TJES

ISSN: 1813-162X
Tikrit Journal of Engineering Sciences
available online at: http://www.tj-es.com

Mediated IBC-Based Management System of Identity and Access in Cloud Computing

Sufyan T. Faraja[a], Sameeh A. Jassima[b], Kashif Kifayatb[a]

[a]*College of Computer, University of Al Anbar, Al Anbar Province, Republic of Iraq.*

[b]*Liverpool, United Kingdom*

(Received 12 July 2012, Accepted 22 November 2012, Available online 18 September 2013)

ABSTRACT

Cloud computing is a new technology that provide to consumers dramatically scalable and virtualized resources, bandwidth, software and hardware on demand. However, cloud computing introduces serious security problems. One of these major security concerns is the management of access and identities of different entities involved in such environment. This paper proposes a new system for Identity and Access Management (IAM) based on combining the techniques of Identity-Based Cryptography (IBC) and security mediated cryptography with the Trusted Cloud (TC) to facilitate the secure management and access control for cloud computing. IBC is an interesting choice for IAM as it significantly reduces the key management complexity. On the other hand, mediated cryptography enables system administrators to achieve access control in a fine grained manner, while a TC can provide a Single Sign On (SSO) ability to users. The paper also presents results of the developed prototype implementation of the proposed IAM system.

Keywords: Identity and access management; Cloud computing; Mediated cryptography; Security.

الخلاصة

الحوسبة السحابية هي تكنولوجيا جديدة توفر للمستهلكين موارد قابلة للتطوير وعرض النطاق الترددي ، والبرمجيات والأجهزة على الطلب بشكل كبير . و رغم ذلك فالحوسبة السحابية تسبب مشاكل أمنية خطيرة. و أحد هذه المخاوف الأمنية هو إدارة الوصول و هويات الكيانات المختلفة المشاركة في مثل هذه البيئة. و يعرض هذا البحث نظام جديد لإدارة الهوية والوصول (IAM) على أساس الجمع بين تقنيات التشفير على نظام (IBC) والأمن بوساطة التشفير (TC) لتسهيل إلادارة والتحكم في الوصول الآمن للحوسبة السحابية. IBC هو خيار مثيرة للاهتمام لـ IAM لأنه يقلل بشكل كبير من تعقيد إدارة النظام. من ناحية أخرى، فان الترميز بالواسطة يمكن مسؤولي النظام لتحقيق التحكم في الوصول بطريقة غرامة الحبيبات ، بينما يمكن أن توفر TC الدخول الموحد (SSO) للمستخدمين. يعرض هذا البحث أيضا نتائج تنفيذ النموذج الأولي المتقدمة في نظام IAM المقترح.

الكلمات الدالة: ادارة الهوية والوصول؛ الحوسبة السحابية؛ التشفير؛ الأمن.

Introduction

Cloud computing is a new technique that often uses virtualized resources to provide dynamically scalable services over the internet. With the cloud computing technology, users can use a variety of devices, such as PCs, laptops, and smart phones to access multiple services such as programs, storage, and application-development platforms. This can be done via services that are offered by cloud computing providers over the Internet. In recent years,

* Corresponding author: E-mail address: sufian.haza@gmail.com

cloud computing has evolved from relatively simple web applications, like Hotmail and Gmail, into commercial propositions such as SalesForce.com, Amazon EC2, etc. Cloud computing can provide critical services for business management, reducing Information Technology (IT) and maintenance costs of hardware and software effectively. In the meanwhile, it can enable enterprises to access the professional IT solutions with less IT investment [1].

Cloud computing can be defined as a model for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly released with minimal management effort. This model promotes availability. It is composed three delivery models and four deployment models. The three delivery models of cloud computing are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The four deployment models of cloud computing include public, private, community (a subset of public/private), and hybrid clouds [2].

When using cloud computing, the applications run in the cloud instead of the user's machines and the users can control applications by interface of user's desktop (webpage). Clouds can store huge amount of data, so that mobile users do not have to carry their data. There are many cloud services providers. For example Google Apps and Microsoft online provides application services, and Amazon's EC2, Eucalyptus, and Nimbus provide infrastructure support. Examples of companies that provide platform to help developers to write applications that will run on the cloud are Amazon's S3 and Windows Azure [3].

Cloud Service Providers (CSPs) use virtualization for sharing their resources and capabilities with customers. Therefore, there are many problems of cloud computing which must be taken into consideration such as security and privacy. 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. Thus, our work is dedicated to describe the design and prototype implementation of a new architecture for Identity and Access Management (IAM) in the cloud. The proposal is based on a flexible and efficient integration of Identity-Based Cryptography (IBC) and security mediated cryptography techniques. Indeed, a Trusted Cloud (TC) entity is an important building block of the proposed system.

This paper is organized as follows: Section 2 reviews some significant earlier works in the field of IAM in cloud computing. Then, theoretical background related to IAM and related cryptographic techniques is presented in Section 3. The proposed IAM system is described in Section 4. Next, Our current prototype implementation of the system is explained in Section 5. Finally, the paper is concluded in Section 6.

Review of Related Work

The goal of this literature survey is to cover some relevant scientific literature of top quality. In 2009, L. Yan, C. Rong, and G. Zhao had proposed federal identity management by using hierarchical identity-based cryptography. This proposal simplified the key distribution and mutual authentication in the cloud [4].

In 2010, R. Ranchal et al proposed an approach for Identity management, which is independent of trusted third party and has the ability to use identity data on untrusted hosts. The approach is based on the use of predicates over encrypted data and multi-party computing for negotiating the use of a cloud service. It uses active bundle-which is a middleware agent that includes personally identifiable information data, privacy policies, and a set of protection mechanisms to protect itself [5].

In 2010, I. K. Kim et al proposed a methodology of SSO for Cloud applications by utilizing peer-to-peer concepts to distribute processing load among computing nodes within the cloud. The proposed scheme was called Chord for Cloud (C4C). This system decreased the number of authentication requests sent to the identity provider and disseminated the authentication process within the federated environment of cloud [6].

In 2010, M. Machulak and A. Moorsel proposed an approach that puts a user in full control of access to their resources which might be scattered across multiple cloud-based web applications. Unlike other authorization systems, it relied on a user's centrally located security requirements for these resources. This approach introduced access control on sharing resources on the web [7].

In 2011, W. Jia et al proposed a secure mobile user-based data service mechanism (SDSM) to provide confidentiality and fine-grained access control for data stored in the cloud. This mechanism enables the mobile users to enjoy a secure outsourced data services at a minimized security management overhead. However, their proposal was specifically tailored to enhance the security of mobile cloud users where mobile users might join or leave the mobile networks arbitrarily [8].

In 2012, L. Sun et al presented a semantic based access control model which considers semantic relations among different entities in cloud computing environment. However, Semantic web applications pose some new requirements for security mechanisms especially in the access control models [9].

Theoretical Background

Managing identities and access control for enterprise applications remains one of the greater challenges facing cloud computing. Unauthorized access to information resources in the cloud is a major concern for an organization, because organizations usually have sensitive data and privacy information[10-11]. 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 [12].

Identity is the set of data that uniquely defines a user and distinguishes him/her from others. In order to operate the system in a secured manner, each user must be given a unique identity that is used to access the resources and services within the system. While the Identity attributes are the individual pieces of information about a user that define the user and its interactions with other users [13].

Identity management refers to the creation, modification, and deletion of identity objects. Identity management is used to provide the first line of access control for a system. The user must identify himself/herself at first to system in order to access services, and the system must be able to determine whether the user should be given access depending on identity of user.

The concept of IBC was firstly proposed in 1984 in order to reduce the need for public key certificates and certificate authorities. IBC uses users' identifier information such as email, IP addresses, and phone numbers instead of digital certificates as public keys for encryption or signature verification. Therefore IBC can solve some of the problems of Public Key Infrastructure (PKI) by reducing the system management complexity and reduce the cost for establishing and managing the public key authentication framework. Shamir used the existing RSA function to construct an identity-based signature (IBS) scheme but he was unable to construct an identity-based encryption (IBE) scheme. In 2001, D. Boneh and M. Franklin solved the IBE problem. Their schemes are based on bilinear pairings on elliptic curves and have provable security [14].

IBS scheme can be used for two parties to exchange messages and effectively verify each other's signatures. Another advantage of IBE is that encryption and decryption can be conducted offline without the key generation center. So, IBC has some attractive characteristics that seem to fit well the requirements of cloud computing. A Private Key Generator center (PKG) in IBC approach should create at first a "master" public key and a corresponding "master" private key. 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 [4].

Mediated RSA (mRSA) algorithm is similar to RSA algorithm but mRSA is a simple and practical method of splitting RSA private keys (as in threshold RSA) between the user and the Security Mediator (SEM). Using mRSA leads to

neither the user nor the SEM can cheat one another since each signature or decryption must involve both parties. mRSA allows fast and fine-grained control (revocation) over users' security privileges [15].

SEM is an on-line partially trusted server that involves in mRSA. To sign or decrypt a message, the user must first obtain a message-specific token from the SEM. Without this token the user cannot use his private key. To revoke the user's ability to sign or decrypt, the administrator instructs the SEM to stop issuing tokens for user's public key. At that instant, user's signature and/or decryption capabilities are revoked. For scalability reasons, a single SEM serves many users. One of the mRSA's advantages is its transparency; SEM's presence is invisible to other users. In signature mode, mRSA yields standard RSA signatures, while in decryption mode; mRSA accepts plain RSA-encrypted messages [16].

In mRSA there are trusted party is used to generate keys for all users with mRSA. The trusted party choose two large prime numbers to generate modulus (n), Ø(n), e and d. all these operations are similar to standard RSA except the secret key (d). The trusted party must partition the (d) in to two halves given one to the user and the other half to the SEM. To do this, the trusted party chooses a random integer in the interval [1,n] and this number will be (dsem) then compute duser by duser = d – dsem . duser is given to the user and dsem is given to the SEM.

Alice can send message to all users by using their public keys ei . Also, Alice can receive message from all users but she can't complete the decryption of the message because she has only one half of private key (duser). Alice also need to cooperate with the SEM to sign the message[17]. Signature verification and encryption with mRSA are identical to that in standard RSA. Fig.1 explains the operations of Mediated RSA [18].

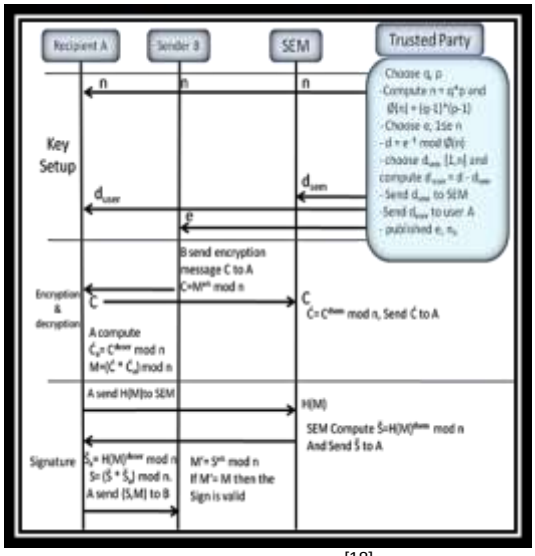

Fig. 1. Mediated RSA operations [18]

Proposed IAM for Cloud Computing

The proposed architecture for IAM in cloud computing consists of four main parts: client, PKG, SEM, and TC (as shown in Fig.2). The management in proposed system is divided into two parts: user's management and CSPs management. The access control of users is controlled by SEM. PKG is used to manage the keys of users and authentications, while the TC is used to manage CSPs companies. This proposal is aimed to reduce the complexity of management of cloud computing system, to provide transparency to users of cloud computing, and to provide more secure method to protect secret data and sensitive information.

The basic idea in this proposed system is to combine IBC and security mediated cryptography with a trusted cloud (TC) entity that is responsible for IAM in the cloud environments. IBC is an interesting choice for IAM as they significantly reduce the key management complexity and reduce the cost for establishing and managing the public key authentication. Mediated cryptography enables system administrator to efficiently achieve access control in a fine grained manner. The users cannot decryption or sign any data without an acceptance from SEM that also controls the revocation of users. The TC concept has at least two main practical benefits. The first one is

preventing denial of service attack (DoS) on CSPs. This is because the TC will have all halves of users keys; therefore it can check the keys of users before it request the services. Another benefit of TC is to provide SSO to users because it choose for users suitable companies from CSPs. Thus, users will not need to repeat the whole operations of log in each time they used cloud services. All these parts of system will increase the strength and resistance of the system. The PKG center and TC are considered as the trusted authority in this proposal.

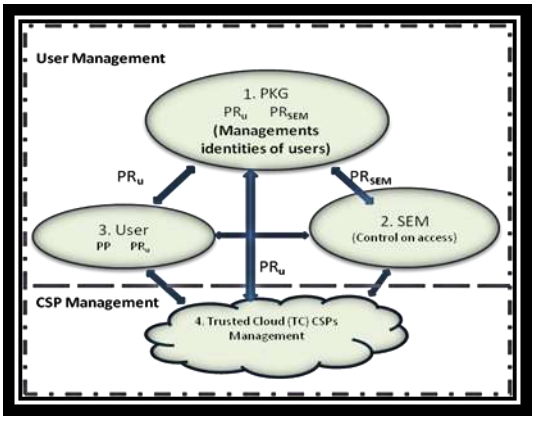

Fig. 2. The general proposed system structure

Some of the basic cryptographic algorithms implemented by the system are:

- Initial Setup Phase: It is composed of the following steps:
  1. PKG chooses random prime's p, q for domain.
  2. PKG computes n = p * q for domain and publishes it. PKG also computes Ø(n)= (p- 1)(q- 1).
     For each user B, PKG carries out steps 3 to 8
  3. PKG computes encryption exponent eB = H(ID).
  4. PKG computes d = 1/eB mod n.
  5. PKG chooses dU, dU=[1,n].
  6. PKG computes dT = (d-dU) mod n.
  7. PKG securely communicates:
     dT to SEM
     dU to B and TC.
  8. PKG publishes IDB.

- Extract: When a user requests his/her private key from the PKG, the user at first must download PP from PKG (in this proposal the public parameters will be (n) and (e). Then PKG will use the identity of this user, public system parameters PP and master key (MK) to generate a private key for this user. PKG will divide the private key into two parts and giving one for user and TC (PRu) and other for the SEM (PRSEM). PRSEM is chosen randomly by PKG between [1, n], PRu = Privateuser - PRSEM
- Verifying (between user and SEM): When a user wants to decrypt the data or sign the message, at first the user will send his/her ID and encryption data (to decrypt) or hash value (to sign) with digital signature to SEM (digital signature that is sent from user to SEM contains original message and hash value encrypted by using the half of user private key (PRu)). User sends the original message (M) and digital signature (DS) to SEM encrypted by PRu as follows. Then SEM will verify the user and decrypt the data or sign the message by using PRSEM.
- Encryption: The user can encrypt his/her request, PRu, SK, and DS by using the identity of TC as input to generate the ciphertext. Also, the user (A) can encrypt any data by using the id's of the receiver (B) as a public key as follows:
  1. User A generates message m.
  2. User A computes eB= H(IDB).
  3. User A computes meB mod n, and sends it to B.
- Decryption: When the user receives the encrypted message (C), he cannot decrypt it because he does not have all the private key. Therefore, the user can decrypt the encrypted message as the follows:
  1. User B receives C= meB mod n from A.
  2. User B sends C to SEM.
  3. SEM computes C1= CPRSEM mod n, and returns is to B.
  4. User B receives C1= (meB)PRSEM mod n from SEM.
  5. User B computes C2= CPRu mod n.

6. User B multiplies C1 by C2, m= C1*C2 mod n, to recover message m.

The TC has complete private key and can use it to decrypt any data encrypted by using the identity of TC without need to help from the SEM because in this proposal the TC is considered a trusted party.

- Signing and verifying (between user and TC): A user can cooperate with SEM to obtain his signature ([H (M)]PRuser), and encrypt the signature by using the public key of TC (PUTC).

DS= E (E [H (M)]PRuser) PUTC mod n

TC must verify the signature based on the ID of user by decrypting the signature using his private key then decrypting the result by using the public key of user (id's of the user) to verify the sender.

DS2= D(E[H(M)]PRuser) PRTC mod n

DSuser= D[H(M)]PUuser mod n

In this proposal, the user sends secret key (SK) with his request to TC so that the TC can choose a suitable CSP and send the SK to it. Thus, the user and CSP will have the same SK so that they can send and receive encrypt data using symmetric methods (e.g. the AES). Symmetric cryptography (block ciphers) is preferred in such applications because they are much faster than asymmetric techniques. The TC has the authorization and can obtain other information about user from SEM. For example, the 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.

System Prototype Implementation

A prototype of the proposed system has been implemented using Microsoft Visual Studio 2010 (Visual C# language) that is considered a familiar programming language with great support of GUI and cloud computing environments. It offers possibilities to efficiently increase or decrease the number, type, and quality of services according to the needs of users. The main user window of the proposed system is illustrated in Fig.3. This window automatically appears when the system starts. The window contains the main options to manage the operations of the users. The user can enter existing ID's, N, Duser, SK, and choose his request from services options. If the user wants to store data in cloud computing, for example, he must choose IaaS STR from services options, press Browse button to upload the data, and then press Send File button. When the user wants to retrieve his data from cloud, he/she must choose IaaS RET from services options and press Download button to download the data from cloud computing.

The performance is a crucial issue in any security implementation. The prototype has four types of requests: Store data (STR IaaS), Retrieving data (RET IaaS), SaaS, and PaaS. The typical execution times of some requested services are shown in Figure 4. The time is measured in millisecond (msec).

Fig. 3. The main user window of the system prototype

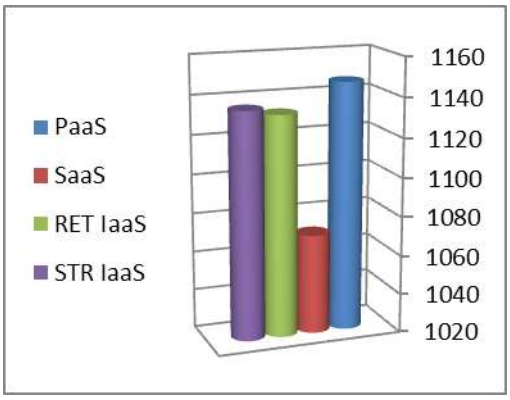

Fig. 4. Typical execution time for some services from TC (msec)

We have also computed the run time of typical SaaS operations in local computer and compared that to the run time of same SaaS operations with cloud environment. Fig.5 shows the relative execution time of the two cases. We can note that the required time in both cases is almost the same. This is a direct consequence of the relatively light characteristics of the involved SaaS operations. Fig.6 illustrates the relative execution time of a typical IaaS case (Storing many files in the cloud compared to store the same files in local computer). In this latter case, we can see a noticeable time difference due to the inherited parallelization offered by cloud model.

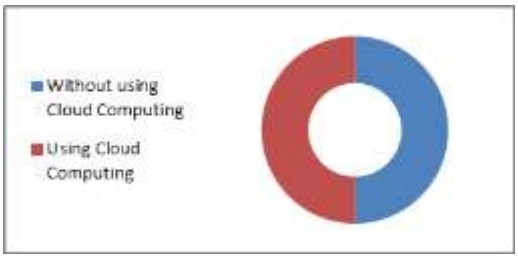

Fig. 5. Relative execution time for a typical SaaS case

Fig. 6. Relative execution time for a typical IaaS case

Fig.7 illustrates the average consumed time (in msec) to achieve the decryption operation of a message with a length of 100 characters using RSA, mRSA in local computer, and mRSA between the user and the SEM. As an additional option to provide more security for the cloud users, users can encrypt their files locally before storing them in the cloud. In this case, we offer symmetric algorithms to do this.

Fig.8 presents the average execution time of the RSA signature and RSA verification algorithms for the same message by using four types of hash function, while Figure 9 shows the average execution time for signing and verifying the same message using mRSA between the users and SEM. In this latter case, much more time is required because the users only have halves of their private keys and need to communicate with the SEM to complete the process. We can also note that in Fig.9 the SHA512 algorithm consumes significant longer time for signing the message. Therefore, users can use another type of hash function to sign and verify their messages.

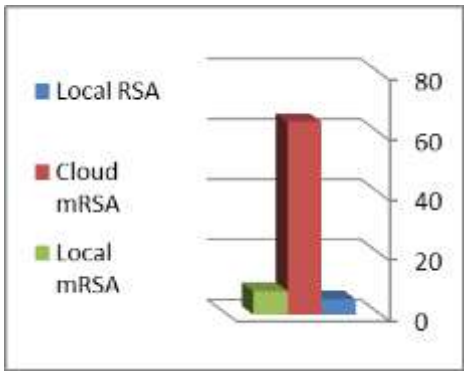

Fig. 7. Execution time for decrypting 100 characters (msec).

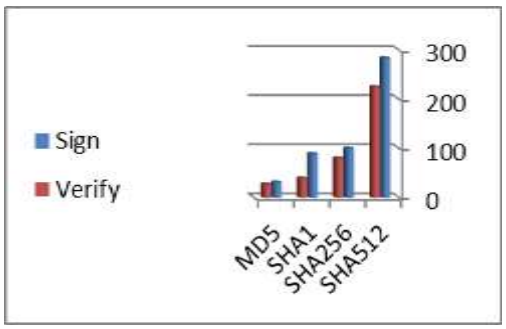

Fig. 8. Execution time for signing and verifying a message using RSA (msec).

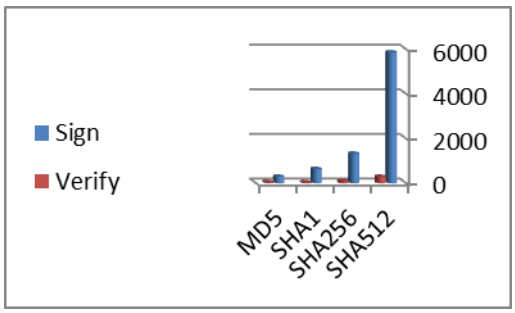

Fig. 9. Execution time for signing and verifying a message using mRSA (msec).

Conclusions

The integration of IBC, TC concept, and mediated cryptography has resulted in efficient and secure IAM system. The proposed IAM architecture has the capability to provide more transparency to users and increase security measures of IAM in cloud environments. The prototype implementation has shown that one of the important restrictions is cloud computing needs a large bandwidth of internet for transferring data between the users and CSPs. Cloud computing is good choice for complex and large applications, but it could be less attractive for small applications. Future research might consider integrating different schemes of IBC to our proposed architecture and compare the pros and cons of various combination. Another direction can be the deployment of our system on a more sophisticated cloud computing environment and measuring its performance and other characteristics in real world setting.

References

1- Sugang Ma, “A Review on Cloud Computing Development”, Journal of Networks, Academy Publisher, Vol. 7, No. 2, P.305, February 2012.

2- 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, P169, 2011.

3- Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic, “DACC: Distributed Access Control in Clouds”, International Joint Conference of IEEEon Trusted Communications, TrustCom-11/IEEE ICESS-11/FCST-11, P. 91, 2011.

4- 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.

5- Rohit Ranchal, Bharat Bhargava, Lotfi Ben Othmane, Leszek Lilien, Anya Kim, Myong Kang and Mark Linderman, “Protection of Identity Information in Cloud Computing without Trusted Third Party”, The 29th IEEE International Symposium on Reliable Distributed Systems, P.368, 2010.

6- Il Kon Kim, Zeeshan Pervez, Asad Masood Khattak and Sungyoung Lee, Chord Based Identity Management for e-Healthcare Cloud Applications, The 10th Annual International Symposium on Applications and the Internet, p.391, 2010 IEEE.

7- Maciej Machulak and Aad van Moorsel, Architecture and Protocol for User-Controlled Access Management in Web 2.0 Applications, IEEE 30th International Conference on Distributed Computing Systems Workshops, Italy, P.4, June 21-25, 2010.

8- Weiwei Jia , Hoajin Zhu, Zhenfu Cao, Lifei Wei, and Xiaodong Lin, "SDSM: A Secure Data Service Mechanism in Mobile Cloud Computing," The first International Workshop on Security in Computers, Networking and Communications, IEEE, 2011, pp. 1060-1065.

9- Lili Sun, Hua Wang, Jianming Yong, and Guoxin Wu, "Semantic Access Control for Cloud Computing Based On E-Healthcare," IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), 23-25 May 2012, pp. 512-518.

10- Luis M. Vaquero , Luis Rodero-Merino and Daniel Morán, “Locking The Sky: A Survey on Laas Cloud Security”, Springer-Verlag, P.95, 2010.

11- Wayne Jansen and Timothy Grance, ”Guidelines on Security and Privacy in Public Cloud Computing”, National Institute

of Standards and Technology, Special Publication 800-144, p.21, January 2011.

12- Sameera Abdulrahman Almulla and Chan Yeob Yeun, ”Cloud Computing Security Management”, Second International Conference on Engineering Systems Management and Its Applications (ICESMA), March 30- April 1, Sharjah, pp. 1-7, 2010.

13- Joonsang Baek, Jan Newmarch, Reihaneh Safavi-Naini, and Willy Susilo, “A Survey of Identity-Based Cryptography”, Proc. of Australian Unix Users Group Annual Conference, p.1-10, 2004.

14- Divya Nalla and K.C. Reddy, “Signcryption Scheme for Identity-Based Cryptosystems”, J. Mathematics of Computation, p.1-10, 2003.

15- Dan Boneh, Xuhua Ding, and Gene Tsudik, Identity-Based Mediated RSA, Dow Jones & Company, Inc, p.1-12, 2002.

16- Sufyan T. Faraj and Hussien K. Abdul-razaaq, "Email Security Using Two Cryptographic Hybrids of Mediated and Identity-Based Cryptography", i-manager's Journal on Software Engineering (JSE), Vol. 6, No. 3, pp. 1-12, January – March 2012,

17- Dan Boneh, Xuhua Ding, Gene Tsudik and Chi Ming Wong, “A Method for Fast Revocation of Public Key Certificates and Security Capabilities”, SSYM'01 Proceedings of the 10th conference on USENIX Security Symposium - Volume 10, Pages 22 – 22, 2001.

18- Liqun Chen, Bristol (GB); Keith Alexander Harrison, wooderoft Chepstow (GB), “Mediated RSA Cryptographic Method And System”, US Patent Application Publication, P.1-18, Dec. 16, 2004.