Journal of Theoretical and Applied Information Technology
10th July 2014. Vol. 65 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FRAMEWORK FOR AUDITING IN CLOUD COMPUTING ENVIRONMENT

[1]SUNEETA MOHANTY, [2]PRASANT KUMAR PATTNAIK, [3]GANGA BISHNU MUND

[1,2,3] School of Computer Engineering., KIIT University, Bhubaneswar, India

E-mail: [1] smohantyfcs@ kiit.ac.in, [2] patnaikprasantfcs@ kiit.ac.in, [3] mund@ kiit.ac.in

ABSTRACT

Cloud Computing is an emerging field in the era of internet where information and Physical resources can be provided to cloud users according to their needs in pay-per-go basis. Security and privacy are the major concerns in Cloud Computing Environment(CCE). To achieve these issues all the physical resources like computing resources, sensitive user data and processes are got managed by the Third Party Service Provider. Audit in CCE provides the way for Cloud Service Provider to make their performance and security data available for the Cloud user readily. Hence to maintain data confidentiality, privacy, integrity and availability, auditing is introduced within Third Party Service Provider. This paper aim to study various issues in auditing that has been in practice and also intended to propose a framework that helps the designer to incorporate auditing aspects in CCE.

Keywords: *Cloud Computing Environment(CCE), Cloud Service Provider(CSP), Third Party Auditing Service(TPAS), Auditing*

1. INTRODUCTION

Cloud Computing is developing based on years' achievement on virtualization, Utility computing, Cluster Computing, Grid computing and related technologies. Cloud computing provides both platforms and opportunity for deployment of user-applications on-demand through Internet. In Cloud computing, on demand shared resources, software, and information are provided to computers and other devices [1][2].Cloud deployment model consists of public cloud, private cloud ,hybrid cloud[7] and community cloud [8].Initially in cloud, different organizations managed their computing resources on their own and vacillate to disclose their raw data to others. They had to bear extra cost for supporting and maintaining all the resources. This concept was going to be highly expensive and extra overhead. Hence, to overcome this kind of burden, they have introduced Third Party Service Provider. In this concept, all the physical resources including computing resources, sensitive user data and processes are got managed by the Third Party Service Provider. The concerned organizations have to provide all the data to the provider and those data are easily accessible by anyone within the third party or it's another user or other organizations related to third party or even any customer of the organization itself. Data security becomes most significant issue in all levels of services such as Resource as a Service (RaaS) [2], Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).At the network level, CSP is monitoring, collecting and protecting firewall, intrusion prevention system and router data flow. At the host level, provider should integrate system log files and at the application level, service provider should also be gathering application log data including authorization and authentication information. So data security is most important concern in the recent cloud scenario. Public clouds are more sensitive to new attacks, threats and vulnerabilities than the private cloud. If we look at the network level of security, we have to ensure the confidentiality and integrity of the transmitting data to and from the public. Therefore, to maintain the privacy of the sensitive data and resources, an auditing concept has been introduced within the Third Party Service Provider for maintaining data privacy and data integrity check.

This paper is organized as follows: In section 2 we have discussed the importance of auditing in Cloud Computing Environment. Section 3 presents the auditing framework. Lastly section 4 concludes our work.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. IMPORTANCE OF AUDITING

In the field of swift usage of cloud, web server, application server, and database server, auditing is needed in every phases of cloud infrastructure due to maintenance of data confidentiality, privacy, integrity and availability. In the recent scenario, data is being stored, transferred and processed outside the company or organization. The raw data is not physically controlled by the organization and shared computing environments are also making it public. These kinds of loopholes need more security and privacy. In respect to data access, no controls have been implemented to restrict data modification and no logging events such as access, transmission, modification on data have not been monitored. Limited capabilities for change control and provider feasibility are also the drawbacks of cloud infrastructure. One more thing is that all the physical and logical accesses are managed and maintained by the Cloud Service Provider (CSP). Hence auditing is highly required to maintain the privacy of the sensitive data, restricted access of computing and physical resources and to check integrity.

2.1 Role of Third Party Service Provider in Auditing

In the surge of rapid usage of internet over the world, several security issues are concerned such as handling web attacks [3], data access control [4], enhancing dynamic allocation strategies [5], and controlling sensitive information flow [6]. According to Information Systems Control and Audit, IT auditing can be defined as a process of aggregating and evaluating evidence to decide whether a computing information system safeguards resources, maintains data integrity and secure sensitive user data, attains organizational objectives effectively and consumes physical and computing resources efficiently. Information assurance controls in Governing documents like DoDI 8500.2, NIST SP800-53 or Common Criteria have supported auditing by dictating minimal requirements for audit[13].Considering the fact that ensures proper access control such as authorization, authentication and auditing to the physical and virtual resources used at public cloud provider. It is also to be ensured the availability of the Internet-facing resources in a public cloud being used by the organization. In the host level of security, virtualization security threats like system configuration change, weak access control of the hypervisor [2], faulty provisioning of resources, proper usage of instances of VMs are to be considered for making secure cloud. The integrity and availability of the hypervisor is to be guaranteed because a vulnerable hypervisor could expose all user domains to malicious insiders. Security controls are to be maintained for platform level (PaaS) applications where user authentication, account management, endpoint security measures including antivirus, and browser with latest patches are to be authorized. However, data security becomes more important while customers' raw data is managed and customized by the Third Party Cloud Service Provider. While accessing those data, cloud providers should be concerned for the security of those data. assets. Security issues and different negotiation protocols are concerned with auditing. Audibility also enables accountability (retrospective). It allows taking an action to be reviewed against a pre-determined policy. Wang et al. [11] have described an auditing system in which an auditor can be able to audit without knowing the user's data contents. They also explained the batch auditing protocols where multiple auditing jobs of different users are concurrently performed by Third Party Auditor.

2.2 Cloud Auditing Outsourcing Lifecycle Phases

Organizations outsourced all its sensitive data, processes and computing resources to the Third Party Vendor for handling and maintenance of those data and resources, it is going through different phases [9] as follows:

Phase1 Selecting the appropriate Third Party vendor: When an organization wants to deploy its application or want to rent the physical resources or need an independent platform where heterogeneous application can be executed, it needs to select the proper vendor which should be able to handle all the requirements.

Phase 2 Define strategy: The service provider vendor should be transparent in defining its business strategy and risk management philosophy. This kind of decision strategy will enable the service provider to meet the baseline requirements of its consumers.

Phase 3 Define policies and workflow: Having defined its strategy and customer-requirements, service provider needs to translate its requirements into policies applicable to industry standards. In this phase, providers need to determine the configuration settings, flow control, platforms and to maintain the workflow.

Phase 4 Establishing business case: Driven by the strategy and policies of the service provider, the business case is established and different concerns related to privacy, security and availability should be in the business protocol.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Phase 5 Due diligence of the Third Party Vendor: An act with a firm standard of care should be established within the Third Party Service Provider. Due diligence process is being concerned with some issues like Compatibility audit, Marketing audit, financial audit, Management audit, Legal audit, and Information systems audit. The technological direction of both the Third Party and the concerned organization should the directly aligned.

Phase 6 Validating Agreement protocol and establishing relationships: A Service Level Agreement (SLA) protocol and escrow service are being established between both vendor and the organization so that both can meet in a standardize platform. Both should know the responsible authorities with their functionalities.

Phase 7 Dynamic monitoring: In this phase of lifecycle, dynamic monitoring service is getting enabled and dynamically monitors whether the vendor can continue the stable operations, can provide services or not. In the meanwhile, Auditors are actively maintaining the privacy of the sensitive data and computing resources and preparing independent auditor's report.

Phase 8 Closing the relationship: In last phase of the cycle, data is transferred and unused data are cleaned up. Acknowledgement message is also transferred from the user and even related organization end. And the concerned vendor will be getting ready for the next transaction.

2.3 Auditing Aspects

The auditing aspects[10] in Cloud Computing Environment are discussed as follows:

1. *Auditing for regulation or compliance*: A set of rules and principles are designed to govern or control the conduct for auditing. Compliance is concerned with legal issues, social activities, marketing strategies, and co-operative conduct. In every aspects of compliance, auditing is highly needed for maintenance of governing conduct. Auditing for regulations and compliance is also needed to restrict increasing complexity to comply with standards and to maintain the agreement for privacy laws.

2. *Auditing for Risk and Governance*: Governance is exceedingly concerned with the performance measurement & its strategies and risk management & its proper administration is also an important issue of an IT landscape. Different management laws and policies, priority & resources needed for the processes, alignment of customs are the basic functionalities of this category.

3. *Auditing for security*: Security issues are the concern for auditing. In the administration security, everyone should know the responsibilities of each designation. Technical auditing is also concerned with security issues.

Physical resources are also in need of auditing for its priority, availability and cost complexity.

4. *Database Auditing*: Database auditing is related with observing a cloud database so as database auditors and administrators can take care of the actions like accesses, modifications, updating issue of the database users. Database auditing is mainly query-based auditing. Queries are presented to the auditor one at a time; auditor checks if answering the query combining with past answers reveals the secret or forbidden information.

5. *Service level agreements (SLAs) Auditing:* In Business Service Provider (BSP) layer [2], SLAs is concerned about business-oriented agreement and laws. So in every level of agreements, auditing is highly required to maintain to proper usage of laws and terms & conditions.

6. *Third Party Storage Auditing Service Provider*: Considering Cloud data storage and database service, four different entities are there in Third Party Storage Auditing Service Provider, as shown in the [Figure1]: The Cloud user, hosting machine in Cloud Service Provider (CSP), Cloud Database Server (CDS) and Third Party Auditing Service (TPAS). The cloud user, having a huge amount of data files which is to be stored in the cloud. The Cloud user interacts with hosting machine in CSP through Cloud-based user Interface and deploys various applications. They may also dynamically communicate with CDS for storing and maintenance of their data files. While deploying their various applications onto host machine, the users may rely on TPAS in assuring the confidentiality, availability and integrity of their outsourced data to preserve the privacy of their own data. TPAS is capable of maintaining the privacy of user-data and can be trusted as it may review the cloud database storage reliability in support of the cloud user upon request. An unauthorized user can put a set of intelligent queries to the database server, of which none of the query is forbidden. So the unauthorized user, combining the set of replies, may get the secret information which is forbidden. Hence TPAS has the responsibility to maintain the privacy of user data.

Journal of Theoretical and Applied Information Technology
10th July 2014. Vol. 65 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

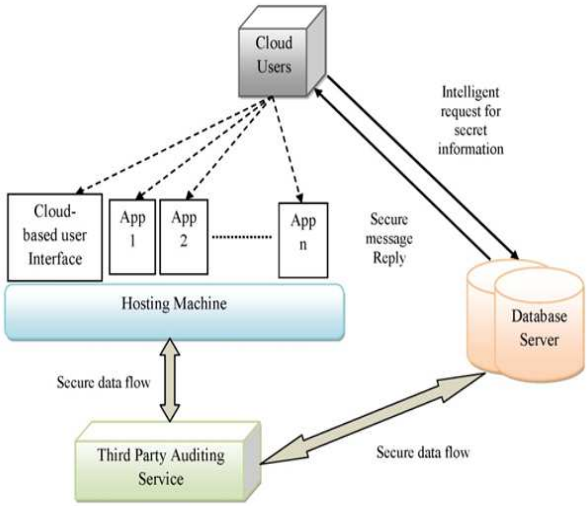

Figure 1: Cloud Data Storage Scenario

3. AUDITING FRAMEWORK

Considering Cloud data storage scenario as given in [Figure 1], we have proposed the framework for auditing technique as shown in[Figure-2] which consists of four entities namely: i)Cloud User or Cloud Subscriber who may either deploy its application or use the Cloud services or use the cloud data storage. ii) Service Broker which maintains the relations between Business Service Provider Layer and Virtual Appliances layer [2] has the responsibility to manage the user-applications.iii)Hosting Service or we can say, the Cloud Service Provider (CSP) provides infrastructure elements for metered usage, service level policy and license management, and authentication control [12]. And iv) Auditing Service which maintains the privacy of the sensitive data, restricted access of computing and physical resources and for integrity check, is responsible for database and policy auditing from log server.

3.1 Service Broker

Cloud subscriber if wants to deploy its application or to use the service, it has to register itself in the broker server that facilitates services like register, request, monitor & manage. So that the service broker can maintain the user-log in the log server and can deliver it to the auditing service. The major aim of the service broker is to arrange the applications optimally so that it can easily monitor the requests of applications and can manage the configuration of the platforms. Then the deployment request is being delivered to the hosting service. While handling the request, we have to consider a directory service which acts as a depository for the credential, identity, and user attributes of the users of the organization. This directory service directly interacts with Identification Management Service (IMS) and Authentication Access Management Service (AAMS).

Journal of Theoretical and Applied Information Technology
10th July 2014. Vol. 65 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

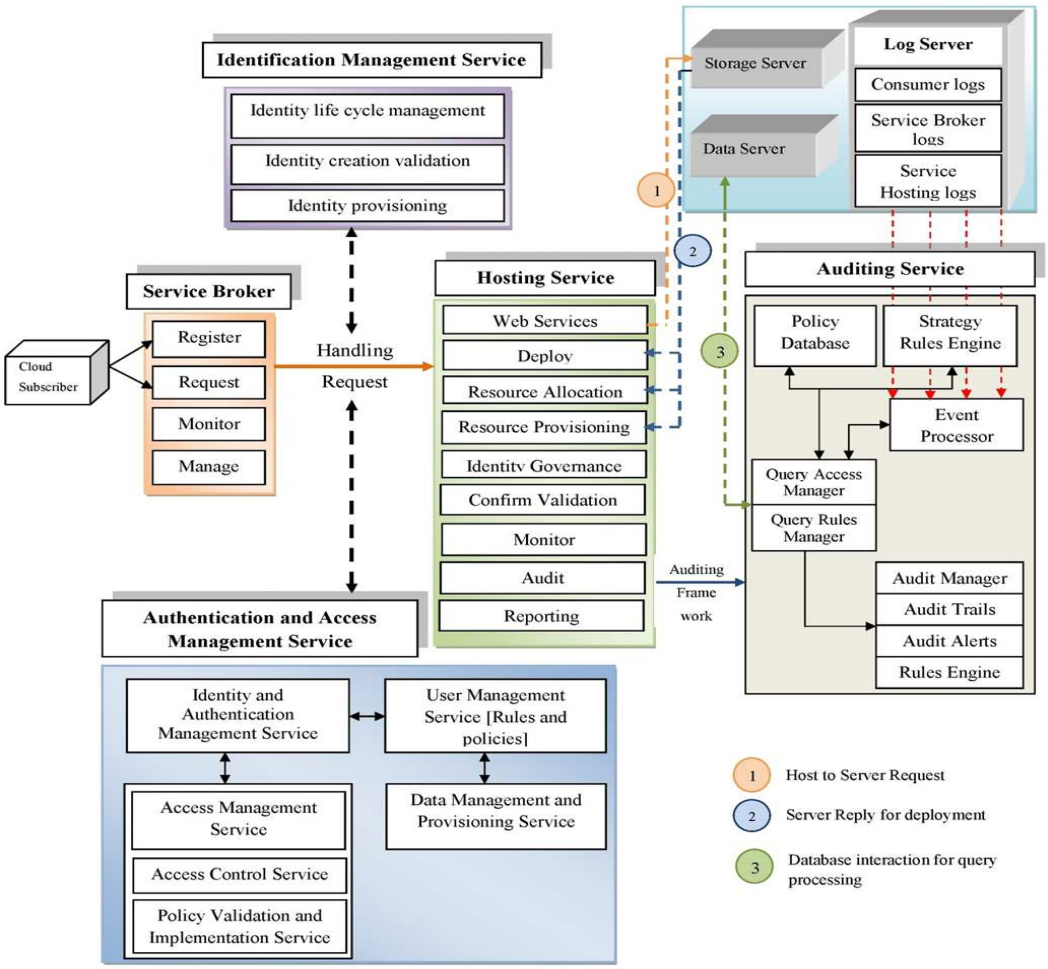

Figure 2: Framework for auditing technique

3.2 Identification Management Service (IMS)

IMS technology consists of life cycle management module, creation of validation module and provisioning module. Life cycle management module identifies different phases when an organization is renting the Cloud infrastructure from the CSPs or going to deploy its user-application onto a cloud. Creation of validation module identifies the proper validation for deployment of user-application. Provisioning is the process which provides users with essential access to data and technology resources. Hence this module is responsible for identification of proper provisioning of resources.

3.3 Authentication and Access Management Service (AAMS)

AAMS comprises of identification and authentication management service, user management service, data management and provisioning service, and access control service module. Identification and authentication management service is responsible for effective governance and management of the proper process. User management service is associated with the rules and policies, and management of identifying life cycles. Data management and provisioning service is responsible for propagation of identifying data for authorization to IT resources. Access management and access control service module enables the rules and policies for access control in response to a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

request from any user or services which are in need of IT resources

within theorganization. Access control service is also responsible for user access management, user responsibilities, network access control, and operating system access control. Policy validation is the important module for validating and implementing the policies.

3.4 Hosting Service

In Cloud Service Provider, hosting service consists of different modules. Web services are meant for interfaces through which users and service brokers interact with the service providers. When all the identification and authentication is done, user application is deployed onto the host machine and host machine make a request for physical resources from Resource as a Service (RaaS) layer through Virtual Machine Manager (VMM) or hypervisor [2]. Then the resource layer allocates the necessary resources for the particular application and physical & virtual resources are immediately provisioned according to the need of the user. In this workflow, identity governance is essentially needed for recognizing virtual machine ID and datacenter ID so that host machine can easily identify the proper request related concerns. After verifying the identifications, host machine confirms the validation for resource allocation. Monitoring, auditing, and reporting compliance by cloud subscribers regarding access to pool of physical resources like Servers, networks, bandwidth, storage, and data center space [2] within the organization depend upon the defined policies. Monitoring service is also responsible for detecting unauthorized information processing activities. After this the Auditing Service plays an important role to preserve the privacy of the user data and application related concerns.

3.5 Auditing Service

Auditing Service consists of Policy database, Strategy rules engine, Event processor, Query manager having two modules like Query access manager and Query rules manager, and Audit control module comprising of Audit manager, Audit trails, Audit alerts and Rules engine. Policy database is the repository of information security policies that provide management direction and support for information security according to the business requirements and relevant laws, policies and regulations. Strategy rules engine defines the strategy plan about the implementation of security policy, asset management, communications and operational management, information systems acquisition & development & maintenance, and business continuity management. Event processor is the most important module in auditing service. Event processor is associated with the dynamic change in the user-events and related with the log server. Log server comprises of consumer logs having details of cloud subscriber details like user ID, usage time

etc., service broker logs containing broker ID and broker details, and service hosting logs having virtual machine ID, datacenter ID, resource usage, storage details etc. Event processor, maintaining all the log tables from log server, also has the authority to set the priority to the events and process activities. Query Access manager manages and controls the access of query processing unit in authorized way and query rules manager set the rules for query processing. These two modules directly interact with the database server for query processing. While processing the database query, it is in need of query audit. Audit manager manages the overall auditing process, whereas audit trails have the responsibilities to trace the unauthorized query and audit alert makes an alert in case of unauthorized query access. Therefore, a set of auditing rules and query accessing policies are made by rules engine.

4 . CONCLUSION

In Cloud Computing Environment, auditing is required to ensure the privacy, data confidentiality, integrity and availability. We summarize our work as follows:
The auditing framework includes all the phases that are intended to access or store the information in the cloud through the Third Party Service Provider. Also this framework shows the communication among the entities like Cloud User, Service Broker, Hosting Service and Auditing service through IMS and AAMS. This framework does not support heterogeneous architectural platform. Federation of audit logs from distributed sources across multiple domains creates a problem for proper auditing. Hence it is difficult to get audit-based access of physical/ network-based resources. So these types of issues have been left for future directions.

-

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES:

[1] V.Sarathy, P.Narayan, Rao Mikkilineni, "Next generation cloud computing architecture -enabling real-time dynamism for shared distributed physical infrastructure", *19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises* (WETICE'10), Larissa, Greece,28-30 June 2010,pp. 48-53.

[2] Souvik Pal and P.K.Pattnaik, "Efficient architectural Framework of Cloud Computing", in *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, Vol.1, No.2,June 2012, pp. 66-73.

[3] M.Jensen,N.Gruschka,R.Herkenhoner,N. Luttenberger,"SOA and Web Services: New Technologies, New Standards – New Attacks", in *5th European Conf. on Web Services,*26-28Nov 2007,pp.35-44.

[4] S. Sundareswaran, A. Squicciarini, D. Lin, S. Huang, "Promoting Distributed Accountability in the Cloud", in *4th IEEE International Conference on Cloud Computing,* 2011,pp. 113 - 120.

[5] R. Hu, W. Doua, X. Liu, Jianxun Liu," WSRank: A Method for Web Service Ranking in Cloud Environment", in *9th IEEE International Conference Dependable, Autonomic and Secure Computing,* 2011,pp. 585 - 592.

[6] W. She, I-L. Yen, B. Thuraisingham, S-Y. Huang, "Rule-Based Run-Time Information Flow Control in Service Cloud", in *IEEE International Conference on Web Services*, 2011,pp. 524 - 531.

[7] R. Buyya, C.S. Yeol, and S. Venugopal (2008) "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities",in *Proc. of 10th IEEE International Conference on High Performance Computing and Communications (HPCC'08),*2008, pp. 5-13.

[8] J.Yang, Z.Chen, "Cloud Computing Research and Security Issues",in *IEEE International Conference on Computational Intelligence and Software Engineering (CiSE)*, 2010,pp.1-3.

[9] Heather Paquetle, Tom Humbert, "Cloud Computing-An Internal Audit Perspective", March 10, 2011.

[10] Jonathan Sinclair, "Cloud Auditing", SAP Research.

[11] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", *2010 Proceedings IEEE INFOCOM*, 14-19 March, California,2010, pp.1-9.

[12] Rajkumar Buyyaa, Chee Shin Yeoa,Srikumar Venugopala, James Broberga, and Ivona Brandicc, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility",*Future Generation Computer Systems, Volume25,Issue6*, June2009,pp. 599-616.

[13] Rui Xie,Rose Gamble," A Tiered Strategy for Auditing in the Cloud", *IEEE International Conference on Cloud Computing*,June 2012,pp. 945-946.