proceedings

MDPI

Abstract

Ethical Considerations in Cloud Computing Systems

Hamid Reza Faragardi

[1] School of innovation, design and engineering, Mälardalen University, Sweden; hamid.faragardi@mdh.se
* Correspondence: hamid.faragardi@mdh.se; Tel.: +46-(0)21-15 17 79
† Presented at the IS4SI 2017 Summit DIGITALISATION FOR A SUSTAINABLE SOCIETY, Gothenburg, Sweden, 12-16 June 2017.

Published: date: 9 June 2017

Abstract: Cloud computing is a new generation of computing systems, increasingly developing as a promising solution to deal with the explosion of computing complexity and data size. One of the main concerns to shift from traditional computing systems to Cloud is ethical consideration. In many cases, ethical issues depend on particular applications and circumstances. However, we intend to identify ethical issues of Cloud, inherent in the fundamental nature of the technology rather than specific circumstances. There are multiple technological criteria affecting ethical issues in Cloud, such as security; privacy; compliance and performance metrics. Along with the technological criteria, a set of rules and regulations called *Terms and Conditions* (T&C) effects on ethics in the Cloud. T&C is an agreement specifying the rights and obligations of users, Cloud providers, and third parties. In this ongoing research work, we aim to firstly investigate the main technological criteria affecting ethics in Cloud, while at the same time, we provide a discussion to indicate that how each of these criteria influences ethics. Secondly, we consider the relationship between the T&C rules and ethics. Finally, we have a quick look at ethical issues in Cloud versus traditional web-based applications.

Keywords: Ethics; Cloud Computing; Security; Privacy

1. Introduction

Cloud computing enables users to access on-demand services in a pay-as-you-go fashion from any corner of the world [1]. Cloud computing, on the other hand, leads to exposing multiple ethical issues inherent in pushing both services and data from local servers into data centers which belong to an external party. Traditionally, enterprises were buying their own computing infrastructures to run their applications, such as financial analysis, distributed data processing, high performance computing, etc. In traditional infrastructures, data and services were stored and processed locally, which results in much more control on data in comparison to Cloud, in which controls and responsibilities are shared between the application owner and Cloud providers. When the hardware is not shared, unauthorized access to data could be restricted easily, due to more concrete data protection solutions in comparison to a shared infrastructure model. However, owning an infrastructure incurs having to purchase hardware and high operating costs, as the result of maintenance and upgrade of software and hardware. Moreover, this approach does not allow the infrastructure capacity to scale up or down depending on the current resource demands. Cloud computing addresses such problems (high maintenance cost and scalability) by outsourcing the services in a pay-as-you-go manner. Nonetheless, Cloud is still new, so ethical discussion is also nascent yet [2], in comparison to that for traditional computing models, hence it needs to be mature. There are different model of services provided by a Cloud. The first model is Software-as-a-Service (SaaS), where specific online services are provided by Cloud providers, e.g., Goggle Docs and Dropbox services. The second form of services is infrastructure as a service (IaaS), where hardware resources (such as CPU, memory, storage and communication bandwidth) are provided for

customers. In this self-service model, users can create their own virtual machines and specify the required processing power of the VMs and networking services (e.g. firewalls). Example of this model is Microsoft Azure and Amazon web services. The third model is Platform-as-a-Service (PaaS), where besides the infrastructures, a platform to develop an application is provided. PaaS (e.g., Apprenda) makes the development, testing, and deployment of applications quick, simple, and cost-effective.

There are various technological criteria having an influence on arising of ethical issues in Cloud. Among them, security, privacy, compliance and performance metrics have a greater impact on ethical issues. In the following, we demonstrate how each of these technological criteria can have a direct impact on ethical considerations in Cloud. In future work, we explain how far these criteria have been elaborated and standardized in the context of Cloud computing.

Privacy and Security: When an unauthorized access to your sensitive data resident in a Cloud is gained-- either by a hacker or by the Cloud provider itself or a third party-- you may never know who and how your data will be abused, which can lead to several ethical challenges. Therefore, privacy and security mechanisms are obviously essential to avoid such ethical issues.

Compliance: A major part of privacy and security mechanisms are formed as a set of standards. A Cloud service should comply with a subset of the standards with respect to the application of the service. In other words, *compliance* covers a set of principles that should be considered during both development and maintenance process of the system. When a Cloud-based application in the SaaS model with some privacy or security requirements (e.g., the application including customer payment credentials) is going to be launched in the market, it should comply with the predefined standards. Moreover, it is one of the significant parameters to choose a Cloud provider to get either IaaS or PaaS services. If the Cloud provider conflicts with the compliance, then it cannot be chosen as a provider by the clients having the compliance requirements.

Performance metrics: The expected performance of the provided services are stipulated in Service Level Agreement (SLA), which is a part of the general terms and conditions, concentrating on performance metrics. Availability and application response time are a couple of examples of SLA metrics. In the case of the violation of the performance metrics of SLA, there is a penalty mechanism to compensate the customers. A part of the SLA performance metrics are not highly strict, meaning that in the case of a minor violation, the compensation for SLA violation is not made.

Generally, there could be three major reasons for why a violation from an SLA metric does not result in compensation, 1. The flexibility of the promising range for a performance metric (it is not highly strict). 2. The metric is not exactly measurable by users, thus a minor violation is not noticeable for them. To illustrate the concept, first have a look at an example from the airline industry. If the departure time is delayed more than a certain number of hours (N hours), then the compensation of passengers is made, however if it does not exceed N hours, no compensation is made. Imagine if the airlines gain a benefit from the minor delays for which do not pay the penalty, then this issue is considered as an ethical issue. Now let us consider an example from the IaaS Cloud services. A client requests for a VM with one CPU, since the CPU utilization of the VM is not 100% all the time, the Cloud resource scheduler dedicates the remaining portion of the CPU utilization to other VMs. When the CPU utilization of the VM goes up, there is a policy to prepare the requested CPU utilization for the VM by either migration of other VMs running on the CPU to other CPUs, or killing them. However, imagine that the policy is not completely fair, in the sense that it does not provide the promising CPU utilization immediately in order to gain a higher profit for the Cloud provider. As long as the delay is minor and does not result in compensation for SLA violation, the customer rights are not respected. In turn, it is a case of ethical issues.

Since in Traditional Web-Based Applications (TWBA) physical servers are outsourced and shared, just similar to Cloud, similar ethical issues can happen. However, in the following, we describe which issues overlap and what are the differences between TWBAs and Cloud in terms of ethical issues. We will also examine that whether Cloud computing provides a better form of computing in terms of ethical issues in comparison to TWBAs, or not.

An acceptable level of security, privacy, compliance and performance in all IT layers should be held to not only fulfill the T&C agreement, but also to expect a reasonable level of ethics for Cloud services.

If only a few of the software and infrastructure components fulfill these criteria, then ethical problems may occur in using Cloud services. For example, if there is a security bug in the level of software components (which basically are a set of software services that a Cloud application in PaaS model is developed as the composition of these services), the Cloud application is not well-secured, and the users' data could be accessed by a hacker through this layer.

In addition to the mentioned technical criteria, other criteria can also cause an ethical issue such as:

Environmental impacts: An important easily forgotten stockholder affected by Cloud computing is the *environment* [2]. In 2007, Gartner estimated that ICT industry generates about 2% of the total global carbon dioxide emission, which is equal to the aviation industry [4]. Even though Cloud data centers afford to pay the cost of their huge energy consumption [1], they must minimize the energy consumption along with striving to use as much as a green source of energy as possible [1].

In addition to the technical aspects, *Terms and Conditions* (T&C) is another criterion, dramatically affecting ethics in Cloud. T&C agreement is a set of rules and obligations that acts as a legal contract between the Cloud provider and customer, determining the obligations and rights of all parties. T&C not only reflects the expectations derived from the technological criteria, but it also contains the conditions and penalties in the case of the violation of the rules, in the sense that what would be the responsibility of Cloud providers, what would be that for the application owner (we call it client), and finally what are the rights of the end users.

2. Ethics borders in Cloud environment

It should be noted that the satisfaction of the above-mentioned criteria (i.e., technical criteria and T&C) is a necessary condition to achieve a desirable level of ethics, not a sufficient condition. In the following, we expound what is the relation between the rules of the mentioned criteria and ethics, in details. Basically, ethical challenges arise when:

1. There is not a set of specific rules, or the rules are ambiguous, in the sense that they can be interpreted in different ways. When there is not a specific rule for an issue came up just now, the role of ethics comes to play. Therefore, both rule-makers for Cloud and negotiators on T&C agreement who come from the client side must struggle to consider as much as possible situations, and make a clear rule to figure out these situations to minimize the ethical issue in the system. As an example of this case, in the negotiated level of security, most likely is mentioned that if somebody tried (either successful or unsuccessful) to gain access to your data, then the Cloud provider will let you know. However, if somebody has already gained access to a part of the data and might not be a clear evidence that your data is also accessed or not, then whether the provider let you know as a warning that there is a risk of stealing the data. Although this may not be mentioned in the agreement, it is admirable to inform customers in term of ethics.
2. During setting up the rules --which is usually driven by big Cloud provider companies, or government IT regulations -- ethical considerations must be taken into account. Particularly, the rules specifying the rights of customers in the case of violation of the rules. In this step, unions and Consumer Protection Organizations (CPO) can play a key role.
3. There are specific rules for an event just happened, but there is not an efficient monitoring to detect whether these rules are violated or not. This case is more likely to happen for the two first criteria and the last one (i.e., privacy, security, and performance). Monitoring could be more complicated when not only the user's data itself, but also meta-data are abused. The two following examples clearly reflect this issue:
    - The visit rate of hospital in a long period could give meaningful information about your health condition without needing any access to the medical information, which can be abused by insurance institutions for the life insurance services.
    - The physical location that from there you access your Cloud service can also give information about your personal life, even though the data itself is not accessed.

[1] The energy consumption of data-centers worldwide is estimated 26GW, corresponding to about 1.4% of the total energy consumption in the world with a grow rate of 12% per year [4].

3. Cloud VS traditional web-based applications

Since responsibilities are divided between the application owner and Cloud provider, the problem of many hands' appears. Since many people have had the opportunity to prevent undesirable consequences, no-one can be held responsible [2], while this problem is not the case for TDWBs, where the host provider is only responsible to physically secure the servers.
Since Cloud service providers uses various resources/ storages in multiple data centers geographically distributed around the world, customers' services and data might be allocated into several physical locations in different countries. When this happens, customers might not have strict control on their data which can be sensitive data, such as applications source code, users credential, encryption algorithms and keys, log servers and operational and security procedures. Cloud providers are allowed to use only the data centers located in the countries that comply with the compliance requirements of the clients, to ultimately avoid data exposure. It is not the case for TWBAs since a client often knows in which state the host is located.
Overall, comparing TWBAs with Cloud applications in terms of ethics, it highly depends on 1. The set of concrete rules and regulations preserving the rights of customers, 2. The negotiation part of the T&C. This problem is more considerable for end users in comparison to Cloud clients that are usually enterprises, because clients usually have a lawyer(s) to not only inspect the fulfillment of the commitments, but also to negotiate to modify a part of T&C to achieve their expectations.

4. Related works

In [2] ethical issues of Cloud computing are taken into account, however technological criteria (such as privacy, security, compliance) are ignored. They start with reviewing the ethical issues exist in the context of ICT, and then the overlapped issues with the Cloud are addressed. Additionally, different stockholders of Cloud computing are thoroughly listed, then the ethical issues may occur from each of these stockholders' sides are briefly indicated. There are also many research papers in the literature which only cover a technological feature, such as privacy and security [3].
In this paper, besides technical issues, the ethical perspective of Cloud is considered.

5. Summary and Concluding Remarks

In this paper, we had a glance at ethical considerations in Cloud. We firstly provided a general picture of the problem through demonstration of the challenges; secondly, clarified the border between technical criteria (such as: privacy, security, compliance and performance metrics) and the ethical issues. In other words, we discussed how the development of solid technical mechanisms could also improve ethical aspects in a Cloud. Moreover, we explained that in addition to the mentioned technical issues, a concrete set of rules and regulations for all parties should be provided to minimize the ethical challenges. We finally explored some differences between traditional web-based applications and Cloud services. In future work, more technical features corresponding to the each of the technical criteria are interleaved.

References

1. H. Faragardi; A. Rajabi; T. Nolte; A. Heidarizadeh. A Profit-aware Allocation of High Performance Computing Applications on Distributed Cloud Data Centers with Environmental Considerations. CSI Journal on Computer Science and Engineering (JCSE). CSI. 2016..
2. B. D. Bruin; L. Florida. The ethics of Cloud computing. Journal on engineering ethics, pp. 614-620. Springer, 2016.
3. J. Zhou; Z. Cao. Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, pp. 26-33. IEEE. 2017.
4. C. Petty. Gartner estimates ICT industry accounts for 2 per-cent of global CO2 emissions. [Online]. Available: http://www.gartner.com/it/page.jsp?id=503867.