Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2016, 9, 347-360
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Extending Auditing Models to Correspond with Clients' Needs in Cloud Environments

Rizik M. H. Al-Sayyed[1], Esam Y. Al-Nsour[2], Laith M. Al-Omari[3]

[1]Department of Business Information Technology, King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
[2]Department of Computer Science, King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
[3]Department of Computer Information Systems, King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
Email: r.alsayyed@ju.edu.jo, esamnsour@yahoo.com, laith.m.omari@gmail.com

How to cite this paper: Al-Sayyed, R.M.H., Al-Nsour, E.Y. and Al-Omari, L.M. (2016) Extending Auditing Models to Correspond with Clients' Needs in Cloud Environments. *Int. J. Communications, Network and System Sciences*, **9**, 347-360.
http://dx.doi.org/10.4236/ijcns.2016.99031

Received: July 29, 2016
Accepted: September 11, 2016
Published: September 14, 2016

Abstract

The user control over the life cycle of data is of an extreme importance in clouds in order to determine whether the service provider adheres to the client's pre-specified needs in the contract between them or not, significant clients concerns raise on some aspects like social, location and the laws to which the data are subject to. The problem is even magnified more with the lack of transparency by Cloud Service Providers (CSPs). Auditing and compliance enforcement introduce different set of challenges in cloud computing that are not yet resolved. In this paper, a conducted questionnaire showed that the data owners have real concerns about not just the secrecy and integrity of their data in cloud environment, but also for spatial, temporal, and legal issues related to their data especially for sensitive or personal data. The questionnaire results show the importance for the data owners to address mainly three major issues: Their ability to continue the work, the secrecy and integrity of their data, and the spatial, legal, temporal constraints related to their data. Although a good volume of work was dedicated for auditing in the literature, only little work was dedicated to the fulfillment of the contractual obligations of the CSPs. The paper contributes to knowledge by proposing an extension to the auditing models to include the fulfillment of contractual obligations aspects beside the important aspects of secrecy and integrity of client's data.

Keywords

Auditing, Public Audibility, Dynamic Data Auditing, Spatial Control, Temporal Control, Logging Data, Contractual Obligations

1. Introduction

Data outsourcing is economically attractive; however, data security, integrity, availability and many other concerns are elements or factors limiting the adoption of data outsourcing by potential users [1]. Many of these factors such as the data secrecy and availability were addressed in the field literature for long time. In addition, the emerging era of cloud computing imposes new challenges such as data monitoring [2]. Data monitoring could be based on real-time "intrusion detection" or on logging and offline auditing [3]. Many aspects of data outsourcing concerns in the cloud were addressed by researchers such as secrecy [4] [5], integrity [6] [7], availability [8] [9].

Data storage and manipulation outsourcing in clouds presents one of the biggest clients' concerns, especially for confidential data, concerns caused by the lack of transparency and limited user control; new attack channels for malicious users can exist due to the clouds multitenancy in conjunction with Virtual Machine Monitor (VMM) vulnerabilities [9]. Data monitoring techniques normally end up with logs that record the activities performed on data over time, such logs are the source for information that enable the process of verification of different aspects of auditing. A data-centric approach for control and auditing that applies across application and service boundaries seems appropriate for the demonstration of compliance with data regulations, and to understand how information is manipulated or generated [10].

Auditing is the systematic evaluation to measure the adherence of a system—such as a cloud service—to the established criteria and pre-specified set of policies imposed by the client on his/her data; auditor is the party that can conduct independent assessments of cloud services. The audit processes have to be highly regarded as it is the shortest way to gain users' trust and satisfaction. Standardization entities such as United States National Institute of Standards and Technology (NIST) have identified the protection of audit data integrity as one of the major concerns for the cloud technology [3].

Maintaining audit data integrity and security is challenging; for example, the CSP may try to hide any trails leading to uncover their responsibility about actions led to data misuse, losses, or security breaches [15]. It is very hard for the ordinary users—in most of the cases—to identify the reasons for such incidents under such circumstances [10] [11]. Therefore, a need for a frequent audit checking is needed to keep an eye on data, and to track the data movement to ensure only allowed flows exist [9], and ensure that the CSPs meet the requirements of the policy being enforced on data [10]. There are no existing internal mechanisms for cloud services users to enforce policy or reliably demonstrate compliance of policies, law, and regulations [12], furthermore, regarding the possibility of monitoring or audit, except for IBM and Microsoft Azure, service providers do not allow customers to hire a third party to perform such activities [13].

Being able to identify the cause of a security breach and the path that has been followed by an attacker is much more difficult in cloud environment than other environments. In addition, a cloud provider may subcontract a third party for some resources or a hardware supplier of poor-quality storage devices that result in loss of data. Traditional investigation methods based on digital forensics cannot be extended to a cloud, since resources are shared among a large user population and the traces of events related to a security incident may be wiped out due to the high rate of write operations on any storage media.

The importance of contractual obligations between tenants and cloud providers related to outsourcing data storage and manipulation were addressed in the literature in the form of guiding notes and recommendations [13]-[17]. In [18] authors stated that although the CSPs provide security services to the clients' data, there is a possibility of data leakage in cloud environment, users must make sure that the data moved into the cloud has not been leaked or modified by some unauthorized users, and to verify the security measures offered by the CSP.

The contractual terms between users and the CSPs make the user trust much worse; it usually places all responsibilities for data security on user's side [3]. Maintaining copies of the data outside the cloud is often unfeasible due to the sheer volume of data. If the only copy of the data is stored on the cloud, sensitive data is permanently lost when cloud data replication fails and is followed by a storage media failure. Because some of the data often includes proprietary or sensitive data, access to such information by third parties could have severe consequences.

Close attention should be paid to both; the security of storage servers, and to data in transit. Data usually is kept in storage for extended periods of time and so the concerns of unauthorized access to confidential information and data theft are more higher when data is in storage than while it is being processed, data exposure to threats during processing is for relatively short periods of time.

The user control over the life cycle of data is also of an extreme importance. How can a user determine whether data that should have been deleted is actually deleted? Even if it was deleted, there is no guarantee that the media was wiped and the next media user is not able to recover any confidential data. The problem is magnified when the CSPs rely on seamless backups to prevent accidental data loss since it is done without users' knowledge or approval. Such behavior may lead to data loss, accidental deletion, or data becomes accessible to an attacker.

In real world, two auditing schemes exist, private auditability and public auditability. In private auditability only the client or the data owner is allowed to check the different aspects of the stored data (*i.e.* secrecy, integrity, etc.), but it is not applicable for all clients and increases verification overhead of the user. Public auditability allows some entity privileged by the data owner to perform data verification check. This entity is called a Third Party Auditor (TPA). TPA has the expertise, capabilities, knowledge and professional skills that client normally does not have. TPAdoes frequent checks against data using different aspects and it reduces the client overhead; the client is no longer required to verify the integrity of the data at the server on his/her own. For data owners to have sufficient proficiency of trust; TPA may have only an encrypted format of the data, and are trusted by the data owner for auditing of the data and to ensure there is no data leakage and verify the compliance of the CSP with the contract.

Figure 1 [1] [19]shows public auditing scheme, in which, cloud users (clients) use the cloud storage provided by the CSP to outsource storage of their data, a TPA entity trusted by the client is entitled to keep checking on user's data periodically to verify data integrity. In the case of any unexpected results, both the client and the CSP are notified, a flow of security messages are exchanged between the three entities. In Figure 2 [11] [20] the public auditing scheme is extended to support public verification and dynamic data auditing, it also supports batch auditing in order to improve efficiency. To overcome data privacy issues, random mask technology is used to avoid TPA getting the client's data information knowledge on every verification process.

In [21], authors proposed a solution where the cloud provider generates audit logs, by which the cloud tenant is able to monitor the enforcement of data location-related regulation. Audit logs confidentiality and integrity should be ensured together with trusted time stamping. Cloud customers should be able to access the logs of every action including VMs' deployment; migrations; and shutdowns. The logs can also be used for the verification of the Cloud's utilization.

In [22], a software that is able to estimate the geolocation of itself, named VLOC, is introduced to verify the physical location of a VM on which the customer applications and data are stored. VLOC notifies users if the location is unauthorized. To get its

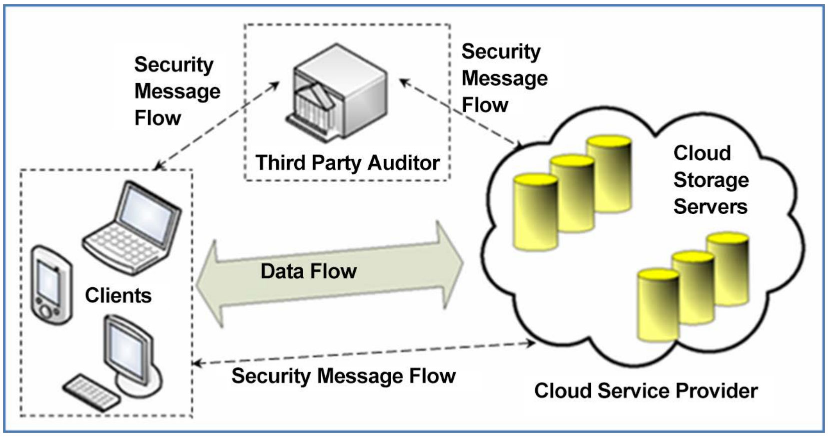

Figure 1. Public audibility in cloud data storage; source: [1].

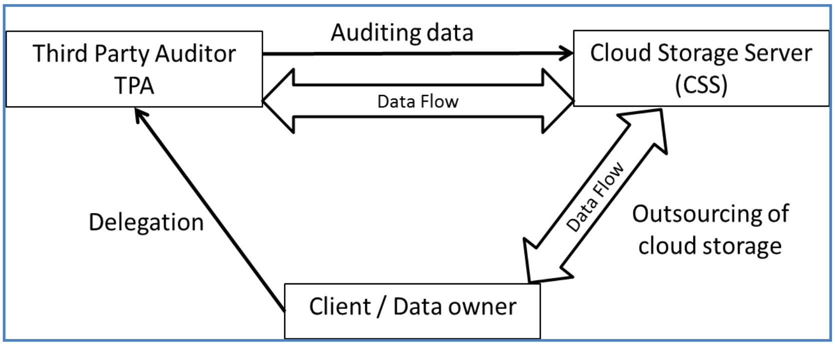

Figure 2. Public auditability in cloud data storage architecture which support dynamic data auditing; source: [11].

location, the software uses arbitrary web-servers as external landmarks, and employs network latency measurement for distance estimation. In the case of latency fluctuation, VLOC employs a machine learning technique in order to adapt.

Authors In [23] introduced a data driven usage control and provenance tracking approach, acts as a light-weight, transparent proxy between storage users and providers to enforce compliance constraints in cloud storage federation scenarios. The compliance constraints in their work were based on the enforcement of regulations, standards, and laws in cloud storage. Constraints were categorized into spatial, temporal, and qualitative restrictions on distribution and replication of data. The proxy intercepts all attempts to retrieve, store, or delete data from a cloud storage provider and forwards the corresponding events to the a policy decision point (PDP), which, based on previously deployed policies, decides on their execution and modification and finally sends its decision back to the proxy, the proxy then, based on the PDP's decision, either executes, modifies, or drops the event. The problems with such design are the high overhead on the cloud infrastructure, the possible single point of failure, the required implementation of the proxy at the CSP side, and it does not address data tracking once it leaves the environment of the federation service. In addition, no audit logs are generated.

In [10] [12] [24], authors introduced Information Flow Audit, as an approach for tracking information flows within cloud infrastructure. This builds upon CamFlow (Cambridge Flow Control Architecture), model for data-centric security in PaaS clouds. CamFlow enforces Information Flow Control (IFC) policy both intramachine at the kernel level, and inter-machine on message exchange to provide datacentric audit logs. Combining a continuously enforced data-centric security mechanism with meaningful audit enables tenants and providers to both meet and demonstrate compliance with their data management obligations. They outlined how IFC can be enforced in the cloud and discussed how audit data can be collected as an intrinsic part of IFC.

Up to our best knowledge, only little work was considering the users' concerns other than data security, integrity, and availability. Recent surveys on cloud computing security and auditing [25]-[28] didn't cover the concerns we talk about here, namely; spatial, temporal, and legal concerns. Although a little work was dedicated to enforce compliance of CSPs with data location regulations using auditing, the demonstration of the compliance of cloud providers to their contractual obligations is not yet convincing and more research is needed [29]. We are proposing an extension to the auditing models to include such concerns in order to increase the trust of data owners in the cloud environment.

The rest of this paper is organized as follows: Section 2 covers data owners' concerns limiting their adoption of clouds in their businesses, in the form of a questionnaire and discussion of results, the proposed extension to auditing models is presented in section 3, and finally; the conclusion along with future work direction is drawn in section 4.

2. Data Owners Concerns and Results Discussion

The cloud computing technology advantages are obvious; however, major challenges do exist such as the availability of services, data confidentiality, and auditability. Clouds in its different deployment and delivery models in Jordan are widely available along with good resources and infrastructure to support this technology, nevertheless, limited adoption among data owners. This limited adoption observation is common to both public and private sectors, but it is more obvious in the public sector.

In order to investigate data owners' concerns which are limiting their adoption of clouds in their businesses, we have conducted a questionnaire with thirteen questions (appendix A). Questions were selected to cover the area of data storage and manipulation outsourcing since it is, in our opinion, the major concerns producing and affecting clouds' area and adoption, such opinion were developed during multi discussions with groups of data owners in different sectors in Jordan. We intended to understand the reasons behind the major concerns limiting the shift towards the clouds, and how it can be tackled. The questionnaire also included questions for the data owners to express their additional important aspects related to the cloud environments.

The questioned sample was carefully chosen to represent: public sector, private sector, and the academic community. Total number of participants who answered the questionnaire is 23, all of them are from the information technology field, working with information systems of very large sizes, and have good background in cloud computing technologies. Persons from the academic field are researchers in the cloud computing technologies. It is worth saying that it wasn't an easy task to find a big number of typical participants to answer the questionnaire in order to get useful feedback because; as we indicated above; we carefully selected participants with the above mentioned knowledge and hence the small number; 23.

As shown in Appendix A, the questionnaire is composed of thirteen questions: eleven "Yes/No" questions and two fill in the blank questions. The results of eleven "Yes/No" questions of the questionnaire are summarized in Table 1, while Table 2 summarizes the two "fill in the blank" questions.

Table 1 represents the percentage results of the participants' answers (see Appendix B) with Yes or No to a pre-specified list of concerns if they were to move their data to the cloud. The concerns list included legal, spatial, and temporal aspects of data outsourcing. Notice that Table 1 shows participants' concerns listed in descending order (highest Yes percentage to lowest Yes percentage). Table 2 represents the recurrence of additional aspects or concerns as listed by the sample, which in their opinion may generate major concerns for a data owner when outsourcing data storage and manipulation (Q8 and Q9).

Results of the questionnaire showed that 100% of the sample believes that data outsourcing will generate major concerns (Q1); most of the concerns are directly related to data security, availability, and location. 91% of the sample believes that specifying a judiciary system and analyzing how information has flowed across the system are two major concerns (Q7 and Q11). Users' ability to control their data, and the lack of CSPs' transparency, were among the major concerns of data owners. About 83% of the sample believes that cloud multitenancy forms a new attach channel, it is important to

Table 1. Questionnaire results.

Question Text	Question No.	Yes %	No %
Data outsourcing in clouds presents a major concerns to data owners	1	100	0
Is it important to the data owner to specify the judiciary system that the data location may or may not belong to	7	91	9
Is it important for the data owner to be able to analyze how information has actually flowed across the system	11	91	9
Cloud multitenancy represent a new attack channels for malicious users	3	83	17
Is it important for the data owner to specify the period for permanent deletion of backup copies of their data	6	83	17
Is frequent Audit checking needed to keep an eye on data, and to track the data movement	10	83	18
Is it important to specify the physical storage location of the data	5	74	26
Concerns are caused by the lack of transparency and limited user control	2	65	35
Is it important to be able to track where, when, how and by whom data was generated or manipulated	4	65	35
Do you think that entities who own the data in general has the possibilities to perform the auditing for their data logs	12	61	41
Do you think that a trusted third party with needed qualifications may be a better option to audit the data logs for entities owning the outsourced data	13	61	41

Table 2. Important aspects for data owners in cloud environment

Aspect/ Concern	%	Aspect/ Concern	%	Aspect/ Concern	%
Availability	74	Security	57	Cost	30
Privacy	30	Data Location	22	Data Backup	17
Speed	9	Trust in CSP	9	Confidentiality	9
Stability	9	Encryption	9	Log security	9
Scalability	9	Data replication	9	Data Consistency	9
SLA	4	Risk Management	4	Change CSP	4
Compliance	4	Location	4	Good computer crime investigator	4

specify a permanent deletion period of backup copies, and it is important to keep an eye on the data by frequent auditing checks (Q3, Q6 and Q10). 74% of the sample thinks that it is important to specify physical storage location of data (Q5). 65% of the sample has concerns that there is lack of transparency and user control, in addition to the need to track all kind of data manipulation (Q2 and Q4). Frequent auditing and data tracking were considered very important by the data owners, however, having an external auditing entity (TPA) was considered important by only 61% of the sample, maybe this is due to a part of the sample background which usually take care of the auditing processes in their premises (Q12 and Q13).

As for Table 2 (Q8 and Q9), we notice that the availability aspect constitutes 74% of the concerns, security constitutes 57% of the concerns, while cost and privacy share the same percentage amount; 30%. Regarding the terms, we believe that the diversity of backgrounds in the sample have led to use different terminology/terms when asked to write their major concerns listed in Table 2, but most of these concerns were focused on the data secrecy and protection. The CSPs service quality was listed by the data owners but was not considered major. Table 2 content is shown in Figure 3 to present the relation of percentages for the aspects concerns.

As a matter of fact, it can be noticed from Figure 4 that the majority of participants (78%) were positive (answered "Yes") regarding the questions that were directed to them (unbiased) with a complete freedom for them to answer either "Yes" or "No" while only a small portion of them answered "No" (22%); this percent is less than

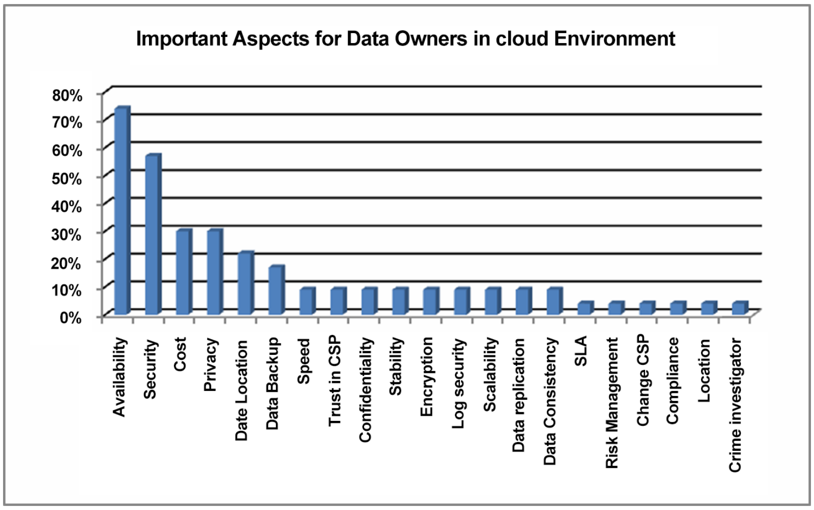

Figure 3. Important aspects for data owners in cloud environment.

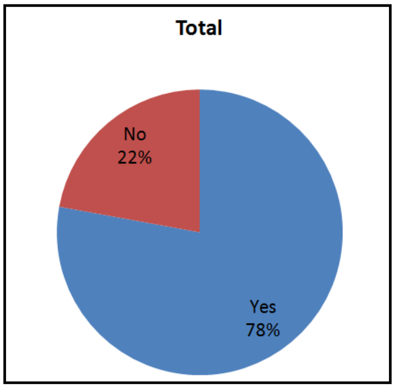

Figure 4. Important aspects for data owners in cloud environment.

the quarter of all answers; this fact helped us investigating in more details the answers of each questions to get realistic results and analysis as explained in the previous two paragraphs.

An overall view on the questionnaire results shows the importance for the data owners to address three major issues: their ability to continue the work, the secrecy and integrity of their data, and the spatial, legal, temporal constraints related to their data.

3. Proposed Extension to Auditing Models

Many aspects of the data owners' concerns are imposed by the nature of their data and the cloud environment specifications, and it can be tackled through the SLAs between the tenants and providers. Some of the contractual obligation may be of a special nature such as having data stored in geographically specific region or location, to adhere to some legal or social aspects, etc. Auditing and compliance checking processes, if enforced in a way that can assure the data owners about their data and the compliance of the CSPs with their obligations, then it shall be a way to an increased adoption of cloud computing services.

Auditing is dealing with entirely different set of challenges in cloud computing that are not yet resolved. Audit must be data-centric and cross-application, providing information on the flow about a particular data item during its whole life cycle, allowing assessment of where responsibility of that data item lies. Audit outcome represents the actions performed on data and the entities that are responsible for those actions [10]. A full audit trail is infeasible in clouds at this time due to lack of standardization in some areas such as the interoperability, and the entirely different set of challenges posed by auditing in clouds [3].

Logging and auditing procedures enforcement are critical to the different aspects concerning data outsourcing. Many of these aspects such as secrecy and availability were addressed in the literature for different types of systems including the clouds, but some other aspects are either had little attention or even overlooked in the literature [2] [12] [25]; following [11] we will refer to such aspects as the contractual obligations. We mean by contractual obligations the set of policies imposed by the data owners and accepted by the service provider to be fulfilled, it encompasses different domains:

- Spatial: refers to the geographical locations or boundaries that the client restricts the service provider from putting his/her data outside it, either during processing or in storage.
- Temporal: refers to the need to permanent deletion of the data or part of it before or after some time point/interval.
- Legal: the client requests of the provider to keep his/her data only in locations that are under-or outside-certain jurisdiction authority, which implies the enforcement or not enforcement of some regulations such as the personal information protection acts.

Figure 5 shows the proposed extension to the auditing models. Cloud deployment models—especially Public deployment model in our context—have different delivery

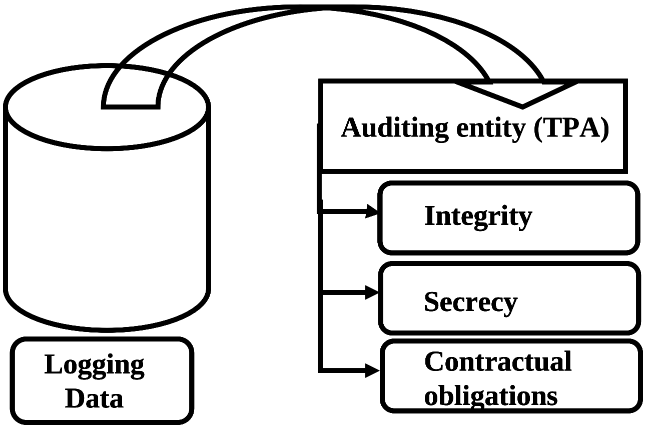

Figure 5. Extending the auditing models to include contractual obligations.

models, each delivery model will have different impacts on the auditability over the clients' data, but in general all models share the same concerns about the adherence to the contractual obligations.

4. Conclusion and Future Work

In this work, we have explored the areas which are overlooked or not given its deserved and actual volume in the auditing literature. Auditing is a crucial process that increases the users trust in cloud technology; the concerns of the users over their data are hindering the shift to use the clouds especially for data that contains sensitive or personal information.

We have conducted a questionnaire on a sample group of IT specialists to understand the different concerns of data owners when deciding to move to the cloud. It was clear that not only the secrecy and integrity of the data are important, but also some other aspects such as the data location (spatial) related issues, time (temporal) related issues, and legal related issues are as well important.

The paper contributed to knowledge by proposing an extension to the auditing models to include the fulfillment of contractual obligations aspects that only had little work in auditing literature; beside the important aspects of secrecy and integrity of client's data. We used the term contractual obligations to refer to these aspects which will reflect the set of policies imposed by the data owners and accepted to be fulfilled by the service provider. The results of a conducted questionnaire showed the importance for the data owners to address mainly three major issues: Their ability to continue the work, the secrecy and integrity of their data, and the spatial, legal, temporal constraints related to their data.

For future research, the proposed extension to the auditing model need to be further investigated, implemented, and tested. We believe that the implementation of the proposed auditing model will leverage the transparency of the clouds and this will lead to more adoption of cloud technology in the field.

References

[1] Pardeshi, P.M. and Borade, D.R. (2015) Improving Data Integrity for Data Storage Security in Cloud Computing. *International Journal of Computer Science and Network Security* (*IJCSNS*), **15**, 75.

[2] Henze, M., Hummen, R. and Wehrle, K. (2013) The Cloud Needs Cross-Layer Data Handling Annotations. 2013 *IEEE Security and Privacy Workshops* (*SPW*), Washington DC, 23-24 May 2013, 18-22. http://dx.doi.org/10.1109/spw.2013.31

[3] Marinescu, D.C. (2013) *Cloud Computing: Theory and Practice*. Newnes.

[4] Liu, C.-W., *et al*. (2016) A Survey of Attribute-Based Access Control with User Revocation in Cloud Data Storage. *International Journal of Network Security*, **18**, 900-916.

[5] Kishore, N. and Sharma, S. (2016) Secured Data Migration from Enterprise to Cloud Storage–Analytical Survey. *BVICAM's International Journal of Information Technology*, *8*(1).

[6] Kumar, D. and Karuppuchamy, V. (2016) Competent Demonstrable Data Possession for Integrity Verification in Multi-Cloud Storage. *International Research Journal of Engineering and Technology* (*IRJET*), **3**, 464-468.

[7] Brandenburger, M., Cachin, C. and Knezevic, N. (2016) Securing Integrity and Consistency of a Cloud Storage Service with Efficient Client Operations. US Patent No. 20,160,048,703.

[8] Ghafghazi, H., *et al*. (2016) Secure Data Storage Structure and Privacy-Preserving Mobile Search Scheme for Public Safety Networks. arXiv preprint arXiv:1602.04493

[9] Wu, S., Li, K.C., Mao, B. and Liao, M. (2016) DAC: Improving Storage Availability with Deduplication-Assisted Cloud-of-Clouds. *Future Generation Computer Systems*.

[10] Pasquier, T. and Eyers, D. (2016) Information Flow Audit for Transparency and Compliance in the Handling of Personal Data. In *IC2E International Workshop on Legal and Technical Issues in Cloud Computing (CLaw'16). IEEE*.

[11] Hsien, W.-F., Yang, C.-C. and Hwang, M.-S. (2016) A Survey of Public Auditing for Secure Data Storage in Cloud Computing. *International Journal of Network Security*, **18**, 133-142.

[12] Pasquier, T.F.M. and Powles, J.E. (2015, March) Expressing and Enforcing Location Requirements in the Cloud Using Information Flow Control. In *Cloud Engineering (IC2E), 2015 IEEE International Conference on* (pp. 410-415). IEEE.

[13] BrancoJr, T. and Santos, H. (2016, June) What Is Missing for Trust in the Cloud Computing? In *Proceedings of the 2016 ACM SIGMIS Conference on Computers and People Research* (pp. 27-28). ACM.

[14] Jain, S., Kumar, R., Kumawat, S. and Jangir, S.K. (2014) An Analysis of Security and Privacy Issues, Challenges with Possible Solution in Cloud Computing. In *National Conference on Computational and Mathematical Sciences (COMPUTATIA-IV), Technically Sponsored By: ISITA and RAOPS, Jaipur*.

[15] Chen, Z. and Yoon, J. (2010, July) IT Auditing to Assure a Secure Cloud Computing. In *2010 6th World Congress on Services* (pp. 253-259). IEEE.

[16] Zaigham, M. (2011) Data Location and Security Issues in Cloud Computing. *International Conference on Emerging Intelligent Data and Web Technologies* (*EIDWT*), Tirana, 7-9 September 2011, 49-54.

[17] Irfan, G., Rehman, A. and Islam, M.H. (2011) Cloud Computing Security Auditing. 2*nd International Conference on Next Generation Information Technology* (*ICNIT*), Gyeongju, 21-23 June 2011, 143-148.

[18] Golzardi, E. (2015) Cloud Computing Security: A Survey. *Journal of Information Sciences and Computing Technologies*, **5**, 377-385.

[19] Deswarte, Y., Quisquater, J.J. and Saïdane, A. (2004) Remote Integrity Checking. In *Integrity and Internal Control in Information Systems VI* (pp. 1-11). Springer US.

[20] Wang, Q., Wang, C., Ren, K., Lou, W. and Li, J. (2011) Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. *IEEE Transactions on Parallel and Distributed Systems*, **22**, 847-859. http://dx.doi.org/10.1109/TPDS.2010.183

[21] Massonet, P., Naqvi, S., Ponsard, C., Latanicki, J., Rochwerger, B. and Villari, M. (2011, May) A Monitoring and Audit Logging Architecture for Data Location Compliance in Federated Cloud Infrastructures. In *Parallel and Distributed Processing Workshops and Phd Forum (IPDPSW), 2011 IEEE International Symposium on* (pp. 1510-1517). IEEE.

[22] Eskandari, M., De Oliveira, A.S. and Crispo, B. (2014) VLOC: An Approach to Verify the Physical Location of a Virtual Machine Cloud. 6*th International Conference on Cloud Computing Technology and Science* (*Cloud Com*), Singapore, 15-18 December 2014, 86-94. http://dx.doi.org/10.1109/cloudcom.2014.47

[23] Wüchner, T., Müller, S. and Fischer, R. (2013, December) Compliance-Preserving Cloud Storage Federation Based on Data-Driven Usage Control. In *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on* (Vol. 2, pp. 285-288). IEEE.

[24] Pasquier, T., Singh, J., Bacon, J. and Eyers, D. (2016) Information Flow Audit for PaaS Clouds. *International Conference on Cloud Engineering* (*IC*2*E*), Berlin, 4-8 April 2016, 81-88. http://dx.doi.org/10.1109/ic2e.2016.19

[25] Tan, Y.S., Ko, R.K.L. and Holmes, G. (2013) Security and Data Accountability in Distributed Systems: A Provenance Survey. 10*th International Conference on High Performance Computing and Communications* & 2013 *IEEE International Conference on Embedded and Ubiquitous Computing* (*HPCC_EUC*), Zhangjiajie, 13-15 November 2013, 1571-1578.

[26] Meena, K. and Gomathy, M. (2016) study on Security Frameworks and Data Protection Techniques for Public Cloud Environment. *APPN Journal of Engineering and Applied Sciences*, **11**, 5933-5939.

[27] Khan, M.A. (2016) A Survey of Security Issues for Cloud Computing. *Journal of Network and Computer Applications*, **71**, 11-29. http://dx.doi.org/10.1016/j.jnca.2016.05.010

[28] Brindha, T. and Shaji, R.S. (2015) An Analysis of Data Leakage and Prevention Techniques in Cloud Environment. 2015 *International Conference on Control*, *Instrumentation*, *Communication and Computational Technologies* (*ICCICCT*), Noorul Islam University, 18-19 December 2015, 350-355.

[29] Singh, J., Pasquier, T., Bacon, J., Ko, H. and Eyers, D. (2016) Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal*, **3**, 269-284. http://dx.doi.org/10.1109/JIOT.2015.2460333

Appendix A. Questionnaire

Please answer the following questions according to your expertise in the IT field and data manipulation practice:

Question No.	Question Text	Answer (Yes ☑ No☒) or Type …
1	Does data storage and manipulation outsourcing in clouds presents major concerns to data owners, (especially for confidential data)?	□
2	Are some of the data owners' concerns are caused by the lack of transparency and limited user control over their data residing in the cloud?	□
3	Does cloud multi-tenancy in conjunction with VMM (or similar technologies) represent a new attack channels for malicious users?	□
4	Does it important to the outsourced data owners to able to track where, when, how and by whom data was generated or manipulated?	□
5	Is it important to data owner to specify the physical storage location of the data (i.e. where it may or may not be)?	□
6	Is it important to the data owner to specify the permanent deletion of backup copies of their data (i.e. after a certain period of time)?	□
7	Is it important to the data owner to specify the judiciary system that the data location may or may not belong to?	□
8	Please give any aspects that you think it may generate major concerns for a data owner when outsourcing data storage and manipulation (beside technical, legal, geographical aspects).	________ ________ ________ ________
9	In addition to the secrecy and integrity concerns of the data, are there more concerns about data outsourcing? List them please…	________ ________ ________ ________
10	Is frequent Audit checking needed to keep an eye on data, and to track the data movement to ensure only allowed flows exist?	□
11	Do you think it is important for the data owner to be able to analyze of how information has actually flowed across the system?	□
12	Do you think entities who own the data in general has the possibilities to perform the auditing for their data logs?	□
13	Do you think that a trusted third party with needed qualifications may be a better option to audit the data logs for entities owning the outsourced data?	□

Appendix B. Participants' Answers

Participant No.	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q10	Q11	Q12	Q13
1	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No
2	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	No
3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
4	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
6	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
7	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes
8	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
10	Yes	No	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes
11	Yes	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
12	Yes	Yes	Yes	No	Yes	No	Yes	Yes	Yes	Yes	Yes
13	Yes	No	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
14	Yes	Yes	Yes	No	No	Yes	No	Yes	Yes	No	Yes
15	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	No	Yes
16	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
17	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
18	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes
19	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
20	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
21	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes
22	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes
23	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No