Head in the clouds: is the ICT industry fooling itself?

Few ICT innovations have **received as much hype as cloud** – but things are more complicated than you might think. Clouds should be operated, automated and governed to the same high standards as today's mobile-telecoms networks – and there's still a long way to go. It's time to start asking **tough questions about cloud**.

"Who can provide the cloud equivalent of a mobile network? Right now, the answer is nobody"

DOES THE ICT INDUSTRY really understand the cloud? I'm not so sure. Talking to people from every part of the business, you'd almost believe that there aren't any fundamental questions to be answered or significant problems to be fixed. You'd more or less accept that today's most visible cloud players already have the entire market sewn up. And you'd just about be convinced that we're not, in fact, at the very beginning of the cloud age, with all the uncertainties, complications and opportunities that would entail.

Of course, you'd be wrong to take any of those suggestions seriously. But first, here's a bit of history. It's fairly obvious that, cloud age or not, there have always been three pillars of the ICT industry – network, compute and data – and that we can basically explain every past or present industry trend in terms of the convergence of at least two of these pillars. Take the PC or smartphone – that's network meets compute. The network-storage industry comes from mixing data and network. Big data is compute plus data, and so on.

Cloud is the ultimate convergence of these three pillars. It's a complete systems approach to network, compute and data under a single operational, automation and governance domain. For the first time, server, storage and network infrastructure is completely integrated, which means that simply thinking of cloud as a different delivery mechanism for software really understates its true significance.

LITTLE FLUFFY CLOUDS

At least, that's the theory. The reality, however, still falls short of this ideal. For example, look at the first of the three aspects of the single domain I just mentioned and ask whether the cloud is easy to operate. Even the biggest cloud players would probably admit that it isn't.

Automation isn't looking much better. Every mature technology goes through a remarkably homogenous cycle of innovation, standardization and then virtualization. Once that's done, you can start automating things (and start governing that automation). And while cloud has made big strides in a short time when it comes to automation, it's not there yet.

But it's the governance domain that poses the most serious questions. Consider that the whole point of cloud is accessibility – unlike traditional IT and telecoms systems, which can be compared to completely closed boxes with a cable going in one end and out the other, almost anybody can get inside a public cloud system and program

HYASS&HANNIBAL

against it. This makes clouds convenient and easy to use, but it also constitutes their major disadvantage. The classical security model is built on the exact opposite principle, namely strictly limited access, and that's simply not an option anymore.

ENCRYPTION PRESCRIPTION

It's hard to overestimate the scale of this challenge. In fact, the classical security model views a public cloud – with unknown numbers of unknown people running unknown applications with accessed hardware – as the very definition of a compromised system. The cloud requires us to start from the point at which this classical model breaks down, and to assume not only that everything been accessed, but that it's actually been done on purpose.

Finding a new model that guarantees the integrity and confidentiality of data in a system without secrets is an enormous task. There are some potential solutions under development – for example, several companies are working on approaches to data integrity based on keyless signatures and keyless encryption, and some of the most interesting research in this area focuses on homomorphic encryption, or trying to figure out how encrypted information can be accessed without unencrypting it. Get this right, and there's no need for a trust model at all, since there's literally nothing that a user has to trust is being kept secret by their cloud provider.

But if this sounds like a Herculean undertaking, that's because it is. The industry is still a long way from cracking this particular nut, and lack of robust governance and transparency remains the number-one stumbling block to widespread enterprise adoption of the public cloud. It's the principal reason why less than 10 percent of today's enterprise IT spend is directed towards cloud.

So while there's no doubt that the arrival of cloud – as the final convergence of network, compute and data – is a landmark event in the history of the ICT industry, major questions around its operational, automation and particularly its governance domains mean that cloud is far from a done deal. And anybody who says otherwise is, quite frankly, fooling themselves.

MAKING THE GRADE

Is there an answer? Here's my modest proposal – we need the cloud equivalent of a mobile-telecoms network. Today's mobile networks are by far the most global, multi-tenant, scalable, secure infrastructure in the world, to the point where many people are willing to use their smartphones as identification devices, and where we can travel to the majority of points on the Earth's surface and make calls without any problem. Our phones switch between different regulatory jurisdictions and we never notice a thing – and we don't get each other's text messages by mistake, either. The degree of operational, automation and governance capacity that these networks offer is quite astonishing, when you stop and think about it.

This, of course, is the reason why telecoms tools and systems have already been applied to many of today's hyperscale web applications. The cross-platform instant-messaging service WhatsApp, to take just one example, was written using the open-source Erlang language originally developed by the telecoms industry. Why? Simple – telecoms tools and systems help create high-performance, policy-driven, business-critical applications with known economics. Amazon's web services may be designed to be resilient, meaning that they can recover more easily from the failure of any unreliable part, but the telecoms industry learned the lessons about resiliency more than thirty years ago.

> "Cloud requires a total reversal of trust and transparency models, and achieving that from a technical point of view could take the next 100 years"

When you tease apart the concept of telco-grade, that's what you end up with. Most IT systems fall some way short of this – even systems that claim to be mission-critical – and there's not a CIO in the world who wouldn't want systems that work in the same way that today's mobile networks do.

LOOK AND LEARN

So look at mobile networks and learn – because that's exactly what the cloud should be. A really good policy-based, governance-focused, highly secure platform-as-a-service that runs on anything can just be rolled out. Fundamental object storage systems that are aware of the countries in which they are located, that automatically adjust to different legal and compliance requirements, and that don't let you break the law by mistake – those are rollouts. Systems that stay resistant even when insiders try to access confidential data – a definite rollout too.

None of these things exist yet, but this is where the industry should be aiming. I'll say it once more – we need a cloud equivalent to a mobile network. And considering the size of the market at stake, whoever gets it right first will be very glad they did.

CUTTING DOWN AMAZON

If we accept this view of what the cloud should be, we also undercut the argument that Amazon, Google and Microsoft have already got the entire cloud market in the bag. Because for all their resources and visibility, none of these companies can realistically claim that their cloud offerings are anywhere close to meeting the standards set by a proper telco-grade cloud. Of course, their ambitions might well lie elsewhere, and they may see sufficient growth potential in addressing the small and medium-sized enterprise market. But that's a very small part of a much bigger opportunity.

There are two areas in particular that today's cloud players have yet to address in any consistent way. The first is clouds for mission-critical infrastructure – defined as infrastructure that if it fails, so does a company's core business. The second is clouds that drive top-line revenue, often for companies that are in regulated environments, such as banks or utilities. Nobody is building clouds for these opportunities, and the only way that's going to change is if somebody can offer a cloud system that works like a mobile network.

HEAD IN THE CLOUDS

That's what's needed. It should be clear by now that we're still at the very earliest stages of the cloud age, and any suggestion that everything is already settled couldn't be further from the truth. In particular, some of the industry discussions about which players will own the market border on the fatalistic. I think there's also a definite tendency to overplay what's been achieved so far while understating the very real issues that still remain to be answered. For one thing, we're talking about a total reversal of trust and transparency models, and achieving that from a technical point of view could take the next 30, 50 or even 100 years – hopefully less, of course. And in the end, it comes down to one question – who can provide the cloud equivalent of a mobile network? Right now, the answer is nobody. ●

ABOUT THE AUTHOR

JASON HOFFMAN is Head of Product Line Cloud Software at Ericsson, where he is responsible for the global design, implementation and rollout of the company's cloud offerings. He is the co-founder and former CTO of cloud solution provider Joyent. Hoffman has a BS and MS in Chemistry & Biochemistry from the University of California, Los Angeles, and completed a PhD in Molecular Pathology at The Burnham Institute and the University of California, San Diego School of Medicine, all in the US.

284 24-0029 | Uen