Volume 3, Issue 12, December 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Overview of Safe and Sensible Outsourcing of Linear Programming in Cloud

T.Amardeep[1],
[1]*M.Tech Student, Dept. of CSE,*
DRK College of Engineering and Technology,
Hyderabad, A.P, India

Dr.R.V.Krishnaiah[2]
[2]*PG Coordinator, Dept. of CSE,*
DRK Group of Institutions,
Hyderabad, A.P, India

Abstract: ***Cloud computing is a new software development concept in which services and storage are provided over the internet which makes possible businesses to evade important capital expenditure on infrastructure and software development services. Cloud computing offers a flexible in line with the businesses requirements. Safety is the major problem which averts the approval of the computing model particularly for the customers, if their private data are consumed and produced during the computation. A method is designed for safeguarding the perceptive information by allowing computations with encrypted data and to defend the customers from malicious behaviours by facilitating the validation of the computation result, treating the cloud as an effectively unconfident computing platform by the customers. By decomposing the linear programming computation outsourcing into community linear programming solvers and private linear programming (LP) parameters owned by customers, realistic competence can be achieved. In recent times in Practical efficiency can be achieved by decomposing the LP computation outsourcing into public LP solvers which are running on the cloud and private LP parameters owned by customers.***

Keywords: Cloud Computing, Software Development, Linear Programming, Practical Efficiency, Secure Computation Outsourcing, Software as a Service, Public Cloud.

I. INTRODUCTION:

The term cloud computing is used to refer to a new concept that agreeably offers IT resources and services over the Internet. Software as a service in the business model, users are provided access to appliance software and databases [1] [2]. The applications run on the infrastructure and platforms of cloud providers. The on-demand software is sometimes referred to as SaaS, and is usually priced on a pay-per-use basis and generally price applications using a subscription fee [3] [4]. The Internet, hardware and the systems software in the data centres provide the services which are referred by Cloud Computing services i.e. Software as a Service (SaaS). We call it a Public Cloud when a cloud is available in a pay per use manner to the general public and the service is Utility Computing [5]. The term private cloud refers to the internal data centres of a business and is not available to the general public. In spite of the great benefits, safety is the major problem which averts the approval of the computing model particularly for the customers, if their private data are consumed and produced during the computation is shown in Fig 1[6] [7].

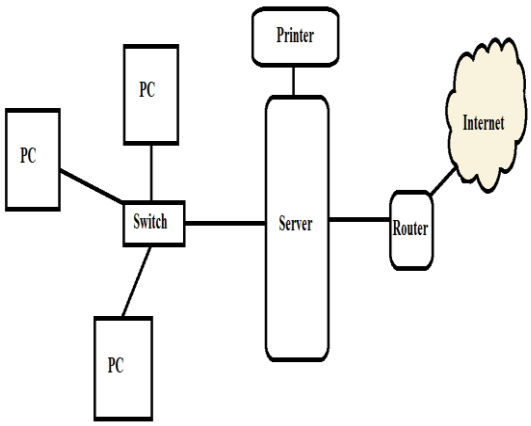

Fig 1. Network Diagram of Cloud Computing

The data have to be encrypted before outsourcing in order to fight against unauthorized information leakage and so as to provide end to end data confidentiality assurance in the cloud. Outsourced computation workloads contain sensitive information [8] [9]. The operational details of customers are not transparent in a cloud. As a result, there exist a various motivations for cloud server to behave unfaithfully and to return incorrect results [10] [11].

2. OVERVIEW OF SECURE COMPUTATION OUTSOURCING:

It would be inflexible to anticipate cloud customers to turn over control of their workloads from local machines to cloud that are based on the cloud's financial savings and resource adjustability without providing a method for secure computation outsourcing [12]. The assault might also affect the quality of the computed results besides the software bugs and hardware failures. A high level demonstration allows us to apply for a set of well-organized secure problem alteration techniques while defending the responsive information and to renovate the original linear programming problem into some arbitrary [13]. The generic mechanism allows the customer to hide the fact that the outsourced computation is linear programming and efficiency can greatly affect by imposing the strict security measures. A set of problem dependent masking techniques are proposed for different scientific applications like linear algebra, sorting and string pattern matching which allows data expose to certain degree and more to the point, they do not handle the case of result confirmation [14] [15]. The protocols use important cryptographic primitive such as homomorphic encryption and unaware transfer and do not extent well for big problem. The both designs are built upon the assumption of two non-colluding servers and are susceptible to colluding attacks. In the recent times secure protocol for secure outsourcing matrix multiplications were given on the basis of undisclosed sharing. This work outperforms their previous work in the sense of single server assumption and computation efficiency.

3. RELATED WORK ON CONFINED COOPERATIVE CALCULATION:

The safe calculation outsourcing fulfils all mentioned requirements, such as confidentiality and accuracy guarantee has been shown in feasible theory. For different scientific applications like linear algebra, sorting and string pattern matching a set of problem dependent disguising techniques are proposed. However, these techniques allow information depiction to certain degree. Besides, they do not handle the case of result verification. The both protocols use heavy cryptographic primitive such as homomorphic encryption and/or oblivious transfer and do not scale well for large problem set. The both designs are built upon the assumption of two non-colluding servers and are vulnerable to colluding attacks. This work outperforms their previous work in the sense of single server assumption and computation efficiency. The other great existing work that is significantly different is Secure Multi-party Computation (SMC). It authorizes more than two parties to mutually calculate some common function by thrashing their inputs. Safe computation outsourcing can be difficult by direct applying the SMC to the cloud computing model due to the reason of not addressing the irregularity among the computational powers possessed by cloud and the customers. In SMC all the problem input information was known to the single involved party and makes the result verification a complex task. Recently a safe and combined computation of linear programming under the SMC framework was provided. The restriction matrix connecting two concerned parties, followed by a series of interactive cryptographic protocols combined are implemented in every iteration step of the Simplex Algorithm. For different scientific applications like linear algebra, sorting and string pattern matching a set of problem dependent disguising techniques are proposed which allows information expose to certain degree and more to the point, they do not handle the case of result verification. A feeble customer can confirm the accuracy of the entrusted computation results from a powerful but un-trusted server without investing too many resources has found great interests in speculative computer science community in the process of Variable computation allocation system. For wide-ranging computation out-sourcing in grid computing, based on the results of computation deception discovery method was proposed. Based on the results of computation the server is required to provide a dedication. The customer then makes use of the dedication combined with a sampling approach to bring out the result verification. All the methods allow server monitor the data and result it is computing with and it is not probable in the cloud computing model for data privacy.

4. CONCLUSION:

To design a practical method this achieves privacy, dishonesty flexibility and effectiveness. Our method designing can able to explore appropriate security tradeoffs by means of higher level linear programming computation than the general circuit representation by explicitly decomposing linear programming computation outsourcing into public linear programming solvers and private data. We extend a problem alteration technique that allows customers to secretly change the original linear programming into some arbitrary one while protecting sensitive input output information. A set of necessary and sufficient condition were derived for result verification by considering duality theorem.

REFERENCES:

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on Jan. 23rd, 2010 Online at http://csrc.nist.gov/ groups/SNS/cloud-computing/index.html, 2010.

[2] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, online at http://www.cloudsecurityalliance.org.

[3] C. Gentry, "Computing arbitrary functions of encrypted data," *Commun.ACM*, vol. 53, no. 3, pp. 97–105, 2010.

[4] Sun Microsystems, Inc., "Building customer trust in cloud computing with transparent security," 2009, online at https://www.sun.com/offers/ details/sun transparency.xml.

[5] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, "Secure outsourcing of scientific computations," *Advances in Computers*,vol. 54, pp. 216–272, 2001.

[6] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in *Proc. of TCC*, 2005, pp. 264–282.

[7] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," *Int. J. Inf. Sec.*, vol. 4, no. 4, pp. 277–287, 2005.

[8] D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in *Proc. of 6th Conf. on Privacy, Security, and Trust (PST)*, 2008, pp. 240–245.
[9] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. Of CRYPTO'10*, Aug. 2010.
[10] M. Atallah and K. Frikken, "Securely outsourcing linear algebra computations," in *Proc. of ASIACCS*, 2010, pp. 48–59.
[11] A. C.-C. Yao, "Protocols for secure computations (extended abstract)," in *Proc. of FOCS'82*, 1982, pp. 160–164.
[12] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc of STOC*, 2009, pp. 169–178.
[13] D. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, 3rd ed. Springer, 2008.
[14] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. of ICDCS'10*, 2010.
[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained access control in cloud computing," in *Proc. of IEEE INFOCOM'10, San Diego, CA, USA, March 2010*.

AUTHORS PROFILE

T.Amardeep has completed B.Tech from S.V College of Engineering and Technology and pursuing M.Tech (C.S.E) in DRK College of Engineering and Technology, JNTUH, Hyderabad, Andhra Pradesh, India. His main research interest includes Data Mining, Information Security, network protection and security control.

Dr.R.V.Krishnaiah, did M.Tech (EIE) from NIT Warangal, MTech (CSE) form JNTU, Ph.D, from JNTU Anantapur, He has memberships in professional bodies MIE, MIETE, MISTE. He is working as Principal in DRK Institute of Science and Technology, Hyderabad. His main research interests include Image Processing, Security systems, Sensors, Intelligent Systems, Computer networks, Data mining, Software Engineering, network protection and security control. He has various publications and presentations in various National and International Journals.

