Volume 4, Issue 9, September 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Domain of Secure and Practical Outsourcing of Linear Programming in Cloud Computing

B. Sandhya Rani[1], D. Suguna Kuamari[2], M. Roshini[3], Siddireddy Parimala[4]
[1, 4]Department of CSE, RGM College of Engineering &Technology, Nandyal, Kurnool Dt., A.P, India
[2]Department of C S E, Gokaraju Rangaraju Institute of Engineering and Technology, RR Dist, TG, India
[3]Department of C S E, Mother Theresa Institute of Engineering and Technology, A.P, India

Abstract: ***Cloud Computing has great potential of providing robust computational power to the society at reduced cost. It enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Despite the tremendous benefits, security is the primary obstacle that prevents the wide adoption of this promising computing model, especially for customers when their confidential data are consumed and produced during the computation. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing 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, 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. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi honest model.***

Key Terms: Encryption, Affine Mapping, Fully holomorphic encryption

I. INTRODUCTION

The outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing 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, 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. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi honest model. Fully homomorphism encryption (FHE) scheme, a general result of secure computation outsourcing has been shown viable in theory, where the computation is represented by an encrypted combinational Boolean circuit that allows to be evaluated with encrypted private inputs.

The term cloud computing is sometimes used to refer to a new paradigm – some authors even speak of a new technology – that flexibly offers IT resources and services over the Internet. Gartner market research sees cloud computing as a so-called "emerging technology"1 on its way to the hype. When looking at the number of searches for the word pair "cloud computing" undertaken with the Google search engine one can get an imagination of the high interest on the topic. Even terms like "outsourcing", "Software-as-a-Service (SaaS)" or "grid computing" have already been overtaken2. Cloud computing can be seen as an innovation in different ways. From a technological perspective it is an advancement of computing, which's history can be traced back to the construction of the calculating machine in the early 17th century3. This development continued with the invention of the analytical engine (1837), the logical engine (1885) and the tabulating machine (1890)4. The actual history of modern computing began with the invention of the first computers (Z3 in 1941 and ENIAC in 1945)5. Since then advancements emerged at a good pace. The sixties and seventies were the ages of mainframe computing. Central computing resources were harnessed through terminals that provided just the input and output devices to interact with the computer. With the development of the first microprocessor (1969) hobbyists began to construct the first home computers, before mail-order kits such as the Altair 8800 were sold in 1975. Other computer manufacturers like Apple, Atari or Commodore entered the market for computer home users, before IBM introduced its personal computer (PC) in 19816. Since then the development paced up, the diffusion of PCs increased significantly and an increasing miniaturization lead to the development of laptop computers and mobile devices. Another important technology, which paved the way for cloud computing was the development of the ARPAnet (1969), a fail-proof communications network which became today's Internet7. Soon, services like e-mail or the World Wide Web, a hypertext based information management system, gained

popularity. Technologies like Java, Ajax, Web Services and many more supported the development of rich, interactive websites. Eventually whole applications could be deployed over the Internet, which was around the year 2000 referred to as Software-as-a-Service8. In analogy to the provision of software via the web, computing resources could also be accessed via the Internet. Especially for scientific purposes grid computing got established in the early 1990ies9. When looking at this brief history of computing, one can easily see the different streams from local calculating machines, to central mainframes, via personal computers and handheld devices to the new
quasi centralization trend that can be seen in cloud computing. Yet a different point of view is to look at cloud computing from an IT provisioning perspective. In this sense cloud computing has the potential to revolutionize the mode of computing resource and application deployment, breaking up traditional value chains and making room for new business models. Many providers like Amazon, Google, IBM, Microsoft, Salesforce or Sun positioned themselves as platform and infrastructure providers in the cloud computing market. Beside them there emerge more and more providers, who build their own applications or consulting services upon infrastructure services offered by other market players.

II. SYSTEM OVERVIEW

Our contribution shall focus on the IT provisioning perspective of cloud computing. It will start with a literature review on current definitions of cloud computing and a conceptual framework of different service layers. It will further examine the evolution from outsourcing to cloud computing as a new IT deployment paradigm. Hereby it highlights the effects on the outsourcing value chain, summarizes market actors and their roles within a new cloud computing value network, and finally discusses potential business models for IT service providers.

Existing System:

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. On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing. 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, 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. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi hones model. For example, for the computations that require a large amount of computing resources, there are huge financial incentives for the cloud to be "lazy" if the customers cannot tell the correctness of the output. Besides, possible software bugs, hardware failures, or even outsider attacks might also affect the quality of the computed results. Thus, we argue that the cloud is intrinsically not secure from the viewpoint of customers. Without providing a mechanism for secure computation outsourcing, i.e., to protect the sensitive input and output information of the workloads and to validate the integrity of the computation result, it would be hard to expect cloud customers to turn over control of their workloads from local machines to cloud solely based on its economic savings and resource flexibility. For practical consideration, such a design should further ensure that customers perform fewer amounts of operations following the mechanism than completing the computations by themselves directly. Otherwise, there is no point for customers to seek help from cloud. Recent researches in both the cryptography and the theoretical computer science communities have made steady advances in "secure outsourcing expensive computations"

Proposed System:

On the one hand, the outsourced computation workloads often contain sensitive information, such as the business financial records, proprietary research data, or personally identifiable health information etc. To combat against unauthorized information leakage, sensitive data have to be encrypted before outsourcing 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, 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. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semi honest model.

III. IMPLEMENTATION

Fully holomorphic encryption (FHE) scheme, a general result of secure computation outsourcing has been shown viable in theory, where the computation is represented by an encrypted combinational Boolean circuit that allows to be evaluated with encrypted private inputs.

Module Description:

1. Mechanism Design Framework
2. Basic Techniques
3. Enhanced Techniques via Affine Mapping
4. Result Verification

Mechanism Design Framework:

We propose to apply problem transformation for mechanism design. The general framework is adopted from a generic approach, while our instantiation is completely different and novel. In this framework, the process on cloud server can be represented by algorithm ProofGen and the process on customer can be organized into three algorithms. These four algorithms are summarized below and will be instantiated later.

KeyGen(1k) → {K}. This is a randomized key generation algorithm which takes a system security parameter k, and returns a secret key K that is used later by customer to encrypt the target LP problem. **ProbEnc(K,_)** → {_K}. This algorithm encrypts the input tuple _ into _K with the secret key K. According to problem transformation, the encrypted input _K has the same form as _, and thus defines the problem to be solved in the cloud.

ProofGen(_K) → {(y, □)}. This algorithm augments a generic solver that solves the problem _K to produce both the output y and a proof □. The output y later decrypts to x, and □ is used later by the customer to verify the correctness of y or x.

ResultDec(K,_, y, □) → {x,⊥}. This algorithm may choose to verify either y or x via the proof □. In any case, a correct output x is produced by decrypting y using the secret K. The algorithm outputs ⊥ when the validation fails, indicating the cloud server was not performing the computation faithfully.

Basic Techniques

Before presenting the details of our proposed mechanism, we study in this subsection a few basic techniques and show that the input encryption based on these techniques along may result in an unsatisfactory mechanism. However, the analysis will give insights on how a stronger mechanism should be designed. Note that to simplify the presentation, we assume that the cloud server honestly performs the computation, and defer the discussion on soundness to a later section. Hiding equality constraints (A, b): First of all, a randomly generated m × m non-singular matrix Q can be part of the secret key K. The customer can apply the matrix to Eq. (2) for the following constraints transformation, $Ax = b \Rightarrow A'x = b'$ where $A' = QA$ and $b' = Qb$.

Enhanced Techniques via Affine Mapping

To enhance the security strength of LP outsourcing, we must be able to change the feasible region of original LP and at the same time hide output vector x during the problem input encryption. We propose to encrypt the feasible region of _ by applying an affine mapping on the decision variables x. This design principle is based on the following observation: ideally, if we can arbitrarily transform the feasible area of problem _ from one vector space to another and keep the mapping function as the secret key, there is no way for cloud server to learn the original feasible area information. Further, such a linear mapping also serves the important purpose of output hiding.

Result Verification

Till now, we have been assuming the server is honestly performing the computation, while being interested learning information of original LP problem. However, such semi honest model is not strong enough to capture the adversary behaviors in the real world. In many cases, especially when the computation on the cloud requires a huge amount of computing resources, there exist strong financial incentives for the cloud server to be "lazy". They might either be not willing to commit service-level-agreed computing resources to save cost, or even be malicious just to sabotage any following up computation at the customers. Since the cloud server promises to solve the LP problem $\_K = (A', B', b', c')$, we propose to solve the result verification problem by designing a method to verify the correctness of the solution y of _K. The soundness condition would be a corollary thereafter when we present the whole mechanism in the next section. Note that

in our design, the workload required for customers on the result verification is substantially cheaper than solving the LP problem on their own, which ensures the great computation savings for secure LP outsourcing. The LP problem does not necessarily have an optimal solution. There are three cases as follows.

Normal: There is an optimal solution with finite objective value.

Infeasible: The constraints cannot be all satisfied at the same time.

Unbounded: For the standard form in Eq. (1), the objective function can be arbitrarily small while the constraints are all satisfied.

Algorithm Used:

KeyGen(1k) → {K}.

This is a randomized key generation algorithm which takes a system security parameter k, and returns a secret key K that is used later by customer to encrypt the target LP problem.

ProbEnc(K,_) → {_K}.

This algorithm encrypts the input tuple _ into _K with the secret key K. According to problem transformation, the encrypted input _K has the same form as _, and thus defines the problem to be solved in the cloud.

ProofGen(_K) → {(y, □)}.

This algorithm augments a generic solver that solves the problem _K to produce

both the output y and a proof □. The output y later decrypts to x, and □ is used later by the customer to verify the correctness of y or x.

ResultDec(K,_, y, □) → {x,⊥}.

This algorithm may choose to verify either y or x via the proof □. In any case, a correct output x is produced by decrypting y using the secret K. The algorithm outputs ⊥ when the validation fails, indicating the cloud server was not performing the computation faithfully.

Conclusion and Perspectives

Considering the historic development of providing IT resources, cloud computing has been established as the most recent and most flexible delivery model of supplying information technology. It can be seen as the consequent evolution of the traditional on-premise computing spanning outsourcing stages from total to the selective, and from the multi-vendor Outsourcing to an asset-free delivery. While from a technical perspective, cloud computing seems to pose manageable challenges, it rather incorporates a number of challenges on a business level, both from an operational as well as from a strategic point of view. As laid out above, cloud computing in its current stage also holds a number of contributions for both theory and practice that this article could reveal and that will be addressed below.

IV. REATED WORK

4.1 Contribution to Research:

The field of cloud computing research is only just emerging. Existing research focuses particularly on the technical aspects of the provision of a cloud, particularly in the area of grid computing and virtualization. Business models and value chains have been studied only to a limited degree. In this respect, this article takes a first step by systematically bringing together the various definitions of cloud computing and combining them under one coherent definition. As a major result, this article could elaborate on the building blocks of understanding the substantial elements of the cloud computing concept, i.e., the characteristics of service, hardware, software, scalability and Internet/network. Also pay-peruse billing models and virtualization belong to the core elements of the new cloud concept. In addition, the article could contribute to a systematic description of major actors (such as, e.g., customer, service provider, infrastructure provider, aggregator, platform, consulting and data integrators) entering the cloud computing market. Such a description can provide a first step towards systematically investigating the value network of cloud actors and can also shed light on analyzing where the value of cloud services is captured.

4.2 Contribution to Practice

The development of outsourcing and cloud computing towards a more flexible delivery model laid out in this paper has a strong impact not only from an academic point of view, but also particularly on practical business issues. Thereby, both the client and provider perspective of cloud computing and outsourcing services have to be taken into consideration.

4.2.1 Perspectives for Customers

Cloud computing is closely related to the general question of whether IT resources should be provided internally or externally and in both cases *how* they should best be delivered. Holding their own IT resources, such as, e.g., a datacenter does often not make sense for many customers and is too much effort, especially for small or startup companies. In Armbrust's words, this "would be as startling for a new software startup to build its own datacenter as it
would for a hardware startup to build its own fabrication line"84. Here, externally sourcing IT resources in a cloud computing model provides new opportunities for a flexible, usage dependent sourcing of IT resources. Besides start-up companies, also established organizations can take advantage of the elasticity of cloud computing regularly. Similar to the underlying idea of selective sourcing or on-demand outsourcing models, cloud computing can provide flexibility and efficiency in terms of cost variabilization (monetary flexibility) and also in terms of availability of IT resources (IT flexibility).

Moreover, the flexibility associated with cloud computing can also be used in settings where clients keep their IT in-house. So-called private clouds allow clients to efficiently manage their IT resources and balance peak loads and idle time in an optimal way. These opportunities should be considered in future decisions. However, the potential gains in flexibility and efficiency come along with some risks, for example, in the field of data security that needs to be taken into account. Breaking up the traditional outsourcing value chain uncovers a variety of new configurations and different actors which may result in the development of complex value networks that need to be identified and managed accordingly.

4.2.2 Perspectives for Service Providers

For service providers new opportunities arise from both a technical as well as from a business view. From a technical view, the construction of very large data centers using commodity computing, storage, and networking resources facilitated the opportunity of selling those resources on a pay-per-use basis below the costs of many medium-sized datacenters, while at the same time serving a large group of customers. From a business view, the challenges and
Opportunities are even more interesting. Here, service providers benefit from breaking up the outsourcing value chain to position themselves in the market and to offer new services. As the market for cloud computing services has not yet a clear shape we now observe a phase of experimentation where new and viable business models are explored. Especially in the field of service aggregation and integration new opportunities for service providers emerge. Even without large investments in infrastructure reliable and powerful services can be offered that use the infrastructure of established providers such as Amazon or Google.

4.3 Outlook and Further Research

In a broad understanding, cloud computing can be regarded as an evolution in the development of outsourcing models, i.e., the provision of IT resources. The business challenges of the user and the specific customer requirements for cost reduction, flexibility, and innovation are met in a more granular and mature way. At the same time, cloud computing as a new technological concept asks the same basic question as outsourcing does: Consequently, the same problems, challenges, and issues are raised that have already been posed in the various stages of the development of outsourcing (see Figure 1). In analogy to the evolution in outsourcing, cloud computing is in the initial phase where asking for the participation ("if or if not"), for the motivation ("why cloud computing", "cui bono?") and for the subject ("what should be done externally") is relevant. While cloud computing might be regarded as the consequent development of the established organizational concept of outsourcing on the basis of a new technological concept, it states an even more holistic claim. Extending many aspects of IT outsourcing, cloud computing shifts the focus from an exclusive technological perspective to a broader understanding of business needs. It addresses the most prevailing business needs of flexibility, availability, and reliability, as well as economies of scale and skill and lays out how the technological concept of cloud computing can meet (both in an aligning and enabling claim) these business challenges.

However, these considerations are only just beginning and focus primarily on the causes and manifestations of cloud computing. From an academic perspective, future research should focus on two major topics in this context: First of all, many practitioners label cloud computing as a disruptive innovation. Although uncovering a number of new features, one has to investigate further whether cloud computing can live up to these expectations and deserves the label disruptive technology. By drawing analogies from other business models and technologies that were successful or not successful in the past, one can evaluate the sustainability of the new cloud computing paradigm.

A second promising research stream focuses on the business challenges associated with the rise of the new computing paradigm. New players – formerly active in other core markets – entered the cloud computing market and are now in competition with established IT (service) providers. As one major consequence, the traditional value chain breaks up and develops a complex value network with a myriad of established and new players on different layers in

the cloud computing stack. It has to be investigated what the newly evolving value network looks like and where the value of cloud computing is captured in the long-run.

V. CONCLUSION

This paper provides a convenient solution to the problem of secure outsourcing of Linear Programming. The computations of LP are taken place in cloud as the client has not equipped with such resources. The proposed system is efficient and provides complete security to outsourced computations and the data while transit. The mechanism practically divides the work into private data and public LP solvers. The important aspect of this system is that it not only provides secure data transmission but provides ways and means to verify the correctness of data as well. Thus it is made cheating resilient. The verification mechanism is bundled with the security solution without any additional computational overhead.

We plan to investigate some interesting future work as follows: Devise robust algorithms to achieve numerical stability; Explore the sacristy structure of problem for further efficiency improvement; Establish formal security framework; Extend our result to non-linear programming computation outsourcing in cloud.

REFERENCE

[1] P. Mell and T. Grance, "Draft nist working definition of cloud com- puting," 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] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. H. Spafford, "Secure outsourcing of scientific computations," AdvancesinComputers, vol. 54, pp. 216–272, 2001.

[4] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proc. ofTCC, 2005, pp. 264–282.

[5] 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.

[6] M. Atallah and K. Frikken, "Securely outsourcing linear algebra com- putations," in Proc. of ASIACCS , 2010, pp. 48–59.

[7] 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.

[8] 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.

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

[10] V. Strassen, "Gaussian elimination is not optimal," Numer. Math , vol. 13, pp. 354–356, 1969.

[11] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," in Proc. of STOC'87, 1987, pp. 1–6.

[12] MOSEK ApS, "The MOSEK Optimization Software," Online at http: //www.mosek.com/, 2010.

[13] P. Paillier, "Public-key cryptosystems based on composite degree resid- uosity classes," in Proc. of EUROCRYPT'99 , 1999, pp. 223–238.

[14] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," Commun. ACM , vol. 28, no. 6, pp. 637–647, 1985.
[15] S. Boyd and L. Vandenberghe, Convex Optimization. Cambridge University Press, 2004.
[16] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, Introduction to Algorithms, 2nd ed. MIT press, 2008.
[17] V. Strassen, "Gaussian elimination is not optimal," Numer. Math., vol. 13, pp. 354–356, 1969.

Author's Profile

Ms. B. Sandhya Rani, Post Graduated in Computer Science & Engineering (M.Tech), **St. Johns college of Engineering &Technology** and Graduated in Computer Science & Engineering (B.Tech), **ALFA college of Engineering & Technology**. She is working presently as an Assistant Professor in the Department of Computer Science & Engineering in **RGM College of Engineering &Technology**, Nandyal, Kurnool Dt., A.P, INDIA. She has 2+ years Experience. She has interest in Cloud Computing, Data Mining, Image Processing, Parallel and Distributed computing and Computer Networks.

Mrs D.Suguna Kuamari, Post Graduated in Computer Science (M.Tech), ANU, 2010, and Graduated in Information Technology (B.Tech) From JNTU Hyderabad, 2006. She is working presently as AssitantProfessor in Department of Computer Science & Engineering in **Gokaraju Rangaraju Institute of Engineering and Technology**, RR Dist, A.P, INDIA. She has 6+ years Experience. Her Research Interests Include Software Engineering, Cloud Computing, Operating Systems and Information Security.

Mrs. M. ROSHINI Post Graduated in Computer Science & Engineering (M.Tech), **Madina Engineering College, KADAPA**, 2011. She is working presently as an Assistant Professor in the Department of Computer Science & Engineering in **Mother Theresa Institute of Engineering &Technology**, Palamaner, Chittoor Dt., A.P, INDIA. She has 3+ years Experience. Her interest in Cloud Computing, Data Mining, Image Processing, Parallel and Distributed computing and Computer Networks.

Ms. Siddireddy Parimala Post Graduated in Computer Science Engineering (**MCA**) From **Kasturbha Gandhi College for Women's**. She is working as Assistant Professor in Department of Computer Science & Engineering in **RGM college of Engineering &Technology**, Nandyal, Kurnool Dt., AP, India. She has 4+ years of Teaching Experience. Her research interests include Network Security, Cloud Computing & Data Warehousing and Data Mining.

