Reputation in Cloud Computing

Adrian Yanes
Aalto University
School of Science and Technology
adrian.yanes@aalto.fi

Abstract

Nowadays the concept of cloud computing is getting popular around the Net. The capacity and scalability that cloud computing offers is making it an alternative to consider when a good infrastructure is needed. It does not matter what kind of application it is, if a cloud is used with it is due to the necessity to scale at any moment, besides the capability to have unlimited resources when they are needed. Cloud companies are offering different combinations of services and configurations, due to the nature of the cloud; software as a service (SaaS) vendors don't usually mention hardware availability, space or process capacity at all, instead promoting their services along with the concept of "unlimited".This paper studies how software as a service could hold problems of performance and availability when the users share the same resources and cloud. The author propose different theoretical mechanisms to avoid the problems of reputation in the cloud computing systems. Thus solutions in which the user's behavior, user's ranking, and the costumer democracy are taken in consideration to develop different ways to fix of the current threads.

Keywords: cloud computing, reputation, social web, user network iteration.

1 Introduction

The concept of cloud computing has been an achievable goal in the Computer Science during the last few years. The possibility of unlimited and instantaneous expansion was one of the objectives for the new age of the Internet. For a while, such idea of utilizing so many processors and capacity available for everyone was inconceivable. Nowadays, in the current market we may find several companies offering cloud computing services. Due to the nature of these services (software as a service), vendors are seizing the opportunity to fully acquit their investment. Claiming them to be a "company's secret", vendors hide the mechanisms used to offer these services; that means that users obtain a certain amount of calculation power, RAM memory, disk space, but they don't know what hardware is beside those numbers. That is not a problem except when the vendors are putting together the users sharing the same resources without preceding notice. As it is evident, cloud computing is powerful but it means high costs [6] with the current technology. For that reason vendors and costumers are finding different formulas to offer their service maintaining quality/price balance. As a result of this we may find nodes shared between users; and here comes the problem of reputation. This practice is creating a new scenario on the market: users should be able to share their cloud resources if they wish to. However, even without the wish of the users, vendors need to share resources internally due to a question of performance. The problem of reputation concerning the user's behavior inside of the cloud has been identified as one of the main problems of the cloud computing [1]. The first cases of this problem have appeared in the last years [11] [3] , although not frequently enough; the cloud's costumers are going to need some reputation system to guarantee the safety of their investment in a specific service. Thus new mechanisms [13] were founded in order to avoid any server abuse, as it has happened in the past with spam. The concept of blacklisting that was applied in other networking fields to be used in the fight spam. Due to the fact that cloud has been used for spam purposes too [10], same solutions have been proposed to fix possible problems within cloud resources. Although companies are worried about their costumers, both sides share mutual interest of that issue and at some point (such as the spam problem) the cooperation is crucial. This paper goes through different architectures and the possible combination of technologies in order to redesign tools to avoid this behavior. The idea is to find new means of assurance of safe and productive co-existence between the users within the cloud. Due to the nature of this technology, the current situation concerning the cloud architecture is difficult to analyze. The concepts showed here should be applied in general and as reference; furthermore it is possible that nowadays some vendors are implementing some kind of mechanism to fix the problem. The best scenario will be to have a non platform-specific "reputation standard" applicable to any cloud. Naturally, this indicates a strong need for cooperation between vendors, as well as their customer's approval. Considering cloud computing as the future of computation in terms of availability and data processing, a good example could be the current social communities on the Internet, in which the interaction is based on user "karma": user contribution appreciation systems. Currently, several examples of communities, which define own users through such systems are easily observable. Such communities can be found at **Digg.com**, **Reddit.com**, **Meneame.net**. The same principles of interaction could be applied to the cloud. This paper takes in consideration the Web 2.0 interaction as a possible basis, on which a rich and functional community can be built. Although the business side in this kind of communities is not quite as strictly defined within such communities, the business involved in the cloud may adopt the same pattern, as user behavior in both

Figure 1: Cloud scenario

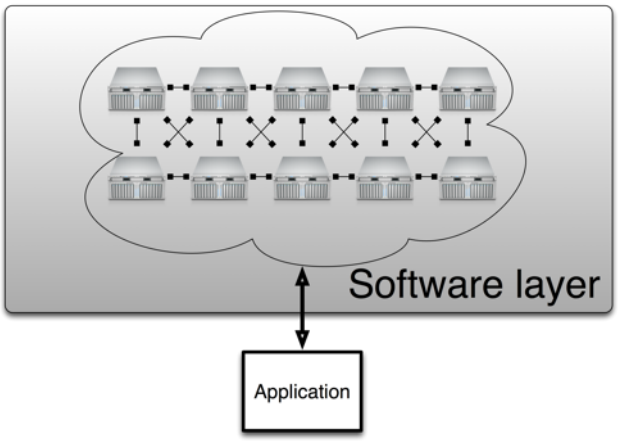

Figure 2: Cloud architecture

is comparable.

2 Background

The following sections analyzes the basic infrastructure and the user participation in the cloud computing.

2.1 Cloud Architecture

The nature of the cloud technology implies completely different concepts when compared with traditional models offered by the service providers. Traditional models are highly-dependent on hardware availability and calculation capacity (memory and CPU cycles available). Cloud computing services are based in the following concepts:

- **Capacity to grow unlimited**
- **Distributed responsibility**
- **Interactive applications**
- **Parallel batch processing**
- **Elasticity**

These concepts define the technical basis of the cloud and convert it in a new paradigm as a service. For years, this kind of architecture has been used internally for ISPs and companies with a big demand for space, bandwidth and calculation capacity. This origin pushed the technology to grow, possessing a mentality of an internal infrastructure. Before Google and Amazon AWS offered such services, the technology was never thought to be used as "public" service, projecting this some issues in the conceptual architecture of the cloud that persists until today creating, as a result, "reputational issues" inside of the clouds. As it is common in terms of technology, nobody gave a thought about the highly demanded capacity and availability needed "on the fly" from the costumer's side. But the current scenario is just the opposite. Several companies are using cloud services generating an amount of traffic and power consumption unimaginable some years ago.

2.2 Cloud providers and ISP's

Traditional models are extremely hardware-dependent due to the architecture (Figure 2) used in them, being based in hardware availability and the old concept of "plug more as is needed". This model caused several issues during years due to it the need of buying new hardware, without considering the matter if the new hardware is needed permanently or only for a few hours. Obviously, the costs of this practice, implies a high short-term risks.

Service providers notice that this practice was valid in the old times, but due to the amount of traffic and the Internet's growing rhythm. The solution came from a dynamic and scalable [2] architecture [8], these concepts were resumed in to order to ignore the traditional models and focus on the new needs. Thanks to the high demand of the availability and reliability of such services [9] the result came as an end of solution-based software (Software as a Service, SaaS). The cloud technology is build, based on a skeleton of a thousand machines running a software model that provides a transparent scenario, ready to offer the same advantages of the traditional models plus the new features mentioned above. This scenario provides a reliable infrastructure although the 100% still not guarantee [14] Cloud is thought to be used as a normal data center infrastructure but at the same time is offering the possibility for small organizations/customers to have available the same services as big corporations. This model increases the investment requirement at first, although it could be even more expensive when adhered to the traditional models. We should have the concept of cloud as a software layer hiding the hardware layer. The software layer offers a transparent way to execute applications with powerful resources. The concept of individual machine disappears, giving room for the concept of "cloud identity" as the representation of software-transparent cluster.

2.3 Costumers and cloud services

With the traditional models the costumer had a more specific description of what they are buying, in terms of hardware. In the traditional models concepts such as number of cores, memory available, etc. were a part of the requirements given. This implies the need to know how many machines are available, the location, the capacity, etc; this scenario disappears with the cloud. The costumer has a scenario in which he only

knows what limits he shouldn't pass if he doesn't pay more than the negotiated. Thus, the costumer gets supplied according to his necessities but assuming an implicit risk: the infrastructure that he is buying is not only for him, as other costumers are using the same setup for their own businesses. This means sharing the resources of the cloud, which implies high risk in certain situations. Although service providers guarantee a minimum of services and a quality of availability and calculation procession, a costumer can collapse the cloud in some sporadic situations. This behavior will affect to all the costumers that are sharing the same cloud "region". Some companies are even offering now services focused in the security at the cloud [7]

2.4 The costumer's behavior within the cloud

The infrastructure created by the cloud service providers changes depending on the specific company. All of them offer security and privacy guarantees inside of the cloud, although such claims cannot be verified deeply by the costumers (due to the architecture used). But the problem doesn't arise from the service provider itself, as they offer a product and they want to maintain customer satisfaction levels. The issue is the behavior of users of the service in terms of resources demand and ethics, concerning the use of the cloud. At the same time the cloud is identified as a service and not as individual machines [10]. This means that if some costumer is abusing the service (such as SPAM, DDoS attacks, etc), the whole number of users of that specific cloud could be prosecuted or at least put through an investigation. The result of this could be that the IP range of the cloud could end up in some anti-spam list or, if the cloud is used for some illegal activity, the service provider will be given a legal issue, which is passed on to its users, along with the corresponding legal implications. Services providers establish different means to maintain the individuality inside of the cloud, assigning identification and isolated spaces to the costumers, but due to the Internet topology, individuals outside of the cloud will be recognized as an individual identity represented by a corporation (Google, Amazon, etc). In the following sections the author proposes some mechanisms to apply inside of the cloud to create and maintain a "reputation" system which objective is to guarantee a legal liability in the cloud services. On the other hand as it is described as the major issue in other papers [5] , the users' behavior cannot be accurately predicted. Labeling concepts applied to users, such as "newcomers" or "veterans" are used in all Internet communities, creating an invisible hierarchy of the users, providing an easy behavior differentiation mechanism. Same structure can be applied to cloud computing: different levels of expertise or usage longevity can define the new communities inside of the cloud.

3 Models proposed

In this section the author analyzes different alternatives proposed based in hypothetical solutions for the current threads. Due to the reputation can't be optimize with high accuracy without human interaction, every model proposed involve some type of interaction in the user's side. Although different automatize mechanisms could be establish to control things as bandwidth, CPU, memory consumption, etc.

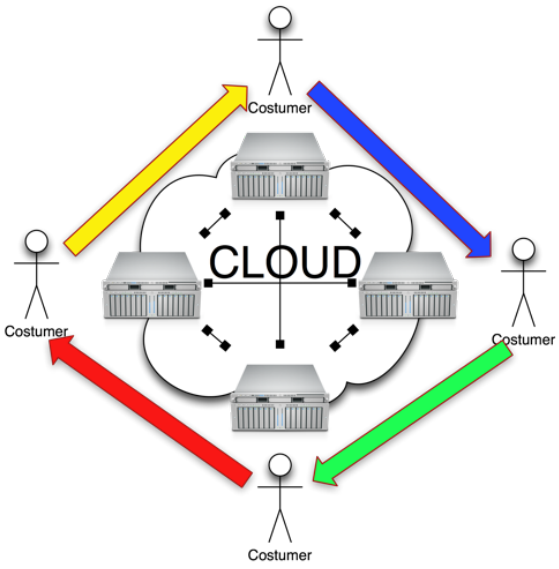

Figure 3: Trusted keyring of costumers

3.1 Public keyring concept in the cloud

A concept of public keyring similar to the one used in cryptography [12], can be applied to the cloud architecture. A public key ring is defined as *"a resource of public keys which a correspondent's key is validated by personally checking his key's fingerprint and then signing his public key with your private key."* In order to have your PGP [13] key signed by other person, you should meet that person and provided some legal proof as passport or an ID card to verify your identity; after that the person will sign your key and export the signature to the public keyring. Same procedure can be applied in a small, modified version. Cloud services provider can offer an optional service in which the costumers can know with who they are sharing the cloud (previous authorization of the customer), after to know the other costumers they should to find an agreement in which the objectives of every costumer are exposed and approved by the other costumers. This survey can be organize and managed digitally with a certain voting mechanism and be put as condition in the agreement when someone is buying a cloud service. The result of this is a democratic decision (Figure 3) about the use of the internal resources of the cloud in some specific region. If the method is accepted as condition of the contract the service provider have a strong legal mechanism to deny the use of service to a certain abuser, with the support of the other costumers of the cloud. The only problem that complicates the use of this method is that the costumer should admit their identity (losing some privacy with such action), but at the same time they will have the ability to know who are their "neighbors" in terms of technology infrastructure.

3.2 Social algorithms

In the introduction of this paper, the author mentioned some web sites in which the iteration is based in anonymous social reputation. In this case the mentioned web sites have a goal to publish the most relevant links based in mechanism of "karma" or "points of trust" of their users. The result of this is that only the links considered "relevant" by the community end up on the main page. Some of the algorithms [5] of these web sites are under company's secrecy policy, but others are public. If we analyze some of them we can see that the most common method to evaluate the behavior of the user (thus the quality of his criteria to vote a link) are the activities that he does at the site and the quality of them. The equation can be viewed as a mix between: visit frequency, comment quality (voted by other users), vote frequency and link submission. Same concept can be applied to the cloud if the necessary mechanisms are established. A cloud can contain a tool to evaluate the behavior of others user through a "costumer voting". The system must show a daily/weekly/monthly resume of the activity of the costumer such bandwidth use, CPU use, memory consumption etc. At the same illegal or non ethics activities should appear in the dashboard. With this system the others costumers can evaluate and vote if they consider if some user of the cloud should be punished. The system can maintain a reputation inside of the cloud based on its own users. At the same time the cloud service provider must be moderating the system as some users can approach the opportunity to punish wrongfully other costumers for commercial reasons.

3.3 Costumer region rotation

The nature of the clouds implies the capability to move data without "limits" inside of the cloud' infrastructure. This capability allows the cloud service provider to re-allocate the workload of the system in different parts of the cloud. A rotation system can be establish to maintain dynamic location (concerning IP's ranges or countries) in which the costumer are executing their software, this rotation could cause some technical problems for some costumers, but in general it shouldn't be a big issue for the services providers due to the setup architecture of the cloud. Costumer will maintain the same services/capabilities but they will have "different" neighbors every certain time, this dynamic re-allocation maintains a ecosystem inside of the cloud due to the problematic costumer can be identified easily (if they are problematic, new neighbors will report a issue).

4 Discussion

The problem of reputation at the cloud has been identified from the first days of the cloud era. Users' behavior is unpredictable and chaotic in most of the cases, although the security mechanisms inside of the cloud guarantee a good security and privacy tools inside, the cloud is viewed as individual identity on the Internet. Probably the problem resides within the topology applied in the architecture: trying to optimize capacity and availability of the cloud service providers are forcing to have a strong decency of the common resources, projecting the problems in reputation, software fails, etc. On the other hand the market spoke regarding the necessity of to have the software as a service linked to the high availability and capacity. Current situation offers different paths to evolve; some of them implied important modifications in the fundamental architecture of the cloud, others, as were exposed in this paper, imply addition of new tools and practices inside of the cloud in order to acquire more reliability.

5 Conclusion

Cloud computing opened a new era of possibilities on the Internet. For a while the same infrastructure used inside of the services worked without big problems. Now the same concept is offered to the general public, all the advantages that the services providers had for a while are availability close to anyone with enough resources to buy a cloud services. The users' behavior is really difficult to put under control and although most of the mainly costumers are companies, some of them have conflict commercial interest and can generate problems of reputation inside of the cloud. Due to modifications of the cloud architecture are highly ambitious, the cloud service providers must think in add-on solutions to the current setup. The software layer offered from the cloud is a good point to start defining democratic process between costumers. At the same time different common practices can be applied some fix partially the problems of reputation, some of them are create rankings of fair use or trust-rings in which other costumers can trust when they are sharing the space with other companies. At the same time the current laws looks obsolete when applied to concepts such as "cloud" or "service community". Maybe one of the biggest issues is the absence of some legal [4] [8] mechanism to stop malpractices, such as SPAM, DDoS attacks, etc. Several points related with the cloud concept must be improved to guarantee the same quality of services (in some aspects) than in the traditional models. As final conclusions is mandatory take in consideration that user reputation is one the current and future threads in terms of cloud computing. Although the technology is getting mature in a short time period, the user interaction is still needed. The different methodologies exposed in this paper are another alternative to the current solutions. At the same time the implementation of mechanisms of reputation depends in a high grade of the user's wishes. Companies and individuals must request these services to the cloud computing vendors. Finally and to complement a successful progress in the cloud computing coexistence, the current laws should be improved to take in consideration new scenarios in which costumer's rights are implied.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[2] A. Corporation. http://aws.amazon.com/autoscaling/.

[3] N. Farrel. Pirate bay raids cause mass fall out. June 2006.

[4] K. Fiveash. Microsoft's top lawyer demands a cloud computing law. January 2010.

[5] M. E.-P. L. Guanfeng Liu Yan Wang Orgun. "a heuristic algorithm for trust-oriented service provider selection in complex social networks". July 2010.

[6] J. HAMILTON. Cooperative expendable micro-slice servers (cems):low cost, low power servers for internet-scale services. *CIDR '09*, January 2009.

[7] http://www.trustedcomputinggroup.org/. Trusted computing group.

[8] A. Khajeh-Hosseini, I. Sommerville, and I. Sriram. Research challenges for enterprise cloud computing. *CoRR*, abs/1001.3257, 2010.

[9] D. Kossmann, T. Kraska, and S. Loesing. An evaluation of alternative architectures for transaction processing in the cloud. In *SIGMOD Conference*, pages 579–590, 2010.

[10] L. Liu and W. Shi. Trust and reputation management. *IEEE Internet Computing*, 14:10–13, 2010.

[11] T. Mennecke. Aftermath of the pirate raids. June 2006.

[12] C. PGP. The pgp encryption platform. Technical report, 2010.

[13] N. F. A. Ramachandran and S. Vempala. Filtering spam with behavioral blacklisting. 2007.

[14] A. STERN. Update from amazon regarding friday s3 downtime.