

# Cloud Computing and Security in the Future

Nigel McKelvey, \*Kevin Curran, Benny Gordon, Edward Devlin, Kenneth Johnston

School of Computing, Letterkenny Institute of Technology,  
Letterkenny, Co. Donegal, Ireland  
Email: nigel.mckelvey@lyit.ie

\*School of Computing and Intelligent Systems, Faculty of Computing and Engineering  
University of Ulster, Londonderry, Northern Ireland, BT48 7JL  
Email: kj.curran@ulster.ac.uk

## Abstract

*We are starting to depend more and more on 'Cloud' technology; in business and in our own personal lives. With so much personal data being stored in our personal clouds questions are being asked about where the responsibility lies for the protection of data. For instance is it with the consumer or with the provider. People have a right to know where their files are being stored and what is protecting them. The same goes for the consumer. They are obligated to ensure that their passwords are of a good strength and that they are safe while browsing the web, especially on public networks. The personal cloud industry is on the rise and if the experts are correct in their predictions, the business world will be a better place for it. Better in terms of portability and flexibility. The power to set your office up wherever you happen to be sitting, anywhere in the world, will be what personal cloud providers are offering. This is the future for cloud computing. Security and privacy are now more relevant than ever. This chapter examines the issues around cloud data protection and security and also investigates if the current data protection act defines sufficient guidelines for data controllers on how they should collect and store user information in relation to thin based clients using online or cloud based service; or if a lack of clarity in the data protection act could cause these services to misuse the user's data.*

## 1. Introduction

Since the inception of the internet in the early 1990's the variety and volume of services on offer has increased exponentially. In recent times a new computing paradigm has emerged to further expand the on-line universe: Cloud computing. Despite what may largely appear to be a general zeitgeist of mass approval and an unstoppable drift towards universal implementation, the adoption rate among many business sectors has been slower than expected. The generally offered justification for this caution is perceived to be an underlying fear that the technology does not offer the same level of security that can be achieved by the traditional, on-site, model of computing. Big business especially seems hesitant to embrace the model. Cloud computing is now an almost ubiquitous concept in modern information technology. First conceived in the early 1960's by John McCarthy, a researcher at MIT, who suggested that one day computing service provision would essentially become a utility; delivered and metered much like the telephone or electricity services. Today cloud

computing, in its various forms, is the dominant force in the IT industry, with market research giant Gartner suggesting that cloud computing based activities will form the bulk of I.T. spending by 2016 (Shetty, 2013).

“Security concerns the confidentiality, availability and integrity of data or information. Security may also include authentication and non-repudiation.” (Robinson, 2011). With the vast majority of people now using multiple devices during their daily lives personal cloud computing has become a major factor in storing our data from multiple devices to the same location. With so many devices which are connected to the internet it is more important than ever to be able to access your files from every one of those devices; from your phone to your laptop, your iPad to your smart TV. An easily accessible, user friendly personal cloud storage system that does not compromise on security is what many users are looking for (Tomonari & Yukio, 2010). Clients using either personal or public cloud services may suffer anxiety due to a lack of control over such things as availability, portability, isolation, integrity, transparency and the confidentiality of their data (Rai & Sharma, 2013).

Privacy is a major concern when referring to the cloud. Every cloud service provider must adhere to the law. This law is dependent on where the service provider is located. In Europe the service must comply with European data protection regulations (Robinson, 2011). Clients need to be made aware of the terms of such a service and users need to be aware of where liability lies if their accounts are breached. For this to work there needs to be a certain amount of trust between the client and provider. Trust the client will not abuse what rights they have and trust that the provider will behave in the way that is expected. According to the National Institute of Standards and Technology (NIST), “Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use, and disposition of personal information (PI) and personally identifiable information (PII) in the cloud system.”(NIST, 2011). It goes on to state that, even though the cloud is available to provide a platform for shared software, resources, and information, the services also pose privacy and security problems to the consumer (NIST, 2011).

The term cloud computing could be considered to have multiple meanings in information technology; from a technical perspective cloud computing may be considered as a means of allowing an application to be deployed to an environment that is easily accessible and one that can be scaled to meet user demand (Varia and Mathew, 2013). Alternatively it could be used as a marketing or business tool to describe a service that allows a user to access data or software from any location in the world (Amazon Web Services, 2013). In both senses cloud computing may be interpreted as online services accessible via the internet. However, it should be realised that although cloud computing supports a remote logical processing environment accessible via the internet, in reality the cloud is manifested in physical servers which may be storing and/or processing user data remotely and like any form of data processing and storage it needs to adhere to the data protection act.

An increase in the number of mobile device has seen more people using cloud based service and application (Cisco, 2014). It could be suggested that with an increase in demand there may be an increase in the number of cloud services offered to user. These services may be storing and processing user data, therefore, it could be suggested that cloud based services need to adhere to legal requirements defined in the data protection act. However, if these cloud services are focused on marketing and profit, the user's data protection may take a back seat.

## 2. The Cloud Model

Grance & Mell (2011) outlines a generally accepted definition of what comprises the cloud. Cloud computing is a blanket term used to describe a computing model where data, resources and/or infrastructure are stored remotely, shared amongst multiple consumers, and accessed via the internet rather than on a local computer or network. The Cloud model is considered to consist of five essential characteristics and three service models. The five characteristics, outline the minimum properties a computing service must possess before it can be considered to be part of the cloud (Figure 1).

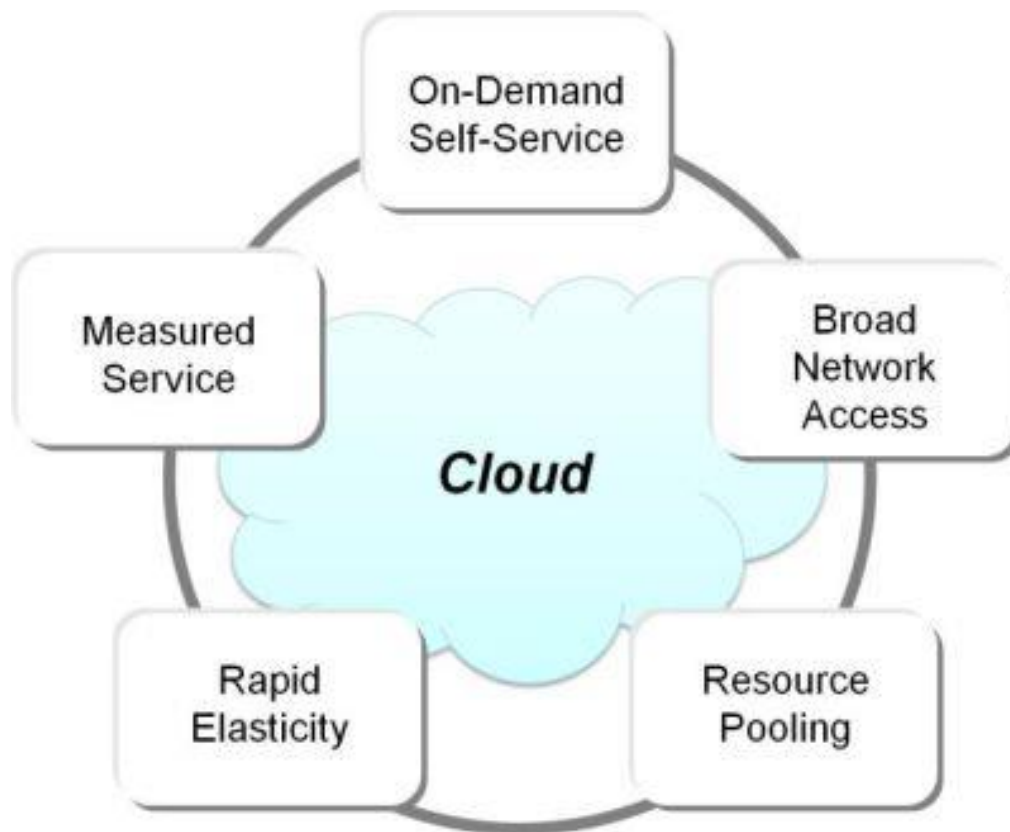


Figure 1. The 5 essential characteristics of the cloud computing model (The Open group, 2013)

1. *On-demand self-service.* The services offered by a vendor must be always available and should be easily configurable by the consumer without intervention from the service provider.
2. *Broad network access.* Services should be available over the internet and should be inclusive in terms of access platforms and client models.
3. *Resource pooling.* Resources provided by the vendor are pooled and shared amongst multiple consumers and should be sufficiently dynamic to quickly react and adapt to changing consumer requirements.
4. *Rapid elasticity.* Service provision should be able to scale quickly, and with little effort, to provide the correct level of service the consumer requires, when it's required.
5. *Measured service.* Vendors should adopt a system which allows service provision to be measured and monitored using a metric that is appropriate to the services being provided. This ensures transparency between consumer and vendor.

The cloud can be conceptually considered to be comprised of a three layered model for service provision. The first layer, *Software as a service*, is a software deployment model where the required functionality is offered as a remote, often bespoke, facility which is adaptable to the customer's demands providing a service which is flexible, scalable and cost effective. The second layer, *Platform as a service*, offers a development environment and associated solution stack as a remote service package. This provides the consumer with the facilities required to conduct a development project using software and services based on the internet, without the need to be concerned with the underlying hardware or infrastructure. The final layer, *Infrastructure as a service*, offers fundamental computing infrastructure delivered as a service. Storage, processing and network capabilities are accessible as a remote, often virtualized, scalable product. This service can be considered analogous to computing as a utility with a similar pricing model. (Jadeja & Modi, 2012)

Supplementary to these characteristics and service models are a further four classifications; the deployment models. In reference to cloud computing, a deployment model is the term used to attempt to classify and group the different configuration possibilities that exist under the cloud computing model. It outlines 4 different deployment categories, loosely based on access rights.

*Public Cloud* - The service vendor provides resources, typically applications or storage, to the public via the internet often using traditional web browsers. This service may be offered free but is more commonly charged using a "pay as you use" model. Leading to the belief that cloud computing may evolve to become the fifth utility. These clouds are usually hosted at the location of the provider.

*Private Cloud* - The service is provided for the use of a single organization. This reduces concerns over security and maintenance as all resources are managed in house by the organization and access is restricted to approved persons. The service may be provided by the organization itself, purchased from a third party or a combination of both.

*Hybrid Cloud* - This category describes a deployment model that combines aspects of both public and private (even community) models. All the components of a hybrid cloud remain discrete entities but are connected in some way via standards or technology, to offer increased business value. A hybrid cloud can have the security of a private cloud but can also employ the resources of the public cloud when required.

*Community Cloud* - Similar to a private cloud, this model allows the infrastructure and services of the provider to be shared among different organizations that share a common purpose or concern or have complimentary requirements and policies.

Cloud computing offers many advantages over traditional computing models. The most obvious is financial savings. Research from Microsoft suggests that pre-2010 up to 89% of a company's I.T. budget was spent on maintenance and infrastructure (Keshavarzi *et al*, 2013). The availability of computing infrastructure, software and processing power to be purchased as a service changes I.T. overheads from being capital expenses into operational costs. Eliminating significant up-front outlay and increasing fiscal efficiency. The cloud model also offers greater flexibility than traditional models. In the past if a company wanted to expand its capabilities it would be required to invest in equipment, software licenses and premises to locate them. Now infrastructure and processing can be purchased when required and can expand and contract as demand dictates. This scalability offers greater control and cost efficiency. The cloud model also provides greater convenience and availability. As services and infrastructure are offered remotely they can be accessed from any geographical location, cultivating collaboration and improving the work/life balance of users. Backup and recovery issues are also improved by the adoption of cloud technology. At its most basic the cloud can be used as a location to store back-ups of data held on

physical machines. In most cases cloud vendors will offer flexible solutions to back-up issues. These benefits can be derived logically from the architectural and deployment structures outlined by Grance & Mell and are increasingly being corroborated both anecdotally and statistically. It is important however to realise that it is only one half of the narrative. The adoption of new technology has never been an entirely positive event and many people believe cloud technology to be no different. Larry Ellison, chairman of I.T. giant Oracle suggests a cautious approach - *"The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements. The computer industry is the only industry that is more fashion-driven than women's fashion. Maybe I'm an idiot, but I have no idea what anyone is talking about. What is it? It's complete gibberish. It's insane. When is this idiocy going to stop?"* (McKendrick, 2013)

The argument exists that there is no such thing as a "personal cloud" system, that the cloud is there to benefit big entities and there is nothing personal about it (Searls, 2013). The "cloud" is an extremely technical term. The "cloud", thanks in part to its name, is extremely marketable therefore it was only a matter of time before a cloud existed for everyone to utilise (Caso, 2014). The cloud in this sense is personal. A personal cloud, for anyone to use. In general there are two main types of personal cloud technologies out there: Public and Private. Public cloud systems such as Box, Dropbox, Google Drive, iCloud etc. are public because it is free and widely available to use. All anyone would need is an internet accessible device and a connection. Public also means that my data is beside your data (Caso, 2014). A private personal cloud however is different when we have companies such as Younity that will create a personal and private cloud service for anyone that is willing to pay. This cloud, built using the users own software and hardware, is the users and the users alone (Caso, 2014). This dramatically reduces the risk involved in using a personal cloud. This service is without doubt the most secure way of moving to the cloud. This is the future and the only reason people seem to be slow to move toward the cloud is that they have so much data which is spread across so many devices. According to Gartner in 2013 the average household contained 1 terabyte of data and Gartner also suggests that this figure will rise to 3.3 terabytes by 2016 (Caso, 2014).

### 3. Privacy and Security

Rajat Bhargava, co-founder of JumpCloud has stated that, "There's no more debate. When you don't own the network, it's open to the rest of the world, and you don't control the layers of the stack, the cloud - by definition - is more insecure than storing data on premises (Perloth, 2014). By 2017 it is estimated that the amount of cloud IP traffic will be up to 443 exabytes per month, this figure will have risen from 98 exabytes a month 5 years previous (Kleyman, 2014). Cloud security is growing and is now an industry on its own. There to protect what privacy we have left. In the past year we have seen a large amount of hacks on various high profile individual's cloud accounts. This makes cloud security and more locally personal cloud security more poignant and important than ever. What is the best way for users to protect their data, to stop pictures leaking to the web? There are a few steps that a user can take to secure their cloud accounts as best as possible. Data encryption, securing their machines and securing their network is just a few (Kleyman, 2014). There are many methods to secure your network. Vigilance is key when browsing the web. If you feel that a website is unsafe then the best approach to take would be to stay well away from it. Never access a banking or high risk site from a public network where a hacker could retrieve some very important details. With some of these practices the user can reduce their chance of account violation. New security concerns seem to appear every week, if not more often. We need to question why we would want to keep all our data on-line, in the same place, where

anyone with the means and motive could try to harvest some of our most personal details. Take iCloud for example and the recent security breaches.

Security practices are ever evolving and now after the most recent batch iCloud hacks there is no doubt that Apple will be concentrating a great deal of their resources on ensuring that no more iCloud accounts are hacked in the future. The one benefit about these extremely high profile hacks is that cloud companies will not want this to happen to them and hoping not to be at the forefront of another international scandal. What can the public learn from what Apple claims are "very targeted attack on user names, passwords and security questions, a practice that has become all too common on the Internet (Gallagher, 2014). None of the cases we have investigated has resulted from any breach in any of Apple's systems including iCloud or Find my iPhone." (Gallagher, 2014). This has happened before and will no doubt happen in the future. The reputation of iCloud and other mobile cloud services has been blemished before and they are no stranger to attacks like this. It was first thought that this attack was what was known as a brute force attack, where a hacker or a group have forcefully gained access to these peoples account through repeatedly attacking the Find My iPhone app to try and get the password using two separate "dictionary" files to crack the passwords of the users account. This was an error in the application as it would not lock the user out for failing to provide the right answer a number of times (Gallagher, 2014). Apple denied this and it is now thought that the hacker(s) used "phishing" emails to gain entry or by using personal information to guess the password on the account (Gallagher, 2014). There is very little that could have been done to prevent this although the affected users account passwords may have been quite weak and a strong password always leads to stronger security (Gallagher, 2014).

A public cloud service stores all the data they are given, yours, mine, ours, in the same location. This puts an enormous target on the back of these service providers. A goldmine of information that is just a security breach away. There are methods that can be taken to try prevent any breaches on these sites. Although total security is a thing of the past, or future, these methods can help reduce the risk of your files being breached. Client-side encryption for example is something that all consumers should think about although very few do (Caso, 2014).

## 4. The Data Protection Act and Cloud Computing

In the past a user may have used software installed locally on their computing devices. If the client machine processed the data, and stored the data locally on their machine then this data may not have been retained remotely. However, a paradigm shift in computing has seen data processing and storage moved online to the cloud; with only a thin client application installed on the user's device (Intel, 2015). The growth in usage of mobile device has seen an increase usage of application installing thin client application on the user's device and the user's data being stored and processed remotely on the cloud (ICS, 2015). These thin client applications may be collecting and processing user information. However, it may not be clear to the user how they're information is being used and how much of their data is being collected and stored by the data controller. There are a number of key aspects in the Data Protection Act. For the purpose of this chapter, the focus will be on those of the data controller and also the data processor.

A data controller is considered the individual or company who controls and is responsible for the storing and controlling of user's personal information. The data controller is legally responsible; therefore it needs to be clear if the party storing or using the data is the data

controller as the responsibilities for data protection will fall with that individual or company (Data Protection Commissioner, 2005). A data controller stores personal information about a person, controls which data is stored, controls how the data is stored and controls how the data is used. All data controllers must comply with certain rules about how they collect and use personal information.

Ultimately, the data controller should ensure that data is obtained and processed lawfully and fairly, data is only stored for a specific purpose, data is only processed as initially defined, data is stored safely and securely, data is accurate and up-to-date, that it is adequate, relevant and not excessive, data is not retained longer than is necessary and a copy of the users data can be provided to them on request.

If an individual or company holds or processes user data on behalf of another party, then the other party is the data controller, and individually or company holding or processing the data is a data processor (Data Protection Commissioner, 2005). A data processor may maintain or process user's personal data, but do not exercise responsibility or control over the personal data. In contrast to data controllers, data processors have a limited set of responsibilities under the Data Protection Act. A data processor should only process data under the instructions of the data controller. The data processor should ensure the data is stored securely and must ensure that it complies with the contract defined by the data controller and does not process and/or share the data in any way that is not defined by the data controller (Data Protection Commissioner, 2010).

Twenty six privacy enforcement authorities participated in the second Global Privacy Enforcement Network Privacy Sweep. The Sweep had identified mobile apps as a key area of focus in light of the privacy implications for consumers (Data Protection Commissioner, 2014). In total, 1,211 apps across a number of platforms and categories were examined. Approximately one-third of the apps (31%), were considered to be requested access to data that was not related to the purpose of their functionality, this was according to the sweepers understanding of the app and the associated privacy policy. Three-quarters of all apps examined requested access to potential sensitive data with little transparency to what purpose the data was collected, and how the apps would use the data (Data Protection Commissioner, 2014d). The results of the mobile application sweep offer some insight into the types of information companies are seeking and the extent to which organisations are informing consumers about their privacy practices. The sweep suggested that more information may have to be collected that is required.

It could be suggested that the mobile application where collecting information to improve the users experience that may not have been apparent during the investigator carrying out the sweep. However, as per the data protection act, the data controller should only collect information that is required. It could be suggested that the data protection act provides a set of rules that may help protect and ensure the user data is managed correctly by the data controller. However, if the data controller does not adhere to these rules or provide transparency then it is difficult to determine if the users data is being stored safely and not being misused. In the case where an investigation was carried out on a number of mobile applications, it was suggested that a number of them were collecting information that was not related to their main purpose, or there was no clarify to why and how the data was being used. As defined in the data protection act, a data controller must only collect pertinent data and indicate their intention for collecting it. As a result it could be suggested that any application not adhering to this is not protecting the user's data correctly. In summation, the data protection act may define rules for handling user data, but due to the changes in how users are disclosing their information to online and cloud services then a new set of rules may be required to manage these type of data controllers, otherwise, it may be difficult to ensure user data is protected.

## 5. The Future

At the keynote at the Net Events EMEA Press & Service Provider Summit in Portugal Tom Homer, Telstra's Head of EMEA and the Americas, Global Enterprise & Services stated that in the future employees will be able to bring their own 'cloud' to their respective jobs with them. This is a major development for the technology. This would lead one to believe that before long cloud computing's influence would lead to the workplace of the future no longer being a physical location. That wherever the employee is, that is their office. This in effect will significantly reduce the daily operating costs for any company. If this really is the future, which many think it, then many personal cloud service providers will be overjoyed. This will mean a great surge in business for companies like Box which Homer says Telstra have invested in with his predictions in mind. According to Homer, "We are responding to the evolution of cloud technologies right now and recognise that computer power is required in many different forms." (Homer, 2014)

There is a new wave coming called *Anything as a Service* (XaaS). This poses new risks that will need to be addressed. XaaS companies provide the consumer with integrated features of cloud-based data, infrastructure, software, and platforms (Balaciart, 2014). Using the cloud so extensively is putting so much faith in a company which you physically cannot see. Trust is most important in these business partnerships. Trust that a business will not regret putting so much faith in one service provider. Although, it has to be said, using a XaaS provider also minimises the risk involved with cloud computing as all of the security needs are going to be dealt with by one product provider whereas with multiple providers it may be difficult to customise the security to the company's needs (Balaciart, 2014). The emergence of these XaaS providers will shape cloud computing in the near future.

## 6. Conclusion

Aside from the security considerations that are inherent in all internet based activities, the cloud model of computing has its own specific concerns. The multi-layered architecture, combined with different modes of deployment, produce numerous specific security issues that continue to affect both the reputation and pervasiveness of the model (Behl & Behl, 2012). The security and integrity of the underlying infrastructure that permits the cloud model of computing has been the subject of much research and is still very much an open topic for both consumers and providers. From the work of Behl & Behl (2012) and Keshavarsi *et al* (2013) it is possible to identify and address three major concerns related to the infrastructure of the cloud. The nature of the cloud model means that not only is the data and applications of users stored and accessed remotely, the responsibility for controlling access and keeping these assets secure has also been devolved. To ensure trust in this system a water-tight understanding between consumers and service providers must exist that addresses the authorisation, authentication and auditing of individuals interacting with the system (Kulkarni *et al*, 2012). The shared computing paradigm that underpins cloud computing evidently involves multiple users accessing the same infrastructure, both virtualised and physical. This, coupled with the characteristic of rapid elasticity, implies that it is possible, even likely, that resources acquired for the use of one tenant were recently under the control of another. For this situation to be considered safe there must exist some mechanism that ensures that data remains isolated and cannot be recovered either by direct methods or inference.

A significant portion of the technology that supports and enables the cloud model of computing was not initially intended for that purpose. Many of the physical components (CPU's, GPU's, etc.) were not designed for a multi-tenant architecture and as such may lack the isolation properties required for the model to be secure (Walker, 2013). The relative infancy of the cloud model can also lead to software based vulnerabilities. Poorly designed API's and user interfaces can lead to possible exposures that not only affect the user involved but may impact other organisations using the same cloud provider (Keshavarsi *et al*, 2013). Massively increasing the potential attack surface for anyone with malicious intent. The cloud security alliance identifies cloud abuse as one of the nine critical threats for cloud security. This report also outlined the daunting scenario of the cloud being used to essentially attack itself, through distributed encryption key cracking or massive DDos attacks. (Walker, 2013). Considerable research has been conducted into ways of mitigating these concerns (Behl & Behl, 2012; Kulkarni, Chavan, Chandorkar, Waghmare, & Palwe, 2012). The author believes that the combined approach of a bespoke, systematic risk assessment such as described by Djemame *et al* (2014) coupled with detailed service level agreements negotiated between provider and consumer can at least ensure that security expectations from both parties are consistent and achievable. This can, and should, be enhanced by adopting a structured testing framework similar to the process developed by Iyer *et al* (2013) to ensure that assurances are met and undertakings are being adhered to. While it is ultimately unlikely that the threat of infrastructure intrusion will ever disappear, collaboration from everyone involved can significantly reduce the potential and increase stakeholder confidence in the integrity of the cloud model.

The structure and characteristics of the cloud computing model intrinsically suggest many potential data protection issues. The distributed nature of the model increases data mobility and raises concerns over where data is stored. It can often be difficult for consumers to find out where exactly their data is being housed and if suitable measures are in place to protect that data. Storage locality may also have serious legal implications as data protection and compliance regulations often vary between countries and jurisdictions (Subashini & Kavitha, 2011). The research of Chen & Hong (2012) outlined how the cloud model requires specific security considerations at every stage in the data life cycle. Data is not only being shared, stored and archived in the cloud but also increasingly generated and destroyed. The privacy and integrity of this data, and any associated metadata, must be assured if confidence in the cloud model is to grow. Assuring the integrity of data is a major open question within the cloud community. Traditional methods of integrity verification are not suitable for data stored remotely as it would require significant data transfer and associated costs. The ACID framework conventionally used to aid data integrity is becoming increasingly irrelevant in the modern world of Big Data and NoSQL. The work of Sugumaran *et al* (2014) and Behl & Behl, offer practical solutions to many of these issues but significant further research and discussion is required if a unilateral approach is ever to be agreed.

The advocates of cloud computing are consistently the darlings of the media offering an ever growing array of sound bites and evangelical predictions on where this journey will take us all. Many of these claims may transpire to be correct but the initial impulse to migrate one's business interests to the cloud should be tempered by a thorough audit of expectations and a realistic assessment of what the technology has to offer. Cloud computing, like every innovation, has its benefits and its limitations. The commercial and economic factors outlined above make it likely that an increasing number of small to medium businesses will indeed be tempted to deploy their I.T concerns onto the cloud. If the security and data protection concerns described previously are to be eradicated, further research is needed to identify the security requirements of stakeholders at every level.

## References

Behl, A., & Behl, K. (2012, Oct. 30 2012-Nov. 2 2012). An analysis of cloud computing security issues. Paper presented at the Information and Communication Technologies (WICT), 2012 World Congress on.

Borrill, S. (2014). *Telstra Keynote Urges CIOs to Master the Art of Shaping Cloud Services* Telecomstalk. Telecomstalk.com. Available at: <http://www.telecomstalk.com/?p=3823>.

Balaciart, D. (2014). *What The Future Of Cloud Computing Will Bring* | clouderPC. clouderPC. Available at: <http://www.clouderpc.com/the-future-of-cloud-computing-includes-combining-all-services-together/#.VD67AGewliY>

Caso, E. (2014). *The Rise of the Personal Cloud* | WIRED. [online] WIRED. Available at: <http://www.wired.com/2014/01/rise-personal-cloud/>

Chen, D., & Hong, Z. (2012, 23-25 March 2012). Data Security and Privacy Protection Issues in Cloud Computing. Paper presented at the Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on.

Data Protection Commissioner (2005). Are you a data controller? Available: <http://www.dataprotection.ie/docs/Are-you-a-Data-Controller-/43.htm>.

Data Protection Commissioner (2014). Global Privacy Sweep raises concerns about mobile apps. Available: <http://www.dataprotection.ie/viewdoc.asp?Docid=1456&Catid=66&StartDate=01+January+2014&m=>

Dinadayalan, P., Jegadeeswari, S., & Gnanambigai, D. (2014, Feb. 27 2014-March 1 2014). Data Security Issues in Cloud Environment and Solutions. Paper presented at the Computing and Communication Technologies (WCCCT), 2014 World Congress on.

Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2014). A Risk Assessment Framework for Cloud Computing. Cloud Computing, IEEE Transactions on, PP(99), 1-1.

Grance, T., & Mell, P. (2011). The NIST definition of cloud computing: National Institute for standards and technology.

Jadeja, Y., & Modi, K. (2012, 21-22 March 2012). Cloud computing - concepts, architecture and challenges. Paper presented at the Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on.

Gallagher, S. (2014). *Update: What Jennifer Lawrence can teach you about cloud security*.

Ars Technica. <http://arstechnica.com/security/2014/09/what-jennifer-lawrence-can-teach-you-about-cloud-security/>

Homer, T. (2014). *2020 Vision for Cloud Services to the Enterprise What Service Should the Enterprise Expect and Demand by 2020?*. 1st ed. [ebook] Quinta do Lago, Portugal: EMEA.

Intel. (2015). Intel's Vision of the Ongoing Shift to Cloud Computing. Available: <http://www.intel.ie/content/dam/www/public/us/en/documents/white-papers/cloud-computing-intel-cloud-2015-vision.pdf>

Kelyman, B. (2014). *How I Secure My Personal Cloud*. Dark Reading. Available at: <http://www.darkreading.com/cloud-security/how-i-secure-my-personal-cloud/d/d-id/1113941>

Keshavarzi, A., Haghighat, A. T., & Bohlouli, M. (2013, 12-14 Sept. 2013). Research challenges and prospective business impacts of cloud computing: A survey. Paper presented at the Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013 IEEE 7th International Conference on.

Kulkarni, G., Chavan, N., Chandorkar, R., Waghmare, R., & Palwe, R. (2012) Cloud security challenges. Paper presented at the Telecommunication Systems, Services, and Applications (TSSA), 2012 7th International Conference on, New York, USA, 30-31 Oct. 2012.

McKendrick, J. (2013). 10 quotes on cloud computing that really say it all. <http://www.forbes.com/sites/joemckendrick/2013/03/24/10-quotes-on-cloud-computing-that-really-say-it-all/>, 29th September 2013, Chicago, USA

NIST Cloud Computing Standards Roadmap. (2011). 1st ed. [ebook] The US Department of Commerce. Available at: [http://www.nist.gov/itl/cloud/upload/NIST\\_SP-500-291\\_Version-2\\_2013\\_June18\\_FINAL.pdf](http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf)

Perlroth, N. (2014). *Security Needs Evolve as Computing Leaves the Office*. [online] Bits Blog. Available at: <http://bits.blogs.nytimes.com/2014/06/11/security-needs-evolve-as-computing-leaves-the-office/>

Shetty, S. (2013). Gartner Says Cloud Computing Will Become the Bulk of New IT Spend by 2016. Analysts Examine Cloud Strategies and Adoption at Gartner Symposium.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1-11.

Walker, K. (2013). The Notorious Nine: Cloud Computing Top Threats in 2013. [www.cloudsecurityalliance.org/topthreats](http://www.cloudsecurityalliance.org/topthreats).: Cloud Security Alliance.

Rai, A. and Sharma, S. (2013). *Privacy Issues Regarding Personal Data In Cloud Computing*. 1st ed. International Journal of Advanced Research in Computer Science.

Robinson, N. (2011). *The Cloud*. 1st ed. Santa Monica: Rand.

Tomonari, K. and Yukio, E. (2010). *Achieving a "Personal Cloud" Environment*. 1st ed. NEC Technical Journal.

### **Review Questions**

1. Why is privacy such a major concern when referring to the cloud?
2. What are the five essential characteristics and three service models of the Cloud?
3. What comprises the three layered model for service provision in the Cloud?
4. What are the key differences between Public, Private, Hybrid and community clouds?
5. How important is the data protection act when it comes to Cloud computing?