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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Authorized Auditing of Big Data on Cloud Storage

Prof. Vijay Sonawane [1], Sachin Kore [2] , Rajendra Mane [3], Ajay Pawar [4], Punam Adling [5] , Vaishali Gorhe [6]

Prof, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India.[1]

B.E Student, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India.[2]

B.E Student, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India.[3]

B.E Student, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India.[4]

B.E Student, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India [5]

B.E Student, Dept. of Computer, Bhivarabai Sawant Institute of Technology & Research Wagholi, Pune, India [6]

ABSTRACT: As the popularity and the proliferation of cloud storage increase, data security is be- coming one of the biggest concerns for users of cloud storage. How to preserve the data integrity, as one of the most important security aspects, has been a research hotspot in the field of cloud security. Many data auditing schemes for checking the data integrity have been presented, however, these schemes are based on the assumption that the third party auditor (TPA) is secure and trustworthy. If TPA becomes wicked, these schemes are easy to make cloud server suffer distributed denial-of-service attack. In order to deal with this problem, we propose an authorized auditing scheme with constrained auditing number in this paper. In our scheme, only authorized TPA can make valid challenges to cloud for data integrity checking. Moreover, the total auditing number that an authorized TPA can make is decided by the user. In our construction, a constrained auditing number is integrated into the authorization generated by user to achieve this property. Once the number of a TPA's auditing reaches the constraint, cloud server will not respond to this TPA's challenges. Analysis and ex- perimental results show the proposed scheme is secure and efficient.

KEYWORDS:- Cloud storage, Data auditing, Constrained auditing number, third-partyauditor (TPA).

I. INTRODUCTION

Cloud computing is excruciating relate to one of the most authoritative innovations in information technology in recent years. A cloud is a type distributed system consisting of a collection of interrelated and virtualized computers that are dynamically contingency and presented as one or more unified computing resources based on service-level agreements established through negotiation between the service provider and consumers. Cloud service is categorized into Infrastructure-as-aservice(Iaas),Software-as-a-service(Saas),Platform-as-a-service(PaaS).IaaS is the way of providing on-demand computing resources like Server, storage array, virtualized data centres etc. PaaS is providing a higher level Software application which can be companionable to the different users requirement. SaaS is the way of providing some specific applications as fully or partially remote services. It may include web based application or network interactions.

In todays world of digitalization cloud computing has occurred as a concept of handling Big data. This paper focus on the nature, origin and security related issues of the Big Data. Many individual enterprises all over the world for example Amazon AWS, IBM Smart Cloud, Microsoft Azure. Which offers power-full public cloud services to users. Here Cloud based infrastructure, storage, network, high computing performance helps to manage the features of big data.The above services provided by CSS makes the cloud user to be relaxed from burden of storing, managing and providing on -demand service to the client.The overhead incurred by implementing these entire infrastructure by own is reduced somehow. So now days Cloud computing is in great demand .Data privacy/security is the major concerns in

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

adoption of cloud computing[3],[4],[5].User will lose direct control over their data by comparing conservative systems.we will investigate the problem of integrity verification for big data storage in cloud .The issues related to security, integrity and availability of data. There is no direct control of user on cloud. But data integrity can be verified without possession of actual data. Verification done by a trusted third party (TPA) called data auditing. TPA can be anyone challenging the integrity of data stored in CSS.

Our research work aim to add modification that can dramatically reduce communication overheads for verification of small updates.It not only enhance security and flexibility, but also significantly lower overheads for Big Data application with large no. of frequent small update such as application in social media and business transactions.

II. PROPOSED SYSTEM

It is essential to guarantee client about the respectability of their information in cloud. Capacity rightness to guarantee that there exists no bamboozling cloud server that can pass the TPA‟s review without for sure putting away users‟ information intact.The relationship between the cloud client and cloud specialist co-op is straightforward. Cloud client will use the asset of cloud on pay as you utilize premise. The SLA marked between the client and specialist organization is not straightforward. This understanding incorporates the Cloud benefit provider‟s nature of ser bad habit, Standard of the administration, benefit observing and controlling. TPA is there to review the SLA and check if CSS isviolating any govern to conceal its blame. TPA has thelist of inspecting methodology and can check the uprightness of information put away in distributed storage. Security pre serving guarantees that TPA can't get user‟s information content from the data gathered amid inspecting process.. The procedure resembles both CSS and Cloud client will approve the third part evaluator by running different calculations keeping people in general key of customer as normal parameter. When TPA is approved it can send test to Cloud server for checking user‟s information uprightness.

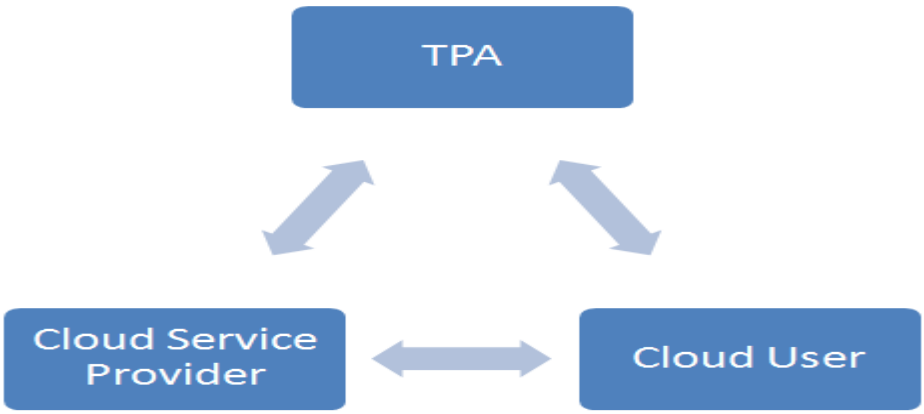


Fig1:Architecture Diagram

Design Goals:

For cloud server, data may get corrupted or lost because of internal and external at- tacks. CSPs are inclined to hide these incidents from users to maintain good reputation. Hence, CSP will try to cheat users when data auditing operation is performed. At this point, CSP may return a proof generated by uncorrupted blocks or even forged data. If TPA is compromised under attacks, authorization information may be disclosed. And ma-

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

licious entity will attempt to modify the constrained auditing number in authorization to sufficient large for DDOS attack. Considering these security threats, the proposed scheme should have the following properties:

1) **Correctness**. Ensure that the cloud correctly storing DO's data can pass data auditing scheme.
2) **Security**. Whenever an adversary against the soundness of our verification scheme causes auditor to accept the proof it provides, there exits an extraction algorithm that can retrieve data back, except with negligible probability [7].
3) **The property of constrained auditing number**. CSS only responds to the TPA that is delegated by DO. And the number of data auditing that can be made with one au- thorization is limited. The constrained auditing number cannot be modified by mali- cious entities.
4) **Low computation and communication costs**. The computation cost for DO to gen- erate authorization for TPA and for CSS to validate the authorization is constant and negligible. And the additional communication cost of checking parameters for TPA validation is very low, comparing to the total size of challenge message.

III. ALGORITHMS

1. Message Digestion (MD5):

MD5 algorithm description

MD5 algorithm takes input message of arbitrary length and generates 128-bit long output hash.MD5 hash algorithm consist of 5 steps:

- **Step 1. Append Padding Bits**
- **Step 2. Append Length**
- **Step 3. Initialize MD Buffer**
- **Step 4. Process Message in 16-Word Blocks**
- **Step 5. Output**

2. Advanced Encryption Standards(AES) :

1. KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. InitialRound
   1. Add-RoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3 Rounds SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   1. Shift-Rows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   2. Mix-Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   3. Add-RoundKey

5 Final Round (no Mix-Columns)
   1. Sub-Bytes
   2. ShiftRows
   3. AddRoundKey

IV. IMPLEMENTATIONS

Various of venture works grew already which can only store information and share information between extensive quantities of client in a gathering. In our proposed work we have exhibited a third party inspecting plan to develop a safe information association instrument with high security assurance technique in addition to likewise dealing with review capacity cognizant information planning framework which is base on need. In this plan the principle

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

qualities are: (1) information security (2) security assurance (3) review points of interest to the information proprietor (4) Auditability mindful information readiness Here we will evaluate the introduction of our future plot in states of the calculation overhead presented by each procedure Calculation trouble: We examine the calculation many-sided quality for the following operations like framework setup, new client concede, new record arrangement and client renouncement and record get to.

- **Software and hardware requirements**

Hardware Configuration
- Processor - PentiumIV 2.6 ghz
- RAM - 512 mbdd ram
- Monitor - 15" color
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard

Software Configuration
- Operating System - Windows XP/7
- Programming Language - Java
- Database - MySQL
- Tool – Eclipse

V. EXPERIMENTAL RESULT

Screen 1 Home Page

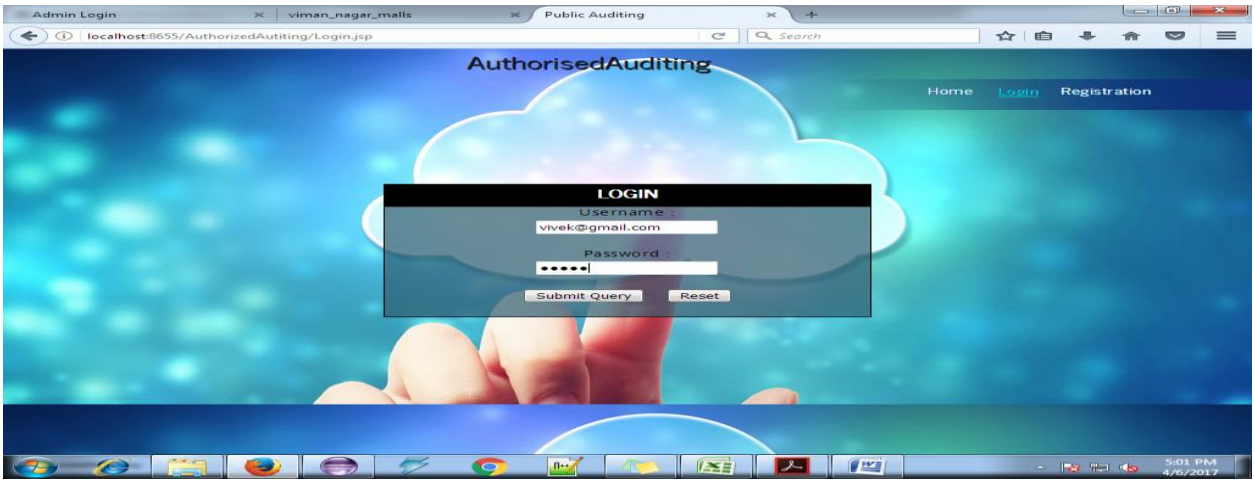
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

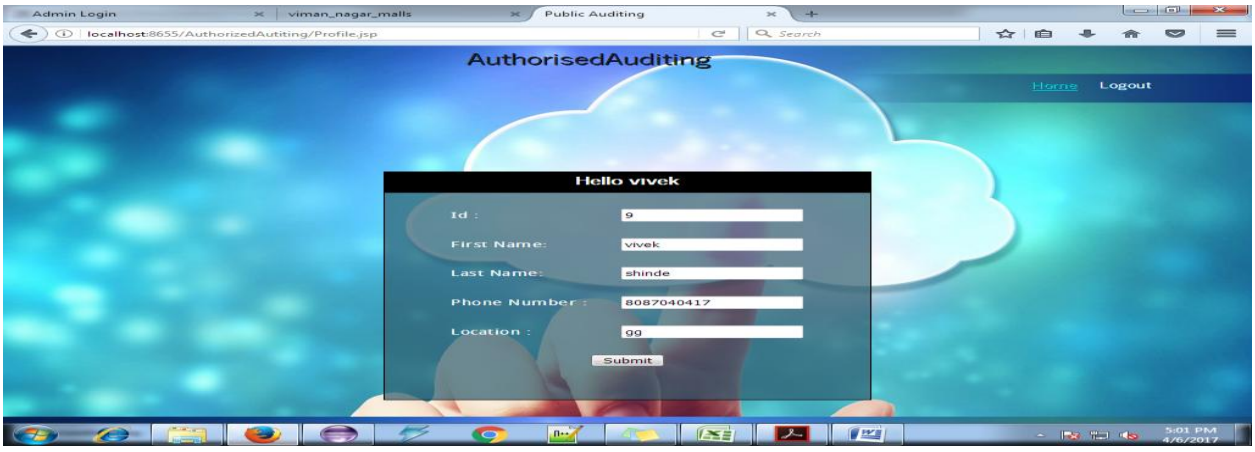
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017



Screen 2 user Login



Screen 3 Profile

Screen 4 All Files

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

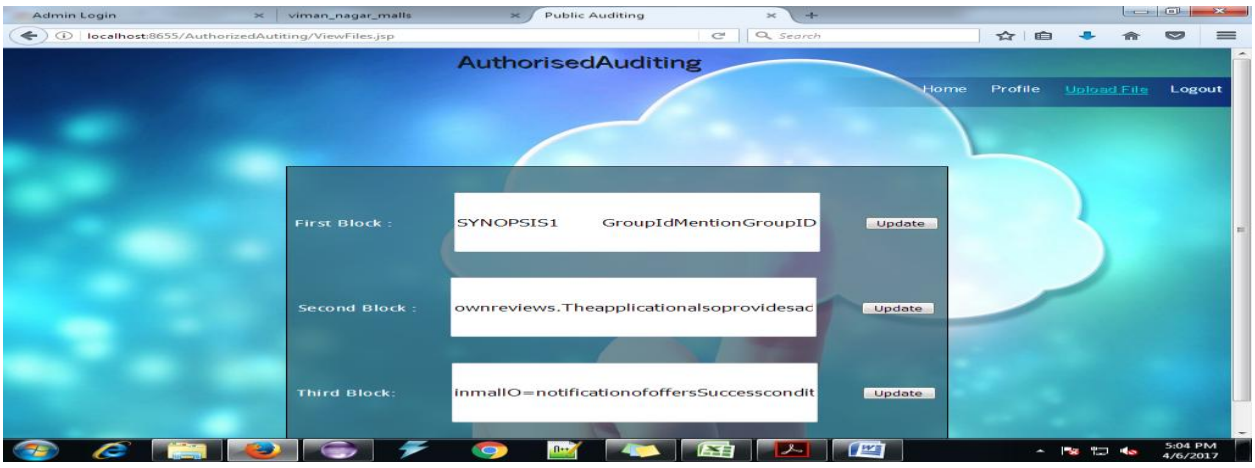
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

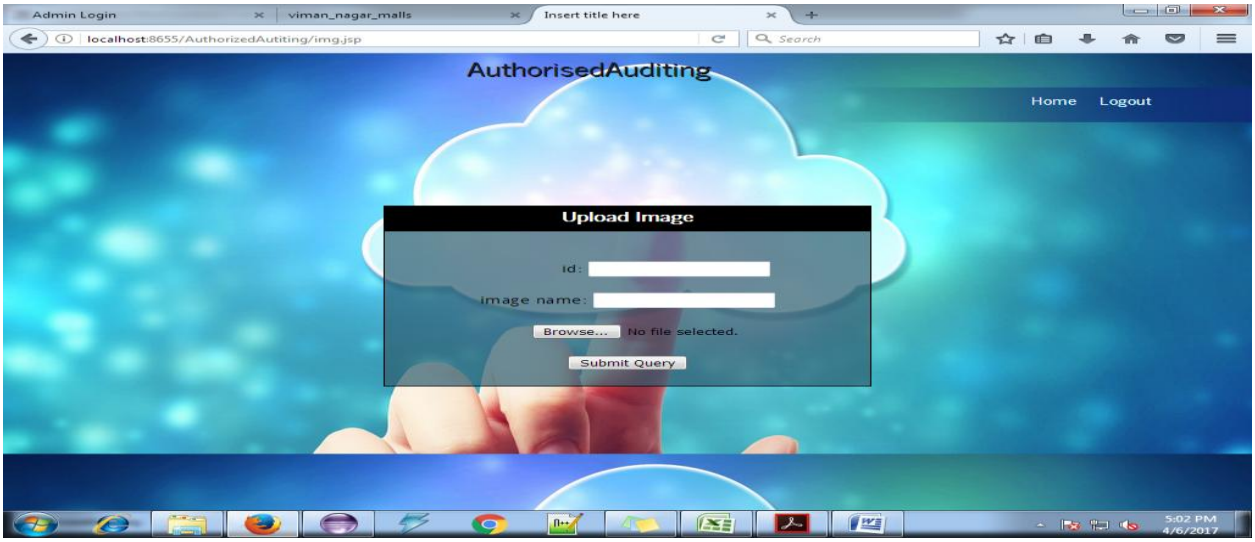
Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Screen 5 Upload File



Screen 6 Show Files



Screen 7 Upload Image

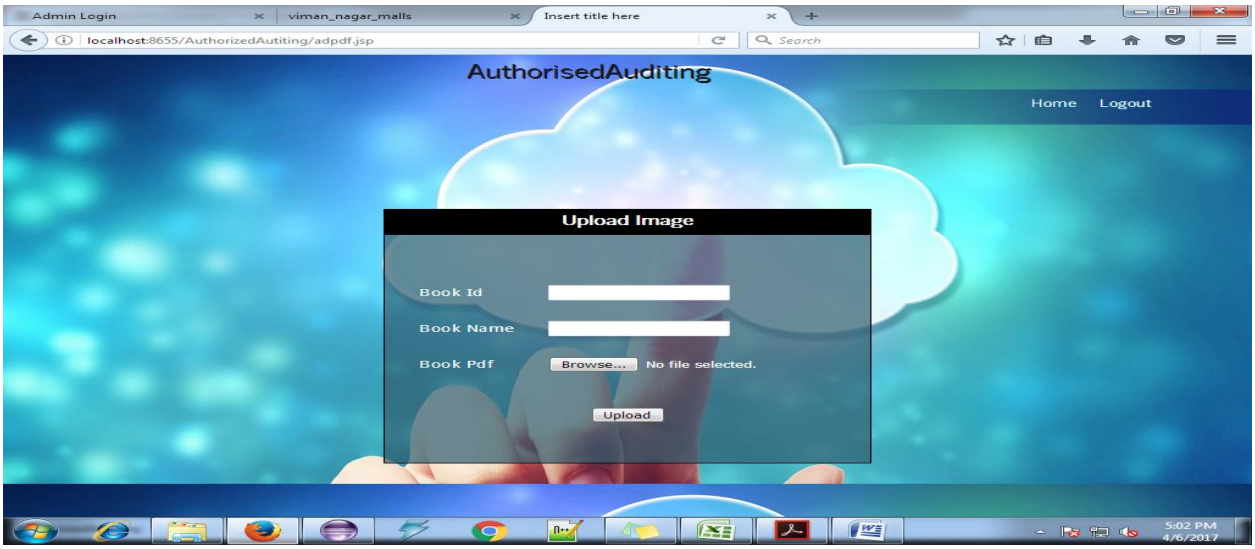
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

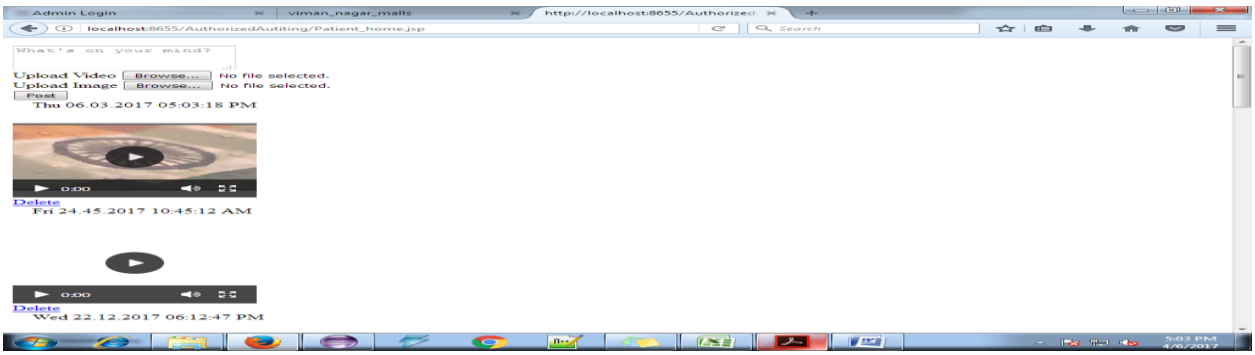
(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017



Screen 8 Upload pdf



Screen 9 Upload and View Video

VII. CONCLUSION

This paper characterizes the formal examination of conceivable sorts of fine grained redesigns and completely bolster approved inspecting and fine grained overhaul requests.We have additionally proposed a change that can drastically decrease the correspondence overheads for the check of little upgrades. Toachieve this we have utilized adaptable information division technique.we have likewise exhibited that it gives improved security and adaptability and essentially bring down overhead for enormous information applications with huge number of regular little upgrades, for example, application in online networking and business exchanges.

VIII. ACKNOWLEDGEMENT

We would like to express my thanks to our guide Prof.Vijay Sonawane for his highly appreciable support and encouragement .Their guidance is a force behind the completion of this paper. We grateful for all the suggestions and hints provided by him. acknowledgment of gratitude to all who supported to make it possible.

.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

REFERENCES

1. Rongxing Lu ; Nanyang Technol. Univ., Singapore, Singapore ; Hui Zhu ; XimengLiu ; Liu, J.K. ―Toward efficient and privacypreserving computing in big data era‖, IEEE Transactions Volume:28 , Issue: 4 ,2014.
2. Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, JinjunChen―MuR-DPA: Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud‖ Co, IEEE Transactions on Vol:PP , Issue: 99, 2014.
3. VenkataNarasimhaInukollu, SailajaArsi and Srinivasa Rao Ravuri ―Security Issues Associated With Big Data In Cloud Computing‖ International Journal of Network Security and Its Applications (IJNSA), Vol.6, No.3, May 2014.
4. Garlasu,D.Sandulescu,V,― A big data implementation based on Grid computing‖ ,RoedunetInternational Conference (RoEduNet), 2011.
5. X. Zhang, C. Liu, S. Nepal, S. Panley, and J. Chen, __A Privacy Leakage Upper-Bound Constraint Based Approach for Cost- Effective Privacy Preserving of Intermediate Datasets in Cloud‖ IEEE Transactions. Parallel Distributed System, vol. 24, no. 6, pp. 1192-1202, June 2013.
6. F.C.P, Muhtaroglu, Demir S, Obali M, and Girgin C. "Business model canvas perspective on big data applications", Big Data, IEEE International Conference,2013
7. A, Katal, Wazid M, and Goudar R.H. "Big data: Issues, challenges, tools and Good practices." Noida: 2013, pp. 404 – 409, 8-10 Aug. 2013.
8. A. Cavoukian and J. Jonas, ―Privacy by Design in the Age of Big Data‖, Office of the Information and Privacy Commissioner, 2012.
9. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable data possession at untrusted stores,‖ in Proc. of CCS‘07. New York, NY, USA: ACM, pp. 598–609, 2007.
10. R. Lu et al., ―EPPA: An Efficient and Privacy-Preserving Aggregation Sheme for Secure Smart Grid Communications‖, IEEE Trans. Parallel Distributed System, vol. 23, no. 9, 2012.
11. Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 2009. pp. 64–76,Apr. 2011.