International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

INTEGIRTY VERIFICATION SCHEME IN CLOUD ENVIRONMENT USING DYNAMIC KEY UPDATE

1Ms. S. PUVINI VIGNESWARI
PG Student,
2Mr. B. SENTHIL RAJA MANOKAR
Assistant Professor
Dept of Computer Science and Engineering,
Shanmuganathan Engineering College,
Arasampatti, Pudukottai.

puvinibe12@gmail.com
rajamanokar@yahoo.com

Abstract - Cloud computing has been imagined as the cutting edge engineering of IT Enterprise. Rather than conventional arrangements, where the IT administrations are under legitimate physical, consistent and work force controls, Cloud Computing moves the application programming and databases to the extensive server farms, where the administration of the information and administrations may not be completely reliable. With Cloud computing and capacity, clients can get to and to share assets offered by cloud specialist co-ops at a lower peripheral cost. With Cloud computing and capacity administrations, information is put away in the cloud, as well as routinely shared among countless in a gathering. In this venture, we propose a protection saving evaluating plan for imparted information to vast gatherings in the cloud. We use hash marks to process check data on shared information, so that the TPA can review the accuracy of shared information, however can't uncover the character of the endorser on every piece. Hash mark and Keys are created by Merkle Hash Tree. We can execute reviewing plan to perform productive open inspecting to secure both character and information protection in cloud situations. And furthermore clients can get to the information from information proprietor through cloud supplier continuously dynamic cloud environment.

Keywords: Data Storage, Computing Resources, Data Outsourcing, Key Updation, Verifiability.

I. Introduction

Cloud computing is a figuring worldview, where a substantial pool of frameworks are associated in private or open systems, to give powerfully adaptable foundation to application, information and record stockpiling. With the approach of this innovation, the cost of calculation, application facilitating, content stockpiling and conveyance is decreased altogether. It is a down to earth way to deal with experience coordinate money saving advantages and it can possibly change a server

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

farm from a capital-escalated set up to a variable evaluated environment.

Cloud processing depends on exceptionally major standards of reusability of IT capacities. The distinction that Cloud computing conveys contrasted with conventional ideas of "matrix registering", "disseminated processing", "utility figuring", or "autonomic registering" is to widen skylines crosswise over authoritative limits. Forrester characterizes Cloud computing as: "A pool of dreamy, exceedingly adaptable, and oversaw figure framework fit for facilitating end client applications and charged by consumption" .It is an innovation that uses the web and focal remote servers to keep up information and applications and permits buyers and organizations to utilize applications without establishment and get to their own records at any PC with web get to. This innovation takes into consideration considerably more productive figuring by concentrating information stockpiling, handling and transmission capacity. Cloud computing cases are Yahoo email, Gmail, or Hotmail.

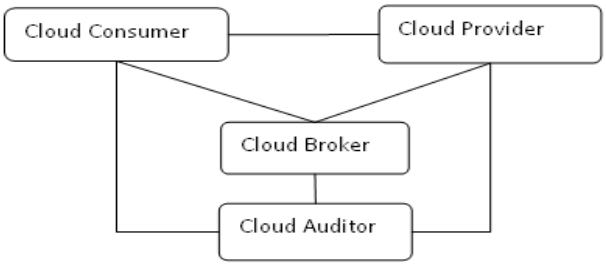

Fig.1 System Architecture Design

A. Cloud Provider

A man, association, or substance in charge of making an administration accessible to invested individuals. A Cloud Provider obtains and deals with the registering foundation required for giving the administrations, runs the cloud programming that gives the administrations, and makes game plan to convey the cloud administrations to the Cloud Consumers through system get to

a) Essential Cloud Provider

A Primary Provider offers administrations facilitated on framework that it claims. It might make these administrations accessible to Consumers through an outsider, (for example, a Broker or Intermediary Provider), however the characterizing normal for a Primary Provider is that it doesn't source its administration offerings from different Providers.

B. Cloud Consumer

"A man or association that keeps up a business association with, and utilizes benefit from, Cloud Providers. A cloud customer peruses the administration inventory from a cloud supplier, asks for the fitting administration, sets up administration contracts with the cloud supplier, and utilizations the administration. The cloud shopper might be charged for the administration provisioned, and needs to mastermind installments in like manner." What is not secured here is the end client that expends the perhaps advanced

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

administration offered by the Cloud Consumer. In SaaS, the Cloud Consumer is frequently indistinguishable with the end client. Nonetheless, in business situations this is not generally the situation. Utilizing the case of GMail, just the paying element is the Cloud Customer (e.g. IT division) while numerous different workers may utilize the mailing administration as end clients.

C. Cloud Auditor

A gathering that can lead free evaluation of cloud administrations, data framework operations, execution and security of the cloud usage. A cloud inspector is a gathering that can play out an autonomous examination of cloud administration controls with the expectation to express a supposition subsequently. Reviews are performed to check conformance to principles through survey of target proof. A cloud reviewer can assess the administrations gave by a cloud supplier as far as security controls, protection affect, execution, and so on.

D. Cloud Broker

"As distributed computing advances, the incorporation of cloud administrations can be excessively intricate for cloud buyers, making it impossible to oversee. A cloud purchaser may ask for cloud administrations from a cloud intermediary, rather than reaching a cloud supplier straightforwardly. Subsequently the agent is an element that deals with the utilization, execution and conveyance of cloud administrations, and arranges connections between Cloud Providers and Cloud Consumers." Brokers give three unique sorts of administrations to the Cloud Consumer.

i. Intervening Broker

A cloud agent upgrades a given administration by enhancing some particular capacity and offering some benefit added administrations to cloud purchasers. The change can oversee access to cloud administrations, character administration, execution detailing, upgraded security, and so on.

ii. Conglomerating Broker

A cloud agent consolidates and incorporates various administrations into at least one new administrations. The merchant gives information reconciliation and guarantees the protected information.

II.Existing System

While Cloud computing makes different focal points, it can be said in section 1 and testing security dangers toward clients' outsourced information. Since cloud specialist co-ops (CSP) are separate regulatory substances, information outsourcing is really surrendering client's definitive control over the destiny of their information. Thus, the accuracy of the information in the cloud is being put at hazard because of the accompanying reasons.

First of all, in spite of the fact that the foundations under the cloud are considerably more capable and solid than individualized computing gadgets, they are as yet confronting the expansive scope of both inner and outer dangers for

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

information honesty. Cases of blackouts and security breaks of significant cloud administrations show up every now and then.

Second, there do exist different inspirations for CSP to carry on unfaithfully toward the cloud clients with respect to their outsourced information status. CSP may recover capacity for financial reasons by disposing of information that have not been or are once in a while gotten to, or even conceal information misfortune episodes to keep up notoriety. To put it plainly, despite the fact that outsourcing information to the cloud is financially appealing for long haul substantial scale stockpiling, it doesn't quickly offer any assurance on information respectability and accessibility.

This issue, if not appropriately tended to, may obstruct the accomplishment of cloud design. As clients no longer physically have the capacity of their information, customary cryptographic primitives with the end goal of information security assurance can't be straightforwardly received. Specifically, basically downloading every one of the information for its uprightness confirmation is not a functional arrangement because of the cost in I/O and transmission cost over the system.

Moreover, it is regularly inadequate to identify the information defilement just while getting to the information, as it doesn't give clients rightness confirmation for those un-got to information and may be past the point where it is possible to recuperate the information misfortune or harm.

III. Proposed System

The framework demonstrates in this venture includes three gatherings: the cloud server, a gathering of clients and an open verifier. There are two sorts of clients in a gathering: the first client and various gathering clients. The first client at first makes shared information in the cloud, and imparts it to gathering clients. Both the first client and gathering clients are individuals from the gathering. Each individual from the gathering is permitted to get to and adjust shared information. Shared information and its confirmation metadata (i.e. marks) are both put away in the cloud server. An open verifier, for example, an outsider inspector giving master information reviewing administrations or an information client outside the gathering meaning to use shared information, can freely confirm the uprightness of shared information put away in the cloud server.

At the point when an open verifier wishes to check the honesty of shared information, it first sends an evaluating test to the cloud server. In the wake of accepting the evaluating challenge, the cloud server reacts to general society verifier with an inspecting verification of the ownership of shared information. At that point, this open verifier checks the rightness of the whole information by confirming the accuracy of the reviewing evidence. Basically, the procedure of open reviewing is a test and-reaction convention between an open verifier and the cloud server.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

TABLE I
NOTATIONS

Notation	Meaning
T	The total periods number of the whole lifetime for the files stored in the cloud
$w_1 ... w_t$	The binary string of the node w^j associated with period j
$w^j\|_k (k \leq t)$	The k-prefix of w^j
$w^j 0 (w^j 1)$	The left child node and the right child node of w^j
$w^j\|_k$	The sibling node of $w^j\|_k$
ϵ	Empty binary string
PK	The public key which is unchanged in the whole lifetime
ES_{w^j}	The encrypted node secret key
R_{w^j}	The verification value which is used to verify the validity of authenticators
ESK_j	The client's encrypted secret key in period j
X_j	A set composed by the key pairs
Ω_j	A set composed by the verification values
(ES, R)	The key pair of the root node
F	A file which the client wants to store in cloud
$m_i (i = 1, ..., n)$	n blocks of file F
DK	The decryption key to recover the encrypted secret key for cloud storage auditing

IV. Literature Survey

In the year of 2012 the authors "M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford", described into their paper titled "Secure outsourcing of scientific computations" such as We investigate the outsourcing of numerical and scientific computations using the following framework: A customer who needs computations done but lacks the computational resources (computing power, appropriate software, or programming expertise) to do these locally would like to use an external agent to perform these computations.

This currently arises in many practical situations, including the financial services and petroleum services industries. The outsourcing is secure if it is done without revealing to the external agent either the actual data or the actual answer to the computations. The general idea is for the customer to do some carefully designed local preprocessing (disguising) of the problem and/or data before sending it to the agent, and also some local post processing of the answer returned to extract the true answer. The disguise process should be as lightweight as possible, e.g., take time proportional to the size of the input and answer.

The disguise preprocessing that the customer performs locally to "hide" the real computation can change the numerical properties of the computation so that numerical stability must be considered as well as security and computational performance. We present a framework for disguising scientific computations and discuss their costs, numerical properties, and levels of security. We show that no single disguise technique is suitable for a broad range of scientific computations but there is an array of disguise techniques available so that almost any scientific computation could be disguised at a reasonable cost and with very high levels of security. These disguise techniques can be embedded in a very high level, easy-to-use system (problem solving environment) that hides their complexity.

In the year of 2008 the authors "D. Benjamin and M. J. Atallah", described into their paper titled "Private and cheating free outsourcing of algebraic computations" such as We give protocols for the secure and private outsourcing of linear algebra computations, that enable a client to securely outsource expensive algebraic computations (like the multiplication of huge matrices) to two remote servers, such that the servers learn nothing about the customer's private input or the result of the computation, and any attempted corruption of the

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

answer by the servers is detected with high probability.

The computational work done locally by the client is linear in the size of its input and does not require the client to carry out locally any expensive encryptions of such input.The computational burden on the servers is proportional to the time complexity of the current practically used algorithms for solving the algebraic problem (e.g., proportional to n^3 for multiplying two n x n matrices). If the servers were to collude against the client,then they would only find out the client's private inputs, but they would not be able to corrupt the answer without detection by the client.

In the year of 2011 the authors "C.Wang, K. Ren, and J.Wang", described into their paper titled "Secure and practical outsourcing of linear programming in cloud computing" such as Cloud computing enables customers with limited computational resources to outsource large-scale computational tasks to the cloud, where massive computational power can be easily utilized in a pay-per-use manner. However, security is the major concern that prevents the wide adoption of computation outsourcing in the cloud, especially when end-user's confidential data are processed and produced during the computation.

Thus, secure outsourcing mechanisms are in great need to not only protect sensitive information by enabling computations with encrypted data, but also protect customers from malicious behaviors by validating the computation result. Such a mechanism of general secure computation outsourcing was recently shown to be feasible in theory, but to design mechanisms that are practically efficient remains a very challenging problem. Focusing on engineering computing and optimization tasks, this paper investigates secure outsourcing of widely applicable linear programming (LP) computations. In order to achieve practical efficiency, our mechanism design explicitly decomposes the LP computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer.

The resulting flexibility allows us to explore appropriate security/efficiency tradeoff via higher-level abstraction of LP computations than the general circuit representation. In particular, by formulating private data owned by the customer for LP problem as a set of matrices and vectors, we are able to develop a set of efficient privacy-preserving problem transformation techniques, which allow customers to transform original LP problem into some random one while protecting sensitive input/output information. To validate the computation result, we further explore the fundamental duality theorem of LP computation and derive the necessary and sufficient conditions that correct result must satisfy. Such result verification mechanism is extremely efficient and incurs close-to-zero additional cost on both cloud server and customers. Extensive security analysis and experiment results show the immediate practicability of our mechanism design.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

V. Experimental Results

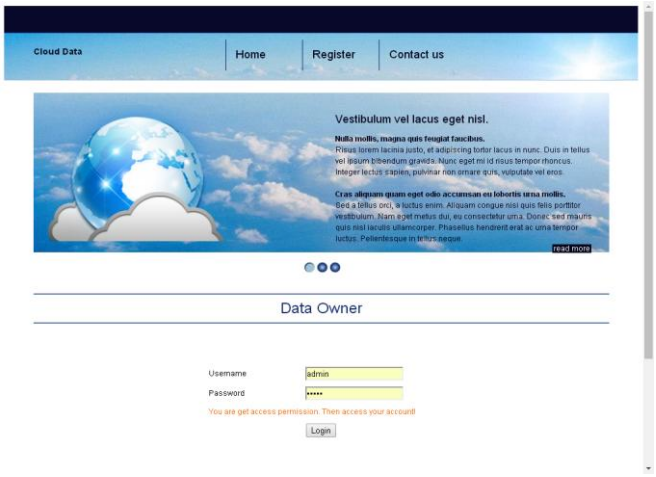

Fig.2. Administrator Login Page

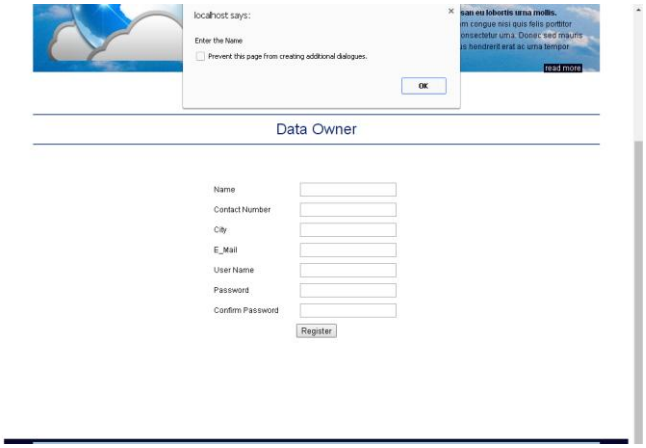

Fig.3. Data Owner Signup Page

V. Conclusion and Future Scope

Cloud computing securities are talked about and examined in past review. In this venture, a portion of the protection dangers are tended to and the methods to conquer them are studied. While some methodologies used conventional cryptographic techniques to accomplish security, some different methodologies kept them away and concentrated on interchange approaches in accomplishing protection. Likewise, ways to deal with save security at the season of open evaluating are additionally talked about.

Consequently, to close it is fundamental that each cloud client must be ensured that his information is put away, handled, got to and reviewed in a secured way whenever. Information freshness is fundamental to secure against misconfiguration mistakes or rollbacks created deliberately and can build up a validated document framework that backings the relocation of a venture class dispersed record framework into the cloud productively, straightforwardly and in an adaptable way. It's confirmed as in empowers an undertaking occupant to check the freshness of recovered information while playing out the record framework operations. The client must be given finished get to control over the Cloud information. Likewise, capable security systems should dependably supplement each cloud application. Accomplishing all these would wind up in accomplishing the long imagined vision of secured Cloud Computing in the closest future.

In future, this proposed model could be utilized to get the safe Cloud computing environment which would be an awesome improvement in the security conservation. At that point conquer client repudiation issue utilizing open key overhauling calculation with element bunch administration.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 20, 2017 ISSN: 2348-6600
Reference ID: IJCS-252 PAGE NO: 1603-1610
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

VI. References

[1] M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," Trends in Software Engineering, vol. 54, pp. 215-272 2002.

[2] D. Benjamin and M. J. Atallah, "Private and cheatingfree outsourcing of algebraic computations," Proc. Sixth Annual Conference on Privacy, Security and Trust, pp. 240-245, 2008.

[3] C.Wang, K. Ren, and J.Wang, "Secure and practical outsourcing of linear programming in cloud computing," IEEE INFOCOM 2011, pp. 820-828, 2011.

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New Algorithms for Secure Outsourcing of Modular Exponentiations," Proc. 17th European Symposium on Research in Computer Security, pp. 541-556, 2012.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[6] A. Juels, J. Burton, and S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 584-597, 2007.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.

[8] G. Ateniese, R.D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. 4th International Conference on Security and Privacy in Communication Networks, 2008

[9] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1-6, 2008.

[10] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PPDP: Multiple-Replica Provable Data Possession," Proc. 28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.

[11] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.

[12] C. Wang, K. Ren, W. Lou, and J. Li, "Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[13] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.