Cloud Computing Security Management

Sameera Abdulrahman Almulla, Chan Yeob Yeun
Khalifa University of Science, Technology and Research (KUSTAR), Shrjah Campus
P.O. Box 573, Sharjah, United Arab Emirates
Auther1 Sameera.almulla@kustar.ac.ae, Auther2 cyeun@kustar.ac.ae

Abstract— Enterprises are seeking toward the cloud horizon to expand their premises facilities. It provides several services in the market, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). This paper will discuss challenges regarding three information security concerns: confidentiality, integrity and availability. Most of the organizations are very much concerned about the ownership of their data. This paper will not only address security challenges for cloud computing including Identity and Access Management (IAM) but also present the current state authentication, authorization and auditing of users accessing the cloud along with emerging IAM protocols and standards.

Keywords- Cloud Computing, Privacy, Security, Identity and Access Management.

1. INTRODUCTION

In order to understand what cloud computing is, first we require to obtain an idea about its evolution. According to Toffler [1], he addressed main three civilization waves: the agricultural, industry and information age. The information age has several sub waves and we are moving in the direction of cloud computing. It refers to delivering services over the internet or based on cloud infrastructure. The cloud computing will bring several advantages to the market and the three most important are: cost effectiveness, security and scalability. Our main concern is to discuss some of the security IAM protocols used to protect cloud users and to conclude which of these protocols will be best for organizations which are moving in the direction of consuming the cloud Services.

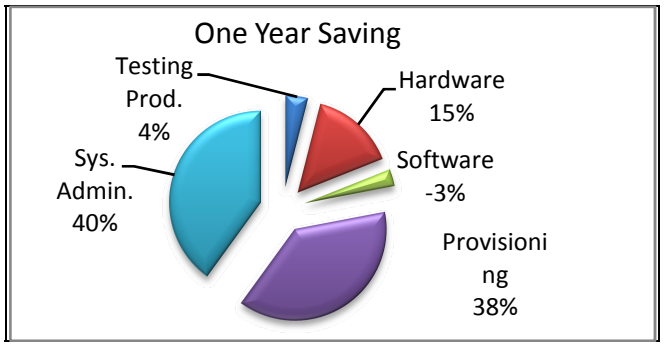
Recently, most of the organizations are analyzing the cloud technology in term of cost saving tool used regardless of the level of the security provided by the Cloud Service Provider (CSP), but it is difficult to measure the benefits in term of one category, as discussed by Richard Mayo and Charles Perng in [2] where the saving represent based on the cloud computing Rate of Interest (RoI) a research conducted by IBM group. The RoI can be based on five categories as in Table 1.

Table 1: Cost saving in cloud

	Saving Factors	Cost Factors
Hardware	• Number of servers required will be reduced. • Reduce cost of floor space required. • Reduction in the power consumption.	• Negligible cost.
Software	• Number of OS to be purchased per client will be reduced. • Supporting and maintenance cost for different implemented software will be reduced.	• Cost required purchasing the virtualization software. • Cost of the cloud services management Software.
Automated Provisioning	• Reduction in number of hours required to provision each task.	• Cost required for training staff to work on automated provisioning systems. • Cost of deployment. • Maintenance Cost.
Productivity	• Having user friendly support service which will reduce time required from staff to wait for IT support.	• Negligible cost.
System administration	• Enhance productivity of administration and support staff where there are more systems to support per administrator.	• Negligible cost.

In Figure 1, shows the result of a case study such as a bank where it requires a huge number of servers to manage their business which results in turning their business into cloud.

Fig 1. One year saving [2]



In the near future, spending on cloud computing will grow rapidly as stated in [3] Page 26, "The US government projects between 2010 and 2015 will increase spending on cloud computing by 40% compound annual rate to reach $7 million by 2015". Cost effectiveness is one of the major motivations to use cloud computing. However, we should consider other challenges such as security. Organizations will upload its databases, user related information and in some cases the entire infrastructure will be hosted in the cloud. Is the organization satisfied with the security level provided by the CSP?

In this paper, we will mainly focus on one data security aspect which is Identity and Access Management (IAM) in the cloud. Firstly, we will start with general overview of current cloud computing structure in Section 2. Then we discuss about security and privacy requirements in Section 3. Having the knowledge of the security requirements, we will discuss in details IAM challenges in Section 4. Also, IAM lifecycle and some of the protocols are discussed in Section 5 and 6, respectively. In Section 7, the best practice for the IAM via the cloud service such as Identity Management-as-a-Service (IDaaS). Finally, we conclude in Section 8.

2. CLOUD COMPUTING STRUCTURE

A. *Types of Cloud Systems*

There are main three systems categories: Software as a Service, Platform as a Service and Infrastructure as a Service. Let's look at them in more details as follows:

1) Software as a Services (SaaS):

Traditionally, users prescribe software and it is license in order to install it on their hard disk and then use it, however, in the cloud users do not required to purchase the software rather the payment will be based on pay-per-use model. It support multi-tenant which means that the physical backend infrastructure is shared among several users but logically it is unique for each user [4].

2) Platform as a Service (PaaS):

In PaaS the development environment provided as service. The developers will use vendor's block of code to create their own applications. The platform will be hosted in the cloud and will be accessed using the browser.

3) Infrastructue as a Service (IaaS):

In IaaS, vendors provide the infrastructure as a service where it is delivered in form of technology, datacenters and IT services to the customer which is equivalent to the traditional "outsourcing" in the business world but with much less expenses and effort [5]. The main purpose is to tailor a solution to the customer based on required applications. Table 2 shows cloud computing services that are currently utilized by several providers.

Table 2: Cloud Computing Services

	Services	Providers
SaaS	• Support running multiple instances of it. • Develop software that is capable to run in the cloud.	• Google Docs • Mobile Me • Zoho
PaaS	• Platform which allows developer to create programs that can be run in the cloud. • Includes several applications services which allow easy deployment.	• Microsoft Azure • Force.com • Google App Engine.
IaaS	• Highly scaled and shared computing infrastructure accessible using internet browser. • Consists of Database, servers and storage	• Amazon S3 • Sun's Cloud Service

B. *Examples of Cloud Services*

In this section we will discuss some applications using cloud computing that proving to be beneficial for users. Rishi Chandra, Google Enterprise product manager point out in an interview [6] what he believe is a key trend toward cloud computing: "*Consumer driven innovation changing economics and lowering of barriers to entry as the major reasons why the cloud model is being so widely adopted*." The success of cloud computing basically depends on the acceptance and satisfaction of the cloud users. In Table 3, we explain some examples of the cloud computing as in [4].

There are several papers [8] and [9] that are published which are related to the usability and functionality of cloud computing. This paper will focus on the identity management and techniques that are used to provide a secure environment. Specifically, IAM security can be achieved via using appropriate protocols and standards. In order to understand the need for IAM security in the cloud, in this paper we will discuss security and privacy for cloud computing in the next section.

Table 3: Examples of cloud providers

Provider	Application	Usage	Description
Amazon (IaaS)	• Elastic Compute Cloud (EC2) • Simple Storage Service (S3)	• Web application hosting • Backup and storage • High performance computing	• Web service provides scalable compute capacity in the cloud [7]. Allows application deployment on the web services interface. • Web services interface which is used for storage and retrieving data.
Google (SaaS, PaaS)	• Gmail • Google Email Security • Google Docs	• Messaging • Securing existing email systems • Collaboration	• Using email services without managing and maintaining message architecture. • Filtering spam and viruses. • Provide collaboration tools without installing software on the machines or servers.
Microsoft Azure (PaaS)	• Windows • .NET services • SQL Services	• Offering application to organization as SaaS • Application Development	• Organization uses Azure Platform to enhance the functionality of existing application without investing in internal infrastructure. • Use Azure platform to develop custom application

3. CLOUD SECURITY AND PRIVACY

In cloud computing, end users' data stored in the service provider's data centers rather than storing it on user's computer. This will make users concerned about their privacy. Moreover, moving to centralized cloud services will result in user's privacy and security breaches as discussed in [4]. Security threats may occur during the deployment; also new threats are likely to come into view. Cloud environment should preserve data integrity and user privacy along with enhancing the interoperability across multiple cloud service providers. Thus, we would like to discuss data integrity, confidentiality and availability in the cloud. The security related to data distributed on three levels in [4]:

- *Network Level:*

  The Cloud Service Provider (CSP) will monitor, maintain and collect information about the firewalls, Intrusion detection or/and prevention systems and data flow within the network.

- *Host Level:*

  It is very important to collect information about system log files. In order to know where and when applications have been logged.

- *Application Level:*

  Auditing application logs, which then can be required for incident response or digital forensics.

At each level, it is required to satisfy security requirements to preserve data security in the cloud such as confidentiality, integrity and availability as follows:

A. Confidentiality

Ensuring that user data which resides in the cloud cannot be accessed by unauthorized party. This can be achieved through proper encryption techniques taking into consideration the type of encryption: symmetric or asymmetric encryption algorithms, also key length and key management in case of the symmetric cipher. Actually, it is all based on the CSP. For instance in [4], MozyEnterprise uses encryption techniques to protect customer data whereas Amazon S3 does not. It also depends on the customer awareness where they can encrypt their information prior to uploading it. Also, The CSP should ensure proper deployment of encryption standards using NIST standards in [10].

B. Integrity:

Cloud users should not only worry about the confidentiality of data stored in the cloud but also the data integrity. Data could be encrypted to provide confidentiality where it will not guarantee that the data has not been altered while it is reside in the cloud. Mainly, there are two approaches which provide integrity, using Message Authentication Code (MAC) and Digital Signature (DS). In MAC, it is based on symmetric key to provide a check sum that will be append to the data. On the other hand, in the DS algorithm it depends on the public key structure (Having public and private pair of keys). As symmetric algorithms are much faster than asymmetric algorithms, in this case, we believe that Message Authentication Code (MAC) will be the best solution to provide the integrity checking mechanism. Studies show that, PaaS and SaaS doesn't provide any integrity protection, in this case assuring the integrity of data is essential.

C. Availability:

Another issue is availability of the data when it is requested via authorized users. The most powerful technique is prevention through avoiding threats affecting the availability of the service or data. It is very difficult to detect threats targeting the availability. Threats targeting availability can be either Network based attacks such as Distributed Denial of Service (DDoS) attacks or CSP availability. For example, Amazon S3 suffered from two and a half hours outage in February 2008 and eight hours outage in July 2008.

In the next section, we will discuss the identity and access management practices of the cloud computing by tackling some protocols such as Security assertion Markup Language (SAML), Open Authentication (OAuth) protocol and a comparison between these two techniques to conclude the best solution.

4. IDENTITY AND ACCESS MANAGEMENT (IAM)

Identity and Access Management (IAM) can be defined as a 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. However, the definition is not restricted to the organization resources and provides privacy and protection for users' personal information and actions. Most of the enterprises based on different information systems to provide their services, managing user's identity and provide adequate privacy and protection will be a great challenge.

Managing digital identities will not be sufficient, unless we describe two main user attributes related to users' digital identities that are presence and location [5]. These three traits used in today's technologies. Presence is associated with the real-time communication systems such as: Instant Message and (IM) and Voice over IP (VoIP), where it provides all required descriptions about users status during or after the communication, whether they are idle or active, online or offline and in some cases providing some specific task they are performing such as writing documents or an email. Location specifies where the geographic location of the users through the longitude, latitude and altitude for example, IP address of the entity can specify the geographic location.

A. Challenges:

- The main challenge for any organization in managing the identities resulted from the variety of the user population that an organization consists- customers, employers, partners, etc.
- Managing and maintaining staff turnover within the organization where it varies based on the current trend of the business in the market and its function.
- Handling user's identities in the case of merges and demerges.
- Avoid the duplication of identities, attributes and credentials.

The above mentioned challenges and more, direct companies to look for centralized and automated identity management systems. This will lead us to describe the concept of the identity federation. It is an arrangement made between groups of enterprises (this relationship based on the trust) so that users can use the same identification attributes to obtain services from the trusted group [4]. The core responsibility is to manage the access control for services beyond the organizations internal network. Federation support for Single Sign On (SSO) techniques where users will not have to sign in multiple times or to remember registration information for each cloud specific services.

Thus, we would like to discuss the current practice of identity and access management (IAM) which is considered a great help in providing Authentication, Authorization and Auditing for users who are accessing the cloud computing as follows:

1) Authentication:

Cloud computing authentication involves verifying the identity of users or systems. For instance, service to service authentication involves in verifying the access request to the information which served by another service.

2) Authorization:

Once the authentication process succeeds, then the process of determining the privileges could be given to legitimate users. In this stage, the system will enforce the security policies.

3) Auditing:

It is the process of reviewing and examining the authorization and authentication records in order to check, whether compliances with predefined security standards and policies. Also, it will aid in detecting any system breaches.

B. Readiness of Cloud Environment:

In order to get ready for the cloud, enterprises should prepare IAM strategy, structure, understand the IAM lifecycle and specify which model of the equipments will support the identity federation technical requirements as follow:

1. Defining authorized source for the identity information.
2. Defining the required attributes for user's profile.
3. Defining the current structure of the identity management system within enterprises (isolated active directories which are connected on the internal network, active directories within the *Demilitarized Zone* (DMZ) and if the company is *id-federation friendly* environment where active directories can be accessed by a trusted third party, where deploying federation can be faster and more cost effective).
4. Implement identity providers which support SSO technology such as OpenID, Microsoft CardSpace and Microsoft Novell Digital Me.
5. Identity Providers compatibility with the internally built active directory.

In order to successfully manage digital identities, we should know what different stages that the digital identity will pass through to provide the appropriate level of security to that stage. This discussion leads us to discuss about the IAM lifecycle. In the next section we will describe digital identity life cycle.

5. IAM LIFECYCLE

In this stage, we should consider all different stages that an identity is going through which known as identity lifecycle. One important question is that we should rise what is happening for the user's identity from the time it has been created, used and terminated. According to Mather, Kumarasuamy and Latif [4], the digital identity management will go through five stages as follow:

1. *Provisioning and deprovisioning :*
   In this process users will be assigned required access to the information based on the role with the organization and in case of the user authority escalation or degradation, proper access roles will be assigned. This process requires numerous amounts of time, effort and staff to keep the identity assigned privileges as adequate as possible. However, cloud management using proper techniques such as identity Management as a Service (IDaaS) it can take this burden off from the organization shoulders.

2. *Authentication and Authorization:*
   A central authentication and authorization infrastructure will be required to build up a custom authentication and authorization model that meets the organization business goals. Having such model will enforce the security policy which should be followed to protect applications and databases.

3. *Self-Service:*
   Enabling self-service in the identity management will enhance the identity management systems. At this stage users can reset their password, maintain and update their own information and view the ability to view? The organizational information from any location.

4. *Password Management:*
   Through implementing federated systems which support Single Sign On (SSO) to access cloud-base services. Password management consists of how the password will be stored in the cloud database using MD5 or SHA1as in [11] and [12].

5. *Compliance and Audit:*
   In this process the access will be monitored and tracked to ensure that there will be no security breaches in the system. It also will help auditors to verify the fulfillment to different access control policies, periodic auditing and reporting.

6. IAM STANDARDS AND PROTOCOL

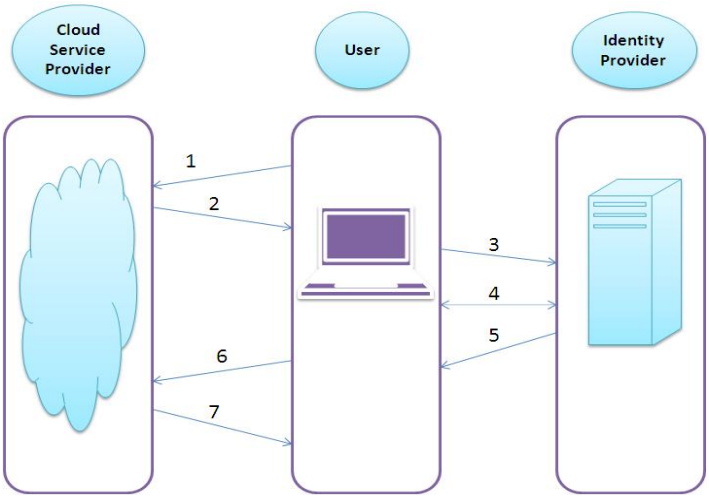
Previously, we discussed what the requirements to apply the IAM structures are. In the following, we will discuss some standards and protocols to manage identities in the cloud; however, it is worth to mention here that the IAM standards and protocols should be considered from both parties: the organizations and consumers.

In this paper, our main concerned is to discuss how the organization will handle IAM using protocols. There are several protocols [4] and standards which organizations should consider such as: Security Assertion Markup Language (SAML) and Open Authentication (OAuth) protocol. We will discuss each of these protocols in details as follows

A. Security assertion Markup Language (SAML)

SAML is based on XML standards [13], used as a tool to exchange the authorization and authentication attributes between two entities – in the case of the cloud, between the Identity provider (IdP) and Cloud Service Provider (CSP)-. The main goal of SAML is trying to achieve is to support SSO using the internet. There are different versions of the SAML for example: SAML v1.0, SAML v1.1 and SAML v2.0. It supports digital signature and encryption. Following is an illustrative example to help in understanding of SAML used for SSO, between the user, IdP and CSP.

Fig 2. SAML communication process



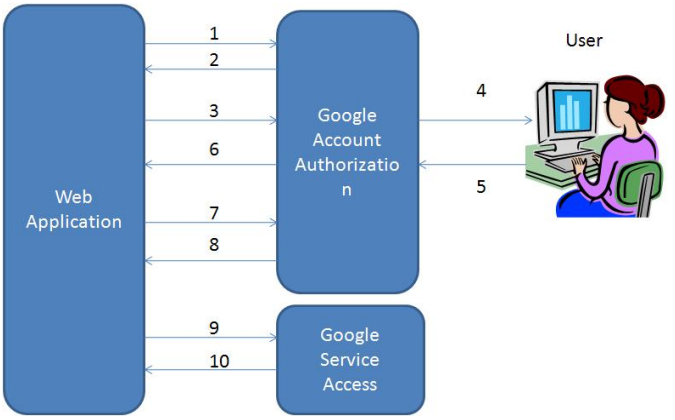
1. User will request a web page from the CSP.
2. CSP will respond to the User by redirecting the user's browser to the SSO website located at the IdP.
3. Browser redirecting process.
4. Exchange authentication protocol between the IdP and user for identification.
5. IdP responds using encoded SAML to user.
6. User browser will send SAML response to CSP to access the URL.
7. User will be able to log in the CSP application.

B. *Open Authentication (OAuth) protocol*

OAuth is a very interactive and interesting protocol which allows users to share their private resources such as files, pictures located on one CSP with another CSP without exposing the personal identity information such as user names and passwords [4]. It is main objective is to build an authorized access to a secure Application Programming Interface (API) used in mobile and desktops designs and it is based on the open source implementations. From the CSP perspective, it provides a service for users to access the programmable application hosted on different service provider without disclosing of the identity credentials. For instance, a consumer (a web site or an application that used to access stored files on behalf of the user) request a print service from a service provider where the file is stored as a result the print will be executed without disclosing the files owner credentials.

In figure3, illustrates the communication process between the user and service provider using OAuth protocol in [4]:

Fig 3. Google OAuth use case



1. Web application well asks Google Authorization for OAuth *request token*.
2. Google will response with *unauthorized request token*.
3. Web application will direct users to Google web authorization page to request *authorized token.*
4. User will access the Google Authorization page to verify their identity and either to allow or deny web application access to their data.
5. If user denies access then he/she will be directed to the Google page rather than the application page.
6. If user grants access, he/she will be redirected to the application web page, which includes *authorized request Token.*
7. The authorized request token will be exchanged between the web application and Google Authorization.
8. Google will verify the request and send *Access Token.*
9. The web application will request for user data from Google Authorization.
10. The request in step 9 will be verified and signed by Google Authorization and if the access token known by the Authorization the requested data will be send.

OAuth Token [4], is used to authenticate users to the service requested, these tokens are specific to the user it can be done through issuing a cookie prior of token request so when the service provider (in our case Google) will redirect to the requested website attached with the token, then the web application can read the cookie and associate the correct token to the correct user identification. In case of some service provider, each user will have limitation on number of tokens to be requested. OAuth has two types: *request tokens* – used for requesting tokens from service provider to establish access token- and *access token* – used to get user data from the service provider to access requested pages. Request tokens can be either authorized or unauthorized. Initially, token are unauthorized, after the user successfully access the web application the requested token will be authorized and only authorized tokens can be used as access tokens.

7. WHICH IS BETTER SOLUTION

It is very difficult to say using one protocol will be better than another, where it is totally dependent on the organizational behavior toward their business goals. Since technologies are overlapping most of the CSP's may prefer to use more than one authentication protocols to provide better security model to control their users identities. SAML is commonly used in enterprises and schools where users will log on once and will be able to authenticate with other websites internally or externally. SAML is part of the "Enterprise" group of digital identities where it has more experience and its library has been developed for a long time. However, in OAuth it belongs to "Open Source" libraries where these libraries are new and need more work to be done to improve the protocols of this category. From our point of view, OAuth will be a very competitive environment for researchers to improve it. However, SAML will be best choice to deploy SSO and federation in the cloud. SAML is mature and exposed for various vulnerability and threats which lead us to recommend it as best solution to deploy IAM security and maintain user's information privacy.

8. IDENTITY MANAGEMENT-AS-A-SERVICE

Since the cloud environment reaches to the level where service providers can provide anything-as-a-service (XaaS), this will lead us to think of outsourcing identity providers such as a Service (IDaaS). Most of the organization might prefer to outsource the partners and consumers identity management, however, yet they are obligated to manage their staff identity and the internal resource access. This model based on software as a service (SaaS), where it supports several services such as: accounts provisioning, auditing, password management and user self services. By adopting this architecture, organization can fully automate user account provision and audit. There are a variety of solutions available in the market which provides identity management such as: Simplified and Ping Identity.

The main advantage of outsourcing the identity management is having a multi protocol environment where it consists of SAML, OAuth and more when it has to interface with different cloud service federation systems. IDaaS will authenticate users prior to accessing any cloud based service via browser SSO.

As it is the case with any cloud-base service, there will be a little change or maybe with no changes any organization can adopt this model. The main downside of the IDaaS is that the enterprise will not be aware about the structure, implementation and services of the CSP. Add to that, the generated report about the users may not match the organization requirement and even if there is a facility to edit the report it will be limited to the CSP capabilities.

9. CONCLUSION

In conclusion, cloud computing is very attractive environment for business world in term of providing required services in a very cost effective way. However, assuring and enhancing security and privacy practices will attract more enterprises to world of the cloud computing. IAM should be properly implemented to ensure the mutual authentication, authorization and auditing for cloud computing management. Our main concern is to discuss some of the security IAM protocols used to protect cloud users and to conclude which of these protocols will be best for organizations which are moving in the direction of consuming the cloud Services.

REFERENCES

[1] A. Toffler, "The Third Wave", Bantam Publisher , 1984.

[2] Richard Mayo, Charles Perng, "An explanation of where the ROIcomes from", IBM, November 2009.

[3] "US Federal Cloud Computing Market Forecast 2010-2015", Tabuler Analysis, Publication, May 2009.

[4] T. Mather, S. Kumarasuwamy and S. Latif, "Cloud Security and Privacy", O'Rielly, ISBN: 978-0-4596-802769, 2009.

[5] J. W. Rittinghouse,J. F. Ransome, "Cloud Computing: Implementation, Management and Security" CRC Press, ISBN: 978-1-4398-0680-7, 2009.

[6] Paul McDougall, "The Four Trends Driving Enterprise Cloud Computing",http://www.informationweek.com/cloud-computing/blog/archives/2008/06/the-four -trends.html, 10 june 2008, retrieved 26 Feb 2009

[7] M. Dikaiakos, G. Pallis, D. Katsaros, P. Mehra and A. Vakali, "Cloud Computing: Distributed Internet Computing for IT and Scientific Research", IEEE Internet Conputing, vol. 13, no. 5, 2009.

[8] *"Architectural Strategies for Cloud Computing",* Oracle Corporation, August 2009.

[9] H. Cademartori, "*Green Computing Beyond the Data Center*", © TechTarget, 2007.

[10] L. M. Kaufman, "Data Security in the World of Cloud Computing", IEEE Security & Privacy, vol. 7, no. 4, 2009.

[11] P. Gauravaram, A. McCullagh and Ed Dawson, "Collision Attacks on MD5 and SHA-1: Is this the "*Sword of Damocles" for Electronic Commerce?*", AusCERT Asia Pacific Information Technology Security Conferenece, pp. 1-13, May 2006.

[12] Z.Y. Hu, "*Password Breaking and Encryption Technology*". Machine Industry Press, 1999.

[13] Eve Maler,Scott Cantor, Jahan Moreh, Sigaba,Rob Philpott, "Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0", Copyright © OASIS Open, 2005.