*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 6, Ver. I (Nov.- Dec. 2017), PP 34-40*
*www.iosrjournals.org*

# Federated Cloud Identity Management: A Study on Privacy Tactics, Tools and Technologies

A. Mary Odilya Teena [1], Dr. M. Aaramuthan[2]
[1]*Assistant Professor, Department of Computer Science, St. Joseph's College of Arts & Science (Autonomous), Cuddalore & Ph.D. (Category-B), Research Scholar, Bharathiar University, Coimbatore.*
[2]*Associate Professor & Head of the Department of Information Technology, Perunthalaivar Kamarajar Institute of Engineering and Technology, Nedungadu, Karaikal.*

***Abstract:*** *With the rapid growth of cloud computing, many users shared sensitive data and multiple applications should be effectively managed via different cloud models and tools and it is needed for the safe management of identities and to avoid negotiating data privacy. The models and tools that speak federated cloud identity management, and it is essential that they use privacy appliances to assist in compliance with current law. So, this article aims to present a study of privacy in federated cloud identity management, presenting and comparing main features and challenges described in the literature. At the end, the use of privacy and future research directions are discussed.*

***Keywords:*** *Cloud Identity, Cloud Computing, Federated Cloud, Federated Cloud Identity Management, Safe Management of Identity, Data Privacy.*

---

Date of Submission: 26-10-2017 Date of acceptance: 16-11-2017

---

## I. Introduction

The goal of Cloud computing is to develop the supervision of computing resources by merging concepts such as elasticity, on-demand use, and dynamic resource allocation [1] [2]. The shared use of resources by different users and a very huge amount of data and information, such as in big data applications, enact more assurance in service providers. Cloud Service provider uses individual cloud providers that work collaboratively to form a federation of clouds. Federated cloud aims to reduce the risk of data intrusion, the loss of service availability and to ensure data integrity. In FCIDM used these models and tools to manage resource permissions with less fuss and high automation.

According to Gartner Research [3], the security discipline of Identity and Access Management (FIAM) by the right individuals to access the right resources at the right times for the right reasons. Nowadays, the process of managing identities in heterogeneous technology environments are getting more complex and remains a challenge regarding privacy issues [4].

To address privacy there are some identity management tools with proper peculiarities [5] [6] using various mechanisms. Leakage of user data, the distribution of unnecessary attributes, and a lack of control on the dissemination of personal data are happened in cloud environments [7–11]. Cloud providers must protect the privacy of users, entities, data, and information throughout their lifecycle.

In this paper Section 2 shows the Related Work, Section 3 explains privacy in identity management in the federated cloud. Section 4 explains about federated cloud identity management concepts, Section 5 presents FCIDM Technologies**,** Section 6 opens a discussion and proposes future research directions on key privacy requirements, identifying research challenges.

## II. Related Work

As in [3] Federation is the ability of multiple independent resources to act like a single resource. Cloud computing itself is a federation of resources, so the many assets, identities, configurations and other details of a cloud computing solution must be federated to make cloud computing practical. Also many issues like trust, Identity access management, Signing-in has been discussed regarding Federation of clouds.

Buyya *et al.,* [13] suggests a cloud federation oriented, just-in-time, opportunistic and scalable application services provisioning environment called InterCloud. In paper by Subashini and Kavitha [14], has discussed cloud computing has significant implications for the privacy of personal information as well as for the confidentiality of business and governmental information. In the case of federated clouds this becomes more serious issue that is to be addressed. For computation exchange of data between clouds in federation is necessary so both privacy and integrity of data should be considered.

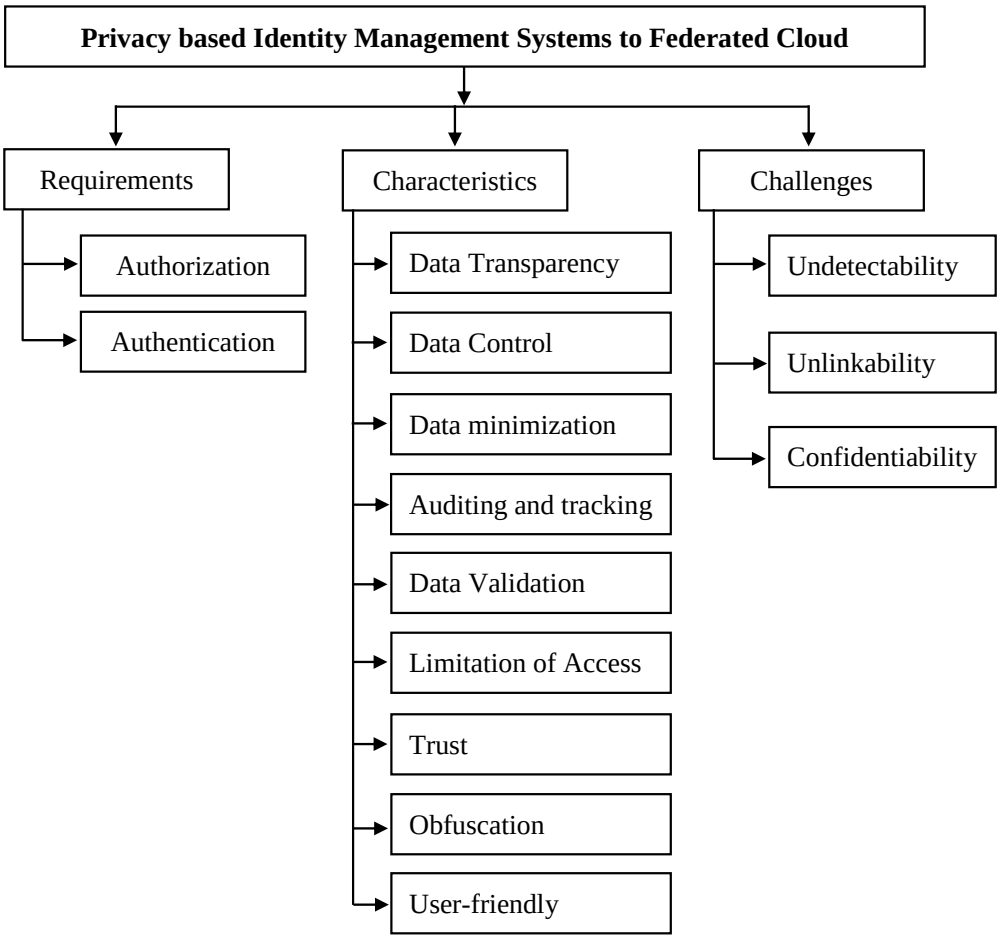
In [15] Mohammed Abdullatif *et al.*, has discussed about data privacy in DAAS. In their paper Shamir's secret sharing mechanism has been used for securing data, so that individual data values will not be visible to the service provider and provider can recover data in case of data loss.

Hence we have proposed different mechanisms and tools to address privacy in identity management system in federated cloud. Our research work founds a relationship among identity management needs, privacy features, approaches, and challenges in the federated cloud environment. Major privacy challenges are identified in this paper and possible solutions are also presented at end of our research.

## III. Privacy In Identity Management In The Federated Cloud

Privacy is the right to be let alone. It refers to the ability of individuals to protect information about themselves (their own information) [11] [16] [17]. The interchange of sensitive information is powerful in large-scale scenarios of cloud computing, with several federations, where multiple Identity Providers (IdP) and Service Providers (SP) work together to provide services. So, identity management system should provide models and privacy mechanisms so as to manage the sensitive data of its users.

**Figure – 1:** *Privacy based Identity Management Systems to Federated Cloud*

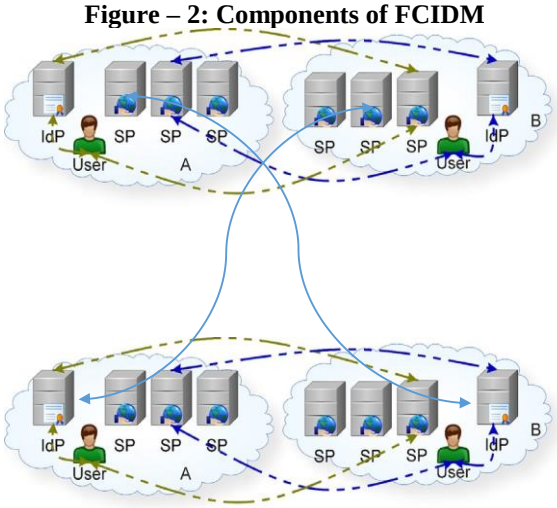



## IV. Federated Cloud Identity Management Concepts

Cloud computing helps the federation and collaboration among independent business organization while gaining the services and resources from different Cloud environments. Identity management services is the basis for all the other services. In Federated Cloud Identity Services an agreement is prepared between group of trusted service providers to share their resources and services in demand basis.

Cloud subscribers are able to use the same identity credentials for acquiring access to the set of shared Cloud resources in Federated Identity Management systems. It brings in economic benefits along with the convenience to the participating organizations and its network subscribers. It provides many security and privacy concerns to the identity information. But still many problems occur in privacy strategies. Interoperability is one of the challenging area in the federated Cloud computing environment. Hence we talk about the privacy in federated cloud identity management in this article.

**Figure – 2: Components of FCIDM**




Federated Cloud Identity management (FCIDM) is the process of creating, managing, and using identities, and the infrastructure that provides support for these processes. In FCIDM each person or application is identified by a user credential (*e.g.,* Name, Date of Birth, Mobile Number, etc.), which represents a set of attributes, issued by a reliable source [18] [19]. An application could have information such as a URL, identifier, and public key in its credential [4, 20–22].

### 4.1. Requirements of Federated Cloud Identity Management Systems

Federated Cloud need IDM systems that can cooperate dynamically with each other by interchanging data and resources in a flexible way. Identity Providers (IdP) and Service Providers (SP) are the two main components in FCIDM systems. User credentials can be created and validated in identity providers to be used by different cloud service providers.

- **Authentication:** Before allowing any one to access the system authentication proves is done. It is the process of identity verification, to ensure that the individual is the right person or not. Authentication is the proof of ownership of the identification attributes and it is the basic and necessary step before to start process. The authentication process is performed in the IdP. It stores the attributes of users. After authentication only it sends a token or credential to the service provider.
- **Authorization:** To deny or allow access in the system, this authorization process take place. After receiving the credential from Multiple Identity Provider (IdP), the Service Provider (SP) should use authorization policies to decide on the release of the requested resource.
- **Single Sign-On/Sign-Off:** The advantage of using an FCIDM system is the ability to use Single Sign-On (SSO) and Single Sign-Off. In SSO process is from a single authentication in the home domain or IdP, the user is able to use other services in the same domain or circle of trust. Similarly, in Single Sign Off or Single Logout Process means the possibility of closing all sessions of access.

### 4.2 Privacy Challenges in Federated Cloud IDM

Without the interference of third parties, the person has to control his/her personal data from the collection, storage, manipulation, and dissemination. [23-27]

According to the United Nations in its Declaration of Fundamental Rights, Article twelve [28], privacy is a fundamental right, everyone is entitled to privacy, and it must be guaranteed by legal means. Moreover, the human rights council [28] declares that the rights that every citizen has in the offline environment should be extended to the digital environment.

Protecting the privacy of any computer system is a technical challenge. In a cloud environment this challenge is complicated by the distributed nature of clouds and possible lack of consumer awareness about where the data is stored and who has access to such data [29]. There should be the possibility of self-management of privacy due to legal claims so that the person can be responsible for his or her information [30].

Privacy is also a challenge in IdM. Since IdM systems share sensible identity attributes, called Personally Identifiable Information (PII) [18] [19] [31]. In IdM there is much concern about privacy, data protection, compliance with the rules, volume of information exchanged between different domains, dynamic exchange of information, execution of policies, consent from users, and control of credentials [32]. It is essential to comply with current legislation regarding the identity lifecycle while maintaining privacy in the exchange of data between different environments and providers.

The challenges that meets identity management are shown below [33],

- **Undetectability:** To hide transactions performed by the user and preventing the detection of the user actions in a given system.
- **Unlinkability:** To hide the connection between user identities and history of transactions (*e.g.*, subjects, messages, events, actions [34].
- **Confidentiality**: To enable the users control over the dissemination of their attributes.

These properties are related with one another because they are concerned with defining actions or methods to deal with the parties involved in access to a range of private and sensitive data.

Privacy in the cloud environment must also involve mechanisms or specific characteristics that consider the subtleties of the environment. If privacy cannot be guaranteed in the cloud, users may not be ready to use these services [35].

### 4.3 Privacy Characteristics in Federated Cloud IDM

A study of the characteristics sought to consider important points to safeguard the privacy of sensitive user data used in identity management, considering the dynamic exchange of information in the elastic environment of cloud computing. The following characteristics shows that the important for identity management in the cloud with an emphasis on user privacy.

- **Data Transparency:** It refers to the notification about the use of attributes or profiles and create awareness by detailing information about the lifecycle of disseminated data. It gives notice to individuals about data collection, usage, disclosure and updating Personally Identifiable Information (PII).
- **Data Controllability:** It is the effective control over their personal data especially in IT holders. Data Selection means that the user chooses what data will be available to access the resource. When the users consent, they agree to the use of their data using predefined profiles of the system.
- **Data Minimization:** User should forward only the data needed to access the resource. Limited spread of data within the cloud should be allowed, especially in the access control process. Selected data must be disseminated. The systems can allow the users participation in the dissemination of attributes.
- **Auditing and Tracking:** It means dynamically trace the footprints of data and users, using history and location of identity and linked attributes. It helps to identify misuse and privacy cracks between different identity and service providers. Laws require identification and punishment of those involved in case of unauthorized access or malicious use of the data accessed.
- **Data Validation:** It refers to checking and validation of attributes. It is essential to ensure the truthfulness of personally identifiable information, confirming and validating the data to be preserved individuals' privacy. Data may or may not be externally checked. It determines the degree of validity of the data. The system can implement a verification about the veracity of the information. If not validated, the system assumes confidence in data, considering the existence of a reliable federation environment;
- **Limitation of Access:** Only authorized persons should have access to personal data to ensure the confidentiality of data. The limitation of use can be accomplished by policies and obligations. A policy is a set of rules that can represent the reason or intention for using the data. An obligation is a directive that must be carried out before or after access is approved.
- **User-friendly:** It refers to the easiness of using applications with privacy features. This system should provide sufficient help and simple interfaces to be used by less experienced users as well.
- **Trust:** In cloud environment, it is necessary to create ways to keep or ensure the confidence among parties. Current studies seek to improve mechanisms to evaluate providers dynamically through risk and/or reputation measures.
- **Obfuscation:** It refers to the use of techniques of anonymity or pseudonyms, important in federations where users have applications of different contexts. Users do not send their attributes to the provider and because of that, for example, potentially identifiable information such as the users IP address or location cannot be revealed. Different approaches are proposed in the literature using nicknames (anonymity or pseudonyms).

**Table - 1:** *FCIDM Privacy Features Versus Properties*

| Properties / Features | Confidentiability | Undetectability | Unlinkability |
|---|---|---|---|
| Data Transparency | ✓ | | |
| Data Control | | ✓ | ✓ |
| Data minimization | ✓ | ✓ | |
| Data Validation | ✓ | | |
| Auditing and Tracking | | ✓ | |
| Trust | ✓ | ✓ | ✓ |
| Limitation of Access | ✓ | ✓ | |
| Obfuscation | ✓ | | ✓ |
| User-Friendly | ✓ | ✓ | ✓ |

## V. FCIDM Technologies

**SAML (Security Assertion Markup Language), JSON (JavaScript Object Notation)** are some of the tools used for creating federated cloud (or also called cloud federation) environments to exchange data.

SAML is an open standard for swapping authentication and authorization data between and IdP (Identity Provider) and SP (Service Provider). It is an XML based markup language specification and states standard authentication, attribute, and authorization decision for security assertions. The Head (or a user), the Identity Provider and Service Provider are the three roles of SAML. The user requests a service from the service provider. The Service Providers requests and obtains an authentication statements from the identity provider. On the basis of this, the service provider can make an access control decision whether to perform some service for the connected user. Before sending, the Identity provider request some data to the user or head (*i.e.*, username and password). In SAML, one IdP may provide assertions to many SP and one SP may rely on and trust assertions from many independent IdP.

JSON is a lightweight data-interchange format and it is easy for humans to read and write. It is also easy for machines to parse and generate. It is a text format used for exchanging data between a browser and a server.

The OpenID Connect is open source, has a standard protocol, has a native support for dynamic associations, and as it uses a lightweight message format (JSON) delivered via the OAuth 2.0 protocol to suit web browser based and native mobile applications. OpenID connect is the new emerging standard for single sign-on and identity provision on the internet. OpenID connect allows clients of all types such as Web-based, mobile and Javascript clients.

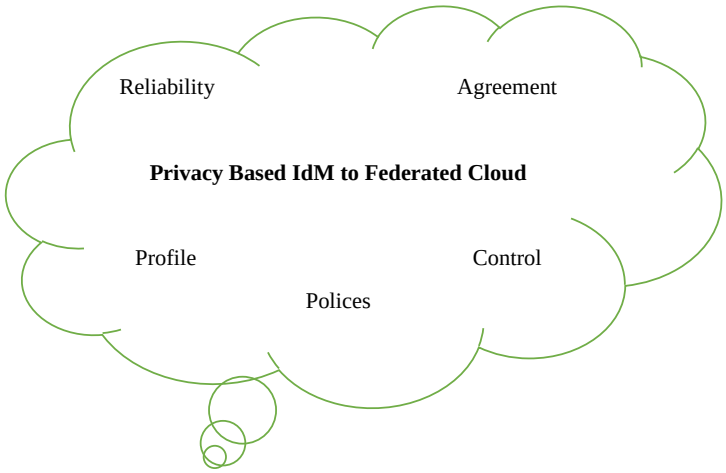
SAML federations are usually static, *i.e.*, metadata should be placed in defined directories and some configuration data must be shared among IdPs and SPs in order to establish the federation. These metadata describe participants of the federation and are cryptographically signed by the federation manager [23] [37].

OpenID Connect does not have the same type of federation as Shibboleth [6]. While Shibboleth requires a strict notion of affiliation to an institution or group, OpenID Connect allows dynamic client registration when clients can register themselves automatically at a provider. Unfortunately, it means a provider will trust any client that asks and provides it with user information. Because of this facility, a dynamic federation can easily be defined [38]. There is work in progress to build OpenID Connect federations that use federation operators to build the identity trust [39].

## VI. Future Discussions

The intense exchange of data between different cloud providers can create problems due to legal compliance and the trust of users. Hence, we try to plan a new anonymous algorithm for cloud computing services. Data only sent to the network after processing by the algorithm so that the data are spread with identifiers that do not expose the true identity of the user. It is more flexible to use and more efficient than other mechanisms.

With the rise of cloud computing, managing thousands of users and resources needs some challenges and techniques to protect user data. These challenges shown in Fig. 3 tends to fill the outstanding gaps regarding the privacy features of Federated Cloud IdM. Reliability is very useful in Identity Management. The risk of access by devices such as mobile device, tablet, etc. or means of access is an important for a provider.




An agreement for Identity Management system is an important task which can assist organization in establishing a federation. Our idea is to have an agreement of privacy options among identity and service providers in order to perform the federation process.

A standard profile is a set of sensitive data or general attributes exchanged among interacting parties. This predefined standard profile to assist users in data dissemination and access control decisions. Different standard of interaction profiles is named as anonymous, pseudonym, partial attributes and total attributes are our research work.

A new mechanism to enable Grained control in the dissemination of personal attributes in different applications contexts are needed. Hence mechanisms should be improved to guarantee the validation of user attributes and the granular dispatch of attributes according to the application context.

Policy definition can be a valuable mechanism to increase and ensure privacy. The various policy languages are EAPL (Enterprise Privacy Authorization), XACML (eXtensible Access Control Markup Language) and P2U(purpose-to-use). The application of policies in access control meets transparency requirements and control over the scattered data in the cloud among different service providers.

## VII. Conclusions

This paper explained a survey about privacy aspects in the cloud, describing characteristics in identity management in federated cloud and tool used in federated cloud IdM systems. The future research work addresses three issues.1. The lack of PII (Personally Identifiable information), 2. The lack of models to assist users in data dissemination during the interaction, 3. The lack of user preference guarantees on the SP side.

## References


[1] R. Buyya, C.S. Yeo, S. Venugopal, *"Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, in: High Performance Computing and Communications",* 2008. HPCC '08. 10th IEEE International Conference on, 2008, pp. 5–13, DOI: 10.1109/HPCC.2008.172.

[2] J. Werner, G.A. Geronimo, C.B. Westphall, F.L. Koch, R. Freitas, C.M. Westphall, "Environment, Services and Network Management for Green Clouds", *CLEI Electron. J., 15 (2)*, (2012). http://www.clei.org/cleiej/paper.php?id=238.

[3] https://auth0.com/learn/cloud-identity-access-management/

[4] M. Hansen, A. Schwartz, A. Cooper, "Privacy and Identity Management", *IEEE Secur. Privacy 6 (2)*, (2008) 38–45, DOI: 10.1109/MSP.2008.41.

[5] O. Foundation, "Openid Connect", 2016, Retrieved: June, 2016, http://openid.net/

[6] Shibboleth, "What's shibboleth? 2016", Retrieved: July, 2016, https://shibboleth.net/about/

[7] J. Werner, C.M. Westphall, R. Weingärtner, G.A. Geronimo, C.B. Westphall, *"An approach to IdM with privacy in the cloud, in: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)"*, 2015 IEEE International Conference on, 2015, pp. 168–175, DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.26.

[8] T. Orawiwattanakul, K. Yamaji, M. Nakamura, T. Kataoka, N. Sonehara, *"User-Controlled Privacy Protection with Attribute-Filter Mechanism for a Federated SSO Environment Using Shibboleth, in: P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)"*, 2010 International Conference on, 2010, pp. 243–249, doi: 10.1109/3PGCIC.2010.40.

[9] D.W. Chadwick, K. Fatema, "A Privacy Preserving Authorisation System for the Cloud", *J. Comput. Syst. Sci. 78 (5)*, (2012) 1359–1373, doi: 10.1016/j.jcss.2011.12. 019. {JCSS} SpecialIssue: Cloud Computing 2011.

[10] R. Sanchez, F. Almenares, P. Arias, D. Diaz-Sanchez, A. Marin, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", *IEEE Trans. Consum. Electron. 58 (1)*, (2012) 95–103, DOI: 10.1109/TCE.2012.6170060.

[11] S. Gürses, J.M. del Alamo, "Privacy Engineering: Shaping an Emerging Field of Research and Practice", *IEEE Secur. Privacy 14 (2)*, (2016) 40–46, DOI: 10.1109/MSP.2016.37.

[12] S. Aruljothy, A. Arvind, B. Sudharsanan & K. Vignesh Babu, "Efficient Rekeying System for Secure Multicast with Differing Membership Period Portable Client", *International Journal of Advanced Scientific Research & Development (IJASRD), 2 (1),* 2015, 101 - 108.

[13] Rajkumar Buyya, Rajiv Ranjan, and Rodrigo N. Calheiros, *"InterCloud: Utility-Oriented Federation of Cloud Computing Environments for Scaling of Application Services"*, ICA3PP,2010, Part I, LNCS 6081, Springer, 2010, pp. 13–31. DOI: 10.1007/978-3-642-13119-6_2.

[14] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing", *Journal of Network and Computer Applications*, (2011), pp. 1-11. DOI: 10.1016/j.jnca.2010.07.006

[15] M. A. AlZain and E. Pardede, *"Using Multi Shares for Ensuring Privacy in Database-as-a-Service"*, 44th Hawaii, International Conference on System Sciences (HICSS), 2011, pp 1-9. DOI: 10.1109/HICSS.2011.478.

[16] C.E. Landwehr, "Computer Security", *Int. J. Inf. Secur. 1 (1)*, (2001) 3–13, DOI: 10.1007/s102070100003.

[17] I. Goldberg, D. Wagner, E. Brewer, *"Privacy-Enhancing Technologies for the Internet"*, in: Compcon '97. Proceedings, IEEE, 1997, pp. 103–109, DOI: 10.1109/CMPCON.1997.584680.

[18] ISO/IEC 24760-1: 2011, *"Information Technology–Security Techniques – A Framework for Identity Management"*, Technical Report, 2011a.

[19] ISO/IEC 29100:2011, *"Information Technology–Security Techniques–Privacy Framework"*, Technical Report, 2011b.

[20] A. Josang, S. Pope, *"User Centric Identity Management"*, in: AusCERT Asia Pacific Information Technology, 2005, pp. 1–13.

[21] A. Maheswari, R. Sanjana, S. Sowmiya, Sudhir Shenai & G. Prabhakaran, "An Efficient Cloud Security System Using Double Secret Key Decryption Process for Secure Cloud Environments", *International Journal of Advanced Scientific Research & Development (IJASRD), 3 (1),* 2016, 134 - 139.

[22] M. Hansen, P. Berlich, J. Camenisch, S. Clau, A. Pfitzmann, M. Waidner, "Privacy-Enhancing Identity Management", *Inf. Secur. Tech. Rep. 9 (1),* (2004) 35–44, DOI: 10.1016/S1363-4127(04)00014-740.

[23] S. Ferdous, R. Poet, "Managing Dynamic Identity Federations using Security Assertion Markup Language", *J. Theor. Appl. Electron. Commerce Res. 10,* (2015), 53–76. http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-18762015000200005&nrm=iso.

[24] B. Sangeetha, E. Saranya & G. Saranya, "A Novel Framework for Secure Sharing of Personal Health Records (PHR) in Cloud Computing", *International Journal of Advanced Scientific Research & Development (IJASRD), 2 (2),* 2015, 08 - 14.

[25] A.F. Westin, *"How the Public Views Privacy and Health Research, Results of a National Survey Commissioned by the Institute of Medicine Committee on Health Research and the Privacy of Health Information: The HIPPA Privacy Rule"*, 2007. 2011–1107.
[26] C. Diaz, S. Gürses, *"Understanding the Landscape of Privacy Technologies"*, in: Extended Abstract of Invited Talk in Proceedings of the Information Security Summit, 2012, pp. 58–63.
[27] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L.B. Othmane, L. Lilien, *"An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing"*, in: Reliable Distributed Systems, 2010 29th IEEE Symposium on, 2010, pp. 177–183, DOI: 10.1109/SRDS.2010.28.
[28] U. Nations, *"The Promotion, Protection and Enjoyment of Human Rights on the Internet (2012)"*. Retrieved: February, 2016, https://daccess-ods.un.org/TMP/208261.31105423.html.
[29] M. L. Badger, T. Grance, R. Patt-Corner, J. M. Voas, *"Cloud Computing Synopsis and Recommendations"*, Technical Report, Gaithersburg, MD, United States, 2012. Retrieved: February, 2016.
[30] D. J. Solove, "Privacy self-Management and the Consent Dilemma", *Harvard Law Rev. 126 (7)*, (2013) 1880–1903.
[31] E. McCallister, T. Grance, K. Scarfone, *"Guide to Protecting the Confidentiality of Personally Identifiable Information"*, Technical Report, 2010. Retrieved: February, 2016.
[32] J. Jensen, *"Federated Identity Management Challenges"*, in: Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, 2012, pp. 230– 235, DOI: 10.1109/ARES.2012.68.
[33] E. Birrell, F.B. Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization", *IEEE Secur. Privacy 11 (5)*, (2013) 36–48, DOI: 10.1109/MSP.2013.114.
[34] A. Pfitzmann, M. Hansen, *"Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology"*, Technical Report, 2010. Retrieved: February, 2016, https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html.
[35] S. D. C. di Vimercati, S. Foresti, P. Samarati, *"Managing and Accessing Data in the Cloud: Privacy Risks and Approaches"*, in: 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2012, pp. 1–9, DOI: 10.1109/CRISIS.2012.6378956.
[36] R. Jayasudha, A. Nandini, R. Naseema Praveen & G. Prabhakaran, "Cloud Based Inventory Control System for Ration Shop Versatile Management", *International Journal of Advanced Scientific Research & Development (IJASRD), 2 (1)*, 2015, 41 - 47.
[37] D.R.D. Santos, T.J. Nascimento, C.M. Westphall, M.A.P. Leandro, C.B. Westphall, "Privacy-Preserving Identity Federations in the Cloud: A Proof of Concept", *Int. J. Secur. Netw. 9 (1)*, (2014) 1–11, DOI: 10.1504/IJSN.2014.059328.
[38] L.M. Bodnar, C.M. Westphall, J. Werner, C.B. Westphall, *"Towards Privacy in Identity Management Dynamic Federations"*, in: ICN 2016, The Fifteenth International Conference on Networks, IARIA, Lisbon, Portugal, 2016, pp. 40–45.
[39] R. Hedberg, R. Gulliksson, M.B. Jones, J. Bradley, *"Openid Connect Federation 1.0 - Draft 01"*, 2016, https://openid.net/specs/openid-connect-federation-1_0.html.

A. Mary Odilya Teena et al., Federated Cloud Identity Management: A Study on Privacy Tactics, Tools and Technologies." IOSR Journal of Computer Engineering (IOSR-JCE), vol. 19, no. 6, 2017, pp. 34-40