ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

A Review on Data Security and Privacy Issues in Cloud Computing

Akanksha Agrawal, Dr. Nitesh Dubey

Research Scholar, Global Nature Care Sanghtan's Group of Institutions, Jabalpur, India

Deputy Director, Global Nature Care Sanghtan's Group of Institutions, Jabalpur, India

ABSTRACT : Cloud computing has gain considerable research interest, due to its vast range of services. The major issue in cloud computing are its data security and privacy. The term security has multiple facets such as confidentiality, availability and integrity. A perfect security solution must ensure all the security parameters effectively. This review paper focuses on the security of data. This paper intends to review various security and privacy related issues and the possible solutions in literature. The challenges associated with the security and privacy related issues are also discussed.

KEYWORDS: Cloud computing, security, privacy, confidentiality, integrity, availability.

I. INTRODUCTION

Cloud computing is an emerging computing paradigm that focuses on services at any time basis. This technology provides services based on demand for a nominal charge. The service models in cloud can be classified into Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

SaaS provides software services to the users with respect to their demand. The software services can be exploited by the users provided they have internet connection and the services can be accessed by the web browser. PaaS is the kind of services that are needed by the end users, so as to solve some application level problems. IaaS is the type of service which intends to improve the performance of the system by boosting the memory space or computational power.

Some of the major advantages of cloud computing are services on demand, charge for the consumed services, easy maintenance, elasticity, distributed storage of services etc., This makes sense that the cloud computing provides services to the clients, whenever the services are requested and the cloud users are accounted for a charge with respect to the consumed services, as cloud computing follows the principle of pay-as-you-go model.

The two major services provided by the cloud are data and computational services. Data services are more popular in cloud computing, as all the memory and data management overheads are tackled by the cloud service providers. On the other hand, all sorts of computational tasks can be accomplished by the computational services, provided the cloud user has got network connection.

Cloud computing is a boon for mid-scale industries, as it incurs lesser charge which when compared to owning licensed versions of softwares. The cloud can be categorized into three kinds, with respect to the access type. They are public, private and hybrid cloud.

Public cloud is the cloud whose services can be exploited by the public users, without any restrictions. Private cloud is another type of cloud and this type of cloud is accessible to limited number of users alone. For instance, such type of clouds is usually owned by a private organization for effective data storage and other related purposes. Hybrid cloud is the combination of both the public and private clouds and the data is accessible with respect to the user privileges.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Owing to the benefits of cloud computing, there is an increased exploitation of this innovative technology and this paves way for the significant research interest. However, there are several issues to be addressed. The major issue to be focused is the security. The security in cloud computing has several facets such as data confidentiality, integrity, availability and privacy and is illustrated in Fig 1.

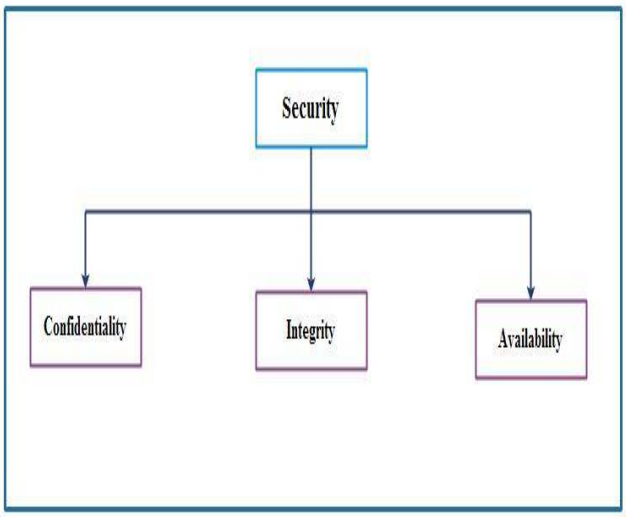

Fig 1 Facets of Security

Data confidentiality is the assurance that the intended users alone can gain access to the data. Data integrity can be ensured by combating against modification or deletion of data. Availability of the data must be ensured by all the cloud systems, such that the required data is available to the cloud users at all time. The privacy of data can be achieved by the selective view of data, such that the data owner of the data cannot be predicted [1, 2]. The security issues and the open challenges associated with it are presented in [3].

Achieving data security in cloud computing is not a simple task, as it has multiple facets. This is because of the distributed storage of data. Many research solutions to address the security issues in cloud computing have been proposed in the literature. However, still there are users who feel reluctant to exploit cloud storage only because of this issue.

This article intends to study the different facets of cloud data security such as data confidentiality, integrity, availability and privacy. The possible solutions for it in the literature are also discussed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

II. DATA CONFIDENTIALITY

can search over the encrypted data in the cloud and rank the search results.

TABLE 1: DATA CONFIDENTIALITY

Literature Reference	Employed Technique	Pros	Cons
8	Lightweight security mechanism by data encryption	Simplicity	Key count Cost
9	Encrypted data searching	Relevant results through ranking	Time complexity
10	Security as a Service	Increased degree of security	Computational complexity Time complexity
11	Layer based security	Follows divide and conquer strategy	-
12	Concealment of data	Misleads attackers	Voluminous data

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

Data confidentiality is one of the major issues, when outsourcing highly sensitive data to the cloud. Data confidentiality makes sense that the confidential data must be inaccessible to the unintended users. Data confidentiality can be ensured by strict access control policies. There must be a policy such that the unintended users must not infer anything from the information being stored in the cloud database.

The best possible solution to ensure data confidentiality is data encryption. However, the serious issue associated with encryption is the management of keys. It is impossible to expect the data owners to manage keys. The cloud service providers are expected to proceed with key management and this is not preferable. Homomorphic encryption is proposed by Rivest et.al. in the year [4]. The resultant data after encryption is observed to be consistent and the data confidentiality is ensured by this sort of encryption.

A fully homomorphic encryption methodology is proposed in [5]. The major drawback of this method is its computational complexity and cost. In [6], multiple encryption algorithms such as RSA, Triple DES and random number generator are clubbed together, in order to provide high security.

RSA is an efficient algorithm, which can provide secured communication by means of digital signature. Triple DES is employed for achieving block encryption. The security issues and different encryption algorithms in cloud computing are presented in [7]. However, homomorphic encryption is difficult and the research interest is then focussed on encrypted search.

The work proposed in [8] presented a lightweight security mechanism to encrypt data through standard manipulations such as transposition, substitution, folding and shifting. However, the key count is directly proportional to the computational complexity and the cost. In [9], a privacy preserving multi-keyword rank based search is presented that
In [10], security is provided as the service for clouds. The security is achieved by decomposing the data into several chunks and each chunk is encrypted. Every encrypted chunk is distributed to different databases and by this way, this work withstands several attacks. A security scheme with layered approach is proposed in [11]. This work possesses three layers, where the first layer is responsible for authentication, second layer deals with the process of encryption and the last layer is responsible for data decryption.

In the work proposed in [12], concealment of data is employed to ensure data confidentiality. This work intends to append fake data with the original data, so as to increase the volume of the data and to confuse the attackers. Table 1 summarizes all the aforementioned works to combat for preserving data confidentiality.

III. DATA INTEGRITY

Data integrity is the most important facet of security in cloud computing. Data integrity aims to safeguard data from alteration or deletion by illegitimate users. Data integrity can be effortlessly accomplished in centralized systems. However, it is a complex task to be achieved in distributed cloud computing environment.

Most of the adversaries aim to delete or modify the cloud data, which is a very serious issue. The integrity of the data cannot be checked by downloading it from the server, as it would be complex and expensive. Data integrity can be ensured by several strategies and they are Provable Data Possession (PDP), Proof of Retrievability (PoR) and Third Party Auditing (TPA) and are depicted in Fig 2.

A. Provable Data Possession (PDP)

The data integrity in the cloud database can be verified by employing PDP [13-16]. The working principle of PDP is that initially the original data to be outsourced is manipulated during the setup phase, so as to produce metadata for the client side. Whenever the data owner feels to check the integrity of the data, the data owner challenges the cloud server. The cloud server responds to the data owner.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

The integrity of the data is verified by the data owner by clubbing the response from the server and the metadata. The main advantages of PDP are its minimal computational and storage overhead. The drawback of PDP is that PDP does not suit dynamic data, which makes sense that the data, once outsourced to the cloud cannot be updated.

3.1.1 Scalable PDP

The drawbacks of PDP are overcome by the scalable PDP [15]. Scalable PDP employs symmetric key encryption in the place of public key encryption. This minimizes the computational overhead; however, this kind of PDP does not support public verification because of the inclusion of symmetric key encryption. Scalable PDP supports dynamic data. The drawbacks of scalable PDP are the challenges and responses are calculated in advance. Besides this, the count of updates is also limited.

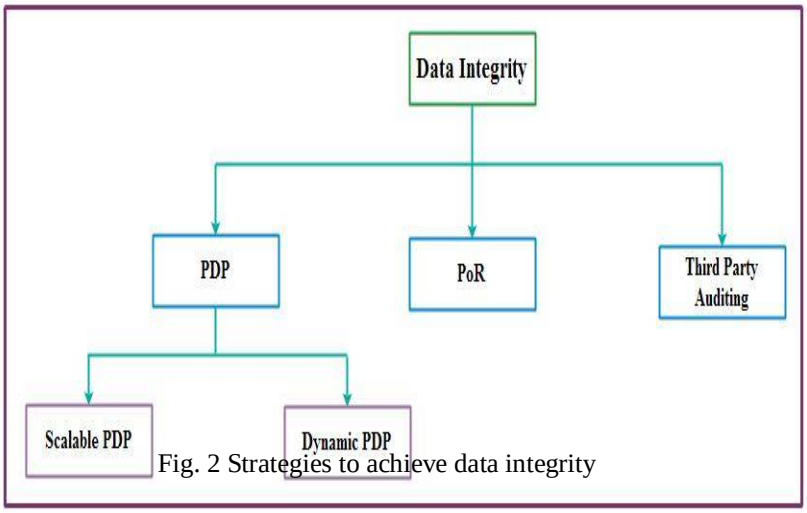

Fig. 2 Strategies to achieve data integrity

3.1.2 Dynamic PDP

The major goal of dynamic PDP is to support dynamic operations without any limits. Some of the dynamic operations are append, modify, delete and insert records. The dynamic PDP involves three important operations namely PrepareUpdate, PerformUpdate and VerifyUpdate [16].

Initially, the data owner raises an update request (PrepareUpdate), which includes the nature of update that is needed to be performed. The server responds to the data owner's request by PerformUpdate and allows the existing file to get updated. Meanwhile, the server provides the proof of update to the data owner, such that the behaviour of the server during the process of updation can be determined by the data owner. Table 2 presents the overview of the literature, which addresses the data integrity related issues.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

TABLE 2 DATA INTEGRITY

Literature Reference	Employed Technique	Pros	Cons
13, 14	Provable Data Possession (PDP)	Minimal computational cost Minimal storage overhead	Doesn't suit dynamic data
15	Scalable PDP	Supports dynamic data	Advance fixation of challenges and responses Limited count of updates
16	Dynamic PDP	Supports dynamic data without any limits for updates	Time complexity
17	Proof of Retrievability (PoR)	Supports dynamic data operations Resilient to reset attacks	-
18	Third Party Auditing	Data audit takes place without local copy of data	Trust related issues
19	Third Party Auditing	Addressed trust related issues to some extent by random masking	Trust related issues
20	Third Party Auditing	Minimal time consumption	-
22	Public auditing mechanism	Introduction of user revocation	Computational complexity
23	Public auditing	Minimal time consumption	Computational complexity
24	Privacy preserving public auditing	Less complexity	Security issues
25	Public integrity auditing scheme	Increased security	Computational complexity
26	Integrity auditing scheme	High error detection probability Efficient user revocation	Data management issues

B. Proof of Retrievability (PoR)

The idea behind this scheme is that in case, if the data is modified or deleted, then the sentinel values may get deleted or damaged. This unfavorable scenario results in the inability to produce the complete proof for the original data, by the server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

In such case, the data owner can come to a conclusion that the original data is corrupted by the server. However, PoR is also restricted to static data similar to that of PDP [14].

The work proposed in [17] comes up with OPoR, which includes a cloud storage server and an audit server. This work supports dynamic data operations and is secure against reset attacks.

C. Third Party Auditing Technique

In all the aforementioned techniques, the data owners check the integrity of the data. However, the third party auditing technique allows a third party inside the system, so as to check for the data integrity.

In [18], a third party auditor is employed to verify the integrity of the data in the cloud. A third party auditor should be able to audit the data effectively without any local copy of the data. In [19] a public homomorphic authenticator is employed to check for the data integrity. When the concept of random masking is clubbed with homomorphic authenticator, then the third party auditor cannot infer anything from the cloud data, while auditing.

A secure cloud storage system is proposed in [20], which supports privacy preserving public auditing. The TPA can perform parallel audits in an effective manner. In [21], the authors review and analyse the security issues associated with the cloud computing. This article also studies the problem that occurs due to the incorporation of TPA.

A novel public auditing mechanism is presented in [22]. The integrity of the shared data is ensured by taking the user revocation into account. This work allows the cloud to re-sign the blocks during user revocation, on behalf of the users by exploiting the concept of proxy re-signatures. In [23], a privacy preserving mechanism that can support public auditing is proposed. This work computes verification metadata by ring signatures, so as to check the correctness of the data. This work can carry out several audits at a time.

In [24], a secure cloud storage scheme that supports privacy preserving public auditing is presented. This work utilizes the public key based homomorphic authenticator with random masking. A public integrity auditing scheme is proposed in [25], with secured group user revocation on the basis of vector commitment and verifier local revocation group signature.

In [26], a novel integrity auditing scheme that focuses on multi-user modification, public auditing, high error detection probability and efficient user revocation is presented.

IV. DATA AVAILABILITY

Data availability must be focused cent percent since, the service created for users must be available to them, round the clock. However, there are certain cases in which the data availability cannot be assured. Some of the possible scenarios associated with data availability are natural calamities such as floods, earthquake, fire, hard disk damage and network failures.

In such unavoidable situations, there is a need to know how far the outsourced data can be utilized, verified or recovered by the data owners. The data owners are very much concerned about the data storage in the servers across the boundary of the country, as the cloud service provider is liable to local laws of the country. All the security measures being practised by the cloud service provider must be open to the data owners.

For instance, the Service Level Agreement (SLA) of Amazon clearly states that the cloud service may not be available all the time. In addition to this, it is stated that the cloud user's web service can expire at anytime, in case of the violation of user's storage policy. The SLA clearly states that the Amazon cannot take responsibility for any damage or failure of the service. Additionally, the companies which prefer to safeguard their possessions can proceed with backups or can lend support from multiple cloud service providers [27, 28].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

In [29], it is cited that 45 percent of the user's data has been lost in LinkUp, owing to a system administrator error. Thus, it is the responsibility of the data owner to safeguard the data and to ensure data availability.

V. DATA PRIVACY

Privacy of data is another important concern, while outsourcing data to the cloud service provider. For instance, all the personal information about the customers along with the business logic is outsourced to the cloud service provider. In such case, the data owner worries about the data privacy, as the outsourced data may be misused. Data privacy must be given much importance and is insisted on [30-32].

The privacy of the data is affected when the illegitimate users infer something from the cloud data. In [18], the privacy of the data is preserved by means of Oblivious RAM (ORAM). ORAM traverses through multiple copies of data and the original visiting intention of the users are hidden. This technology is very popular in software protection and privacy preservation.

The problems associated with privacy vary with respect to the cloud [19, 33, 34]. The most serious privacy threats to cloud storage are the misuse of the data and averting attacks. The attackers try hard to misuse the cloud data and to destroy it.

Cloud storage employs de-duplication, which makes sense that the same data is stored once, but shared by many users. This functionality reduces the storage space and cost involved. However, the adversary can gain access to the data with the hash code. This paves way for the leakage of the sensitive data. In order to overcome with this issue, proof of ownership is employed in [35]. The work presented in [36] focuses on data leakage and privacy issues in cloud computing.

VI. CONCLUSION

The security and privacy issues in cloud computing are discussed in this paper. Multiple facets of security such as data integrity, confidentiality and availability are also discussed along with the solutions in the literature. This article strives to boost up the research ideas and can serve as a stepping stone for future research.

REFERENCES

[1] A. Avi˘zienis, J. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.
[2] J. Krumm, "A survey of computational location privacy," Personal and Ubiquitous Computing, vol. 13, no. 6, pp. 391–399, 2009.
[3] Deepak Puthal, B. P. S. Sahoo, Sambit Mishra, and Satyabrata Swain, "Cloud Computing Features, Issues and Challenges: A Big Picture", International Conference on Computational Intelligence & Networks, pp. 116-123, 2015.
[4] R. L. Rivest, L. Adleman, andM. L.Dertouzos, "On data banks and privacy homomorphisms," Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978.
[5] C. Gentry, A fully homomorphic encryption scheme [Ph.D. thesis], Stanford University, 2009.
[6] A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security," Journal of Engineering Science Technology, vol. 2, pp. 737–741, 2012.
[7] R. Arora, A. Parashar, and C. C. I. Transforming, "Secure user data in cloud computing using encryption algorithms," International Journal of Engineering Research and Applications, vol. 3, no. 4, pp. 1922–1926, 2013.
[8] D. Manivannan and R. Sujarani, "Light weight and secure database encryption using tsfs algorithm," in Proceedings of the International Conference on Computing Communication and Networking Technologies (ICCCNT '10), pp. 1–7, IEEE, 2010.
[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," IEEE Transactions on Parallel andDistributed Systems, vol. 25, no. 1, pp. 222–233, 2014.
[10] C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data," in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.
[11] E. M.Mohamed, H. S. Abdelkader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Proceedings of the 8th International Conference on Informatics and Systems (INFOS'12), pp. CC-12–CC-17, IEEE, 2012.
[12] C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, security and data concealment," in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11), pp. 424–431, Kerkyra, Greece, July 2011.
[13] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," In ACM

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 6, June 2017

CCS, pages 598-609, 2007.
[14] A. Juels and B. S. Kaliski, "PORs: Proofs of retrievability for large files," In ACM CCS, pages 584-597, 2007.
[15] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," SecureComm, 2008.
[16] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Proc. 16th ACM conference on Computer and communications security, 2009, pp. 213-222.
[17] Jin Li, Xiao Tan, Xiaofeng Chen, Duncan S. Wong, and Fatos Xhafa, "OPoR: Enabling Proof of Retrievability in Cloud Computing with Resource-Constrained Devices", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 3, NO. 2, pp. 195-205, 2015.
[18] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," IEEE INFOCOM 2010, San Diego, CA, March 2010.
[19] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. ESORICS'09, Saint Malo, France, Sep. 2009.
[20] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, pp. 362-375, 2013.
[21] Ling Li, Lin Xu, Jing Li, Changchun Zhang, "Study on the Third-party Audit in Cloud Storage Service", International Conference on Cloud and Service Computing, 2011.
[22] Boyang Wang, Baochun Li and Hui Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 8, NO. 1, pp. 92-106, 2015.
[23] Boyang Wang, Baochun Li and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, pp.43-56, 2014.
[24] Pritee Parwekar, Mayuri Saxena, Prakash Kumar, Sakshi Saxena, "Public Auditing: Cloud Data Storage", 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence), pp. 169-173, 2014.
[25] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma, "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE Transactions on Computers, 2015.
[26] Jiawei Yuan and Shucheng Yu, "Public Integrity Auditing for Dynamic Data Sharing With Multiuser Modification", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 8, pp. 1717 - 1726, 2015.
[27] Amazon, Amazon Web Services. Web services licensing agreement, Accessed in May-2011 (2006).
[28] S. L. Garfinkel, An evaluation of amazon's grid computing services: EC2, S3, and SQS, http://simson.net/clips/academic/2007.Harvard.S3.pdf, 2007, pp. 1-15.
[29] C. Cachin, I. Keidar and A. Shraer, Trusting the cloud, ACM SIGACT News, 40 (2009), pp. 81-86.
[30] J. Liu, Y. Xiao, S. Li, W. Liang, C. L. P. Chen, "Cyber Security and Privacy Issues in Smart Grids," IEEE Commun. Surveys Tuts., DOI: 10.1109/SURV.2011.122111.00145, in press.
[31] Y. Xiao, X. Shen, B. Sun, and L. Cai, "Security and Privacy in RFID and Applications in Telemedicine," IEEE Commun. Mag., Vol. 44. No. 4, Apr. 2006, pp. 64-72.
[32] H. Chen, Y. Xiao, X. Hong, F. Hu, J. Xie, "A Survey of Anonymity in Wireless Communication Systems," (Wiley Journal) Security and Communication Networks, Vol. 2 No. 5, Sept./Oct., 2009, pp. 427-444.
[33] W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy Aware Data Storage and Processing in Cloud Computing Architectures," IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 711-716.
[34] A. Haeberlen. "A Case for the Accountable Cloud," 3rd ACM SIGOPS International Workshop on Large-Scale Distributed Systems and Middleware (LADIS '09), Big Sky, MT, October 2009
[35] C. Wang and Y. Zhou, "A Collaborative Monitoring Mechanism for Making a Multitenant Platform Accountable." Hotcloud 2010.
[36] W. Wei, J. Du, T. Yu, and X. Gu, "SecureMR: A Service Integrity Assurance Framework for MapReduce," Proc. 2009 Annual Computer Security Applications Conference, 2009, pp. 73-82.