Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Privacy and Dynamic Trust Establishment in Identity Management

Pradeep A. Aher*
Dept. of Computer Engineering
University of Pune
India

Manisha R. Patil
Dept. of Computer Engineering
University of Pune
India

Abstract— Consumer cloud computing phenomenon has been important in the process of the natural evolution and integration of advancements in many areas such as distributed computing and consumer electronics. In today's era, there are many challenges for security and identity management due to their dynamic nature. Due to this, dynamic federated identity management with improved privacy has emerged as an indispensable technique to have the global scalability and usability necessary for the successful implementation of Cloud technologies. Considering these all things, an IdM architecture based on privacy and reputation standards is presented and using that architecture, an application is developed which will allow user's account management and dynamic data movement when user transfers from one cloud to another cloud. Dynamic trust establishment is an important aspect in this application. Also audit management and privilege transfer of an identity provider are added functionalities.

Keywords— Cloud service provider, Identity Provider, Enhanced Client Profile, Identity Management, Privacy, Trust Manager.

I. INTRODUCTION

Cloud computing phenomenon has been important in the process of the natural evolution and integration of advancements in many areas such as distributed computing and consumer electronics. Similarly cloud computing integrated with home network is called as the consumer cloud computing which is also evolving fast. There are different applications of the cloud platform integrated with consumer electronics such as CloudTV. Consumer Electronics is nothing but the electronic appliances which is used in day-to-day life. In today's era, there are many challenges for security and identity management due to their dynamic nature. For example there should be interoperability between the private cloud and the community cloud as long as the users using the clouds have the trust established among both the clouds. Due to the open and distributed attributes of the cloud environments, dynamic trust propagation among the parties is necessary to manage the digital identity such as the accesses, privacy of data and other attributes, etc. Privacy is important across different domains and cloud environments. Hence dynamic federated identity management (IdM) with improved privacy has emerged as an indispensable technique to have the global scalability and usability necessary for the successful implementation of Cloud technologies.

In terms of consumer electronics, cloud federations have the capability to see how CE devices are developed, implemented or used and at the same time eliminating the constraints on device operability; considering home private clouds, public clouds, etc. For example, consider a consumer cloud scenario, in which cloud federation enables Ram to develop certain layers in his tempo navigation map to acquire suggestions for the best routes (CSP1); as well as consult corresponding information on sites close to his position, in a Cloud Tourist Information Provider (CSP2), with the help of the cooperation between his mobile and the tempo navigator. Also, Ram can connect to his Social Network (CSP3) to check if some of his friends have been on that site and share information with them with checking his privacy.

In this paper, dynamic privacy-enhanced federated identity management solution is proposed for cooperation, on demand resources provisioning and delegation in cloud computing scenarios with preservation of the user's privacy. The proposal defines an enhanced privacy module, a new data storage algorithm, and taking the Enhanced Client Profile (ECP) proposed in [5] under consideration, to provide an efficient identity management and access control, as well as dynamic trust establishment in cloud federations.

Further sections discuss the related works, existing trust aware IdM architecture, proposed system based on the existing architecture, conclusion and future work.

II. RELATED WORK

There has been some work done about IdM in consumer cloud computing, mainly focusing on identity management, dynamic federation and privacy issues. The proposals described are mainly centred in cloud computing, because consumer cloud computing is still an evolving paradigm. Also, considering trust management based on reputation within identity management is a new paradigm. The report also addresses the management of trust relationships dynamically including unknown entities and trust evolution.

A. Identity management and authentication

Though there exist some current works which propose to share media, cloud services and personalized content by means of a user-centric approach using different authentication and authorization mechanisms, none of them deals with dynamic federated identity management along with privacy tools in the consumer cloud computing scenarios. There are some authors who have focused on using the zero knowledge proof techniques to preserve the user privacy while providing his/her identity. But it doesn't consider the dynamic property of management of trust relationships. The application based on the existing architecture focuses on the trust evaluation and audit services.

B. Dynamic federation between cloud providers

There is not much work done on the area of dynamic trust establishment but it has always been identified as the important area to achieve the usability and scalability in cloud applications. Approaches related to trust management in distributed environments is found for peer to-peer systems that are basics of emerging next generation computer applications.

C. Privacy

Privacy management is an important factor for consumer cloud computing and needs to be considered in order to offer a solution compliant with legislation and improve user trust while accessing to different environments through their CE devices. Legislation differs according to the country block and national legislation. But most privacy attributes [7] apply country wide. Pearson suggested many guidelines and techniques to design privacy-aware IdM architectures for cloud services viz. minimizing customer personal information sent to and stored in the cloud, protecting sensitive customer information, maximizing user control, allowing user choice, specifying and limiting the purpose of data usage and providing the customer with privacy feedback. Such suggestions are addressed in this paper. Also, the cross-site sharing and collection of user data while surfing also needs to be considered but again that can distrust the user and bring the negative feelings in the user's mind. In general, the work in the field of privacy is still at the early stages but many suggestions and recommendations can be found to maintain the user privacy in consumer electronics.

D. Existing Architecture

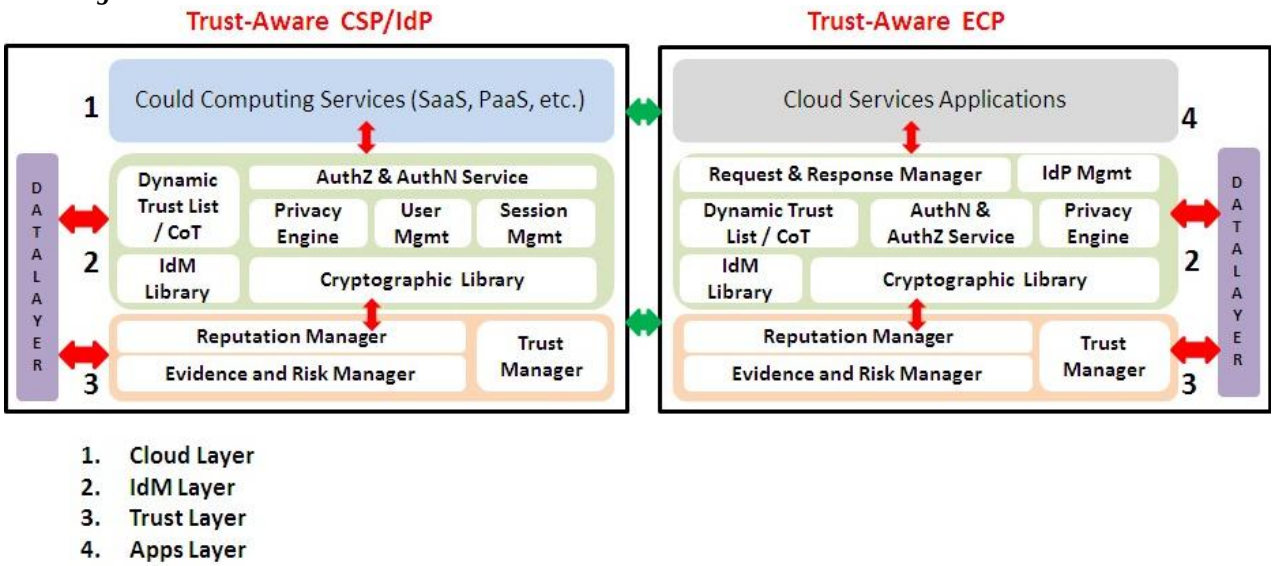

Fig. 1 Trust-Aware IdM Architecture [1]

The IdM infrastructure considers the functionality to allow Identity Providers (IdPs), Service Providers (SPs), and enhanced clients to share common knowledge. The ECP provides the required user-centric approach for cloud computing applications in consumer electronics devices. The ECP enables to minimize direct interactions between SPs and IdPs, and provides full control to users over their identities, and hence improving mainly privacy.

The architecture for the dynamic IdM system is represented in Fig. 1. The layered architecture shows the logic blocks and the relationship between them. At the top of the architecture, there can be either the Cloud or the Apps layers. The first one contains cloud services ordered by cloud providers (SPs or IdPs). The second one is located on the the ECPs, containing client applications. Next layer if IdM layer which mainly deals with dynamic trust establishment with DTL or CoT (Circles of trust) which stores the trust information. This trust information is updated through modules in underlying trust layer. IdM layer also deals with Session management, user account management, authentication and authorization services. The main part is cryptographic libraries which will store the data in encrypted form. The proposed application is focussing on this part as well which will use a separate algorithm to store the data. In addition, IdM layer focuses on the privacy by adding the Privacy Engine module. Privacy engine consists of the privacy preference services, personal identifier manager to manage the user identifiers, audit services to focus on data sharing and capturing the event when user data is requested from the cloud service provider. It also consists of action monitoring module which keeps track of the user activities and events in a consistent manner amongst all the cloud service providers.

Finally, there is a Trust layer, focusing on the reputation manager in order to allow secure interaction between unknown parties. This last layer combines reputation information with other related data, for example, historical interactions. So the user can request access, through the ECP installed on his/her mobile, to services provided by SPs and IdPs that are initially unknown in a dynamic and secure way. It also consists of the evidence and risk manager which analyses the risk factors associated with each user transaction and also keeps track of past interactions. It also calculates the trust values associated with each entity. Trust information is maintained by the trust manager which contains the data related to the behaviour of entities and trust information from the trusted third parties with whom user had interacted earlier.

III. PROPOSED SYSTEM

The proposed application attempts to implement the above mentioned architecture with some modifications. Basically the application is implemented in a private cloud for an institute, say SKNCOE private cloud. There are different types of user accounts maintained viz., student, teacher, accounting staff, non-teaching staff, etc. The Principal is the identity provider (IdP) or admin in the application which performs the user authentication and identity provision task and also if required, it communicates with IdP in another CSP to establish trust values for a particular user. Users can set their own privacy attributes based on which the user account is maintained and granted access to other users.

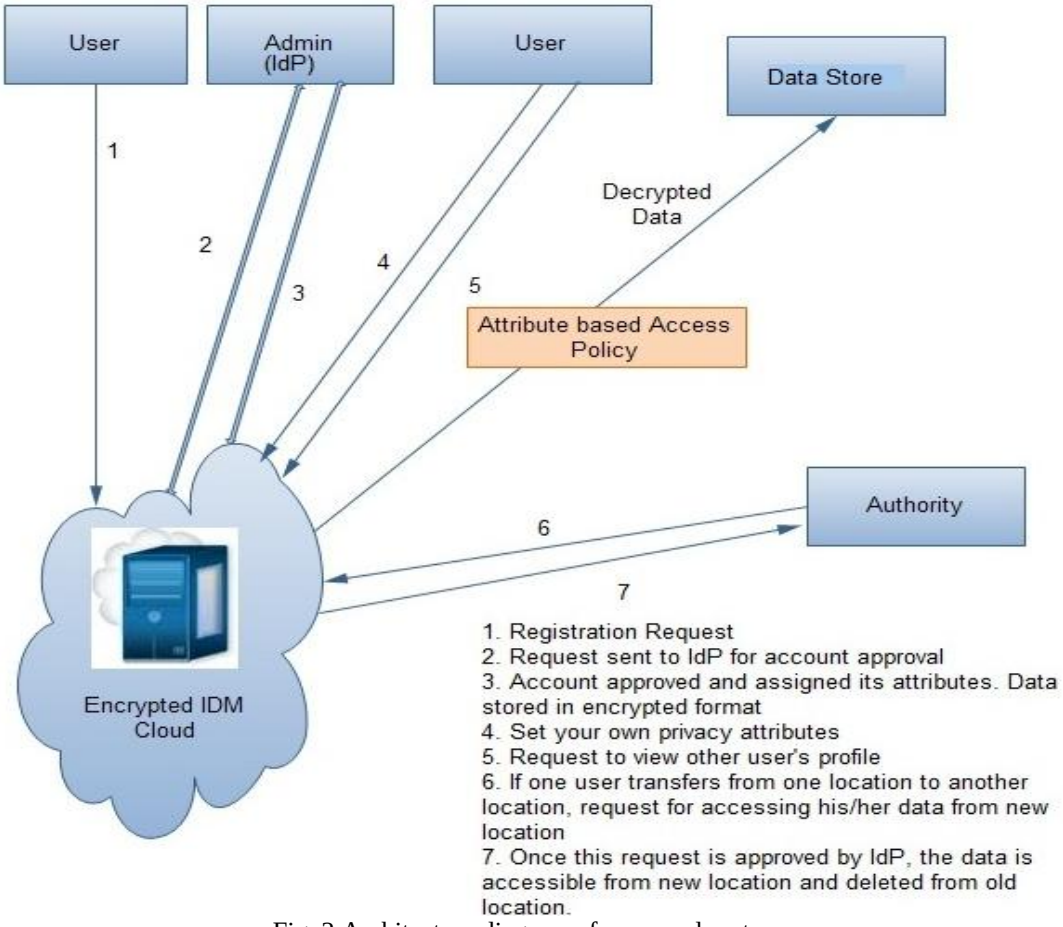

Fig. 2 Architecture diagram of proposed system

In the proposed system as shown in the above Fig. 2, a private cloud is setup and there are different user entities which resembles the enhanced client profile in the existing architecture, request the services from the cloud. Cloud service provider will reply to the services from the user. There can be following sequence of steps during the execution of the application.

1. User requests to have access to the services provided by the private cloud which he does by registering on the application. The cloud service provider needs to authenticate the user before he/she can be allowed to access the application services.

2. CSP identifies that the user identity is provided by the IdP i.e. the admin, Principal and forwards the identity provision request to IdP.

3. IdP then checks if the user has the trust values maintained in the trust table and he/she can be authenticated. Based on the trust values, IdP provides the identity to CSP to grant permission to the user. If in case, user wishes to transfer from one CSP to another CSP, then the IdP seeks the identity attributes and trust values from the IdP in another CSP.

4. Once the CSP approves the user request then user account is created by taking some information from the user. User needs to select the type of account and set the privacy attributes. Based on these privacy attributes set by the user, the access to user data is granted for the other users. All the user data is stored in encrypted format using RSA, AES & DES algorithms.

5. When the user transfers from one CSP to another then the data stored in the old CSP is transferred to a new CSP and then old copy is deleted from that CSP.

6. Attribute based access policy is used in which an attribute key is generated by the admin of the application which will be required to access the data of other users. Also there is a limitation to the access of data based in the type of account as discussed earlier as student or teaching staff or non-teaching staff, accounting staff, etc.

A. Planning of the proposed system

Initially, a private cloud is setup which stores the user information. The different entities in the system communicate through web services written on the provider side. Users need to create their own account to access the data stored on the private cloud. The user identity provision and trust management is maintained by the identity provider i.e. the admin of the application. Important part of the application is the data storage, which is in encrypted format and also the privacy attributes set by the user itself so that privacy is not compromised. Trust values are maintained by the IdP are based on the past interactions and those obtained from other IdPs, so user has the positive feeling and can trust the dynamic federation provided by the IdP. The overall high level flow of execution of the proposed application is as shown in the Fig. 3.

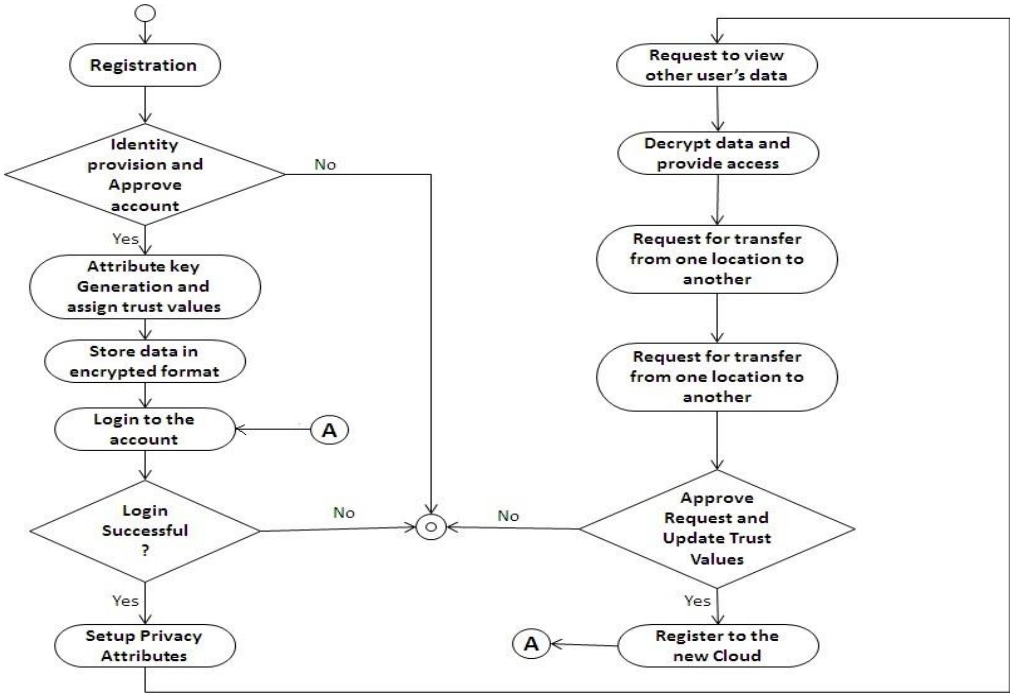

Fig. 3 Execution of proposed system

1) *Major input to the System:* Input to this system consists of the user information when user attempts registration on the application. When user transfers from one location to another, then the new location's IdP requires the trust information about the user from old location's IdP, as an input.

2) *Output from the System:* System generates outgoing emails to the users on registration containing the password of their account. Also admin gets an email when a user requests for a transfer from one location to another. System stores all the user information in encrypted format. System also provides trust values of the users.

B. Proposed Mathematics

1) *Input Data Sets:*

$U = \{U_i\}$ $\quad i \in [1, n]$

2) *Intermediate Results:*

$A = \{At_i\}$ $\quad i \in [1, m]$

$AK = \{Ak_i\}$ $\quad i \in [1, p]$

$PR = \{Pr_i\}$ $\quad i \in [1, q]$

3) *Output:*
Attribute keys generated by the admin
Email alerts to users on registration
Email alerts to admin on user's transfer request
Encrypted user data
Dynamic trust values maintenance and provision

TABLE I: SYMBOL TABLE

Symbol	Representation
U	Set of user account types
A	Set of user attributes
AK	Set of attribute keys
PR	Set of Processes

C. Implementation Details

The proposed system is implemented on the Windows 7 Ultimate operating system. It can be implemented on any other operating systems as well above Windows XP. It is implemented on the .Net platform in C#.net and ASP.net. Overall communication between the participating entities in the system, that is, user, CSP, IdP, etc. takes place with the help of web services written in C#.net. In built web services in .Net are used for encryption purpose. The database is Microsoft SQL server 2008 wherein the user data is stored in encrypted format. The encryption algorithms used are RSA, AES (for attributes having common values among different users like Name, City, etc.) & DES (for images).

IV. PERFORMANCE ANALYSIS

The proposed system makes use of three encryption algorithms namely; RSA, AES (Advanced encryption standard) & DES (Data encryption standard) based on the different data categories. Thus the encryption time is improved. Also when user tries to search or access any other user's data, these algorithms provides faster decryption and more efficient results. Thus overall encryption and decryption time is improved w.r.t the existing system which has used public key encryption i.e. RSA algorithm. Since RSA produces different encrypted key each time for the same value, it takes longer to search for a value because it involves decrypting each value stored and then compare it with the search string. Whereas, AES algorithm produces same encrypted key each time for a same value. Hence while searching, only the search string needs to be encrypted and compare it against the encrypted values in the database. This increases the search efficiency. Also, security is improved in the proposed system with the use of different encryption algorithms for different data categories. The graph comparison between the existing system and the proposed system for the encryption and decryption time while searching is as shown in Fig. 4.

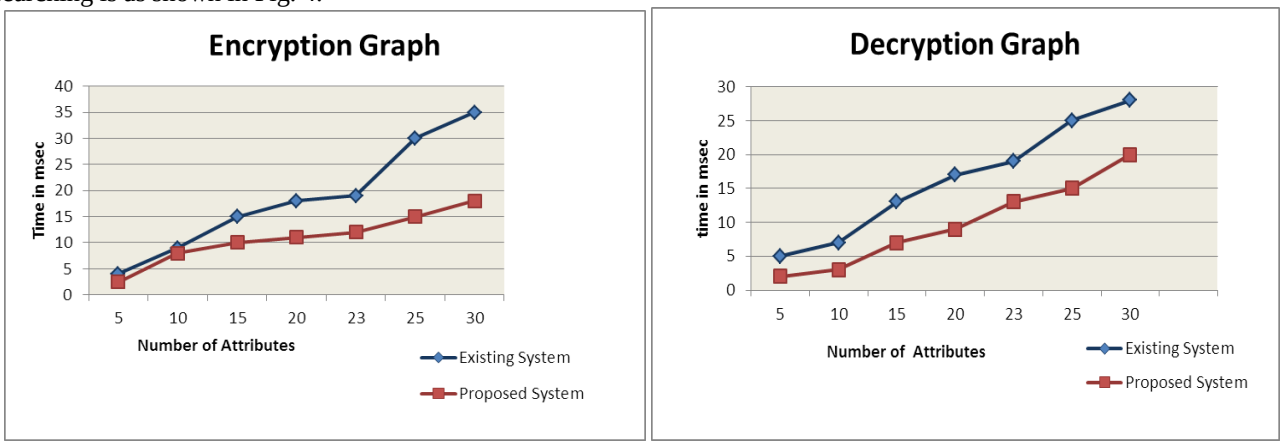

Fig. 4 Encryption and Decryption Time Efficiency Graph

Also, privacy attributes are in user control, so user can control which attributes should be visible to other users. This also helps to increase the security and maintain data integrity.

V. CONCLUSION

Cloud Computing has become the most important part of everyday life for almost all users. Subsequently, cloud computing is bring applied in many different areas such as consumer electronics. The main focus should be the privacy maintenance of the user data and trust establishment between different communicating entities.

Thus the proposed system makes use of the trust-aware IdM architecture and the privacy and trust aspects associated with the existing architecture. Also it helps users in private cloud to maintain privacy without bothering about their identity as it is handled by IdP. Also the system improves the security of user information and the search efficiency. This increases the overall performance of the system. The system can be improvised based on the area of application and the user requirement. Also different security attacks and risk management techniques can be focussed on, as a part of the future work.

ACKNOWLEDGMENT

For proposing this model referred the IEEE Transaction paper under the title "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing" published in IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, Vol. 58, No. 1, February 2012. This paper describes the enhanced-privacy and trust-aware IdM architecture which is taken as basis for the proposed system that is developed.

REFERENCES

[1] F. Almenarez, P. Arias, D. Diaz-Sanchez, A. Marin, and R. Sanchez, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", *IEEE Transactions on Consumer Electronics*, vol.58, no.1, February 2012.

[2] Open Cloud Manifesto Group: "Open Cloud Manifesto", 2009.

[3] P. Arias, F. Almenarez, A. Marin, and D. Diaz, "Enabling SAML for Dynamic Identity Federation Management", *Wireless and Mobile Networking Conference (WMNC'09)*, 2009.

[4] N. Ragouzis, J. Hughes, R. Philpott, E. Maler, P. Madsen, and T. Scavo (Eds.), *"Security Assertion Markup Language (SAML) V2.0 Technical Overview"*, Mar.2008.

[5] F. Almenarez, P. Arias, D. Diaz-Sanchez, A. Marin, and R. Sanchez, "fedTV: Personal Networks Federation for IdM in Mobile DTV", *IEEE Transactions on Consumer Electronics*, vol.57, no.2, May 2011.

[6] S.Grzonkowski and P.Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking", *IEEE Transactions on Consumer Electronics*, vol.57, no.3, May 2011.

[7] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", in Proc. of the Software Engineering Challenges of Cloud Computing (CLOUD'09), ICSE Workshop, 2009.

[8] A. Cavoukian, "Privacy in the clouds", Identity in the Information Society, Dec. 2008.

[9] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", Network Working Group, IETF Request for Comments: 5280, May 2008.

[10] E. Hammer-Lahav (Ed.), D. Recordon, and D. Hardt, "The OAuth 2.0 Authorization Protocol", IETF Network Working Group, draf-ietf-oauth-v2- 22, Sep. 2011.

[11] Liberty Alliance, "Identity Federation Framework (ID-FF) 1.2.Specifications", 2004.

[12] F. Hirsch, R. Philpott, E. Maler, "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0", OASIS Standard, March, 2005.

[13] P. Arias, F. Almenares, R. Sánchez, A. Marín and D. Díaz-Sánchez, "Multidevice Single Sign-On for Cloud Service Continuity", in Proc. of 30th *IEEE International Conference on Consumer Electronics (ICCE 2012)*, Las Vegas, Nevada, U.S.A, Jan. 2012.

[14] ETSI, "Identity and access management for Networks and Services; Dynamic federation negotiation and trust management in IdM systems", PN-fed Draft ETSI GS INS-004 V 0.0.5, Group Specification. Jan. 2010.

[15] S. Cantor, J. Kemp, R. Philpott, and E. Maler (Eds.), "Assertions and Protocols for the (OASIS) Security Assertion Markup Language (SAML) V2.0", OASIS Standard, Mar. 2005.

