Securing Cloud System via Internal Control Management

Ashwin Alfred Pinto, Shvetank Verma, Satyam Singh, Prashant Srivastava, Rahul Gupta, and Vijay Chourasia

Abstract— **Data protection in cloud computing is constantly been an issue of discussion. There will always be something left undone, incomplete, insecure and unestablished. But a chance of improvement will be there every time. The data access should be monitored whenever there is a move from the client side. Also the privacy checks via internal control should be done in order to ensure the confidentiality of sensitive data. In this paper, a new entity has been introduced for managing the data accessibility and for assigning apt controls with respect to the business levels by employing Statement of Applicability (SOA) concept. Also the application of internal controls mentioned in this paper has a significant meaning. The issue of data security is also considered within this paper and therefore the sense of data protection is involved by implementing the respective internal controls. Service Level Agreements (SLAs) will also be discoursed as it is necessary to include a third party hand for smooth running of cloud applications.**

Index Terms— **Cloud security manager (CSM), service level agreements (SLAs), statement of applicability (SOA)**

I. Introduction

The need for revision is required in the security matter of cloud computing. The issue of data protection in this area is now a days boiling in the corporate world. The existing network architecture is far different from what the cloud network avers. Therefore, it is bit complex or novel to understand the form of protection required for cloud computing.

The cloud computing concept facilitates with the access of your own data remotely in the supervision of a cloud server. This means one can store their data in the database of the server and can be retrieved whenever needed. But the question arises whether the data stored is secure enough or not, how it is being processed, who is going to process your data, what control are applied to make your data secure and several other questions are there that has to be answered.

There are lots of research work has been done in this area but following are some issues that are still untouched:

- Reviewing access record: There should be an entity to keep track of all transaction that are been done by the client and should generate a weekly report of it. So that the client can also assure secure data usage.
- The concept of SOA with respect to the business needs: The internal controls should be provided at each business level and the applicability of controls should be reviewed time to time.

Our approach is to explain the existence of a new entity called cloud security manager who will be keeping records of each and every access done by clients as well dealing with the third party processing. Also the internal control being applied at each stage of the cloud system is to be monitored and modified if needed. The overall management in the cloud system will be performed by the cloud security manger, who will employ an internal control matrix which is explained afterwards.

This paper is including some other subsisting ideas which made an easy way for explaining the introduced approach. We have gone through following concepts that already exist in recent papers, they are as follows:-

A. Aware *design for cloud computing-*

The design for data protection is introduced with the help of a capability maturity model. Also the role of third party has been brought up via SLAs (Service Level Agreements). But, still there is a need of advancement in cloud governance, cloud application and third party responsibilities.

B. Data protection challenges in cloud computing-

The theme of data security and benefits of using cloud computing has been addressed, along with privacy risks involved in the processing within cloud computing. The idea of implanting the privacy controls on the respective business levels is to be attained yet.

C. Cloud solution for compliance-

Various common compliance standards have been introduced on the cloud methodology. But, DPA (Data Protection Policy) has its own significance and is to be introduced amongst those compliance standards especially for cloud computing. Hence the issue of trans-border data flow can be resolved easily.

Manuscript received March 25, 2011; revised April 14, 2011.This work was supported in part by the Indian Institute of Information Technology, Allahabad under Sec .3 of UGC Act, 1956.The paper title is Securing Cloud System via Internal Control Management.

Ashwin Alfred Pinto is student of Master of Science in Cyber Law &Information Security in Indian Institute of Information Technology, Allahabad, India (phone: 9651908593; e-mail: ashyalfred23@gmail.com).

Shvetank Verma is student of Master of Science in Cyber Law &Information Security in Indian Institute of Information Technology, Allahabad, India (e-mail: vshvetank @gmail.com).

Satyam Singh is student of Master of Science in Cyber Law &Information Security in Indian Institute of Information Technology, Allahabad, India (e-mail: isatyam@live.com).

Prashant Srivastava is student of Master of Science in Cyber Law &Information Security in Indian Institute of Information Technology, Allahabad, India (e-mail: prashant_srivastava@live.com).

Rahul Gupta is Lecturer in Indian Institute of Information Technology, Allahabad, India (e-mail: rahulgupta@iiita.ac.in).

Dr. Vijay Chourasia is Assistant Professor in the Dept. of Master of Science in Cyber Law &Information Security in Indian Institute of Information Technology, Allahabad, India (e-mail: vijayk@iiita.ac.in).

II. CONSTITUENTS OF THE PROPOSED MODEL

A.Cloud server-

The cloud server is loaded with dedicated software, hardware and efficient processors. A cloud operating system will be installed to carry on the processes regarding cloud computing.

B.Cloud security Manager (CSM)-

The cloud security manager will be responsible for governing the cloud system. The CSM will generate a processing report monthly that will mention the activities and will monitor the abidance of standards and policies, the report will also contain the issues of internal controls if any. The CSM will generate another report of client transaction at every week covering the throughout data access activities of the client and this report will be sent to the client for crosscheck.

C.Third party-

The third party is a separate entity that has been assigned for entertaining the client`s requests by providing them respective services. The CSM will be responsible to assign a third party on the basis of their qualification. The third party will sign an agreement with the CSM for providing the services. This agreement is termed as SLA (Service Level Agreement) that will hold a control upon the third party.

D. Cloud repository-

This particular repository consists of the global database containing the relevant data of each and every client associated with the cloud. The data kept in the repository will be kept secret and will be made available to the client whenever needed.

E.Client-

The client is the entity associated with the cloud system whose information is stored in the cloud repository and to whom various requested services and applications are provided with the help of the third party. The clients have to associate themselves by getting registered with the known cloud.

III. PROPOSED MODEL

The proposed model is termed as Cloud Management Model which explains about the responsibility of the CSM. The CSM is assigned as the authoritative body for monitoring the activities going on in the cloud system. The CSM will be managing the cloud server and will carry on interaction with the third party. The third party is to be allotted on the basis of their qualification which is deemed by the CSM. The CSM will sign an agreement with the third party, i.e. termed as Service Level Agreement (SLA). The SLA will define the overall duties and liabilities of third party. The CSM is responsible for defining the rules of thumb, penalties and internal controls. The internal controls are the vouchers that ensure whether the third party services and other functionalities are carried out properly or not.

The CSM will maintain the repository where client`s data will be stored. Each client will be provided with some portion of the cloud database to store their useful information. Firstly every participating client has to register themselves in the dedicated cloud. They can also utilize the cloud services and applications by disclosing their respective unique identity to the cloud server. The authentication mechanism will be installed at the front end. The client will be associated to the cloud server, with the help of third party. The third party will be interacting to the clients for entertaining their requests.

The CSM will generate to types of report that will help in achieving confidence of CSM and client as well. The "functional report" is for drafting following points:-

(a) Monthly report for each client`s transaction
(b) Applicability of internal controls
(c) Consistency of cloud matrix
(d) Feasibility of authentication mechanism
(e) Abidance of Service Level Agreement (SLA) by the third party
(f) Accountability of each client
(g) Database security position

All of these facts are reviewed by CSM before releasing the report. The report will be undersigned by CSM.

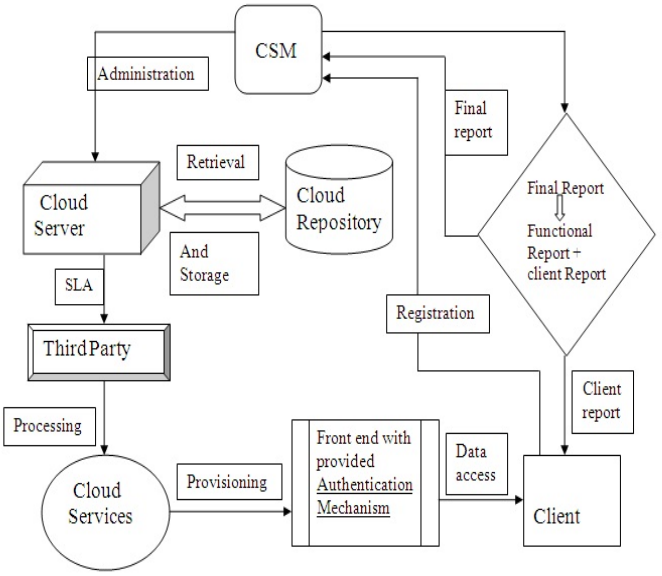


Fig.1 Cloud Management Model

The "Client report" is the report of individual client, which will be issued every week and will be provided to the respective client. This report explicates following points:-

(a) Client`s user ID
(b) Client`s access date, time and session ID
(c) Accessed information
(d) Itemized subscription
(e) Pending subscription (if any)
(f) Complaint response (if any)
(g) Data controllers ID (who is processing client`s data)

All of these details are reviewed by CSM before issuing the report to client. The report will be undersigned by CSM.

IV. INTERNAL CONTROL MATRIX

The cloud matrix is a representation of the internal controls that are applied in the cloud system. This matrix is crucial enough to observe the functionalities across the cloud system. Dedicated internal controls are implemented at different levels. The matrix is consisting of five levels and at each level; the internal controls are implemented according to the need of the environment. Cloud security manager (CSM) has to follow the matrix for monitoring the activities taking place around the cloud system.

The matrix has been discussed below with the help of internal controls implanted at each level:

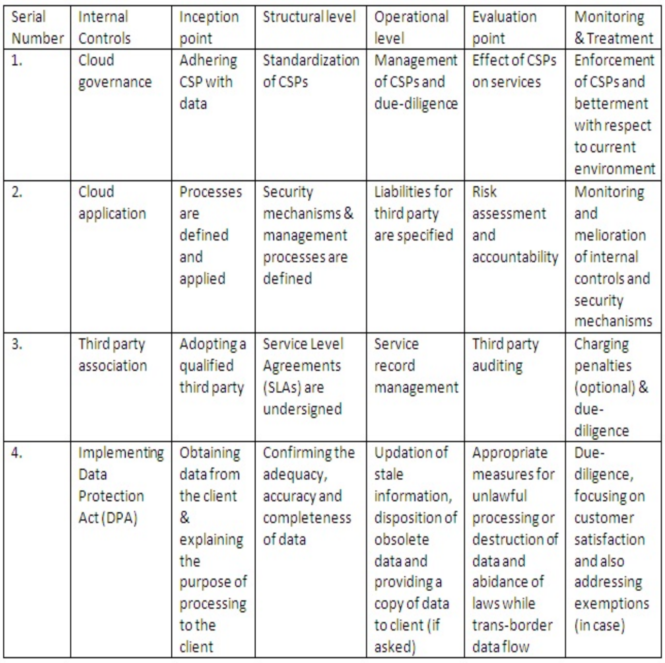
(1)Cloud governance-

At the inception level, the cloud security policies (CSPs) are adhered with the data provided. The standardization of these cloud security policies is being done at the structural level. Then at operational level, management of such cloud security policies done and also the due-diligence practices are carried on. There will be periodic evaluation of cloud security policies, to see the effectiveness on the services. Also, time to time new cloud security policies will be introduced and betterment of the existing policies will be done.

(2)Cloud application-

In this particular field, the beginning level involves the explication and application setup of processes. Then security mechanisms and management processes are defined at the very structural level. There by the guidelines and penalties are specified while operating the system. Following this, regular due-diligence is carried on with proper procedures.

TABLE I
INTERNAL CONTROL MATRIX



Serial Number	Internal Controls	Inception point	Structural level	Operational level	Evaluation point	Monitoring & Treatment
1.	Cloud governance	Adhering CSP with data	Standardization of CSPs	Management of CSPs and due-diligence	Effect of CSPs on services	Enforcement of CSPs and betterment with respect to current environment
2.	Cloud application	Processes are defined and applied	Security mechanisms & management processes are defined	Liabilities for third party are specified	Risk assessment and accountability	Monitoring and melioration of internal controls and security mechanisms
3.	Third party association	Adopting a qualified third party	Service Level Agreements (SLAs) are undersigned	Service record management	Third party auditing	Charging penalties (optional) & due-diligence
4.	Implementing Data Protection Act (DPA)	Obtaining data from the client & explaining the purpose of processing to the client	Confirming the adequacy, accuracy and completeness of data	Updation of stale information, disposition of obsolete data and providing a copy of data to client (if asked)	Appropriate measures for unlawful processing or destruction of data and abidance of laws while trans-border data flow	Due-diligence, focusing on customer satisfaction and also addressing exemptions (in case)

(3)Third party association-

The CSM is responsible for opting a qualified and well trained unit of third party that is capable of performing their duties consistently and faithfully. While structuring the framework of the cloud system (including third party), service level agreement (SLA) is offered by the CSM and is undersigned by third party. This SLA will declare the responsibility of third party for their liabilities. The service record of third party is managed at the operational level. At the time of evaluation, third party auditing is performed to keep an eye on the actions of third party. These activities are done with proper monitoring and also penalties are defined in case of risk assessment and accountability is observed. Periodic monitoring and improvement of internal controls and security mechanisms are done, with respect to the current requirements on the system.

(4)Implementing data protection act (DPA)-

The eight principles of data protection are duly followed in order to ensure the security of personal data of the client. At the first level, the personal data of the client is obtained.

The third party will assign a data controller and a data processor for his further activities. The data controller has to define the purpose of processing that data. This personal data is taken from the concern of the respective client.

This data is then transferred to the data processor for further processing of data. The data processor will ensure that the data obtained is adequate, accurate and complete. During the operational level, it is advised to keep the data up-to-date and the obsolete data should be disposed properly. Meanwhile, if the client requests for acquiring the data or if there is some processing related requests, then a copy of currently existing data is forwarded to the client.

Also the information about the data processor or any other entity (considered for the processing of data with the concern of client) who is involved in the processing is given to the client under his request. While evaluating this processing action, appropriate measures should be taken in case of any unlawful or unauthorized processing. Also the client should be satisfactorily compensated in case of any damage or data loss.

Besides this, it should be observed that the third party is abiding the laws at the time of trans-border data flow.

While monitoring third party, CSM should focus on the customer`s confidence and the level of satisfaction, also due-diligence is to be carried on regularly. Exemptions are considered if there is a call for serious action. These DPA principles are implemented as internal controls into the cloud system for holding the actions of third party.

V. CONCLUSION

This paper is basically explaining the enhancement of the cloud structure by introducing a new entity that is CSM. The CSM here by, will be performing his duties that are helping the cloud environment in doing more efficient exercises. In addition to it, we have introduced an internal control matrix which will direct CSM to monitor the system, client and third party. This matrix is effective enough and also useful for the CSM to administer the working of internal controls at each and every level of the cloud system. The internal control matrix is also facilitated with the implementation of DPA (Data Protection Act) that assist in treating the personal data of the client.

The proposed model is more efficacious than the existing models, as the role of CSM is a new concept whose responsibilities are capable enough in covering lots of loopholes in the cloud system. Also the proposed internal control is highly dominating on the currently introduced matrices, because the proposed matrix is including all possible controls like governance, third party responsibilities as well as DPA (Data Protection Act).

VI. FUTURE WORK

This paper is covering management and control component of the cloud system, but still the issues of secure authentication mechanism and secure transaction protocol has to be dealt with. These improvements will not be ending until the system resides in a constant position, because the system changes with time and time needs betterment of the system, so this cycle goes on continuing.

ACKNOWLEDGMENT

Authors would like to thank Indian Institute of Information Technology-Allahabad (A university Established under Sec.3 of UGC Act) for their constant support and for providing better opportunities.

REFERENCES

[1] Sadie Creese, Paul Hopkins, Siani Pearson, Yun Shen, *Data Protection-Aware Design for Cloud Services*, Aug 21, 2009, [Online] Available: http://www.google.co.in/url?sa=t&source=web&cd=1&ved=0CBYQFjAA&url=http%3A%2F%2Fwww.hpl.hp.com%2Ftechreports%2F2009%2FHPL-2009-192.pdf&rct=j&q=data%20protection-%20aware%20design%20for%20cloud%20services&ei=_2lmTby_G4eecKmZ6I0M&usg=AFQjCNHLo8-2X4rJ2mtlSeBaBxgcATHgIg&cad=rja

[2] CITRIX, *Citrix Cloud Solution for Compliance*, [Online] Available: http://www.google.co.in/url?sa=t&source=web&cd=2&ved=0CCcQFjAB&url=http%3A%2F%2Fwww.citrix.com%2Fsite%2Fresources%2Fdynamic%2Fsalesdocs%2FCitrix_Cloud_Solution_Compliance.pdf&rct=j&q=citrix%20cloud%20solution%20for%20compliance&ei=2m1mTe7kC470ccXwiY8M&usg=AFQjCNE5ej2d0aquqsRWvvhmBLwyahPJPg&cad=rja

[3] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, *Ensuring Data Storage Security in Cloud Computing*, 2009, [Online] Available: http://www.google.co.in/url?sa=t&source=web&cd=1&ved=0CB8QFjAA&url=http%3A%2F%2Fwww.ece.iit.edu%2F~ubisec%2FIWQoS09.pdf&rct=j&q=ensuring%20data%20storage%20security%20in%20cloud%20computing&ei=dW9mTbX3LcuPccaR8I0M&usg=AFQjCNGqgSQLxnoetXQHBDchdh0qqNkHxw&cad=rja

[4] Data Security Council of India-DSCI, *Legal Framework for Data Protection and Security and Privacy norms*, 5th July, 2010, [Online] Available: http://www.dsci.in/sites/default/files/Legal%20Framework%20for%20Data%20Protection%20and%20Security%20and%20Privacy%20norms_0.pdf

[5] Nethology Privacy Policy, *Data Protection Cloud Computing Privacy Policy*, 2010, [Online] Available: file:///H:/Mas%20proj/data%20protection%20for%20cloud%20computing/privacy-policy.htm

[6] Katharine Stuart, David Bromage, *Current state of Play: records management and the cloud*, 2010, [Online] Available: http://www.google.co.in/url?sa=t&source=web&cd=1&ved=0CBYQFjAA&url=http%3A%2F%2Fwww.emeraldinsight.com%2Fjournals.htm%3Farticleid%3D1875529%26show%3Dpdf&rct=j&q=current%20state%20of%20play%3A%20records%20management%20and%20the%20cloud%20pdf&ei=qnZmTenmDNLzcYi77Y4M&usg=AFQjCNEtGp5kuAMsNsg5a_xlCklO5xbQZQ&cad=rja

[7] Marc Vael, *Cloud Computing An Insight In The Governance & Security Aspects*, 2010, [Online] Available: http://www.isaca.org/Groups/Professional-English/information-secuirty-management/GroupDocuments/Across%20Cloud%20Computing%20governance%20and%20risks%20May%202010.pdf

[8] Andreas Krisch, *Data Protection In The Cloud*, 11th March, 2009, [Online] Available: http://www.edri.org/files/akrisch_TPV_CloudPrivacy_20091103.pdf

[9] Kynetix Technology Group, *Cloud Computing A Strategy Guide For Board Level Executives*, 2009, [Online] Available: http://www.google.co.in/url?sa=t&source=web&cd=1&ved=0CBsQFjAA&url=http%3A%2F%2Fdownload.microsoft.com%2Fdownload%2F1%2F5%2FD%2F15DA1ED7-6005-4D18-A592-12EA315A3F4A%2FKynetixCloudComputingStrategyGuide.pdf&rct=j&q=cloud%20computing%20management%20pdf&ei=_thwTYO6IsLIcajL5PgC&usg=AFQjCNHW7EeqwRcE6AfUl6w4xy3xNnXfkw&cad=rja

[10] Anu Gopalakrishnan, *Cloud Computing Identity Management*, 2009, [Online] Available: http://www.infosys.com/research/publications/setlabs-briefings/Documents/cloud-computing-identity-management.pdf

[11] John Verity, *Cloud Computing Changing Data Management*, 28th Feb, 2009, [Online] Available: http://www.cloud9technology.com/SiteResource/Site_103317/Customize/Image/Cloud_computing_changing_data_management_.pdf

[12] Trend Micro Group, *Cloud Computing Security*, May 2010, [Online] Available: http://www.securecloud.com/imperia/md/content/us/pdf/solutions/enterprisebusiness/serversecuritysolutions/deepsecurity/wp04_vm_cloudsecurity100528us.pdf