Chapter 16
Security Issues to Cloud Computing

Cyril Onwubiko

Abstract With the growing adoption of cloud computing as a viable business proposition to reduce both infrastructure and operational costs, an essential requirement is to provide guidance on how to manage information security risks in the cloud. In this chapter, security risks to cloud computing are discussed, including privacy, trust, control, data ownership, data location, audits and reviews, business continuity and disaster recovery, legal, regulatory and compliance, security policy and emerging security threats and attacks. Finally, a cloud computing framework and information asset classification model are proposed to assist cloud users when choosing cloud delivery services and deployment models on the basis of cost, security and capability requirements.

16.1 Introduction

As organisations seek new ways of driving businesses forward, increasing demands are now placed on computer networks to provide competitive edge and create new opportunities at reduced cost. This has accelerated business and technological initiatives that promise to provide services at comparably low infrastructure and operating costs. The rapid growth of cloud computing is a good example.

This new model of service (cloud computing) offers tremendous reduction in operating cost; unfortunately, it has also introduced a set of new and unfamiliar risks. Most networks today are borderless, spanning across different network estates, security domains and enterprise, whose security policies, security protection mechanisms and business continuity plans are different, varying and diverse. Consequently, new security requirements are needed, new forms of protection strategies become essential and existing practices may require reviewing.

C. Onwubiko (✉)
Security & Information Assurance, Research Series Limited, 1 Meadway,
Woodford Green, IG8 7RF, Essex, UK
e-mail: cyril.onwubiko@research-series.com

N. Antonopoulos and L. Gillam (eds.), *Cloud Computing: Principles, Systems and Applications*, Computer Communications and Networks,
DOI 10.1007/978-1-84996-241-4_16,

To address the inherent risks in cloud computing, fundamental security issues that exist in traditional networks must be evaluated in relation to cloud computing. Risks to cloud computing delivery models, such as software as a service (SaaS), hardware as a service (HaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) must be identified and discussed in detail. Interdependent risks and cumulative risk arising from private, public, virtual private, localised and federated clouds must be outlined and discussed. Issues of information ownership, trust, confidentiality, integrity, privacy and anonymity must be addressed. It is pertinent to note that understanding risks that exist in the cloud is fundamental to understanding how best to treat risks inherent in cloud computing.

16.2 Cloud Computing ('The Cloud')

Cloud computing is an emerging technological development that leverages the Internet to provide unparalleled distributed computing service based on service-oriented architecture (SOA) and virtualisation. Cloud computing appears to be ubiquitous, dynamically scalable and on-demand, which can be purchased on a 'pay-as-you-go' basis without under or over provisioning or prior subscription. According to NIST, 'cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1,2]'. This implies that cloud computing offers on-demand self-service, a highly scalable shared pool of network resource that offers broad network access to users. These services are dynamic and affordable with minimal consumer configurable interfaces.

There are five main attributes of cloud computing:

- On-demand self-service
- Ubiquitous network access
- Location independence and homogeneity
- Elastically scalable
- Measured service

First, the cloud offers on-demand self-service; this means that the cloud can be used as and when required without prior subscription. It does not require pre-booking or 'phased-delivery' for the consumer; hence, there is no need for under or over subscription in the cloud.

Second, the cloud offers almost infinite network access to vast infrastructure and computing resources, such as storage facility, memory, processor, hosting and myriad applications. Third, the cloud uses a shared pool of resources, platforms and infrastructure residing on the Internet, which is located at various parts of the world, making the cloud location-independent. The services offered in the cloud are homogenous. The same service is provided exactly in the same way to all users.

This is because of its multi-tenancy delivery model. Fourth, cloud computing capabilities, such as storage, computing power, processing and hosting are elastic; resources are pooled together to provide vast amount of computing power. Finally, cloud computing services are measured; each service purchased or utilised by a consumer is measured and billed accordingly.

With the economic downturn in 2009, cloud computing has become a viable business and technological proposition, because of the significant reduction in both infrastructure and operational costs that it offers when compared with the traditional IT services. The cloud offers huge economies of scale and enhances outsourcing and consumerisation. It is understandable that cloud computing is attractive to users who range from government agencies, financial institutions, individual and corporate users to cybercriminals. This opportunity to cohabit and share a pool of resources with all consumers including cybercriminals brings to bear a significant element of risk. Therefore, a cloud computing environment requires an implicit level of trust as well as explicit level of vigilance and risk management to ensure success [3].

Figure 16.1 is a cloud computing deployment and delivery model. It comprises five cloud delivery models, namely, public or external cloud, community cloud, agency cloud, private and hybrid clouds. The models consist of three service methods, namely, cloud software computing (SaaS), cloud platform computing (PaaS) and cloud infrastructure computing (IaaS).

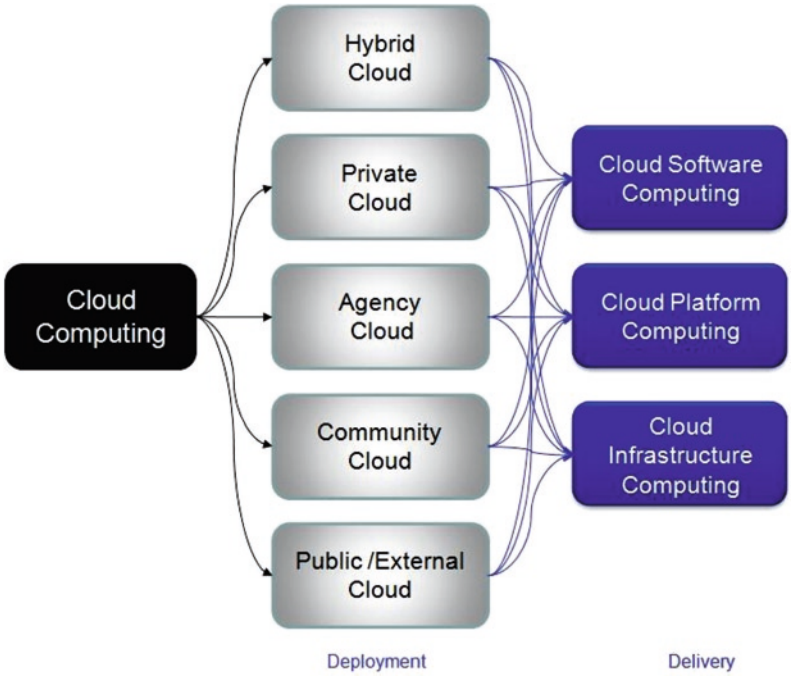

Fig. 16.1 Cloud computing deployment and delivery model

A public or external cloud is a general-purpose cloud computing environment managed by a cloud provider. The cloud provider could be external provider, such as Amazon EC2, Google Apps, Salesforce, Rackspace, etc. that leases third-party cloud resource to the consumer. However, a cloud could be public even when third-party cloud resources are not used; the most important aspect of a public cloud is its content. A community cloud is a cloud specifically consumed by a particular set of community, such as financial institutions cloud, health services cloud, etc. An agency cloud is a form of community cloud solely for the military, agency, or defence institutions, such as the Defense Information Systems Agency (DISA) cloud [4] and the NBC Federal Computing Cloud [5]. Agency clouds are not for public consumption. They are regulated and operated by the agencies themselves. A private (localised) cloud is an enterprise-owned cloud exclusively accessed for its operation or activity. It is not shared or co-owned with another enterprise, such as the Microsoft Azure on-premise platform cloud [5]. A hybrid cloud comprises two or more clouds, such as a private cloud joining another vendor's provisioned public cloud. For current cloud offerings, see Fig. 16.2 [4].

Cloud Market Types	Types of Offerings	Examples
Software-as-a-Service	• Rich Internet application web sites • Application as Web Sites • Collaboration and email • Office Productivity • Client apps that connect to services in the cloud	• Flikr • Myspace.com • Cisco WebEx office • Gmail • IBM Bluehouse
App-components -as-a-Service	• APIs for specific service access for integration • Web-based software service than can combine to create new services, as in a mashup	• Amazon Flexible Payments Service and DevPay • Salesforce.com's AppExchange • Yahoo! Maps API • Google Calendar API • zembly
Software-platform-as-a-Service	• Development-platform-as-a-service • Database • Message Queue • App Servicer • Blob or object data stores	• Google App Engine and BigTable • Microsoft SQL Server Data Services • Engine Yard • Salesforce.com's Force.com
Virtual Infrastructure-as-a-Service	• Virtual servers • Logical disks • VLAN networks • Systems Management	• Akamai • Amazon EC2 • CohesiveFT • Mosso (from Rackspace) • Joyent Accelerators • Nirvanix Storage Delivery Network
Physical Infrastructure	• Managed Hosting • Collocation • Internet Service Provider • Unmanaged hosting	• GoDaddy.com • Rackspace • Savvis

Fig. 16.2 Current cloud market offering [4]

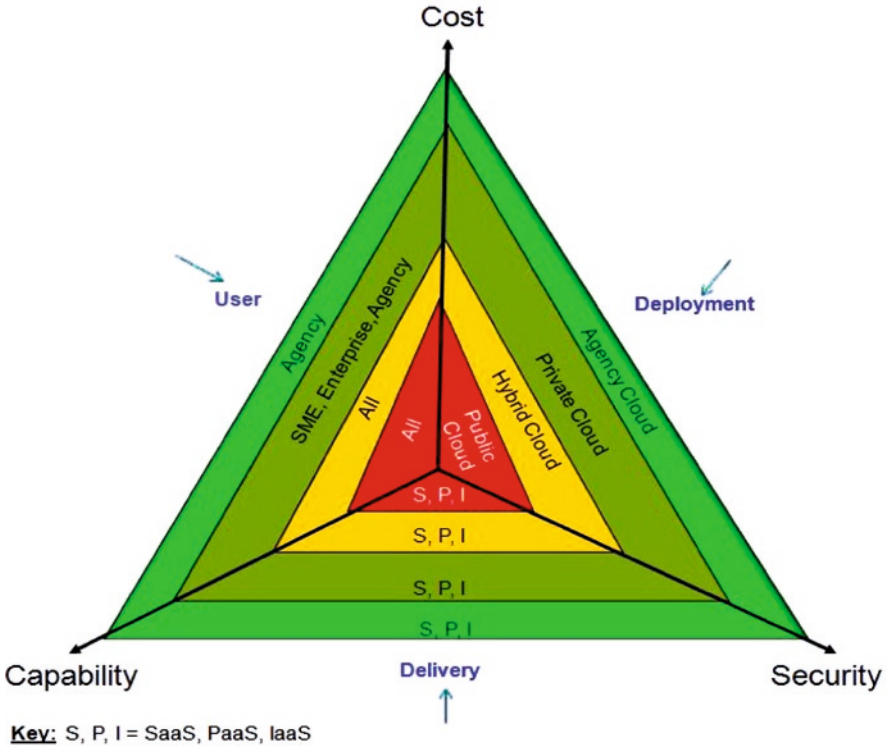

Fig. 16.3 Cloud security relationship framework

The risks inherent in cloud computing are similar irrespective of the cloud model in use; however, there are unique security and information assurance requirements for each cloud deployment model. For example, security requirements for private clouds are different from that of a public cloud. Private clouds are perceived to be more secure than public clouds. Similarly, privacy concerns vary from private to public clouds.

To provide a realistic risk management to cloud computing, each cloud deployment model must be evaluated in its own right. In this respect, a cloud security relationship framework is proposed to provide this assessment (see Fig. 16.3). A cloud security relationship model is a theoretical framework to evaluate cloud deployment and delivery models based on security, cost and capability requirements.

16.3 Understanding Risks to Cloud Computing

A major concern with cloud computing is that the cloud provider offers the resources in the cloud, that is, the software, platform and infrastructure to the user (cloud consumer). In addition, user data/information also reside with the cloud

provider. The risk with this type of service is that user information could be abused, stolen, unlawfully distributed, compromised or harmed. There is no guarantee that user's information/data could not be sold to its competitor. Unfortunately, this particular risk applies to all the three types of cloud delivery models, namely, SaaS, PaaS and IaaS.

Other risks to cloud computing also exist, and range from privacy, data protection, ownership, location and lack of reliable audit standard to data security procedure of most pioneer cloud providers, such as Google, Amazon, etc. According to Rick Gordon of Civitas Group, a concern with regard to cloud providers, especially Google Apps includes the lack of reliable security audit standard, data lock-in and Google's opacity regarding its internal data security procedures [7].

In this section, risks to cloud computing are discussed with the view to outlining technical, administrative and ethical controls to provide guidance to cloud users.

16.3.1 Privacy Issues

Privacy even with traditional information security systems and networks is difficult to satisfy, and is a challenging issue to cloud computing. Cloud computing has significant implications for the privacy of personal information as well as maintaining the confidentiality of business and government information [6]. Concerns over privacy with current cloud computing offerings are apparent and real. For example, in a letter from Pam Dixon, executive director of the World Privacy Forum to the Los Angeles Mayor, Antonio Villaragosa, it was stated that, 'our concern is that the transfer of so many City records to a cloud computing provider may threaten the privacy rights of City residents, undermine the security of other sensitive information, violate both state and federal laws, and potentially damage vital City legal and other interests [7]'. This concern is valid and true, especially with public clouds where sensitive individual and corporate information is put in the hands of third-party cloud providers, whose cloud infrastructure may not be regulated, and could traverse through geographical borders that impact both legal and regulatory requirements of the information being transported or stored.

Further, information in the cloud is perceived to have weaker privacy governance over that held in a personal physical computer system [6]. Hence, cloud users must be aware of the terms of contract they sign with a provider, and should be informed of the provider's privacy and security guidelines and practices.

We recommend that privacy and security requirements of the different forms of cloud models are investigated and assessed, because not all cloud models raise the same privacy and confidentiality issues. As shown in Fig. 16.3, each cloud model offers unique security requirements, privacy capabilities and varying cost implications. For example, private or agency clouds are most suitable for protectively marked materials or classified information, but are more expensive to operate, while public clouds are suitable for personal non-confidential information such as sharing photos or pictures with friends.

Again, it is important that cloud consumers (individual or corporate) assess the information requirements and understand the underlying regulatory and compliance requirements of their assets before migrating such assets to the cloud. Otherwise, they risk violating or undermining privacy, regulatory and compliance requirements of such assets.

Finally, users must apply due diligence on each cloud provider they intend to use, and must ensure that the necessary privacy laws are included in the service contract issued by the cloud provider.

16.3.2 Data Ownership and Content Disclosure Issues

Another issue to consider before migrating to the cloud includes ownership of information or data residing on the provider's cloud. The moment a user puts data to the cloud, not only could the privacy of the data be lost, but also the ownership 'authority' over the data and right of disclosure could well be lost (by alienating ownership to the cloud provider). Although the lawful ownership and right of disclosure remains with the originating data owner, this could change quite quickly. Some providers retain the right of disclosure as data custodians, while others do not. This practice is gradually changing depending on the terms of the contract, which the provider issues to its customers.

There is a concern when the cloud provider becomes both the data owner and the data custodian. Even with traditional IT services, it is best practice to have separation of duties, where a different individual is the data owner, while another individual or group is the data custodian. This shifting paradigm with the cloud means that the cloud provider is both the data owner and data custodian for all data stored or transmitted from their cloud, including data from 'delinquent organisations', such as cybercriminals and organised crime groups. This practice violates the principle of separation of duties and job rotation; a fundamental principle of information security best practices.

We recommend that cloud users protectively mark their information and explicitly specify the ownership of information in the service contract. The service contract must be signed and indorsed by the cloud provider in form of a declaration. Protective marking is an administrative control used to classify information assets based on the degree of sensitivity afforded to that asset. For example, information can be protectively marked as 'TOP SECRET', 'SECRET', CONFIDENTIAL, etc.

16.3.3 Data Confidentiality

When a user puts information to a public cloud, what control does that user have over the data, its confidentiality, integrity or availability? When we consider small to medium-sized organisations or individual users, one could easily discuss the

risks associated with cloud computing services. What happens to the government, the enterprise in relation to the cloud? Can the cloud be used for government-protected marked information? For example, 'SECRET' document for defence agencies, such as for the CIA, MI5 or the MOD. I certainly do not think so, especially at this current stage of the cloud. These agencies have their own clouds, such as the MOD cloud, the DISA cloud, etc.; however, what is put in these clouds are still of great concern. It is pertinent to note that cloud computing is not ideal for all use cases. For example, protectively marked information asset up to the level of 'SECRET' or 'TOP SECRET' is not suitable for cloud computing (see Fig. 16.4). Similarly, 'STRICTEST IN CONFIDENCE' and 'IN CONFIDENCE' data may not be suitable for the cloud.

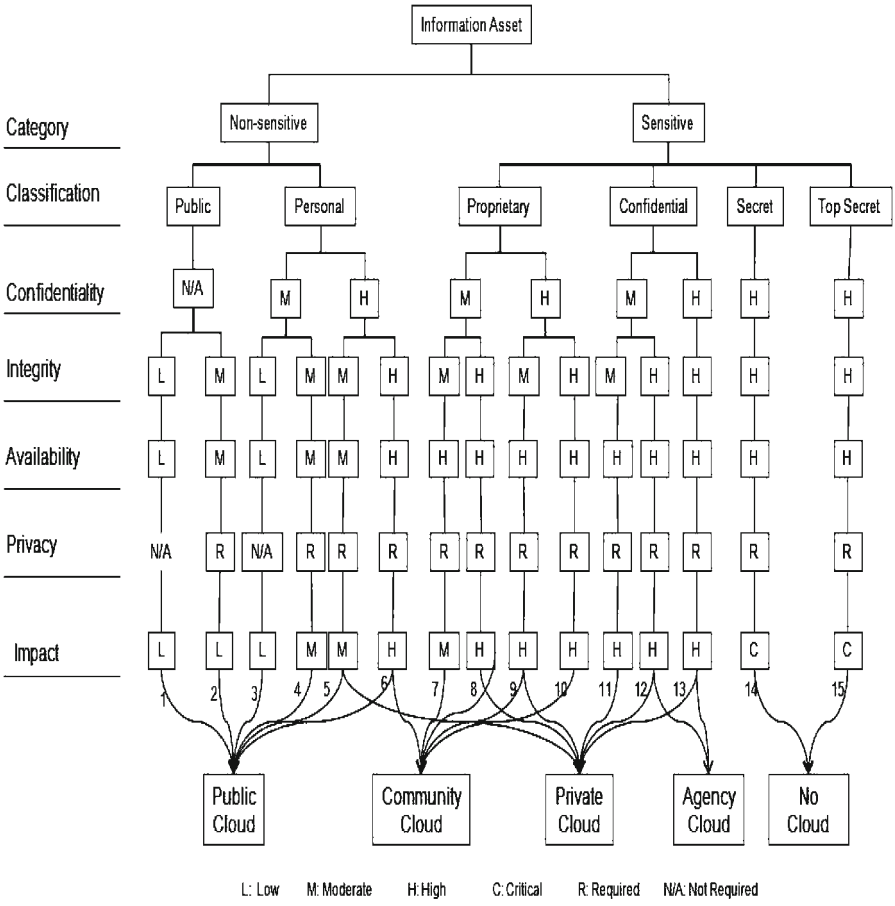

Fig. 16.4 Information classification to cloud mapping

We recommend a risk-management approach when evaluating information assets to be migrated to the cloud, giving conscious attention to the security and information assurance requirements of those assets.

16.3.4 Data Location

Where does the data that an end-user has created on an MCSP's system reside? Location of end-user data is of great importance. For example, the EU Directive on Data Protection (Safe Harbour [8,9]) stipulates countries where EU private and personal data can and cannot reside or traverse.

The EU Directive on Data Protection of 1998 [9] is a comprehensive data protection legislation that orders its member states to establish a legal framework to protect the fundamental rights to privacy with respect to processing personal data that has *extraterritorial effect*. It prohibits the transfer of personal data or health records data to non-EU nations that do not meet the European '*adequacy*' standard for privacy protection. The US and the EU share the goal of enhancing privacy protection for their citizens [9]. Clearly, achieving regulatory and legislative compliance in the cloud requires concerted effort from both the user and the provider, where the user knows the information requirements and is able to communicate that clearly to the provider, and in return, the provider is transparent and thus willing to address the regulatory and legislative mandates required with regard to the assets.

With the infrastructure as a service, the cloud provider can dynamically use localised infrastructures that exist outside the EU or US territories. This may contravene or abuse fundamental privacy and legislative mandates, especially if the end-user is not aware of where the information is held or transported to/from. This applies specifically to EU and US cloud consumers, SMEs, government and enterprise who may wish to use the cloud for delivering service. Other countries have other legislations that should be considered when using the cloud. Certain types of assets may easily be abused with cloud computing, for instance, personal medical data (health record data) are subjected to strict compliance act, such as the health information privacy and portability act (HIPPA). A significant concern is that personal medical data can be easily circumvented with the SaaS or IaaS models of the cloud. This highlights some of the inherent risks that exist with cloud computing [10].

That being said, there are cloud providers that operate territorial cloud service. For example, there are UK cloud providers that lease zoned UK only localised resources. In addition, there are US and Canadian cloud providers that offer localised provincial cloud services.

Cloud users whose information assets require location-specific data storage or transit requirements must confirm these with cloud providers that offer location-based cloud service, and must ensure that they are included in the service contract offered by the cloud provider.

16.3.5 Control Issues

It is not until recently that many cloud security interest groups, such as the Cloud Security Alliance [11], the Cloud Computing Interoperability Group [12] and the Multi-Agency Cloud Computing Forum [4] began to seek ways of delivering efficient and effective controls in the cloud to ensure that information in the cloud are secure and protected.

Currently, clouds are hugely uncontrolled, especially the public ones. Recommendations like the use of legal, regulatory, compliance and certification practices have been suggested in order to adequately control cloud services and practices [3,11,12]. Unfortunately, maintaining compliance with regulatory and legislative requirements in the cloud can be much more difficult to demonstrate. The attributes of cloud computing as being location-independent, with unclear borders and boundaries, providing shared pool of resources on a multi-tenancy architecture further make achieving demonstrable regulatory security compliance untenable.

The legal landscape, regulatory compliance and certification are constantly changing, and organisation must understand and evaluate current legal, regulatory compliance needs of their information before moving them to the cloud.

16.3.6 Regulatory and Legislative Compliance

Regulatory compliance and certification are security initiatives with significant impact on information security practices [8]. Standards regulate how information security management is being implemented, managed and conducted. For example, ISO 27001–2005 is a security standard that recommends best practices for information security management. Organisations seeking accreditation go through a regulatory compliance process. Compliant organisations are perceived to possess essential drivers to earn trust, and hence, attract business relations with other organisations. This proposition applies to cloud computing. In fact, obtaining certification to a particular standard is not going to be the only driver, and the coverage of each security accreditation or certification is anticipated to contribute towards establishing trust. Furthermore, compliance to regulatory authorities will certainly earn some ‘Brownie points’ for corporate organisations. For example, corporate organisations that are regulated by the financial services authority (FSA) must seek advice before using public clouds for their operations or risk of facing huge fines, and could possibly lose their practicing license. There should be guidance on what corporate financial institutions can put out in the cloud and what may not be permissible. As the cloud phenomenon unfolds and inherent risks understood, adequate guidelines must follow.

The legal landscape of traditional IT is continuously changing. A significant concern is that some of these legislations are territorial, even within a country, with separate pieces of jurisdiction. For example, the California Security Breach Information Act (SB-1386) legislation mandates Californian organisations that maintain personal information about individuals to inform those individuals if the

security of their information is compromised [13]. This piece of legislation stipulates the disclosure of security breaches only in California. The application of SB-1386 and other legislations in the cloud are unclear.

16.3.7 Forensic Evidence Issues

Information security forensic evidence and e-discovery possess a challenge too. In the cloud, what information constitutes legally acceptable forensic evidence? How is such information received in relation to the different cloud deployment models? If evidence is gathered from a public cloud, how authentic is that information perceived to be compared with when similar information is obtained from a private cloud? Similarly, with pre-trial discovery and e-discovery, as the cloud provider is the data custodian, while the user is the lawful owner of the data, who should provide pre-trial evidence in a court of law, and who is responsible with respect to discovery and other litigation subjects? With copies of most information at different clouds, which information/data constitutes an authentic copy of the information that is admissible in a court of law?

It is pertinent to note that the different cloud deployment models offer varying levels of security, privacy and acceptability; therefore, it is imperative that cloud users must evaluate the security, legal, regulatory and legislative requirements of their valued assets before choosing a particular cloud model, and a cloud vendor or provider.

16.3.8 Auditing Issues

Auditing for security management aims to evaluate policies, practices, operations and technical controls of an organisation in order to assess compliance, detection, protection and security forensics [14]. The need for regular security audits is essential, and should not focus only on the reactive audits done when an incident has occurred, but also on proactive security audits done in order to assess whether security controls, security processes, procedures and operations are adequate and practical in protecting critical assets of the organisation. Two factors make demonstrating security audit in the cloud a critical issue:

First, cloud providers must demonstrate their security audit procedure to their customers. Second, the level of audit coverage being conducted must be acceptable, bearing in mind the myriad of diverse and varied information assets that the cloud providers are data custodians for.

Auditing security requirements in a cloud environment can be difficult and significantly challenging [15]. One approach to addressing auditing issues in the cloud is transparency from the cloud provider in managing information security. That is, the cloud provider must make its customers aware of its audit processes and the different levels of audit coverage. In this way trust and good relationship between the provider and its customers can be achieved.

16.3.9 Business Continuity and Disaster Recovery Issues

Cloud computing is dynamic and offers ubiquitous network access to vast amount of significant resources, and these resources are meant to be available swiftly and on-demand to legitimate users. Unfortunately, there have been cases when the availability of data in the cloud has become a major concern. For example, Amazon's Elastic Compute Cloud (EC2) service in North America was temporarily unavailable at significant times due to 'lightning storm that caused damage to a single power distribution unit (PDU) in a single availability zone [16]'. This highlights the importance of disaster recovery and business continuity plans in the cloud. The availability of resources in the cloud is of least importance to users according to most surveys. This is because the cloud offers ubiquitous and on-demand network access. Unfortunately, information in the cloud could still be unavailable when needed due to natural disasters, vulnerability exploits and deliberate attacks.

There are three reasons why cloud users must be concerned with the availability of their valued assets in the cloud. First, most cloud providers rent computing and data-centre infrastructures from other cloud providers. This means that when one cloud infrastructure is affected (unavailable), most probably, other providers will suffer similar losses, hindering the availability of resources to a wilder audience much more possible than with the traditional IT networks.

Second, the possibility that a cloud provider can file for bankruptcy, where the provider goes out of business with consequential financial liability to offset makes the availability of cloud resources a serious issue to consider. Finally, cross-vulnerability in the cloud due to the multi-tenancy implementation of cloud infrastructures and services makes the availability of resources in the cloud an important issue to consider.

In these respects, we recommend that users engage with their cloud providers to understand their disaster recovery processes and procedures, and where possible, make inputs as to how best this can be achieved. For instance, users may be provided backup copies of data on a monthly basis as part of the agreement. This practice can be extremely helpful, for example, in the case of bankruptcy of a cloud provider, or when natural disaster threatens the existence of a data centre. Further, users must be aware of their provider's business continuity plans, for instance, whether the provider has hot-standby sites and whether resilience is built as an abstraction to all layers of its services.

16.3.10 Trust Issues

Trust in both the traditional IT services and cloud computing must be earned. Trust is a major issue with cloud computing irrespective of the cloud model being deployed. Nevertheless, the cloud like traditional IT services can be secured, protected and dependable. It is believed that the cloud offers security advantages.

For example, intruders do not have access to the source code and providers often work hard to provide clean, unbreakable barriers between the customers [17]. However, this requires conscientious effort from both cloud providers and users; in addition, cloud providers must be transparent about their security policies, audit practices, data backup procedures and certification/accreditation. Once users are comfortable with a particular provider's practices, together with the service level agreement (SLA) agreed upon, they are more willing to do business.

Nevertheless, cloud users must be open-minded and must not whole-heartedly trust a provider just because of the written-down service offerings, without carrying out appropriate due diligence on the provider and where certain policies are not explicit, they should ensure that missing policies are included in the service contract. By understanding the different trust boundaries, each cloud computing model assists users when making decision as to which cloud model they can adopt or deploy. For example, with infrastructure cloud computing, a great trust relationship is created because user data backup is possible and applicable, where copies of a user's data are backed up. Similarly, there is a possibility for the user to create and configure additional and customised access controls to protect its data. This level of trust is not possible with software cloud computing, for instance.

16.3.11 Security Policy Issues

Whose security policy governs the cloud, the user or the MCSP? Obviously, the cloud provider's security policy is what stipulates acceptance uses, specifies service level agreements and governs the cloud environment. What if the security policy of the MCSP is not acceptable to a cloud user, because the policy may be missing some policies that the users consider essential towards achieving the security and information assurance requirements for their assets? To ensure that information assets in the cloud are adequately maintained, we recommend that cloud users must:

- Carry out due diligence on the provider
- Appropriately classify the information assets to determine their security, regulatory and compliance requirements
- Consider the viability of each cloud model in relation to their information assets requirements
- Consider return on investment (RoI) of the cloud in relation to the security of the asset

16.3.12 Emerging Threats to Cloud Computing

New and unfamiliar threats to cloud computing are emerging. Examples include cross-virtual machine (VM) exploits, inter-processor exploits and cross-application vulnerability exploits. Although most of these widely publicised attacks to cloud

computing are theoretical [18], it is possible that within the next couple of years, these attacks may be realised. Therefore, precautionary measures must be put in place; mitigation plans and risk treatment plans must exist to address emerging vulnerability exploits and current attacks to cloud computing.

Above all, to appropriately profile cloud computing risks, each cloud service and deployment model must be evaluated against its security requirements (see Fig. 16.4).

16.4 Cloud Security Relationship Framework

Managing security in the cloud is different from managing security in traditional IT systems or networks. The difference is significant from the level of trust of machine data to management of information in the cloud. Cloud computing is a new and emerging technology, and hence, inherent and cumulative risks to cloud computing are new, evolving and unfamiliar. Like any new technology, new and unfamiliar risks exist. Therefore, conscientious effort must be dedicated towards understanding risks that exist, in addition to finding appropriate ways of addressing such risks.

The current stage of the cloud is very immature. A lot of the offerings are geared towards adopters with little to no risk and a lot to gain from low-cost, pay-as-you-go resources [19]. Thus, current cloud computing deployments are not suitable for all use cases. However, like other utility services, such as electricity, cloud computing can be secured. To make the cloud secure, security must be built into every aspect of the cloud starting from its foundation stage.

To understand risks associated with cloud computing, risks that exist with traditional IT must be properly evaluated (as discussed in Section 3), while new and emerging risks to the cloud are investigated on a per cloud service and deployment model basis. To assist with this assessment, a framework is proposed (see Fig. 16.3). A cloud security relationship framework is a framework for assessing cloud computing offerings (cloud service model, cloud deployment model and use cases) on the basis of cost, security and capability. The cloud computing framework comprises three components, *deployment*, *delivery* and *user*. These components are evaluated against three metrics, *cost*, *security* and *capability*.

Cost relates to the amount that users pay to use a particular cloud computing service operating on a specific delivery model in a given deployment. A *cloud delivery model* is a cloud computing service, for instance, SaaS, PaaS and IaaS, where each delivery model provides a set of specific functionalities. A *cloud deployment model* is a cloud computing type that offers a set of unique attributes and coverage, such as private, public, hybrid, community, localised, virtual private and external clouds. There is a considerable number of cloud computing models currently being used and developed. These terminologies are used loosely in many publications today; however, early taxonomies are provided in [20,21].

Security relates to the protection afforded to cloud computing services, such as confidentiality, integrity and availability. It is difficult to quantify security offerings

in the cloud. Thus, instead of using formal (mathematical) metrics as those discussed by Pfleeger [22], we have used metrics (low, medium and high) that are in current use and applicable to many use cases. In this study, low security is when one security requirement (confidentiality, integrity and availability) can be achieved; medium security is when two of the requirements are achievable, while high is when all the three requirements can be achieved.

Capability relates to the variety of offerings available with each cloud computing deployment. There is a direct relationship between cost and security of the cloud deployment models, such as public, community, agency, hybrid and private. This implies that private clouds provide 'pre-requisite' security requirements when compared with hybrid or public clouds. Similarly, the cost implication for the same type of service grows from public to private clouds, while the capability (service-offering capabilities) is directly related to the cloud service type deployed. For example, infrastructure cloud computing (IaaS) offers more capabilities than PaaS or SaaS.

It is pertinent to note that not all cloud computing deployment models (public, private, agency, community and hybrid) raise the same security concerns, or offer the same confidentiality, integrity, availability or privacy of data or information. Certain cloud deployments are most appropriate to certain organisations. For example, government, financial or health institutions are more inclined to hybrid or private clouds than public clouds. Similarly, users transmitting or storing classified information, such as confidential information, should use hybrid or private clouds (see Fig. 16.4), while agencies, such as MOD, CIA or DISA, must use agency or privately operated clouds.

The cloud security framework (see Fig. 16.3) must be used in conjunction with the information assets classification model (see Fig. 16.4) when deciding which information assets need to be mitigated to the cloud.

We have shown that based on security and privacy requirements of information assets (confidentiality, integrity, privacy and impact), some assets are not suitable for the cloud. For example, 'SECRET' and 'TOP SECRET' information assets (information assets #14 and #15) are not suitable for the cloud (see Fig. 16.4).

Similarly, information assets #12 and #13 require minimum agency cloud, but can also use private clouds. Information asset #13, for instance, is classified as 'confidential' and needs high confidentiality, high integrity, high availability and privacy requirements. However, if this asset is to be compromised, then the impact to the organisation will be critical. Therefore, based on the information requirements and impact level of this information asset, agency cloud, at the minimum, is required to host, store and transport this asset.

Information assets #1–#6 can be hosted in a public cloud, and information assets #6–#10 require a community cloud of some sort. For example, a financial community cloud, if the information assets are owned by a financial institution, or a health community cloud, if owned by a medical or health institution.

Note that while information asset #5, for example, may require at the minimum a public cloud, this information asset may well be hosted in a private cloud too. The zoning of information assets to clouds is done based on the minimum security and privacy requirements of that information asset (see Fig. 16.4).

16.4.1 Security Requirements in the Clouds

A private (localised) cloud is a solely owned cloud, operated and used by an enterprise. It may be regulated and governed like other clouds, and most importantly, it is for 'restricted' users only. Private clouds are more secure than public clouds, and therefore, private clouds are most suitable for transmitting classified information, such as confidential and/or proprietary information. Information assets with lesser security requirements, such as personal information may still use a private cloud (see Fig. 16.4). It is pertinent to note that the use of a private cloud offers no guarantee as to the security or privacy of the information assets that it stores or transports. For example, the use of Microsoft Azure on-premise cloud platform does not provide any guarantee to the security and compliance of information that is stored or transported using this cloud. We recommend that organisations seeking to use the cloud for classified information or regulated transactions should use a private cloud, but must do so bearing in mind that the necessary security requirements of that information asset are constantly assessed and reviewed. Furthermore, private clouds come with a prize; for instance, the cost to rent, deploy or operate a private cloud is comparably and considerably higher than a public cloud.

A public cloud is an open cloud maintained by a cloud vendor for the general use of everyone including cybercriminals. A public cloud is most probably the most currently used cloud, such as Salesforce, Amazon EC2 and Amazon web services (see Fig. 16.2, [4]). A public cloud is relatively safe and offers a wide range of capability at reduced cost.

Agency clouds, like private clouds, are perceived to be secure and reliable because they are privately owned by the military or defence agencies. Hence, rigorous and complex security requirements are thought to be applied. Defence agency cloud may require separate legal, regulatory and security compliance measures different from those of public clouds. For example, the DISA cloud is subject to government legislation, while UK government clouds would be subject to CESG information assurance compliance and protective handling.

A community cloud is governed by the regulatory controls of that community,for example, health and financial institutions clouds. Integrated (hybrid) clouds combine a set of requirements from two or more co-joining clouds. These requirements are bound to vary depending on the specific requirements of the co-joining clouds. It is an illusion to think that hybrid clouds provide 'high' security. Each cloud must be assessed in its own right to determine its privacy, security and regulatory policies and practices.

16.5 Conclusion

Cloud computing is an emerging technology that offers unparalleled distributed computing resources at affordable infrastructure and operating costs. The cloud requires conscientious and diligent attention from both users and providers due to the inherent risks associated with its operating paradigm, such as ubiquitous network access, multi-tenancy service delivery, location independence, homogeneity and openness.

In this chapter, cloud computing has been explained. Three of the widely used cloud services, namely, software computing, platform computing and infrastructure computing, and five of the deployment models, namely, private (localised), public, community, agency and hybrid clouds have been discussed.

Cloud computing, like existing utility services such as electricity, water and telephone, can be secure, safe and reliable; however, this can be achieved when security issues that exist with traditional IT services are evaluated in relation to cloud computing. Unfortunately, cloud computing offers varying levels of security and privacy based on the cloud model being deployed.

The proposed cloud security framework to assess cloud offerings provides a systematic assessment of cloud computing services based on cost, capability and security. It has been shown that the three cloud service models offered unique security requirements. Similarly, the capability of the deployment models (public, community, agency, private and hybrid) has been found to be unique and varied.

As organisations use the framework and information classification model proposed in this chapter to evaluate cloud services and information requirement respectively, we recommend that they do so by knowing that not all information assets should be migrated to the cloud.

About the Author

Dr. Cyril Onwubiko is a CLAS Consultant at Cable and Wireless, where he is responsible for providing information assurance to information assets of varying business impact levels (ILs) in accordance with the HMG security policy framework. Cyril is also currently the chair of the Security and Information Assurance Committee, E-Security Group at Research Series.

Prior to C&W, Cyril was an Information Security Consultant at British Telecom (BT), providing strategic information security undertakings. Earlier, Cyril worked at COLT Telecommunications Group for 8 years, participating in several projects, while helping COLT develop their IP VPN service – IP Corporate, a Pan-European IP VPN service for managed customers. Cyril also assisted COLT to roll out their enterprise-MPLS VPN core and was a focal engineer supporting SWIFT. He is experienced in VPN Security, Security Information and Event Management (SIEM), Data Fusion, IDS and Computer Network Security, and knowledgeable in Information Assurance, HMG Security Policy Framework (SPF) and Risk Assessment and Management.

Cyril holds a Ph.D. in Computer Network Security from Kingston University, London, UK, a Masters of Science degree (M.Sc.) in Internet Engineering from the University of East London, London, UK and a Bachelors of Science and Technology degree (B.Sc.), first class honours, in Computer Science and Mathematics from Federal University of Technology, Owerri. He is the author of two books, ‘Security Framework for Attack Detection in Computer Networks’ and ‘Concepts in Numerical Methods’.

References

1. Mell P, Grance T (2009) Draft NIST working definition of cloud computing. http://csrc.nist.gov/groups/SNS/cloud-computing/index.html. Accessed 16 Sept 2009
2. Mell P, Grance T (2009, August 12) Effectively and securely using the cloud computing paradigm, NIST
3. Kaufman LM (2009 July/August) Data security in the world of cloud computing. IEEE Sec Priv 7(4):61–64
4. Greenfield T (2009) Cloud computing in a military context – Beyond the Hype, Defense Information Systems Agency (DISA), DISA Office of the CTO. http://www.govinfosecurity.com/regulations.php?reg_id = 1432. Accessed 20 Sept 2009
5. NBC Federal Cloud Playbook (2009) National business center, Department of the Interior, Washington DC. http://cloud.nbc.gov/PDF/NBC%20Cloud%20White%20Paper%20Final%20(Web%20Res).pdf. Accessed 23 Sept 2009
6. Microsoft Azure Services, http://www.microsoft.com/azure/services.mspx. Accessed 23 Sept 2009
7. Gellman R (2009) Privacy in the clouds: risks to privacy and confidentiality from cloud computing. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf. Accessed 17 Sept 2009
8. Claburn T (2009) Google Apps contract in LA hits security Headwind, http://www.informationweek.com/news/showArticle.jhtml?articleID=218501443. InformationWeek. Accessed 20 July 2009
9. Onwubiko C, Lenaghan A (2009, March) Challenges and complexities of managing information security. Int J Elect Sec Digit Forensic IJESDF 3(2). ISSN (Online): 1751-9128 – ISSN (Print): 1751-911X
10. Safe Harbour (1998) European commission's directive on data privacy and protection legislation, http://www.export.gov/safeharbor/SafeHarborInfo.htm. Accessed 17 Sept 2009
11. Onwubiko C (2008) Security framework for attack detection in computer networks. VDM Verlag, Germany
12. Cloud Security Alliance (2009), http://www.cloudsecurityalliance.org/. Accessed 19 Sept 2009
13. Cloud Computing Interoperability Forum (2009), http://www.cloudforum.org/. Accessed 17 Sept 2009
14. SB-1386, The California Security Breach Information Act (2002) SB1386 amending civil codes 1798.29, 1798.82 and 1798.84. http://en.wikipedia.org/wiki/SB_1386. Accessed 20 Sept 2009
15. Onwubiko C (2009), A security audit framework for security management in the enterprise. Commun Inform Sci 45:9–17, Springer. ISSN 1865-0929 (Print) 1865-0937 (Online)
16. Chaput SR (2009) Compliance and audit, security guidance for critical areas of focus in cloud computing, Cloud Security Alliance
17. Cohen R (2009) Lightning knocks out amazon's compute cloud. Cloud Comput J. http://cloudcomputing.sys-con.com/node/998582. Accessed 11 June 2009
18. Viega J (August 2009) Cloud computing and the common man. IEEE Comput 42(8):106–108
19. Ristenpart T, Tromer E, Shacham H, Savage S (2009) Hay, you, get off of my cloud: exploring information leakage in third-party compute clouds. ACM Computer Communications Security Conference CCS'09, November 2009
20. Cheesbrough P (2008, Dec) Into the cloud, lessons from the early adopters of cloud computing. Information Age
21. Youseff L et al. (2009) Toward a **u**nified **o**ntology of **c**loud **c**omputing. http://www.cs.ucsb.edu/~lyouseff/CCOntology/CloudOntology.pdf Accessed 15 Sept 2009
22. OpenCrowd (2009) The OpenCrowd cloud taxonomy. http://www.opencrowd.com/views/cloud.php. Accessed 26 Sept 2009
23. Pfleeger SL (May/June 2009) Useful cybersecurity metrics. IEE IT Pro J 11(3):38–45