Clients:

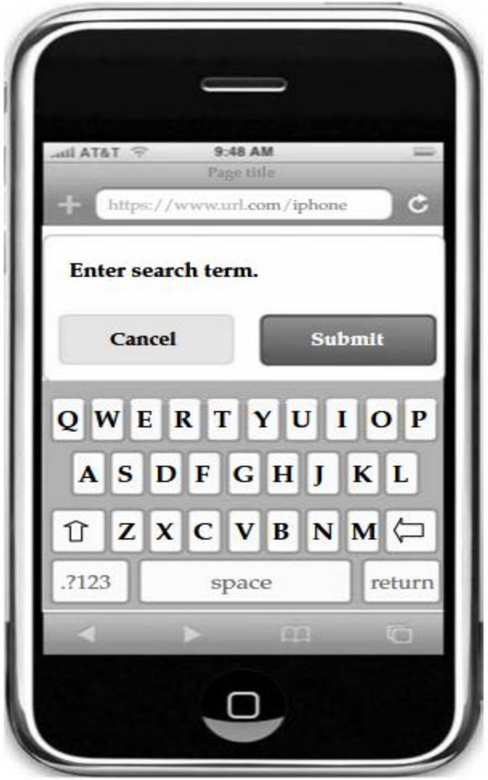
- The clients on your end users’ desks are how you will interact with the cloud.
- There are different types of clients that can link to the cloud, and each one offers a different way for you to interact with your data and applications.
- Depending on your organization and its needs, you may find yourself using any combination of these devices.
- How you interact with your data based on these clients will be a combination of factors what your needs are and the benefits and limitations of these client types.

Mobile :

- Mobile clients run the gamut from laptops to PDAs and smartphones, like an **iPhone or BlackBerry.**
- You’re not likely to utilize a particularly robust application on a **PDA or smartphone, but laptop** users can connect to the cloud and access applications just as if they were sitting at their desk.
- Mobile clients, of course, have security and speed concerns. Because the clients will be connecting to the cloud from various locations that may not have an optimized connection, as in a hotel, you can’t expect the speed that a desk-bound client will achieve.

Cloud Computing Technology

- All applications need speedy connections, and mobile users probably aren’t inputting gigabytes worth of data into a database.
- You can create your own applications in the cloud, they can be crafted with a mobile client in mind.
- While a mobile user won’t put tons of information into a database, an application can still be developed to let them access it.
- Security is a major concern, but it’s a two-sided issue. On the one hand, it’s easier to lose or misplace a laptop, and whatever information is on it could be compromised.
- On the other hand, if data is maintained on the cloud and the user only has select files on his or her laptop, if the laptop were to be stolen, only a minimal set of data would be compromised.



Enter search term.

Thin:

- Thin client computers that have **no hard drives, no DVD-ROM drives, and simply display what's on the server.**

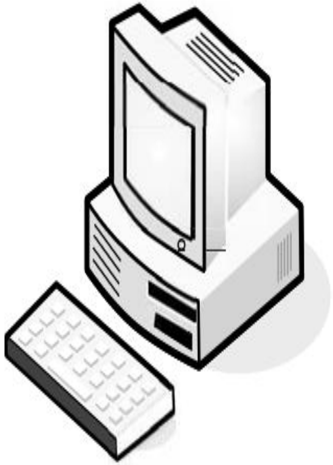
- Thins may have a role in your organization, but likely only if you have an in-house cloud. Of course, it depends on what applications and services you're accessing on the cloud.

- If a client only needs to access cloud-based services or is accessing a Virtualized server, then thin clients are a great option. They're less expensive than thick clients, are much less expensive to maintain, and use less energy.

- There's also a high level of security, because no data is stored on the thin client. All the data resides in your data centre or on the cloud, so the risk of a physical breach is small.

Thick:

- Thick clients are the clients you already use and are likely to use to connect to applications in the cloud.
- You likely already have applications installed on your end users' machines.
- While you can offload some of your applications to the cloud, chances are there are still going to be some mission-critical applications that simply need to stay in-house.
- These machines can certainly still connect to a virtualized server, and if you don't want to spend any more money for clients, just use the machines that you already have.
- Thick clients are good choices if users need to maintain files on their own machines or run programs that don't exist on the cloud.



Thick:

- Security-wise, thick clients are more vulnerable to attack than thins. Since data is stored on the machine's hard drive, if the machine is stolen then the data could be compromised.

- There's also an issue of reliability. If a thin client fails, all it takes is for another thin to get plugged in and the user's work environment is right there.

- If a thick client fails, whatever data is stored on the machine, including the operating system and all the configuration settings, is lost and a new computer will have to be configured for the user.

Security

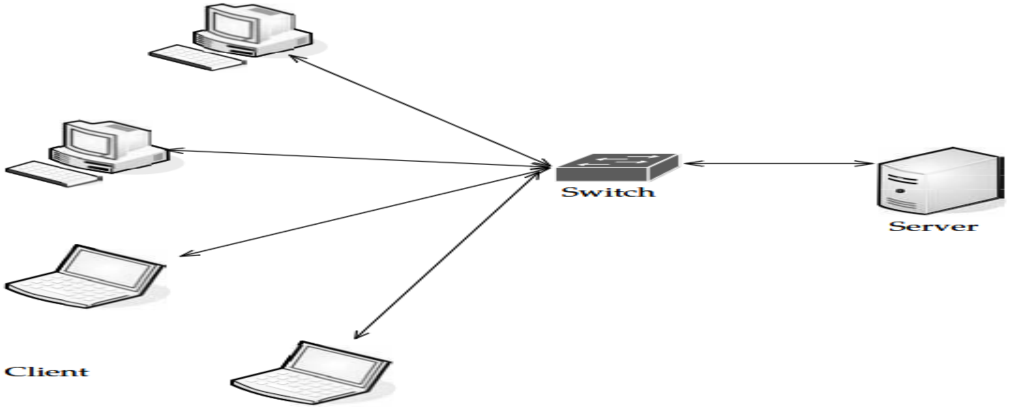
- Security is the number one issue when it comes to cloud computing, and that only makes sense.
- Third party stores your data, you don't know what's going on with it. It's easy to worry about the security risks of a cloud solution, but let's not overlook the inherent security benefits, as well.

Data Leakage:

- The biggest benefit is the centralization of data. Organizations have an issue with asset protection, in no small part because of data being stored in numerous places, like laptops and the desktop.

- Thick clients are apt to download files and maintain them on the hard drive, and there are plenty of laptops out there with non encrypted files.

- Thin clients creates a better chance for centralized data storage. There’s less chance for data leakage.



Data store on local server with clients that store data has more opportunity for data leakage than clients that maintain no permanent storage.

Cloud Computing Technology

Offloading Work :

- Another security benefit isn’t so much a technology, but the fact that you don’t have to do it yourself. It’s up to the cloud provider to provide adequate security.
- The fact of the matter is that your cloud provider might offer more security features than you had before. Many clients are paying allows cloud providers to have beefier security.
- Simply because of the economy of scale involved. That is, there are many paying clients so the provider is able to do more, because there is more money in the pot. additionally, it’s to the provider’s benefit to offer more, because they want to get a good reputation.

Logging

- Logging is also improved. It’s something that, in-house, usually gets the short end of the stick. But in the virtualized world of cloud computing, providers can add as much memory as they need to extend logging.

Cloud Computing Technology

Forensics

- If there is a breach, the cloud provider can respond to the incident with less downtime than if you had to investigate the breach locally. It is easy to build a forensic server online, and it costs almost nothing until it comes into use.

- If there is a problem, the virtual machine can be cloned for easy offline analysis. Further, many companies don’t have a dedicated in-house incident response team.

- If there is a problem, IT staff have to quickly figure out their new job of taking the server down, quickly investigating, and getting it back online for minimal production downtime.

Development

- Even more good news is that security vendors aren’t in the dark about this whole cloud thing. They are actively developing products that can apply to virtual machines and the cloud.

- Security vendors also have a unique opportunity in the cloud. Since it’s new ground, there are new opportunities for the vendors who are open-minded enough to imagine them.

Auditing

- As an IT professional, you already know the headache of securing your own local network. But when you send your data to the cloud, a whole new set of issues arise. This is largely because your data is being stored on someone else’s equipment.

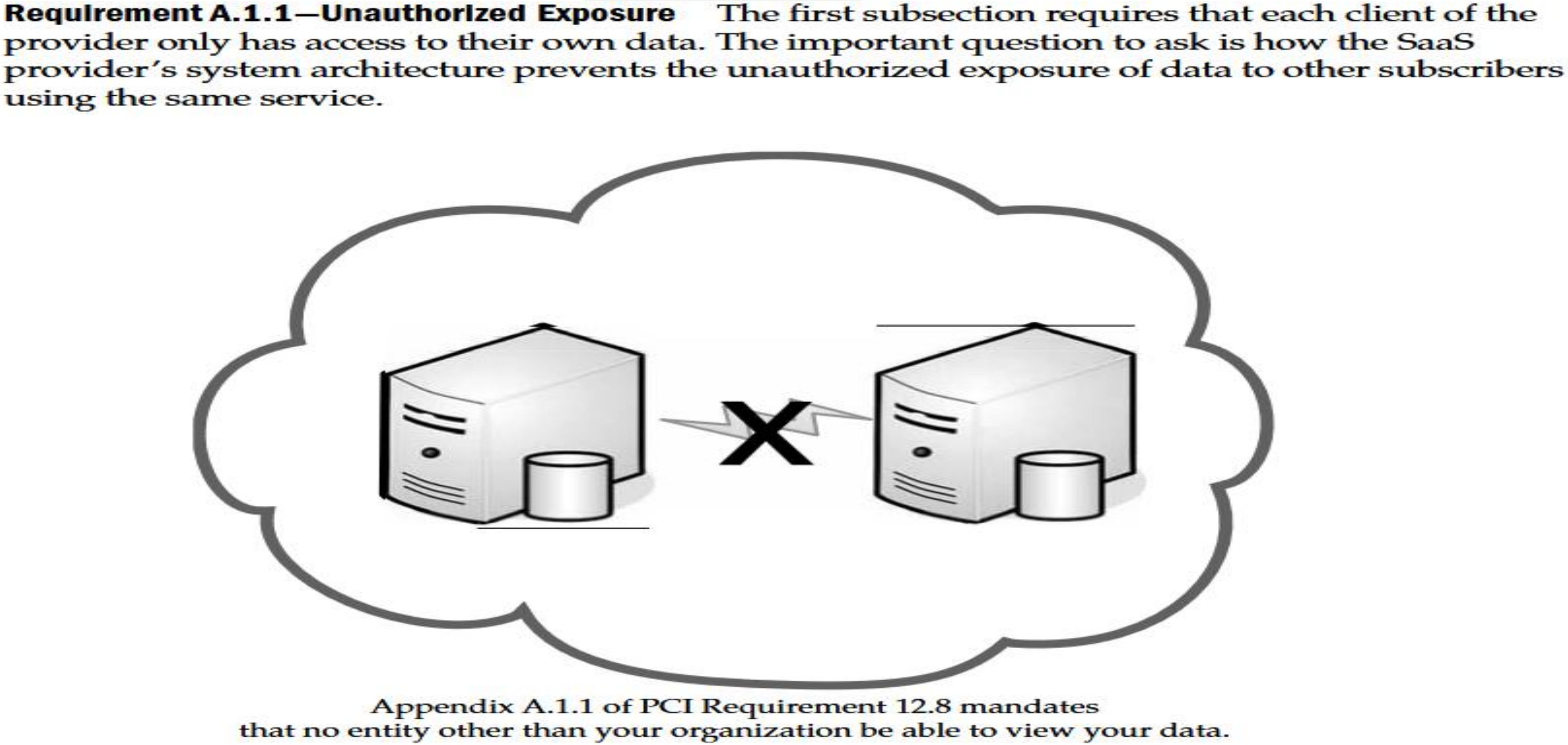
Compliance

- The same security issues that your organization deals with are the sorts of issues that SaaS providers face—securing the network, hardware issues, applications, and data.

- But compliance adds another level of headache. Regulations like Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), and HIPAA, and industry standards like the Payment Card Industry Data Security Standard (PCI DSS) make things particularly challenging.

Prior to SaaS, compliance could be managed by a few tasks:

- Identify users and access privileges
- Identify sensitive data
- Identify where it's located
- Identify how it is encrypted
- Document this for auditors and regulators
- SaaS makes these steps even more complicated. If you store compliance-sensitive data with an SaaS provider, it is difficult to know where the data is being stored.
- It could be on the provider's equipment, or it could even be on the equipment of one of the provider's partners.



Requirement A.1.1—Unauthorized Exposure The first subsection requires that each client of the provider only has access to their own data. The important question to ask is how the SaaS provider's system architecture prevents the unauthorized exposure of data to other subscribers using the same service.

Appendix A.1.1 of PCI Requirement 12.8 mandates
that no entity other than your organization be able to view your data.

Web Application Breaches

- Service providers use so many web connections, they should be asked about the security of their web applications.

- This should include whether they follow Open Web Application Security Project (OWASP) guidelines for secure application development.

- This is similar to Requirement 6.5 of PCI, which requires compliance with OWASP coding procedures.

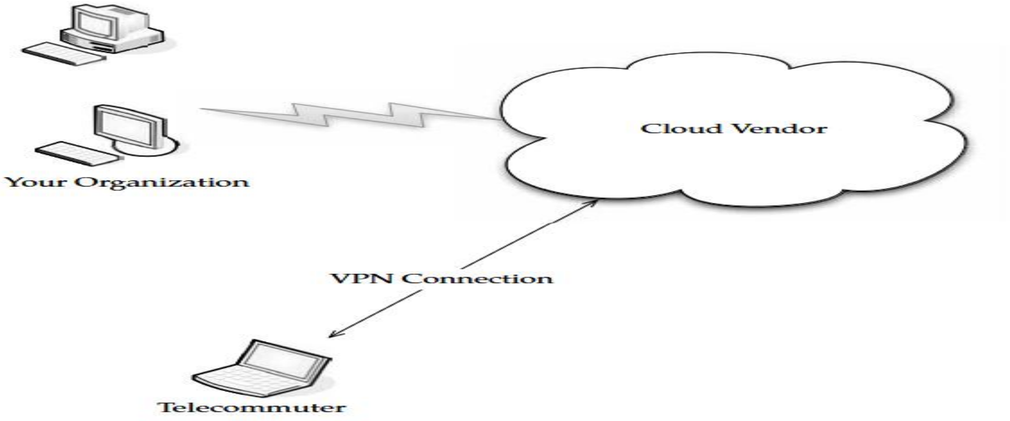
- When dealing with a provider, you should seek out those who are able (willing) to talk about how they handle breaches among their staff as well as where data is stored.

- Given the wide range of server deployment, your data could be sitting on a server in Brazil, Germany, or Thailand.

VPNs

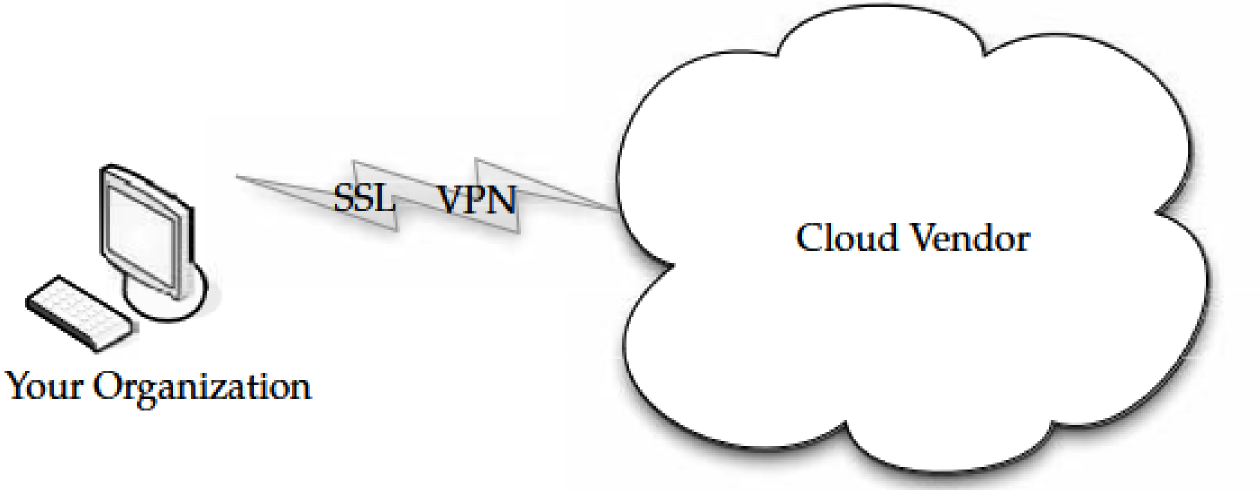
- With applications being moved to the cloud, it makes it possible for each and every worker to be a telecommuter. Thus, the organization doesn’t have to lease as much space, pay as much for utilities, and those stupid holiday parties can be eliminated.

- Your organization might not lend itself to telecommuting simply by the work you do, or maybe you like those holiday parties and warm bodies in chairs. But the more applications get offloaded to the cloud, the fewer things you have to worry about in-house.



Cloud Computing Technology

- There is certainly more to your datacenter than web applications. You have file storage, email, productivity applications, and anything else that doesn't lend itself to being web-based.
- But in any event, whether your employees access the cloud across the public Internet or from your office, you need a secure remote access solution, like an SSL VP.
- **What SSL Is An SSL VPN (Secure Sockets Layer virtual private network)** is a VPN that can be used with a standard web browser.
- As compared to the traditional IPsec (Internet Protocol Security) VPN, an SSL VPN does not require you to install specialized client software on end users' computers.
- SSL is a protocol for managing the security of message transmission on the Internet. SSL is included as part of popular web browsers and most web server products. It employs a public and private key encryption system from RSA.



SSL VPNs use an established protocol to connect to the cloud securely.

Cloud Computing Technology

- An SSL VPN cloud computing connection between your data center and the cloud provider secures your data without a lot of the Public Key Infrastructure (PKI) overhead that comes from an IPsec-based VPN solution.

- Most SSL VPN gateways provide an on-demand client, so there's very little management overhead on the client side and it's easy for the end user to use.

- Better Security Practices An SSL VPN also makes sure that end users are compliant with your organization's security policies through the use of endpoint security.

Those measures include

- Requiring antivirus software to be running
- Verifying that OS patches have been installed
- Checking to see if malware or bots are running
- The SSL VPN is a great security solution because it secures access to your applications in a simple, inexpensive, and efficient way.
- If you were so inclined, you can offer your employees more chance to telecommute.