การประมวลผลแบบเมฆ
Single Sign-On in Cloud Computing

ดร. ธนัญชัย ตรีภาค[1]

บทคัดย่อ

การประมวลผลแบบเมฆ (cloud computing) เป็นเทคโนโลยีที่ได้รับความนิยมมากขึ้นเรื่อย ๆ จากจุดเด่นด้านความยืดหยุ่นในการบริหารจัดการทรัพยากรระบบ แต่ด้วยคุณลักษณะการทำงานที่เป็นสถาปัตยกรรมแบบกระจาย ทำให้การประมวลผลแบบเมฆจำเป็นต้องมีการรักษาความปลอดภัยในระดับสูง นอกจากนี้ในการประมวลผลแบบเมฆซึ่งมีบริการที่หลากหลายให้บริการอยู่ภายในเครือข่ายจำเป็นต้องมีระบบพิสูจน์ตนที่มีประสิทธิภาพ เพื่อให้ผู้ใช้งานสามารถใช้งานบริการต่าง ๆ ได้อย่างสะดวก รวดเร็ว และปลอดภัย จากความต้องการทั้งหมดทำให้ระบบการพิสูจน์ตนที่เหมาะสมที่จะใช้งานภายในการประมวลผลแบบเมฆคือระบบการพิสูจน์ตนแบบลงชื่อเพียงครั้งเดียว (single sign-on)

คำสำคัญ: การประมวลผลแบบเมฆ, การพิสูจน์ตนแบบลงชื่อเพียงครั้งเดียว

Abstract

Cloud computing technology has become increasingly popular from the advantage of flexibility in system resource management. However, a distributed architecture of cloud computing require a high level of security method. Furthermore, many service providers in cloud network need efficient authentication system to identify many users from various systems. To hide any complexity and maintain security level, the suitable authentication method for every users who require access many services in cloud computing is single sign-on

Keywords: cloud computing, single sign-on authentication

[1]อาจารย์ประจำสาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
E-mail: ktthanun@yahoo.com

ความนำ

การประมวลผลแบบเมฆ (cloud computing) เป็นโมเดลสำหรับระบบสารสนเทศขนาดใหญ่ซึ่งมีวัตถุประสงค์เพื่อสร้างสภาวะการให้บริการแบบกระจาย (distributed service environment) โดยสามารถปรับเปลี่ยนปริมาณทรัพยากร (resources) ได้อย่างอิสระตามความต้องการ (requirements) ของผู้ใช้งาน โดยระบบประมวลผลแบบเมฆจะซ่อนการเชื่อมต่อและบริหารจัดการทั้งหมดไว้ไม่ให้ผู้ใช้งานทราบองค์ประกอบและการเชื่อมต่อภายใน (Cisco Systems, Inc., 2012) โดยผู้ใช้งานจะมองสิ่งต่าง ๆ ภายในเป็นเพียงจุดให้บริการเท่านั้น ซึ่งคุณลักษณะของการประมวลผลแบบเมฆตามนิยามของ NIST (National Institute of Standard and Technology, 2011) คือ

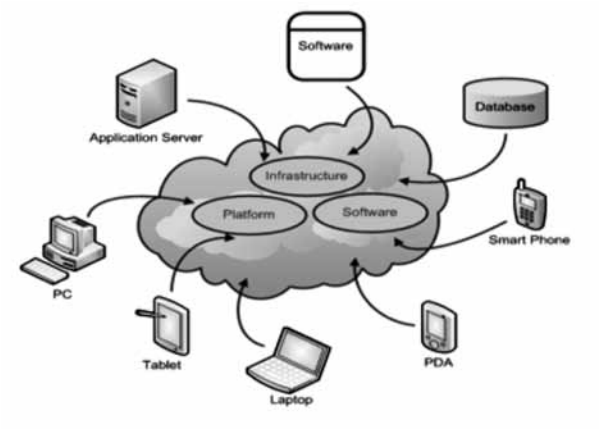
- ผู้ใช้บริการสามารถปรับเปลี่ยนการใช้ทรัพยากรภายในระบบได้ด้วยตนเอง ตามความต้องการที่เปลี่ยนแปลงไปโดยอัตโนมัติ

- ผู้ให้บริการสามารถบริหารจัดการทรัพยากรของตนเองแบบรวมศูนย์ (resource pooling) และให้บริการกับผู้ใช้บริการหลายคนได้ ทำให้ผู้ให้บริการสามารถบริหารทรัพยากรระบบได้เป็นอย่างดี

- การเปลี่ยนแปลงความสามารถในการให้บริการของระบบได้อย่างรวดเร็ว จนผู้ใช้งานอาจรู้สึกว่าระบบมีทรัพยากรให้ใช้งานไม่จำกัด

- มีระบบตรวจสอบการใช้ทรัพยากรและควบคุมการใช้ทรัพยากร เช่น หน่วยเก็บข้อมูล ระบบเครือข่าย ปริมาณผู้ใช้งานระบบ หรือโพรเซสในระบบ อย่างละเอียด ทำให้สามารถปรับเปลี่ยนการใช้ทรัพยากรต่าง ๆ ได้อย่างรวดเร็ว

- บริการต่าง ๆ สามารถเรียกใช้งานได้ผ่านระบบเครือข่าย โดยใช้กระบวนการเชื่อมต่อที่กำหนดเป็นมาตรฐาน โดยใช้เครื่องลูกข่ายในลักษณะต่าง ๆ ได้ เช่น เครื่องคอมพิวเตอร์ โทรศัพท์มือถือ หรืออุปกรณ์ต่าง ๆ ที่สามารถเชื่อมต่อเครือข่ายได้ ดังภาพ



ภาพ 1 คุณลักษณะของระบบ Cloud Computing

Single Sign On ในระบบประมวลผลแบบเมฆ

เนื่องจากระบบประมวลผลแบบเมฆเป็นรูปแบบหนึ่งของการประมวลผลแบบกระจาย (distributed computing) ซึ่งการประมวลผลและทรัพยากรต่าง ๆ จะไม่ยึดติดอยู่ในตำแหน่งใด ๆ ในเครือข่าย บริการต่าง ๆ สามารถเปลี่ยนตำแหน่งและเปลี่ยนจากระบบหนึ่งไปยังอีกระบบหนึ่งได้โดยอัตโนมัติ จากสถาปัตยกรรมดังกล่าวทำให้การพิสูจน์ตนของผู้ใช้งานเพื่อเข้าใช้บริการในระบบประมวลผลแบบเมฆเป็นเรื่องที่ต้องดูแลเป็นพิเศษ บริการการระบุตัวตน (Identity as a service--IDaaS) ในระบบประมวลผลแบบเมฆจึงเกิดขึ้นโดยมุ่งเน้นให้เกิดการทำงาน คือ การพิสูจน์ตัวตน (authentication) การกำหนดสิทธิการเข้าถึงทรัพยากร (authorization) การตรวจสอบการทำงาน (auditing) และการบริหารบัญชีผู้ใช้ (account management) นอกจากการใช้งานระบบประมวลผลแบบเมฆแบบพื้นฐานที่ต้องใช้ IDaaS ช่วยในการระบุตัวตนผู้ใช้งานแล้ว ในการใช้งานบริการอื่น ๆ ในระบบประมวลผลแบบเมฆซึ่งผู้ใช้งานในระบบหนึ่งมักมีการร้องขอเพื่อขอใช้บริการในระบบงานอื่น ๆ เสมอ จึงมีการพัฒนาระบบ Single Sign On ในระบบประมวลผลแบบเมฆขึ้น เพื่อให้ผู้ใช้งานสามารถเข้าใช้งานบริการที่หลากหลายโดยสะดวกปลอดภัยโดยรหัสเดียวกันทั้งหมด ผู้ดูแลระบบสามารถบริหารจัดการบัญชีผู้ใช้ได้อย่างมีประสิทธิภาพ และเพิ่มความปลอดภัยในการใช้งานบริการต่าง ๆ ให้ผู้ใช้งานมีความเชื่อมั่นว่าจะยังคงรักษาความเป็นส่วนตัว (privacy) ได้

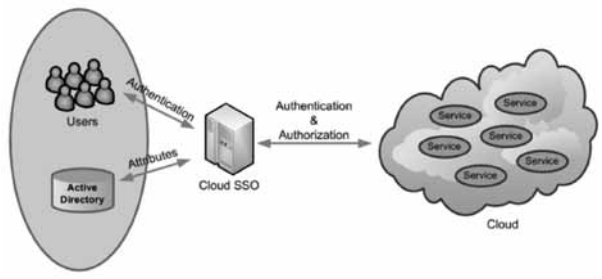
ในการนำ Cloud SSO มาใช้งานมีวัตถุประสงค์คือป้องกันผู้ใช้งานในการใช้บริการภายนอก โดยทำให้ผู้ใช้งานสามารถใช้งานบริการได้อย่างถูกต้องปลอดภัยและมีความสะดวกถึงแม้ว่าจะมีการใช้บริการที่หลากหลายก็ตาม และทำการป้องกันบริการภายในระบบจากผู้ใช้งานภายนอก โดยทำให้บริการต่าง ๆ มั่นใจได้ว่าผู้ใช้งานที่ร้องขอบริการเป็นผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบ และมีการร้องขอจากระบบที่เชื่อถือได้เท่านั้น เพื่อป้องกันการโจมตีหรือลักลอบใช้บริการ โดยการจะบรรลุวัตถุประสงค์หลักทั้ง 2 ข้อได้ ระบบ Cloud SSO จะต้องมีองค์ประกอบพื้นฐานที่สามารถทำงานร่วมกันได้ดังนี้

1. ผู้ใช้งานระบบที่จะขอใช้งานบริการต่าง ๆ โดยจะป้อนชื่อผู้ใช้และรหัสผ่านหรืออาจจะใช้ Secure Token อื่น ๆ เพื่อขอพิสูจน์ตัวตนของผู้ใช้งานในระบบงาน

2. Directory Service ที่เก็บข้อมูลต่าง ๆ ที่จำเป็นในการพิสูจน์ตัวตนของผู้ใช้งานภายในระบบ

3. ซอฟต์แวร์ หรือระบบที่ให้บริการ Cloud SSO เพื่อทำการพิสูจน์ตัวตนของผู้ใช้งานระบบแล้วทำการส่งข้อมูลไปยังบริการต่าง ๆ เพื่อสร้างความน่าเชื่อถือ (trust) ในระบบ โดยอาจส่งรายละเอียดเกี่ยวกับการพิสูจน์ตัวตนและการให้สิทธิ หรือการทำบัญชีผู้ใช้ให้สอดคล้องกัน (account sync) กับบริการต่าง ๆ

4. บริการต่าง ๆ ที่ให้บริการในการประมวลผลแบบเมฆ ซึ่งรองรับการทำ Single Sign On เมื่อมีการขอใช้บริการ



ภาพ 2 การเชื่อมต่อในการทำ Single Sign-On ใน Cloud Computing

โดยกระบวนการพิสูจน์ตัวตน และการสร้างความเชื่อถือระหว่างบริการต่าง ๆ ของ Cloud SSO จะใช้เทคโนโลยีและมาตรฐานอื่น ๆ เพื่อสนับสนุนการทำงาน ยกตัวอย่างเช่น

• Security Assertion Markup Language (SAML) ซึ่งเป็นมาตรฐานสำหรับการพิสูจน์ตนและพิสูจน์สิทธิในการทำ SSO ซึ่งมีการรับส่งข้อมูล XML ที่เกี่ยวข้องกับการทำการพิสจน์ตนและพิสูจน์สิทธิระหว่าง identity provider และ service provider ของโดเมนต่าง ๆ เหมาะสำหรับการประยุกต์ใช้ในการทำ SSO ข้ามระบบ ซึ่งเป็นมาตรฐานที่ผู้ให้บริการ SaaS Application ต่าง ๆ นำมาประยุกต์ใช้อย่างกว้างขวาง SAML เป็นมาตรฐานหนึ่งที่ไม่มีการใช้รหัสผ่านในการทำงาน โดย SAML จะป้องกันบริการต่าง ๆ โดยการสร้าง trust กับ identity provider เพื่อตรวจสอบ user identity

• WS-Federation เป็นรายละเอียดกระบวนการที่ทำให้ security realms ที่แตกต่างกัน สามารถสื่อสารกันเพื่อแลกเปลี่ยนข้อมูลเกี่ยวกับ identity identity attributes และการพิสูจน์ตนระหว่างกันได้

• OpenID เป็นเทคนิควิธีการที่ผู้ให้บริการใช้ในการพิสูจน์ตัวตนผู้ร้องขอใช้งานระบบ โดยการ redirect หน้าต่างเว็บบราวเซอร์ไปยัง identity provider ของผู้ใช้งานระบบที่เชื่อถือได้เพื่อทำการพิสูจน์ตัวตนผู้ใช้งาน ซึ่งการออกแบบของ OpenID ออกแบบสำหรับการใช้งานกับเว็บบราวเซอร์เป็นหลักและใช้งานผ่าน HTTP Protocol

• OAuth เป็นมาตรฐานเปิดสำหรับการพิสูจน์ตัวตนผู้ใช้งาน โดยจะทำการแลกเปลี่ยน Authentication Token เพื่อทำการพิสูจน์ตน ผ่านโพรโตคอลที่หลากหลาย หรือเรียกผ่าน API เฉพาะต่าง ๆ ทำให้ผู้ใช้งานสามารถอนุญาตให้ระบบอื่น ๆ เข้าถึงข้อมูลของตนเองที่เก็บอยู่ใน Service Provider ใด ๆ ได้โดยไม่ต้องให้ข้อมูลเกี่ยวกับ Permission ของข้อมูลของตนเองในระบบงานนั้น ๆ

นอกจากนี้บริการใดที่ต้องการเชื่อมต่อกับระบบ SSO ยังสามารถสร้างระบบพิสูจน์ตัวตนโดยใช้ HTML Form เพื่อให้ผู้ใช้งานป้อนข้อมูลชื่อผู้ใช้และรหัสผ่าน

หรือสร้างเป็น API เพื่อให้ระบบ SSO ต่าง ๆ ที่เชื่อมต่อด้วยสามารถเรียกใช้งานได้ สำหรับผลิตภัณฑ์ที่มีอยู่ในท้องตลาดที่สามารถให้บริการ Cloud SSO ได้ยกตัวอย่าง เช่น

• PingFederate® และ PingConnect™ ของบริษัท Ping Identity ซึ่งใช้เทคโนโลยีหลักในระบบคือ SAML และ WS-Federation (Ping Identity Corporation, 2011)

• Intel Cloud SSO ของบริษัท Intel ซึ่งใช้เทคโนโลยีหลักคือ SAML OpenID และ OAuth (Intel Corporation, 2012)

• Cloud Identity Manager ของบริษัท McAfee ซึ่งใช้เทคโนโลยีหลักคือ SAML, OpenID, OAuth (McAfee, Inc., 2012)

สรุป

เทคโนโลยีการประมวลผลแบบเมฆมีการใช้งานอย่างแพร่หลายมากขึ้น ซึ่งจากคุณลักษณะที่เป็นสถาปัตยกรรมแบบกระจายของการประมวลผลแบบเมฆทำให้การเรียกใช้บริการที่มีอยู่หลากหลายภายในระบบประมวลผลแบบเมฆของผู้ใช้งานแต่ละคนมีความยุ่งยากมาก กระบวนการพิสูจน์ตัวตนแบบลงชื่อเพียงครั้งเดียวจึงถูกนำมาใช้ โดยการนำเทคโนโลยีต่าง ๆ มาประยุกต์ใช้งาน เช่น SAML, OpenID, OAuth หรือ WS - Federation ซึ่งจะทำให้เกิดผลลัพธ์เดียวกันคือผู้ใช้งานสามารถใช้บริการต่าง ๆ ภายในการประมวลผลแบบเมฆได้โดยง่าย โดยทำการพิสูจน์ตนเพียงครั้งเดียว และบริการต่าง ๆ ภายในการประมวลผลแบบเมฆจะเชื่อถือและอนุญาตให้ผู้ใช้งานที่ผ่านการพิสูจน์ตัวตนสามารถใช้งานได้ตามสิทธิที่ระบุ

เอกสารอ้างอิง

National Institute of Standard and Technology. (2011). *The NIST definition of cloud computing*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Ping Identity Corporation. (2011). *Cloud single sign-on & federated identity*. Retrieved from https://www.pingidentity.com/resource-center/SSO-and-Federated-Identity.cfm

Intel Corporation. (2012). *Cloud identity buyer's guide*. Retrieved from http://www.intelcloudsso.com/pdfs/Intel-Cloud-SSO-Buyers-Guide.pdf

Cisco Systems, Inc. (2012). *Cisco cloud computing-data center strategy, architecture, and solutions*. Retrieved from http://www.cisco.com/web/strategy/docs/gov/CiscoCloudComputing_WP.pdf

McAfee, Inc. (2012). *McAfee cloud identity manager*. Retrieved from http://www.mcafee.com/us/resources/data-sheets/ds-cloud-identity-manager.pdf