Abstract:
Cloud computing empowers clients with constrained computational assets to outsource their substantial calculation workloads to cloud, and financially appreciate the gigantic computational force, data transmission, stockpiling, and even suitable programming that can be partaken in a pay-per-use way. Security is the essential snag that keeps the wide reception of this promising figuring model, particularly for clients when their private information are devoured and created amid the calculation. Regarding the cloud as a characteristically frail processing stage from the cloud's perspective clients, we must outline systems that not just secure delicate data by empowering calculations with encoded information, additionally shield clients from noxious practices by empowering the calculation's acceptance result. So as to accomplish handy proficiency, our system plan unequivocally deteriorates the Linear Programming (LP) calculation outsourcing into open LP solvers running on the cloud and private LP parameters possessed by the client. The subsequent adaptability permits us to investigate fitting security tradeoff by means of more elevated amount deliberation LP calculations than the general circuit representation. Specifically, by detailing private information claimed by the client for LP issue as an arrangement of networks and vectors, we have the capacity to build up an arrangement of productive security saving issue change strategies, which permit clients to change unique LO (P) issue into some discretionary one while ensuring delicate data/yield data.

Keywords: Public Cryptography, LP Parser, LP Definition Creator, RSA Algorithm, Robust Algorithm

I. Introduction
Cloud computing gives advantageous on-interest system access to a common pool of configurable figuring assets that can be quickly conveyed with extraordinary productivity and insignificant administration overhead. One principal point of interest of the cloud worldview is calculation outsourcing, where the computational force of cloud clients is no more restricted by their asset requirement gadgets. By outsourcing the workloads into the cloud, clients could appreciate the actually boundless processing assets in a pay-per-use way without submitting any extensive capital costs in the buy of equipment and programming and/or the operational overhead there in. The outsourced calculation workloads frequently contain delicate data, for example, the business money related records, restrictive examination information, or actually identifiable wellbeing data and so on. To battle against unapproved data spillage, touchy information must be scrambled before outsourcing [3] in order to give end-to-end information classification confirmation in the cloud and past. Then again, the operational subtle elements inside the cloud are not sufficiently straightforward to clients [5]. Thus, there exist different inspirations for cloud server to carry on unfaithfully and to return inaccurate results, i.e., they may act past the traditional semi-legit model. For instance, for the calculations that oblige a lot of processing assets, there are enormous monetary motivating forces for the cloud to be "apathetic" if the clients can't tell the yield's rightness. Plus, conceivable programming bugs, equipment disappointments, or considerably outcast assaults may likewise influence the nature of the processed results. In this way, we contend that the cloud is inherently not secure from the perspective of clients. Without giving an instrument to secure calculation outsourcing, i.e., to ensure the touchy data and yield data of the workloads and to accept the calculation's honesty result, it is difficult to anticipate that cloud clients will turn over control of their workloads from neighborhood machines to cloud
Direct Optimization (LO) [also called Linear Programming] is a strategy to accomplish the best result, (for example, most extreme benefit or least cost) in a scientific model whose necessities are spoken to by straight connections. Straight Optimization is an exceptional instance of scientific programming. Straight programming can be connected to different fields of study. It is utilized as a part of business and financial matters, yet can likewise be used for some building issues. The issue of unraveling an arrangement of straight imbalances goes back in any event to the extent Fourier, after whom the technique for Fourier-Motzkin disposal is named. The Linear Optimization strategy was initially created by Leonid Kantorovich in 1939.[2] Leonid Kantorovich built up the most punctual Linear Optimization issues in 1939 for utilization amid World War II to arrange consumptions and returns keeping in mind the end goal to lessen expenses to the armed force and build misfortunes to the foe. The system was kept mystery until 1947 when George B. Dantzig Cloud the simplex strategy and John von Neumann built up the hypothesis of duality as a direct enhancement arrangement [1] We utilize the Random Number Generation procedure; Quality in the irregular number era (RNG) procedure is quite often needed for security, and absence of value by and large gives assault vulnerabilities thus prompts absence of security, even to finish bargain, in cryptographic frameworks. The RNG procedure is especially alluring to assailants in light of the fact that it is regularly a solitary secluded equipment or programming part simple to find. On the off chance that the aggressor can substitute pseudo-irregular bits produced in a manner he can foresee, security is completely traded off, yet for the most part imperceptible by any upstream test of the bits. LO (P) calculations oblige a significant measure of computational force and for the most part include secret information, we propose to expressly break down the LO (P) calculation outsourcing into open LO (P) solvers running on the cloud and private LO (P) parameters possessed by the client. The adaptability of such deterioration permits us to investigate larger amount reflection of LO (P) calculations than the general circuit representation for the handy effectiveness. In particular, we first define private information claimed by the client for LO (P) issue as an arrangement of networks and vectors. This larger amount representation permits us to apply an arrangement of effective security saving issue change systems, including framework augmentation and relative mapping, to change the first LO (P) issue into some self-assertive one while ensuring the delicate data/yield data. One critical advantage of this more elevated amount issue change strategy is that current calculations and devices for LO (P) solvers can be straightforwardly reused by the cloud server.

II. Related Work

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.

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.

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 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.

**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.

**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.

![Classificatory framework](image)

**III. Problem Statement**

We consider a computation outsourcing architecture involving two different entities, as illustrated in fig. 1, the cloud customer, who has large amount of computationally Expensive LP problems to be outsourced to the cloud; the Cloud Server (CS), which has significant computation resources and provides utility computing services, such as hosting the public LP solvers in a pay-per-use manner. The customer has a large-scale linear programming problem $\Phi$ to be solved. However, due to the lack of computing resources, like processing power, memory, and storage etc., he cannot carry out such expensive computation locally. Thus, the customer resorts to CS for solving the
LP computation and leverages its computation capacity in a pay-per-use manner. Instead of directly sending original problem $\Phi$, the customer first uses a secret $K$ to map $\Phi$ into some encrypted version $\Phi_k$ and outsources the problem $\Phi_k$ to CS. CS then uses its public LP solver to get the answer of $\Phi_k$ and provides a correctness proof $\Gamma$, but it is supposed to learn nothing or little of the sensitive information contained in the original problem description $\Phi$. After receiving the solution of encrypted problem $\Phi_k$, the customer should be able to first verify the answer via the appended proof $\Gamma$. If it’s correct, he then uses the secret $K$ to map the output into the desired answer for the original problem $\Phi$. The security threats faced by the computation model primarily come from the malicious behavior of CS. We assume that the CS may behave beyond “honest-but-curious”, i.e. the semi-honest model that was assumed by many previous researches (e.g., [4], [5]), either because it intends to do so or because it is compromised. The CS may be persistently interested in analyzing the encrypted input sent by the customer and the encrypted output produced by the computation to learn the sensitive information as in the semi-honest model. In additions can also behave unfaithfully or intentionally sabotage the computation, e.g. to lie about the result to save the computing resources, while hoping not to be caught at the same time. We also use the robustness for numerical stability.

IV. Security Analysis
More specifically, a verifiable computation scheme consists of three phases:

Preprocessing A one-time stage in which the client computes some auxiliary (public and private) information associated with $F$. This phase can take time comparable to computing the function from scratch, but it is performed only once, and its cost is amortized over all the future executions.

Input Preparation When the client wants the worker to compute $F(x)$, it prepares some auxiliary (public and private) information about $x$. The public information is sent to the worker.

Output Computation and Verification Once the worker has the public information associated with $F$ and $x$, it computes a string $p_x$ which encodes the value $F(x)$ and returns it to the client. From the value $p_x$, the client can compute the value $F(x)$ and verify its correctness.

Ciphertext-Policy FE: It is possible to obtain a ciphertext-policy FE scheme by constructing a dual of the above scheme. The structure of the ciphertext and key get interchanged. A key will encode a string $w$ and a ciphertext [13] will encode an automaton $M$. Also, randomization in $G_p$ is done only for the key (i.e., components corresponding to the input string $w$). The same assumptions can also be used for the proof of security.

V. 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. The Linear Programming outsourcing scheme which provides a complete outsourcing solution for not only the privacy protection of problem input/output, but also its efficient result checking. It start from an overview of secure LP outsourcing design framework and discuss a few basic techniques and their demerits, which leads to a stronger problem transformation design utilizing affine mapping. The process on cloud server can be represented by algorithm ProofGen and the process on customer can be organized into three algorithms (KeyGen, ProbEnc, and Result Dec). Note that our proposed mechanism provides us one-time pad types of flexibility. Namely, we shall never use the same secret key $K$ to two different problems. Thus, when analyzing the security strength of the mechanism, we focus on the cipher text only attack.
VI. Experimental Results

Linear Results:

Table 1: Linear Results

<table>
<thead>
<tr>
<th>Equation</th>
<th>Benchmark</th>
<th>Original Problem</th>
<th>Encrypted Problem</th>
<th>Cloud Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>7</td>
<td>0.7</td>
<td>0.957142857</td>
</tr>
<tr>
<td>2</td>
<td>109</td>
<td>200</td>
<td>0.127</td>
<td>0.947761194</td>
</tr>
<tr>
<td>3</td>
<td>45</td>
<td>198</td>
<td>0.2</td>
<td>0.740740741</td>
</tr>
<tr>
<td>4</td>
<td>300</td>
<td>200</td>
<td>0.321</td>
<td>0.990740741</td>
</tr>
<tr>
<td>5</td>
<td>233</td>
<td>700</td>
<td>0.544</td>
<td>0.961130742</td>
</tr>
<tr>
<td>6</td>
<td>1500</td>
<td>3</td>
<td>0.666</td>
<td>0.951428571</td>
</tr>
<tr>
<td>7</td>
<td>2344</td>
<td>2000</td>
<td>0.899</td>
<td>0.977173913</td>
</tr>
</tbody>
</table>

NonLinear Results:

Table 2: Nonlinear Results

<table>
<thead>
<tr>
<th>Equation</th>
<th>Benchmark</th>
<th>Original Problem</th>
<th>Encrypted Problem</th>
<th>Cloud Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>N</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1.66</td>
<td>18.59</td>
<td>0.245</td>
<td>0.907407</td>
</tr>
<tr>
<td>2</td>
<td>39.45</td>
<td>89.99</td>
<td>0.297</td>
<td>0.99</td>
</tr>
<tr>
<td>3</td>
<td>39.54</td>
<td>89.99</td>
<td>0.432</td>
<td>0.903766</td>
</tr>
<tr>
<td>4</td>
<td>90.00037</td>
<td>90.00082</td>
<td>0.544</td>
<td>0.959436</td>
</tr>
<tr>
<td>5</td>
<td>-116.11</td>
<td>106.43</td>
<td>0.788</td>
<td>0.987469</td>
</tr>
<tr>
<td>6</td>
<td>1887.7</td>
<td>899</td>
<td>0.9</td>
<td>0.986842</td>
</tr>
<tr>
<td>7</td>
<td>2787.7</td>
<td>899</td>
<td>1.2</td>
<td>0.973236</td>
</tr>
</tbody>
</table>


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.

VII. 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.

Reference


Fig. Graph of Non Linear results

![Graph of Non Linear results](image_url)