Engineering for a Trustworthy Cloud

Jim Miller
Microsoft Corporation

A Bit of History: 1960 - 2010

1960 — Multics: The Information Utility

"…computing may someday be organized as a public utility just as the telephone system... The computer utility could become the basis of a new and important industry."
– John McCarthy, 1961

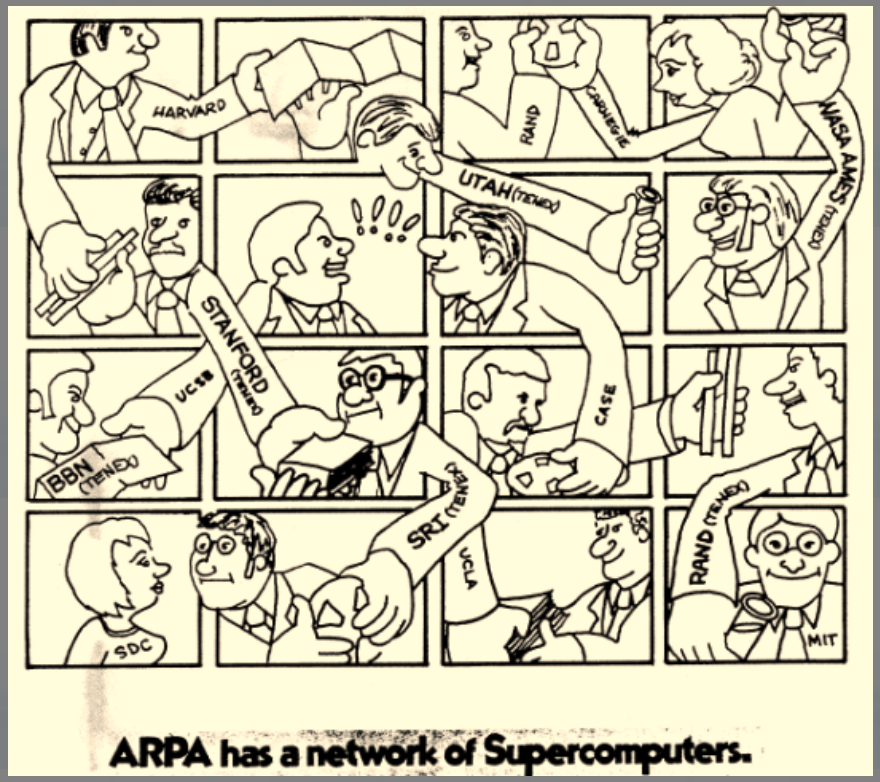
"…a large computer utility … must run continuously and reliably 7 days a week, 24 hours a day in a way similar to telephone or power systems, and must be capable of meeting wide service demands."
– Corbató and Vyssotsky, 1965

Multics as a "Computer Utility"

- …Continuous operation analogous to … electric power and telephone
- …Capacity to allow growth … without either system or user reorganization
- … File system so reliable that users trust their only copy of programs and data to be stored in it
- Sufficient control of access to allow selective sharing of information

(from Corbató, Saltzer, and Clingen)

1970 — ARPANet: Digital Communication Utility



"If such a network … could be brought into operation, we would have at least four large computers, perhaps six or eight small computers, and a great assortment of disc files and magnetic tape units–not to mention the remote consoles and teletype stations–all churn ing away" – J.C.R. Licklider, 1963

"Email was not invented in 1972; It was 1971" – Ray Tomlinson

- ARPANet, 1969: Reliability
- TCP, 1974: End-to-End guarantees
- InterNet, 1977: Decentralized control

1980 — Personal Computers: Private Computing Utility

"The Alto ... [executes] about1.5 μs/instruction … [this] computational overkill … will allow us to concentrate on the capabilities of the system rather than on optimizing its performance." – Butler Lampson, 1972

On 12 August 1981, the first IBM PC went on sale.

The first Macintosh was introduced on January 24, 1984; it was the first commercially successful personal computer to feature a mouse and a graphical user interface rather than a command-line interface

1990 — WWW: The Data Utility

- provide a … [way to get] information stored at a remote system
- provide a … [way to] exchange [data]
- provide some method of reading at least text (if not graphics)
- provide … [a] collection of documents … [with] much existing data.
- provide a … search option [as well as] navigation by [links]
- allow … collections of documents to be linked to … other collections
- interface to proprietary systems

– Tim Berners-Lee and Robert Cailliau, 1990

2000 — Web 2.0: The Social Utility

"[Facebook is] a directory that is reinforcing a physical community. What exists on the site is a mirror image of what exists in real life." – Mark Zukerberg, 2004

- Facebook had over 500,000,000 active users as of 2010, who used over 700,000,000,000 minutes per month on the site
- Hotmail had over 360,000,000 active email users as of May 2010
- Gmail had over 176,000,000 active email users as of December 2009

Introducing (?):
The Cloud:

It's 2010: What's The Cloud?

- It's just Multics
  - With a lot more CPUs
- Connected to a high bandwidth network
  - But you may not have high bandwidth
  - And no one has increased the speed of light ☹
- And you are using a personal computer
  - Even if you think it's a cell phone
- And it has over 4,000,000,000 users

What's Changed Since Multics?

- More than 50% of the 1st and 2nd world population has access to *fixed broadband* networking (OECD)
  - Even more have access to a home computer
  - Even more businesses have broadband
  - *Mobile* broadband lags, but is growing rapidly with special importance in rural areas and 3rd world countries
- Each home computer is more than 1000 times as powerful as the shared Multics system
- About 28,000,000,000 web pages were on-line in August, 2010
- **We really do have an Information Utility**
  - On a scale not imagined in 1960
  - On an international scale not imagined in 1990

We Asked For It …

- Now that we have what we asked for, is it what we want?
- One key question remaining is *trust*
  - Is it reliable?
  - Is my information secure and under my control?
  - Is data about me private?
- Another is *access*
  - Are we creating a new cultural divide?
  - Over time will the divide grow?
  - This is a great question, but another talk ☺

Trust …
and The Cloud

Trust Questions

- Do you trust the water in your hotel room to be safe to drink?
- Do you trust your car to stop when you press the brake pedal?
- Do you trust the bridge to hold your car while you drive across it?
- Do you trust the dam to protect your house?
- Do you trust your bank to hold your money?
- Now ask yourself “why”?

Official Microsoft Position

Trustworthy Computing

"The continually evolving computing landscape has two primary macro-level developments: more people and businesses rely on computing every day, and the threats that can undermine trust in computing are increasingly sophisticated and malicious." – Microsoft Trustworthy Computing home page

The Pillars of Trustworthy Computing

- Security
- Privacy
- Reliability
- Business Practices

Four Pillars

- Security
  - Users must *authenticate* themselves; access is provided based on an *authorization* policy
  - Access, especially "administrative access," is logged and audited
  - Systems are developed and deployed using transparent mechanisms
  - SD^3: Secure by design, secure by deployment, secure by default
- Privacy
  - Policies are clearly stated, enforced, and audited
  - Policies comply with both legal requirements and user expectations
  - Data expires in a timely manner, and can be removed when necessary
- Reliability
  - It Just Works
    - And when it doesn't, it's for short periods of time with appropriate remediation and reimbursement
- Business Practices
  - Integrity and honesty
  - Self-critical, questioning, and committed to excellence
  - Personal responsibility and accountability

Jim Miller's Additions

- Security
- Privacy
- Reliability
- Business Practices
- Simplicity
- Education
- International Legal Framework

Three Additions

- Simplicity
  - If people don't understand the system
    - it can't be secure
    - they won't be able to manage their privacy
    - it won't appear reliable
- Education
  - The creator of the system is responsible for educating the public about the technology, it's limitations, and possible failings
- International Legal Framework
  - Jurisdiction over data
  - Jurisdiction over service offering
  - Legal recourse for consumers and companies
  - Law enforcement and security forces

A Cloud Scenario

Swiss Lecturer

Rich Client Software

Visiting China

Using a US-based Server

Caching data in Japan

- Whose law applies where?
- What's encrypted, and when?
- Who retains what information, and for how long?

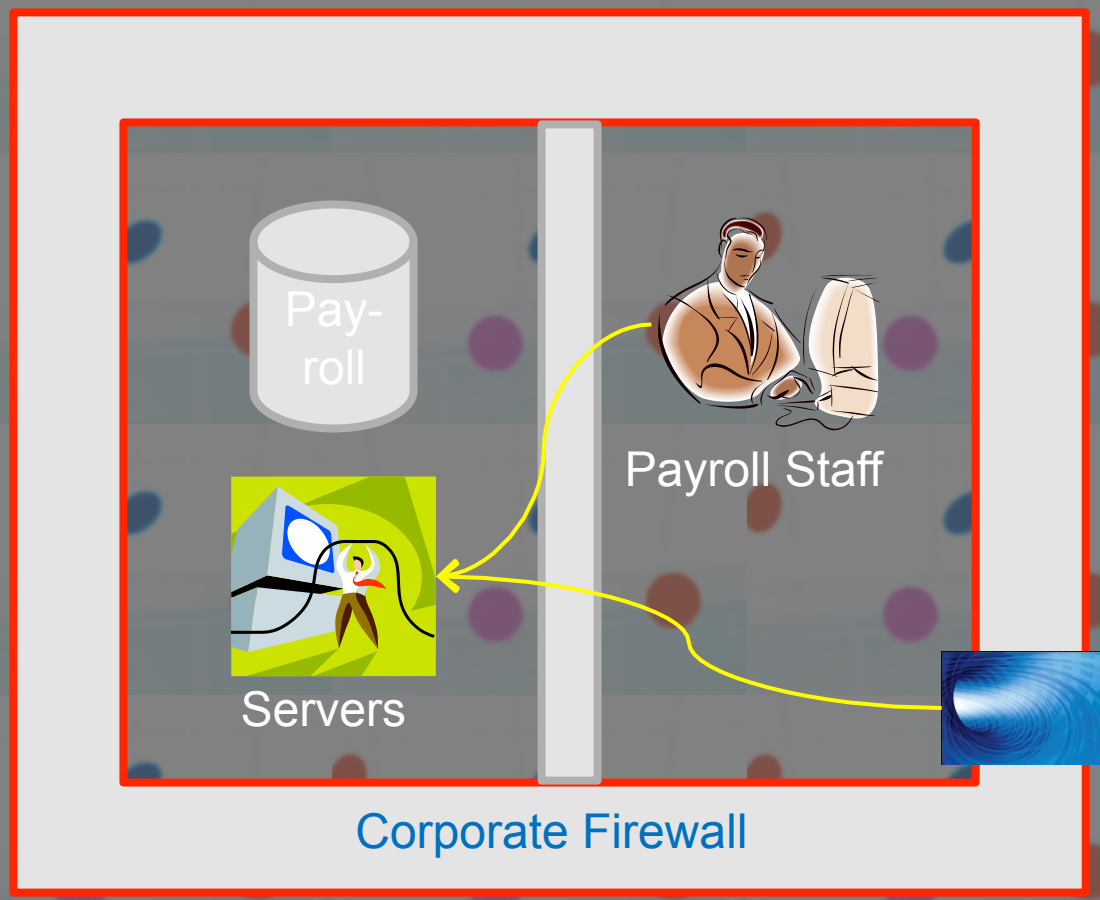
Where Do I Put the Data?

- Technology answer
  - Near the customers
  - Near power and telecommunications hubs
  - Use content distribution networks (CDNs) and caching to optimize delay / bandwidth / cost equation
- Legal issues
  - US law requires repatriation of data
  - US law prohibits foreign wire taps in US
  - Some countries tax all corporate income if any service facilities are in-country
  - Pass-through of auditing, measurement, and regulatory requirements
- Net result
  - It costs a *lot* of money to decide whether to operate a data center in a location
  - It costs a *lot more* money to decide how data (especially PII) must be located
  - It costs a *lot of on-going money* to handle compliance issues (over and above "normal" operating costs)

Engineering The Cloud: One Technical Challenge

Securing Data

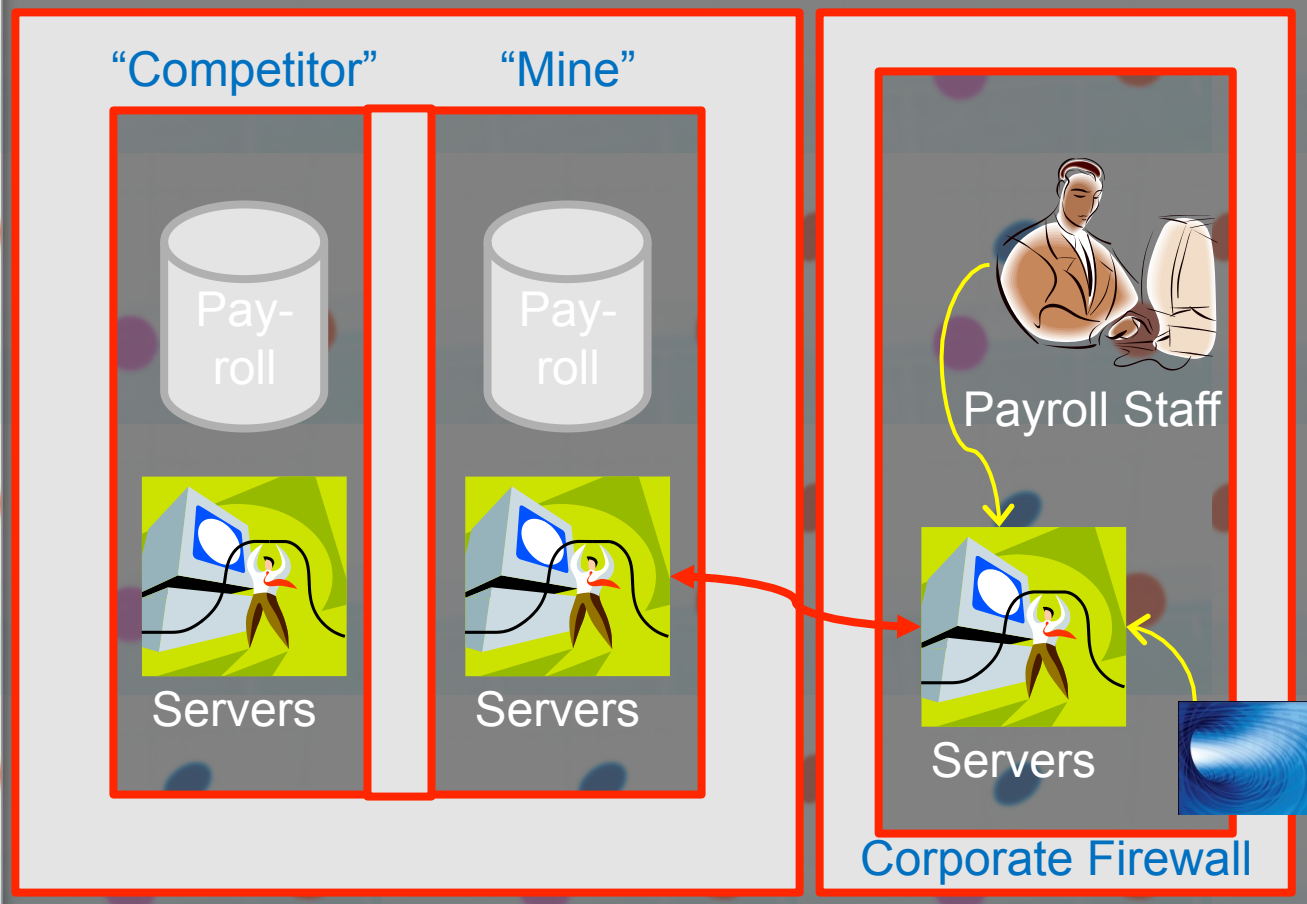
The Way It ~~Is~~ Was: On-Premise Computing



I'm Not Worried because

- It's on my premises
- The server staff
  - are chosen by me
  - are scheduled by me
  - are subject to audit by me
- Payroll and normal staff access is controlled and audited

The Way It ~~Is~~ Was: Out-Sourced Computing



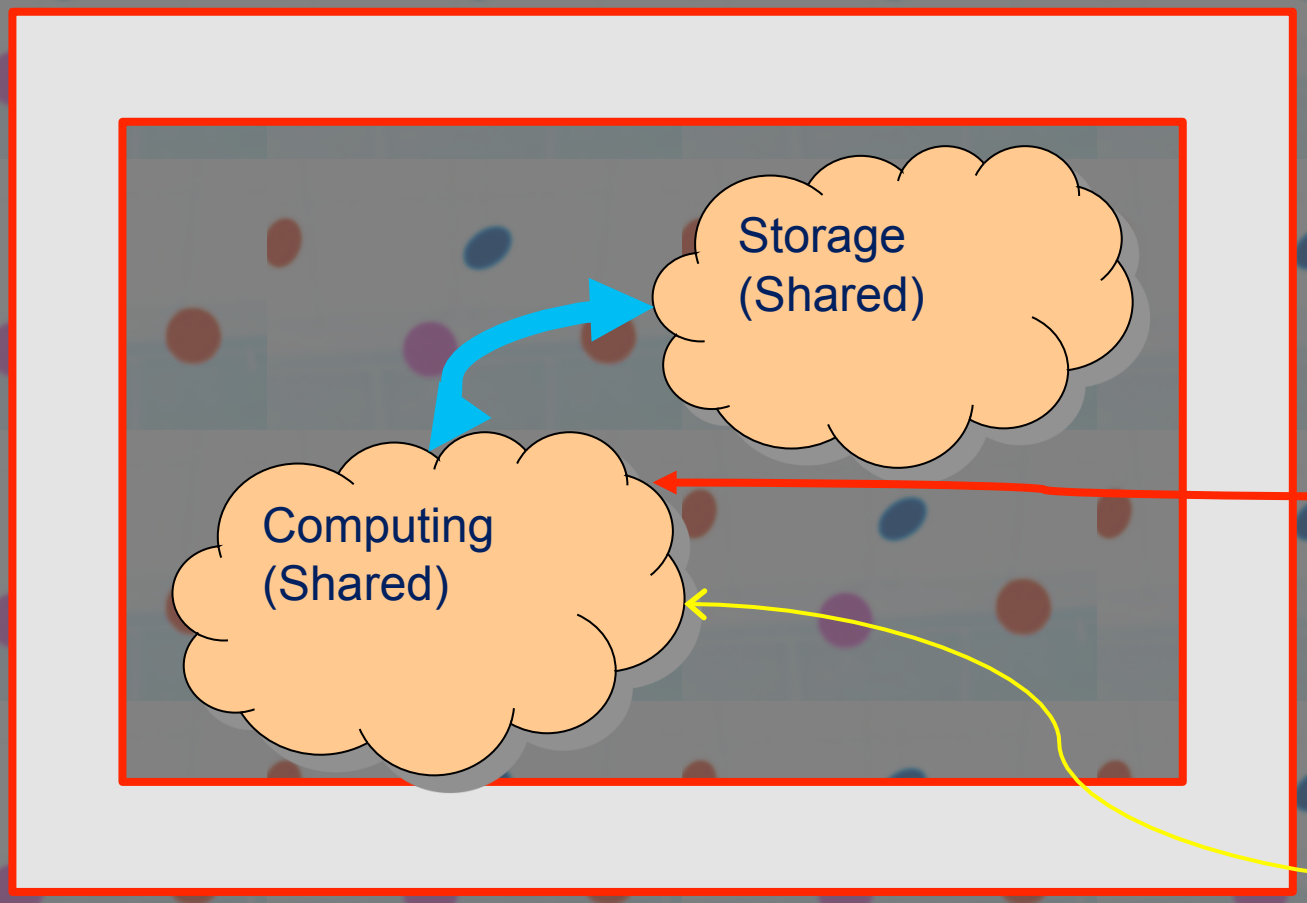
I'm Not Worried because

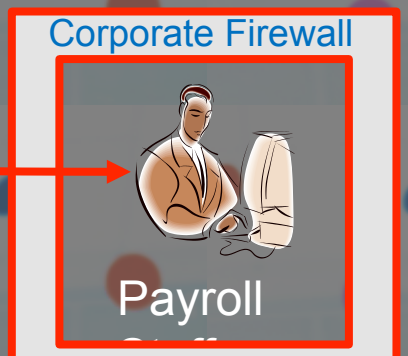
- I have a contract with the hoster
- I can audit the hardware and software
- Only my servers can access the hoster's computers from outside
- I still audit payroll and user access

The Way Of The Cloud (?)

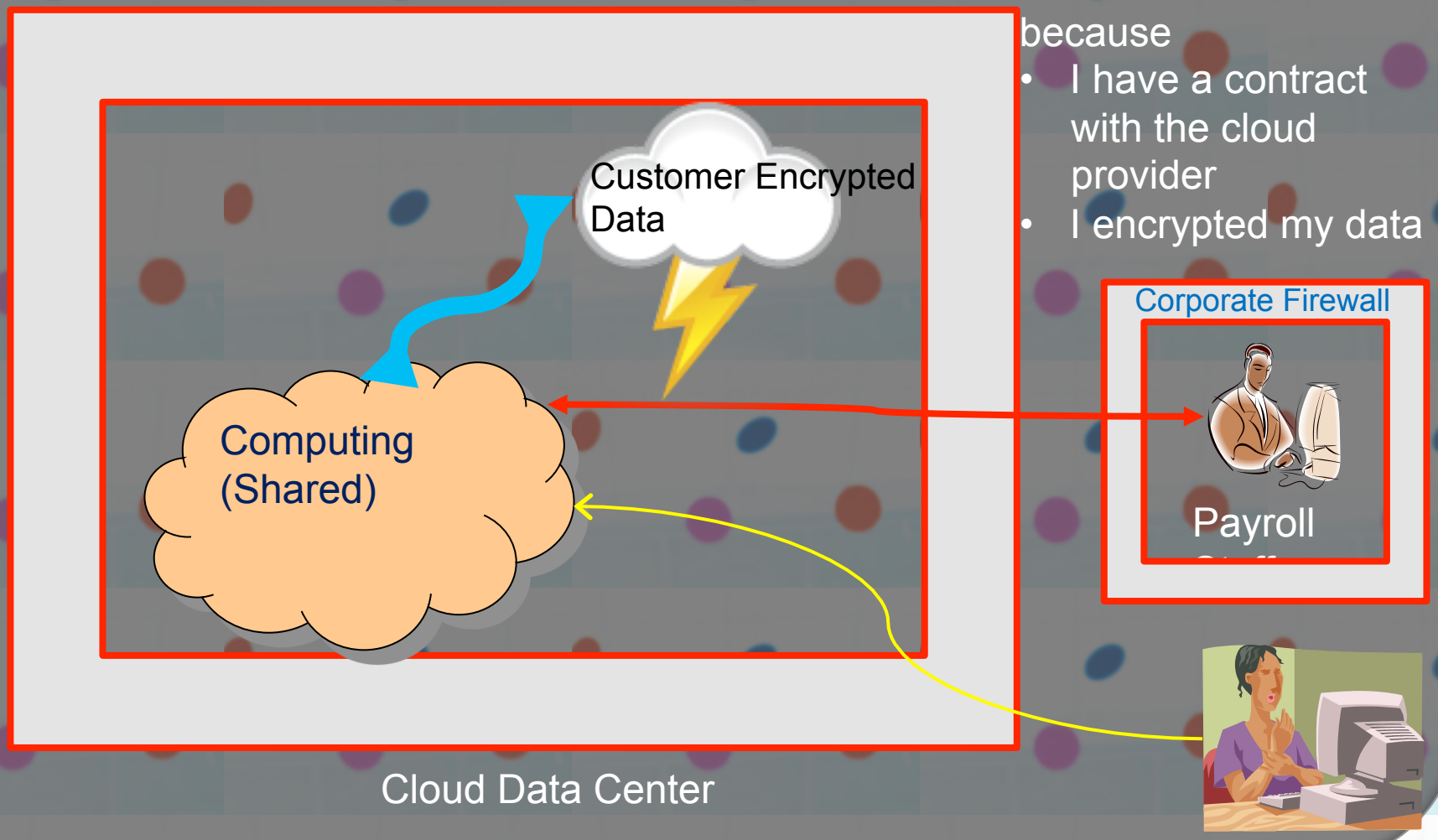
I'm Not Worried because

- I have a contract with the cloud provider





The Way Of The Cloud (?)



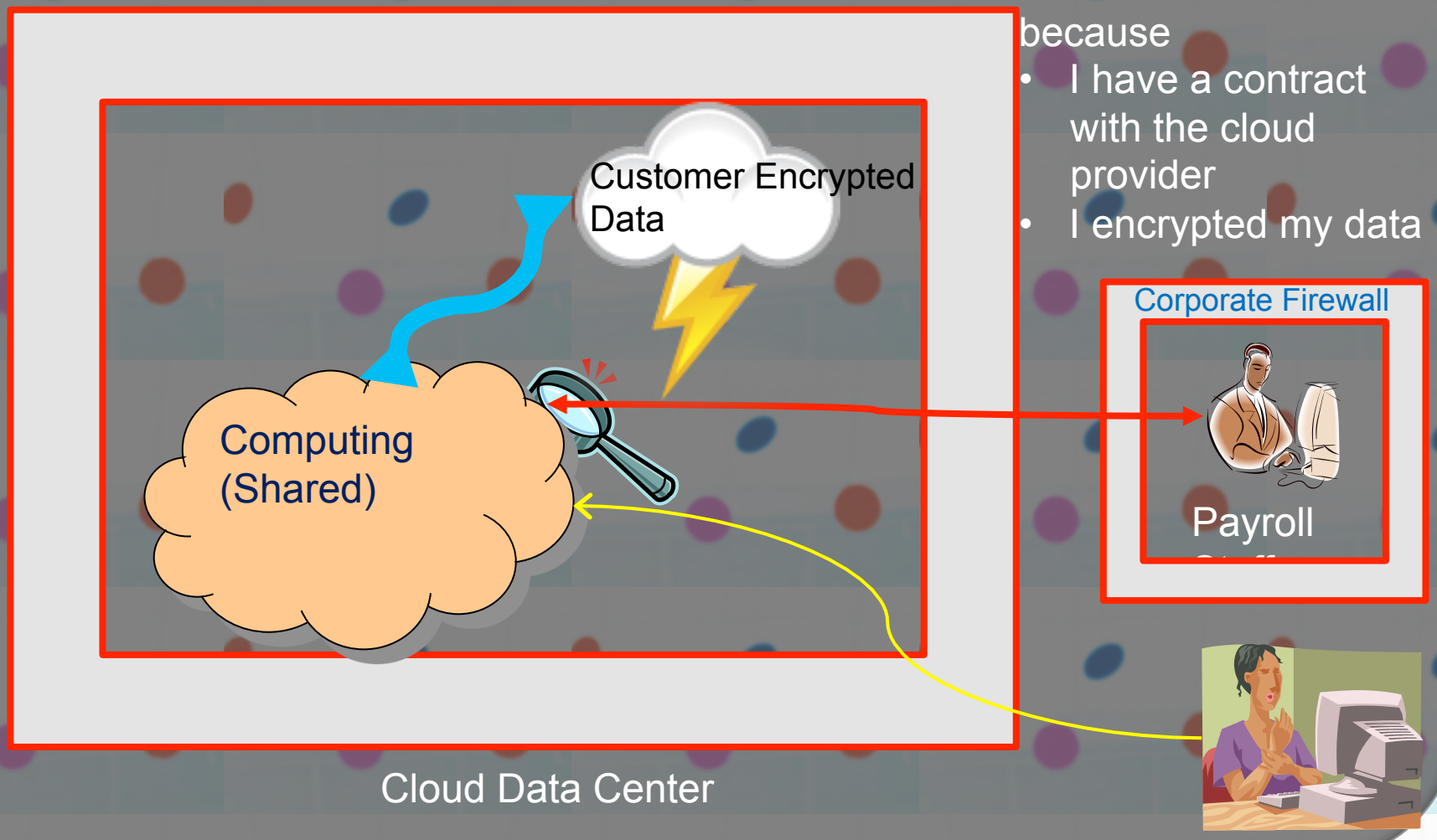
I'm Not Worried because

- I have a contract with the cloud provider
- I encrypted my data

The Way Of The Cloud (?)

I'm Not Worried because

- I have a contract with the cloud provider
- I encrypted my data



Who Decrypts Your Data?

- The cloud provider?
  - I'm worried, again
- My application?
  - How do I know it's my application?
  - Oh, the cloud provider promised me it is
  - I'm worried, again

Who Decrypts Your Data?

- The cloud provider?
  - I'm worried, again
- My application?
  - How do I know it's my application?
  - It needs a little secret ….

Keeping An Application's Secret

1. Give the secret to the cloud provider to hold and trust it to hand it only to your application
2. Embed it in the application, protected by obfuscation, and change the secret and the obfsucation frequently
3. Use a secure hardware measurement device to check the application at boot time
4. **All of these are adequate, none are good**
   - **And that's my technical challenge to you**

It's 2010:
Shape The Cloud You Want

Make it trustworthy

- Secure
- Private
- Reliable
- Business Practices
- Simple
- Education
- Legal structure

Let it grow

- Decentralized
- Federated
- Innovative

Thank you!

And Happy Birthday!

С днем рождения

Joyeux Anniversaire

Alles Gute zum Geburtstag

Ne gelukkege verjoardach

Ick gratuleer di scheun

Buon Compleanno

Gratulerer med dagen

Ois guade winsch i dia zum Gbuadsdog

bil hoozhoo bi'dizhchi-neeji' 'aneilkaah

Vsechno nejlepsi k Tvym narozeninam