SWCP Portal
April 2013

Let's look at clouds from both sides now

The Forecast Calls for Clouds

The Internet is full of buzzwords, ubiqitous terms that seem to promise everything but mean nothing. One of the more recent and baffling of these is **cloud computing**. It has been sprinkled in articles and conversations everywhere over the last year or so. But seeking the actual meaning can leave one feeling, well, a bit nebulous.

The easiest definition is that cloud computing is just a way of talking about **applications that run over the Internet** or the Net iself. That's not very helpful for those folks who still think the Internet has something to do with tubes. So this article will define cloud computing, talk about its advantages, potentials, and risks, how you're using it right now and why you will rely on it much more in the future.

"Out there" versus "in here"

The big difference between cloud and traditional computing is that the former relies on the resources and power of the Internet as opposed to that of a single isolated device.

The simplest way to understand the real though subtle distinctions between this new approach and the way it has always been done is to compare products that do much the same thing: say, Google Maps and a mapping program. Both can find locations for nearly anything anywhere but one program lives somewhere "out there" on the Net and the other resides entirely within your laptop.

Note the resulting differences:

- Google Maps can be accessed from any device anywhere: PC, laptop, smartphone, or tablet. The mapping program is likely to be used on just one computer.
- Online access means that Google Maps can work with other apps on your smartphone, such as a GPS tracker to provide you with up-to-the-minute location data.
- The downside is that the "anywhere at any time" convenience of Google Maps is absolutely limited by Internet access and availability. If your journey takes you outside of communication range, you could find yourself, like early explorers , somewhere in the white space right off the edge of the known world. With a map program, you're not lost as long as you've still got power.

- Google Maps are likely to be updated more often, and have new features added without you even noticing. Your mapping utility likely has to get its updates at intervals and you may have to reinstall it. But as Apple found out when they introduced their iCloud mapping app, a faulty Net application can generate a whole lot of unhappiness on the fly very quickly.
- Google Maps are free to use, but you likely had to fork out real cash for the map program. But this means you own the data on your computer. Nobody can snoop on where you're going. Yet if you're using Google Maps, the company can do whatever it feels like with your location data. The government might want to track you secretly for some reason. Or Google could sell it straight to advertisers, for instance, allowing them to bombard you with pitches all along the way to your destination. Whether that would be a major annoyance or a helpful feature depends on how useful you find it.
- As a public provider, Google Maps can be censored. There are certain areas that governments or other entities don't want us to be too curious about which Google Maps kindly blurs. There's somewhat less chance this would happen with a private, commercial product.
- Being online, Google Maps are constantly vulnerable to hackers, power interruptions, bad programming, and even bureaucratic foul-ups. It could be taken offline just like Microsoft's worldwide cloud was in February when a company-wide security certificate expired. A commercially-produced mapping program should be far less subject to such bugs by the time you get it. But, of course, it's only as reliable as your own computer is.

Continued on back

Continued from front

How it works

From this, it's clear that the cloud concept, like the Internet itself, offers users a great number of helpful advantages, as well as some pretty serious risks. For software developers, or service providers such as SWCP, the challenge is how to utilize the tremendous potential of the cloud as much as possible while diminishing those dangers for users.

Cloud computing is made possible by **virtualization**. The basic functioning of the Internet remains unchanged. It's still a client computer (yours) connecting with a server that supplies data or gets it from other servers. Virtualization allows a single server to act like a bunch of different servers, allowing the creation of huge **webfarms** on the one hand, or, on the other, allowing a large array of servers to pretend they are but one enormous platform.

Grid computing builds on this by co-ordinating masses of servers to act in concert as a virtual **supercomputer**. It's how Google can find millions of references to a few obscure words among acres of computers in just a few milliseconds. Accessing the grid through the cloud sounds strange, but it enables home users to tap into computing power far beyond any they could ever hope to own.

Clouds enable new service categories beyond searches. If it can be delivered over the Net, cloud computing can provide it, and likely for less expense and trouble. Many kinds of software services and even infrastructure can be supplied by distant clouds over highspeed connections.

Possibly the fastest growing cloud services are online data storage and back-ups. Southwest Cyberport's own back-up service, ***SWCP BUS***, is based in the cloud. Our Web-based **email readers** like Roundcube also reside there.

It's not just us and Google, either: nowadays, the bigger the online player is, the more dependent they are on their clouds. But some have been more successful than others. Like Google, Amazon has done quite well and continues to invest heavily, as does Facebook. Microsoft has had a few glitches, but Apple seems to have had the worst luck so far. The **iCloud** is at least their fourth attempt at cloud-building, and one still fraught with serious problems.

Dark clouds

Clouds can be public, readily accessible by anyone, or private, protected behind firewalls and other precautions. As with anything important on the Internet, **security** is the key issue, especially for the latter type. This depends largely on identity authentication and verification, which gets back into password usage and all that.

With the cloud, privacy and security become even more important than ever. As ever more of our lives are accessible online, they become more vulnerable. But it's the power and risks inherent in virtualization that are the most dangerous. Keeping all that data separate and private is a big challenge, especially with this new and still largely untested technology. For instance, a cloud server company in New York was lately found to be accidentally leaking data between accounts, some from former customers, and there's probably much more of that to come.

More severe hazards come from **collateral hacking**. While old-time criminal crackers may look for any way in to steal financial information, the new breed of cyberspy seeks other data as well. Google's Gmail system, for instance, was penetrated last year by Chinese looking not only for political dissenters but proprietary American technical data also. As the potential for **cyberwar** grows, chances of being caught in the digital crossfire grows as well.

One of the most significant issues surrounding the cloud is who actually **owns the data** there. Many people balk at giving their precious information – whether it be plans for a new missile, family photos, or a music collection lovingly gathered over a lifetime – into the hands of a third party, and for good reason. According to some terms of service, notably Google's, once you upload your information, you don't own it anymore. Not only could the service be hacked or go down, or the government decide to check on what everybody's holding, but if the company decided to resell that information, there's no way to prevent them.

Cloud computing is here to stay, giving users vastly more data and power than they get out of their little boxes otherwise. Relying on programs online permits Google to offer its new **Chromebook** laptop far cheaper than any comparable model. The cloud also offers big savings to developers and information managers, too, but the price is that data security becomes crucial. Cloud providers must furnish robust defenses with flexible responses to problems and have firm policies of data management in place.

Southwest Cyberport recognizes these imperatives. Access to SWCP BUS behind our firewall, for example, is password-based like most private cloud services. But it also supports encryption, and the information is stored redundantly in two separate data centers. And users own their data. After all, we don't want the cloud to rain on anybody's parade.

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**