

Can a Mobile Cloud Be More Trustworthy than a Traditional Cloud?

Mufajjul Ali

Orange Lab UK

Building 10, Chiswick Park,

Chiswick, London, W4 5SX

Mufajjul.ali@orange-ftgroup.com

Abstract. Cloud computing is deemed to be the next big trend nebulous. Various sectors have expressed interest in its adoption, including banking, the government, education, manufacturing and telecommunication. With the promise of cost saving and flexibility also comes the greater challenge of security in-particularly "trust". One of the common questions asked by many users is "Can the cloud be trusted?" Telecommunication service providers have been trusted for many years, and have been adopted by millions of users world wide. With the emerging vision of new mobile cloud providers, the ultimate question lies in asking, can a mobile cloud provider be a more trustworthy provider than the traditional ones?

Keywords: Cloud computing, Trust, Security, Telco.

1 Introduction

Cloud computing (CC) is built on many existing tools and technologies reducing the cost of service delivery whilst increasing the speed and agility of service deployment [1]. The core technology behind cloud computing is virtualization; it empowers the whole cloud computing paradigm. The virtualization technology allows the separation of physical hardware and the operating system by creating an abstract layer between both. This allows a greater degree of flexibility by being able to share the same physical resources virtually by more than one OS.

1.1 Cloud Service Models

Cloud computing has various service models to cater for the need of different market segments. Infrastructure as a Service (IaaS) is designed to meet the requirement for businesses that need their infrastructure to be hosted remotely. There are several benefits to this approach; upgrade, management and security of physical resources are provided by the host. The infrastructure can scale at will, and does not require any in-house experts. The down side of this approach is that the logical and physical security is outside the businesses' physical boundaries [2]. Sensitive and private data being hosted remotely raises security concerns and requires trust of the provider.

Platform as a Service (PaaS) on the other hand is designed for companies who require a development environment for developing application/services and hosting facilities remotely. It is especially designed to take away the complexity of setting-up the environment, maintaining and managing software updates.

A relatively new service model proposed by Ali. M [3] is Network as a Service (NaaS). The concept is based on allowing application(s) to dynamically fluctuate the required bandwidth at close to real-time. This greatly improves the performance of bandwidth hungry applications. The customer is charged based on their bandwidth usage, rather than a fixed monthly term.

And finally Software as a Service (SaaS) model is where application(s) and services are hosted by a service provider or a vendor. These application/services are typically accessed remotely via the Internet using a Web browser. From an end user's prospective, this is a fairly attractive model, since installation, upgrade and patches are not required to be managed by the user. User's can be assured that they are using the latest version of an application and are only paying for the actual usage of the service [6].

1.2 Cloud Computing Deployment Models

More recently, there have been four different deployment models defined by the cloud community: private cloud, public cloud, community cloud and hybrid cloud.

Private clouds require the complete cloud infrastructure to be hosted locally with the company's local network. No external network traffic has access to this cloud. There are several benefits to this approach: first, to maximize and optimize in-house resources [7, 8]. Second, the organization has full control of the resources, and finally it is fully secure and operations within the private cloud can be fully trusted.

Public clouds on the other hand are the opposite of private clouds. The complete infrastructure is hosted by a 3rd party provider remotely. The cloud provider has full ownership of the cloud; it may have its own pricing, security and other policies. A public cloud consumer must have significant trust in the provider, since all the data resides under their control.

The community cloud enables several organizations to share the same resources, infrastructure and policies. This collaboration allows them to be more cost effective with better management of available resources.

And finally, a hybrid cloud can be a mixture of different clouds, typically private and public clouds combined together. An organization may use their private cloud for developing in-house service, then migrate to a public cloud for their end users.

2 Background

Over the last 30 years there has been a great advancement in mobile telecommunication networks. The first generation of network, also known as 1G was released in 1980's. It was primarily designed for human to human communication (voice). The advancement from circuit-switch to packet switch network arrived in early 90's. The 2G (GSM) network was designed for machine to human communication (SMS), packet data was added later via the GPRS protocol.

The 3G network, which is hybrid between packet switch and circuit switch, was designed in mind for machine to machine communication. Apart from voice and SMS, it provides various value added services, such as networking games, web browser, etc.

The all IP vision of the 4G network has set the trend for Telcos broadening their horizon in embarking into the service market; this has lead to the optimism of becoming the mobile cloud provider.

2.1 Mobile Cloud Computing (MCC)

Telco operator Orange has been actively involved in defining their concept of mobile cloud computing. Their provisional definition is as follows:

"Mobile cloud computing is a device-centric cloud that aids the creation, composition and provision of mobile cloud services"

There are two aspects to this definition, firstly the device-centric cloud, which is designed to handle the physical infrastructure requirements. This provides the backbone required for creating innovative services that may not be possible with current deployment models.

Secondly, mobile cloud services are empowered by platforms that provide the necessary building components for the creation, composition and provisioning of mobile cloud services.

The key characteristics of mobile cloud computing is as follows:

State Preservation – capabilities are available for preserving the state and data of an application that can be restored at any point in time (t_0 , $t-1$, $t-n$) on different devices.

Resource Fragmentation – Intelligent resource scheduling (off-loading/on device execution) and optimized algorithms are used to minimize the impact on the device's battery life, RAM, CPU and storage (data sync)

Network Optimization – Edge locality for optimal communication (physical distance) between the device and the service (s) (hosted on the cloud).

Data Sync Management – Near real-time sync of data amongst shared devices for both on line and partially off-line connectivity; this includes appropriate locking and data collision/corruption avoidance management.

Provenance Aware – Advance trust management based on Provenance for each and every operation which are recorded and analyzed to ensure that the operation(s) are legitimate, data confidentiality/integrity is maintained, and accountability/liability is satisfied.

Access Mobility – Device is agnostic to static physical location for access; services can be provisioned and accessed seamlessly.

The characteristics of mobile cloud computing are catered towards meeting device constraints needs (such as increasing processing and memory capability, and device environment portability).

The two service models provided by MCC are PaaS and SaaS (see table 1), which is the same as cloud computing at conceptual level. However, IaaS is not supported by mobile cloud computing - mainly due to security reasons. It however, provides a new service model, known as Network as a Service (NaaS) which was briefly discussed earlier.

Table 1. Comparison of Service models

| Type | NaaS | IaaS | PaaS | SaaS |
|------|------|------|------|------|
| CC | - | X | X | X |
| MCC | X | - | X | X |

The NaaS allows services to be optimized according to the level of bandwidth requirement, which ultimately minimizes network lag and improves the user experience.

Unlike the traditional cloud computing where the client is device agnostic and virtualization mainly powers the server end. With MCC there is also device virtualization; amongst other benefits, this provides smart phone capabilities on featured phones.

The deployment models for MCC is restricted to public and private cloud (see table 2 below)

Table 2. Comparison of deployment model

| Type | Public Cloud | Private Cloud | Hybrid Cloud | Community Cloud |
|------|--------------|---------------|--------------|-----------------|
| CC | - | X | X | X |
| MCC | X | X | - | - |

Many of the core assets of Telco provider Orange (location, presence and others) have been opened up from the core network, and are accessible using restricted API's provided via the MCC.

3 Trust

Trust is a term used in many disciplines such as sociology, psychology, computing and so on. The official Oxford dictionary definition of the term "trust" is as follows: *"Firm belief in the reliability, truth, or ability of someone or something"*

In the notion of computing, trust is orthogonal to security; trusted components/entities are required to build a secure system. In the context of the cloud, three areas concerning trust are (see fig 1 below): Security, Availability and Performance.

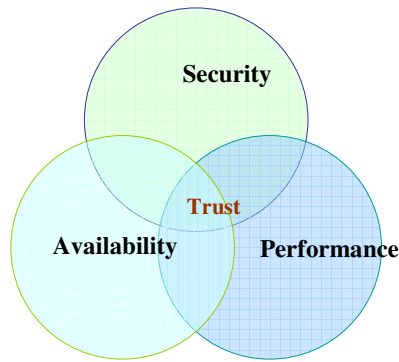


Fig. 1. Notion of trust

These areas are of most concern when it comes to trusting cloud providers and the services they provide. In a recent poll carried out by an IDC enterprise panel [5], 87.5% of voters voted security as their main concern, followed by availability at 83.3%, and performance at 82.9%.

MCC characteristics are *inherently* leverages on the existing trust of Telco network, and it is focused on providing the much needed building blocks that can enhance the customer's service trust.

The characteristics defined in section 2.11 can be complimentary to the "Trust" factor shown above.

The first characteristic ("State Preservation") can improve the usability of services by being able to restore/resume state of the service(s) from any device that are considered to be trusted by the IAM (Identity and management system) mechanism. This is particularly useful in cases where the battery life of the device is at minimal and there is an explicit need for switching of devices; which can greatly improve the performance factor of the service.

Characteristic two ("Resource Fragmentation") on the other hand is an important feature of the MCC. The sole purpose of this is to alleviate the performance and computational issues faced by many devices by extending its capability to almost limitless. The customer would greatly benefit from the enhanced performance of their services. One point to note is that this feature is service specific; the performance factor is heavily dependent on how the service is fragmented and algorithms have been implemented.

Characteristic three ("Network Optimization") can greatly enhance the performance of the service access, by ensuring that the optimal distance of the physical locality of data/service is selected. This would greatly benefit users who are constantly on move, possibly from one country to another or moving between cities. However, this is assuming that latency is constant amongst the nodes, and same level of bandwidth between user's device and nodes.

Characteristic four ("Device Sync Management") is more specific to the device content. It provides the facilities for structured data to be synced between the device and the cloud. The benefits are that a user can trust their data will remain safe even if the device is lost or stolen or, can access his/her data from different devices.

Characteristic five ("Provenance Aware") is probably the most important feature related to trust in MCC. The main purpose of this feature is providing the end user with greater transparency by providing provenance data for each individual application. The provenance data has many usages. Firstly, it can be used for determining the liability and accountability in case any faults occur in the cloud. Secondly, it can be used to detect anomalies, and can also be used for better policy control.

Characteristic six ("Access Mobility") is designed for continuous service access. If a device is on Wifi, and the signal is getting weaker due to mobility, the device would automatically switch to the stronger 3G network, and vice versa. This ensures that minimal disruption is caused to the network access. The advantage of this approach is that it does not explicitly require user's interaction.

3.1 Security

Security is one of the key factors of trust. Many cloud providers are unlikely to guarantee the security of data [10], hence breaching the DPA 1998 [11]. There is an explicit need for security of the data as it faces the potential threats from forth-coming cloud malware. Cloud malware is likely to be a new breed of innovative and sophisticated techniques being developed and used to compromise the cloud.

3.2 Platform

Malicious threats such as viruses, worms and trojans [17] are also major security concerns for companies and organizations. Statistics shows that the Windows platform is most susceptible to malware (see table 3 below). Linux and Mac platforms on the other hand are less prone to the attack; this is may be due having a more robust OS core, or due to occupying a smaller market share compared to Windows.

Table 3. Platform threats

| OS | Viruses | Worm | Trojan |
|---------|------------|---------|---------|
| Windows | 60000+[18] | 1000+ | 1000+ |
| Linux | 40+ | Limited | Limited |
| Mac OS | 5+ | Limited | Limited |
| Symbian | 10+ [21] | - | 52 |
| Android | 1[15] | - | 1[16] |
| Iphone | 1 [12] | 1 [13] | 1 [14] |

Mobile OSes however are still relatively safe for terminal operations for MCC, despite new potential malware threats. The current wave of threats on Android and Linux only affect devices that have been hacked ('jail-broken').

3.3 Network/Infrastructure

Traditionally, an IP Telecoms network (3G) is considered to be more secure than the standard Ethernet network (Internet) (see table 4 below comparing a specific Telco Operator's network with the Ethernet network).

Table 4. Network Security

| OS | 3G Network | Ethernet Network |
|-------------------------|---------------------------------|---|
| Authentication | Sim-based | None/application specific |
| Network access | Secure, Authentication required | Non-secure, ISP specific authentication |
| Data | Ciphered | Plain/application specific |
| Network standardization | 3GPP standardized | IETF |
| Network implementation | Operator specific | Shared |

There are several reasons for greater Telco security. Firstly, a Telco's core network is standardized by 3GPP. Each of the components is well defined and huge amounts are invested each year on maintenance and upgrades. This is to ensure that there are no defects and the highest level of quality of service is achieved.

Secondly, the physical core network is generally closed from outside; only the operator has access to many of its sensitive assets, such as the HLR. However, with the vision of providing APIs for third-parties to create innovative services, it is slowly becoming more and more open.

Thirdly and most importantly, access to the network requires secure authentication, this is not the case in an IP network. Each device is authorized by using a non-temperable SIM. And most significantly, all communication is carried out under a secure communication channel. The actual transmissions of data are ciphered for additional security [20]. This is contrary to the Internet where prior authentication is not required, as long as there is an ISP providing the Internet connection. A secure IP communication channel is optional (SSL/VPN) and it is based on specific application/service needs.

3.4 Availability

Availability is a key measurement of Quality of Service (QoS). It is defined by the equation below (See figure 1), which calculates the uptime of a service during its life span.

$$A = \frac{E[\text{Uptime}]}{E[\text{Uptime}] + E[\text{Downtime}]}$$

Fig. 2. Availability Equation

Google have recently been sued for inappropriate security on its Cloud services [9] and a recent problem with their mail system caused dismay amongst many businesses and consumers, who were denied service for several hours. This further highlights the potential danger of fully trusting cloud service providers.

Table 5. Network Availability

| Feature | Availability |
|---------|--------------|
| CC | 99.5 [4] |
| MCC | 99.9999 |

Telcos however are not known for unexpected denial of critical services. They have very high threshold values for availability (see table 5 above) for their PSTN service. Given the fact that operator such as Orange owns their own broadband network. It should be possible to offer very high availability for end-to-end services. The high availability offered by Amazon is server end only. The true end-to-end availability would be dependent on the ISP providing the connection, which may significantly affect the overall availability threshold. The superior end-to-end availability promise of MCC would be the preferred choice of being highly trusted by critical sectors such as Banking, Medical and the Government.

3.5 Performance

Performance is determined by systems or applications performing to levels either defined by a contractual obligation or industry-recognized acceptable levels. It is directly related to the second factor 'availability' where the higher availability is likely to be paralleled by high performance levels.

There are various matrices can be used to determine the performance level. MCC, and CC both rely on physical networks to deliver services to the customers; which makes network delivery capability a good matrix to measure trust in performance.

Table 6. Comparison of deployment model

| Type | 3G | 4G | WiMax | Broadband |
|----------|---------------------------------|-----------------------|--------------------------------------|-------------------------|
| Speed | 3.6-7.2Mb/s | >100 Mb/s [19] | 108 Mb/s | 50 Mb/s |
| Coverage | 93% UK | Yet to be released | 50km (fixed), 5-15 km (mobile) | Physical connection |
| Latency | Increases in built up areas, | Not yet known | Increases with distance | Application specific |
| Speed | 3.6-7.2Mb/s | >100 Mb/s [19] | 108 Mb/s | 50 Mb/s |

The speeds defined in Table 6 above are theoretically achievable speeds in UK; the actual speeds may be slightly lower due to overall network overhead and latency.

The speed of a 3G network is fairly modest; it is likely to perform reasonably well with applications and services that require low bandwidth, but may not be optimized for bandwidth-hungry applications. However, with the proposal of 4G this obstacle can be minimized. The speed of broadband is a highly attractive proposition for performance for CC, but would not have the benefit of "anywhere anytime" capability of MCC and does not have the support of NaaS model.

3.6 Other Trust Factors

Reputation - With any cloud computing service, it's important that the provider have a trusted relationship with those people using the service based on reputation"[23] also highlights a significant point that could sway the trust factor in favour of MCC.

Large Telco providers have been serving customers for several decades, and within this period, they have served and built a trusted relationship with millions of their customers. As general consensus suggests, that based on reputation, customers are more likely to trust their personal data with a Telco provider than traditional cloud providers such as Google.

It is not common for Telcos to loose their customers' data, although recently a Telco provider had their repetition slightly dented by loss of their customers' personal data on their 'Sidekick' devices [22]. The device stored its data in the cloud (provided by Microsoft) with the mishap affecting thousands of its customers.

Community/Experts - It is commonly accepted that the opinions of experts are trusted over those of lay-persons. In this regards, Telcos follow the principle of standardization followed by implementation and MCC is no stranger to this approach. CC on the other hand follows the 'implementation that may lead to standardization' approach. This may carry a greater risk of mistrust as unproven services may be provided to customers, possibly containing unknown defects.

4 Conclusion

Three areas of concerns have been highlighted in this paper; Security, Availability and Performance, which mainly contribute to level of trust by service providers. Mobile cloud models seem to provide more robust security mechanisms than traditional cloud computing models at the infrastructure level. However MCC is lagging behind when it comes to delivery of service to the client. The expected arrival of 4G networks could be the holy-grail for realizing MCC's service performance potential and making the NaaS a reality.

Cloud computing is certainly a more mature technology than Mobile cloud computing, and in the short term customers may be more willing to trust it. However, given the nature of malware threats that exist on CC, MCC would be a better alternative.

Reputation is also an important indicator for trusting a provider. Telco's reliable service history will have a positive affect on gaining trust in MCC solutions, but this reputation itself may not be enough for customers to fully trust in MCC to give up control of their sensitive and person data. Alongside reputation, transparency will also

be paramount. The customer should be able to access the full history of every action, transaction, operation occurred on their data, on request. At present, this is not guaranteed; however, with the emergence of provenance technology, it might be sooner rather than later to become a reality.

References

- [1] Voas, J., et al.: Cloud computing: New wine or just a new bottle? vol. 11(2), pp. 15–17. IEEE Computer Society (March/April 2009)
- [2] John, W., et al.: Cloud computing: Implementation, management and security, pp. 153–180. CRC Press (2010)
- [3] Ali, M.: Green Cloud on the Horizon. In: Jaatun, M.G., Zhao, G., Rong, C. (eds.) CloudCom 2009. LNCS, vol. 5931, pp. 451–459. Springer, Heidelberg (2009)
- [4] Amazon (2010), <http://aws.amazon.com/ec2/>
- [5] http://blogs.idc.com/ie/wp-content/uploads/2009/12/idc_cloud_challenges_2009.jpg
- [6] Khalid, A.: Cloud computing: Applying Issues in Small. In: 2010 International Conference on Signal Acquisition and Processing. IEEE (2010)
- [7] Dillon, T., et al.: Cloud computing: Issues and Challenges. In: 24th International Conference on Advanced Information Networking and Applications. IEEE (2010)
- [8] Jesen, M., et al.: On Technical Security Issues in Cloud Computing. In: IEEE International Conference on Cloud Computing (2009)
- [9] Marshall, R.: Google explains Gmail troubles (February 2009), <http://www.vnunet.com/vnunet/news/2237201/google-gmail-troubles-explained>
- [10] Mari, A.: Cloud computing could bring security threats (February 2009), <http://www.vnunet.com/computing/news/2237013/cloud-computing-bring-security>
- [11] Data Protection Act (1998), http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1,1998
- [12] Claire, B.: First malicious virus hit iPhone...but only on mobiles cracked by users (November 2009), <http://www.dailymail.co.uk/sciencetech/article-1230223/First-malicious-virus-hits-iPhone-mobiles-cracked-users.html>
- [13] BBC news, Worm attack bites at Apple iPhone, <http://news.bbc.co.uk/2/hi/technology/8349905.stm>
- [14] Dinah, G.: Trojan targets iPhone users (August 2010), <http://www.talktalk.co.uk/technology/news/articles/trojan-targets-iphone-users.html>
- [15] Mills, E.: First SMS sending Android Trojan reported (August 2010), http://news.cnet.com/8301-27080_3-20013222-245.html
- [16] Beavis, G.: Expensive virus hit Android Users, fake application sucks mega-bucks from your phone (August 2010), <http://www.techradar.com/news/phone-and-communications/mobile-phones/expensive-virus-hits-android-users-709260>
- [17] Ali, M., et al.: A Review of Security Threats on Smart Phones. In: ICGeS (February 2005), Conference Paper (April 2005)

- [18] The register, Linux vs windows viruses (October 2003),
[http://www.theregister.co.uk/2003/10/06/
linux_vs_windows_viruses/](http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses/)
- [19] Santhi, K.R., et al.: Goals of True Broad band's Wireless Next Wave (4G-5G). In: 2003 IEEE 58th Vehicular Technology Conference, VTC 2003-Fall, vol. 4, pp. 2317–2321 (May 2004)
- [20] Smith, C., et al.: 3G Wireless Networks. McGraw-Hill Telecom professional (2002)
- [21] Top 10 Most Dangerous Viruses on Symbian based Cell phones (April 2010),
[http://www.worldinterestingfacts.com/lifestyle/
top-10-most-dangerous-cell-phone-viruses-on-symbian-based-
cell-phone.html](http://www.worldinterestingfacts.com/lifestyle/top-10-most-dangerous-cell-phone-viruses-on-symbian-based-cell-phone.html)
- [22] Malik, When the Cloud Fails: T-Mobile, Microsoft Lose Sidekick Customer Data (October 2009), [http://gigaom.com/2009/10/10/when-cloud-fails-t-
mobile-microsoft-lose-sidekick-customer-data/](http://gigaom.com/2009/10/10/when-cloud-fails-t-mobile-microsoft-lose-sidekick-customer-data/)
- [23] BBC (April 2010), [http://news.bbc.co.uk/1/hi/programmes/click_
online/8625625.stm](http://news.bbc.co.uk/1/hi/programmes/click_online/8625625.stm)