International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP—28-35

Understanding the Mass Storage and Bringing Accountability

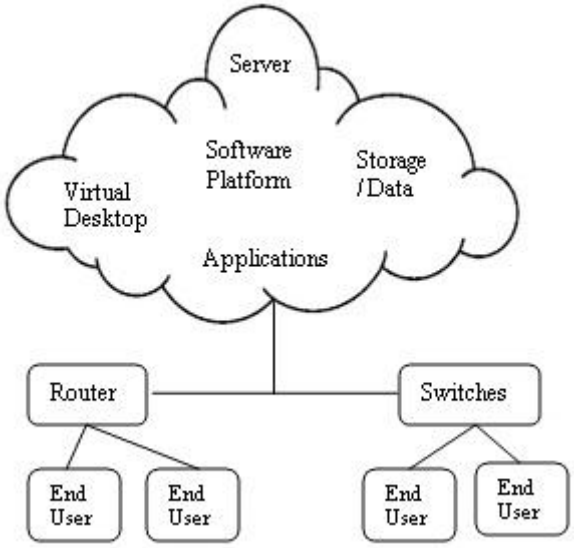
Biswajit Nayak [1], Sanjaya Kumar Padhi[2], Prasant Kumar Patnaik [3]
[1](*Sri Sri University (SSU), Odisha, India)*
[2](*Biju Patnaik University of Technology (BPUT), Odisha, India)*
[3](*Kalinga Institute of Industrial Technology (KIIT) University, Odisha, India)*

ABSTRACT: *Cloud computing is becoming gradually more well known and accepted among very small to big size businesses. Technology provides facility to work on shared resources as well as the same document in real time. Such facility grabs the immense attention among users, individuals at home and also different organization and government bodies since it provides such facility for us as anyone can ~~to~~ access his or her information from anywhere at any time. In the context of cloud computing, accountability is meant to develop a comprehensive approach to achieve privacy, trust, accuracy and security in the cloud, encompassing Legal, Regulatory and Technical Mechanisms.*

KEYWORDS: *Accountability, Cloud, Log Services, Service Level Agreement.*

I. INTRODUCTION

Cloud computing is a internet based technology that enables user to access convenient pool of shared computing resources like- services, storage, servers, applications and networks on demand which can be provisioned rapidly and managed with minimal interaction with service provider or low management effort.



(Fig.1.1 Process of Cloud Computing Environment)

The location of physical resources and devices being accessed are typically not known to the end user. End users don't have the knowledge regarding the location of resources and devices which are used. In case of Cloud computing, a large pool of devices/systems are connected in several deployment models that may be private or public networks, to provide confidential , accountable and dynamically scaleable infrastructure for different application, data and file storage. In case of Cloud computing technology cost of computation is minimised along with hosting of application, content storage and delivery significantly. It can be accessed from all over the world through the device, it is connected. [1][2].

II. CLOUD COMPUTING BENEFITS

There are some benefits on the basis of which the popularity of cloud computing increases. They are listed as:

A. Self Healing:

Some systems have the ability to correct itself for normal operation. The property which describes that a device or system can make out that the system not working correctly and makes the necessary adjustments to restore itself to perform usual operation without human interference.

B. Multi-Tenancy:

It is a concept where multiple customer or tenant shares a particular instance of a application software in a single instance of time while preserving the privacy or security of the users or their data respectively.

C. Linearly Scalable:

It is an application which means the system can be able to break down the work load and also can scale just by adding and service it across the infrastructure.

D. Service-Oriented:

It means, if we need a large logic to solve a problem then it better to construct by decomposing it into smaller parts and each part is solved by individual logics. Many such individual units of logic combined together to form service.

E. Reduced Cost:

As the infrastructure of cloud not purchased, the cost of establishing infrastructure is not there only maintenance cost is there and that is very low. In addition to this, it also minimises the cost of initial and recurring expenses. Payment of bill is also as per the use.

F. Increased Storage:

Cloud storage is a model that provides facility for large data store. Maintenance of large volumes of data is also provided by cloud providers. There is no restriction for storage capacity of cloud and it can scale dynamically.

G. Virtualized:

Virtualization is a concept where applications are separated from underlying physical hardware. It makes possible to run multiple applications as well as operating systems at same time and server.

H. Flexible:

It provides the flexibility to access data from anywhere from the world. It also provides to provide large variety of applications. To change the business condition, enterprises adapt the condition more rapidly, but the most critical thing is speed to deliver. Cloud computing takes the responsibility for getting applications to market as much quick as possible, through the proper elements required for deployment.[1][2][3]

The use of cloud motivation comes from certain factor like cost, scalable, speed of development, improving access facility, freeing up internal storage/compute cycles, mobility of workforce, regulatory compliance, and access to compute cycles.

III. DEPLOYMENT MODELS

A. Private Cloud

The private computing is a dedicated infrastructure to a particular organization and not shared with other organizations. It is more expensive as it owned by single organisation and also more secure with respect to the other cloud models. It can be of two types (a) On-premise private clouds and (b) externally hosted private clouds. On-premise private clouds are hosted by organisation itself where as Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party but used by one organization. Externally hosted private clouds are cheaper than On-premise private clouds.

The main idea of deploying a private cloud in an organization is to utilize the existing internal resources, so that security and privacy will be more. The data transfer rate can also be minimised.

B. Public cloud

Like private cloud it is not a dedicated infrastructure to a particular organization rather is hosted by the third party or cloud vendor at the vendor's premises. The customer is not aware of where this infrastructure is deployed or hosted. Customer has no control over the deployed computing infrastructure. It can be shared among any organisation.

C. Hybrid cloud

As it is the combination of private cloud and public cloud, the organizations may host applications with high security concern, on private clouds where as the applications with comparatively not as much of security concerns on the public cloud. In this environment, organization uses their own computing infrastructure for normal usage but accesses the cloud using services. This guarantees that a sudden increase in computing requirement is managed elegantly.

D. Community cloud

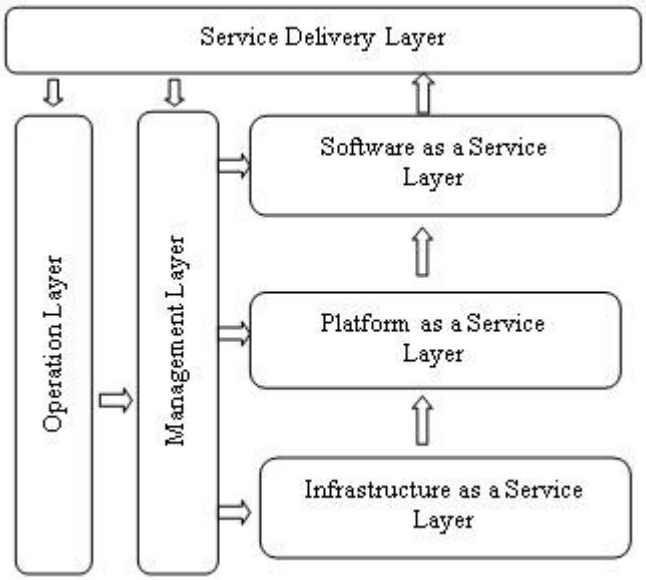
This is the cloud which allows multiple organization of same community. It emphasises on sharing between organizations. It is the use of multiple cloud computing services in a single diverse architecture to minimise dependence on single vendors, enhance flexibility through choice, mitigate against disasters, etc. It is

more secure than public cloud. It disagrees with hybrid cloud as it emphasis on multiple cloud services, rather than multiple deployment modes. [3][4]

IV. CLOUD BASED DELIVERY

A. Software as a service (SaaS)

The SaaS provides the facility to deploy software on cloud. This software is accessed through internet. Maintenance of software is carried out by the cloud provider. There are several applications like CRM applications, HR solutions, etc. The end user need not required to install any specific software and also don't require for maintenance so this means it is also cost effective for end user. Cloud applications run and maintained on the server of cloud. The system administration of SaaS may deploy the applications on several servers but it enables the end user be capable of accessing the application without installing at local system. SaaS provides the service on-demand to the end user.



(Fig.4.1 Different Services for Cloud Consumers)

B. Platform as a service (PaaP)

Platform as a service is service which provides platform to develop, run and manage the system. It provides software or development environment, which is encapsulated & offered as a service and other higher level applications can work upon it. The Platform as a service allows customer to create his own applications on cloud infrastructure provider and run. Platform as a service providers offer a predefined combination of OS and application servers. The most known instance is "Google's App Engine".

C. Infrastructure as a service (IaaS)

It is defined as the hardware made available as service (NIST). It is possible only because it supports the concept of virtualisation that means the server, storage, application, network available for all existing in the cloud. This is the equivalent to infrastructure and hardware in the traditional (non-cloud computing) method running in the cloud. It allows essential storage and computing capabilities as standardized services over the network. It pooled Servers, storage systems, network, data space etc. and made available to manage workloads. It allows customer to set up his own software on the infrastructure. The most known instance is "Amazon". [4][5].

V. ACCOUNTABILITY IN CLOUD

Accountability ensures the trust among the users and the service providers of cloud. is a mechanism which makes the system accountable and helps to increase the trust among the cloud users and the cloud service providers. It defines the way through which storing, accessing, sharing and processing of the data occurs in the cloud computing environment according to the service level agreement. It also observes the lack of control over the data and service or breach of SLA.

Accountability can be achieved by using log to the events, services and applications running on virtual machine and making audit to these actions. Accountability also acts as a responsible steward of the individual information of someone else, to provide safeguard and proper use of that individual information ahead of legal requirements. A few major sections of accountability are transparency, responsibility, assurance, and remediation. Responsibility of an organization should be to report, explain and answerable to the decision with

respect to the data protection. It is an approach of accountability with respect to the current thinking and requirement that an organization should:

- Positive approach to accountability.
- Establish policies that should include be aware of external criteria.
- Provide transparency and mechanisms for entity participation.
- Provide transparency for sharing policies with stakeholders and ask for feedback and advice.
- Make clear documentation and communication regarding ethical code, mechanism to implement policies which will be supported by all level in the organization.
- Consent to validation.

It is a legal responsibility on an organization to ensure that the data it supplies are agrees with the other. [6][7]

VI. ATTRIBUTES OF ACCOUNTABILE CLOUD

Accountability for an organization emphasis on ensuring responsibility for data with which it is entrusted in a cloud environment, for its use of the data from the time it is collected until when the data is destroyed. Some of the attributes of accountability model are: [13][14]

- Transparency: It is the property of providing clarity of managing rules, behavior and the facts of behavior according to the rule of a system, organization or individual.
- Responsiveness: It is a concept refers to the ability of a system or organization to complete the task in given stipulated time period.
- Remediability: It is the property to take action that will correct and /or provide remedy for the part or full failure of the system, organization or individuals according to the rule.
- Responsibility: It is a property that considers some inputs from stakeholders or external stakeholders and responds to their queries. The property may be of a system, organization or individual.
- Verifiability: It is a property of system or organization that enables to check the behavior in opposition to the norms.
- Appropriateness**:** It is the property of system, organization or individual that ensures the quality is just right as per the requirement.
- Effectiveness: It is the property of system, organization or individual that accomplishes and expecting the measure actually contributing to the accountability.

VII. CLOUD ACCOUNTABLE CHALLENGES

A. Isolation failure

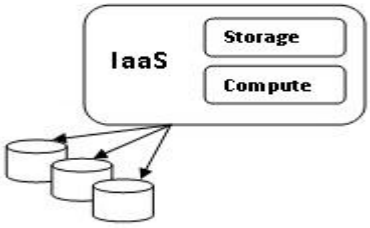
Cloud computing support the concept of sharing of resources and multi-tenancy. So if one tenant of cloud affects the resources of another then it is called isolation failure. It may leads to the insecurity of private data. The figure Fig-7.1 represents the isolation failure. [12][13]

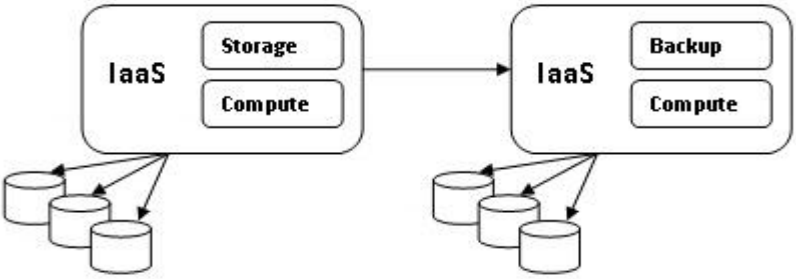
B. Compliance Hazard

The concept of cloud compliance arises when there is a use of cloud back-up or storage services. When the data moves from one place to another then it requires examining what data should be moved and what should be kept inside and what question should be asked to cloud provider. Data flows are dynamic. So the cloud compliance hazard should not be there. The figure Fig-7.2 represents compliance hazard.

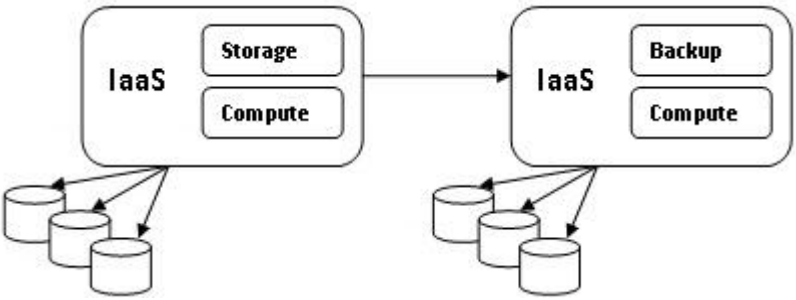
C. Incomplete Data Deletion

The cloud computing supports the concept of sharing resources that means one resource can be shared by numbers of user. For the purpose of data security cloud stores the data in more than one storage places of cloud environment. When one wants to delete data then it will not be easy because data stored in more than one places or resource are shared. The figure Fig-7.3 represents Incomplete Data Deletion Challenges.





(Fig.7.1 Shows Isolation Challenges) (Fig.7.2 Shows Compliance Challenges)



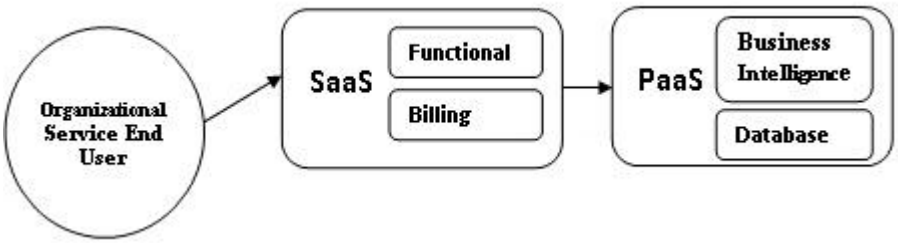
(Fig.7.3 Shows Incomplete Data Deletion Challenges)

D. Lock-in Hazard

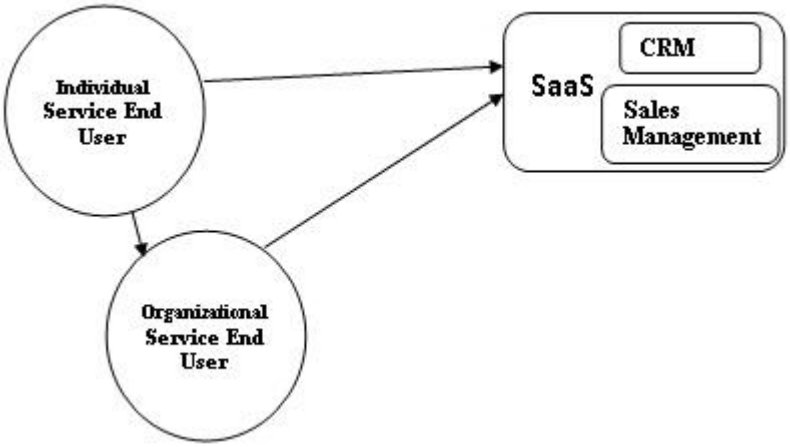
Lock-in restrict to migrate or transfer data from one provider to another so that the portability and interoperability reduced and increases the frustration for the cloud computing user's to take advantages of cloud computing benefits. For example, to move from one Customer Service Management (CRM) to different Customer Service Management (CRM) it is very difficult. The figure Fig-7.4 represents Lock-in-Hazard Challenges.

E. Loss of Governance

Cloud consumer should have the sufficient control over cloud provider and several service issues. If the service level agreement fails to provide the committed services then there will be loss of governance. For which it is required to take back-up for the important data. The figure Fig-7.5 represents Loss-Governance Challenges.



(Fig.7.4 Shows Lock-in-Hazard Challenges)



(Fig.7.5 Shows Loss-Governance Challenges)

VIII. BUILDING BLOCKS FOR AN ACCOUNTABLE CLOUD

Here we planned to explain the different parameters that are responsible or could form the basis to build an accountable cloud. From these parameters, for some of the parameters, we can proceed based on some existing work; others have yet to be developed, and we simply draw them here.

A. Tamper-evident logs

It is a solid technology which can be a basis for accountable clouds. It is used to recognize the earlier acts of customer, provider, users, and cloud machines. Each knob keeps a record in which it not-only keeps all of its inputs and outputs to or from the system respectively but also keeps messages, which it sends or receives. Some other nodes are allowed to audit this record.

B. Virtualization-based replay

Due to this, it is possible to run unchanged s/w in VM and it can be possible to keep track of non deterministic event or inputs. At the time of audit, it is possible to reproduce this execution by any other virtual machine having identical image and through injecting the input or event at the time of execution and also at same time. Thus we can get the accountability.

C. Trusted Time Stamping

The above two technique generally used to detect incorrect executions, and this can be one thing which a cloud customer might be interested in detecting. Service level agreement is another most important problem. Trusted time stamp uses or add timing information to the previous technique known as: tamper-evident log. For example, we can periodically include in the log a certificate from a trusted third-party time stamping service.

D. Sampling

Another way is the samplings where you will realize a probabilistic assurance, as the cloud perform regular checkpoints and by allowing the customer to investigate or audit segments between checkpoints randomly. Since several problems will affect many or most of the segments, the customer can still detect them with high probability even if the sampling rate is low. It is good because it is impractical for most of the application to check the performance of the first by taking second cloud.

E. Challenges

Confidentiality: accountability can't be achieved at least not without the use of heavyweight primitives such as dynamic taint analysis.

Legacy users: Users those who uses cloud without temper-evident record or log. It is possible to deploy proxies to add accountability to a legacy web server. This is one of the better solutions.

Performance: Although there will be overhead. It will be manageable. [10][11]

IX. HOW TO PROVIDE ACCOUNTABILITY IN THE CLOUD

Accountability can be achieved by designing various mechanisms, procedure and technical measures to support the approach. The cloud is a special example of how businesses must assess and manage risk better. For that some preventive control like policy enforcement, obfuscation techniques, identity management, decision support tools and risk analysis must be there. In addition to preventive control it also required some detective controls. Using preventive control prospective accountability can be achieved where as Retrospective accountability can be achieved by using detective controls. Detective control can be achieved through tracking, auditing, , monitoring and reporting. It also requires corrective control that helps to fix the undesired outcomes.

To provide accountability, it also required determine cloud service provider's capabilities, the organisation also required to appoint data protection officer and encryption for data security, privacy and trust as technical measures. [10][11][12]

A. Mechanisms for Achieving Accountability in the Cloud

Accountability is the major part of data in the cloud. [14][15] There are various mechanisms through which accountability can be achieved in the cloud as follows:

- A service-level Management (SLM)

A service level management is carried out with SLA.SLA is an agreement or contract between service provider and service user. Contract occurred to provide service like scope, responsibilities, performance and quality. It is also responsible for various data rate, throughput, reporting faults, jitter, paying fees and other measurable details.

- Incident Management

It is a new direction for area of research which focuses on accomplishing forensic investigations, discovery and other security issues because of multi-tenant, virtualized environment, along with any standards that need to be followed. An Incident can be described as an event that occurs outside the standard operation plan and that may show the way to reduce or interrupt the quality of service. Incidents, in Cloud Computing, can lead to service shortages at different levels of infrastructure like: IaaS, PaaS and SaaS.

The objective of current research focus on addressing a series of research challenges pertaining to the Cloud Incident management field.

Automated management of incident prevention, detection and response also recovery via clear service level agreement commitments and uninterrupted supervising will enhance reliability, resilience, availability, trustworthiness and even accountability of CSP and clients.

- Trust Management

It is an effective approach that enables us not only to assess but also to establish trusted relationships. From certain approaches trust management can be classified into two different prospective: a) Service Provider Perspective (SPP) and b) Service Requester Perspective (SRP). In SPP, is system that is responsible for service requesters' trustworthiness .It is the main driver of the trust management system where service requesters' trustworthiness is assessed. On the other hand, in SRP, is a system that is responsible for the service who evaluates the trustworthiness of the service provider.

- Policy Enforcement

A general policy enforcement framework for cloud data management1 must consider three important dimensions: a) Data type, b) Computation and c) Policy requirements. Data type may deal with text data, relational data, etc. Computation may deal with SPARQL, SQL queries, etc, and Policy requirements may deal with data sharing policies, access control policies, etc.

- Impact Assessment

This is the concept says about information that is identified and explains the way the gathered information is maintained, protected and shared. It is also responsible for checking:

- ✓ Legal and regulatory information which are being collected.
- ✓ Possible risks present in collecting, maintaining and disseminating information.

- Audit and Certification

Audit is a concept in cloud computing that provides CSP to make their performance and secure data voluntarily available for their clients. The pattern provides facility to give a standard way to present and share detailed, automated statistics about security as well as performance. Looking for a way to benchmark your cloud computing you need extra edge cloud computing certificate. [13][16]

X. CONCLUSION

It is always important to defend and maintain data confidentiality or privacy on the Internet. This is only because to protect from unwanted and unauthorized disclosure of their private or confidential data. This analyses cloud based framework, which is used for generating, storing, and optimizing data storage in cloud. Our approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Because accountability is all about to achieve trust and confidentiality.

REFERENCES

[1] Theoharidou. M., Papanikolaou. N., Pearson. S. & Gritzalis. D. (2013), "Privacy Risk, Security, Accountability in the Cloud*"*, *IEEE International Conference on Cloud Computing Technology and Science*, Page(s):177-184, DOI 10.1109 /Cloud.Com. 2013.31.

[2] Yao. J., Chen. S., Wang. C., Levy. D. & Zic. J. (2010), "Accountability as a Service for the Cloud", *IEEE International Conference on Services Computing*, IEEE, Pages-81-88, DOI 10.1109/SCC.2010.83.

[3] Begum. R, Kumar. R. N. & Kishore. V. (2012), "Data Confidentiality Scalability and Accountability (DCSA) in Cloud Computing", International *Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 11, ISSN: 2277 128X.

[4] Armbrust. M., Fox. A., Griffith. R., Joseph. A., Katz. R., Konwinski. A., Lee. G., Patterson. D., Rabkin. A. & Stoica. I. (2009), "Above the clouds: A Berkeley view of cloud computing", *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28,*.

[5] Dash. S. K., Mohapatra. S. & Pattnaik. P. K. (2010), "A Survey on Applications of Wireless Sensor Network Using Cloud Computing", *International Journal of Computer Science & Emerging Technologies,* Volume 1, Issue 4, E-ISSN: 2044-6004.

[6] Sundareswaran. S., Squicciarini. A C. & Lin. D. (2012), "Ensuring Distributed Accountability for Data Sharing in the Cloud", *IEEE Transaction on dependable a secure computing*, VOL. 9, NO. 4, pg 556-568.

[7] Doiphode. N. P &. H. P. Channe. H. P. (2015), "A Survey on Accountability of Data usage in Cloud Computing", *International Journal of Science, Engineering and Technology Research (IJSETR),* Volume 4, Issue 3.

[8] Pearson. S. (2011), "Toward Accountability in the Cloud", View from the Cloud, IEEE Internet Computing, IEEE Computer Society, July/August issue, vol. 15, no. 4, pp. 64-69.

[9] Ko. R. K. L., Jagadpramana. P, Mowbray. M, Pearson. S, Kirchberg. M, Liang. Q, Lee. B. S. (2011), "TrustCloud: A Framework for Accountability and Trust in Cloud Computing," *2nd IEEE Cloud Forum for Practitioners*. Pages 1-8.

[10] Wang. B., Li. B. & Li. H. (2014), *"*Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", *IEEE 5th International Conference on Cloud Computing*.
[11] Haeberlen. A. (2010)," A Case for the Accountable Cloud", *ACM SIGOPS Operating Systems Review*, Pages 52-57, Volume 44 Issue 2, doi>10.1145/1773912.1773926.
[12] Jaatun. M. G. & SINTEF (2013), "Accountability Challenges for Cloud Computing", *Trust in the Digital World and Cyber Security & Privacy EU Forum Brussels*, (http://A4Cloud.eu)
[13] Nakahara. S. & Ishimoto. H. (2010), "A study on the requirements of accountable cloud services and log management ",*8th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT), IEEE*, Page(s):1 - 6
[14] Jaatun. M. G., Pearson. S., Frederic Gittler. F. & Ronald Leenes. R (2014), "Towards Strong Accountability for Cloud Service Providers", 6th International Conference on Cloud Computing Technology and Science, IEEE,DOI 10.1109/CloudCom.2014.123, Page(s):1 - 6
[15] Acheampong. F. & Vimarlund. V. (2016), "Innovating Healthcare through Remote Monitoring: Effects and Business Model", *International Journal of Information System Modeling and Design*, Volume 7, Issue 1.
[16] Kan. Y. & Jia. X. (2013), "An efficient and secure dynamic auditing protocol for data storage in cloud computing", *IEEE Transactions on Parallel and Distributed Systems,* Volume 24, Issue 9.