Defining a Pure, Open Cloud

debunking the three myths surrounding cloud adoption and building an open, pure cloud

September 2012
## Contents

Executive Summary

The Pure, Open Cloud

What is Cloud Computing

Security in the Cloud

Integration in the Cloud

Scalability in the Cloud

Next Steps
Executive Summary

Cloud Computing is quickly becoming the design focus and investment objective for IT organizations between now and 2025. The vast majority of organizations have already begun projects to investigate, pilot, learn, and understand the models and issues that they need to address.

The three issues often cited by early adopters, as well as detractors of cloud computing, are security, integration, and scalability. This is because there are few working examples of what cloud computing could ultimately deliver to the organization, and because these issues are leftovers conflicts between client-server (albeit hybrid) and internet architectures. An open cloud model, what has been proposed since the mid-1960s as a corporate model of distributed computing to be used in the organization, is the solution to the three problems.

An open cloud model can address security by leveraging the distributed services, their inherent trust of each other, and tokenized service calls. While it may sound complicated, it simply states that by leveraging the infinitely scalable and replicated aspects of the open cloud, and the secure model on which it relies to authenticate trusted, secure connections between components and services, any organization can have far more secure implementations than they do today, and rely on third parties to make sure this is the status quo – as opposed to having to continuously worry about it.

Similarly, integration is handled in cloud computing by leveraging the security model, but most importantly the ability of the cloud to transfer data and information between components faster, easier, and better – without requiring additional hardware or software components that what it provides (applications will need to be redesigned to take advantage of this, but similarly to the security issues – it is then left to providers to serve your needs better). Not only can an open cloud model integrate data faster, it can include more data elements in a far more secure, and compliant environment, than today’s vendors can do.

However, it is with the scalability issue that cloud computing can truly deliver. Cloud computing is based on distributed architectures models that are purely meant to scale execution to infinite levels. This almost endless source of scalability is what makes the cloud computing model a place to invest for organizations. In an era where computational requirements grow at an accelerated pace, as more business functions are moved online and to the internet – and ultimately to the cloud, unlimited scalability to support this growth is the foremost concern for IT organizations – and something that cloud computing can deliver.

Adopting an open cloud model is not simple or fast. We estimate it will take the best part of the next 10-15 years for most organizations. However, as providers begin to make significant improvements to their offerings and to deliver enterprise-quality solutions, wise organizations are investigating how that changes their architectures, and making the necessary changes.

This white paper summarizes these issues and the steps to take to get to an open cloud model.
The Pure, Open Cloud

The Cloud is here, no questions about it.

No, not talking about “the cloud” as a misnomer for the Internet, rather talking about Cloud Computing – a concept that is bound to change the way organizations work and interact.

Unfortunately, today cloud computing is misrepresented by vendors and misunderstood by IT departments and users hoping to embrace it. At the very core of this discussion is the issue of using an open or private cloud; an issue pushed forward by vendors that are unable to use cloud computing as intended and are looking for a way to simulate Cloud Computing. Their argument says that establishing a Private Cloud is the only way for nervous CIOs that need to adopt cloud computing to solve the main issues with cloud computing: security, scalability and integration.

CIOs and IT personnel listening to that message are easily convinced: closed, protected solutions implemented behind a firewall (the model for a Private Cloud) with monitored connection to the public internet sounds attractive for organizations that look at the Internet as “the Wild Wild West”.

Except, that the argument is awfully wrong; there is no such thing as a Private Cloud.

Reading Wikipedia’s\(^1\) definition of Cloud Computing, we quickly see many statements that call for openness, sharing of resources, elasticity, and abstraction of infrastructure delivered over an open network (“typically the Internet”).

Cloud providers, like Rackspace\(^2\), define cloud computing as “simply a set of pooled computing resources and services delivered over the web”.

The NIST\(^3\) (National Institute of Standards and Technology) while addressing the existence of the concept of Private Cloud as a deployment model still highlights one of the five essential characteristics of Cloud Computing to have a “Broad Network Access”.

Alas, this is not an exercise on splitting hairs and fighting over the words in a definition. Rather, it is an attempt to show why Private Cloud cannot address these three core concerns of cloud adoption as well as a real open cloud model.

Let’s start with the basics.

---

2. [http://www.rackspace.com/cloud/what_is_cloud_computing/](http://www.rackspace.com/cloud/what_is_cloud_computing/)
What is Cloud Computing

The concept behind cloud computing originated in the 1930s from experiments carried out by the US military in how to implement distributed systems for faster execution of tasks. It was not until the 1950s that we have the first mentions of cloud computing (back then the references were made to distributed computing or network computing). Through the past few decades, cloud computing became better developed and defined. Today we call cloud a distributed model of computing that leverages an open and extensible network to allocate processing power from many different independent computers to accomplish a single task faster and simpler.

A Cloud Computing model must have three-layers. In spite of the commonly embraced misconception that "the cloud" is an equivalent with the Internet, a misconception that oversimplifies a complex concept with a half-truth, the cloud computing model cannot function effectively without the three layers.

These three layers are what allow those adopting the model to solve the issues of security, integration and – most importantly – scalability; it is inherent to their existence. The next sections will explore these in more detail.

Security in the Cloud

This is a big topic, if you use your favorite search engine (Google\(^5\), but don’t let me bias you – go ahead and use Ask.com or DogPile.com or your favorite one) and enter the phrase (that means use quotation marks when searching) “Is the Cloud Secure” and you will be the proud owner of 167,000+ links. Apparently lots of people want to talk about Security in the Cloud.

Even Gartner stepped up to the plate and talked about security in the cloud. In a report from the Global IT Council on deploying cloud services\(^6\) they highlighted Security as the 6\(^{th}\) (out of seven) concerns. That means it is there, but not top priority and does not deserve as much time to figure it out.

The high-level argument on security in the cloud can be summarized in one paragraph:

> The fear of security is created by two factors: one, the data that travels in open networks is potentially unsafe and hackers can get to it; two, the data that is not stored in protected equipment within the control of the organization can be accessed by anyone. An additional layer of misunderstanding is brought about by the embracing of multi-tenancy: the fear that in multi-tenant systems that store all data in a single database accessible by anyone, the commingling of data can lead to confusion and the wrong people accessing the wrong data.

Let’s tackle each of these factors separately.

First, data traveling in open networks is susceptible to being hacked. In theory, this is true, a proper cloud implementation leverage security tokens (created and managed in the platform layer, using one of many solutions that can provide virtually unlimited options) that can easily encrypt and protect the data with little or no performance penalty for using them. This is core to the cloud: the communication between platform layers definitely can handle the tokenization and authorization that comes with it.

There are, still, ways for hackers to get the data if they really, really want to – there are always ways to do so. The only fail-safe method against that is to disconnect the computer for all networks and prevent it from


communicating with the outside world. This is not feasible, which is why we developed many different methods for protecting the data. If a hacker were to want to get the data, it would be far simpler to break into the database where it is stored than to try to intercept the many encrypted packages (if they could guess which ones they are from the many traveling through the network) and rebuild the data.

Besides, cloud computing deployments – even if you remove the tokenized security model – are better than most other systems when it comes to exposing data. The fact that it breaks down tasks into several smaller steps and executes each one separately makes a big difference in how secure it can become.

Proper cloud development adds another layer of security to the application by breaking down the transaction, distributing the processing among many servers, and forcing it to make calls to different systems to resolve the different pieces of logic. That makes tracking and retrieving all of the necessary packets from the network virtually impossible.

In addition to this distributed model and the tokenization model inherent to cloud computing, there is always the weakest point in all security models to consider: people. There is nothing you can do that is fool-proof in security; chances are high you already hired the “fool” that can break it. The best model for security, in the cloud or outside of the cloud, comes down to proper training of people, implementation of many tiers of security, and a comprehensive security model that targets your solution and your needs. Intel and many others have built their models (either for internal consumption or for their customers) and they have shared them. I cannot say that I fully agree with both of them (they cover what to do with virtualized and private clouds – neither are models of cloud I endorse), but the rest of the documents are very nicely done and cover all this in more detail.

The second part of the myth of lack of security has to do with Data Residency, or where the data lives. There are many compliance implications behind data residency beyond the scope of this publication but let’s assume, for the sake of brevity, that compliance on data residency is not an issue or the solution implemented is compliant. The fear that organizations have is that by placing their data elsewhere they lose control and secure access to the data. In a recent blog post for Forbes, Eric Savitz explained it very well in these terms:

> Most cloud computing companies are like experienced airline pilots. They are well trained, have backup systems and contingency plans in case they encounter an issue, and they have a full staff of professionals regularly checking and maintaining their service. Cloud software companies, knowing the implications of a crash on their business’ bottom line, invest significant resources into insuring that such a disaster never occurs. Cloud computing companies can invest far more resources in data backup and security than your business can.

I don’t know how much more I can say, but in simple terms – if you believe you data is no safer in a company whose long-term survival depends on simply ensuring that your data is available, safe, and

---

protected versus your setup that simply wants to keep the data backed up periodically – well, you need to rethink your concept of data security.

Finally, my most favorite myth: the fact that deploying your data in a multi-tenant database will expose your data to be (potentially) accessible by someone else when they (or the cloud services providers) make a mistake. As it has been proven time and time again, this is simply not true – and will just leave it at that instead of mentioning the campaigns from vendors to grow FUD in this market before sweeping in with their awesome solutions to resolve that fear, uncertainty and doubt.
Integration in the Cloud

Security seems like a simple solution, a tokenized model allows for easy and fast connections to virtually anywhere the cloud reaches, and it is fully protected by many layers of verification. Integration is a little more daunting; the high level issue with integration in the cloud is:

(...) integration between bottom-layers (IaaS – Infrastructure as a Service) that leverage the security model explained above are far more secure than trying to send data over the open internet or opening ports in the firewall. The lack of integration stem from the fact that without a corporate cloud computing infrastructure in place (which the vast majority of organizations don’t have in place yet), the connectivity among IaaS layers is not possible. (...) Embracing a cloud computing infrastructure inside the organization can easily address Integration in an open cloud.

In reality, there are two models for integration in the cloud: data connectors and platform (or infrastructure) connections (a good summary of both models can be found here⁹). They both leverage the service delivery model of cloud computing, but in different manners.

A platform-level connection will establish a trusted, semi-permanent link between two platforms, allowing each one to “do their job” and transfer data back-and-forth. Each of the platforms will be aware of the existence of each other, the rules that each follows for security and access, and the services that each supports. The calls between platforms are not application driven, rather requesting data and access to certain applications or infrastructure resources that they have access to. Applications request the data from the platform, which in turn requests the data from the other platform or infrastructure providers. A good example of how this is done is TIBCO and similar EAI-style providers.

Let’s use an example, for simplicity. Organization A has a CRM solution that is cloud-based and needs to access partner-owned data about common customers (provided the agreements are in place already and architects created the platform-to-platform links) from organization B. Organization’s A CRM

solution (a SaaS-based one) will make the request from the platform supporting it, which in turn will
travel over the internet and request from platform B the necessary data, provide all the identification
and security elements necessary to make the request, and bring the data back to platform A, which will
then provide it back to CRM A.

While this may sound like a point-to-point integration play of on-premise and similar to what we do
today there are a few differences: if organization B were to change their CRM solution or database
solution, A would not mind and would (if B did a good job) not even notice. Further, if organization C
comes into play at a later stage with more data that must be accessed by A – the hard work of creating
rules and security setup is already done and can be easily replicated with any other platform. Even
better, A can either bring new SaaS solutions or use Applications via an Enterprise Application Store that
will leverage that connection without even having to worry about it.

The second model, data connectors, is simpler to setup and has fewer benefits – but nevertheless can
leverage cloud computing equally well.

A data connector in the cloud is a service call that is embedded within a SaaS application to draw data
from another SaaS. This occurs over the open network, following fewer rules than in a platform-to-
platform connection and, obviously, yielding a lot less flexibility and data. In a service all between SaaS
layers the amount of data that can be transferred is very limited due to security and privacy rules in play at each
application. This is what we think of, traditionally, when we talk about “cloud integration”.

Let’s use the same example as above between organization A and organization B, but this
time they make a service call as opposed to rely on their platform-to-platform
integration. The amount of data that each application can
expose to service calls is very

limited and mostly relegated to cross-reference, non-contextual, and non-identifiable information (this
is usually controlled by the security and privacy rules resident in the platform that supports each
software application). Thus, A can request a confirmation that a customer does exist, that a specific
data element (if approved before hand) exists, but they cannot expect much more from B.
This is a very simplistic view of the two models for integration and the benefits are understandable when explained this way. The actual level of complexity is not quite so easy and there are many more elements to address when doing integration in the cloud – but the bottom line, it is not as hard as most people would expect, it is quite similar to what organizations are doing today (but with tons more flexibility and dynamism), and it actually works the same (if not better) than on-premise.

For more information on the different models, you can find a more detailed explanation of the different methods for application integration in the cloud is provided by IBM here\textsuperscript{10} and more on the SaaS-to-SaaS integration model provided by Dell here\textsuperscript{11}.

\textsuperscript{10} \url{http://www-01.ibm.com/software/integration/cast-iron-cloud-integration/#}
\textsuperscript{11} \url{http://www.boomi.com/files/boomi_whitepaper_the_quest_for_cloud_integration_strategy_final.pdf}
Scalability in the Cloud

Having solved the issues of security and integration in the cloud are actually the hard things to do. Alas, most cloud detractors focus on the issue as scalability as the sine-qua-non for cloud adoption. Which is actually almost laughable, since the early concept of cloud (and ever since then continues to be) was focused on leveraging scalable models. Distributed architectures, the underlying architecture for cloud computing, are all about almost infinite scalability. The most concerning aspect of scaling the cloud is that organizations are replacing the three-layer model with components that can be replicated in infinite scalability with virtualization (which provides a “private”, secure cloud that has unlimited scalability according to their proponents).

While it is true that virtualization can provide scalable resources on-demand12 (with certain limitations), it is also true that since it happens inside a private and protected network it depends on the provider of virtualization (which is always the enterprise) to provide as many resources as necessary making the growth of the model dependent on the resources available at any time. Public IaaS providers (Amazon’s Elastic Compute Cloud13 model is the most famous, but there are others like Microsoft’s Azure14 and Rackspace15 among many) can provide virtually unlimited resources by working together to provide capability as needed.

Let’s start at the end, why may we want to scale?

According to F516 scalability is a way for organizations to know that they have CAP (capacity, availability, performance) under control for their applications. While in non-cloud environments this is achieved by using load-balancing and HA (high-availability) models, in the cloud this is far simpler to achieve by using distributed computing techniques and replication of resources. This model of scalability in the cloud is called Elasticity and it is at the heart of what Amazon EC2 offers. Of course, there are plenty of other vendors who offer it as well (there are other models, like Grid Computing, that offer a similar solution not exclusively for cloud environments, but the performance in a Grid setup is not comparable to what a cloud solution can provide – but that is the topic of another publication17).

The problem that most organizations face is that they equate cloud or even elasticity with automatic scalability. This is not the case, but it is easy to see why that thought is prevalent. In traditional scalability, non-cloud computing models, the scalability is done in a “scale up” model – more hardware is necessary, more hardware can be brought online and when it is no longer needed, it can be “put away”. Since the model of adding hardware is left to the provider, and they sell this specific feature, the organizations that moved their resources to the cloud assume they are fully covered in regards to scalability.

13 http://aws.amazon.com/ec2/
14 http://www.microsoft.com/windowsazure/
15 http://www.rackspace.com/cloud/
There is one problem that remains. In stark contrast with non-cloud computing, scalability in the cloud must address two other aspects: design and “scaling out” capabilities. Without addressing these three areas, scalability is not addressed.

Design is the ability of the application to leverage and use scalability provided by the cloud. This is not something that happens automatically, but something that must be designed into the application. Having the cloud infrastructure does not guarantee that the applications can use it – it simply means that the investment was done to have a scalable, flexible, secure, and integration-ready architecture. The next step is to redesign the applications, or to find the providers with the right SaaS applications, that can take advantage of that. In a manner similar to High Availability implementations – just because they are there does not mean that your applications can use them.

Finally, in addition to “scaling up” (the most common model of scaling known to organizations, and the one used by High Availability solutions), the true cloud application will be designed to also “scale out”. This is where infinite scalability, and frankly the most promising feature of an open cloud, comes in handy. Scaling out is not about throwing more hardware to a problem in one location, but about distributing the workload to more services available in different locations. At the heart of distributed architectures, scaling out is what makes the cloud what it is.

SaaS, PaaS, and even IaaS can replicate their services as much as they want, but organizations can also find other providers that can deliver similar, if not best results, and use them to scale their implementations. Indeed, the ultimate challenge of designing for the cloud is not to find a provider and use their “scaling up” model of throwing more hardware at any problem, but to find several providers of similar services, find the way to use them all for appropriate distribution of resources, and design that into your cloud-bound applications.

That is how the cloud will be run in the next few years, and what your organization should have as the goal and the objective for your cloud applications.

That is the open cloud.
Next Steps

There are several links provided throughout this white paper to further provide information on these topics, and literally millions more online. Cloud computing is becoming a big topic, and a core investment destination for organizations and IT departments for the next several years.

We are very early in the game, organizations are mostly starting to investigate, understand, and learn what needs to be done, how, and by when. We have seen budgets for cloud become standard, as opposed to add-on, line items for virtually all IT organizations, and we have seen a lot of “try-and-test” implementations of “private” cloud, virtualized setups, and many other different models of cloud and semi-cloud computing.

We estimate that by 2015 we will begin to see the early adopters deliver open clouds ready to take advantage of the few providers we have now, that by 2020 we will see plenty of providers and a mainstream adoption (more than thirty percent of organizations will have deployed their own open cloud infrastructure) for the model, and that by 2025 it is going to be the reigning model for organizations to implement their applications. Any change of this magnitude requires this slow, methodic change to succeed.

The time to plan and investigate is now. Compare models – either if you have tried them or are testing them now, or if you are looking for a new strategy for cloud computing – and decide for yourself in the next two-to-three years how to adopt and implement cloud for your business. Read further to understand why the current crop of providers is barely scratching the surface when it comes to cloud computing, and make the decision to implement an open cloud model for your organization.

As you grow into a cloud computing architecture you will see how the three issues that most people mention (security, integration, and scalability) are not issues that should concern you – but features you can leverage in that new architecture. Make the investment then to make it your business’ business to use an open cloud, and leverage the benefits for years to come.

You will be glad you did it