International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-7)

Research Article

July 2015

Enhancing the Security of Identity and Access Management in Cloud Computing using Elliptic Curve Cryptography

Assist. Prof. Dr. Salim Ali Abbas
Department of Computer Science, College of Education,
Al-Mustansiryah University
Iraq

Abstract—

Cloud computing is the new technology that aims to provide software, hardware, bandwidth, and virtualized resources on demand via the internet based on the principle of pay per use. There are many challenges that facing the cloud computing, one of the main concerns is managing the identity and access control. This paper focuses on improving the security of identity and access management (IAM) in cloud computing. The proposed scheme combines the security of Identity-Based Cryptography (IBC), Trusted cloud (TC), and Elliptic Curve Cryptography (ECC). IBC is suitable choice for IAM because it reduce the key management complexities, and an ECC is robust algorithm and resistance against attacks.

Keywords— Cloud computing, Cryptography, Elliptic Curve, Identity and Access Management

I. INTRODUCTION

Cloud computing is a new technology often used virtualized with resources to provide dynamically scalable service via the internet. In the cloud computing, users can access to the resources by using a various devices, such as laptops, PCs, smart phone, etc. to access multiple service such as storage, programs, and application-development platforms, over service that provided by cloud providers via the internet. Through the last years, Cloud computing improved from simple web applications, such as Gmail and Hotmail, into business propositions like SalesForce.com, AmazonEC2, etc [1].

Cloud computing may be supply service for reducing IT costs, business management, and maintenance costs of hardware and software are effective. At the same time, it makes the enterprises able to access to professional IT solutions. Data storage center in cloud computing can be reliable and secure, because the world's most advance data center is helping the users save the data. The users must not concern about virus attack, data loss, and other problems when they used the cloud in correct form [2].

User with cloud computing can use the cloud services anywhere, everywhere, on-demand and based on pay per use principle. Cloud computing has two types of models: services models (SaaS, PaaS, and IaaS), and deployment models (Public, Private, Community, and Hybrid cloud). Also the cloud computing is contains five essential characteristics (On-Demand, BroadNetwork Access, Rapid Elasticity, Measured Service, and Resource pooling). There are many companies that provide cloud services such as Amazon, Google, Microsoft, and SalesForce.com, etc.

There are many concerns about the security of cloud computing should be taken into account such as violation of the confidentiality and privacy of customers' data via unauthorized parties. The major concern is managing the identity of users [3]. Therefore, we have dedicated our work to design a new architecture to improve performance of Identity and Access Management (IAM) in the cloud computing by using Identity-Based Cryptography (IBC) and Elliptic Curve Cryptography (ECC) with a Trusted Cloud (TC).

This paper organized as follows: Section 2 displays some works that related to the field of Identity and Access Management in cloud computing. Section 3 reviews some techniques that used in AIM. Section 4 explains Identity-Based cryptography (IBC). Section 5 review the general concept of ECC. Section 6 illustrates the implementation of our system. Section 7 shows our work conclusion.

II. LITERATURE SURVEY

Several works related to our work, which presents the security of identity access management in cloud computing as follow:

In 2009 Liang Yan, Chunming Rong, and Gansen Zhao proposed to use hierarchical identity-based cryptography (HIBC) with federated identity management, not only to key distribution but also the reciprocal authentication may be simplified in the cloud [4].

In 2010 Rohit Ranchal, and et al. proposed a method for Identity management (IDM) without relying on of Trusted Third Party (TTP) and has the possibility to use identity data on untrusted hosts [5].
In 2012 Chunming Rong and Hongbing Cheng propose a secure data access mechanism based on identity-based encryption and biometric authentication for cloud tenants [6].
In 2013 Sameeh A. Jassim propose a new system for Identity and Access Management (IAM) depend on combination of the techniques of security mediated cryptography and Identity-Based Cryptography (IBC) with the Trusted Cloud (TC) to simplify the management and offer more security and access control for cloud computing [2].
In 2013 Shan-Shan Tu, Meng-Jiao Li, and Xiao-Zhang Niu proposed an effective access control system for cloud environment based on Attribute-Based Encryption (ABE) and Identity-Based Signature (IBS) schemes using bilinear pairings [7].
In 2014 Nagendra Kumar, Ashok Verma and Ajay Lala proposed a framework double authentication techniques and specialized procedures that can effectively protect the data during the period of transition from the user to the cloud. This method for Access, identity and secure data storage in private cloud by utilize DS (Digital Signature) using RSA algorithm [8].

III. IDENTITY AND ACCESS MANAGEMENT (IAM)

Managing the access control and identities for company applications still the major challenges that facing the cloud computing. Unauthorized access to the cloud resources is a major concern for the company's, because companies have sensitive and private information. CSP must provide appropriate IAM solutions to ensure secure access to the data [9]. IAM is a set of technologies, processes and data required for managing access to organizational resources. IAM is the basic building block of any informational security program and most widely interactive security areas by users [10].
IAM can be considered as the first layer of defense in cloud security. CSP used IAM to validate claimed user by verifying the user's credentials against a directory, and allow the customers to manage identities and authorizations to the resources of customers that are hosted by the vendor [11]. IAM technology are creating, register and manage user's identities and access permissions. This ensures that users access privileges are given by company according to its policies, and all services and customers are correctly authorized, authenticated, and audited [12].

III.1 IAM Life Cycle

The management of user identity and access control permissions can be analyzed as multiple stages. Figure (1) illustrates the IAM life cycle the stages that users follow when they join an organization and obtain access to the tools, assets required to do their jobs. The IAM life cycle also includes stages to ensure that employees hold appropriate access as they go within the organization with access being revoked or modified when they separate or change their roles [10].

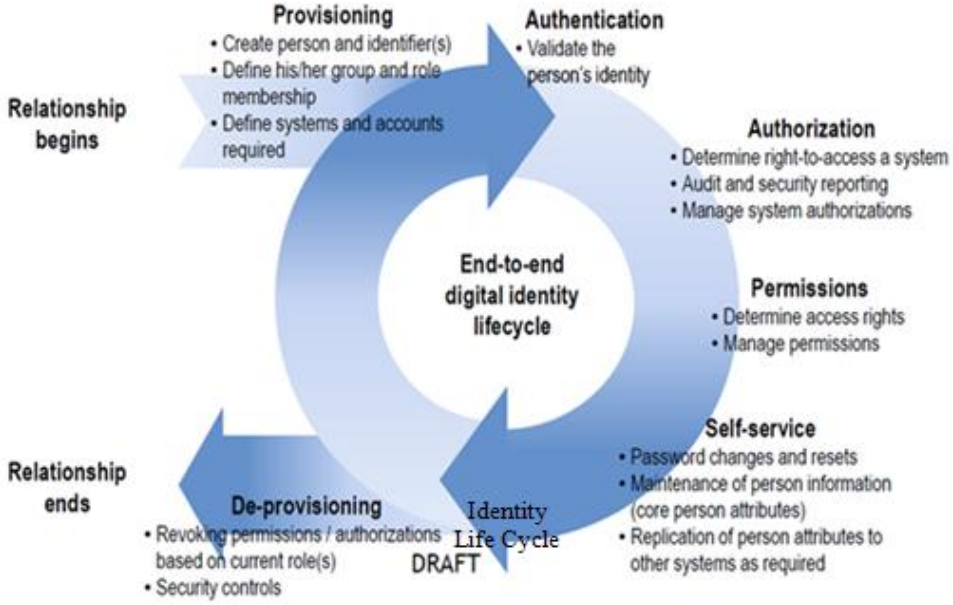

Figure 1: The IAM Life Cycle [13]

III.2 Single Sign-On

A Single Sign-On (SSO) is the process that facilitates maintenance tasks for SPs and allows users access to all the services one logged in [14]. With using SSO users can gain access to the resources from multiple systems by using the

same username and password. This can reduce the number of passwords that the user needs to remember and the number of logons [15]. The passwords must be transmitted or stored in encrypted form to save security of SSO. SSO has many benefits such as ease in the process of administration of deleting or changing the passwords, the ability to use strong passwords, reduce the time that require to access resources. The main disadvantage of SSO is that the user can access to whole system without any restrictions through the single logon, this property may exploit by attacker [16]. The problem is how to collect the information of user login across many applications and platforms to facilitate the signing and increase security? The solution is a federal identities.

III.3 Federated Identities

Federated identity is a set of standards, agreements, and technologies that allow to a group of SPs to recognize the identifiers and dues of users from other SPs within a federated scope [17]. Federated Identity Management (FIM) System helps to avoid replication of user identities at multiple locations and several security domains, thereby provides an easy way to manage user identities and allowing them to access information available at several related domains in a trusted mode [10]. FIM System has two basic types of entities: service providers (SPs) which provide services to users, and identity providers (IDPs) which manage the authentication of user and the information that related to user identity [15].

There are three major protocols for federated identity: SAML, OpenID, and OAuth.

1. **SAML:** SAML (Security Assertion Markup Language) is one of an open standard protocols created by OASIS and its main mission is to solve the Web Browser SSO problem [18]. SAML was started in 2001, uses protocol XML, HTTP, and SOAP in which user registration is not required [10]. SAML is based XML that exchange authorization and authentication data between multiple applications and organizations. It can remove most passwords in the cloud and enable the use of SSO, this feature is required because it does not need login for each application. Rather than use password the application which use SAML accept secure tokens to identify what is required to get to the applications. This reduces the number of passwords that can be stolen or forgotten. SAML has three entities: SP, IDP, and the user who asks the service from SP and gets validate by IDP [19].

2. **OpenID:** OpenID is an open standard which issued in 2005. The functions of OpenID like that of SAML, but OpenID was prepared for consumer services and applications rather than using for a specific enterprise users. The enterprise users can also use OpenID now. OpenID is sponsored by Google, Facebook, Yahoo, Microsoft, etc. In the OpenID user can use only one user name and one password to gain access to many Web applications. An OpenID server allow user authenticate to get and use the token to authenticate the web applications. The user of OpenID doesn't need to supply the SP with his credential or other sensitive information like an email address [20].

3. **OAuth:** OAuth (Open Authorization) is an open standard authorization protocol that allows sharing of security context without the need to share identity/credentials. For instance users might share private resources such as contacts, photos and videos that is stored in one website to another website without the need to deliver a user name and password of their own. OAuth is complementary to OpenID, but a separate service. OAuth was born when Blaine Cook, who was working in the OpenID for authentication development of Twitter, note that OpenID is not sufficient to authenticate users of Twitter so began searching for another way and in collaboration with Chris Messina to produce OAuth. OAuth is an authentication platform protocol enables intermediate applications have access to the user's private data through the service based on the HTTP protocol. There are many application use OAuth such as Facebook, Dropbox, Flickr, Google, Instagram, LinkedIn, etc. Finally, the use of any application broker asking the user access to a private data does not use protocol OAuth is not secure application and must never be used[18].

IV. IDENTITY BASED CRYPTOGRAPHY (IBC)

IBC is one of the types of public key cryptography, which was initially proposed by Adi Shamir in 1984 to reduce the need for certificate authorities to distribute public key certificate. In IBC use users' identifier information such as phone number, email, IP addresses, or domain name as a public key rather than used digital certificates. Shamir implemented an identity based signature (IBS) by used RSA algorithm to allow users to verification from digital signatures. Although he tried to implement an identity based encryption (IBE), but he was unable to reach a solution and IBE remained open problem for many years. Until 2001, Franklin, Boneh, and Cocks independently proposed scheme to solve IBE problem by using bilinear pairings and have provable security. IBC allow to any two users to communicate securely, and verification of signatures each other without exchanging any type of keys [21, 22, 23].

The Identity-based cryptography systems contain the Private Key Generator (PKG) that act as a trusted third party, which create a master private key (Mk) and a master public key (Ps), then PKG will publish the master public key and keeps a master private key secret. Any user can generate his public key by combining a master public key and his identity. The user must connects the PKG with his identity to obtain his private key (Pr). PKG will use the master private key and user's identity to generate user's private key [4].

V. ELLIPTIC CURVE CRYPTOSYSTEM

Elliptic curve cryptography (ECC) is one of the public key encryption algorithms which is depend on elliptic curve theory over finite fields. It used to make cryptographic keys smaller, faster, and more efficient. The functions and characteristics of an elliptic curves have been studied in mathematics for 150 years. Their use has been suggested in cryptography for the first time by Neal Koblitz and Victor Miller in 1985, separately [24]. ECC has begun to obtain acceptance of many of the accredited organizations, and many of the security protocols since the beginning of 1990 [25].

V.1 Elliptic Curve Arithmetic

The main attraction of ECC is that it provides an equal level of security, but much smaller key size compared with RSA. We can defined an elliptic curve by equation all its coefficients and variables take values in the set of integers within the range from 0 to p-1, which is performed calculations modulo p. When use an elliptic curve for cryptography, the coefficients and variables are restricted in a finite Abelian group* [26, 27]. The group that has a finite number of elements, it's known as a finite group and the number of elements in $\mathbb{G}$ is known as the order of $\mathbb{G}$ [28]. ECC equation over $\mathbb{Z}_p$:

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

The rules for addition over $E_p(a,b)$ for all points $P, Q \in E_p(a,b)$:

1. $P + \infty = P$.
2. If $P = (x_P, y_P)$, then $P + (x_P, -y_P) = \infty$. The point $(x_P, -y_P)$ is the negative of (P), denoted as (-P).
3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$y_R = (\lambda^2 (x_P - x_R) - y_P) \bmod p$$
$$x_R = (\lambda - x_P - x_Q) \bmod p$$

Where

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{If } P \neq Q \\ \dfrac{3x_P^2 + A}{2y_P} & \text{If } P = Q \end{cases}$$

4. Multiplication is defined as repeated addition; for example, $4P = P + P + P + P$.

V.2 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Assume that E is an elliptic curve over some finite field $\mathbb{F}_q$, and P a point of order n on E. ECDLP on E is to find the integer $d \in [1,n-1]$, if such an integer exists, so that

$$Q = dP, \text{ where } dP = \underbrace{P + P + \ldots + P}_{d \text{ times}}$$

The discrete logarithm problem (DLP) is does not look like ECDLP, and that ECDLP is considerably more difficult than the DLP. This is due to the lack of known subexponential-time algorithm to solve ECDLP in general [29].

V.3 Security of Elliptic Curve Cryptography

ECC algorithm is one of the most powerful asymmetric algorithms for a particular key length, so that it is attractive especially for security applications where integrated circuit space and computational power is limited, such as PC

* We can say about the group ($\mathbb{G}$) is an Abelian group or commutative group if achieved the following condition: $m * n = n * m$ for all m, n in $\mathbb{G}$.

(personal computer) cards, smart cards, and wireless devices. ECC algorithm security is relies on the difficulty of solving ECDLP. Currently it seems that ECC that be implemented on 160-bit nearly offer the same level of security in the resistance against compared with 1024-bit RSA attacks. That led to improved performance and better storage requirements [27]. Table (1) presents a comparison of the approximate parameter size between strength elliptic curve systems and RSA.

Table 1: Comparative Bit Lengths [29]

Elliptic Curve Cryptosystem (order of base point P)	RSA (length of the modulus n)
106 bit	512 bit
132 bit	768 bit
160 bit	1024 bit
224 bit	2048 bit
384 bit	7680 bit

VI. THE ESSENTIAL MODULES OF THE PROPOSED IAM SYSTEM

The proposed system contain three parts: Private Key Generator (PKG), Trusted Cloud (TC), and User. The system management, access control, and user authentication are done by Trusted Cloud, while the PKG is use to manage users' keys. This proposal aims to provide more secure method to secure users' login and data protection, reduce the complexity of management by using IBC, and provide transparency to cloud computing users'. The main idea of this proposal is combine the security of IBC and ECC with Trusted Cloud (TC) which used for system management. The use of IBC will significantly decrease the key management complexity and not need to certificate issued. Also the use of TC has many benefits such as decrease the denial of service attack (DOS) on CSPs, this important attraction because TC has all users' information. Also TC provide SSO property to users by chosen suitable companies to provide service, thereby the user does not need to repeat login operation each time they use cloud services. All these parts increase the strength and resistance of the system. Figure 2 explains the general structure of the proposed system.

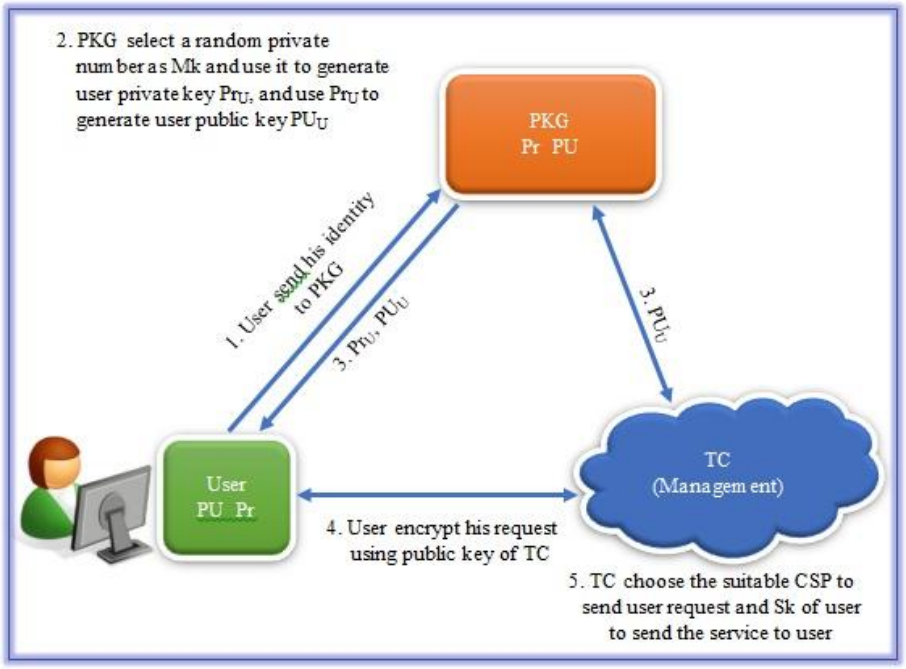

Figure 2: General Structure of Proposed System

The Proposed algorithm

a. Setup: the **PKG** do the following functions:

1. Chooses a prime number **p** that has the prime order **n**, and a finite filed $\mathbb{F}_p$.

2. Chooses the curve **E** over $\mathbb{F}_p$ in the form where ***a*** and ***b*** are the curve parameters.

3. Chooses the base point **P** in **E($\mathbb{F}_p$)** whose order **n** should be very large.

4. $y^2 = x^3 + ax + b$Selects a random number smaller than the base point **P** order as a private number, this number will be a master private key **Mk**.

b. Extract: when user wants to get his private and public key from **PKG**, he must send his identity ($\mathbf{ID_U}$) to **PKG**. Then the **PKG** will compute the hash value to the identity of user ($\mathbf{ID_U}$) and use it with master private key **Mk** to generate user private key, and use this private key to generate user public key.

$\mathbf{Q_U = H\ (ID_U)}$
$\mathbf{Pr_U = Mk*Q_U}$
$\mathbf{PU_U = Pr_U*P}$

Then send copy from user's private key to user, and copy of public key to user and TC.

c. Encryption: If user requests a service from TC, he can encrypt his request by using the public key of TC to generate his ciphertext. If Alice want to send a message to Bob, she will use the public key of Bob, the following steps will explain this operation:

1. Alice encodes her message to points $\mathbf{P_m}$.
2. Alice encrypts her message as follows:
a. Selects a random integer number **J**.
b. Calculates the ciphertext $\mathbf{C_m}$ consists of the pair of points

$$\mathbf{C_m = \{J*P,\ P_m + J*PU_B\}}$$

c. Alice
d. sends $\mathbf{C_m}$ to Bob.
e. Decryption: When Bob receives the encrypted message $\mathbf{C_m}$ from Alice, he will decrypted the message by computes:

$\mathbf{P_m + J*PU_B - Pr_B(J*P)}$
$\mathbf{P_m + J(Pr_B*P) - Pr_B(J*P) = P_m}$

Then he decodes $\mathbf{P_m}$ to get the original message **m**.

f. Signing and Verifying: Alice can signing the message **m** by using her private key **Pr** as follows:

1. Calculates the hash value to the message
2. Chooses a random positive integer **J** in interval [1, n-1].
3. Calculates **(x,y) = J*P**.
4. Calculates

$\mathbf{e = H\ (m)}$
$\mathbf{r = x \bmod n}$, if $\mathbf{r = 0}$ go to step 2.
$\mathbf{S = J^{-1}\ (e + Pr_A*r) \bmod n}$, if $\mathbf{S = 0}$ go to step 2.

5. Calculates
6. The message's signature is the pair **(r,S)**.
7. Sends the signature **(r,S)** to Bob.

Bob when receive the message he must verify the signature based on the public key $\mathbf{PU_A}$ of Alice as follows:

1. Calculates
2. Calculates
3. Calculates

$\mathbf{e = H\ (m)}$
$\mathbf{w = S^{-1} \bmod n}$.
$\mathbf{u1 = e*w \bmod n}$ and $\mathbf{u2 = r*w \bmod n}$.
$\mathbf{= u1*P + u2*PU_A,}$

4. **(x,y)** if **(x,y)=**∞ then reject the signature, otherwise calculates
5. If then the signature is valid otherwise invalid.

$\mathbf{v = r}$
$\mathbf{v = x \bmod n}$.

VII. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

Cloud computing is good choice for large and complex systems, but it less attractive for small applications. This paper propose a more flexible and effective verification scheme to address the security of IAM in cloud computing. The combining of IBC, TC, and ECC led to secure and efficient IAM system. The proposed IAM system has the ability to increase the security of IAM, which provides transparency to users in cloud environments. Future researches might consider in future such as combining different schemes of IBC to the proposed scheme architecture and compare the advantages and disadvantages of various combination.

REFERENCES

[1] Jeffrey Voas and Jia Zhang, "Cloud Computing: New Wine or Just a New Bottle?", Published by the IEEE Computer Society, 2009.

[2] Sameeh A. Jassim, MSc thesis, "Mediated IBC-Based Management System of Identity and Access in Cloud Computing", College of Computer, University of Anbar, 2013.

[3] Sameera Abdulrahman Almulla and Chan Yeob Yeun, "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), Presented at 2nd IEEE International Conference, 30 march 2010.

[4] Liang Yan, Chunming Rong, and Gansen Zhao, "Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography", Springer-Verlag Berlin Heidelberg, 2009.

[5] Rohit Ranchal and et al, "Protection of Identity Information in Cloud Computing without Trusted Third Party", 29th IEEE International Symposium on Reliable Distributed Systems, 2010.

[6] Chunming Rong and Hongbing, "A Secure Data Access Mechanism for Cloud Tenants", The Third International Conference on Cloud Computing, GRIDs, and Virtualization, May 2012.

[7] Shan-Shan Tu, Shao-Zhang Niu, and Meng-Jiao Li, "An Efficient Access Control Scheme for Cloud Environment", CYBERNETICS AND INFORMATION TECHNOLOGIES, Volume 13, No 3, 2013.

[8] Nagendra Kumar, Ashok Verma and Ajay Lala, "Access, Identity and Secure Data Storage in Private Cloud using Digital Signature", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[9] S.Sudha and V.Madhu Viswanatham, "Addressing Security and Privacy Issues in Cloud Computing", Journal of Theoretical and Applied Information Technology, Vol. 48, No. 2, 20 February 2013.

[10] Nida et al, "A Survey on Identity and Access Management in Cloud Computing", International Journal of Engineering Research & Technology (IJERT), Vol. 3 Issue 4, April 2014.

[11] Many Siddiqui, "Cloud Computing Security", Paper Blog, INFO 661, spring 2011.

[12] Ali M. Al-Khouri, "Optimizing Identity and Access Management (IAM)", International Journal of Engineering Research and Applications (IJERA), Vol. 1, Issue 3, 2011.

[13] Sonja van der Westhuizen, "Identity and Access Management", Stellenbosch University, Available at http://blogs.sun.ac.za/it/tag/ sunid/identity_and_access_management_101.pdf.

[14] Independent Centre for Privacy Protection (ICPP) / Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and Studio Notarile Genghini (SNG), "Identity Management Systems (IMS): Identification and Comparison Study", September 2003, Available at:https://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf.

[15] Roberto Baldoni, "Federated Identity Management Systems in e-Government: the Case of Italy", Electronic Government, an Inanrnational Journal, 2009 Inderscience Enterprises Ltd.

[16] Ronald L. Krutz and Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., 2010.

[17] Audun Jøsang and Simon Pope, "User Centric Identity Management", AusCERT Conference, 2005.

[18] Tor Anders Johansen, MSC thesis, "Identity management in future personalized service Environments", Department of informatics, UNIVERSITY OF OSLO, 30 April 2010.

[19] Ardi BENUSI, "An identity management survey on cloud computing", Int. Journal of Computing and Optimization, Vol. 1, no. 2, 2014.

[20] Bharat Bhargava, Noopur Singh and Asher Sinclair, "Privacy in Cloud Computing Through Identity Management" GIT Journal of Engineering and Technology, 2011.

[21] Marc Joye and Gregory Neven, "Identity Based cryptography", IOS Press, 2009.

[22] Joonsang Baek et al, "A Survey of Identity-Based Cryptography", Australian Unix Users Group Annual Conference, 2004.

[23] Divya Nalla and K.C.Reddy, "Signcryption scheme for Identity-based Cryptosystems", Mathematics of Computation, 2003.

[24] Ravi Gharshi and Suresha, "Enhancing Security in Cloud Storage using ECC Algorithm", International Journal of Science and Research (IJSR), Volume 2 Issue 7, July 2013.

[25] Chester Rebeiro, M.Sc. thesis, "Architecture Explorations for Elliptic Curve Cryptography on FPGAS", Department of Computer Science and Engineering, Indian Institute of Technology, Madras, February 2009.

[26] William Stallings, "Cryptography and Network Security", principles and practice 5th edition, Pearson Education, Inc., 2011.

[27] Ali Makki Sagheer, MSc thesis, "Enhancement of Elliptic Curve Cryptography Methods", Computer Science, University of Technology, 2004.

[28] Darrel Hankerson, Alfred Menezes and Scott Vanstone, "Guide to Elliptic Curve Cryptography", Springer-Verlag New York, 2004.

[29] Majid Khabbazian, MSc thesis, "Software Elliptic Curve Cryptography", Department of Electrical and Computer Engineering, University of Victoria, 2004.

