International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 3, Issue 3, 2012, pp 368-372
http://bipublication.com

# APPLICATIONS AND PROGRAMMING IN CLOUD COMPUTING

**A. Kapil Kumar, Vijaykumar Mantri, Dasaradh Ramaiah**

Dept of IT, Dr.B.V. Raju Institute of Technology, Hyderabad, A.P, India

## ABSTRACT:

This next generation of computing holds enormous potential to stimulate economic growth and enable governments to reduce costs, increase transparency and expand services tocitizens. However, how to protect customers confidential data processed and generated during the computation is becoming the major security concern. Focusing on engineering computing and optimization tasks, this paper investigates secure outsourcing of widely applicable linear programming (LP) computations. To battle against unauthorized information leakage have to be encrypted before outsourcing. so as to provide end to- end data confidentiality assurance in the cloud and beyond.

**Indexing terms**: Cloud computing, economic growth,Linear Programming, computing and optimization tasks

## INTRODUCTION

It is a paradigm shift following the shift from mainframe to client-server that preceded it in the early '80s. Details are abstracted from the users who no longer have need of, expertise in, or control over the technology infrastructure "in the cloud" that supports them.[31] Cloud computing describes a new supplement, consumption and delivery model for IT services based on the Internet, and it typically involves the provision of dynamically scalable and often virtualized resources as a service over the Internet.[32, 33] It is a byproduct and consequence, of the ease-of-access to remote computing sites provided by the Internet.[34]. The term cloud is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network [35], and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents.[36] Typical cloud computing providers deliver common business applications online which are accessed from another web service or software like a web browser, while the software and data are stored on servers.A technical definition is "a computing capability that provides an abstraction between the computing resource and its underlying technical architecture (e.g., servers, storage, networks), enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."[37] This definition states that clouds have five essential characteristics:

on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[37]

Cloud Computing provides convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management overhead [1]. One fundamental advantage of the cloud paradigm is computation outsourcing, where the computational power of cloud customers is no longer limited by their resource-constraint devices. By outsourcing the workloads into the cloud, customers could enjoy the literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays in the purchase of hardware and software and/or the operational overhead therein.

Despite the tremendous benefits, outsourcing computation to the commercial public cloud is also depriving customers' direct control over the systems that consume and produce their data during the computation, which inevitably brings in new security concerns and challenges towards this promising computing model [2].

To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing [2] so as to provide end to- end data confidentiality assurance in the cloud and beyond. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying plaintext data [3], making the computation over encrypted data a very hard problem. On the other hand, the operational details inside the cloud are not transparent enough to customers [4]. Recent researches in both the cryptography and the theoretical computer science communities have made steady advances in "secure outsourcing expensive computations"[5-10]. Based on Yao's garbled circuits [11] and Gentry's breakthrough work on fully homomorphic encryption (FHE) scheme [12], a general result of secure computation outsourcing has been shown viable in theory [9], where the computation is represented by an encrypted combinational Boolean circuit that allows to be evaluated with encrypted private inputs. However, applying this general mechanism to our daily computations would be far from practical, due to the extremely high complexity of FHE operation as well as the pessimistic circuit sizes that cannot be handled in practice when constructing original and encrypted circuits. This overhead in general solutions motivates us to seek efficient solutions at higher abstraction levels than the circuit representations for specific computation outsourcing problems. Although some elegant designs on secure outsourcing of scientific computations, sequence comparisons, and matrix multiplication etc. have been proposed in the literature, it is still hardly possible to apply them directly in a practically efficient manner, especially for large problems. In those approaches, either heavy cloud-side cryptographic computations [7], [8], or multi-round interactive protocol executions [5], or huge communication complexities [10], are involved. In short, practically efficient mechanisms with immediate practices for secure computation outsourcing in cloud are still missing.

## KEY FEATURES:

Agility improves with users' ability to rapidly and inexpensively re-provision technological infrastructure resources [13]. Cost is claimed to be greatly reduced and capital expenditure is converted to operational expenditure [50]. This ostensibly lowers barriers to entry, as infrastructure is typically provided by a third-party and does not need to be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained with usagebased options and fewer IT skills are required for implementation (in-house) [51] Device and location independence[52]enable users to access systems using a web browser regardless of their location or what device they are using (e.g., PC, mobile). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.[51]Multi-tenancy enables sharing of resources and costs across a large pool of users thus allowing for:Centralization of infrastructure in locations with lower costs (such as real estate, electricity, etc.), Peak-load capacity increases (users need not engineer for highest possible load-levels)Maintenance cloud computing applications are easier to maintain, since they don't have to be installed on each user's computer. They are easier to support and to improve since the changes reach the clients instantly.Although cloud computing is often assumed to be a form of "green computing", there is as of yet no published study to substantiate this assumption.[53]

**APPLICATIONAL REVIEWS:**

Peer-to-Peer (P2P) computing allows peer nodes (computers) to share content directly with one another in a decentralized manner. In pure P2P computing, there is no notion of clients or servers since all peer nodes are equal and concurrently be both clients and servers. The goals of P2P computing include cost sharing or reduction, resource aggregation and interoperability, improved scalability and reliability, increased autonomy, anonymity or privacy, dynamism, and ad-hoc communication and collaboration [38]. Market-oriented computing views computing resources in economic terms such that resource users will need to pay resource providers for utilizing the computing resources [39]. Industry analysts have made bullish projections on how Cloud computing will transform the entire computing industry. According to a recent Merrill Lynch research note [40], Cloud computing is expected to be a “$160-billion addressable market opportunity, including $95-billion in business and productivity applications, and another $65-billion in online advertising”. Another research study by Morgan Stanley [41] has also identified Cloud computing as one of the prominent technology trends.

As the computing industry shifts toward providing Platform as a Service (PaaS) and Software as a Service (SaaS) for consumers and enterprises to access on demand regardless of time andlocation, there will be an increase in the number of Cloud platforms available. Recently, several academic and industrial organizations have started investigating and developing technologies and infrastructure for Cloud Computing. Academic efforts include Virtual Workspaces [42], OpenNebula [43], and Reservoir [44].Amazon Elastic Compute Cloud (EC2) [45] provides a virtual computing environment that enables a user to run Linux-based applications. The user can either create a new Amazon Machine Image (AMI) containing the applications, libraries, data and associated configuration settings, or select from a library of globally available AMIs.The user then needs to upload the created or selected AMIs to Amazon Simple Storage Service (S3), before he can start, stop, and monitor instances of the uploaded AMIs. Amazon EC2 charges the user for the time when the instance is alive, while Amazon S3 [46] charges for any data transfer (both upload and download). Google App Engine [47] allows a user to run web applications written using the Python programming language.Microsoft Azure [48] aims to provide an integrated development, hosting, and control Cloud computing environment so that software developers can easily create, host, manage, and scale both Web and non-web applications through Microsoft data centers. To achieve this aim, Microsoft Azure supports a comprehensive collection of proprietary development tools and protocols which consists of Live Services, Microsoft .NET Services, Microsoft SQL Services, Microsoft SharePoint Services, and Microsoft Dynamics CRM Services. Microsoft Azure also supports Web APIs such as SOAP and REST to allow software developers to interface between Microsoft or non-Microsoft tools and technologies.Sun network.com (Sun Grid) [49] enables the user to run Solaris OS, Java, C, C++, and FORTRAN based applications. First, the user has to build and debug his applications and runtime scripts in a local development environment that is configured to be similar to that on the Sun Grid. Then, he needs to create a bundled zip archive (containing all the related scripts, libraries, executable binaries and input data) and upload it to Sun Grid. Finally, he can execute and monitor the application using the Sun Grid web portal or API. After the completion of the application, the user will need to download the execution results to his local development environment for viewing.

This higher level representation allows us to apply a set of efficient privacy-preserving problem transformation techniques, including matrix multiplication and affine mapping, to transform the original LP problem into some arbitrary one while protecting the sensitive input/output information. One crucial benefit of this higher level problem transformation method is that existing algorithms and tools for LP solvers can be directly reused by the cloud server. Although the generic mechanism defined at circuit level, e.g. [9], can even allow the customer to hide the fact that the outsourced computation is LP, we believe imposing this more stringent security measure than necessary would greatly affect the efficiency. To validate the computation result, we utilize the fact that the result is from cloud server solving the transformed LP problem. In particular, we explore the fundamental duality theorem together with the piece-wise construction of auxiliary LP problem to derive a set of necessary and sufficient conditions that the correct result must satisfy. Such a method of result validation can be very efficient and incurs close-to-zero additional overhead on both customer and cloud server. With correctly verified result, customer can use the secret transformation to map back the desired solution for his original LP problem.

## CONCLUSION

As organizations cope with a dynamically changing business environment, IT managers look to cloud computing as a means to maintain a flexible and scalable IT infrastructure that enables business agility. In June 2009, F5 Networks conducted a study examining the adoption of cloud computing by enterprise IT managers. The study found that although significant confusion regarding the definition of the cloud exists, IT managers are aggressively deploying cloud computing initiatives to accomplish business objectives. Additionally, the study found that widespread enterprise adoption is contingent upon solving access, security and performance concerns.

## 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] Infrastructure Agility: Cloud Computing as a Best Practicehttp://www.computerguys.sg/2011/02/cloud-computing/

[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.

[16] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[17] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 2nd ed. MIT press, 2008.

[18] V. Strassen, “Gaussian elimination is not optimal,” *Numer. Math.*, vol. 13, pp. 354–356, 1969.

[19] D. Coppersmith and S. Winograd, “Matrix multiplication via arithmetic progressions,” in *Proc. of STOC’87*, 1987, pp. 1–6.

[20] MOSEK ApS, “The MOSEK Optimization Software,” Online at http: //www.mosek.com/, 2010.

[21] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *Proc. of EUROCRYPT’99*, 1999, pp. 223–238.

[22] S. Even, O. Goldreich, and A. Lempel, “A randomized protocol for signing contracts,” *Commun. ACM*, vol. 28, no. 6, pp. 637–647, 1985.

[23] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[24] O. Goldreich, S. Micali, and A. Wigderson, “How to play any mental game or a completeness theorem for protocols with honest majority,” in *Proc. of STOC’87*, 1987, pp. 218–229.

[25] W. Du and M. J. Atallah, “Secure multi-party computation problems and their applications: a review and open problems,” in *Proc. of New Security Paradigms Workshop (NSPW)*, 2001, pp. 13–22.

[26] J. Li and M. J. Atallah, “Secure and private collaborative linear programming,” in *Proc. of CollaborateCom*, Nov. 2006.

[27] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, “Delegating computation: interactive proofs for muggles,” in *Proc. of STOC*, 2008, pp. 113–122.

[28] P. Golle and I. Mironov, “Uncheatable distributed computations,” in *Proc. of CT-RSA*, 2001, pp. 425–440.

[29] W. Du, J. Jia, M. Mangal, and M. Murugesan, “Uncheatable grid computing,” in *Proc. of ICDCS*, 2004, pp. 4–11.

IEEE TRANSACTIONS ON CLOUD COMPUTING April 10-15, 2011

[30] Secure and Practical Outsourcing of Linear Programming in Cloud Computing Cong Wang, Kui Ren, and Jia Wang

Department of Electrical and Computer Engineering Illinois Institute of Technology, Chicago, IL 60616, USA Email: {cong, kren, jwang}@ece.iit.edu

[31]Distinguishing Cloud Computing from Utility Computing

[32] Gartner Says Cloud Computing Will Be As

[33]Influential As E-business3. Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved
2009-06-02.

[34]"Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03.. [35]http://www.sellsbrothers.com/writing/intro2tapi/default.aspx?content=pstn.htm

[36] The Internet Cloud-

[37] Cloud Computing Definition, National Insitute of Standards and Technology, Version 15

[38]D. S. Milojicic, V. Kalogeraki, R. Lukose, K.Nagaraja, J. Pruyne, B. Richard, S. Rollins, and Z. Xu. Peer-to-Peer Computing. Technical Report HPL-2002-57R1, HP Laboratories, Palo Alto, USA, 3 July 2003.

[39] D. Abramson, R. Buyya, and J. Giddy. A Computational Economy for Grid Computing and its Implementation in the Nimrod-G Resource Broker, Future Generation Computer Systems,18(8):1061-1074, Oct. 2002.

[40]D. Hamilton. 'Cloud computing' seen as next wave for technology investors. Financial Post, 4
June 2008.

[41]http://www.financialpost.com/money/story.html?id=562877 [18 July 2008]

[42]Morgan Stanley. Technology Trends. 12 June2008. http://www.morganstanley.com/institutional/techresearch/pdfs/TechTrends062008.pdf [18 July 2008]

[43]K. Keahey, I. Foster, T. Freeman, and X. Zhang. Virtual workspaces: Achieving quality of service andquality of life in the Grid. Scientific Programming, 13(4):265-275, October 2005.

[44]OpenNebula Project. http://www.opennebula.org/ [23 July 2008]

[45]Reservoir Project. http://www.reservoir-fp7.eu/ [30 Oct. 2008]

[46]Amazon Elastic Compute Cloud (EC2). http://www.amazon.com/ec2/ [18 July 2008]

[47]Amazon Simple Storage Service (S3). http://www.amazon.com/s3/ [18 July 2008]

[48] Google App Engine. http://appengine.google.com [18 July 2008]

[49] Microsoft Azure. http://www.microsoft.com/azure/ [30 Oct. 2008]

[50] Recession Is Good For Cloud Computing –Microsoft Agrees- http://www.cyberls.com/forum/Thread-Key-features-of-Cloud-computing

[51] Defining “Cloud Services” and “Cloud Computing”

[52] The new geek chic: Data centers-http://simple.wikipedia.org/wiki/Cloud_computing

[53] James Urquhart (January 7, 2010). "Cloud computing's green paradox". CNET News. Retrieved March 12, 2010. "...there is some significant evidence that the cloud is encouraging more compute consumption