"HARNESSING THE CLOUD FOR SECURELY OUTFORCING LARGE SCALE SYSTEM OF LINEAR EQUATIONS"

PROJECT REFERENCE NO. : 37S1289

COLLEGE : K.S. SCHOOL OF ENGINEERING AND MANAGEMENT, BANGALORE
BRANCH : COMPUTER SCIENCE AND ENGINEERING
GUIDE : GOVINDARAJU G.N
STUDENTS : DIVYANAGARAJ
            POOJA N
            SREEVATHSA B.S

Keywords: Cloud Computing, System of Linear Equations, Iterative Method

Introduction:

Cloud Computing has a large potential computational power, at a reduced cost. It enables customers with the limited computational resources to outsource their large scale computations. Besides these benefits, security is the primary problem that prevents the wide usage of the cloud computing model when the customers’ confidential data is consumed and produced during the computation.

To overcome the above problem, in this project a secure framework is provided, that protects the sensitive information and enables computations with encrypted data. And it also helps the customer with cheating detection mechanism, by enabling the verification of the computation results.

The framework provides a secure outsourcing mechanism for the customers. To solve the large scale systems of Linear Equations (LE) in cloud, iterative method is used. This method is easier to implement when compared to direct method and it demands only simple matrix-vector operations.

Objectives:

- To study the Techniques currently available to outsource the system of equations.
➢ To develop a Framework for processing large scale LE using iterative method to 
increase the efficiency in Cloud computing Environment.

➢ To verify the results obtained from the Framework developed.

➢ To refine the Framework for improved efficiency.

**Methodology:**

➢ Refereed journal, publications to understand and identify the drawbacks in current 
  Direct processing Techniques.

➢ A system design will be created and AES and Jacobi method algorithms or pseudo 
  codes will be formulated.

➢ The results of the programs will be compared with the existing system using different 
  methods & technologies.

➢ Various parametric studies will be done using the framework for improved efficiency 
  of processing.

**Modules:**

➢ Problem Transformation

➢ Problem Solving

➢ Result Verification

**Problem Transformation**

- accept the system of equations, Ax=b, from the user;
- check whether the diagonal elements are dominant; if not display error 
  message;
- Transform the original problem Ax=b into Ay=b’ as follows;
- split the matrix A into D and R, where D consists of diagonal elements ,rest in R;
- accept a random number ‘r’ from the user;
- Compute b’=b + A r ,
- Compute T= -D-1.R and c= D-1.b’
Problem Solving

- Initially guess $y(0)$ vector as 0;
- Cloud computes $\text{Enc}(T \cdot y(k))$
- Customer finds next approximation using the relation, $y(k+1) = T \cdot y(k) + c$
- Continue the iterative method until result is obtained

Result Verification

- On computation of $y(k+1)$, verify the convergence condition, $||y(k+1) - y(k)||$

Results and Conclusion:

- The algebraic property of matrix-vector multiplication results in the development of efficient and effective scheme for result verification.
- Computation outsourcing using iterative method provides the benefit of easy-to-implement and less memory requirement in practice.
- The designed mechanism results in computational savings for the customer and demands for no unrealistic IO cost

Future Work:

- Devise a robust algorithm to achieve numerical stability.
- Explore the sparsity structure of problem for further efficiency improvement.
- Advance security algorithms for preserving privacy of data.