Federated Identity Management for the Cloud

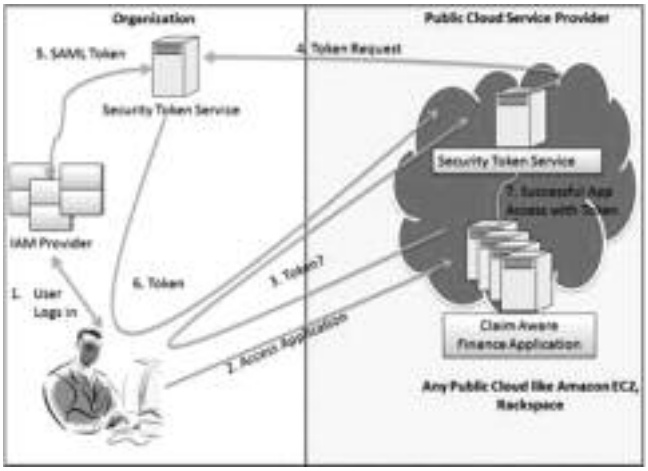
Mohammad Jabed Morshed Chowdhury

Areas such as eGovernment, eMedicine, media, and telecommunications are becoming more dependent on data storage services. Emerging high quality digital media formats require larger storage facilities. The emergence of digital devices (smart phones, tablets, etc.) generates additional data such as photos, videos, etc. which preferably has to be backed up even though that data is not often used. Thus data storage services are gaining a significant role in our lives.

Moving data storage services to the cloud has its advantages and disadvantages. Businesses and individuals can achieve capital cost savings and simplify their operations with cloud storage, since they do not have to invest in their own storage servers nor do they have to maintain them. Most importantly these cloud storage services are scalable; with a few simple clicks your storage capacity will be expanded. Technical support, hardware renewal, and upgrades are no longer the customers' responsibility. Although these features seem very tempting, many customers are not rushing to transfer their data into the cloud.

Moving data into the cloud offers great convenience to users since they don't have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) are both well known examples. While these Internet-based online services provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon's S3 is such an example.

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. However, this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. Last but not the least, the deployment of Cloud Computing is powered by data centers running in a simultaneous, cooperated and distributed manner. Individual user's data is redundantly stored in multiple physical locations to further reduce the data integrity threats.



Federated Identity in Public Cloud

The final barrier to adopting cloud storage is usually whether it is sufficiently secure. Privacy issues, data leakage, improper data sanitization; all of these and a lot more are reasons why a customer will choose a particular cloud storage provider.

Additionally, changes in the customer's requirements or in the provider's offering may lead the customer to migrate their storage to another cloud storage provider. Providing a secure service which handles sensitive data transfers between cloud storage providers in a federated cloud is an interesting and new problem domain. Data transfers between the customer and the provider and between providers must be handled securely. Achieving this security is the obvious objective, but this has to be done in the context of maintaining compliance with the customer's security policies and meeting various regulatory and legislative requirements. Traditional security mechanism is not very effective for cloud environment. A new service scheme is proposed which utilizes various encryption techniques and also includes identity and key management mechanisms, such as "federated identity management".

Identity federation conquers the concern of "securely" managing identities, enabling the organization to share employee identity information with the Cloud Service Provider (CSP) or any other resource over the Internet. This allows the organization to boost their control over "who" has access to "what" information and resources, regardless of where those resources. Federated identity management improves security by controlling access on an operation base and providing a detailed audit trail.

Federated identity management enables : easier access to consume cloud resources, superior end-user experience through SSO and just-in-time account provisioning, reduced cost and time to incorporate authentication and authorization and elimination of non-scalable proprietary SSO applications

Identity Federation can be accomplished any number of ways with the use of formal internet standards such as SAML, Information Cards, and OpenID etc. Identity Federation has following solution areas:

Single Sign On, 2. Application based Web Services Security and 3. Identity Lifecycle CJ