Towards a Privacy Mechanism for Preventing Malicious Collusion of Multiple Service Providers (SPs) on the Cloud

Maria M. Abur[1], Sahalu B. Junaidu[1], Sani Danjuma[2], Syafri Arlis[3], Rajab Ritonga[4], and Tutut Herawan[5,6(✉)]

[1] Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria
{mmaburl,abuyusra}@gmail.com
[2] Department of Computer Science, Northwest University, Kano, Nigeria
sani_danjuma@yahoo.com
[3] Universitas Putra Indonesia (YPTK), Padang, Indonesia
syafri_arlis@upiyptk.ac.id
[4] Universitas Prof Dr Moestopo (Beragama), Jakarta, Indonesia
rajab.ritonga@dsn.moestopo.ac.id
[5] Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia
tutut@uty.ac.id
[6] AMCS Research Center, Yogyakarta, Indonesia

Abstract. Cloud computing is cyberspace computing, where systems, packages, data and other required services (such as appliances, development platforms, servers, storage and virtual desktops) are dispensed. It has generated a very significant interest in educational, industrial and business set-ups due to its many benefits. However, cloud computing is still in its early stage of development and is faced with many difficulties. Researchers have shown that security issues are the major concerns that have prevented the wide adoption of cloud computing. One of the security issues is privacy which is about securing the personal identifiable information (PII) or attributes of users on the cloud. Although researches for addressing privacy on the cloud exist (uApprove, uApprove.JP and Template Data Dissemination (TDD)), users' PII remains susceptible as existing researches lack efficient control of user's attribute of sensitive data on the cloud. Similarly, users are endangered to malicious service providers (SPs) that may connive to expose a user's identity in a cloud scenario. This paper provides a mechanism to solve the malicious SP collusion problem and control the release of user's attribute in the cloud environment. This will require the use of policies on the SPs, where SPs are only allowed to request for attributes that are needed only to process a user's service at any point in time. This can be achieved using a combination of Kerberos ticket concept, encryption and timestamp on the attribute to be released to SPs from the identity provider (IdP), thereby helping to control attributes given to SPs for processing the release of services to users for one-time usage by the SPs and not kept for future use by them. Thus, replay attacks and blocking other SPs from accessing them are prevented. Hence, any malicious intention of assembling users' attributes by other SPs to harm them is defeated.

V. Bhateja et al. (eds.), *Information Systems Design and Intelligent Applications*, Advances in Intelligent Systems and Computing 672,
https://doi.org/10.1007/978-981-10-7512-4_72

Keywords: Cloud computing · Attributes · Privacy · Service providers and control

1 Introduction

Cloud computing is cyberspace computing, where systems, packages, data and other required services (such as appliances, development platforms, servers, storage and virtual desktops) are dispensed. It is based on pay before accessing services involved in distributing hosted facilities over the Web. Cloud computing has generated a very significant interest in educational, industrial and business set-ups due to its many gains [1–3]. However, cloud computing is in its early stage of development and is faced with many difficulties [4–8]. Researches in [9–11] have shown that security issues are the major concerns that have prevented the wide adoption of cloud computing. One of the security issues is privacy which is about securing the PII of users on the cloud [12–14]. Although researches for addressing privacy on the cloud exist: Switch (2010) added a Plugin solution called uApprove—to provide awareness of data disclosure when accessing some resource on the cloud. Orawiwattanakul et al. in [15] extended uApprove to uApprove.JP. Furthermore, Weingatner et al. in [12] added a lightweight extension on uApprove.JP called Template Data Dissemination (TDD) to tackle some privacy issues on IdP and to assist users on PII disclosure. However, users' PII remains vulnerable as existing researches require enhancements to be effective and efficient.

The general problems of cloud computing are: privacy, performance and interoperability. Privacy issues include: lack of control of user's attribute, data breaches, leaks and loss of data. uApprove, uApprove.JP and Temple Data Dissemination (TDD) were used in addressing these challenges. Despite all these solutions, the cloud is still without adequate protection. Users are endangered to malicious service providers (SPs) that may connive to expose a user's identity in a cloud atmosphere. For instance, if we have ten service providers (SPs) and each of them have partial information about a user, what measure can one put in place to prevent these SPs from colluding to profile users' attributes?

In Fig. 1, the relationship between users, SP and IdP on the cloud environment is indicated. Although researches so far have worked on securing the privacy of users' attributes on the IdPs end, the other end (i.e. from IdP to SP) does not protect privacy by itself; users are still vulnerable to malicious SPs that may collude to profile a user identity in a federated environment, Weingartner et al. in [12]. However, there are still issues to be dealt with from the SP side; this paper proposes a mechanism to control the SP, thereby preventing the collusion that may occur due to malicious activities in the cloud that cause harm to users.

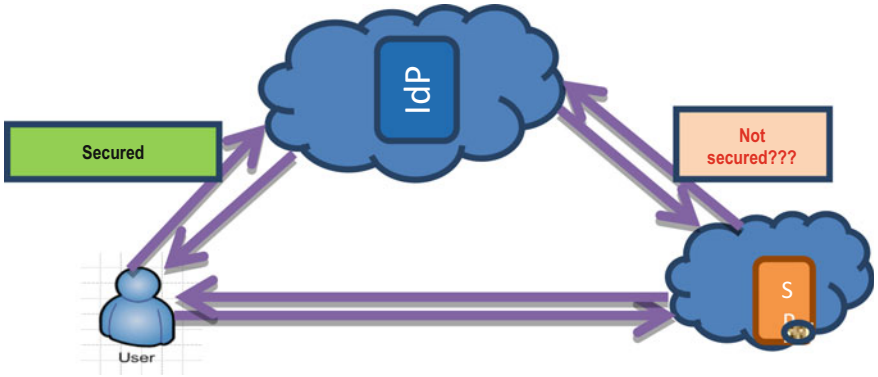

Fig. 1. Relationship between user, SP and IdP

The rest of the paper is organized as follows: Sect. 2 presents a short review on existing works connected to cloud computing privacy. Section 3 presents cloud computing service models. Section 4 presents cloud computing deployment models. Section 5 presents challenges of cloud computing. Section 6 presents our proposed solution. Lastly, Sect. 7 concludes the paper.

2 Related Work

Orawiwattanakul et al. worked on user-controlled privacy protection with attribute-filter mechanism for a federated SSO environment using Shibboleth. Their proposal tackled the lack of control on PII disclosure in cloud federations in [15]. Their proposal added uApprove.JP, an extension of Shibboleth framework, that would permit users to make their choice from all optional attributes which one they wish to reveal to the SP that is being accessed. As a limitation, there is a flaw in the case of releasing user's attribute (mandatory/optional) to the SP in order to get their consent before they can access the service. An intruder can study the part through which these attributes flow and pretend to be a user, then capture the attributes and try to utilize them in order to cause harm to the stored attribute. Hence, privacy is compromised.

Sanchez et al. in [16] worked on "Enhancing Privacy and dynamic federation in IdM for consumer Cloud Computing". They proposed a new reputation protocol and implemented Enhanced Client Profile (ECP). It weighs the reputation of entities in a federation in order to support data disclosure [16]. It gives users room for checking what is being done with their data, and on that note, they could decrease or increase the reputation provided. As a limitation, their model could not demonstrate how privacy is handled in a real-life scenario [16]. Their research requires validation of the most favourable values of the parameters of the reputation model. However, their model is vulnerable to some attacks, thereby lacking some measures to fully guarantee users' privacy.

Weingartner et al. in [12] worked on "Enhancing Privacy on Identity Provider". They proposed a model for addressing some security and privacy issue called Template

Data Dissemination (TDD) with cryptography keys. Their solution is a lightweight extension on top of Shibboleth identity provider and its uApprove.JP Plugin [12]. They also attempted the problem of lack of users' awareness to their data (i.e. PII) when it is been disseminated. As a limitation, there are still issues to be dealt with at the service provider side, such as means to control attributes that were released from an IdP to a SP. Their solution is inefficient, as far as user's privacy is concern, since users' attributes are still at risk of malicious SPs that may plot to expose user's identity in a federated cloud atmosphere. Hence, the need for investigating means of enforcing user's privacy in service providers (SP).

In the light of the above, this paper provides a mechanism to solve the malicious SP collusion problem and then control the release of user's attribute in the cloud environment.

3 Cloud Computing Service Models

Cloud computing service models consist of Cloud Clients, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [17]. As cloud computing is advancing, different vendors offer clouds that have different services associated with them. The collection of services offered put in another set of definitions is called the service model Mell et al. in [17]. Usually, cloud service model takes the following form: XaaS, where X is anything. Many cloud service models have been described here using this format. They have different strengths and are appropriate for different users and business purposes. The Service Models are presented below based on the definition of the National Institute of Standard and Technology (NIST), Mell et al. in [17].

a. Software-as-a-Service (SaaS): The consumer uses the provider's applications, which are hosted in the cloud [17].
b. Platform-as-a-Service (PaaS): Consumers deploy their own applications (home-grown or acquired) into the cloud infrastructure. Programming languages and application development tools used must be supported by the provider [17].
c. Infrastructure-as-a-Service (IaaS): Consumers are able to provide storage, network, processing and deploying resources, and controlling arbitrary software, ranging from applications to system software [17].

Following the service model, clients have different levels of control over the infrastructure management. In the SaaS model, control is normally narrowed to user-specific application configuration settings. PaaS provides control over the deployed applications and perhaps application hosting environment configurations. IaaS provides control over operating systems, storage and deployed applications [18]. Figure 2 shows the cloud computing service models.

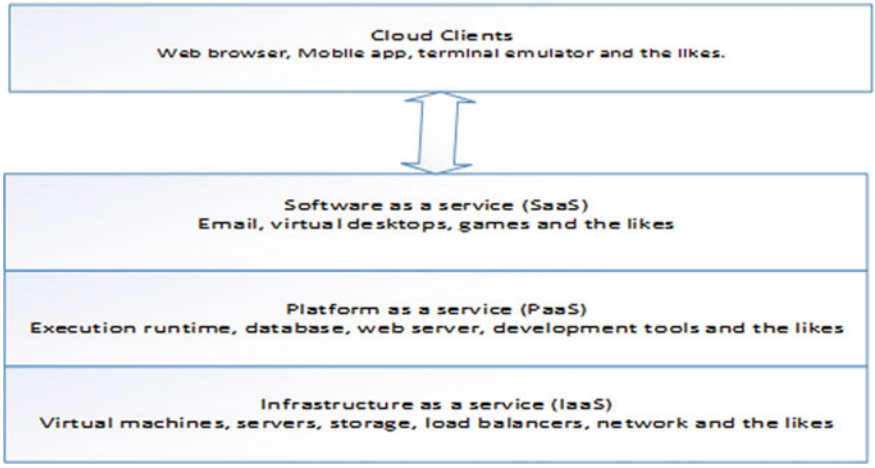

Fig. 2. Cloud computing service model [18]

4 Cloud Computing Deployment Models [17–19]

Another relevant concept of cloud computing is the cloud deployment models. The most recognized are the following four (public, private, community and hybrid), but it is important to note that other models can be developed from them.

a. Public: Resources are usually available to the general public via the Internet. In this case, "public" characterizes the scope of interface accessibility, whether or not resource usage is charged. This environment emphasizes the benefits of scalability, rationalization and operational simplicity (since the environment is hosted by a third party, i.e. the cloud provider). The main issue is security, since the environment is shared and managed by the cloud provider, and accordingly, the consumer/subscriber has little control over it.
b. Private: Resources are accessible within a private organization. This environment emphasizes the benefits of scalability, integration and optimization of hardware investments. The main issue is operational complexity, since the environment is hosted and managed by internal resources.
c. Community: Resources on this model are shared by several organizations with a common mission. It may be managed by one of the organizations or a third party [17].
d. Hybrid: This model combines the techniques of public and private clouds. A private cloud can have its local infrastructure supplemented by computer capacity from a public cloud [18, 19]. The benefits and challenges of the hybrid cloud is a combination of the items above.

In this research, the private cloud is intended to be used to actualize our solution.

5 Challenges of Cloud Computing

Cloud computing is still in its infancy and is faced with many challenges, and users are doubtful about its genuineness. Following an investigation conducted by International Data Corporation (IDC) in 2009 [20]. The most important challenges that prevented cloud computing from being widely adopted are: security challenge (which ranked highest on the survey), trust, performance issues, cloud interoperability issue, costing model, charging and service-level agreement (SLA). Figure 3 shows the cloud computing challenges based on the IDC findings:

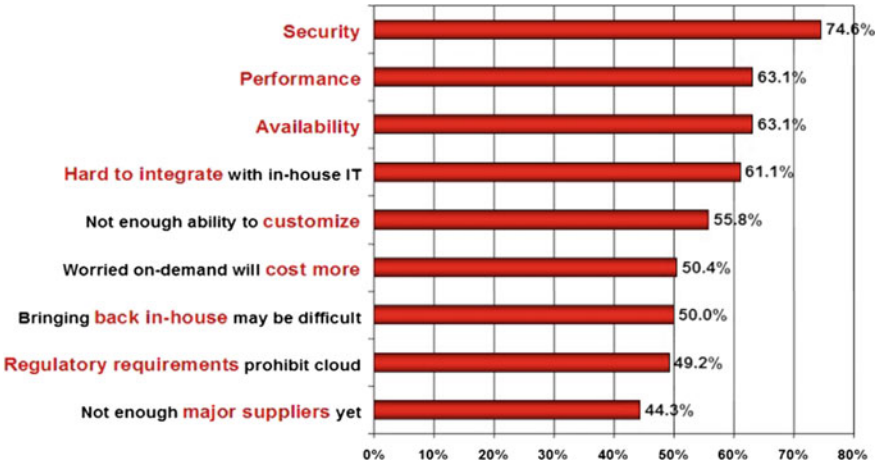

Fig. 3. Challenges to cloud computing adoption [20]

According to Rima et al. in [9], Zhou et al. in [10] and Chen and Zhao in [11], there are a lot of challenges that hamper the effectiveness and efficiency of these services such as security issues (authentication and identity management issues, privacy, trust, data confidentiality and integrity issues, non-repudiation, numerous threats, data leakages, vulnerabilities and the likes). These security issues among others are the biggest barrier to the adoption of cloud computing.

Similarly, in 2013, the Cloud Security Alliance (CSA) [21] put together a list of the nine most prevalent and serious security threats in cloud computing, known as the "*Notorious Nine: Cloud Computing Threats*". They are data breaches, data loss, account or service traffic hijacking, insecure interfaces and APIs, denial of service, malicious insiders, cloud abuse, insufficient due to diligence and shared technology [21]. Furthermore, researches have been done on the security challenges hindering the acceptance of cloud computing and these challenges directly affect the deployment models, service models and networks. They include lack of data security such as data leakage, authentication and identity management and consequent problems, malicious

attacks, backup and storage, shared technological issues [22], service hijacking, virtualized machine (VM) hopping, VM mobility, VM denial of service, browser security, SQL injection attack, flooding attacks, locks and the likes. These challenges are further categorized into various groups by Parekh et al. in [22] as shown in Fig. 4. Some other security threats are phishing, password cracking and botnets.

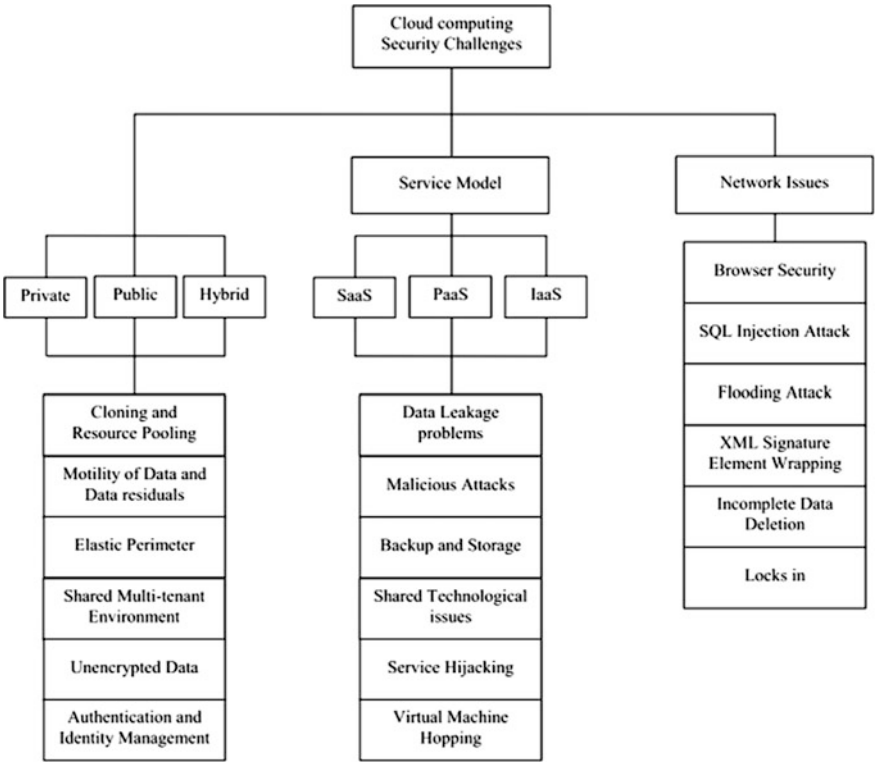

Fig. 4. Classification of security challenges [22]

6 Proposed Solution

Considering the fact that no IdP can stop or reduce the number of attributes required by an SP to process the release of resources for a user, in this paper, the following solutions were proposed below:

a. Let *n* represent number of SPs i.e. SP_1, SP_2, SP_3… SP*n* and *n* number of resources, R requested by users are represented as (R_1, R_2, R_3… R*n*) as indicated in Fig. 5.
b. We propose to use policies on all SPs, where each SP shall be allowed to request for attributes that are needed only to process a user's service at any point of time.

c. Then, we shall introduce two Kerberos tickets: T_1 for the IdP and T_2 for SP. T_1 is encrypted with IdP secret key and T_2 with the SP's secret key, the requested attributes with timestamp and a session key K_{US} for both IdP and SP. The IdP, opens T_1 extracts the IdP's secret key and sends messages to the SP; containing Ticket T_2 with the SP's secret key, the requested attributes with Timestamp and a session key, K_{US}. The SP on receiving the ticket opens the message, uses the secret key to decrypt information and releases resource to the user. At the expiration of the timestamp, the session key, K_{US}, attributes in the possession of the SPs within that timestamp becomes worthless, rendering them invalid. Even if the SP may want to play smart by decrypting the ticket and want to share user's attributes before releasing resources to the user, anything contained in the ticket is rendered invalid to anyone who receives them.

Consequently, this is to ensure that all attributes given to SPs for processing or releasing services to users are within a given timestamp and allow one-time usage, thereby preventing any malicious intention to expose users' attributes by SPs.

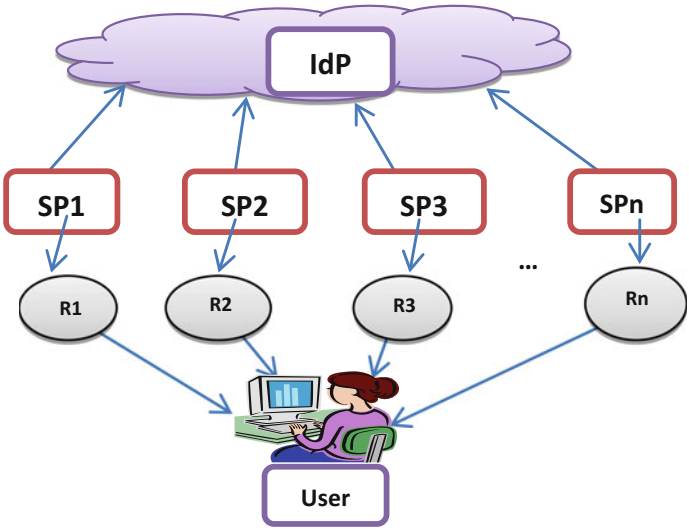

Fig. 5. Illustration the flow of resources from SPs to the users

7 Conclusion

Cloud computing is cyberspace computing, where systems, packages, data and other required services (such as appliances, development platforms, servers, storage and virtual desktops) are dispensed. It is still in its early stage of development and is faced with many difficulties. Cloud computing is characterized by security challenges, one of which is privacy concern. This includes lack of control of user's attributes, data breaches and loss of data. Researches based on Shibboleth have added uApprove,

uApprove.JP and Template Data Dissemination in tackling privacy issues; nevertheless, users' personal identifiable information remains vulnerable as existing researches lack efficient control of user's attribute of sensitive data on the cloud. Similarly, users are endangered to malicious service providers (SPs) that may connive to expose a user's identity in a cloud scenario. This paper provides a mechanism to solve the malicious SP collusion problem and control the release of user's attribute in the cloud environment. This will require the use of policies on the SPs, where SPs are only allowed to request for attributes that are needed only to process a user's resource at any point of time.

Acknowledgements. The work of Syafri Arlis is supported by Universitas Putra Indonesia YPTK under Research Grant No 094/UPI-YPTK/RG/IX/2016. The work of Tutut Herawan is supported by Universitas Teknologi Yogyakarta under Research Grant No vote O7/UTY-R/SK/0/X/2013.

References

1. Fauzi, A.A.C., Noraziah, A., Herawan, T. and Zin, N.M., 2012, March. On cloud computing security issues. In *Asian Conference on Intelligent Information and Database Systems* (pp. 560–569). Springer Berlin Heidelberg.
2. Noraziah, A., Azila, A., Fauzi, C., Herawan, T. and Zailani, A., 2015. Binary Vote Assignment on Cloud Quorum Algorithm for Fragmented MyGRANTS Database Replication. *Wulfenia Journal*, *22*(1), pp. 375–386.
3. Fauzi, C., Azila, A., Noraziah, A., Mohd, W.M.B.W., Amer, A. and Herawan, T., 2014. Managing Fragmented Database Replication for Mygrants Using Binary Vote Assignment on Cloud Quorum. In *Applied Mechanics and Materials* (Vol. 490, pp. 1342–1346). Trans Tech Publications.
4. Khan, N., Noraziah, A., Ismail, E.I., Deris, M.M. and Herawan, T., 2012a. Cloud computing: Analysis of various platforms. *International Journal of E-Entrepreneurship and Innovation (IJEEI)*, *3*(2), pp. 51–59.
5. Khan, N., Noraziah, A., Herawan, T., Ismail, E.I. and Inayat, Z., 2012b, September. Cloud Computing: Architecture for Efficient Provision of Services. In *NBiS* (pp. 18–23).
6. Khan, N., Noraziah, A., Herawan, T. and Deris, M.M., 2012c, September. Cloud computing: analysis of various services. In *International Conference on Information Computing and Applications* (pp. 397–404). Springer Berlin Heidelberg.
7. Khan, N., Noraziah, A. and Herawan, T., 2012d, September. A cloud architecture with an efficient scheduling technique. In *International Conference on Information Computing and Applications* (pp. 381–388). Springer Berlin Heidelberg.
8. Khan, N., Ahmad, N., Herawan, T. and Inayat, Z., 2012e. Cloud Computing: Locally Sub-Clouds instead of Globally One Cloud. *International Journal of Cloud Applications and Computing (IJCAC)*, *2*(3), 68–85.
9. Rima B. P., Choi E., & Lumb I. (2009): A Taxonomy and Survey of Cloud Computing Systems. In *Proc. of the 5Th International Joint Conference on INCIMS and IDC, NCM'09*, IEEE Press, 44–51.
10. Zhou M., Zhang R., Xie W., Quian W. & Zhou A., (2010) Security and Privacy in cloud: Survey. In *Proc. Of the 6Th International Conference on Semantics, Knowledge and Grids*, IEEE Press, 105–112.

11. Chen D. & Zhao H. (2012): Data Security and Privacy Protection Issues in Cloud Computing. In *Proc. of the 1st International conference on Computer Science and Electronics Engineering*, 647–651.
12. Weingartner, R. (2014) "Dissemination control of data Sensitive environment in Federated Systems". *M.Sc. Computer Science Thesis*, Department of Informatics and Statistics, Federal University of Santa Catarina, Brazil.
13. Betg´e-Brezetz S., Kamga G. B., Ghorbel M., and Dupont M.P., "Privacy control in the cloud based on multilevel policy enforcement," In *Proceedings of 2012 IEEE 1st International Conference on Cloud Networking* (CLOUDNET), IEEE Press 2012, 167–169.
14. Betge-Brezetz S., Kamga G. B., Dupont M. P. & Guesmi A. (2013). End-to-end Privacy Policy Enforcement in Cloud Infrastructure," In *Proceedings of IEEE 2nd International Conference Cloud Networking* (CloudNet 2013), 25–32.
15. Orawiwattanakul T., Yamaji K., Nakamura M., Kataoka T. & Sonehara N. (2010): "User-controlled privacy protection with attribute-filther mechanism for a federated SSO environment using Shibboleth," in *IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (3PGCIC), IEEE Press, 243–249.
16. Sanchez R., Almenares F., Arias P., D´ıaz-S´anchez D. & Marın A., (2012). "Enhancing Privacy and dynamic federation in IdM for consumer Cloud Computing," *IEEE Transactions on Consumer Electronics*, 58(1), 95–103.
17. Mell P. & Grance T. 2011. "The NIST Definition of Cloud Computing," *NIST Special Publication* 800-145 (draft), 1–7.
18. Abur, M. M., Adewale O. S., Junaidu S.B., (2015): Cloud Computing Challenges: A review on Security and Privacy issues. *Proceedings of the ACM International Conference on Computer Science Research and Innovations* (CoSRI), 89–92.
19. Pearson S. 2011 "Taking account of privacy when designing cloud computing services", HP Laboratories, Tech. Rep. HPL- 2009-54, 2009, http://www.hpl.hp.com/techreports/2009/HPL2009-54.pdf.retrieved.
20. Gens F. (2009). "New IDC IT Cloud Services Survey: Top Benefits and Challenges", IDC eXchange, Available: http://blogs.idc.com/ie/?pp730.
21. Cloud Security Alliance (2013): The Nine Notorious Threats. Top threats working group.
22. Parekh D. H. and Sridaran R., (2013): "An Analysis of Security Challenges in Cloud Computing". *International Journal of Advanced Computer Science and Applications*, Vol. 4, No.1 pp. 38–46.