P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2012,(6), (2) :22-33

Management of Identity and Access in the Cloud.

Sufyan T. Faraj* **Sameeh Abdulghafour Jassim*** **Kashif Kifayat****

*University of Anbar - College of Computer
**LJMU-School of Comp. & Math.Liverpool, UK

ARTICLE INFO

Received: 00 / 00 /00
Accepted: 00 / 00 /00
Available online: 9/12/2012
DOI: 10.37652/juaps.2012.63234

Keywords:
Access Control;
Cloud computing;
Cryptography;
Identity and access management;
Security.

ABSTRACT

Cloud computing is new technology that provides cheaper, easier, and more powerful processes to customers over internet. The cloud service provider (CSP) provides virtualized resources on Internet instead of using software or storage on a local computer. The economic benefits are the main reason for using cloud computing. Cloud computing dynamically delivers everything as a service (XaaS) over the internet based on user demand, such as network, operating system, storage, hardware, software, and resources. Thus, many security and privacy issues must be taken into consideration. The services of cloud computing are usually classified into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This paper aims to achieve two main goals. The first is to review the field of cloud computing with an emphasis on the identity and access management (IAM) in the cloud. Secondly, we will report on our ongoing work for developing a novel system for IAM based on the techniques of Identity-Based Cryptography (IBC) security mediated cryptography. The proposed system architecture will be outlined along with some of the major operational steps.

Introduction

The great developments that have happened in computer technology and Internet are opening up the era of cloud computing. Cloud computing is now used by global companies such as Amazon, Microsoft, Google, and IBM to provide cheaper and easier services on demand for end users over the internet. This is mainly achieved by combining several computing resources which are in different places instead of using software or storage on a local computer.

Cloud Computing is a modern technology which is developed in last few years. The US National Institute of Standards and Technology (NIST) defines it as follows:"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models"[1].

* Corresponding author at: University of Anbar - College of Computer.E-mail address: sufyantaih@ieee.org

This is definition is depicted in Figure 1. The three delivery models of cloud computing are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS), While the four deployment models of cloud computing include public, private, community (a subset of public/private), and hybrid clouds.

Another definition of cloud computing was also proposed by Buyya et al in terms of its utility to end user: "A Cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers" [2].

Cloud Computing systems includes a large amount of various computing resources, most data and software reside on the Internet, and it provide digital identity for users to access their services, This requires more flexibility for the users. Using cloud computing service, users can store their critical data in servers and can access their data anywhere and anytime via the

Internet and they should not worry about system attacks, breakdown, or disk faults [3].As there are many vulnerabilities that need to take care of them in cloud computing, this brings some challenges for the system, especially security and privacy.

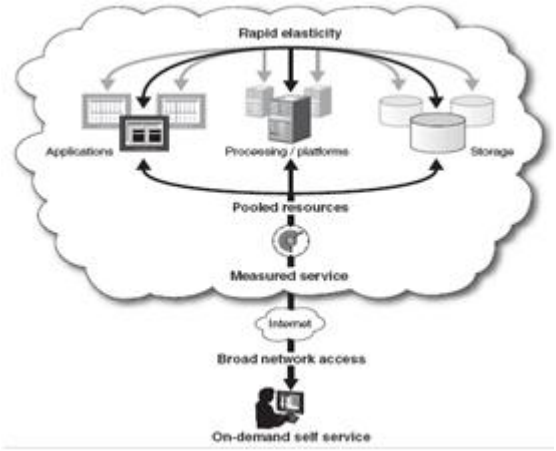

Figure 1.Cloud computing according to NIST definition [1]

Cloud computing provides services to customers at low cost and on-demand over the network. Because the cloud computing transactions involve money and also cloud computing contain sensitive information, the data must be protected from unauthorized person. Protecting personal privacy and proprietary information from unauthorized user can be done by keeping authorized restrictions on access and disclosure. Managing user's identity and providing adequate privacy and protection will be a great challenge because most providers are depending on different information systems to provide their services.

Cloud computing model uses virtual machines. This enables the cloud service provider (CSP) to share the cloud infrastructure located in a datacenter between multiple customers and cloud computing services[4]. The customer does not need to maintain servers, train IT employees or even purchase software licenses[5]. Hence, the customer has transparency. This leads to lower cost in many things that are usually required by users such as management, training, power consumption, infrastructure maintenance, and storage space. Also, cloud computing can offer a high security for datacenters located in secret and well-protected places.

Furthermore, cloud computing increases scalability (if the customer demand is increased then computer capability is responded and can grow), expediency in new service roll out, availability (a failure of one component will not disconnect all components), and mobility [5]. Cloud computing increases the flexibility of organizations due to information sharing and collaboration (multi-tenancy).The characteristics of clouds include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service[6].

The remaining of this paper is organized as follows: Section 2 describes in detail various cloud computing models and services. The issue of identity and access management (IAM) in cloud computing environments is explored in Section 3. Then, some significant earlier works in the field of IAM in cloud computing are reviewed in Section 4. Our proposed IAM system that is based on combined techniques of Identity-Based cryptography (IBC) and mediated cryptography (mediated RSA) is introduced in Section 5. Finally, the paper is concluded in Section 6.

Cloud Computing Services and Types

The most important advantages of cloud computing can be summarized as follows [7]:

- Cloud computing is easy to be used, and do not need high quality equipment from users.
- The user that use cloud computing do not need to worry about the problems such as data loss or virus, because cloud computing provides dependable and secure data storage center.
- Cloud computing can realize data sharing between different equipment.
- Cloud provides nearly infinite possibilities for users to use internet.

A. Types of Cloud Services

Cloud computing vendors are classified into three main categories based on the fundamental nature of the cloud-based solution they provide: IaaS, PaaS, or SaaS[8]. The three fundamental classifications are often referred to as the "SPI Model", where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively.

SaaS is a way of providing users with software through the Internet(See Figure 2). In the cloud, users do not required to purchase the software rather the payment will be based on pay-per-use model. The provider offers everything to the costumers in order to use the provider's applications running on a cloud infrastructure. Various client devices can access on-demand to the provider's applications through a thin client interface such as a web browser. The cloud service provider (CSP) controls and manages the underlying of cloud infrastructure including network, servers, operating systems, storage, etc.[9], [10]. Thus cloud computing can provide transparency to the end user. SaaS also operates on the virtualized and pay-per-use costing model whereby software applications are leased out to contracted organizations by specialized SaaS vendors. SaaS applications are accessed using web browsers over the Internet therefore web browser security is vitally important[11], [12].

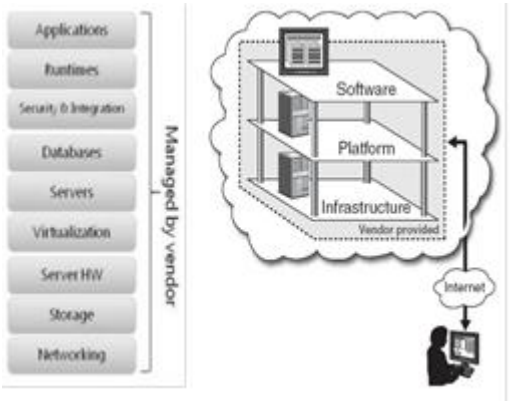

Figure 2.Software as a Service (SaaS) [9].

In PaaS, the cloud provider provides the hardware, and also provide a toolkit and a number of supported programming languages to build higher level services (i.e. software applications that are made available as part of a specific platform). The users of PaaS are typically software developers who host their applications on the platform and provide these applications to the end-users[5]. The concept of PaaS is illustrated in Figure 3.

The number of the services that are available in the cloud increases, so a platform has to be developed to effectively leverage these services. This platform not only provides a place where applications can be stored and deployed, but also an IDE (Integrated Development Environment) that supports a complete life cycle for developing applications that can be easily made available on the Internet. With PaaS, the cost and complexity of evaluating, buying, configuring, and managing all of the hardware and software needed to develop an application is drastically lowered. This is because the development tools (IDE, Graphic User Interface (GUI) Tools, database connectivity, etc.) and delivery tools (hosting, metering, storage, etc.) are made available inside the cloud itself. The advantage of PaaS is related to the fact that customers are not required to invest in expensive hardware or software to develop or make use of the applications offered in the cloud[9]. The CSP manages and controls the underlying infrastructure, and the costumers control and configure the deployed applications and platform. Consumers can deploy consumer-created or acquired applications created using programming languages and tools supported by the provider[12].

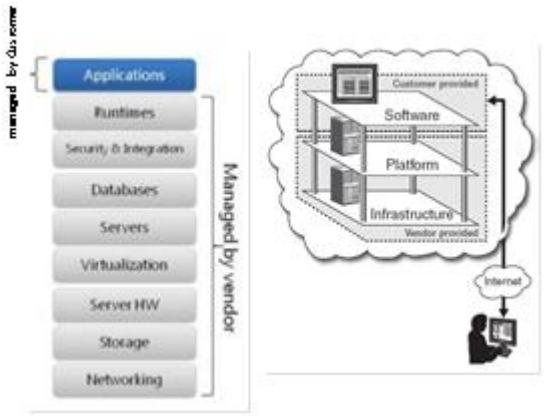

Figure 3. Platform as a Service(PaaS)

In IaaS (See Figure 4), the vendor provides physical computer hardware including CPU processing, memory, data storage, and network connectivity. Clients purchase resources as a fully outsourced (datacenters and IT services) service (servers, software, data center space or network equipment). IaaS delivers a platform virtualization environment as a service[13]. There are many providers for IaaS such as Amazon S3 and Sun's Cloud Service[14]. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)[12]. IaaS services can further be categorized as hardware-as-a-

service (Amazon Web Services, for example), database-as-a-service (which Oracle and Enterprise DB offer), and storage-as-a-service (such as Amazon Simple Storage Service)[8].

B.Types of cloud computing:

There are four deployment models of cloud computing (Public clouds, Private clouds, Community clouds, Hybrid clouds) depending on their own characteristics, as illustrated in Figure 5. And there are four owner characteristics used to describe the deployment models: (i) who owns the infrastructure; (ii) who manages the infrastructure; (iii) where is the infrastructure located; and (iv) who accesses the cloud services [3].Table 1 summarizes the four primary cloud deployment models. These deployment models are described as follows:

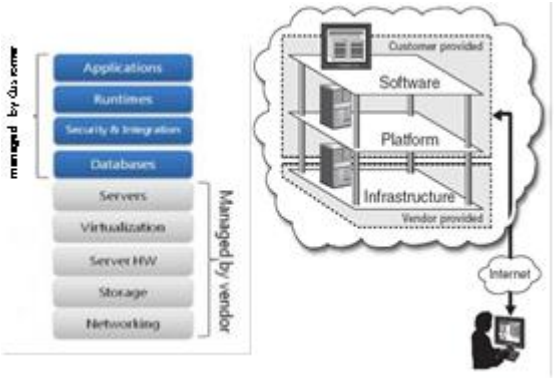

Figure 4. Infrastructure-as-a-Service (IaaS)

1. *Public Cloud:* Generally the service provider manages and owns the physical infrastructure. The provider owns and runs the technology to deliver the service and the costumers have no control over the operations of the service. It makes the resources available to the customers over a public network like the Internet. Usually the company documents which use the public cloud are stored outside its buildings by a third party which they trust. It raises concerns about the data privacy security since the computing infrastructure (computers, network and storage) is contained remotely outside the firewall of the company[15]. Public cloud providers need high speed network to support thousands of public domain users and datacenters[6]. Some of the famous public clouds are Amazon Web Services (AWS), Microsoft Azure Google, and AppEngine. A public cloud can offer any of the three types of services: IaaS, PaaS, and SaaS. For example, Amazon EC2 is a public cloud providing infrastructure as a service, Google AppEngine is a public Cloud providing an application development platform as a service, and Salesforce.com is public Cloud providing software as a service[6]. There are two main benefits for a public cloud: (i) cost effective; (ii) and an external provider performs the security. And two disadvantage to a public cloud which include: (i) client concerns about the level of security, (ii) and the difficulties with a provider showing securing compliance[5].
2. *Private Cloud:* In private clouds the resources are not shared by other entities and the service is implement for a single organization, The private Cloud services access is restricted to one or few organizations, So its offer greater control over the infrastructure, improving security and service resilience[6]. Private cloud perhaps is managed by the organization or a third party, and may exist on-buildings or off-buildings[10]. Private cloud is only accessible by the company and its users via a local network or virtual private network connections from outside. Vendor controls the maintenance schedule and the upgrades. If hardware fails, the server is automatically booted on the remaining node[15]. IT infrastructure of the private cloud allows custom configuration and implementation according to business processes[16]. Private cloud differs from the public cloud in that the organization is managing all the cloud resources and applications by itself, similar to Intranet functionality. Secure of utilization of the private cloud can be much more than that of the public cloud because of its specified internal exposure. Only the organization and designated stakeholders may have access to operate on a specific private cloud[11]. There are two main benefits to a private cloud: (i) it is the “most secure model” based on a client implementing the solution in a secure manner; and (ii) it is of a "more efficient use of physical IT assets" when contrasted with a traditional data center. However, it also has three disadvantages to a public cloud: (i) more cost (loss of monetary efficiencies and savings gained from an outsourced cloud), (ii) traditional data implementation difficulties

cannot be solved by a private cloud, and (iii) the burden of internal network management[5].

3. *Community Clouds:* This model attempts to obtain most of the security benefits of a private cloud, and most of the economic benefits of a public cloud. It is a private cloud that is shared by several organizations with similar security requirements and a need to store or process data of similar sensitivity[17]. Community clouds perhaps are managed by the organizations or a third party and may exist on- buildings or off-buildings[10]. There are three benefits to a community cloud which include: (i) community cloud is custom-made, which means it can meld to response with given standards; (ii) it contains the economic efficiencies and advantages of a public cloud; and (iii) the customer is only required to pay for services used. And there is one disadvantage to a community cloud solution which is the potential for data leakage[5].

4. *Hybrid Cloud:* The hybrid cloud is composed of two or more cloud types (private, community, or public). Hybrid cloud deployment model have three necessary characteristics to build the foundation of it. First, overcoming the barriers of varied clouds must be achieved with interfaces, middleware and standards. Second, the integration of heterogeneous cloud environments of different companies and third-party vendors to a homogenous interface for the end user. Third, establishing trust between customers (companies) and vendors for data security and compliance[16]. A hybrid cloud provides more secure control of the data and applications and allows various parties to access information over the Internet. It also has an open architecture that allows interfaces with other management systems[11].

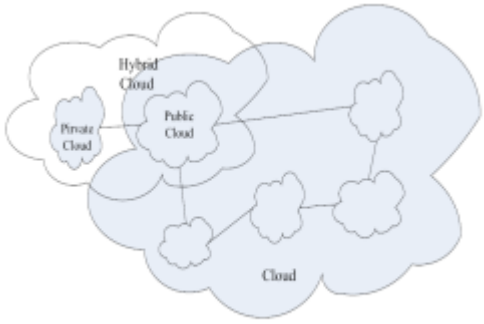

Figure 5. Cloud types

Table 1. The four primary cloud deployment models

5.	6. 7. 8. Managed 9. by	10. 11. Infrastructure Owned 12. By	13. 14. 15. Infrastructure Located	16. 17. Accessible 18. and Consumed 19. By
20. Public	21. 3rd party provider	22. 3rd party provider	23. Off-premise	24. Untrusted
25. 26. Private/ Community	27. 3rdparty provider / 28. Organization	29. 3rd party provider / 30. Organization	31. Off-premise / on-premise	32. Trusted
33. 34. 35. Hybrid	36. Both Organization & 3rd party provider	37. Both Organization & 3rd party provider	38. Both Off-premise & on-premise	39. Trusted and Untrusted

C. Data Storage and Data location

Providers store data in the cloud redundantly by keeping redundant copies of the data at many different locations. This provides transparency to the customers. However, this also implies the fact that there are multiple copies of this data could be lying around in different corners of the world. Redundancy is required and data centers must be protected against physical compromising and modifying by other customers[18]. There may be locations where the data must travel following a non-optimal path because the ideal path crosses countries with restrictive laws. The exact location of data in the cloud is often unknown. Datacenters may be located in systems in other countries. The user might not even know what country the data will be stored in [19].

The cloud providers must not only worry about the data's location, but the path the data follows may also matter. The main compliance concerns with transporter data flows include whether the laws in the jurisdiction where the data was collected permit the flow, whether those laws continue to apply to the data post-transfer, and whether the laws at the destination present additional risks or benefits. Technical, physical and administrative safeguards, such as access controls, often are applied

[10]. For example, if the user datacenter is stored in X country then service providers will be subjected to the security requirements and legal obligations of X country. It may also happen that a user does not have the information of these issues[20].

Currently the user can choose the datacenter location that is provided by cloud providers. For instance, Amazon offers two locations in the US and one in Europe. Very likely, other providers will add to Amazon's region choice offer as the location of data is an increasing important requirement of potential customers[4].

Identity and Access Management

Unauthorized access to information resources in the cloud is a major concern for an organization, because the organizations have sensitive data and privacy information[21]. Identity and access management (IAM) is a critical function for every organization[22]. IAM can be defined as the "methods that provide an adequate level of protection for organization resources and data through rules and policies which are enforced on users via various techniques such as enforcing login password, assigning privileges to the users and provisioning user accounts"[14]. Managing user's identity and providing adequate privacy and protection in the cloud is a great challenge because most providers are depending on different information systems to provide their services.

There are two main attributes related to users that are presence and location. Presence is associated with the real-time communication systems such as Instant Message (IM) and Voice over IP (VoIP). Such systems usually provide descriptions about users' status during or after the communication, whether they are idle or active, online or offline, etc. Geographic location can be specified by IP address of the entity[14].IAM can also be considered as the first layer of defense in cloud security. A cloud provider used IAM to (i) validate claimed user by verifying the user's credentials against a directory, and (ii) allow the customers to manage identities and authorizations to the resources of customers that are hosted by the vendor[18].

Users accessing cloud services have three features of IAM: Authorization, Authentication, and Auditing (AAA). Typically the trust boundary in any organization is mostly static and is monitored and controlled for applications which are deployed within the organization's boundary. The trust boundary is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication. The organization's trust boundary with cloud computing will become dynamic and the application, system, and network boundary of an organization will extend into the service provider domain. Thus, application security and user access controls must compensate for the loss of network control and to strengthen risk assurance[23].

A. Benefits of Identity and Access Management

IAM solutions offer to consumers and providers of cloud services a proven solution to protect critical IT assets within public, private, and hybrid clouds delivery models. Some of these IAM benefits are [24]:

- Improved controls by reduced security risk.
- Providing transparency by eased regulatory compliance.
- Reduced administrative expenses and improved efficiency.
- Improved IT agility through automated security processes.

B. Access Control

Access controls are known to be the security features that control how users and systems communicate and interact[5]. Access control encompasses all mechanisms which allow managers direct and control the system and user behavior. Managers control subjects (person, machine, or processes) and their permissions to access resources (read, write, or execute) in a system. If any of these mechanisms fail then the system will be exposed to exploitation. The attacks can take place by insiders or outsiders. Systems use access control mechanisms to decide which kind of accesses should be either allowed or denied in order to be able to protect resources and data[25]. There are many types of threats to access control in cloud computing such as frictionless registration processes, account hijacking, generic authentication attacks, and insecure IAM. These can be summarized as follows [5]:

- *Frictionless registration processes*: Frictionless registration means the ability to access to a cloud without credentials or authorized access. It was reported that enabling anyone with a credit card to access to a cloud, the cloud will be exposed to malicious activities such as spamming and propagating malicious code in an anonymous manner.
- *Account hijacking*: Attack methods to hijack an account include phishing, fraud, and exploitation of software vulnerabilities. These methods can be used to get password and access to the account and associated data.
- *Generic authentication attacks:* Cloud computing authentication mechanisms can be vulnerable to some attacks. Potentially vulnerable authentication data include user identities, passwords, biometric information, and user access capabilities.
- *Insecure IAM problems:* There are many insecure IAM problems which include the adoption and/or implementation of wrong AAA practices.

C. Virtualization

Users of cloud computing can get services anywhere, anytime, through any kind of terminal. Hence, security concerns must be taken into consideration if the virtualization technologies are used. The costumer can complete all what he/she wants through net service using a notebook PC or a mobile phone. Users can reach data or share it safely through an easy way, anytime, anywhere. A task can complete by users that can't be completed in a single computer[7].

Virtualization is the process of decoupling hardware from the operating system on a physical machine. A Virtual Machine (VM) is the virtualized representation of a physical machine that is run and maintained on a host by a software virtual machine monitor or hypervisor[26]. The ability to provide some form of virtualization often led to provide multi-tenant cloud services at the infrastructure, platform, or software level to create economic scale[10]. The level of virtualization of what is offered depends on which of the three (SaaS, PaaS, or IaaS) service models the user requires[4]. Virtualization of virtual machines allows cloud computing to make the most efficient use of the currently available physical resources[4]. The main reason for operating a virtualized IT environment is the reduction of hardware so that the cost is reduced. This can also improves management, security, and computing efficiency. Figure 6 visualizes a comparison between traditional and virtualized environments.

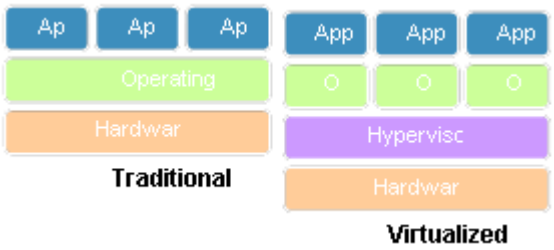

Figure 6. Traditional and Virtualized stack

Review of Some Related Work on IAM in Cloud Computing

In 2009, Yan at al [3] proposed an federated identity management system using Hierarchical Identity-Based Cryptography (HIBC) to provide strengthen cloud computing security. Most cloud computing systems use asymmetric and traditional public key cryptography to provide data security and mutual authentication. In this proposal, not only the key distribution but also the mutual authentication can be simplified in the cloud. IBC scheme is a kind of public-key based approach that can be used for two parties to exchange messages and effectively verify each other's signatures. Unlike in traditional public-key systems that using a random string as the public key, with IBC user's identity that can uniquely identify that user is used as the public key for encryption and signature verification. IBC can ease the key management complexity as public keys are not required to be distributed securely to others. Another advantage of IBC is that encryption and decryption can be conducted offline without the key generation center.

In the IBC approach, the private key generation center (PKG) should create a "master" public key and a corresponding "master" private key firstly, and then it will make this "master" public key public for all the interested users. Any user can use this "master" public key and the identity of a user to create the public key of this user. Each user wants to get his private key needs to contact the PKG with his identity. PKG will use the

identity and the "master" private key to generate the private key for this user.

The federated identity means a standard-based mechanism for different organization to share identity between them and it can enable the portability of identity information to across different networks. One common use of federated identity is secure Internet single sign-on. Using identity federation can increase the security of network since it only requires a user to identify and authenticate him to the system for one time and this identity information can be used in different networks. Using identity federation in the cloud also enables users from different clouds can use a federated identification to identify themselves[3].

In May2010, CA Technologies proposed three ways for IAM. CA's IAM include large enterprise as well as a small organizations cloud service providers. Each of these communities has different business goals and needs. Hence, CA Technologies divided these communities into three broad IAM/cloud categories [24]:

- *Extending the enterprise up to the cloud (IAM up to the cloud):*This method assumes enterprises will migrate applications and data off-premise to the cloud.
- *IAM to secure cloud service providers (IAM inside the cloud):*A cloud provider in this model can be a third-party offering public cloud services or an enterprise managing its own private cloud. So the resources of users they access must be secured and managed by public cloud service providers.
- *IAM services delivered down from the cloud (IAM down from the cloud):* This method puts separate IAM services in the cloud for on-demand consumption.

In 2010, B. Blakley (Burton Group) proposed trust cloud operating system. This cloud-based ecosystem has created a new ways for people to deploy, access, and use networked information, applications, and resources. This proposal contains a simplified trust cloud in the middle between customers and cloud providers. It can achieve authentication, authorization, network security, provisioning, and auditing. In this way, the system provides services to users transparently[27].

Proposed IAM for cloud computing

The attacker in grid computing attacks each system alone but in cloud computing the attacker can access to all computers in the cloud if he/she success to attack the hypervisor. This is a direct result of cloud computing is relying on virtualization. Thus, IAM is very important in cloud computing. This paper proposed anew way for IAM in cloud computing, as shown in Figure 7.The basic idea in this proposed system is to combine IBC and security mediated cryptography (SEM) to develop a trusted cloud (TC) entity that is responsible for IAM in the cloud environments. In this section, we are reporting on our ongoing work in developing this system. We will present the system general architecture and the basic operational steps. IBC is an interesting choice for IAM as they significantly reduce the key management issue and thus increase usability. On the other hand, mediated cryptography enables system administrator to efficiently achieve access control in a fine grained manner. The GC (Generator Center)and TC are considered as the trusted authority in this proposal. The general structure of proposed system consists of four main parts:

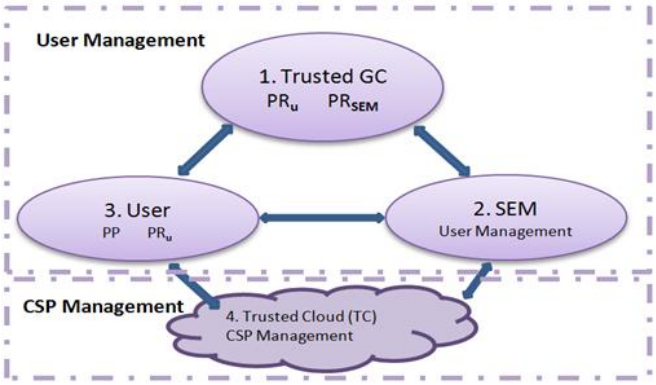

Figure 7.The general proposed system structure

1. *Trusted Generator Center (GC):*The first part of the system is the trusted GC. It has three responsibilities: generating a "master" private key and corresponding "master" public key (generating public parameters-PP), dividing the private key into two parts, and giving one for user and other for the SEM. There are many algorithms used to split the private key of user. GC will make the "master" public key public for all the interested users. Any user can use this "master" public key and the identity of a user (identity must be unique) to create the private key of this user. Each

user wants to get his private key needs to download public parameters and contact the GC with his identity(as shown in Figure 8). GC will use the identity and the "master" private key to generate the private key for this user. GC and the user need session key to exchange the key information secretly. The CG also verifies users' identities and establishes secure channels to transmit private keys.

2. Security Mediated Center (SEM): SEM is the second part of the system which will have the half of the user's private key(PR_{SEM}). SEM takes all the halves of the users' private keys from GC and stores them in the database with other information of user.SEM have many advantages such as: (i) the full operation cannot be accomplished without acceptance of SEM because it has the half of user private key, (ii) it manages all user activities such as (request, timestamp, authorization, etc.), and (iii) it sends to TC and user the half of user private key (PR_{SEM}). SEM adds a time period to the identifier of the user in order to solve the revocation problem. Revocation problems may occur because all the users in the system use some unique identifiers (such as email address, user's name, address, etc.) as their public keys. Hence, SEM adds some time period to the identifier of the user to control public keys of users and prevent (or reduce) the unauthorized usage of identities by an attacker if the attacker success to get user's private key.

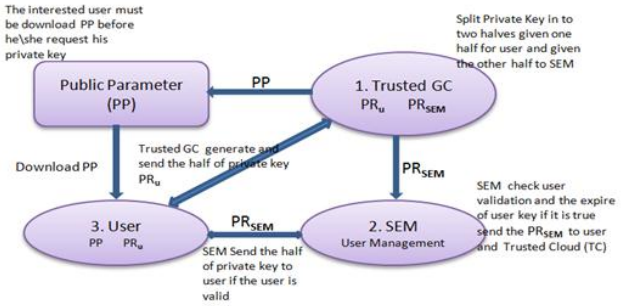

Figure 8. Upper part of proposed system architecture

3. *The Use:* The third part of the proposed system is the user which should download the parameters before requesting his private key from GC in order to use the system. GC will provide the user with the half of private key of him/her (PR_u). The SEM must provide the other half of user private key (PR_{SEM}). Then the user sends user private key (PR_u) and ID to Trusted cloud (TC). TC combines the two halves of private key (PR_{SEM} and PR_u) by using a suitable algorithm and generates the private key. TC can use symmetric cryptography method to encrypt the data (such as AES) and send it to client.

4. The Trusted Cloud (TC): TC is used to manage virtualization, federation, and update as shown in Figure 9. TC also manages all cloud server providers (CSPs). For example, if a user using Google CSP want to use another cloud provider (such as Amazon) of different infrastructure, then the user does not need to repeat the whole registration procedure. Using identity federation can increase the security of network since it only requires a user to identify and authenticate himself/herself to the system for one time and this identity information can be used in different networks. Using identity federation in the cloud enables users from different clouds to use a federated identification to identify themselves. Updates are done by TC to add new CSP or to add new branch for old CSP.

Security Assertion Markup Language (SAML) is an XML standard that allows secure web domains to exchange user authentication and authorization data. Using SAML, an online service provider can contact a separate online identity provider to authenticate users who are trying to access secure content. TC used SAML to contact the CSPs. There are three types of CSP: SaaS, PaaS and IaaS. In SaaS, CSP manages and controls the underlying infrastructure and the individual application capabilities, while in PaaS CSP manages and controls the underlying infrastructure, and the users control and configure the deployed applications and platforms. Finally in IaaS, the consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components.

If the user wants SaaS services, CSP of SaaS will use IaaS and PaaS to provide service to the user. Also if the user want PaaS services, CSP of PaaS will use IaaS to provide service to the user, as shown in Figure 10. CSPs can also cooperate with each other to provide more transparency to the users of cloud. So CSP of SaaS can

use or rent PaaS or IaaS or both from other CSP, or CSP of PaaS can use or rent IaaS from other CSP.

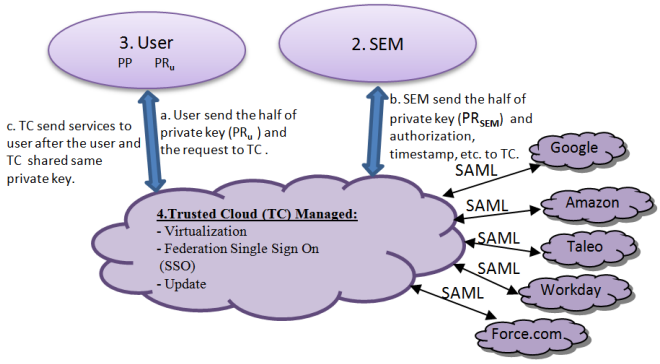

Figure 9. Lower part of proposed system architecture

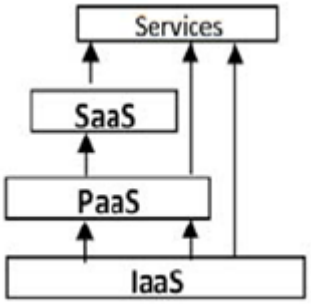

Figure 10. Types of services in CSPs

As our work is still in progress, we are trying to properly define and implement all the required security protocol such that to make the IAM system secure and robust against all possible attacks. Some of the basic cryptographic algorithms required to be implemented by the system are:

- *Setup:* GC creates a master key and the public system parameters (PP). The master key is kept secret and used to generate private key for users. Public system parameters are made public for all the users and can be used to generate users' public key with their identities.
- *Extract:* When a user requests his/her private key from the GC, the user at first must download PP from GC. Then GC will use the identity of this user, public system parameters PP and master key MK to generate a private key for this user. GC will divide the private key into two parts and giving one for user (PR_u) and other for the SEM (PR_{SEM}).
- *Verifying (between user and SEM):* When a user wants to send a request, at first the user will send his/her ID and PP to SEM. Then SEM will verify the user and send the second half of private key (PR_{SEM}) to the user. It also SEM sends PR_{SEM}, authorization, ID of user, timestamp to TC.
- *Encryption:* The user can encrypt his/her request and PR_u by using the identity of TC as input to generate the cipher text.
- *Decryption:* When receiving the encrypted message, TC can use his private key to decrypt the cipher text and get the request of user and the second part of private key (PR_u).
- *Signing and verification (between user and TC):* A user can use his/her private key to generate a digital signature and send it to the TC. TC must verify the signature based on the ID of user.

When the user and TC have the same private key, they can send and receive encrypt data using symmetric methods (e.g. the AES). Symmetric cryptography (block ciphers) are preferred in such applications because they are much faster than asymmetric techniques. TC has the authorization and can obtain other information about user from SEM. When updating the keys of a user, TC will use the new key with the user ID to encrypt the store data in CSP. TC can contact with CSPs by using SAML. This will reduce the complexity of the key distribution and simplifies the mutual authentication in the cloud.

Summary and Conclusion

In cloud computing, it is crucial to protect personal privacy and proprietary information from unauthorized users by keeping authorized restrictions on access and disclosure. The success in achieving this goal highly depends on finding secure, efficient, and reliable procedures for IAM. This paper can be viewed as a work-in-progress report on our proposed system of IAM in cloud computing. The system is based on efficient and secure combination of IBC and SEM. The proposed system is expected to provide more transparency to users and increase security measures of IAM. More detailed implementation issues and experimental results will be presented in a subsequent paper.

References

[1] Peter Mell and Timothy Grance, "The NIST definition of cloud computing," Recommendations of National Institute of Standards and Technology, National Institute of Standards and Technology Special Publication 800-145, September 2011.

[2] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, " The 10th IEEE International Conference on High Performance Computing and Communications, 2008.

[3] Liang Yan, Chunming Rong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography," M.G. Jaatun, G. Zhao, and C. Rong (Eds.): CloudCom 2009, LNCS 5931, pp. 167–177, 2009, Springer-Verlag Berlin Heidelberg 2009, pp.167-169.

[4] Kungliga Tekniska Högskolan, "Exploring the limits of cloud computing," Masters Thesis, Stockholm, Sweden , October 4, 2010, pp.7-20.

[5] Noemi Antedomenico, "Optimizing security of cloud computing within the DoD," Thesis, NAVAL POSTGRADUATE SCHOOL, MONTEREY, CALIFORNIA, December 2010. Approved for public release.

[6] Saurabh Kumar and Rajkumar Buyya, Green Cloud Computing and Environmental Sustainability, Harnessing Green IT: Principles and Practices, S. Murugesan and G. Gangadharan (eds), Wiley Press, UK, 2011 (in press, accepted on April 2, 2011), pp. 4-8.

[7] Shuai Zhang, Shufen Zhang, Xuebin Chen and Xiuzhen Huo, "Cloud Computing Research and Development Trend," IEEE, Second International Conference on Future Networks, 2010.

[8] Rajarshi Chakraborty, Srilakshmi Ramireddy, T.S. Raghu and H. Raghav Rao, "The Information Assurance Practices of Cloud Computing Vendors", presented at IT Professional, 2010, pp.29-37 , Artical published by the IEEE computer society, pp.29-30.

[9] Eystein Mathisen, "Security Challenges and Solutions in Cloud Computing", 5th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2011), 31 May -3 June 2011, Daejeon, Korea.

[10] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus In Cloud Computing", V2.1, Article, December 2009, http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf, pp.16-68.

[11] S. Ramgovind, M. Eloff, and E. Smith, "The Management of Security in Cloud Computing", Information Security for South Africa, IEEE, 2010.

[12] United States Government Accountability Office, Report to Congressional Requesters, GAO, "INFORMATION SECURITY Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing", Articale, May 2010, pp.12-14.

[13] Jianfeng Yang and Zhibin Chen, "Cloud Computing Research and Security Issues", Journal: 2010 International Conference on Computational Intelligence and Software Engineering Year: 2010 Pages: 1-3 Provider: IEEE Publisher.

[14] Sameera Abdulrahman Almulla and Chan Yeob Yeun, "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), 2010 Second International Conference on Issue Date: March 30 2010-April 1 2010 , pp 1 - 7, Sharjah, pp.2-5.

[15] Ngongang guy mollet , "Cloud computing security", Thesis, Helsinki Metropolia University of Applied Sciences, April 11, 2011.

[16] Dirk C. Aumueller, "IT-Compliance Analysis for Cloud Computing", Thesis, University of Applied Sciences Darmstadt, 16 August 2010.

[17] Cyber security operations centre, "Cloud Computing Security Considerations", Initial Guidance, Australian government, depertment of defence, 12 April 2011.

[18] Manny Siddiqui, "Cloud Computing Security", Paper Blog, INFO 661, Spring 2011.

[19] Guido Kok, "Cloud Computing and confidentiality", Thises, Univirsity of Twente, May2010.

[20] Amit Sangroya, Saurabh Kumar, Jaideep Dhok, and Vasudeva Varma, "Towards Analyzing Data Security Risks in Cloud Computing Environments", S.K. Prasad et al. (Eds.): ICISTM 2010, CCIS 54, pp. 255–265, 2010.

[21] Wayne Jansen and Timothy Grance, "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology Draft Special Publication 800-144, January 2011.

[22] Krešimir Popović and Željko Hocenski, "Cloud computing security issues and challenges", IEEE, MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[23] V.KRISHNA REDDY and Dr. L.S.S.REDDY, "Security Architecture of Cloud Computing", V.Krishna Reddy et al. / International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. 9 September 2011, pp.7151-7152.

[24] J. Tony Goulding, "Identity and access management for the cloud: CA's strategy and vision", White Paper, CA Technologies, May 2010, pp.3-13.

[25] Steffen Schreiner, "The Impact of Linux Superuser Privileges on System and Data Security within a Cloud Computing Storage Architecture" , Thesis, Technische Universität Darmstadt, April 2009.

[26] Frank John Krautheim, "Building trust into utility cloud computing", Dissertation, Faculty of the Graduate School of the University of Maryland, Baltimore County, 2010.

[27] Bob Blakley, "Symplified the cloud security company", Burton Group, Services data sheet, 2010, PP.1-7.

ادارة الهوية والاستخدام في حوسبة السحابة

سفيان تايه فرج سميح عبد الغفور جاسم كاشف كفايات

E.mail : sufyantaih@ieee.org

الخلاصة

ان حوسبة السحابة من التقنيات الحديثة التي تحاول ان تزود المستخدم بما يحتاجه من برامج أو مساحات خزنية أو معالجات وغيرها بأسهل طريقة وبأقل تكلفة وأكثر رصانة عن طريق الانترنت. ان مزود خدمة حوسبة السحابة(CSP) يزود مصادر افتراضية عبر الانترنت بدلاً من استخدام برامجيات أو مصادر موجودة في حاسوب محلي، وان الاسباب الاقتصادية كانت هي السبب الرئيسي لظهور مثل هذه الخدمات، حيث ان مزود الخدمة يزود كل شئ عبر الانترنت حسب طلب الزبون مثل انظمة تشغيل أو مساحات خزنية أو معالجات وغيرها لذلك هناك عدة قضايا امنية يجب أن تؤخذ بنظر الاعتبار عند استخدام هذه الخدمة. ان الخدمات المقدمة في حوسبة السحابة تقسم الى ثلاث أقسام رئيسية هي: البرامجيات (SaaS)والمنصات التي تبنى عليها البرامج(PaaS) والبنى التحتية التي تخص المكونات الفيزيائية(IaaS)، هذا البحث يهدف لتحقيق هدفين الأول لتسليط الضوء على خدمات حوسبة السحابة والتركيز على ادارة الهوية والاستخدام فيها. والهدف الثاني هو اقتراح نظام جديد في ادارة الهوية والاستخدام استنادا إلى تقنيات التشفير المستند إلى الهوية(IBC) و أمن التشفير بوساطة(mRSA) .