพ เพื่อให้เกิดความเชื่อมั่นในเรื่องความปลอดภัยสำหรับผู้ใช้บริการคลาวด์บนอุปกรณ์เคลื่อนที่ รวมถึงเพิ่มประสิทธิภาพในการบริหารจัดการระบบอีกด้วย



รูปที่ 13 แผนผังแสดง Framework ที่แต่ละงานวิจัยได้ศึกษา

กรอบการสร้างการรักษาความปลอดภัยเครือข่ายของอุปกรณ์เคลื่อนที่บนคลาวด์นั้น ส่วนใหญ่มีแนวคิดหลักคือต้องการให้มีความปลอดภัยสูงสุดสำหรับข้อมูลที่ผู้ใช้บริการต้องการเก็บไว้บนเครือข่าย หรือส่งให้ผู้ใช้บริการอื่นๆ โดยข้อมูลนั้นๆ ต้องได้รับความมั่นใจว่าจะไม่มีการเปลี่ยนแปลงระหว่างทาง หรือผู้อื่นที่ไม่เกี่ยวข้องต้องสามารถดูหรือจัดการใดๆ กับข้อมูลได้ ซึ่งกระบวนการสร้างการรักษาความปลอดภัยที่ถูกพัฒนาเป็น Framework ได้มีการนำมาศึกษาดังนี้

A. PCFC (Private Cloud and File Characteristic Based) [9]

ใน PCFC Framework คลาวด์ส่วนตัวจะเชื่อมต่อโดยตรงกับเครือข่ายหลัก ในขณะที่คลาวด์บนอุปกรณ์เคลื่อนที่แบบเก่าจะใช้งานบนอินเตอร์เน็ตลักษณะหลักของ PCFC Framework คือความเป็นคลาวด์ส่วนตัว ซึ่งส่วนตัวในที่นี้ไม่ได้หมายความว่ามีคลาวด์เซิร์ฟเวอร์แยกออกมาโดยเฉพาะ แต่หมายถึงว่าคลาวด์นั้นๆเชื่อมต่อโดยตรงกับเครือข่ายหลัก ขึ้นอยู่กับผู้ให้บริการว่าจะให้บริการอย่างไร

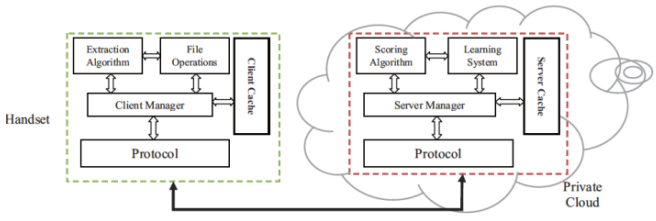
ตามทฤษฎีแล้ว PCFC จะครอบคลุมทุกข้อจำกัดที่เกิดขึ้นดังที่กล่าวไป ถึงแม้ผู้ใช้จะมีการเชื่อมต่อกับอินเตอร์เน็ตผิดพลาด อุปกรณ์เคลื่อนที่ก็จะยังเชื่อมต่อกับ PCFC ที่ใช้อยู่ได้ และการรักษาความปลอดภัยก็จะยังคงอยู่ อีกทั้งความเร็วในการส่งข้อมูลระหว่างอุปกรณ์เคลื่อนที่และคลาวด์เซิร์ฟเวอร์ก็จะเพิ่มขึ้นอย่างรวดเร็วหรือกล่าวอีกนัยหนึ่งคือช่วงเวลาระหว่างการ “Request” and “Response” จะลดลง

ระบบ PCFC ประกอบด้วยสามส่วนประกอบหลัก เรียกว่า mobile client, private cloud service และ PCFC protocols รายละเอียดมีดังนี้

a) Mobile Client

A PCFC mobile client คือแอพพลิเคชั่นที่ทำงานอยู่บนแฮนด์เซต ดังตัวอย่างในรูปที่ ซึ่งเป็นส่วนหนึ่งของส่วนประกอบย่อยสี่อย่าง ในระหว่างสี่อย่างนี้ ตัวจัดการลูกข่ายจะทำงานไปพร้อมๆกับแอพพลิเคชั่น และภายใต้การควบคุมของตัวจัดการลูกข่าย จะมีการแตกอัลกอริทึมเพื่อค้นหาข้อมูลที่มีประโยชน์จากไฟล์ที่ถูกป้องกันเหล่านั้น การดำเนินการนี้ต้องกระทำกับกับส่วนประกอบที่ดำเนินการเกี่ยวกับไฟล์ เพราะส่วนนั้นจะจัดหาการเชื่อมต่อต่างๆ เช่น เปิด เข้าถึง หรือแม้แต่ลบไฟล์ (ในกรณีที่น่าสงสัยว่าจะอันตราย) ส่วนแคชจะจัดหาวิธีการที่ง่ายในการตรวจสอบในกรณีไฟล์ที่ประมวลผลถูกสแกนมาแล้วก่อนหน้านี้ โดยอาจใช้วิธีการแนบไฟล์ที่มีไอดีไม่ซ้ำกันไว้เพื่อระบุตัวตนของไฟล์แต่ละไฟล์ได้

b) cloud service



รูปที่ 14 ส่วนประกอบหลักของ PCFC

ส่วนประกอบย่อยของบริการคลาวด์ส่วนตัว ดังที่แสดงในรูปที่ 14 (เป็นส่วนขวาของรูป ซึ่งส่วนซ้ายคือ mobile client) คล้ายกับส่วนของ mobile client

ซึ่งหน่วยจัดการในเซิร์ฟเวอร์จะคิดค่าบริการจากตารางการทำงานที่ควรดำเนินการ และการดำเนินงานเหล่านี้จัดออกเป็นสองประเภทคือ

- Scoring process การประมวลผลประเภทนี้จะกระทำทั้งโดยหน่วยจัดการเซิร์ฟเวอร์และscoring algorithm รายละเอียดคือ scoring algorithm จะนำเสนอวิธีการรับข้อมูลจาก mobile client ที่ควรจะได้รับการวิเคราะห์และจะให้คะแนนในตอนสุดท้ายเพื่อให้เห็นระดับความเสี่ยงของไฟล์
- Learning process. ระบบการเรียนรู้มีจุดมุ่งหมายเพื่อสอนวิธีการให้คะแนนเนื่องจากไม่มีหลักการตายตัวที่จะตัดสินใจว่าไฟล์ที่ถูกสแกนเป็นอันตรายหรือไม่ เราต้องรีเฟรชวิธีการให้คะแนนตลอดเวลาด้วยชุดข้อมูลสอนต่างๆ

อีกทั้งหน่วยความจำแคชของเซิร์ฟเวอร์ยังต้องเก็บข้อมูลที่ระบุว่าการตรวจสอบควรจะดำเนินการหรือไม่ เพราะจะไม่มีการดำเนินการถ้าไฟล์มีการตรวจสอบมาก่อนแล้ว

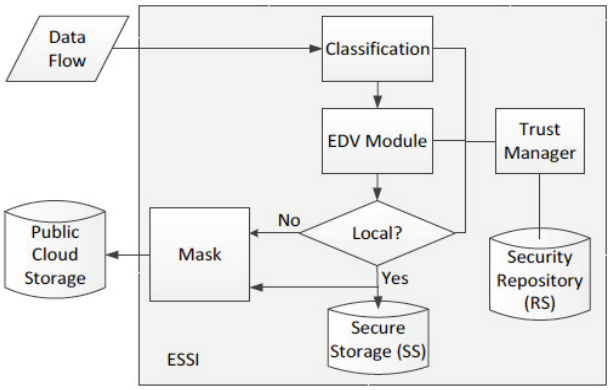
c) Protocol

ส่วนประกอบของโปรโตคอลมีจุดประสงค์คือสร้างการเชื่อมต่อที่ปลอดภัยและมั่นคงระหว่าง Mobile client และคลาวด์เซิร์ฟเวอร์ว่ารูปแบบของข้อมูลแบบไหนที่สามารถส่งได้และเงื่อนไขอะไรที่จะต้องต้องตรวจสอบก่อนที่การดำเนินการจะเริ่มต้นขึ้น (ตัวอย่างเช่น จะใช้วิธีการให้คะแนนแบบใดเนื้อหาข้อมูลของไฟล์ไหนน่าจะถูกตรวจสอบก่อนส่งออก) ซึ่งการทำงานของโปรโตคอลจะประกอบด้วยขั้นตอนต่อไปนี้ คือ

- ขั้นตอนการ Handshake เป็นขั้นตอนเบื้องต้นที่จะตรวจสอบว่าทั้งลูกข่ายและแม่ข่ายพร้อมสำหรับการทำงานหรือไม่
- ขั้นตอนการยืนยันตัวตน ขั้นตอนนี้จะถูกรักษาความปลอดภัยด้วยวิธีการ RSA ก่อนอื่นเราควรจะแน่ใจก่อนว่าคลาวด์เซิร์ฟเวอร์บนลูกข่ายในปัจจุบันมีการเชื่อมต่อกันแล้ว การเข้ารหัสตัวเลขแบบสุ่มด้วยคีย์สาธารณะของเซิร์ฟเวอร์ปลายทางจะถูกส่งออกจากไคลแอนต์ ซึ่งจะเหมือนกับตัวเลขที่เซิร์ฟเวอร์ส่งกลับเป็นคำตอบ เซิร์ฟเวอร์หลอกจะไม่มีคีย์ส่วนตัวที่ถูกต้องเพื่อถอดรหัสข้อความที่บรรจุตัวเลข ดังนั้นมันจะไม่ผ่านการยืนยันตัวตน ขั้นตอนที่สองคือการการันตีว่าอุปกรณ์เคลื่อนที่ลูกข่ายต้องเข้าถึงคลาวด์เซิร์ฟเวอร์อย่างถูกต้อง ไอดีและพาสเวิร์ดของผู้ใช้ที่ส่งมาจากลูกข่ายจะถูกตรวจสอบโดยแม่ข่ายเพื่อตรวจสอบความถูกต้องของการเข้าถึง พร้อมกับข้อความการตรวจสอบ วิธีการ DH ที่เกี่ยวกับพารามิเตอร์จะแลกเปลี่ยนในช่วงนี้ด้วยเช่นกัน วิธีการ DH ได้ถูกใช้อย่างกว้างขวางในการแลกเปลี่ยนคีย์สมมาตรระหว่างสองหน่วย
- ขั้นตอนการส่งผ่านข้อมูลหลังจากช่วงที่สองตอนนี้ไคลแอนต์และเซิร์ฟเวอร์จะพร้อมรับข้อมูลแล้วข้อมูลทั้งหมดควรจะถูกเข้ารหัสด้วยคีย์ DH ซึ่งถูกแลกเปลี่ยนกันในขั้นตอนการยืนยันตัวตน
- ขั้นตอนการออกจากระบบเป็นการบอกว่าไคลแอนต์ต้องการจบการเชื่อมต่อกับเซิร์ฟเวอร์เพื่อให้มีการปล่อยทรัพยากรทั้งหมดที่ถูกจัดสรรมาก่อนซึ่งทั้งไคลแอนต์และเซิร์ฟเวอร์จะกลับมาสู่สถานะแสดนด์บาย

B. ESSIs Framework [10]

ใน [11] ได้กล่าวถึง Extended Semi-Shadow Images (ESSIs) ซึ่งเป็นนโยบายรักษาความปลอดภัยที่ควรปฏิบัติสำหรับอุปกรณ์เคลื่อนที่ที่เกี่ยวข้องผู้ใช้สามารถที่จะระบุได้ว่าข้อมูลอะไรควรจะป้องกันและจัดเก็บใน ESSI ของมัน และข้อมูลส่วนตัวของผู้ใช้ต้องคงอยู่ใน Secure Storage (SS) ที่สัมพันธ์กันแบบจำลองการประมวลผลข้อมูลใน ESSIs ที่สร้างขึ้น ใช้ได้สำหรับ Linux Kernel 2.2 และสูงกว่า ขึ้นอยู่กับแบบจำลองความสามารถในการรักษาความปลอดภัย เรามีการสร้าง Trirooted ESSI ที่มี cloud root, user root และ auditing root เป็นส่วนประกอบ สิทธิของ user root คือการรักษาข้อมูลของผู้ใช้ใน Secure Storage (SS) ของมัน และการเข้ารหัส การถอดรหัส และกระบวนการตรวจสอบที่เกี่ยวข้อง cloud root โดยจะดำเนินการในฟังก์ชั่นการบำรุงรักษาของ ESSI แต่ไม่ได้มีการเข้าถึง SS และฟังก์ชั่นการรักษาความปลอดภัยที่เกี่ยวข้อง auditing root จะถูกใช้บันทึกกิจกรรมของทั้ง cloud root และ user root ซึ่ง log data สามารถเข้าถึงได้เฉพาะวัตถุประสงค์การตรวจสอบ



รูปที่ 15 แบบจำลองการประมวลผลใน ESSIs

เมื่อการละเมิดกฎถูกระบุ โดยปกติแล้ว log data จะถูกเก็บรักษาโดย A third trusted party (องค์การที่ให้บริการด้าน security) ดังนั้น ผู้ให้บริการคลาวด์ไม่สามารถละเมิดความเป็นส่วนตัวของผู้ใช้ได้ง่ายๆ

แบบจำลองการประมวลผลข้อมูลแบบ ESSI ที่ถูกแสดงดังรูปที่ 15 นั้น SS ถูกติดตั้งในฮาร์ดไดร์ฟเสมือน ข้อมูลส่วนตัวของผู้ใช้และสิทธิการรักษาความปลอดภัยถูกจัดเก็บใน Security Repository (RS) บริหารงานโดย ESSI เพื่อวางแผนบริการอุปกรณ์เคลื่อนที่ของผู้ใช้ ข้อมูลสำคัญถูกจัดเก็บใน SS การไหลของข้อมูลที่มายัง ESSI มีการประมวลผลดังนี้ : (1) การไหลของข้อมูลจะถูกตรวจสอบโดยแบบจำลองการจัดหมวดหมู่ ที่จะแบ่งกลุ่มข้อมูลออกเป็นข้อมูลสำคัญและข้อมูลธรรมดา (2) ถ้าข้อมูลที่ถูกจัดกลุ่มเป็นข้อมูลแบบธรรมดา ข้อมูลนั้นจะถูกไปยังหน่วยจัดเก็บข้อมูลบนคลาวด์แบบสาธารณะผ่านทางกระบวนการที่ซ่อนไว้ (3) โมดูลการเข้ารหัส ถอดรหัส และตรวจสอบ (Encryption /Decryption /Verification (EDV)) จะถูกใช้กับข้อมูลสำคัญ และจัดกับข้อมูลที่ถูกประมวลผลลงใน SS กระบวนการที่ซ่อนไว้จะถูกใช้ลบข้อมูลส่วนตัวที่เกี่ยวข้องกับผู้ใช้ และลบเนื้อหาข้อมูลที่สามารถย้อนรอยได้ กระบวนการที่ไม่เปิดเผยสามารถกำหนดค่าที่แตกต่างกันตามระดับความสำคัญของข้อมูล ขึ้นอยู่กับการตั้งค่าของผู้ใช้ และการถูกดำเนินการผ่านหน่วยจัดการความถูกต้อง ตัวอย่างเช่น ESSI สามารถสร้างค่าดัชนีลับในหน่วยจัดเก็บข้อมูลบนคลาวด์แบบสาธารณะได้ เพื่อวัตถุประสงค์ในการทำดัชนี ค่า

ดัชนีนี้ ประกอบด้วย ค่าเฉพาะตัวของ ESSI (สามารถใช้เป็นนามแฝงได้) และหมวดหมู่ดัชนีที่สัมพันธ์กัน เมื่อบริการจัดเก็บบนคลาวด์แบบสาธารณะได้รับค่าดัชนีมา มันก็จะใช้ในการระบุว่า ESSI อันไหนที่รับผิดชอบในข้อมูลการค้นหาที่ถูกร้องขอ

C. *MobiCloud Framework* [11]

การใช้งานโทรศัพท์มือถือเพื่อระบบการสื่อสารแบบ Ad-hoc เป็นทางออกที่ดีสำหรับการเชื่อมต่อทั่วโลกเพื่อสนับสนุนให้การใช้งานกว้างขึ้น ซึ่งการพัฒนาเทคโนโลยีการทำงานแบบไร้สายเช่น 3/4G, LTE, และ WiMax จะทำให้อุปกรณ์เคลื่อนที่สามารถเข้าถึงเครือข่ายได้ในระยะทางยาวขึ้น และแบนด์วิธที่สูงขึ้น ซึ่งช่วยให้การสื่อสารระหว่างโทรศัพท์มือถือและ cloud มีประสิทธิภาพสูง สถาปัตยกรรมความปลอดภัยของการบริการคลาวด์บนมือถือรูปแบบใหม่เป็นสิ่งจำเป็น อยู่ที่ความต้องการผู้ใช้ในสภาพแวดล้อมที่แตกต่างกัน โดยทั่วไป ผู้ใช้โทรศัพท์มือถือสามารถได้รับประโยชน์มากมายจากบริการคลาวด์สำหรับการเก็บและประมวลผลข้อมูลที่เข้มงวด เช่น การค้นหาข้อมูล การประมวลผลข้อมูล การทำเหมืองข้อมูล การตรวจสอบสถานะเครือข่าย เป็นต้น

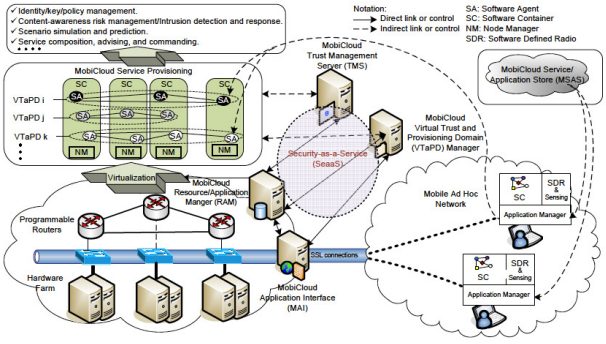
จากรูปที่ 16 คือโครงร่างการประมวลผลความปลอดภัยของคลาวด์บนอุปกรณ์เคลื่อนที่ เรียกว่า MobiCloud ซึ่งแปลง Mobile Ad hoc NETwork (MANETs) แบบเดิมมาเป็นสถาปัตยกรรมแบบใหม่ที่มุ่งเน้นการบริการเป็นหลัก ซึ่งแต่ละอุปกรณ์มือถือจะถือว่าเป็น Service Node (SN) และมันจะสะท้อนไปยัง Extended Semi- Shadow Images (ESSIs) ในคลาวด์เพื่อที่จะสื่อสารกับข้อผิดพลาดในการคำนวณและสื่อสารของอุปกรณ์เคลื่อนที่ ใน MobiCloud อุปกรณ์เคลื่อนที่สามารถแบ่งการคำนวณและการเก็บข้อมูลของมันออกเป็นส่วนๆ เพื่อให้สอดคล้องกับ ESSI และ Secure Storage (SS) ยิ่งไปกว่านั้น อุปกรณ์จะส่งข้อมูลของมันไปยังคลาวด์ด้วย เช่น การย้ายเส้นทางในทางกลับกัน คลาวด์สามารถให้บริการ location-based ที่ดีกว่าตามข้อมูลการเคลื่อนย้ายที่อุปกรณ์เคลื่อนที่มีฟังก์ชั่นนี้ไว้บริการใน MobiCloud ผู้ใช้ต้องไว้ใจผู้ให้บริการคลาวด์ในการดูแลข้อมูลที่ได้รับจากอุปกรณ์เคลื่อนที่ ซึ่งเป็นสิ่งที่น่าเป็นห่วงมากสำหรับผู้ใช้ โดยแต่ละอุปกรณ์เคลื่อนที่จะเป็นเสมือน ESSI ในคลาวด์โดเมนและแต่ละ ESSI สามารถนำมาใช้เพื่อเชื่อมต่อกับข้อผิดพลาดของการคำนวณและการติดต่อสื่อสาร และเพิ่มความปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคล อุปกรณ์เคลื่อนที่และ ESSI ที่สอดคล้องกันสามารถทำหน้าที่เป็นผู้ให้บริการหรือตัวแทนให้บริการเท่าที่ความสามารถของมันจะทำได้อีกด้วย เช่น ความสามารถในการคำนวณและการสื่อสารที่มีอยู่ซึ่งสนับสนุนการเชื่อมต่อโดยเฉพาะ วิธีการนี้จะใช้ประโยชน์ของแต่ละโหนดในระบบอย่างเต็มที่โดยใช้เทคโนโลยีการประมวลผลแบบคลาวด์ ถ้าเป็นเช่นนี้ขอบเขตของคลาวด์จะขยายไปยังอุปกรณ์ของลูกค้าได้ ระบบเครือข่ายระหว่างผู้ใช้ และ ESSI ที่มีการเชื่อมต่ออย่างปลอดภัย เช่น SSL, IPSec เป็นต้น

งานวิจัยนี้ มีรายละเอียดหลัก คือ

- MobiCloud สนับสนุน ฟังก์ชั่น MANET ของการกระจายข้อมูล การกำหนดเส้นทาง การจำกัดพื้นที่ และการจัดการความน่าเชื่อถือ
- MobiCloud นำเทคโนโลยีการประมวลผลแบบคลาวด์ มาสร้างสภาพแวดล้อมเสมือนจริงสำหรับการดำเนินการ MANET ในขอบเขตการเตรียมบริการแบบหลากหลาย ตามปัญหาของ บริการ MANET และความต้องการความปลอดภัยที่สอดคล้องกัน
- MobiCloud มีรูปแบบพื้นฐานที่เชื่อถือได้ เช่น การจัดการลักษณะเฉพาะตัว, key management และการบังคับใช้นโยบายการรักษาความปลอดภัยในการเข้าถึงข้อมูล ซึ่งสามารถพัฒนาในโปรแกรมบนอุปกรณ์เคลื่อนที่ต่อไป
- สามารถใช้ MobiCloud ในการตรวจสอบประสิทธิภาพการทำงานที่หลากหลายและตรวจสอบปัญหาด้านความปลอดภัยของ MANET และสร้างข้อมูลที่นำไปใช้ประโยชน์ได้

จากรูปที่ 16 แสดงแนวคิดพื้นฐานของ MobiCloud คล้ายกับการประมวลผลและการจัดเก็บแบบคลาวด์ที่มีอยู่เดิมโดยดึงประสิทธิภาพแหล่งฮาร์ดแวร์ในคลาวด์เพื่อเพิ่มความสามารถในการประมวลผลของมันให้มากยิ่งขึ้น MobiCloud ถูกออกแบบเพื่อให้บริการคลาวด์สำหรับ MANETs ดังนี้

โครงสร้างของ MobiCloud



รูปที่ 16 แบบจำลองของ MobiCloud

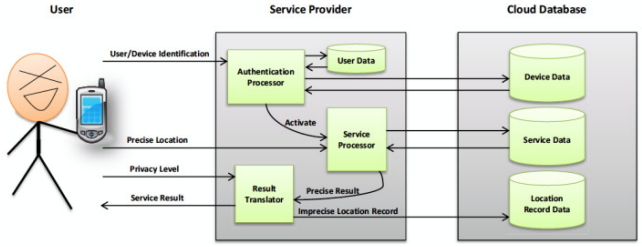
- ทำหน้าที่ตัดสินใจในเรื่องเอกลักษณ์ คีย์ และการจัดการนโยบายการเข้าถึงข้อมูลอย่างปลอดภัย
- มีการรักษาความปลอดภัยเพื่อป้องกันข้อมูลของผู้ใช้อุปกรณ์เคลื่อนที่โดยเฉพาะ
- มีการตรวจสอบสถานะของ MANET เพื่อประเมินความเสี่ยง ในการตรวจจับการบุกรุกและการตอบสนอง
- จำลองสถานการณ์และทำนายสถานการณ์ของ MANET ล่วงหน้าเพื่อใช้ในการตัดสินใจ
- ให้บริการต่างๆสำหรับอุปกรณ์เคลื่อนที่

MobiCloud ใช้ Software Agents (SAs) เพื่อเชื่อมต่อกับบริการคลาวด์และอุปกรณ์เคลื่อนที่ เหมือนกับ SA ที่สามารถทำงานทั้งบนอุปกรณ์เคลื่อนที่และโครงสร้างของคลาวด์ควบคู่กัน แต่ละอุปกรณ์สามารถมี SAs อย่างหลากหลายสำหรับบริการคลาวด์หรือ MANETS ที่แตกต่างกัน ซึ่งถูกจัดการโดยหน่วยจัดการการทำงานของอุปกรณ์ แต่ละอุปกรณ์จะมีข้อมูลตรวจสอบเกี่ยวกับอุปกรณ์ของมันเอง (เช่น ชนิดของหน่วยประมวลผล ฟังก์ชั่นการทำงาน สถานะแบตเตอรี่ และพิกัดสถานที่จาก GPS) และข้อมูลเกี่ยวกับโหนดอุปกรณ์ใกล้เคียง (เช่น ที่อยู่หรือคุณสมบัติของโหนดใกล้เคียง ประสิทธิภาพการเชื่อมต่อ ช่วงเวลาใกล้เคียง) ซึ่งจะถูกจัดการโดยระบบตรวจสอบของอุปกรณ์นั้นๆ

ในฝั่งของคลาวด์ MobiCloud Application Interface (MAI) จะมีบริการส่งออกสิ่งที่สามารถใช้งานได้ไปยังอุปกรณ์เคลื่อนที่ นอกจากนี้ MAI ยังมีอินเตอร์เฟซไปยังหน่วยจัดการ Virtual trusted and provisioning domain (VTaPD) และ Resource and Application Manager (RAM) ซึ่งจะต้องมีการแก้ปัญหาซอฟต์แวร์เมื่อส่วนประกอบของคลาวด์ไม่สามารถทำงานผ่านทาง Browser ได้ VTaPDs จะถูกสร้างขึ้นเป็นหลัก สำหรับแยกการส่งข้อมูลและควบคุมการเข้าถึง โดยการสร้างโดเมนเสมือนแบบ multiple มีโดเมนเสมือนแบบ multiple นี้มีคุณสมบัติหลักสองประการคือ (1) ความปลอดภัย อุปกรณ์ของผู้ใช้อาจจะทำงานได้หลายแอพพลิเคชั่นบนการรักษาความปลอดภัยที่แตกต่างกัน เช่น การสื่อสารพร้อมกันจากสองบุคคลจากโดเมนของผู้ดูแลระบบ และ (2) การล่วงรู้บริบท มันน่าจะเป็นสิ่งจำเป็นที่จะบริการแยกต่างหากสำหรับการตั้งค่าท้องถิ่นและเครือข่ายที่แตกต่างกัน เช่น MobiCloud สามารถจำลองการดำเนินงานของ MANETs โดยใช้พารามิเตอร์ของระบบหรืออัลกอริทึมการเลือกเส้นทางที่แตกต่างกัน เพื่อเปรียบเทียบวิธีต่างๆ ที่ใช้การประมวลผลแบบคลาวด์เป็นแหล่งข้อมูลการสื่อสาร วิธีนี้จะให้ทราบภาพรวมการดำเนินงานของ MANET ที่ครอบคลุมและให้ข้อมูลแก่อุปกรณ์เคลื่อนที่และหน่วยจัดการระบบเพื่อใช้ในการตัดสินใจ

D. *A Security Framework of Group Location-Based Mobile Applications in Cloud Computing* [12]

ใน [13] ได้มีการพูดถึง ODB (Outsourced Databases) ซึ่งเป็นองค์ประกอบสำคัญของ Database as a Service (DaaS) ในการประมวลผลแบบคลาวด์ จากรูปที่ 17 แสดงแบบจำลองการรักษาความปลอดภัยของ location-based services (LBS) สำหรับระบบ ODB ประกอบด้วย ผู้ใช้ ผู้ให้บริการ และ



รูปที่ 17 แบบจำลองของระบบ ODB

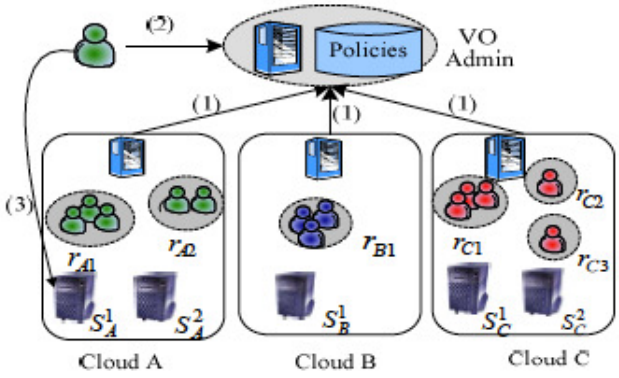
ฐานข้อมูลบนคลาวด์ มีสามหน่วยประมวลผลหลักในแต่ละผู้ให้บริการ: หน่วยประมวลผลการตรวจสอบ หน่วยประมวลผลการบริการ และหน่วยแปลผลลัพธ์ ฐานข้อมูลคลาวด์เป็นแหล่งจัดเก็บข้อมูลที่เกี่ยวข้องกับอุปกรณ์ บริการและสถานที่ โดยข้อมูลผู้ใช้จะถูกจัดเก็บไว้เฉพาะที่ผู้ให้บริการ แต่ไม่ได้เก็บที่ฐานข้อมูลคลาวด์ การไหลของข้อมูลสำหรับลูกค้าที่ใช้ LBS ได้อธิบายไว้ดังนี้ อันดับแรก ผู้ใช้ส่งข้อมูลการยืนยันตัวตนและระบุอุปกรณ์ที่เกี่ยวข้องให้แก่ผู้ให้บริการ จากนั้น หน่วยประมวลผลการตรวจสอบจะทำการตรวจสอบความถูกต้องของข้อมูลการยืนยันตัวตนเหล่านั้น ถ้าข้อมูลถูกตรวจสอบเรียบร้อยแล้ว หน่วยประมวลผล ABS จะถูกเปิดใช้งาน และผู้ใช้จะให้ข้อมูลสถานที่ของตนได้อย่างแม่นยำ ผู้ให้บริการก็จะสามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับบริการอื่นๆได้จากฐานข้อมูลคลาวด์ (เช่น ที่อยู่ของสถานที่ใกล้เคียง) สุดท้ายหลังจากได้รับระดับความเป็นส่วนตัวที่ลูกค้าต้องการ หน่วยวิเคราะห์ผลลัพธ์จะส่งผลการบริการให้แก่ผู้ใช้ และจัดเก็บระเบียนสถานที่เบื้องต้นลงในฐานข้อมูลคลาวด์ สำหรับระดับความเป็นส่วนตัวต่างๆ เห็นได้ชัดว่า คุณภาพการให้บริการอาจจะได้รับอิทธิพลโดยตรงจากระดับความเป็นส่วนตัว เช่น ความเป็นส่วนตัวระดับต่ำสามารถแสดงให้ผู้ใช้คนอื่นเห็นในระดับของถนน ในขณะที่ความเป็นส่วนตัวระดับสูงสามารถแสดงให้ผู้ใช้คนอื่นเห็นในระดับเมืองเท่านั้น

ความท้าทายในปัญหาของ LBS คือการพัฒนาเทคนิคที่มีประสิทธิภาพเพื่อปรับปรุงการรักษาความปลอดภัยข้อมูลสถานที่ไปพร้อมๆกัน ปัญหาของการรักษาความปลอดภัยข้อมูลแบ่งออกเป็น การรักษาความปลอดภัยในระหว่างการส่งข้อมูลและการรักษาความปลอดภัยในการจัดเก็บข้อมูล ปัญหาของการรักษาความปลอดภัยในระหว่างการส่งข้อมูลได้รับการวิจัยกันอย่างแพร่หลายในเครือข่ายและอินเทอร์เน็ต (เช่น SSL, IPsec) สำหรับปัญหาความปลอดภัยในการจัดเก็บข้อมูลมีการศึกษาน้อยมาก ซึ่งอาจส่งผลกระทบมากมายในการประมวลผลแบบคลาวด์ งานวิจัยนี้มุ่งเน้นไปที่สองปัญหาของความปลอดภัยในการจัดเก็บข้อมูล: ปัญหาแรกคือการยืนยันความถูกต้องและและปัญหาที่สองคือความเป็นส่วนตัว

E. *CloudVO* [13]

CloudVO คือกรอบการทำงานแบบองค์กรเสมือนตามหลักการการจัดการความไว้วางใจแบบกระจายอำนาจ และมีสภาพแวดล้อมการทำงานร่วมกันแบบกระจายและแบบส่วนตัว

Framework ของ CloudVO ดังแสดงในรูปที่ 18 องค์กรเสมือนประกอบด้วยบริการพิเศษและกฎจากคลาวด์ตัวอย่าง เช่น Cloud A, B, C เป็นที่น่าสังเกตว่าเซิร์ฟเวอร์ส่วนกลาง virtual organization (VO) (หรือเรียกว่าผู้ดูแลระบบ VO) จะยังเป็นที่ยอมรับจากทั้งหมด และการกำหนดบทบาทที่ดีที่สุดยัง

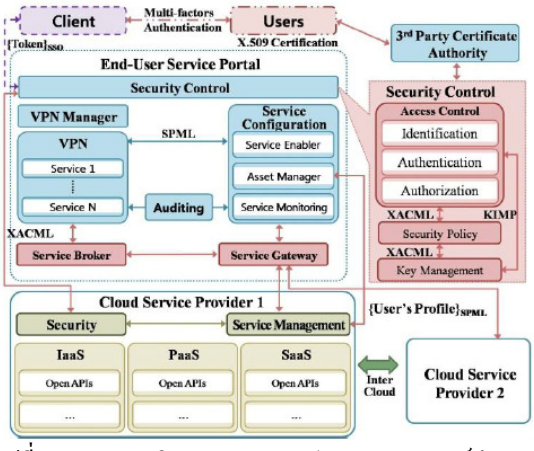


รูปที่ 18 กรอบแนวคิดของ CloudVO

ขึ้นอยู่กับนโยบายของคลาวด์แบบเดิม ซึ่งหน่วยตรวจสอบ VO จะถูกจัดส่งจากทุกๆคลาวด์โดยจะเป็นการอธิบายคลาวด์ที่สัมพันธ์กัน หมายความว่าอันดับแรกผู้ใช้บริการคลาวด์ควรจะได้รับกฎของสมาชิกจากเซิร์ฟเวอร์ VO ก่อนที่จะเข้าถึงเซิร์ฟเวอร์เป้าหมายที่อยู่ในคลาวด์ต่างๆได้ โดยมีสองขั้นตอนสำคัญของการจัดการองค์กรเสมือน ขั้นตอนหนึ่งคือการสร้างองค์กรผ่านนโยบายการทำงานร่วมกัน และผู้ดูแลระบบจะระบุบทบาทและความสัมพันธ์ภายใน CloudVO โดยทั่วไปแล้ว เซิร์ฟเวอร์ CloudVO จะทำการเลือกและยอมรับโดยการตัดสินใจแบบขั้นสูง อีกขั้นตอนคือบริการการยืนยันตัวตนในคลาวด์เป้าหมายเมื่อมีการร้องขอจากคลาวด์อื่นๆ อีกทั้งโปรโตคอลใน CloudVO จะมุ่งไปที่ปัญหาของข้อตกลงในการเป็นสมาชิกเป็นหลัก มีการจัดการความ

ขัดแย้งและความไว้วางใจ ดังแสดงในรูปที่ 2 โดยมีโปรโตคอลย่อยอยู่ใน CloudVO สามส่วน ส่วนแรกคือโปรโตคอลข้อตกลงของสมาชิกในองค์กรเสมือน ส่วนต่อมาคือโปรโตคอลตรวจสอบความขัดแย้ง และส่วนที่สามคือโปรโตคอลตจัดการความไว้วางใจ

F. Personal Cloud Security Framework [14]



รูปที่ 19 กรอบแนวคิดการรักษาความปลอดภัยบนคลาวด์ส่วนตัว

Framework แสดงอยู่ในรูปที่ 19 ซึ่งเป็นโมเดลบริการที่จะอธิบายรายละเอียดของแต่ละส่วนประกอบ และการประยุกต์ใช้เทคโนโลยีการรักษาความปลอดภัยที่จำเป็น สำหรับดำเนินการระหว่างส่วนประกอบในการประมวลผลคลาวด์ส่วนบุคคล

กระบวนการควบคุมการเข้าถึงที่ให้บริการบนแต่ละส่วนดังนี้

ลูกข่าย : ผู้ใช้จะเข้าถึงส่วนลูกข่าย (เช่นเวปบราวเซอร์หรือแอพพลิเคชั่นที่ติดตั้งบนโฮสต์) ผ่านอุปกรณ์ต่างๆ ด้วยการตรวจสอบหลายๆปัจจัยจากจุดบริการผู้ใช้ ฝั่งลูกข่ายคือจุดที่ผู้ใช้จะได้รับคลาวด์ส่วนตัวของตนเอง การตรวจสอบปัจจัยต่างๆจะอยู่ภายใต้การรับรองของ 3rd party CA

จุดบริการผู้ใช้ : เมื่อได้รับการตรวจสอบแล้ว a Single Sign-on Access Token (SSAT) จะมีการออกใบรับรองให้แก่ผู้ใช้ จากนั้นส่วนที่ควบคุมการเข้าถึงจะแชร์ข้อมูลที่เกี่ยวข้องกับผู้ใช้ด้วยนโยบายรักษาความปลอดภัยและตรวจสอบด้วยส่วนประกอบอื่นๆในจุดบริการผู้ใช้ ต่อมาจึงให้บริการคลาวด์โดยใช้ XACML [15] and KIMP [16] ซึ่งผู้ใช้จะใช้บริการได้ไม่จำกัด

การตั้งค่าการบริการ : เครื่องมือช่วยให้บริการ จะใช้รายละเอียดของผู้ใช้ในการจัดหาบริการคลาวด์ส่วนบุคคล รายละเอียดของผู้ใช้นี้จะใช้กับการจัดการบริการในผู้ให้บริการคลาวด์สำหรับการบูรณาการและการทำงานร่วมกันของการร้องขอการจัดเตรียมบริการจากผู้ใช้ The SPML [11] สามารถใช้แชร์รายละเอียดผู้ใช้ได้ หน่วยจัดการข้อมูลจะร้องขอทรัพยากรส่วนบุคคลของผู้ใช้ไปยังผู้ให้บริการคลาวด์และตั้งค่าบริการผ่าน VPN

บริการเกตเวย์และตัวแทนให้บริการ : บริการเกตเวย์จะจัดการทรัพยากรในเครือข่ายและและ VPN ที่อยู่บนวงจารข้อมูลของตัวแทนให้บริการ

การควบคุมการรักษาความปลอดภัย : ส่วนประกอบของการควบคุมการรักษาความปลอดภัยจะให้การป้องกันที่สำคัญสำหรับควบคุมการเข้าถึงนโยบายรักษาความปลอดภัย และการจัดการคีย์ เพื่อป้องกันการคุกคาม

การตรวจสอบบริการ : ระบบจะตรวจสอบบริการโดยอัตโนมัติเพื่อการีนตีประสิทธิภาพและการได้รับที่อยู่ในขั้นสูงของบริการ

เปรียบเทียบบทความที่เกี่ยวข้อง

ได้มีการเปรียบเทียบบทความที่เกี่ยวข้องดังตารางที่ 4 ตามฟังก์ชั่นการทำงานและส่วนประกอบที่สำคัญดังนี้

- การพิสูจน์ตัวตนผู้ใช้ (Authentication)

กระบวนการตรวจสอบตัวตนของผู้ใช้ ที่จะเข้ามาใช้งานในเครือข่ายเพื่อรักษาความปลอดภัยของระบบ สำหรับป้องกันผู้ไม่หวังดีที่จะเข้าใช้ระบบของผู้อื่น

- การกำหนดสิทธิ (Authorization)

ขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ซึ่งก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

- การป้องกันการเข้าถึงบริการ (Service Access Protection)

การรักษาความปลอดภัยในการเข้าถึงบริการ เพื่อป้องกันเหตุการณ์ที่ข้อมูลอาจรั่วไหล โดยจะป้องกันในส่วนของรายละเอียดการให้บริการผู้ใช้

- การจัดการสิทธิในการเข้าถึงและนโยบายความปลอดภัย (Access Rights and Policy Management)

เป็นการกำหนดสิทธิต่างๆในการให้บริการและการเข้าถึงข้อมูล และกำหนดนโยบายในการจัดการเกี่ยวกับความลับและความปลอดภัยของข้อมูล

- ความเป็นส่วนตัว (Privacy)

การบริการความเป็นส่วนตัวของผู้ใช้ คือการป้องกันมิให้ข้อมูลรั่วไหล และผู้ใช้อื่นที่ไม่เกี่ยวข้องสามารถกระทำการกับข้อมูลได้ รวมถึงความเป็นส่วนตัวของรายละเอียดการใช้บริการของผู้ใช้

- การรักษาความปลอดภัยการเชื่อมต่อ (Connection Security)

คือเมื่อมีการเชื่อมต่อต้องมีกลไกในการรักษาความปลอดภัย มีการตรวจสอบความถูกต้องในการเชื่อมต่อและในกรณีที่การเชื่อมต่อผิดพลาด

- การเข้ารหัสข้อมูล (Data Encryption)
- ข้อมูลที่การส่งผ่านกันระหว่างเครือข่าย หรือข้อมูลต่างๆของผู้ใช้ มีการเข้ารหัสเพื่อป้องกันการรั่วไหลของข้อมูลและป้องกันการโจมตีจากผู้ที่ไม่หวังดี
- การจัดการความไว้วางใจ (Trust Management)

มีการจัดการการสร้างกฎหรือข้อตกลงระหว่างสมาชิก และกฎในการเข้าถึงข้อมูลต่างๆ เพื่อให้ระบบมีความปลอดภัยมากที่สุด

- หน่วยเก็บข้อมูล (Cloud Storage)
- โปรแกรมเชื่อมต่อระหว่างสองแอพพลิเคชั่น (Application Interface)
- โปรโตคอลรักษาความปลอดภัย (Security Protocol)

จากการเปรียบเทียบฟังก์ชั่นการทำงานของ Framework ต่างๆ ดังในตารางที่ 5 พบว่า MobiCloud Framework [12] มีการทำงานที่ครอบคลุมและค่อนข้างที่จะปลอดภัยมากกว่า Framework อื่นๆ เพราะสามารถนำไปประยุกต์ใช้กับการรักษาความปลอดภัยคลาวด์บนอุปกรณ์เคลื่อนที่เพื่อให้เกิดความปลอดภัยสูงสุดและตอบสนองความต้องการของผู้ใช้ได้อย่างเต็มที่ และยังรวมไปถึงการประยุกต์ใช้กับแอพพลิเคชั่นเกี่ยวกับความเป็นส่วนตัวด้านสถานที่ ซึ่ง Framework อื่นอาจจะยังไม่ครอบคลุมในจุดนี้ และในส่วนของการส่งผ่านข้อมูลก็จะมีการเข้ารหัสด้วยอัลกอริทึมที่สร้างความปลอดภัยได้ดี

ตารางที่ 4 แสดงการตรวจสอบคุณสมบัติของ Framework ที่แต่ละงานวิจัยได้พัฒนา

	Authentication	Authorization	Privacy	Connection Security	Data Encryption	Trust Management	Cloud Storage	Application Interface	Security Protocol
[9]	✓			✓	✓				✓
[10]	✓	✓		✓	✓	✓	✓		
[11]	✓		✓	✓		✓		✓	
[12]	✓	✓	✓		✓		✓	✓	
[13]	✓			✓	✓	✓	✓	✓	✓
[14]	✓	✓						✓	

ตารางที่ 5 แสดงวิธีการของการรักษาความปลอดภัยใน Framework

	Authentication	authorization	Privacy	Connection Security	data encryption	Trust Management	Cloud storage	Application Interface	Security protocol
[9]	วิธี RSA			เข้ารหัสด้วย Public key	เข้ารหัสข้อมูลแบบ DH key				เข้ารหัสคีย์ยืนยันตัวตน
[10]	ตรวจสอบคีย์ส่วนตัว คีย์สาธารณะ	PoNP (point of network presence)		e.g., SSL, IPSec	identity cryptography	Attribute-Based Identity Management	Secure Storage (SS)		
[11]	Attribute-Based Identity Management (ABIDM)		identity cryptography	SSL connections		MobiCloud Trust Manager Server (TMS)		MobiCloud Service/ Application Store	
[12]	ใช้รหัสจาก encrypted IMSI และตัวตนผู้ใช้	ใช้การรวมกันของคีย์เฉพาะและรหัสส่วนตัวของผู้ใช้	เก็บสิ่งระบุตัวตนของผู้เป็นเจ้าของเป็นความลับ		Advanced Encryption Standard (AES)		Cloud database	LBS applications	
[13]	**VO Manager**			SSH	VO Credential	decentralized internet	VO database	Web portal	โปรโตคอล3 ชนิด
[14]	Single Sign-on Access Token (SSAT)	{user's profile}$_{SPML}$						End-user Service portal	

IV. Cloud Storage

การประมวลผลแบบคลาวด์ แบ่งเป็นประเภทของระบบเป็นแบบขนานและแบบกระจาย ประกอบด้วยคอลเลกชั่นของคอมพิวเตอร์ที่เชื่อมต่อและระบบคอมพิวเตอร์เสมือนจริงที่เป็นแบบไดนามิก การนำเสนอแบบหนึ่งหรือมากกว่าทรัพยากรคอมพิวเตอร์แบบครบวงจรบนพื้นฐานบนการบริการข้อตกลงในการให้บริการด้านรักษาความปลอดภัย ระหว่างผู้ให้บริการและผู้รับบริการ

การเก็บรักษาบน Cloud แนวคิดใหม่ที่พัฒนามาจากแนวคิดของการประมวลผลแบบคลาวด์ ซึ่งระบบที่ใช้แอพพลิเคชั่นซอฟต์แวร์เพื่อให้การทำงานร่วมกันของอุปกรณ์จำนวนมากในการจัดเก็บข้อมูลโดยเทคโนโลยีแบบกระจายระบบแฟ้มและข้อมูลอื่นๆ ผ่านการบริการของแอพพลิเคชั่น

การจัดเก็บข้อมูลแบบประมวลผลบนคลาวด์ คือการที่เราเช่าพื้นที่จัดเก็บข้อมูลกับบริษัทผู้ให้บริการโดยรูปแบบของการให้บริการเรียกว่า Cloud Storage

รูปแบบของ Cloud Storage เกิดขึ้นนานแล้ว ตัวอย่างบริษัทผู้ให้บริการ Web Hosting ก็อาจจะจัดได้ว่าเป็นผู้ให้บริการ Cloud Storage ประเภทหนึ่ง จากที่การค้นคว้าข้อมูลบนอินเตอร์เน็ตและดูแนวโน้มของเทคโนโลยี แนวโน้มน่าจะมาจากคำว่า Web 2.0 Storage อย่างเว็บ community ที่มีบริการให้ผู้ใช้สามารถอัพโหลดรูปภาพ, วิดีโอ, ไฟล์เอกสาร, และไฟล์อื่นๆเพื่อแชร์กับบุคคลอื่น อย่างบริการจาก Flickr, Hi5, Picasa และ Youtube เป็นต้น และเมื่อ Web 2.0 ได้รับความนิยมระดับหนึ่ง บวกกับความต้องการพื้นที่เก็บข้อมูลของบุคคลธรรมดาที่มากขึ้น รวมทั้งองค์กรต่างๆต้องการลดต้นทุนในการจัดซื้อและดูแลทรัพย์สินของบริษัท และความต้องการพื้นที่จัดเก็บข้อมูลที่เลือกสรรขนาดได้ตามต้องการ

ตัวอย่าง รูปแบบของพื้นที่การจัดเก็บคลาวด์เป็นรูปแบบของการจัดเก็บข้อมูลแบบออนไลน์ผ่านเครือข่ายอินเตอร์เน็ต ที่เก็บข้อมูลไว้บนเซิร์ฟเวอร์เสมือนหลายพื้นที่ โดยทั่วไปผู้ใช้งานอาจจะมีการใช้งานได้หลายคน บริษัทผู้ให้บริการพื้นที่จัดเก็บข้อมูลขนาดใหญ่จะให้บริการเช่าพื้นที่รวมถึง Cloud

ด้วย Cloud มีประโยชน์มากในการจัดเก็บข้อมูล ผู้ให้บริการอาจจะมีการเก็บค่าบริการการจัดเก็บ การถ่ายโอนไฟล์

ประโยชน์ที่ได้จากการใช้ Cloud Storage

- สามารถเข้าถึงข้อมูลหรือไฟล์ ได้จากทุกที่ทุกเวลา ผ่านการเชื่อมต่ออินเตอร์เน็ต
- เลือกขนาดจัดเก็บข้อมูลได้ตามต้องการ และสามารถเพิ่มหรือลดขนาดในภายหลังได้
- ราคาถูกกว่าการลงทุนซื้ออุปกรณ์จัดเก็บข้อมูลจริง
- ไม่ต้องลงทุนและเสี่ยงในการดูแลอุปกรณ์จัดเก็บข้อมูลด้วยตนเอง
- ได้รับการบริการเสริม เช่น การสำรองข้อมูล, การรับประกันในกรณีข้อมูลสูญหาย และการให้บริการความช่วยเหลือตลอด 24 ชั่วโมง เป็นต้น

ความน่าเชื่อถือของ Cloud Storage

ผู้ให้บริการ Cloud Storage โดยส่วนใหญ่จะมีห้อง Data center สำหรับเป็นที่อยู่ของอุปกรณ์จัดเก็บข้อมูลและเซิร์ฟเวอร์หลายเครื่อง มีระบบรักษาความปลอดภัยที่ป้องกันการลักขโมยข้อมูล ทั้งระบบ Firewall และระบบล็อคห้อง Data Center ที่น่าเชื่อถือ และในห้อง Data Center มีระบบทำความเย็นให้กับอุปกรณ์ ทำให้ระบบทำงานได้ต่อเนื่องเป็นเวลานานและมีอายุการใช้งานที่ยืนยาว หลายเจ้าจะมีระบบสำรองไฟ บางบริษัทใช้เทคโนโลยีในการจัดเก็บข้อมูลที่มีความเร็วและน่าเชื่อถือสูง หลายบริษัทใช้เทคโนโลยีสำหรับสำรองข้อมูลไว้หลายชุดเพื่อป้องกันกรณีที่ข้อมูลสูญหาย บางบริษัทมีระบบซ้ำซ้อน (คัดลอก)ข้อมูลเดียวกันเก็บไว้หลายๆ data center (หลักการ Redundancy) ด้วยวัตถุประสงค์ในการสำรองข้อมูลและการเพิ่มความเร็วในการเข้าถึงข้อมูลจากพื้นที่ที่ใกล้เคียง และป้องกันเหตุการณ์ที่หากมี data center แห่งหนึ่งล่ม (เช่น ไฟไหม้หรือตึกถล่ม) ก็ยังมี data center ที่อื่นเก็บข้อมูลสำรองไว้อยู่และสามารถให้บริการได้อย่างต่อเนื่อง

อย่างไรก็ตาม คงไม่มีบริษัทไหนกล้ารับประกันความน่าเชื่อถือของ Cloud Storage ได้ถึง 100% โดยส่วนมากจะบอกว่าประกัน 99.9% – 99.9999% โดยความน่าเชื่อถือจะถูกอิงอยู่บนเอกสารข้อตกลงที่เรียกว่า Service-Level-Agreement หรือ SLA (ลองดูตัวอย่าง SLA ของ Amazon ผู้ให้บริการ Cloud Storage รายหนึ่ง) [17]

A New Feature on Cloud Storage

- มีหน้าเว็บหรือแอพพลิเคชันเป็นPortal จัดเตรียมไว้สำหรับเข้าถึงและจัดการ Cloud Storage
- สำหรับสนับสนุนการเข้าถึงและจัดการ Cloud Storage ผ่านโปรโตคอล REST
- สำหรับสนับสนุนการเข้าถึงและจัดการ Cloud Storage ผ่าน Web Services
- สนับสนุนการเมาท์ (mount) พื้นที่ของ Cloud Storage ให้สามารถเข้าถึงและจัดการผ่านไดเร็กทอรีหรือไดร์ฟบนคอมพิวเตอร์โลคอลได้เลย (ส่วนใหญ่ใช้โปรโตคอล WebDAV)

ผู้ให้บริการ Cloud Storage แต่ละผู้ให้บริการจะมีฟีเจอร์ของบริการแตกต่างกันไป

1. โครงสร้างพื้นฐานของการบริการ

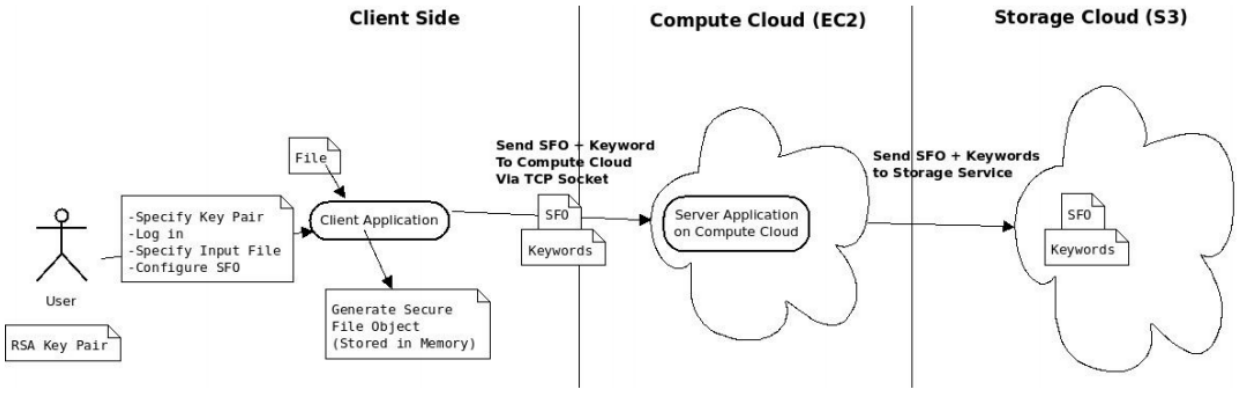
การจัดการ IPs มีการจัดการทรัพยากรขนาดใหญ่ การใช้งานเกี่ยวกับความจุเนื้อที่ และการประมวลผล โดยผ่านแบบจำลอง โดยที่จะสามารถแยกการปรับขนาดแบบไดนามิก ตามโครงสร้างของทรัพยากรตามกิจกรรมของระบบ ซึ่งเป็นโครงสร้างพื้นฐานของการบริการ

2. รูปแบบของการบริการ

ระบบของคลาวด์ สามารถเสนอรูปแบบ ที่เป็นโครงสร้างพื้นฐานแบบนามธรรมเสมือนจริง รูปแบบของซอฟต์แวร์ที่รันบน Thesizing กับฮาร์ดแวร์ที่ใช้บน Platform as Service (PaaS) เช่น Google Apps

A. สถาปัตยกรรมการบริการจัดเก็บคลาวด์คอมพิวติ้ง [18]

สถาปัตยกรรมของระบบประกอบด้วย Client อุปกรณ์สำหรับเข้าใช้งานคลาวด์คอมพิวติ้ง เช่น Mobile, Thin Client โดยที่ Services บริการต่างๆที่เปิดให้บริการบนคลาวด์คอมพิวติ้ง เช่น Web service, Application บริการ Software ต่างๆ ที่เปิดให้ใช้งานบนคลาวด์ โดยที่ผู้ใช้บริการไม่จำเป็นต้องลง Software ไว้บนเครื่องของตัวเอง อาจมีการใช้งานรวมกับ Services ด้วย แอพพลิเคชั่นจะเป็นตัวจัดการทั้งหมดด้านการรักษาความปลอดภัย



รูปที่ 20 สถาปัตยกรรมของระบบโดยรวม

Infrastructure โครงสร้างพื้นฐานที่รองรับกับระบบคลาวด์ โดยใช้ร่วมกับเทคโนโลยีเวอร์ชวลไลเซชั่น (Virtualization) Platform เลือกเทคโนโลยีที่จะนำมาใช้งาน โดยอาจจะเลือกจาก Open Source หรือ Open System ที่มีหลากหลายในท้องตลาด Storage เป็นปัจจัยหลักในการให้บริการ โดยอาจจะให้บริการพื้นที่จัดเก็บข้อมูล หรือรวมไปถึงการให้บริการด้านระบบฐานข้อมูลด้วย Standard ระบบคลาวด์เป็นระบบที่สร้างจาก Open Source หรือ Open System เป็นหลัก ควรเลือก standard ต่างๆที่สามารถปรับเปลี่ยนได้ง่าย คือการนำเอาซอฟต์แวร์ระบบที่รองรับการให้บริการคลาวด์คอมพิวติ้งโดยอาศัยฮาร์ดแวร์และซอฟต์แวร์มาทำงานร่วมกันให้บริการผ่านทางระบบอินเทอร์เน็ต สามารถรองรับกับความต้องการและปริมาณของผู้ใช้งานจำนวนมากๆ ได้ การรักษาความปลอดภัยดำเนินการบนข้อมูล รวมทั้งการบันทึก การดึงข้อมูลมาจากการบริการที่เก็บข้อมูล แอพพลิเคชั่นเซิร์ฟเวอร์ ดำเนินการประมวลผลที่เกี่ยวข้องในการจัดการการเข้ารหัส ประสิทธิภาพของการทำงาน ขนาดของข้อมูล โดยจะเกี่ยวข้องกับค่าใช้จ่ายในการรักษาความปลอดภัยของข้อมูล

A. Client

ไคลเอนต์จะรับผิดชอบสำหรับการดำเนินการเข้ารหัสลับทั้งหมด ที่จะกระทำบน SFO ผู้ใช้ล็อกลงในแอพพลิเคชั่นให้กับ RSA Keypairตามที่ระบุในแฟ้มการตั้งค่า รวมไปถึงการคำนวณ Math State Server ID ของผู้ใช้ระบบในนามแฝงภายในตัว keystoreและแป้นการเข้าถึงเก็บข้อมูลเมื่อผู้ใช้ถูกบันทึกไว้ใน พวกเขาสามารถทำได้จำนวนหนึ่งฟังก์ชันตามสิทธิการเข้าถึง ผู้ใช้ที่ มีสิทธิในการอ่านสามารถทำการดำเนินการดังต่อไปนี้:

- โหลด SFO จากการบริการที่เก็บข้อมูล
- การตรวจสอบความสอดคล้องของ SFO และข้อมูล
- ผู้ใช้รายชื่อและสิทธิ
- บันทึก SFO เป็นการบริการเก็บข้อมูล
- บันทึกเนื้อหา SFO ไปยังระบบแฟ้ม

การดำเนินงานเท่านั้นที่อาจดูเหมือนว่าจะกลายมาเป็น "บันทึกการSFO เพื่อการบริการที่เก็บข้อมูล" ผู้ใช้เหล่านี้สามารถดำเนินการนี้การดำเนินการเนื่องจากไม่อนุญาตให้มีการเปลี่ยนแปลงเนื้อหา ดังนั้นเป็นเพียงแค่อัพโหลด SFO อย่างเดียว ได้ดาวน์โหลด ผู้ใช้ที่ มีสิทธิการเข้าถึงการเขียนที่สามารถทำการดำเนินงานผู้อ่านรวมทั้งการดำเนินการดังต่อไปนี้:

- การปรับเปลี่ยนเนื้อหา
- สร้างแบบแยกย่อยข้อมูลที่เข้ารหัสลับ

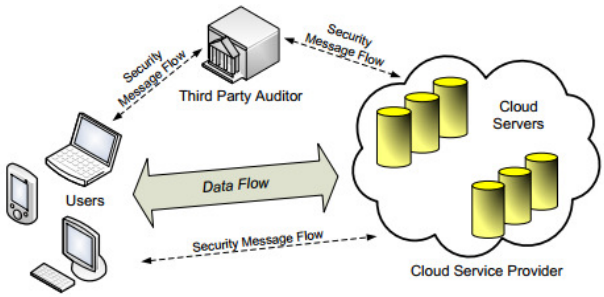
เจ้าของแฟ้มมีสิทธิในการดำเนินงานทั้งหมดของผู้ใช้ที่ก่อนหน้านี้สองคนรวมทั้งการดำเนินการดังต่อไปนี้:

- สร้าง SFO
- เพิ่มผู้ใช้
- ปรับเปลี่ยนสิทธิ์ของผู้ใช้
- การเอาผู้ใช้ออก
- สร้างแยกย่อย SFO
- สร้างรายการคำสำคัญที่มีความปลอดภัย
- มุมมอง / แก้ไขคำสำคัญ
- สร้างความสามารถในการค้นหา

แอพลิเคชันไคลเอนต์กับคำสั่งระบบแฟ้ม คำสั่งคือ:ย้าย รับ ลบ รายการ ค้นหา

B.แอพพลิเคชั่นเซิร์ฟเวอร์

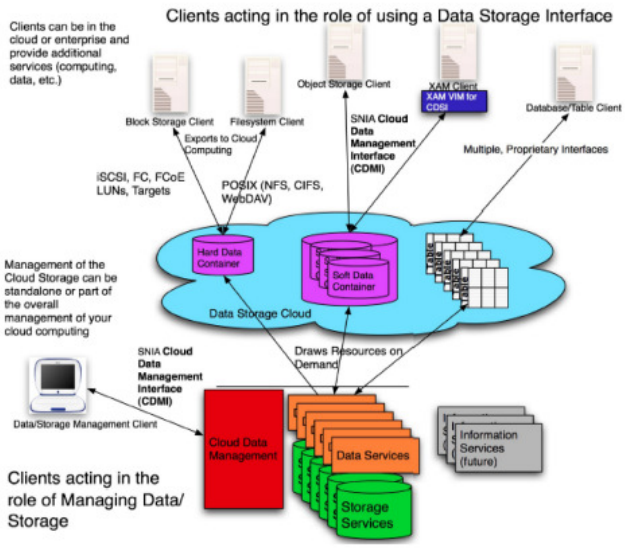
แอพลิเคชันของเซิร์ฟเวอร์ถูกใช้เพื่อจัดการการร้องขอของไคลเอ็นต์ทั้งหมดและทำงานในคลาวด์คอมพิวติ้งโปรแกรมประยุกต์นี้ถูกใช้ในการไคลเอ็นต์การรับรองความถูกต้อง และให้การเชื่อมต่อที่ปลอดภัยระหว่างไคลเอนต์และการบริการที่เก็บข้อมูล การประมวลผลจำนวนมากคือ เมื่อมีการตอบสนองในการค้นหาแบบสอบถามร้องขอบริการก็เพียงรับคำขอและ Pushes เหล่านั้นส่งต่อไปยังบริการเก็บข้อมูล



รูปที่ 21 สถาปัตยกรรมการบริการพื้นที่การจัดเก็บข้อมูล

B. แบบจำลองอ้างถึงการจัดเก็บข้อมูลแบบคลาวด์

Cloud Storage มีส่วนที่เกี่ยวข้องในการจัดเก็บข้อมูล จะพูดถึงการบริการและการใช้งานความจุ โดยอาศัยความง่ายต่อการใช้งาน อินเตอร์เฟสมีความสำคัญสำหรับการใช้งานการจัดเก็บแบบคลาวด์ ยิ่งกรณีผ่านอุปกรณ์สมาร์ทโฟนแล้วนั้น การออกแบบก็จำเป็นมากด้วยเช่นกัน แบบจำลองสร้างขึ้นและเผยแพร่โดยการเก็บข้อมูลผ่านทางเครือข่าย แสดงข้อมูลหลายชนิดของอินเตอร์การจัดเก็บแบบคลาวด์ การบริการและการนำข้อมูลไปใช้กับข้อมูลแต่ละองค์ประกอบ ขึ้นกับการจัดเก็บข้อมูล metadata ระบบฐานข้อมูล ระบุข้อมูลที่ต้องการ โดยใช้ข้อมูลแต่ละองค์ประกอบ



รูปที่ 22 แบบจำลองอ้างถึงการจัดเก็บข้อมูลแบบคลาวด์

C. ข้อกำหนดของระบบ

ก่อนที่จะออกแบบระบบ เป็นสิ่งจำเป็นในการพิจารณาความต้องการด้านความปลอดภัยสำหรับระบบนี้ การรักษาความปลอดภัยจำเป็นต้องใช้ข้อจำกัด

จะแสดงอยู่ในตารางที่ ระบบจำเป็นเพื่อให้แน่ใจว่าข้อมูลถูกจัดเก็บเป็นความลับ ซึ่งหมายความ ว่า เฉพาะผู้ใช้ที่ให้สิทธิสามารถเข้าถึงเนื้อหาที่ถูกเข้ารหัสไว้ ระบบต้องการให้แน่ใจว่า เป็นรักษาความสมบูรณ์ของแฟ้มและการตรวจสอบใด ๆการเปลี่ยนแปลงไม่ได้รับอนุญาต ด้วยระบบแฟ้มใด ๆ ต้องมีกลไกในเพื่อให้แน่ใจว่า แฟ้มสามารถถูกใช้ร่วมกันในหมู่ผู้ใช้งาน มีสิทธิในการให้ผู้ใช้ มีสิทธิการเข้าถึง ระบบนอกจากนี้ควรจะเอาสิทธิ์ของผู้ใช้ การกรองผ่านข้อมูลที่เข้ารหัสเป็นปัญหา ดังนั้นมันเป็นความจำเป็นในการให้ผู้ใช้สามารถค้นหาผ่านการเข้ารหัสเนื้อหา และการส่งคืนผลลัพธ์ที่ตรงกับแบบสอบถามระบบ นอกจากนี้ควรสามารถกู้คืนจากคู่คีย์ที่ถูกโจมตีระบบต้องแน่ใจว่า โปรแกรมประยุกต์ไคลเอ็นต์ที่ถูกต้องเท่านั้นสามารถเชื่อมต่อกับเซิร์ฟเวอร์

ตารางที่ 4 แสดงความต้องการของระบบการบริการพื้นที่การจัดเก็บคลาวด์

การรักษาความลับ	โดยให้แน่ใจว่าข้อมูลจะต้องถูกจัดเก็บเป็นความลับ
ความสอดคล้อง	ความสมบูรณ์ของข้อมูลเพื่อให้แน่ใจได้ว่าข้อมูลมันไม่ถูกแทรกแซง
การใช้แฟ้มร่วมกัน	ผู้ใช้งานแฟ้มร่วมกัน สามารถยกเลิกการใช้งานได้
ความสามารถในการค้นหา	ให้แน่ใจว่ามีความสามารถในการค้นหาภายในข้อมูลเข้ารหัสลับ
คู่คีย์ที่ถูกบุกรุก	ระบบสามารถกู้คืนจากคู่คีย์ที่ถูกบุกรุก ที่ละเมิดได้
ควบคุมการเข้าถึง	ตรวจสอบควบคุมการเข้าถึงไปยังเซิร์ฟเวอร์

D. โครงสร้างข้อมูลของระบบ

A. ความปลอดภัยแฟ้มวัตถุ

การรักษาความปลอดภัยของไฟล์ (SFO) คือ การจัดเก็บข้อมูลอย่างปลอดภัยในบริการการจัดเก็บข้อมูล การดำเนินการทั้งหมดดำเนินการบนคอนเทนเนอร์นี้ได้รับการจัดการบนไคลเอ็นต์ใด ๆ การเปลี่ยนแปลงที่ไม่ได้รับอนุญาตหรือการปรับเปลี่ยนบนคอนเทนเนอร์นี้จะถูกตรวจพบที่ไคลเอ็นต์เพื่อตอบสนองความต้องการที่ระบุไว้ในส่วนที่โครงสร้างระบบข้อมูล การ SFO ต้องมีหมายเลขของเขตข้อมูล เขตข้อมูล จำเป็นต้องมี (แสดงในรูปที่ กก) แต่ละผู้ใช้ของระบบนี้จำเป็นต้องเป็น Public/Private Key-คู่ช่วยให้สำหรับการบอกไม่เป็นรักษาความสมบูรณ์ของข้อมูลและ SFO โดยข้อมูลเข้ารหัสลับและการรักษาความปลอดภัยแฟ้มวัตถุ digests การแยกย่อยการรักษาความปลอดภัยแฟ้มวัตถุสามารถสร้างเท่านั้นโดยเจ้าของแฟ้ม ขณะเข้ารหัสลับมีการแยกย่อยข้อมูลถูกสร้างขึ้น โดยผู้ใช้ใด ๆ ที่มีการเข้าถึงแบบเขียนการแยกย่อยของ SFO เป็นแบบเซ็นชื่อ (เซ็นกับเจ้าของคีย์ส่วนตัว) ของเขตข้อมูลทั้งหมดซึ่งเจ้าของเท่านั้นที่สามารถปรับเปลี่ยน จำแนกข้อมูลเข้ารหัสลับมีเพียงแค่เซ็นชื่อของเขตข้อมูลของข้อมูลที่เข้ารหัสลับ การเซ็นชื่อ โดยล่าสุดเมื่อผู้ใช้คีย์ส่วนตัว เขตข้อมูลคำสำคัญที่เข้ารหัสลับเป็นรายการของคำสำคัญที่เข้ารหัสลับโดยใช้อัลกอริทึมการเข้ารหัสลับ symmetric

สิทธิ์ของผู้ใช้จะถูกเก็บรักษาโดยใช้สองรายการ ได้แก่การอ่านรายชื่อและรายการของคีย์สาธารณะ รายการที่อ่านเป็นเพียงการการแปรรหัสผู้ใช้กับคีย์การเข้ารหัสลับแฟ้มเข้ารหัสลับ(FEK) ถูกเข้ารหัสลับ ด้วยคีย์สาธารณะของผู้ใช้นี้ช่วยให้ผู้ใช้สามารถเรียกใช้ FEK การ โดยการหาค่าID ของผู้ใช้จากรายการและการถอดรหัสลับกับการสอดคล้องคีย์ส่วนตัวรายการคีย์สาธารณะจะใช้สำหรับการดำเนินงาน

ความสอดคล้องของการตรวจสอบเขียน Access และคีย์เพิกถอน คีย์สาธารณะรายการแผนที่ Id ของผู้ใช้ไปทูเปิล เมื่อผู้ใช้ปรับเปลี่ยนเนื้อหาเข้ารหัสลับ สร้างผู้ใช้ที่มีจำแนกข้อมูลที่เข้ารหัสลับซึ่งได้รับการรับรองกับผู้ใช้ของส่วนตัวคีย์ นอกจากนี้ผู้ใช้แล้วตั้งล่าสุดปรับเปลี่ยนฟิลด์ ID ผู้ใช้กับรหัสผู้ใช้ของเขาเอง ต่อมาผู้ใช้สามารถแล้วค้นหาล่าสุดแก้ไขผู้ใช้ ID สาธารณะคีย์ในรายการคีย์สาธารณะและการใช้ที่ตรวจสอบความสมบูรณ์ของการแยกย่อยการเข้ารหัสลับข้อมูลรายการคีย์สาธารณะจะใช้ในการรักษารายการของผู้ใช้ที่มีสิทธิในการเข้าถึงแบบเขียน ทำ โดยการตั้งค่าเขตข้อมูล ถ้ามีการตั้งค่าของผู้ใช้เขียนธง ซึ่งหมายความ ว่า ผู้ใช้มีสิทธิ์ในการปรับเปลี่ยนเนื้อหา ถ้าผู้ใช้ไม่ได้รับอนุญาตที่มีการปรับเปลี่ยนเนื้อหาแล้ว transgression นี้จะถูกตรวจพบโดยผู้ใช้ตามมาคีย์เพิกถอนตาม FEK การใหม่ในการสร้าง และโดยใช้คีย์สาธารณะที่ถูกเก็บไว้ในรายชื่อคีย์สาธารณะเพื่อสร้างรายการอ่านใหม่

1) ผู้ใช้ที่เป็นอันตราย การออกแบบของระบบที่ผู้ใช้เชื่อถือได้ เช่น ถ้าเจ้าของมอบให้แก่ผู้ใช้ผู้ใช้จะไม่เป็นอันตราย อย่างไรก็ตาม การวัดควรอยู่จะอยู่ในที่ระบบสามารถตรวจสอบกิจกรรมใด ๆ ที่อาจเป็นอันตรายได้ถ้าผู้ใช้ไม่อนุญาตให้เข้าถึงแบบอ่านได้อย่างเดียว ผู้ใช้สามารถปรับเปลี่ยนการเข้าถึงเนื้อหา สร้างแยกย่อยข้อมูลการเข้ารหัสลับ และการตั้งค่าล่าสุดฟิลด์ ID ผู้ใช้ที่ปรับเปลี่ยน อย่างไรก็ตาม เมื่อผู้ใช้ถัดไปโหลดแฟ้ม ผู้ใช้จะทำการตรวจสอบความสมบูรณ์ของข้อมูลดังกล่าวการตรวจสอบความสมบูรณ์ของสามารถทำได้ ด้วยการมองหาคีย์สาธารณะของการปรับเปลี่ยนครั้งล่าสุดผู้ใช้ เนื่องจากไม่มีการตั้งค่านี้ค่าสถานะ IsWriterการระบบจะสร้างข้อผิดพลาดเนื่องจากผู้ที่ไม่ได้รับอนุญาตมีการปรับเปลี่ยนเนื้อหาหากผู้ใช้เปิดอ่านเพิ่มสิทธิในการเขียนแล้วการเปลี่ยนแปลงนี้จะตรวจพบ โดยผู้ใช้ตามมาเนื่องจากผู้ใช้ที่เป็นอันตรายไม่สามารถสร้างการจำแนกวัตถุแฟ้มการรักษาความปลอดภัย นี้จะแจ้งผู้ใช้ที่ตามมาว่า มีการไม่ได้รับอนุญาตการเปลี่ยนแปลงไปยังรายการสิทธิ์ของผู้ใช้

B. ความปลอดภัยของไฟล์

การรักษาความปลอดภัยแฟ้มวัตถุ (คำสำคัญ SFO) คือใช้ในการเก็บคำที่มีความปลอดภัยตามที่สร้างขึ้นโดยการเจ้าของ สำหรับทุก ๆ SFO ที่เก็บไว้ในเครื่องบริการที่เก็บข้อมูล มีข้อสำคัญ SFO แนบแฟ้ม มีใช้แฟ้มเหล่านี้โดยแอพลิเคชันเซิร์ฟเวอร์จะทำการเข้ารหัสลับการดำเนินการที่จำเป็นสำหรับการเข้ารหัสลับที่สามารถค้นหาได้เป็นรายละเอียดในส่วน V-E.คำสำคัญของ SFO สามเขตข้อมูลเป็นดังนี้

- สุ่มบิตสตริง
- รายการคำสำคัญที่เข้ารหัสลับ

C. ข้อความเครือข่าย

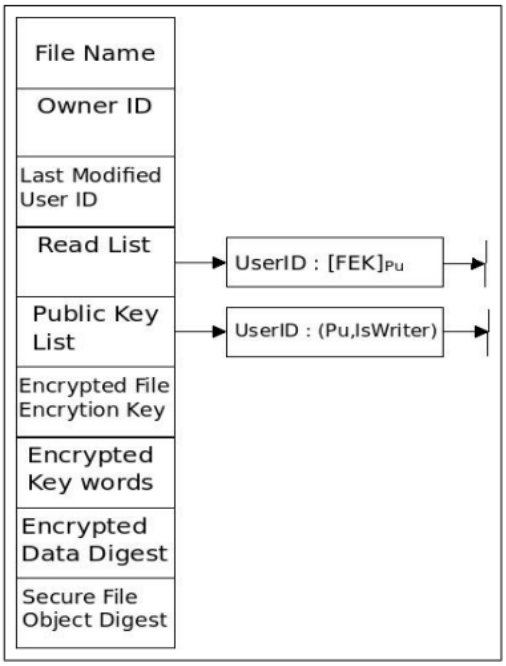
ระบบนี้ใช้ข้อความของเครือข่ายสองประเภท การร้องขอการรับรองความถูกต้องและข้อความโทเค็นการรับรองความถูกต้องถูกใช้โดยไคลเอนต์อย่างปลอดภัยส่งผ่านข้อมูลข้ามเครือข่ายไปยังเซิร์ฟเวอร์ เขตข้อมูลในโทเค็นการรับรองความถูกต้องเป็นดังต่อไปนี้

- Key / คอนเทนเนอร์
- Nonce ที่เข้ารหัสลับ
- Hash

เขตข้อมูลเหล่านี้จะถูกใช้ โดยระบบการในการรับรองความถูกต้อง กระบวนการสร้างเซสชันคีย์ คีย์ / ฟิลด์คอนเทนเนอร์ใช้ในการขนส่งคีย์การเข้ารหัสลับเช่นเดียวกันข้อมูลเช่น Hash คีย์การเข้าถึง Nonce เข้ารหัสลับใช้สำหรับการใช้เป็นเซิร์ฟเวอร์การรับรองความถูกต้อง ที่แฮฟิลด์เป็นการแยกย่อยของข้อความ ข้อความร้องขอถูกใช้สำหรับการดำเนินงานของระบบแฟ้มของระบบ ข้อความนี้ถูกส่งจากไคลเอนต์ไปยังเซิร์ฟเวอร์สั่งเซิร์ฟเวอร์การดำเนินการใดเพื่อดำเนินการ ที่เขตข้อมูลของข้อความนี้มีดังต่อไปนี้:

- คอนเทนเนอร์
- ชนิดของข้อความ
- การแยกย่อย

เขตของข้อมูลถูกใช้ผ่านใด ๆ พร้อมกับคำขอ เช่น ความสามารถในการค้นหา หรือ Id ของฟิลด์ เขตข้อมูลนิดข้อความบอกให้เซิร์ฟเวอร์ที่เป็นชนิดของการร้องขอที่ถูกส่งและแยกย่อยที่ใช้ในการรักษาความสมบูรณ์ของรายละเอียดของการดำเนินการเหล่านี้และการใช้ได้ของข้อความที่ร้องขอ



รูปที่ 23 แสดงการเข้ารหัส

E. ภาพรวมของ Cloud Storage

ตารางที่ 5 แสดงภาพรวมการเปรียบเทียบของสถาปัตยกรรมการบริการจัดเก็บคลาวด์คอมพิวติ้ง

	[17]	[18]	[19]	[20]	[21]
Mobile Client	✓	✓	✓	✓	✓
Server	✓	✓	✓	✓*	✓
Application	✓	✓	✓**	✓	✓
Service	✓			✓	✓
Infrastructure		✓	✓		✓
High Level***	✓	✓			

* Mirror server **แอพพลิเคชั่นที่ไม่มีการใช้งานร่วมกับ services *** สถาปัตยกรรมพื้นฐานของกรอบการนำเสนอและวิธีการโต้ตอบของส่วนประกอบของกันและกัน

ตารางที่ 6 แสดงการเปรียบเทียบแบบจำลองอ้างถึงการจัดเก็บข้อมูลแบบคลาวด์

	[17]	[18]	[19]	[20]	[21]
การรักษาความลับ	✓	✓	✓	✓	
ความสอดคล้อง	✓		✓	✓	✓
การใช้แฟ้มร่วมกัน			✓	✓	✓
ความสามารถในการค้นหา			✓	✓	✓
คู่คีย์ที่ถูกบุกรุก	✓	✓	✓	✓	✓
ควบคุมการเข้าถึง	✓	✓	✓	✓	
การปกป้องข้อมูลที่รับเข้าส่งออกด้วยการนำข้อมูลมาเข้ารหัสพิเศษ	✓	✓			

ผลการเปรียบเทียบแบบจำลองและสถาปัตยกรรมของ Cloud Storag

ภาพรวมการเปรียบเทียบสถาปัตยกรรมการบริการจัดเก็บคลาวด์คอมพิวติ้งได้แบ่งตามส่วนประกอบที่มีการพูดถึงแต่ละงานวิจัยที่เกี่ยวข้องกับสถาปัตยกรรมการบริการคลาวด์คอมพิวติ้ง ได้ดังนี้ 1. Client เป็นส่วนประกอบในแต่ละงานวิจัยพูดถึง ในส่วนนี้ใช้ Mobile phone เป็น Client เครื่องลูกข่ายที่ร้องขอการใช้บริการจากเครื่องแม่ข่าย 2.Server เครื่องแม่ข่ายสำหรับพื้นที่ในการจัดเก็บข้อมูล โดย งานวิจัยที่ [20] ใช้ Server แบบ Mirror Server3. Appilcation ใช้ในการเชื่อมต่อกับ Server ทำงานร่วมกับ services งานวิจัยที่ [20] กล่าวถึงแอพพลิเคชั่นที่ไม่มีการใช้งานร่วมกับ services4.Serviecs การบริการพื้นที่จัดเก็บจากผู้ให้บริการ [18] กล่าวถึง Amazon, Google, Salesforce, IBM, Microsoft, and Sun Microsystems [21] Amazon 5. Infrastructure กล่าวถึงในงานวิจัยที่ [18], [19], [21] 6.High Level อธิบายถึงสถาปัตยกรรมพื้นฐานของกรอบการนำเสนอและวิธีการโต้ตอบของส่วนประกอบของกันและกันในงานวิจัยที่ [18] มีการใช้การทดสอบแบบ High Level Architecture

การอ้างถึงการเปรียบเทียบของแบบจำลอง การใช้แฟ้มร่วมกันหรือการแชร์ไฟล์ยังเป็นข้อจำกัดบางงานวิจัยที่ไม่ได้มีการกล่าวถึง ประสิทธิภาพของแบบจำลองเกี่ยวเนื่องกับความสามารถในการค้นหาข้อมูล โดยเรื่องที่น่าสนใจในการศึกษาเพื่อการพัฒนาศึกษาวิจัยต่อไป บางงานวิจัยไม่ได้กล่าวถึง การปกป้องข้อมูลที่รับเข้า – ส่งออกด้วยการนำข้อมูลมาเข้ารหัสพิเศษ (SSL) ส่วนด้านความปลอดภัยอื่นๆ การเข้ารหัส การคู่คีย์ การควบคุมการเข้าถึงเป็นพื้นฐานด้านความปลอดภัยของการใช้งานพื้นที่การจัดเก็บอยู่แล้ว โดยงานวิจัยที่ [20], [19] หากมีการศึกษาเพิ่มเติมจะเป็นแนวทางในการพัฒนา Secure Cloud Storage ได้มายิ่งขึ้น

V. Authentication

เป็นวิธีการตรวจสอบผู้ที่มาใช้งานระบบเครือข่ายอินเทอร์เน็ตรวมถึงการให้บริการการประมวลผลแบบคลาวด์บนอุปกรณ์เคลื่อนที่ อย่างโทรศัพท์มือถือ แท็บเล็ตหรืออุปกรณ์อื่นๆ โดยระบบจะทำการตรวจสอบจาก username และ password ว่าถูกต้องหรือไม่**จุดประสงค์หลัก**ของการ Authentication คือพิสูจน์ตัวบุคคลว่าคน ๆ นั้นที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตคือใคร พร้อมทั้งทำการตรวจสอบสิทธิ์ว่าผู้ใช้งานระบบเครือข่าย

อินเทอร์เน็ตนั้นมีสิทธิ์ใช้ได้นานมากน้อยเพียงใดและสามารถ upload หรือ download ได้ด้วยความเร็วเท่าใด ซึ่งระบบนั้นจะทำการตัดผู้ใช้ออกไปจากการให้บริการทันทีที่เวลาหมด อีกทั้งยังสามารถกำหนดเวลาและความเร็วได้ตามความเหมาะสมด้วย ต่อจากนั้นจะทำการบันทึกข้อมูลการใช้งานระบบเครือข่ายอินเทอร์เน็ตหรือระบบ Cloud Mobile ซึ่งจุดประสงค์หลักของขบวนการนี้เพื่อรายงานการใช้ระบบเครือข่ายอินเทอร์เน็ตและ Cloud Mobile พร้อมทำการยืนยันบันทึกข้อมูลในการใช้งานระบบเครือข่ายอินเทอร์เน็ตและ Cloud Mobileไว้อย่างละเอียดโดยสามารถทำรายงานสรุปและสถิติต่างๆ ได้ตามความต้องการ

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms) สามารถแบ่งออกได้เป็น 3 คุณลักษณะคือ

1. สิ่งที่คุณมี (Possession factor) เช่น กุญแจหรือเครดิตการ์ด เป็นต้น หรือภาษาอังกฤษเรียกว่า something you have (for example, your house keys)
2. สิ่งที่คุณรู้ (Knowledge factor) เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs) เป็นต้นหรือภาษาอังกฤษเรียกว่าsomething you know (for example, your password)
3. สิ่งที่คุณเป็น (Biometric factor) เช่น ลายนิ้วมือ รูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns) เป็นต้นหรือภาษาอังกฤษเรียกว่า something you are (for example, your fingerprints)

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ตัวอย่างเช่น สิ่งที่คุณมี (Possession factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

ดังนั้นจึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (multi-factor authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATMเป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูลซึ่งการพิสูจน์ตัวตน (Authentication) ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

1. การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใครเช่น ชื่อผู้ใช้ (username)
2. การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

จากเหตุผลข้างต้น Authentication ก็เป็นส่วนที่สำคัญมากสำหรับการใช้งานระบบเครือข่ายอินเทอร์เน็ตและระบบ Cloud Mobileในปัจจุบัน ดังนั้น เราจึงขออธิบายลักษณะที่สำคัญของงานวิจัย แต่ละเรื่องพร้อมเปรียบเทียบข้อดีข้อเสียที่เกิดขึ้น ทั้งนี้แสดงให้เห็นถึงการพิสูจน์ตัวตนในรูปแบบต่างๆ ที่แต่ละงานวิจัยได้นำมาใช้ ตามลำดับ

A. Multimodal Biometric Authentication using Teeth Image and Voice in Mobile Environment [22]

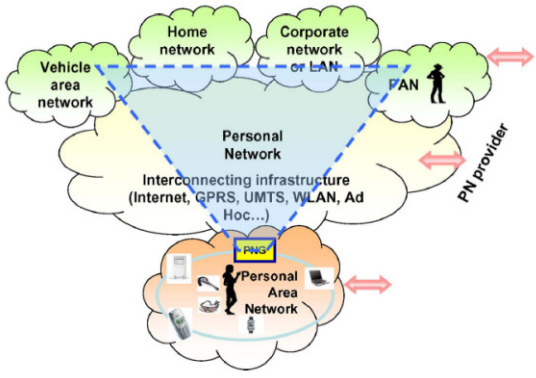
งานวิจัยนี้กล่าวถึงการป้องกันการโจรกรรมและการสูญเสียของข้อมูลในโทรศัพท์มือถือโดยมีวิธีการตรวจสอบที่สำคัญคือการใช้ภาพฟันและเสียง ซึ่งเป็นลักษณะหนึ่งของการพิสูจน์ตัวตน โดยงานวิจัยนี้นักวิจัยได้นำค่าถ่วงน้ำหนักในการวัดค่าความถูกต้อง ซึ่งได้นำกลุ่มตัวอย่างภาพฟันจำนวน1,000 ภาพ และตัวอย่างเสียงที่ได้มาจำนวน 50 คน ผลการทดลองได้ค่า EER เท่ากับ 2.13% ขั้นตอนการตรวจสอบและการดำเนินการจะใช้วิธี 2D-DCT และ EHMM ตามลำดับ ซึ่ง 2D-DCT คือ การแปลงโคไซน์ไม่ต่อเนื่อง 2 มิติ นอกจากนี้ยังตรวจสอบเสียงโดยใช้ลักษณะการทำงานร่วมกันของ MFCC และอัลกอริทึม GMM นอกจากนี้ ผู้วิจัยได้นำค่าที่ได้จากอัลกอริทึมองภาพฟันและเสียง มารวมกันโดยได้ค่าผลการทดลองจากการทดสอบภาพฟันเท่ากับ 6.42 % และค่าการทดสอบเสียงเท่ากับ 6.24% ทำให้ได้ค่าการวิเคราะห์สุดท้ายเท่ากับ 2.13% ซึ่งถือว่าการยืนยันตัวตนโดยวิธีนี้เกิดประสิทธิภาพมากขึ้น นอกจากนี้ผู้วิจัยได้ศึกษาและทดสอบตัวแปรเสียงให้เกิดประสิทธิภาพมากขึ้นและยังหาวิธีการยืนยันตัวบุคคลโดยวิธีอื่นๆ อีกด้วย

B. Person Authentication using Face, Teeth and Voice Modalities for Mobile Device Security [23]

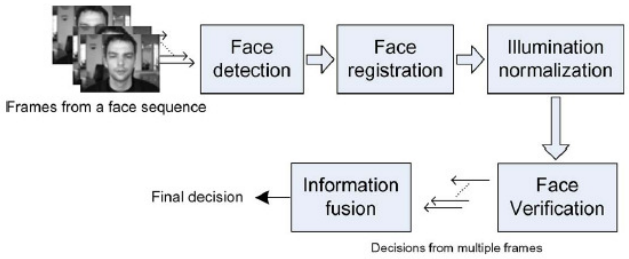
งานวิจัยนี้ได้กล่าวถึงการยืนยันตัวบุคคลโดยใช้ใบหน้า รูปฟัน และรังสีเสียง ในการเข้าใช้งานบนโทรศัพท์มือถือ โดยจะใช้เทคนิค การบวกค่าน้ำหนัก K-NN และการแยะแยะเสียงแล้วทำการประเมินประสิทธิภาพ ซึ่งในงานวิจัยนี้ได้นำตัวอย่างจำนวน 1,000 ตัวอย่าง ใช้คนจำนวน 50 คน โดย 1 คนต่อ 20 ตัวอย่าง ผลการทดสอบได้ค่าความผิดพลาดเพียง 1.64% 4.70% 3.06% 1.98% ซึ่งถือเกิดข้อผิดพลาดน้อยมากในการตรวจสอบ งานวิจัยนี้ได้แสดงถึงประสิทธิภาพมากขึ้นเพราะได้นำลักษณะของบุคคล ทั้งรูปหน้า รูปฟัน และเสียงในการยืนยันตัวบุคคล ทำให้การป้องกันการโจรกรรมหรือบุกรุกจากผู้ไม่ประสงค์ดีมาดักจับข้อมูลในเครือข่ายโทรศัพท์มือถือ เกิดประสิทธิภาพมากยิ่งขึ้น

C. Biometric Authentication System on Mobile Personal Devices [24]

งานวิจัยนี้ได้นำเทคนิคการจดจำใบหน้ามาใช้การในการพิสูจน์ตัวตนเพื่อให้สามารถเข้าใช้งานในเครือข่ายมือถือได้ โดยนำตัวบุคคลกับเครือข่ายมาใช้ในการยืนยัน ซึ่งงานวิจัยนี้ใช้วิธีการตรวจหาใบหน้า ลงทะเบียนใบหน้า การฟื้นฟูใบหน้า เพื่อเชื่อมโยงความปลอดภัยระหว่างตัวบุคคลและเครือข่ายในอุปกรณ์มือถือส่วนบุคคล



รูปที่ 24 แสดงถึงเครือข่าย Personal Network

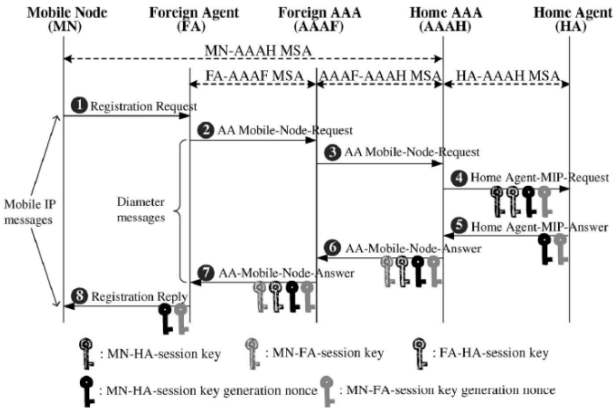


รูปที่ 25 แสดงขั้นตอนการตรวจสอบใบหน้า

ผลการทดลองดังกล่าวทำให้ได้ค่าความผิดพลาดเพียง 2% ภายใต้ประสิทธิภาพของอุปกรณ์ที่ต่ำและค่าใช้จ่ายของระบบสูงมาก ซึ่งก็ถือได้ว่าเกิดประสิทธิภาพในการยืนยันตัวบุคคลและความปลอดภัยในการเข้าถึงข้อมูลมากขึ้น

D. Modeling Key Caching for Mobile IP Authentication, Authorization and Accounting (AAA) Services [25]

งานวิจัยนี้เป็นการสร้างแบบจำลองเพื่อเป็นกุญแจในกระบวนการ AAA (Authentication, Authorization and Accounting) ซึ่งเป็นกลุ่มของกระบวนการที่จำเป็นต่อการให้บริการอินเตอร์เน็ตผ่านเครือข่ายไร้สายซึ่งจำเป็นที่จะต้องมีระบบที่มีประสิทธิภาพและปลอดภัยรองรับการทำงาน อีกทั้งมีบุคลากรที่มีความรู้และประสบการณ์ในการดูแลและบริหารจัดการระบบ



รูปที่ 26 แสดงการไหลของข้อความสำหรับกระบวนการ AAA ในมือถือ

ในงานวิจัยนี้ ได้เสนอแบบจำลองการวิเคราะห์และดำเนินการจำลองเพื่อการศึกษาประสิทธิภาพของแคชคีย์กลไกสำหรับขั้นตอนการตรวจสอบ IP ของโทรศัพท์มือถือในแง่ของที่คาดการณ์จำนวน E[N] ของ retrievals-คีย์การตั้งค่าเซสชั่นจาก AAAH (เมื่อ theMN อยู่ในพื้นที่บริการของ AAAเซิร์ฟเวอร์) ปริมาณการใช้แบนด์วิดธ์รวมวัสดุ C(K) สำหรับข้อความแลกเปลี่ยนและแฝงสำหรับการเคลื่อนไหวของ MN การศึกษาในงานวิจัยนี้ทำให้ค่าสังเกตที่สาม

1) เพิ่มขนาดแคชที่ K สามารถลดการคาดว่าตัวเลข E [N] ของ retrievals-คีย์การตั้งค่าเซสชั่นจากAAAH และเวลาแฝง averaged โอน L(K) เมื่อMN เป็น SDA เมื่อมีขนาดของแคชใหญ่พอ การปรับปรุงไม่สำคัญ

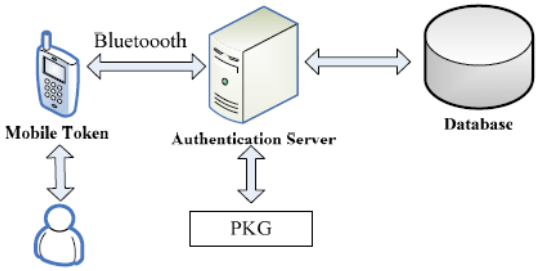
2) ปริมาณค่าใช้จ่ายการใช้แบนด์วิดธ์ C(K) สำหรับ AKC ด้วยขนาดแคชK เป็นเส้นโค้งเว้า นั่นคือ เป็นการเพิ่ม KC(K) ลดลงอย่างรวดเร็ว และจากนั้นเพิ่มขึ้นเล็กน้อยมีค่า K ที่ลด C(K) เหมาะสมที่สุด

3) ประสิทธิภาพการทำงานของ C(K) ความเป็นอิสระของการแจกแจงเวลา

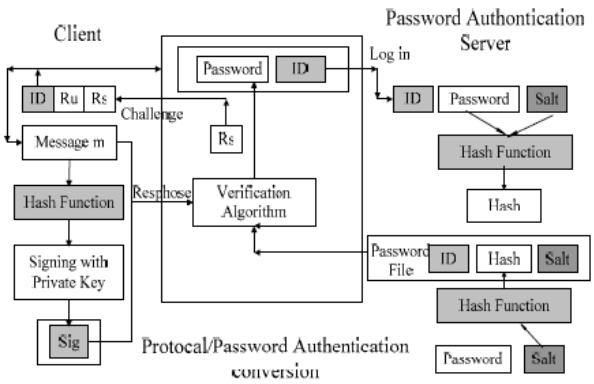
การศึกษากลไกการ AKC ด้วยขนาดแคชK แนะนำK ต้องปรับตามปริมาณการใช้งานการรับรองความถูกต้องดังนั้นต้นทุนของ C(K) สามารถจะลดลง จากนั้นได้นำเสนออัลกอริธึม K เลือกอัตโนมัติเลือกแบบไดนามิกค่าของ K ตามประสิทธิภาพของ C(K) การศึกษาในงานวิจัยนี้แสดงว่า K-เลือกอัตโนมัติอัลกอริทึมระบุค่าที่มีความเหมาะสมของ K ในการได้อย่างมีประสิทธิภาพลดปริมาณการใช้แบนด์วิดธ์ซึ่งได้จำลองวิเคราะห์สำหรับคีย์แคชยังสามารถขยายไปยังเครือข่ายบางอื่นๆ เช่นข่าย IEEE 802.11rการวิเคราะห์ประสิทธิภาพการทำงานที่เสร็จสมบูรณ์แล้วสำหรับมือถือ IP AAA คีย์และการศึกษานี้ยังถือได้ว่าเป็นงานวิจัยแรกที่ได้แก้ไขปัญหานี้ให้เกิดประสิทธิภาพมากยิ่งขึ้น

E. An identity Authentication System Basedon Mobile Phone Token [26]

งานวิจัยนี้เป็นการตรวจสอบรหัสประจำตัวบนเครือข่ายโทรศัพท์มือถือ ซึ่ง Authentication เป็นกลไกการสร้างการพิสูจน์ของผู้ใช้อีเมล์ ไม่สามารถรับรองความถูกต้องของรหัสผ่านเดิมได้ และไม่มีความปลอดภัยเพียงพอสำหรับข้อมูลปัญหาไม่สามารถแก้ไขได้ โดยการใช้โทเค็นรับรองความถูกต้องแต่เป็นระบบรับรองความถูกต้องใหม่ โดยเฉพาะอย่างยิ่งในการควบคุมการเข้าถึงระบบที่ได้รับอนุญาต ในงานวิจัยนี้ เราได้นำเสนอโทเค็นใหม่ซึ่งสามารถรวมอย่างใกล้ชิดกับระบบรับรองความถูกต้องแบบดั้งเดิมกับแพลตฟอร์มการจำแนกอินเทอร์เฟซ การอนุญาตและการบริการควบคุมการเข้าถึงข้อมูลโดยตรง นอกจากนี้ทำให้ตระถึงระบบต้นแบบที่ดีที่สุดในงานวิจัยนี้ การรับรองความถูกต้องนี้สามารถแปลงการตอบสนองความท้าทายการตรวจสอบ Token เพื่อตรวจสอบความถูกต้องของรหัสผ่านซึ่งจะช่วยแก้ปัญหาและรักษาความปลอดภัยของรหัสผ่านอีกทั้งยังช่วยรักษาข้อมูลให้มีความปลอดภัยอีกด้วย ซึ่งแบบจำลองการสื่อสารระหว่างโทรศัพท์มือถือนี้ ได้ดำเนินการพัฒนาพัฒนากับโทรศัพท์มือถือซึ่งถือว่าเป็นต้นแบบที่ดีที่สุดเลยทีเดียว



รูปที่ 27 แสดงโครงสร้างการรับรองของเครือข่ายโทรศัพท์มือถือ

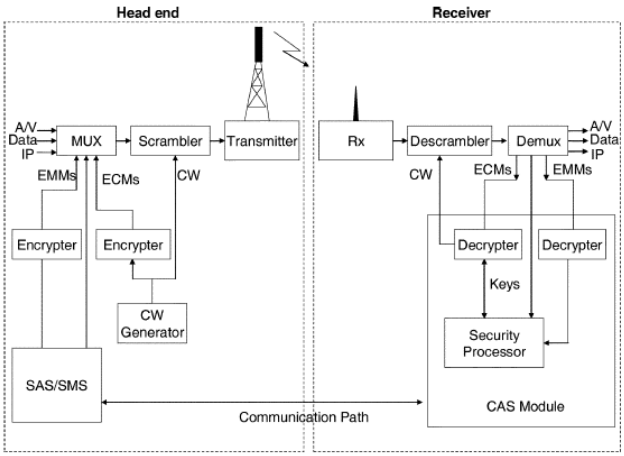


รูปที่ 28 แสดงถึงระบบการรับรองความถูกต้องของรหัสผ่านโทเค็นของโทรศัพท์มือถือ

F. An Efficient Authentication Scheme for Access Control in Mobile Pay-TV Systems [27]

งานวิจัยนี้ ได้นำเสนอการตรวจสอบโครงการที่มีประสิทธิภาพและการควบคุมการเข้าถึงในระบบ Pay-TV มือถือ นอกจากยังเพิ่มประสิทธิภาพดีกว่าที่มีอยู่ยังให้กลไกเพิ่มเติมสำหรับการตรวจสอบโทรศัพท์มือถือในขณะที่ปิดอยู่ Pay-TV ยังสามารถรับรองความถูกต้องเพิ่มขึ้น ในขณะที่ปกป้องการเข้าถึงการโจมตีในกรณีโทรศัพท์มือถือปิดอยู่ โดย ECC และการจับคู่ ยังเป็นการตรวจสอบซึ่งกันและกัน นอกจากนี้ยังมีข้อได้เปรียบในการใช้งานซึ่งจะมีประสิทธิภาพด้วยสิ่งอำนวยความสะดวกโดยการจัดการตรวจสอบพารามิเตอร์และการทำงานการจับคู่ที่ระบบต้นแบบชุดมือถือยังสามารถดำเนินการตรวจสอบเป็นรายบุคคลจากการคำนวณ token

นอกจากนี้ โครงร่างยังเสนอข้อดีของ ECC กับขนาดของคีย์ที่มีขนาดเล็กและความปลอดภัยสูง นอกจากนี้เค้าโครงรหัสประจำตัวตามแผนก็เป็นข้อดีที่ไม่จำเป็นต้องมีการอ้างอิงและค่าใช้จ่ายจะลดลง จากการวิเคราะห์การรักษาความปลอดภัยของงานวิจัยนี้ยังให้ผลการวิเคราะห์ประสิทธิภาพการโครงการที่เสนอเป็นโครงการตรวจสอบความปลอดภัยและมีประสิทธิภาพสำหรับโทรศัพท์มือถือระบบ Pay-TV โดยการจับคู่และโครงการ ECC สามารถป้องกันการโจมตีการปลอมแปลงและการโจมตีท่ามกลางผู้ใช้ ซึ่งในอนาคตคาดว่าระบบนี้จะมีประสิทธิภาพมากยิ่งขึ้น



รูปที่ 29 แสดงแบบจำลองทั่วไปของ CAS

G. Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks [28]

งานวิจัยนี้เน้นการพิสูจน์ตัวตน ซึ่งการตรวจสอบจะมีระยะไกลนอกจากนี้เพื่อความถูกต้องและความลับที่ไม่ซ้ำกัน คุณสมบัติของบริการออนไลน์ที่มีมูลค่าเพิ่มก่อให้เกิดความท้าทายความปลอดภัยมากขึ้นสำหรับการตรวจสอบระยะไกล ในสภาพแวดล้อมเครือข่ายมือถือที่มองไม่เห็นอุปกรณ์อาจจะรวบรวมและจัดเก็บภาษีข้อมูลประจำตัวของลูกค้าที่เข้าร่วมโครงการไม่เปิดเผยชื่อลูกค้ามักจะต้องเพื่อให้แน่ใจว่าตัวตนของไคลเอนต์ร้องขอ

ตารางที่ 8 แสดงการเปรียบเทียบลักษณะของงานวิจัยที่มีการพิสูจน์ตัวตนในการเข้าถึงข้อมูล

งานวิจัย / ลักษณะของงานวิจัย	[22]	[23]	[24]	[25]	[26]	[27]	[28]
Possession factor				✓	✓	✓	
Knowledge factor				✓	✓		✓
Biometric factor	✓	✓	✓				

ตารางที่ 9 ตารางแสดงเปรียบเทียบแบบ Possession factor

งานวิจัย/ลักษณะของงานวิจัย	[25]	[26]	[27]
Efficiency	ปานกลาง	ต่ำ	สูง
Access to information	ต่ำ	ปานกลาง	สูง
Fast to Authentication	สูง	ปานกลาง	ปานกลาง
The possibility of an attack	ปานกลาง	ต่ำ	สูง
Confidentiality	ปานกลาง	ต่ำ	สูง

ตารางที่ 10 ตารางแสดงการเปรียบเทียบงานวิจัยในการพิสูจน์ตัวตน ด้าน Possession factor

	ข้อดี	ข้อจำกัด
[25]	มีประสิทธิภาพในการตรวจสอบตัวตนเนื่องจากมีการเข้ารหัสใหม่และสร้างแบบจำลองในการตรวจสอบคีย์การ์ด	แบบจำลองจากการวิเคราะห์อาจไม่มีประสิทธิภาพทำให้การตรวจสอบไม่มีประสิทธิภาพตามไปด้วย
[26]	พัฒนา Token ใหม่เพื่อตรวจสอบการพิสูจน์ตัวตน	Token ที่ได้อาจมีประสิทธิภาพน้อย ทำให้การถูกโจมตีนั้นมีมาก
[27]	พัฒนา Token และใช้วิธี ECC (เทคนิคการจับคู่) มาใช้ร่วมกัน	หากใช้วิธี ECC แล้วทำให้ค่ามีความคลาดเคลื่อนอาจทำให้การพัฒนา Token ขาดประสิทธิภาพตามไปด้วย

ตารางที่ 11 ตารางแสดงเปรียบเทียบแบบ Knowledge factor

งานวิจัย/ลักษณะของงานวิจัย	[25]	[26]	[28]
Efficiency	ปานกลาง	สูง	สูง
Access to information	ต่ำ	ปานกลาง	ปานกลาง
Fast to Authentication	สูง	ปานกลาง	ปานกลาง
The possibility of an attack	ปานกลาง	ต่ำ	ปานกลาง
Confidentiality	ปานกลาง	สูง	ปานกลาง

ตารางที่ 12 ตารางแสดงการเปรียบเทียบงานวิจัยในการพิสูจน์ตัวตน ด้าน Knowledge factor

	ข้อดี	ข้อจำกัด
[25]	การสร้างแบบจำลองใหม่ขึ้น โดยเพิ่มอัลกอริทึม ปรับ Dynamic และปรับขนาด Catch ซึ่งทำให้ลดค่าใช้จ่ายและทำให้การพิสูจน์ตัวตนมีประสิทธิภาพ	หาก อัลกอริทึมที่ได้มานั้น ไม่สัมพันธ์กับการปรับ Dynamic จะทำให้การพิสูจน์ตัวตนล้มเหลว
[26]	พัฒนา Token ใหม่เพื่อตรวจสอบการพิสูจน์ตัวตน การตรวจสอบ token เพื่อตรวจสอบรหัสผ่าน ซึ่งจะช่วยแก้ปัญหาการรักษาความปลอดภัยของรหัสผ่าน	Token ที่ได้อาจมีประสิทธิภาพน้อย ทำให้การถูกโจมตีนั้นมีมาก
[28]	วิธี ID-Based เป็นวิธีพื้นฐานในการพิสูจน์ตัวตนและช่วยลดระยะเวลาในการดำเนินการ	วิธี ID-Based อาจถูกคุกคามจากสิ่งไม่พึงประสงค์ได้ง่าย

ตารางที่ 13 ตารางแสดงเปรียบเทียบแบบ Biometric factor

งานวิจัย/ลักษณะของงานวิจัย	[22]	[23]	[24]
Efficiency	ปานกลาง	สูง	ต่ำ
Access to information	ต่ำ	ปานกลาง	สูง
Fast to Authentication	สูง	ปานกลาง	ปานกลาง
The possibility of an attack	ปานกลาง	ต่ำ	สูง
Confidentiality	ปานกลาง	สูง	ต่ำ

ตารางที่ 14 ตารางแสดงการเปรียบเทียบงานวิจัยในการพิสูจน์ตัวตน ด้าน Biometric factor

	ข้อดี	ข้อจำกัด
[22]	เสนอโปรโตเมตริกซ์ใหม่ โดยวิธีการตรวจสอบการใช้ฟันและภาพเสียงในการพิสูจน์ตัวตน	หากฟันและเสียง มีการคลาดเคลื่อนก็ไม่ทำให้การพิสูจน์ตัวตนมีประสิทธิภาพได้
[23]	เป็นการพิสูจน์ตัวตนจากฟัน ใบหน้าและรังสีเสียงเพื่อปรับปรุงประสิทธิภาพและเพื่อบูรณาการฟิวชั่นต่างๆ เทคนิคต่าง ๆ เช่นกฎการบวกน้ำหนัก K-NN	หากใบหน้า รูปฟัน เสียง มีการเปลี่ยนแปลงก็ไม่สามารถดำเนินการให้สมบูรณ์ได้ อาจถูกโจมตีได้ง่าย
[24]	ใช้โปรโตเมตริกซ์การรักษาความปลอดภัยที่แข็งแกร่งและต้นทุนต่ำ ประกอบด้วย 5 ลักษณะดังนี้ 1) การตรวจหาใบหน้า 2) ลงทะเบียนหน้า 3) แสงการฟื้นฟู 4) ฟิวชั่นข้อมูลและ 5) การตรวจสอบใบหน้า ทำให้ลดต้นทุนและเกิดประสิทธิภาพมากยิ่งขึ้น	นำหลายลักษณะมาประมวลผล อาจทำช้า เปลืองเวลา

VI. Access Control

จากที่ได้ศึกษางานวิจัยที่เกี่ยวข้องกับการควบคุมการเข้าถึงข้อมูลบนคลาวด์ที่ผ่านมา ส่วนใหญ่จะกล่าวถึงโมเดลในการควบคุมการเข้าถึงข้อมูลเพื่อรักษาความปลอดภัยให้แก่ข้อมูลต่างๆ บนคลาวด์ จึงได้มีการนำโมเดลในลักษณะต่างๆ นี้มาศึกษาเพื่อทำการเปรียบเทียบการทำงานหรือหน้าที่การทำงานในลักษณะต่างๆ

Access Control คือ ระบบควบคุมการเข้าถึงหรือควบคุมการผ่านเข้าออก ซึ่งมีหน้าที่ทำการควบคุมการผ่านเข้าออกของประตูต่างๆ และกำหนดสิทธิให้กับแต่ละบุคคล ว่าสามารถเข้าออกประตูใดได้บ้าง ภายในช่วงเวลาใดบ้าง การทำ Access Control เป็นกระบวนการที่ใช้ในการป้องกันการใช้งานทรัพยากรโดยผู้ที่ไม่ได้รับอนุญาต ซึ่งกระบวนการ Access Control นั้นมีการใช้งานในหลากหลายรูปแบบซึ่งตัวอย่างในชีวิตประจำวันเราจะเห็นได้ทั่วไป เช่น การใช้กุญแจไขปิดล็อคประตู ซึ่งมีเพียงเจ้าของกุญแจเท่านั้นจึงจะสามารถเปิดประตูได้ การตรวจบัตรเข้าชมภาพยนตร์ซึ่งอนุญาตเฉพาะผู้ที่มีบัตรเท่านั้นจึงจะเข้าชมภาพยนตร์ได้ การใช้บัตรผ่านประตูและรหัสเปิดประตูเพื่อเข้าไปยังห้องที่เก็บข้อมูลสำคัญในธนาคาร หรือหน่วยงานต่างๆ และการใช้ Username และ Password ในการเข้าอ่าน E-mail ต่างๆ ของผู้ใช้งานแต่ละคนเป็นต้น

โดยหลักการทำงานของ Access Control มีกระบวนการในการดำเนินการดังนี้

1. กำหนดผู้ใช้งานระบบว่ามีใครบ้าง
2. กำหนดค่าทรัพยากรที่ต้องการควบคุมการใช้งานว่ามีอะไรบ้าง
3. กำหนดกระบวนการใช้งานของผู้ใช้งานระบบว่ามีอะไรบ้าง
4. กำหนดการใช้งานของผู้ใช้งานแต่ละคนว่าผู้ใช้งานแต่ละคนสามารถทำงานอะไรได้บ้างและใช้งานทรัพยากรใดได้บ้าง

ความหมายของ Identification, Authentication, Authorization

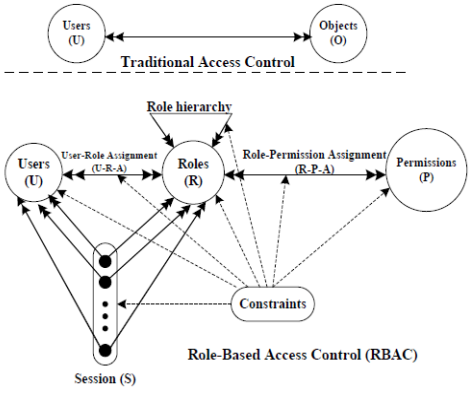
Identification หมายถึง การระบุตัวตนของสิ่งต่างๆ ในระบบ จะเป็นกระบวนการที่ผู้ใช้งานระบบจะแจ้งหลักฐาน (Identity) การมีตัวตนของตัวเอง สำหรับ Identification สำหรับผู้ใช้งานระบบสามารถใช้เช่นชื่อผู้ใช้ เป็นต้น ซึ่งโดยหลักการของ Identification จะต้องการสิ่งของ หรือข้อมูลใดๆ ก็ตามที่ผู้ใช้งานคนนั้นๆ “เป็นเจ้าของ” สำหรับคุณสมบัติของ Identity ที่ดีควรปลอมแปลงยาก และเป็นของบุคคลนั้นๆ เท่านั้น

Authentication หมายถึง กระบวนการในการพิสูจน์ตัวตนว่าบุคคลที่ใช้งานระบบอยู่นั้นใช่บุคคลคนนั้นๆ จริงหรือไม่ เนื่องจากการใช้งานระบบต่างๆ จะเป็นแบบการใช้งานระยะไกล ไม่สามารถพิสูจน์ตัวตนได้ เนื่องจากไม่เห็นหน้า ไม่ทราบลักษณะ แต่จะเห็นเพียงข้อมูลที่วิ่งผ่านไปมาเท่านั้น ซึ่งหมายถึงการใช้งานระบบต่างๆ เป็นแบบ Logical ทั้งสิ้น กระบวนการ Authentication จึงเป็นกระบวนการที่ตรวจสอบว่า Logical ที่แทนบุคคล หรือระบบต่างๆ นั้นเป็นตัวแทนของบุคคลหรือระบบนั้นๆจริง กระบวนการในการทำ Authentication ได้แก่ การพิสูจน์หลักฐานที่บุคคลนั้นๆ นำมาเสนอเพื่อบ่งบอกว่าคนๆ นั้นเป็นคนๆ นั้นจริงๆ เช่น Username และ Password

Authorization หมายถึง การพิสูจน์สิทธิว่าบุคคลที่ผ่านกระบวนการ Authentication นั้นมีสิทธิในการใช้งานระบบหรือทรัพยากรใดได้บ้าง จะเป็นกระบวนการที่เกี่ยวข้องกับการการตั้งค่าของสิทธิต่างๆ ของผู้ใช้งานในระบบ เพื่อให้การดำเนินการต่างๆ ถูกต้องตาม Role ของระบบที่ได้กำหนดไว้ล่วงหน้า ทั้ง Identification Authentication และ Authorization มีส่วนเกี่ยวข้องในการควบคุมการเข้าถึงทรัพยากรโดยในการเข้าใช้งานระบบผู้ใช้งานจะแสดง Identity ของตนเองเพื่อ Authentication และระบบจะทำการ Authorization เมื่อมีการใช้งานทรัพยากรใดๆ ในระบบ โดยโมเดลในการควบคุมการเข้าถึงข้อมูลส่วนมากที่ปรากฏ มีดังนี้

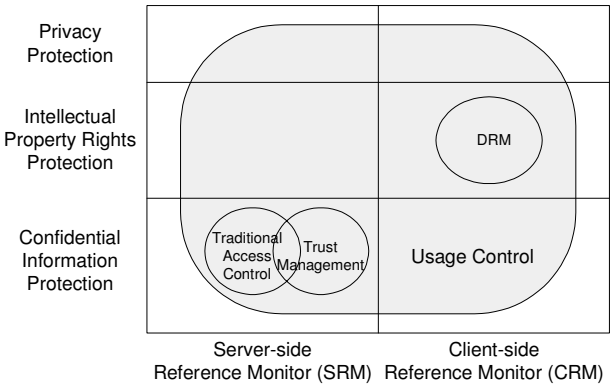
(1) Role-Based Access Control – RBAC

การควบคุมบทบาทการเข้าใช้งาน เรียกกว่า กฎควบคุมการเข้าถึงสิทธิ์ (Role Based Access Controls: RBAC) ซึ่งกำหนดตามหน้าที่ ความรับผิดชอบและความสามารถ เช่น บทบาทที่เกี่ยวข้องกับโรงพยาบาลที่ประกอบด้วยหมอพยาบาล ผู้เชี่ยวชาญ และเภสัชกร ซึ่งมีการควบคุมการเข้าถึงข้อมูลอย่างเคร่งครัดในการการอนุญาตการเป็นสมาชิกการระบุกระบวนการยกเลิกการอนุญาตสมาชิกและในการเข้าใช้งานข้อมูลอย่างถูกต้องของแต่ละวัตถุประกอบด้วย 6 องค์ประกอบ คือ ผู้ใช้ บทบาทหน้าที่ การตรวจสอบสิทธิ์ การดำเนินการ วัตถุ และระยะเวลา



รูปที่ 30 แบบจำลองการควบคุมการเข้าถึง

(2) Usage Control – UCON เป็นการควบคุมการใช้งาน



รูปที่ 31 UCON Coverage

- Traditional Access Control การควบคุมการเข้าถึงแบบดั้งเดิม

เพื่อป้องกันทรัพยากรของคอมพิวเตอร์โดยการจำกัดพฤติกรรมของผู้ใช้หรือการดำเนินงานภายในระบบปิด

- Trust Management การจัดการความไว้วางใจ

เสนอด้วยกระบวนการการกำหนดสิทธิ์ในสภาพแวดล้อมระบบแบบกระจายสำหรับการเข้าถึงข้อมูล

- Digital Rights Management การจัดการสิทธิดิจิทัล

เป็นเทคโนโลยีที่ใช้โดยเจ้าของสิทธิ์ เพื่อควบคุมการเข้าถึงและการใช้งานข้อมูลดิจิทัล

(3) Discretionary Access Control – DAC

เป็นการควบคุมการเข้าถึงระบบให้กับผู้กระทำนั้นเป็นไปอย่างยืดหยุ่น โดยการทำงานของแบบจำลองนี้จะไม่ยึดติดกับระบบปฏิบัติการ พัฒนาจากแนวคิดที่ถูกขยายของ System Management ที่มีอยู่ในปัจจุบัน มีการวางนโยบายการเข้าถึงที่หลากหลาย เช่นป้องกันการใช้งานคำสั่งต่างๆบนระบบเป็นต้น

ปัญหา : ยากต่อการดูแลและจัดการเมื่อมีจำนวนเซิร์ฟเวอร์ที่ต้องดูแลมากขึ้น รวมไปถึงหากมีการวางนโยบายหรือ Policy ผิดพลาด จะมีผลกระทบกับระบบอื่นๆ โดยตรง

(4) Mandatory Access Control – MAC

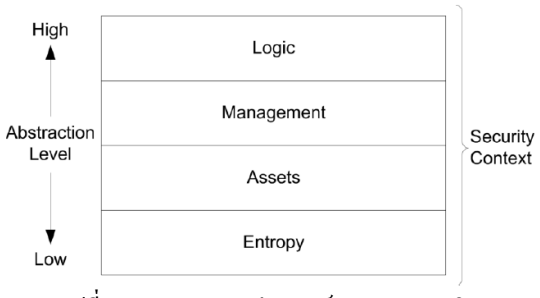
เป็นการทำงานแบบการควบคุมของส่วนกลางหรือ Centrally Control หมายถึง user ไม่มีสิทธิในการตั้งค่า Access Control โดยองค์กรจะเป็นผู้กำหนด Security Policy สำหรับการเข้าถึงของข้อมูลเท่านั้นเพื่อลดความเสียหายและการรั่วไหลของข้อมูลในเบื้องต้น ง่ายต่อการวางระบบและดูแลรักษานโยบาย (Security Policy) ในองค์กรที่มีเซิร์ฟเวอร์อยู่จำนวนมากสะดวกต่อการเปลี่ยนแปลงนโยบายจากจุดเดียว มีระดับความปลอดภัยในเกณฑ์ที่สูงและทำงานในระดับของ Kernel จึงไม่สามารถบุกรุกแอพพลิเคชั่นได้

ปัญหา : ยากต่อการดูแลหากต้องการวางนโยบาย Policy ในระบบปฏิบัติการที่หลายหลายแพลตฟอร์ม

จากการศึกษาเกี่ยวกับกระบวนการในควบคุมการเข้าถึงข้อมูล ส่วนใหญ่มีจุดประสงค์เพื่อรักษาความปลอดภัยก่อนมีการเข้าถึงข้อมูลนั้นๆ ทั้งในรูปแบบที่เป็นโมเดลในการควบคุมการเข้าถึงข้อมูลและโครงสร้างในการควบคุมการเข้าถึงข้อมูล ซึ่งจากการศึกษาโมเดลในการควบคุมการเข้าถึงข้อมูลจากงานวิจัยที่เกี่ยวข้อง มีดังนี้

A. Towards new access control models for Cloud computing systems [29]

ในงานวิจัยนี้ได้มีการนำเสนอวิธีการในการเข้าถึงข้อมูลขั้นพื้นฐาน เพื่อตรวจสอบและควบคุมการเข้าถึงข้อมูลแบบคลาวด์ ซึ่งได้นำเสนอรูปแบบและเปรียบเทียบการควบคุมการเข้าถึงข้อมูลในสองลักษณะ ได้แก่ Role Based Access Control (RBAC) และ Usage Control - $UCON_{ABC}$ โดย RBAC เป็นระบบการจัดการสิทธิโดยดูตามภารกิจการใช้งาน มีการจัดการที่ง่ายสามารถเพิ่ม layer ของลำดับสิทธิได้ และ $UCON_{ABC}$ จะเป็นในส่วนของการควบคุมการใช้ และได้มีการแบ่งระดับตามลักษณะของเลเยอร์ต่างๆ ในการควบคุมการเข้าถึง ดังนี้



รูปที่ 32 แสดงการจัดแบ่งเลเยอร์ตามแนวความคิด

1. Entropy layer เป็นการประยุกต์ใช้แก่ผู้บริโภคผ่านรูปแบบการบริการแบบ SaaS

2. Assets layer เป็นการกล่าวถึง assets ในระบบคลาวด์ซึ่งมีสองประเภท ได้แก่ ซอฟแวร์และฮาร์ดแวร์

3. Management layer เป็นนโยบายในการจัดการในระบบคลาวด์โดยส่วนใหญ่จะมีการจัดการแบบ centralized

4. Logic layer เป็นการสนับสนุนเกี่ยวคุณภาพของนโยบายการบริการ (QoS) พร้อมกับข้อตกลงของระดับการให้บริการ (SLAs)

ซึ่งการเปรียบเทียบระหว่าง RBAC และ $UCON_{ABC}$ โดยการเปรียบเทียบระหว่างสองสิ่งนี้ได้ทำการจัดแบ่งประเภทของแนวความคิดในระบบคลาวด์กับมุมมองการระบุจำนวนข้อบกพร่องในการควบคุมการเข้าถึงของโมเดลดังกล่าว ซึ่งแสดงได้ดังรูปภาพต่อไปนี้

Access control models	Conceptual categorization layers			
	Entropy	Assets	Management	Logic
RBAC	Low / Medium	Low / Medium	Medium / High	Medium
$UCON_{ABC}$	High	Medium	Low	Medium

รูปที่ 33 แสดงการเปรียบเทียบการควบคุมการเข้าถึงของโมเดลแบบต่างๆ

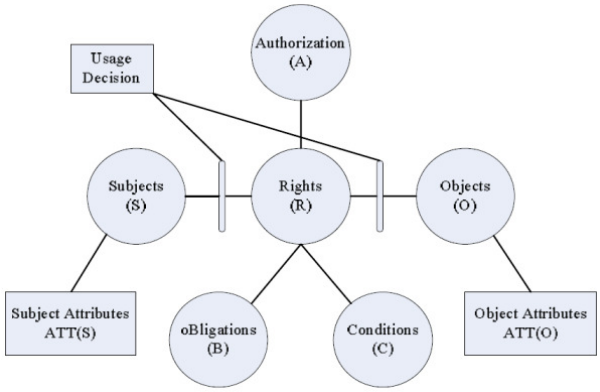
B. Access Control of Cloud Service Based on UCON [30]

งานวิจัยนี้ได้แนะนำเบื้องต้นเกี่ยวกับ Cloud Computing, Cloud Service และการใช้ UC4krON ในการควบคุมการเข้าถึงข้อมูล เทคนิค negotiation และการออกแบบโมดูล negotiation

Cloud Services Access Control Based UCON

(1) UCON Model

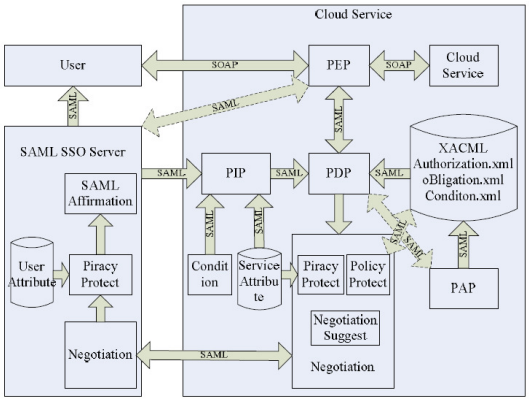
รูปแบบในการควบคุมการเข้าถึงข้อมูลแบบเดิมประกอบไปด้วย DAC, MAC และ RBAC ส่วนรูปแบบที่เกิดขึ้นใหม่ประกอบไปด้วย TBAC, ABAC และ UCON ซึ่งจะเน้นที่รูปแบบของ UCON โดยจะประกอบไปด้วย 6 ส่วนต่างๆ ได้แก่ Subjects, Rights, Objects, Authorization, Obligation และ Conditions ดังภาพ



รูปที่ 34 แสดงรูปแบบของ UCON

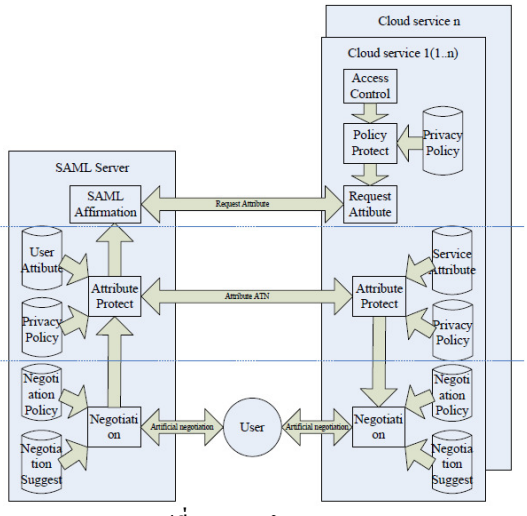
(2) Cloud Services Access Control Based UCON

2.1 Nego-UCON$_{ABC}$ Model



รูปที่ 35 แสดงรูปแบบของ Nego-UCON$_{ABC}$

2.2 Nego Module



รูปที่ 36 แสดงโมดูล Nego

C. Methods for Access Control: Advances and Limitations [31]

เป็นการนำเสนอโมเดลแบบต่างๆ เกี่ยวกับระบบการควบคุมการเข้าถึง โดยประกอบไปด้วย Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC) และ Domain Type Enforcement (DTE)

จากที่ได้ศึกษางานวิจัยทั้งหมดที่เกี่ยวข้องกับเนื้อหาการควบคุมการเข้าถึงข้อมูลบนคลาวด์งานวิจัยที่กล่าวถึงโมเดลในลักษณะต่างในการควบคุมการเข้าถึงข้อมูล ซึ่งสามารถแสดงได้ดังตารางต่อไปนี้

ตารางที่ 15 แสดงการเปรียบเทียบโมเดลในการควบคุมการเข้าถึงข้อมูล

งานวิจัย / ลักษณะโมเดล	[29]	[30]	[31]
RBAC	✓		✓
UCON$_{ABC}$	✓		
UCON		✓	
MAC			✓
DAC			✓

สรุปผลการเปรียบเทียบโมเดลในการเข้าถึงข้อมูลงานวิจัยที่เกี่ยวข้อง

งานวิจัย [29] สำหรับชั้นระดับปฏิบัติการได้มีการกำหนดลักษณะความต้องการที่สนับสนุนการควบคุมการเข้าถึงข้อมูลจากทั้งแบบส่วนกลางและแบบกระจายของโดเมนที่ต่างกัน โดยการนำเสนอรูปแบบ RBAC แสดงให้เห็นว่าการจัดการด้านสถาปัตยกรรมส่วนกลางมีการจัดการที่ดีขึ้นแต่ค่อนข้างอ่อนแอในความร่วมมือระหว่างโดเมน เช่น ฟังก์ชันการทำงานที่หายไปจากรุ่นมาตรฐาน อย่างไรก็ตามการค้นคว้า (Shafiq et al., 2005) ได้พิสูจน์แล้วว่า RBAC สามารถนำมาประยุกต์ใช้ในสภาพแวดล้อมแบบหลายโดเมน ในทางตรงกันข้ามรูปแบบ UCON$_{ABC}$ จากการสนับสนุนคุณลักษณะที่สามารถรับมือกับสภาพแวดล้อมแบบกระจายสูง นอกจากนี้หนึ่งในคุณสมบัติของ UCON คือความเป็นไปได้ที่จะเข้าถึงผู้ใช้ในสภาพแวดล้อมร่วมกันโดยไม่จำเป็นต้องรู้จักแหล่งที่มามาก่อน

งานวิจัย [30] รูปแบบ UCON ให้ความสามารถในการตัดสินใจที่ดีกว่ามากหากเปรียบกับรูปแบบ UCON$_{ABC}$ และเป็นทางเลือกที่ดีที่จะใช้ในการสร้างการบริการในการเข้าถึงคลาวด์ โดยรูปแบบการควบคุมแบบ UCON เป็นเพียงรูปแบบความคิดและข้อกำหนดไม่ก่อให้เกิดเป็นรูปธรรม ดังนั้น ยังคงต้องมีการพัฒนางานอีกมากสำหรับการสร้างรูปแบบการควบคุมการเข้าถึงตามรูปแบบของ UCON

งานวิจัย [31] ข้อเสนอแรกที่เสนอโดย Ferraiolo และ Kuhn ในปี 1992 กล่าวว่ารูปแบบ RBAC ส่วนใหญ่ได้จัดการกับปัญหาความล้มเหลวของ DAC ในขณะที่ DACs เน้นไปที่ระบบที่ไม่ใช่ทหาร ซึ่ง RBAC ได้เสนอแนวทางในเชิงพาณิชย์และความปลอดภัยของรัฐบาลพลเรือนว่าต้องการความสมบูรณ์ก่อนเพื่อการรักษาความลับ ข้อเสนอถัดมาในงานวิจัยของ Clark และ Wilsons ได้แสดงนโยบายการรักษาความปลอดภัยในเชิงพาณิชย์โดยนโยบายนั้นจะอยู่ในรูปแบบ RBAC โดยจะมีการให้สิทธิในการมีบทบาทสำคัญมากกว่าประชาชนและการบังคับใช้นโยบายรวมอยู่ในมือของการรักษาความปลอดภัยผู้ดูแลระบบและผู้ใช้จะถูกปกป้องจากการโอนสิทธิที่กำหนดจากบทบาทที่

ได้รับอนุญาตให้ดำเนินการกับผู้ใช้อื่นๆ ซึ่งกฎนี้จะเอากรรมสิทธิ์เพื่อรับสิทธิใน DAC และมักทำตัวเป็นส่วนย่อยรุ่นของรูปแบบ MAC ดังนั้น RBAC จึงต่างจากแบบ MAC และ DAC และรับสิทธิโดยการทำธุรกรรมที่เกี่ยวกับวิชาพื้นฐานได้อย่างรวดเร็วต่างจากกลุ่ม DAC ที่ประกอบไปด้วยตัวเลือกของผู้ใช้และตัวเลือกของรูปแบบของ Clark-Wilson ในสิทธิของการทำธุรกรรม

VII. สรุป

เทคโนโลยีด้านการประมวลผลแบบคลาวด์คอมพิวติ้งที่เป็นเทคโนโลยีที่ได้รับความนิยม ผ่านอุปกรณ์ที่ใช้ในการเข้าถึงข้อมูล เข้าถึงบริการ ร่วมไปถึงบนอุปกรณ์โทรศัพท์ สมาร์ทโฟนผ่านแอพพลิเคชั่นที่ใช้บริการการประมวลผลแบบคลาวด์ การเข้าถึงบริการเข้าใช้บริการนี้จำเป็นต้องมีการรักษาความปลอดภัยของการเข้าใช้บริการ การเข้าถึงข้อมูลสารสนเทศต่างๆ ของผู้ใช้หรือการกำหนดสิทธิ์ให้สิทธิ์ผู้ใช้ที่แตกต่างกัน โดยทีมผู้วิจัยได้ทำการศึกษาเปรียบเทียบความสามารถในด้านความปลอดภัยในการประมวลผลแบบคลาวด์ผ่านอุปกรณ์โทรศัพท์มือถือหรือสมาร์ทโฟน โดยได้ทำการแบ่งเรื่องที่ศึกษาออกเป็น 5 ส่วน

ส่วนแรก เป็นเกี่ยวข้องกับการบริการการรักษาความปลอดภัย วิเคราะห์จากการนำเสนอแนวคิดวิจัยของแต่ละงานวิจัยที่ศึกษา โดยวิเคราะห์ในส่วนการบริการรักษาความปลอดภัยในด้านต่างๆที่เกี่ยวข้องกับผู้ใช้ โดยทุกงานวิจัยขาดการบริการปกปิดชื่อของผู้ใช้

ส่วนที่ 2 กรอบการสร้างการรักษาความปลอดภัยเครือข่ายของอุปกรณ์เคลื่อนที่บนคลาวด์ ใช้การเปรียบเทียบคุณสมบัติ โดยการจัดการสิทธิในการเข้าถึงและนโยบายความปลอดภัย การเข้ารหัสข้อมูล และโปรแกรมเชื่อมต่อระหว่างสองแอพพลิเคชั่น เป็นหัวข้อที่งานวิจัยที่ทำการสำรวจให้ความสำคัญ

ส่วนที่ 3 การบริการจัดเก็บแบบคลาวด์ มีการอ้างถึง การเปรียบเทียบสถาปัตยกรรมการจัดเก็บแบบคลาวด์ และการเปรียบเทียบแบบจำลองการอ้างถึงแบบคลาวด์ โดยภาพรวมของงานวิจัยพูดถึง การตรวจสอบตัวตนผู้ใช้ การกำหนดสิทธิ ความเป็นส่วนตัว การรักษาความปลอดภัยในการเชื่อมต่อ การเข้ารหัส และการลงลายเซ็น

ส่วนที่ 4 การอ้างถึงตัวตน เปรียบเทียบการพิสูจน์ตัวตนด้วยวิธีต่างๆ โดยทุกงานวิจัยให้ความสำคัญกับ Efficiency, Access to information และ Confidentiality

ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูล มีการใช้การเปรียบเทียบจากโมเดลในการเข้าถึงข้อมูล ลักษณะโมเดลที่ได้รับความนิยมในการศึกษา คือ RBAC จากการสำรวจและการวิเคราะห์ศึกษางานวิจัยด้านความปลอดภัยการประมวลผลแบบคลาวด์บนอุปกรณ์โทรศัพท์หรือสมาร์ทโฟน มีความสำคัญเป็นอย่างยิ่งต่อการพัฒนาระบบของคลาวด์คอมพิวติ้ง โดยจะต้องมีความปลอดภัย มีประสิทธิภาพและน่าเชื่อถือได้

VIII. ข้อเสนอแนะงานวิจัยในอนาคต

สำหรับการศึกษาและวิจัยในอนาคตจากการนำผลสำรวจไปวิเคราะห์ผลและอภิปรายผลร่วมกันแล้ว สามารถนำผลที่อธิปรายไปต่อยอดในงานวิจัยด้านเครือข่ายการประมวลผลแบบคลาวด์ได้ ได้ทราบถึงแนวทางที่เป็นปัจจุบันแนวทางที่ได้รับความนิยม เพื่อการนำผลไปใช้ในการวิจัยต่อไป

ข้อเสนอแนะในการสำรวจนำเสนอในงานวิจัยในอนาคต ควรจะมีการวิเคราะห์ภาพรวมที่หลากหลาย รวมไปถึงทางด้านประสิทธิภาพของการใช้คลาวด์บนสมาร์ทโฟน เพื่อนำไปใช้ประโยชน์ในงานวิจัยในอนาคต

IX. กิตติกรรมประกาศ

งานวิจัยเชิงสำรวจเรื่องการรักษาความปลอดภัยการประมวลผลแบบคลาวด์บนโมบาย นี้เป็นส่วนหนึ่งของการทำวิจัยวิชา เครือข่ายคอมพิวเตอร์ ต้องขอขอบพระคุณอาจารย์ผู้สอนและผู้ช่วยสอนที่มีส่วนให้เกิดงานวิจัยเชิงสำรวจนี้ขึ้นมาได้ และขอขอบคุณเพื่อนๆ สมาชิกที่ร่วมมือ ร่วมใจกันจนได้งานเรื่องเกิดขึ้น

เอกสารอ้างอิง

[1] D. G. Rosado, E. Fernández-Medina, and J. López, "Security services architecture for Secure Mobile Grid Systems," *Journal of Systems Architecture,* vol. 57, pp. 240-258, 2011.

[2] น. ท. นิวัติ เนียมพลอย. (2010). *การรักษาความปลอดภัยของข้อมูลข่าวสาร* Available: http://nniwat.wordpress.com/2010/10/27/การรักษาความปลอดภัยของ/

[3] I. Bilogrevic, M. Jadliwala, P. Kumar, S. S. Walia, J.-P. Hubaux, I. Aad, and V. Niemi, "Meetings through the cloud: Privacy-preserving scheduling on mobile devices," *Journal of Systems and Software,* vol. 84, pp. 1910-1927, 2011.

[4] Z. Lian-chi and X. Chun-di, "Cloud Security Service Providing Schemes Based on Mobile Internet Framework," 2012, pp. 307-311.

[5] Y. Zhu, H. Hu, G.-J. Ahn, and S. S. Yau, "Efficient audit service outsourcing for data integrity in clouds," *Journal of Systems and Software,* vol. 85, pp. 1083-1095, 2012.

[6] M. Nkosi and F. Mekuria, "Improving the capacity, reliability amp; life of mobile devices with Cloud Computing," 2011, pp. 1-9.

[7] S. Horrow, S. Gupta, A. Sardana, and A. Abraham, "Secure Private Cloud Architecture for Mobile Infrastructure as a Service," 2012, pp. 149-154.

[8] W. Ren, L. Yu, R. Gao, and F. Xiong, "Lightweight and Compromise Resilient Storage Outsourcing with Distributed Secure Accessibility in Mobile Cloud Computing," *Tsinghua Science & Technology,* vol. 16, pp. 520-528, 2011.

[9] Xuesen Lin. "Survey on cloud based mobile security and a new framework for improvement." *IEEE International Conference on* Information and Automation (ICIA), pp. 710 – 715, 2011.

[10] Dijiang Huang, Zhibin Zhou, Le Xu, Tianyi Xing and Yunji Zhong. "Secure Data Processing Framework for Mobile Cloud Computing." *IEEE Conference on* Computer Communications Workshops (INFOCOM WKSHPS), pp. 614 – 618, 2011.

[11] Dijiang Huang, Xinwen Zhan, Myong Kang and Jim Luo. "MobiCloud: Building Secure Cloud Framework for Mobile Computing And Communication." *Fifth IEEE International Symposium on* Service Oriented System Engineering (SOSE), pp. 27 - 34, 2011.

[12] Yu-Jia Chen, Li-Chun Wang. "A Security Framework of Group Location- Based Mobile Applications in Cloud Computing." 40th International Conference on Parallel Processing Workshops (ICPPW), pp. 184 - 190, 2011.

[13] Jianxin Li, Bo Li, Zongxia Du and Linlin Meng. "CloudVO: Building a Secure Virtual Organization for Multiple Clouds Collaboration." *11th ACIS International Conference on* Software Engineering Artificial Intelligence Networking and Parallel/Distributed Computing (SNPD), pp. 181 - 186, 2010.

[14] Sang-Ho Na, Jun-Young Park and Eui-Nam Huh. "Personal Cloud Computing Security 104ty Framework." IEEE *Asia-Pacific* Services Computing Conference (APSCC), pp. 671 - 675, 2010.

[15] OASIS, "eXtensible Access Control Markup Language(XACML)"

[16] OASIS, "Key Management Interoperability Protocol (KMIP)"

[17] J. Wu, L. Ping, X.Ge, Y. Wang, J. Fu, "Cloud Storage as the Infrastructure of Cloud Computing," *Intelligent Computing and Cognitive Informatics (ICICCI), International Conference. 2010*, pp.380-383.

[18] Houmansadr, A. Zonouz, S.ABerthier, R., "A cloud-based intrusion detection and response system for mobile phones," Dependable Systems and Networks Workshops (DSN-W), IEEE/IFIP 41st International Conference. 2011, pp.31-32.

[19] S. Hsueh, J. Lin, M.Lin, "Secure cloud storage for convenient data archive of smart phones," *Consumer Electronics (ISCE), IEEE 15th International Symposium.* 2011, pp.156-161.

[20] Houmansadr, A. Zonouz, S.ABerthier, R., "A cloud-based intrusion detection and response system for mobile phones," Dependable Systems and Networks Workshops (DSN-W), IEEE/IFIP 41st International Conference. 2011, pp.31-32.

[21] Y. Wang, X. Wen, Y. Sun, Z. Zhao, T.Yang, "The Content Delivery Network System Based on Cloud Storage," Network Computing and Information Security (NCIS), International Conference. 2011, vol.1, no., pp.98-102.

[22] Dong-Ju Kim and Kwang-Seok Hong , "Multimodal Biometric Authentication using Teeth Imageand Voice in Mobile Environment" , IEEE Transactions on Consumer Electronics, Vol. 54, No. 4, NOVEMBER 2008.

[23] Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong , "Person Authentication using Face, Teeth and Voice Modalitiesfor Mobile Device Security", IEEE Transaction on Consumer Electronics, Vol.56, No. 4, November 2010.

[24] Qian Tao and Raymond Veldhuis. "Biometric Authentication Systemon Mobile Personal Devices" IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 59, NO. 4, APRIL 2010.

[25] Phone Lin, Senior Member, Shin-Ming Cheng, Member, and Wanjiun Liao, Senior Member. "Modeling Key Caching for Mobile IP Authentication, Authorization and Accounting (AAA) Services". IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009.

[26] PengKunyu, ZhengJiande and Yang Jing. "AN IDENTITY AUTHENTICATION SYSTEM BASEDON MOBILE PHONE TOKEN" Proceedings of IC-NIDC2009.

[27] Hung-Min Sun and Muh-ChyiLeu. "An Efficient Authentication Scheme for AccessControl in Mobile Pay-TV Systems". IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 11, NO. 5, AUGUST 2009

[28] Xuefei Cao, XingwenZeng, *Member, IEEE*, Weidong Kou, *Senior Member, IEEE*, and Liangbing Hu. "Identity-Based Anonymous Remote Authentication for Value-Added Services in Mobile Networks" . IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58, NO. 7, SEPTEMBER 2009

[29] G. Antonios, "Towards new access control models for Cloud computing systems," pp. 1-6, 2004.

[30] C. Danwei, H. Xiuli and R. Xunyi, "Access Control of Cloud Service Based on UCON," pp. 559-564, 2009.

[31] R. AusankaCrues, "Methods for Access Control: Advances and Limitations," pp. 1-5, 2001.