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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Cloud Computing Model for Large Scale System through Merkle Hash Tree

S.Dhivyabala[1], K.Gopalakrishnan[2]

M.E, Department of CSE, Nandha College of Technology, Erode, India[1]

Assistant Professor, Department of CSE, Nandha College of Technology, Erode, India[2]

Abstract: Dynamic resource management in cloud server provisioning has become an active area of research in the Cloud Computing. Cost of resources varies significantly depend on configuration for using them. An efficient management of resources is of prime interest to both Cloud Providers and Cloud Users. In this work Cloud Computing problem can be resolve through the large scale System of Linear equation, it can be achieved by the examining the comprising interior points of the problem arise due to non linear equation with optimization problem. The Cloud computing problem of the resources in terms of hardware constraints can be converted to sequence of linear problems and solved using linear equations. System Storage is mentioned using System Coefficient Matrix of user requirement increases Resource Units is expressed in the Matrix vector format that statistically characterizes extreme rare events through proposed estimation factor, such as the ones produced by varying resource demands that may cause workload overflow in the resource on demand context. This analysis provides valuable insight on expectable abnormal behavior of systems. The information obtained using the Dynamic heuristic constraints for the proposed on Demand use-case for defining policies. The policies of elastic resource provisioning and usage may be of some interest to all stakeholders in the emerging context of cloud networking.

Keywords: Cloud Computing, Confidential data, computation outsourcing, system of linear equations.

I. INTRODUCTION

Cloud computing is an expression used to describe a variety of computing concepts that involve a large number of computers connected to the internet. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. The cloud are more commonly refer to network-based service, which appear in the real server hardware, and in fact served by virtual hardware, software run on one or more real machines. Such virtual server which do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user - arguably, rather like a cloud.

Efficient Memory management is one of the hot topics these days in Cloud because of the augmenting need of integrated data handling and exigency of optimized memory management algorithm. The trend Application Service Provider (ASP) and Database-as-a-Service (DaaS) paradigms are in need of smart memory management protocols to be integrated in Cloud in order to get rid of the latency and load balancing issues. Hardware Constraints: Hardware Constraints may lead to poor performance in terms of Network, processor, Memory unit or physical components in the cloud resource provider.

Secure outsourcing for widely applicable large-scale systems of linear equations (LE), which are among the most popular algorithmic and computational tools in various engineering disciplines that analyze and optimize real-world systems. Also, by interior point method, system optimization problem can be converted to nonlinear equation, which is solved as a sequence of systems of linear equation. SMC model do not address the asymmetry among the computational power possessed by cloud and the customer framework of SMC usually does not directly consider the computation result verification as an indispensable security requirements, due to assumption that each involves party is the semi honest traditional direct method for jointly solving the LE, the Gaussian elimination method or the secure matrix inversion method While working well for small size problem, these approach that general do not derive

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

practically acceptable solution time for large-scale LE, due to the expensive cubic time computational burden for matrix-matrix operations and the huge IO cost on customer's weak devices

II. PROBLEM STATEMENT

Cloud computing economically enables customers with limited computational resources to outsource large-scale Computation. However, how to protect user confidential data involved in the computations then become a major security concerns.

Concerns of computing performance in cloud based on the two cases

1. Cloud provider resources
2. Weakness of the client Resources

Lower end computing devices due processing Speed, less memory, financial benefits of cloud providers, Execution time may be factor to determine the performance of cloud based on the no. of operations and based on Memory hierarchy for scheduling.

2.1Computation Outsourcing Model

Secure outsourcing for widely applicable large-scale system of linear equations (LE), are the most popular algorithmic and computational tools in various engineering disciplines that analyze and optimize real-world systems. Also, by interior point method, system optimization problem can be converted to a system of nonlinear equation, then it solved as a sequence of linear equations. SMC model do not address the asymmetry among the computational power possessed by cloud and the customer framework of SMC usually does not directly consider the computation result verification as an indispensable security requirement, with assumption that each involved in semi honest traditional direct method for jointly solving the LE, the joint Gaussian elimination method or the secure matrix inversion methods, While working well for small size problem, these approaches that do not derive practically acceptable solution time for large-scale LE, and the expensive cubic time computational for matrix-matrix operations and the huge IO cost on customer's weak devices.

2.2. Privacy-preserving Public Auditing for Secure Cloud

Storage

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for user with constrained computing resource. Moreover, users should be able to use the cloud storage as in local, without worrying about the need to verify its integrity. Thus, the enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. The securely introducing an effective TPA, are the auditing process which bring in no new vulnerabilities toward the user data privacy, and introduce no additional online burden to user. A secure cloud storage system supporting privacy-preserving public auditing. In further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive securities and performance analysis show the proposed schemes are provably secure and highly efficient. And our preliminary experiment conduct on Amazon EC2 instance further demonstrates the fast performance of the design.

III. SYSTEM METHODOLOGY

Cloud Computing problem can be resolve through the large scale System of Linear equation ,it can be achieved by the examining the interior points of the problem arise due to non linear equation with optimization problem . The Cloud Computing problem of the resources in terms of hardware constraints can be converted to sequence of linear problems and solved using linear equations.

System Storage requirement used in the System Coefficient Matrix of user requirement increases. Resource Units is expressed in the Matrix vector format

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

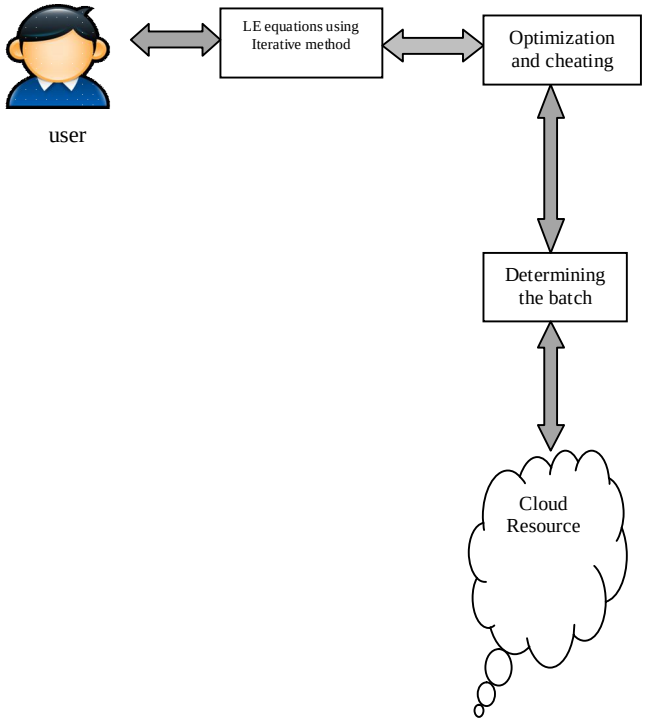

Fig. 1 System Architecture.

IV. EXISTING SYSTEM

Secure outsourcing mechanism for solving large-scale system of linear equations (LE). Applying traditional approaches like Gaussian elimination or LU decomposition (aka. direct method) to such large-scale LEs would be prohibitively expensive, many systems has builded the secure LE outsourcing mechanism via a completely different approach iterative method, it is much easier to implement in practice and only demands relatively simpler matrix-vector operations. Specifically, many existing mechanism enables a customer to securely harness the cloud for iteratively finding successive approximations to the LE solution, which keep both the sensitive input and output of the computation private. For robust cheating detection, solutions further explore the algebraic property of matrix-vector operations and propose an efficient result verification mechanism, which allow the customer to verify all answers received from previous iterative approximations in one batch with high probability.

- System proposed is Silent to the attacks and computing performance
- Mechanism proposed in literature is less preserved in terms of data and resource integrity
- System has leads to the high computational cost in terms of computation abilities in terms of both on client and cloud provider in scheduling the hardware utilities.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. PROPOSED SYSTEM

Cloud Computing by harnessing the scheduling performance through trust establishing through Secure outsourcing mechanism for solving large-scale systems of linear equations (LE). Because applying traditional approaches like Gaussian elimination or LU decomposition (aka. direct method) to such large-scale LEs would be prohibitively expensive, and the secure LE outsourcing mechanism via a completely different approach iterative method, it is easier to implement in practice and only demands relatively simpler matrix-vector operations. Our mechanism enables a customer to securely harness the cloud for iteratively finding successive approximations to the LE solution, which keeps both the sensitive input and output of the computation. For robust cheating detection with merkle hash tree, The algebraic property of matrix-vector operations through the proposed scheme and propose an efficient result verification mechanism, which allow the customer to verify all answers received from previous iterative approximations in one batch with high probability.

- Our Scheme benefit from less computation time.
- System is highly privacy preserved and resilient for cheating.
- System eliminates the high IO cost.
- Ensuring the high Computing integrity.

VI. SYSTEM IMPLEMENTATION

6.1 Cloud architecture

The systems architecture of the software systems involved in the delivery of cloud computing, typically involve multiple cloud component communicating with each other over application programming interface, usually on web services. This resembles the UNIX philosophy of having multiple programs each doing one thing well and working together over universal interface. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts.

The two most significant components of cloud computing architecture are known as the front end and the back end. The front ends are the part by the client, i.e. the computer user. This includes the client's network (or computer) and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, comprise various computer, servers and data storage devices.

Applications that work best with a hybrid cloud application architecture are multi-tiered applications; where the application components can be scaled based on one or more key metrics. In our example a Java application serviced by an Apache Tomcat server, where the web and application tiers are collapsed into a single layer, connected to a database with in-built caching and replication capabilities. The components that selected allow for scaling the application components together, caching shared application data on each node and replicating dynamic data to and from each site.

Large-scale cloud implementations may require more robust cloud management tools that include specific characteristic, the ability to manage the multiple platform from a single point of reference, which include intelligent analytic to automate processes like application lifecycle management. The high-end managing tools should also be able to handle system failures automatically with capabilities such as self-monitoring, an explicit notification mechanism, which include failover and self-healing capabilities.

6.2 Establishing Securing Outsourcing The Large Scale System of LE Through Iterative Method

A threshold proxy re-encryption scheme with multiplicative homomorphic property to secure data outsourced to a cloud .An encryption scheme is multiplicative homomorphic if it supports a group operation on encrypted plaintexts without decryption. Thus, a multiplicative homomorphic encryption scheme supports the encoding operation over encrypted messages. a proxy re-encryption scheme with multiplicative homomorphic property into a threshold version. Thus, a multiplicative homomorphic encryption scheme supports the encoding operation over encrypted messages. Then convert a proxy re-encryption scheme with multiplicative homomorphic property into a threshold version. A secret key are shared to key server with a threshold value t via the Shamir secret sharing scheme. Error localization is a key prerequisite for eliminating errors in storage system. It is also importance to identify potential threats from external attack. However, many previous schemes that do not explicitly consider the problem of data error localization, thus

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

provide the binary result for the storage verification. Thus outperform are integrating the correctness verification and error localization (misbehaving server identification) in our challenge-response protocol: the response values from servers for each challenge not only determine the correctness of the distributed storage, and also having information to locate potential data error.

6.3 Cheating Detection Mechanism for Batch Verification Through Matrix Vector Operation

A decentralized erasure code is an erasure code that independently computes each codeword symbol for a message. The encoding message can be split into n parallel tasks of generating codeword symbol. A decentralized erasure code is suitable for a distributed storage system. After the message symbol is sent to storage server, storage server independently compute a codeword symbol for the receiver message symbols and store it. Thus finish the encoding and storing the process. The recovery processes are same.

Direct method-based approach might not be a good option for resource-limited customers for secure outsourcing large-scale LE with computational saving in mind. This Motivate us to design the secure outsourcing mechanism with the usage of iterative method.

Our goal is to let the customer securely harness in the form of matrix-vector multiplication. An iterative computing is the very first round of the process as follow. The analysis of convergence and input/output protection in later section. It assumes our main protocol of solving LE works over integers. All arithmetic modular are with the respect to modulus N of the homomorphic encryption, and the module is large enough to contain the answer. When dealing with iterative method, it must be determine whether and when the iteration will converge. The unfaithful cloud server could sabotage the protocol execution by either being lazy or intentionally corrupting the computation result. The design result verification method is to handle those two malicious behavior. Our goal is verifying the correctness of the solution by using as few as possible expensive matrix vector multiplication operations.

6.4 Performance Evaluation

The problem of data security in cloud data storage is essential for distributed storage system. To achieve the data integrity and availability and the quality of dependable cloud storage service for user, an effective and flexible distributed scheme are explicitly dynamic data support, it includes block updating, deleting, and appending. The rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. The homomorphic tokens are distributed verification of erasure coded data, and our scheme to achieve the integration of storage correctness insurance and data error localization. The storage correctness verification across the distributed server the data are corrupted, the simultaneous identification of the misbehaving server. Consider the time, computation resource, the related online burden of user, the extend the proposed main scheme to support the third-party auditing, where customer can safely delegated the integrity checking tasks to third party auditors and be worry-free to use the cloud storage services.

VI. CONCLUTION

Secure outsourcing mechanism for solving large-scale systems of linear equations (LE) in cloud. Because applying traditional approaches like Gaussian elimination or LU decomposition (aka. direct method) to such large-scale LEs would be prohibitively expensive, The secure LE outsourcing mechanism via a completely different approach iterative method, which is much easier to implement in practice and only demands relatively simpler matrix-vector operations. Specifically, our mechanism enables a customer to securely harness the cloud for iteratively finding successive approximations to the LE solution, user does not have the time, feasibility or resources to perform the storage correctness verification, he can optionally delegate this task to an independent third party auditor, making the cloud storage publicly verifiable while keeping both the sensitive input and output of the computation private. For robust cheating detection, In further, the algebraic property of matrix-vector operations and propose an efficient result verification mechanism, which allows the customer to verify all answers received from previous iterative approximations in one batch with high probability.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

REFERENCES

[1] Bhartiya A.S. , Agrawal L.S., Gawande Y.V. And Rapartiwar S.S. "Achieving Sheltered, Scalable And Fine-Grained Data Access Control In Cloud Computing" World Research Journal of Engineering and Technology ISSN: 2278-8530 & E-ISSN: 2278-8549, Volume 1, Issue 1, 2012, pp.-04-07.

[2] Cengiz Örencik, Erkay Sava¸s "Efficient and Secure Ranked Multi-Keyword Search on Encrypted Cloud Data" ACM 978-1-4503-1143, March 30, 2012.

[3] Jan Camenisch , Susan Hohenberger , and Michael stergaard Pedersen "Batch Verification of Short Signatures" Research performed while at IBM Research, Zurich Research Laboratory. International Association for Cryptology Research, LNCS 4515, pp. 246–263, 2007.

[4] John Bethencourt, Dawn Song And Brent Waters "New Techniques for Private Stream Searching" SRI International ACM Transactions on Information and System Security, Volume 12, Number. 3, Article 16, Publish date January 2009.

[5] Jyothi U , Nagi Reddy K and Ravi Prasad B "Achieving Secure, Scalable, and inegrained Data Access Control in Cloud Computing" International Journal Of Engineering And Computer Science ISSN:2319-7242, Volume 2, Page No. 2440-2447, Issue 8, August, 2013.

[6] Michael Backes, Dario Fiore, aphael Reischuk M "Verifiable Delegation of Computation on Outsourced Data" ,Publication rights licensed to ACM, November 4–8, 2013

[7] Rosario Gennaro, Bryan Parno, Craig Gentry "Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers" the US Army Research laboratory and the UK Ministry of Defence under Agreement Number W911NF-06-3-0001, February 1, 2010.

[8] Treesa Maria Vincent and Sakunthala J "Data Storage in Cloud Environment Enhance Privacy" International Journal of Computer Trends and Technology- volume 4, Issue 3- 2013.

[9] valeria Nikolaenko, Stratis Ioannidis , Udi Weinsberg "Privacy-Preserving Matrix Factorization" ACM 978-1-4503-2477, CCS'13, November 4–8, 2013.

[10] Wee Keong Ng and Li Wan "Privacy-Preservation for Gradient Descent Methods" KDD'07,August12 15,2007.