Cloud computing: a review of security issues and solutions

Article *in* International Journal of Cloud Computing · January 2014

DOI: 10.1504/IJCC.2014.064760

1 author:

Tawfiq Alashoor
Copenhagen Business School
24 PUBLICATIONS **165** CITATIONS

SEE PROFILE

Cloud computing: a review of security issues and solutions

Tawfiq Alashoor

School of Business Administration,
The Pennsylvania State University-Capital College,
777 West Harrisburg Pike, Middletown, PA 1707, USA
E-mail: tma178@psu.edu
E-mail: aashoor3@hotmail.com

Abstract: Cloud computing technology is an old concept which has become one of the most widespread technologies in the last few years. It is a pay-per-use service which enables users to perform computing services anytime and anywhere as long as an internet connection is available. There are four major cloud deployment models: public, private, community and hybrid. The cloud's prominence originates from its valuable advantages. However, security issues threatening data confidentiality, integrity, availability and auditing in the cloud might hamper this technology diffusion. Thus, deciding whether or not to move to a cloud service provider, or rely on available IT resources to run a business, is indeed a critical step. This paper presents an overview of cloud computing and describes this technology in detail. It also summarises most of the current security issues menacing the cloud providers and users, and presents and summarises the available countermeasures to the proposed security issues.

Keywords: cloud computing; cloud deployment models; cloud services; cloud review; cloud providers; security issues; confidentiality; integrity; availability; auditing; solutions; countermeasures.

Reference to this paper should be made as follows: Alashoor, T. (2014) 'Cloud computing: a review of security issues and solutions', *Int. J. Cloud Computing*, Vol. 3, No. 3, pp.228–244.

Biographical notes: Tawfiq Alashoor is currently a Graduate Assistant at King Fahd University of Petroleum and Minerals. He received his BS in Management Information System from KFUPM, and he is, at this time, pursuing his Master in Information Systems at the Pennsylvania State University, Capital College. He is a member of HonorSociety.org. His current research interests include cloud computing, big data, database design and social media.

1 Introduction

Cloud computing revolution, as the 5th utility after water, gas, telephony, and electricity, has the potentiality to renovate the nature of information technology (IT) in different aspects. Conceptually, cloud computing affords an innovative approach of computing technology by allowing users to access, share, store, and work on information via the internet (Kalapatapu and Sarkar, 2012).

This new utility has recently attracted a large proportion of businesses due to its affordable benefits. A recent survey conducted by Financial Planning Association, which aimed to assess the use of technology by financial advisers, shows that 28% of advisers use cloud service for all or most of their software. Additionally, 34%, that use in-house IT for their software, are moving toward cloud computing. And 30% of advisers, that use in-house IT for their software, are not planning to move toward cloud computing (Huxford, 2012).

One of the prominent characteristics about utility services is the low-cost. Cloud computing not only offers low rates to business users but also eliminates the need to manage hardware, software, and IT infrastructure (Wang et al., 2011). Advantages of Cloud computing include but are not limited to the list in Table 1 (Kalapatapu and Sarkar, 2012).

Table 1 Cloud computing advantages

Advantage	*Description*
Location independence	The ability to access resources from anyplace at any time, users need only internet access and a browser to use cloud services.
Scalability	The ability to simply fulfil business's growth in terms of infrastructure and software needs.
Flexibility	The ability to promptly provide users with resources and capabilities without human interaction.
Reliability	A dependable technology that provides users ease of access to resources.
Multi-tenancy	The ability to share resources amongst a large number of users.
Space saving	The ability to make extra physical space available due to the fact that cloud computing eliminates the need to acquire and manage IT infrastructure (servers, air conditioning, networking devices, and storage rooms)

Cloud computing diffusion is increasing more and more due to the invaluable advantages the cloud computing grants to businesses. However, deciding whether to move to a cloud service provider (CSP), or rely on available IT resources to run a business, is indeed a critical step. One of the most significant influences that keeps businesses away from using cloud computing is cloud security. Cloud computing security issue is, to date, an ongoing consideration due to businesses' misunderstanding of cloud computing's nature and the opportunity that this technology provides crackers to perform illegal actions. This paper aims to conceptually summarise the different types of cloud security breaches in terms of confidentiality, integrity, availability and to depict auditing difficulties in the cloud. In addition, this paper will summarise and discuss available solutions to the security issues exposed.

2 Cloud computing overview

"Cloud computing is really old wine in a new bottle", according to Professor Laplante (2012, p.12), from the Pennsylvania State University. He also states that nothing is new about Cloud computing by referring to John McCarthy's utility computing notion which was presented in 1961. In addition, Rose (2011) says that cloud computing is a merging of available technologies and it is not a new invention. In contrast, others consider cloud computing as a new term (Kerr and Teng, 2012; Wang et al., 2011; Zissis and Lekkas, 2012). It is clear that there is no consensus amongst IT professionals about the emergence of cloud computing, and the fact that cloud computing is a utility might be a critical point in this debate.

In the 1990s, cloud computing existed to support e-business services such as e-commerce, internet-based supply chain, web-based app design, internal protocols and technology-centric design. Then, the second generation of cloud computing started to include IT as a service which is considered as internet services consumption. This current generation provides low cost IT, highly virtualised infrastructure, cloud-based platforms, and service-centric design. These days, cloud computing, via the centralised resources, possesses and exceeds the capability of high-performance supercomputers. Further, when this technology is obtainable in an on-demand basis, it is definitely a worthy technique for individuals, businesses, organisations, and governments to perform computing processes smoothly and less-costly. By 2020, it is highly expected that users will depend on cloud computing services to access software application and to share and acquire information. In other words, cloud computing will replace the desktop in future. A survey with a highly diverse population conducted by Pew Internet and American Life Project supports these predictions; 71% of the survey takers believe that by 2020 people will no longer use applications running on personal computers. However, they will use online-based applications such as Google Docs and smart phone applications (Kalapatapu and Sarkar, 2012). Other experts expect that cloud computing will embrace about 90% of the world's computing and data storage processes within five to ten years (Nicolaou et al., 2012).

Cloud computing is basically connected to many areas of our lives in today's technologies, such as e-business, search engines, operating systems, global positioning systems (GPS), and more (Kalapatapu and Sarkar, 2012). According to Rose (2011), others believe that by the widespread acceptance of netbooks, small portable devices, and low power notebook computers, consumers' level of accepting cloud computing has been proven.

Cloud computing is enabled by virtualisation technology which has empowered mainframe systems since 1967. Virtualisation has also been the apparent point that distinguishes cloud computing from grid computing and supports cloud computing's independence of location merit (Zissis and Lekkas, 2012).

Recent studies have shown that a traditional stand-alone IT system usage rate fluctuates from five per cent to 20% (Nicolaou et al., 2012), which only proves the truth and rationality of John McCarthy's statement in 1960 that "computation may someday be organised as a public utility" [Kalapatapu and Sarkar, (2012), p.5]. Cloud computing definitely increases the rate of IT facility utilisation and may maximise that rate, because it employs the pay-per-use or pay-as-you-go basis.

Apparently, due to the advantages which cloud computing promises businesses, the number of organisations shifting toward the cloud is rapidly rising. Gartner, Inc. had

expected that worldwide cloud services sales will increase 16% from 2009 to 2010 and its revenue will double in 2014 internationally (Srinivasan, 2012). However, others suggest that organisations start with available computation services in the internet to estimate how the cloud may fulfil their business needs before rushing entirely to the cloud (Wang et al., 2011).

Researchers claim that the benefits of cloud computing play a major role in growing cloud computing's popularity at a rapid pace. However, the more the demand increases, the more the security issues rise (Jamil and Zaki, 2011). According to Rose (2011), internet capacity has to be leveraged as a result of the increase of cloud users as well. Rose also considers that the shift from service-oriented architecture (SOA) to cloud makes the governance more challenging to determine the best practices to be used to overcome security issues such as data loss and integrity compliance, liability, reliability, and authentication.

The research areas in cloud computing are still in their early period. Further, there are few numbers of studies with respect to the reliability of cloud, social issues in cloud computing, and privacy, security, and trust issues in cloud computing that need to be studied and investigated (Wang et al., 2011). Security of virtualisation, which is the core technology of cloud computing, has not yet been investigated fairly enough and there is not much known about it (Tsai et al., 2012).

3 Cloud computing definition

Rose (2011) believes that a unique definition for cloud computing is still obscure because of the different models and categories provided by the cloud service. In Beijing, the 2008 IEEE International Conference on Web Services (ICWS) discussed the definition of cloud computing and agreed that cloud computing definition is closely dependent and correlated to the type of users. Cloud computing for applications and IT users is IT as a service, which includes online-based computing processes, data storage, and applications. For internet application developers, it is online development platform and runtime environment software. Also, it is the enormous disseminated data centre infrastructure that is connected by IP networks for infrastructure providers and administrators.

According to the National Institute of Standards and Technology (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" [Kalapatapu and Sarkar, (2012), p.3]. Generally speaking, cloud computing technology is a computing service that is delivered in the same way other utility services are delivered, such as electricity, water, or phone service; the user has to pay per use. Cloud computing is also an online-based service which means that without internet connection this technology is totally out of service. Practically, CSPs such as Amazon, Google, and Microsoft deliver this service by using server farms to enable users to access and share information or using software over the internet anytime anywhere. In other words, cloud computing is based on SOA and virtualisation. According to Qaisar and Khawaja (2012), cloud computing became popular in 2007 after the partnership between IBM and Google followed by the arrival of Amazon Elastic Compute Cloud (EC2).

4 Cloud computing deployment models

The way a cloud is designed to provide a specific service is referred to as cloud deployment. Basically, it depends on the user specification; a deployment model may embrace diversified attributes such as security and independency. As displayed in Figure 1, there are four main cloud architecture deployment models:

- Public cloud: a traditional deployment model of cloud service that serves the general public or organisations and contains more than one subscriber in a cloud, e.g., Amazon's Web Services, Google AppEngine, and salesforce.com. In this type of cloud deployment technique, providers share resources with users on pay-per-use (utility) basis. Some of the pros in this type, which is highly viable for small businesses, include easy resource management, scalability, and flexibility. However, the public cloud offers less visibility and control over the computing infrastructure for its users due to the shared infrastructure amongst subscribers.

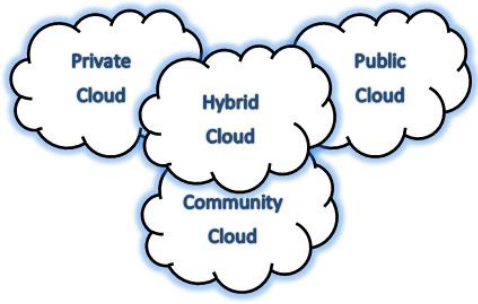
- Private cloud: a cloud service in which the computing infrastructure is dedicated only to a specific organisation or business. This type of cloud computing is considered more secure and expensive than the public cloud due to the independence property of the cloud infrastructure, e.g., Windows Azure.

  Private clouds are categorised based on their location and access level. On-premise clouds refer to private clouds that are hosted and maintained by a particular organisation, for example, clouds for military are most likely of this type because of the considerable amount of confidential data. Externally hosted clouds are private clouds dedicated to a particular organisation by a third party that hosts and maintains the cloud infrastructure, e.g., Vmware and Amazon.

- Community cloud: a cloud similar to the public cloud but there are specific restrictions of sharing different resources amongst the cloud users or businesses, e.g., Google's GovCloud. In this type, the computing resources are shared amongst organisations that share similar activities or businesses. In other words, the community clouds are classified based on the nature of business.

- Hybrid cloud: a combination of public, private, or community cloud services, e.g., Amazon virtual private cloud. In this cloud model of deployment, the positive attributes of remaining models are integrated together in this model depending on the user's requirements. Hybrid cloud is currently the leading model amongst other deployment models (Kalapatapu and Sarkar, 2012).

Figure 1 Cloud deployment models (see online version for colours)



5 Cloud computing services

Cloud computing services are the several products that CSPs deliver to their users. Generally, there are three major services that include software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS).

- SaaS: this service allows consumers to access and use software applications hosted by the cloud vendor on a pay-per-use basis using a thin client interface. This service is not necessarily implemented in the form of web-based applications; however, it is sometimes delivered through non-remote applications with internet-based storage or other network connections. In general, people using internet have already been exposed to dealing with SaaS in different manners such as using Google's Gmail, Microsoft's Hotmail, Google's docs, or Apple's iCloud, although, Salesforce.com has been the leader in this area with its customer relationship management (CRM) space.
- IaaS: this service virtually provides consumers with hardware related services such as servers, storages, and networks. IaaS eliminates the operation of keeping IT infrastructure up-to-date by allowing organisations to easily and quickly update current operating systems or build new versions of applications on a pay-per-use basis. Accordingly, organisations save vast amount of budget dedicated for purchasing and configuring new hardware or software facilities. Amazon, Rackspace, GoGrid, AT&T, and IBM are the major companies providing IaaS.
- PaaS: this service provides consumers with facilities related to application design, application development, testing, hosting, and several application services like database integration, security, scalability, team collaboration, storage, and developer community facilitation. These services can also be delivered in one package over the internet on a pay-per-use basis to provide higher-level software infrastructure to develop particular applications. Companies that provide this service include Google, Microsoft, and Salesforce.

Table 2 Cloud service providers

Cloud computing service	*Cloud provider*	*Product example*
SaaS	Amazon	Amazon SES
	Google	Google Docs
	IBM	SmartCloud Solutions
	Microsoft	Microsoft Hotmail
	Rackspace	Rackspace E-mail
	Salesforce	Sales Cloud
IaaS	Amazon	Amazon S3
	Google	Google Cloud Storage
	IBM	SmartCloud Enterprise+
	Microsoft	Azure Storage
	Rackspace	Rackspace Cloud Files
PaaS	Amazon	Amazon SQS
	Google	Google AppEngine
	IBM	SmartCloud Application Services
	Microsoft	Azure SQL Database
	Rackspace	Cloud Sites
	Salesforce	Heroku

However, some providers categorise their services more precisely which are as follows: hardware as a service (HaaS), development, database, or desktop as a service (DaaS), business as a service (BaaS), framework as a service (FaaS), organisation as a service (OaaS), security as a service (SeaaS), etc. (Kalapatapu and Sarkar, 2012). Table 2 lists some major CSPs and a product of each as an example.

6 Security issues with cloud computing

As the centralisation model is used to implement cloud computing technology, it is claimed that cloud computing providers most often implement advanced security technologies due to the benefits imposed, such as centralisation of security, data and process segmentation, redundancy, and high availability. As a result, providers devote all their security resources to secure the cloud architecture (Zissis and Lekkas, 2012). In contrast, a recent survey shows that security and privacy issues are major concerns for people to move towards the cloud, since data storage and processes take place in a centralised location (data centres) which is not necessarily known by users (Che Fauzi et al., 2012). Some researchers claim that cloud computing's security and privacy issues are the main obstacles to move forward with the cloud services (Hamouda and Glauert, 2012). With respect to the centralisation model and the predictions of cloud computing technology boost, security issues will certainly play a major role in slowing this technology diffusion.

Cloud computing means the transformation of IT's responsibilities from managing infrastructure, software, and hardware to dealing with information by ensuring

connectivity with the cloud and evaluating CSPs (Cunningham, 2010). In addition, security is a significant concern for organisations because of the indistinct transparency level of the cloud security by many CSPs (Srinivasan, 2012). Organisations that consider transferring their IT services into the cloud are not confident about several areas in the cloud and some of these areas are not expected to be illuminated by the provider. From consumer perspectives, the ambiguity of security in the cloud falls under one or more of the following aspects:

- Location of data stored: consumers will not be comfortable if they have no knowledge about their data location, particularly if data confidentiality is very high. Moreover, some providers set up their data centres in different countries in which data privacy laws might not truly be employed or even exist.
- Protection level: consumers are also concerned about the level of protection conducted in the cloud in the process of data transmission and deletion.
- Multi-tiered service: providers sometimes use different vendors' services to deliver computing services which exacerbates the level of security concern for consumers due to a multi-tiered service in which security policy and data distribution variations exist amongst vendors.
- Sharing the cloud: for instance the public cloud serves more than one subscriber which makes consumers suspicious about their data privacy. Rose (2011, p.61) describes the threat of sharing data in a network serving many users as 'the tragedy of the commons'.
- Applications programming interfaces (API): the security level of applications used among applications for interoperability, such as tokens and cookies, is considered by the consumer side as well (Zissis and Lekkas, 2012).
- Data breach activities: consumers might be more anxious about the impact of any data breach or hacking act to the cloud, because the consequences could be massive compared to a singular physical server over which consumers have more control.
- Level of control: in most cases, consumers have low levels of control on the cloud.

It is the provider's ethical responsibility to deliver secure cloud service to consumers, and it is also necessary in order to elevate the cloud computing industry; because if consumers are not confident with the security level provided, the cloud computing growth will be decelerated (Miller, 2010). The whole story is, in fact, subjected to the consumer's trust level with the provider after negotiating the service level agreement and declaring security attributes, governance level, and every vague aspect regarding the cloud service. In the next section, cloud computing security issues will be categorised depending on four broad concepts which are confidentiality, integrity, availability and auditing.

6.1 Confidentiality

Confidentiality is the process of allowing privileged entities only to have access to information, which means preventing intentional or unintentional unauthorised disclosure of information (Hamouda and Glauert, 2012). Confidentiality risks increase in the cloud

due to several attributes that facilitate action of unauthorised entities. The threating to compromise data results from some of the security aspects discussed above. This section presents eight factors by which data confidentiality security becomes vulnerable.

First is the multi-tenancy characteristic of cloud computing, which permits resource sharing among several parties. Second, according to Tsai et al. (2012), is the non-existence of physical isolation amongst multiple users in a single infrastructure, which may affect confidentiality by opening the chance for some users to view another user's memory status or resource use. Third, data residual, which is the remaining representation of data after deletion, may lead to unintentional private data disclosure due to virtual separation of logical drives and absence of hardware separation amongst users (Zissis and Lekkas, 2012). Fourth, application security, which is as important as data confidentiality, is the software level of security delivered to users. In practice, users put their trust on the provided application by the CSP and they expect secure interaction between users and applications. However, lack of security and vulnerability in software will lead to confidentiality and privacy breaches (Zissis and Lekkas, 2012). Fifth, weak data segmentation, which is correlated to the multi-tenancy attribute and how data crosses logical or physical boundaries in the Cloud, way allow savvy attackers to exploit data confidentiality (Wheatman, 2012). Sixth, user authentication and intellectual property of resources are also exposed to being violated in the cloud. As a consequence of the immunity gap in the cloud against software piracy, an unauthorised individual or enterprise may gain access to resources and, moreover, they may be able to permit others to access and use resources without being detected by the owner of the cloud and its subscribers (Business Software Alliance, 2012). Seventh, data location and internationality of data centres, which are highly ambiguous to consumers, put data confidentiality in vague situations particularly if data centres are located in countries in which IT laws differ. Eighth, traffic analysis, which means analysing data, users, speed, capacity or operability in the cloud, is subjected to breaching data confidentiality by enabling new parties that might not necessarily be identified in the service level agreement to access information.

Table 3 Confidentiality attack types

Attack	*Definition*
Man in the middle	An attacker who impersonates a user's character in an independent connection, where secure socket layer (SSL) is not properly configured, to control the session and to gain some information.
Network sniffer	An attacker who can possess confidential data such as passwords by decoding weakly encrypted or unencrypted data.
Port scanner	An attacker who searches and uses open ports such as Port 80 for the purpose of disclosing data.
SQL injector	An attacker who uses special characters to manipulate SQL or website source code through existing vulnerabilities to return data.
Cross site scripter	An attacker who redirects the user to impersonated website with the unconsciousness of the user through XSS vulnerabilities to possess user's credentials.
Unsecure browser sniffer	An attacker who intermediate an SSL connection to install sniffing packages to intercept user's credentials.

There are different types of attacks that can compromise data confidentiality in the cloud. Table 3 explains six types of attack that might take place in the cloud if networks are not neatly safeguarded. Tsai et al. (2012) state that data confidentiality compromise exists in SaaS when access to software or stored data is unauthorised, in PaaS when the status of resource use is unprotected, and in IaaS when the resources amongst the multiple users are not tightly isolated.

6.2 Integrity

Integrity is a fundamental aspect of IT where only authorised users can change, modify, copy, or delete data. In the cloud, integrity becomes a more critical issue. According to Tsai et al. (2012), if an integrity breach happened in Paas and IaaS by malicious modification to some setting or files in the platform or configuration, an action will not only impact PaaS and IaaS but also will affect all services deployed through them such as SaaS. As a result, a business operating under the cloud will be extremely influenced by this malicious action and experience tremendous loss.

Integrity in the cloud must meet three principles. First, changes and modifications to data must not be done by unauthorised individuals or processes. Second, unauthorised changes and modifications must not be done by authorised individuals or processes. Third, internal data in the cloud and external data used by the cloud user must be consistent (Hamouda and Glauert, 2012).

Unfortunately, several CSPs depend on the regular method of authentication, which is user name and password, and are not able to provide a robust protection mechanism (Cunningham, 2010). Moreover, in terms of integrity, a study conducted by Queen Mary University, which included Amazon, Microsoft 365, and Apple, examined cloud service terms and conditions. Researchers found that CSPs have the power to redeem themselves from any clutter that goes with the cloud (Neroth, n.d.). That is the real threat of integrity issues in the cloud when SLA is not transparent, in which the cloud user may not have the power to claim CSP regarding intentional or unintentional malicious acts. Likewise, the eight factors discussed in the previous section that affect data confidentiality are also impacting data integrity in the cloud.

In addition, CSPs should maintain and ensure users about the following integrity factors. First, software integrity, which refers to protecting applications from unauthorised change, modification, deletion, or theft, must be firmly handled by the CSP. Further, hardware and network integrity is another CSP duty to handle, and to protect hardware from robbery, alteration, and fabrication (Zissis and Lekkas, 2012). Third, the level of supervision of highly privileged users is important to both consumers and CSPs. Consumers, in most cases are not able to, but strive to know what highly privileged administrators are capable of with their data. However, CSPs direct and monitor their administrators for their own needs which might not be consistent with their customers' needs and this could result in insufficient data protection (Wheatman, 2012). Fourth, the legitimate way used in data protection and transformation; the way data is protected from unauthorised modification, deletion or fabrication.

In addition to the attacks presented in Table 3, Qaisar and Khawaja (2012) consider XML signature element wrapping as another attack that is capable of breaching data integrity in the cloud. Such attacker is able to break the signature algorithm and to

manipulate the Simple Object Access Protocol (SOAP) messages by inserting a malicious code without being detected.

In effect, data integrity contraventions are implicitly data confidentiality compromised. In other words, when an attacker is able to spitefully modify, change or delete data, he/she in most cases might be able to view those resources. Similarly, when an unauthorised user is able to change unprivileged resources, this user most likely has already broken data confidentiality notion.

6.3 Availability

Availability of data is one of the most crucial security issues in cloud computing due to its influential effect on cloud-based businesses operations. For instance, when the cloud server is not able to provide data on time to its business user, that business in that moment is totally out of service and is not eligible to operate properly. According to Rose (2011), when companies move toward cloud computing services, they must be conscious they will lose governing security of their data and also they might find themselves unable to access or view data due to intentional or unintentional disruption to the cloud server.

Availability concept in the cloud means ensuring functionality, reliability, security and timely access of data when demanded by the cloud's authorised users (Hamouda and Glauert, 2012). In addition, it refers to the availability of software and hardware to authorised users upon demand (Zissis and Lekkas, 2012). According to Tsai et al. (2012), spoofing, penetrating, or suspending the cloud server may jeopardise data availability in the cloud. However, CSPs must have the ability to provide users with data, software, and hardware upon demand even in the situation of a security breach (Zissis and Lekkas, 2012). Table 4 describes attack types that threaten availability in the cloud.

Table 4 Availability attack types

Attack	*Definition*
Denial of service (DOS)	An attack which stops, delays, or denies web services by sending thousands of requests to the server; which results in dis-functionality of that server.
Domain name system	An attack which changes and redirects requested IP address to another destiny.
Malware injection	An attack which spitefully embeds malicious pieces such as viruses or destructive applications after compromising the file transfer protocol aiming the user to open such harmful application.
Flooding	Another DOS attack that overflows a network or a server with thousands of non-sense requests which malfunctions the service provided.

In addition to the attacks, cloud users should pay attention and understand the agreement of incidents such as lock ins, cloud maintenance and data loss. According to Qaisar and Khawaja (2012), lock ins mean that once cloud user transfers data, applications and services to the cloud server, the possibility to turn back into in-house IT or to migrate to another provider will be difficult. Currently, there are no guaranteed tools, procedures, and standards that could undertake data, application, and service. Then, the actual noteworthy threat of lock ins occurs when a CSP goes out of business which might result in data loss or when a CSP raises up the service cost in which the cloud user has low

bargaining power. Another issue is when the cloud provider wants to perform maintenance to the cloud infrastructure; a CSP should carefully manage maintenance alerts. Especially for sensitive applications that affect global businesses, so that businesses become informed of possible service outages.

Despite all discussed attacks and issues putting data availability at risk, a cloud service user should realise that internet service provider (ISP) or technology used to connect to the internet affects data availability. For instance, if an ISP is encountering difficulties providing internet connection, data availability in the cloud is compromised due to an ISP service outage not the CSP. After all, due to the broad access network required to run a cloud, many security breach intentions become appealing to vicious attackers. "The converse of confidentiality, integrity, and availability is disclosure, alteration, and removal" [Hamouda and Glauert, (2012), p.394].

6.4 Auditing

Auditing refers to collecting and assessing evidence to decide whether an information system (the cloud) preserves assets, ensures data integrity, and fulfils client business goals effectively and efficiently (Sinclair, 2010). Organisations apply two main methods to control operational assurance: system audits and monitoring. System audits are executed one at a time to assess security. Monitoring, however, is a progressive evaluating of either the system or the users (Hamouda and Glauert, 2012).

Implementing cloud-based systems leads to several significant risks with respect to the unique advantages of cloud computing technology. This practice impacts the effectiveness of internal controls and may also affect the nature of the external auditor's job due to several current unmeasured security risks in the cloud. For auditors to properly audit a cloud computing installation and to accurately perform their auditing job, it is essential for them to grasp cloud computing technology. In addition, auditors encounter technical difficulties auditing and controlling a company based on the cloud as they might not have the authorisation to access data and systems in the cloud at all times (Nicolaou et al., 2012).

In terms of auditing in the cloud, a survey conducted by PrincewaterhouseCoopers using 7,200 IT executives showed 22% of them had insufficiency in training and IT auditing; 10% had vague knowledge regarding auditing the provider; and 14% were uncertain about how to acquire privileged access control at the provider site (Cunningham, 2010). Unfortunately, cloud audit requirements have not yet been defined by professional organisations such as AICPA, CICA, and ISACA which makes the auditing process difficult to auditors (Nicolaou et al., 2012). There is no blueprint to follow while assessing cloud-based companies; hence, the control and audit issues in the cloud have to be investigated to streamline internal and external auditing processes to guarantee the accuracy of the cloud auditing.

7 Solutions

Cloud computing will no-doubt leverage an organisation's productivity, cut costs, and increase profits. However, before planning to move toward this technology, organisations should rationally estimate, rate, and speculate on the downsides which mainly swivel

around security breaches. Making matters worse, there are still several enterprises that do not technically understand cloud computing and the way the cloud works. This section presents countermeasures that can be implemented to tackle security breaches in the cloud.

Traditional static security solutions such as antivirus, firewalls, or passwords do not last permanently in encountering savvy malicious attackers. According to a study in 2011, 59% of the survey takers admit that employees do not follow security standards such as passwords and key locks (Jaeger, 2012). The same study also showed that 51% of the companies encountered data loss due to employees' insecure mobile devices and 59% believe that the escalating in malware infections resulted from the same reason, "It's clear that employees are deliberately disabling security controls, which is a serious concern" said Larry Ponemon (Jaeger, 2012). Interestingly, Ponemon Institute published a study which revealed that 69% of CSPs believe that it is the customers' responsibility to secure the cloud not the provider's (Winterberg, 2012). Hence, not only providers but also cloud client organisations must be fortified with more advanced solutions to encounter intentional or accidental security threats in the cloud.

Secure sockets layer (SSL) and HTTPS connections should always be implemented whenever possible for web-based tools, said Brad Burgess (Winterberg, 2012). There are several practices that assist in measuring and elaborating the level of security in the cloud including: historical security records, open source cloud, ideal service level agreement, Trusted Third Party (TTP), effective firewalls, mystery shoppers, and information security standards. The founder of Right Size Solution, Wes Stillman requires CSPs to identify security measures and provide historical records about security incidents. In addition, he recommends that planners request vulnerability testing history from service providers before using the cloud (Winterberg, 2012). This practice is rationally what every organisation should keep an eye on after deciding to transfer to the cloud but before implementation, planning and analysing stage.

Open source software users suggest developing open source cloud computing standards to benefit general users and the open source community. Yet, there are many clouds which were developed using open source standards, e.g., AppScale, cloud Foundry, Eucalyptus, and Open Stack (Wang et al., 2011). Open source clouds might be more secured than regular clouds. Similarly to how open source are more secure than non-open source operating systems due to the collaboration and combination of different developers and expertise from the entire world. However, this notion might not be as satisfactory to general users as to business organisations.

Different cloud clients have different security procedures. One way to measure security in the cloud is to use maturity models such as COBIT, SSE-CMM or CERT/CSO security capability assessment model. However, these models need to be customised to fit in with the cloud user organisation. Another suggested model to ensure and assess security in the cloud is a customised ISO/IEC 27002 framework which investigates several aspects of the cloud security. International Organisation for Standardisation/International ElectroTechnical Commission 27002 is an updated version of ISO 17799 which provides a thorough security framework. Cloud user organisations can apply ISO/IEC 27002 framework which investigates three categories: organisational infrastructure, information protection, and technical infrastructure to sharpen and start up an ideal SLA. This framework tests and ensures each of the following areas: organisation security, asset classification and control, information security policy, access control,

systems development and maintenance, communication and operations management, physical and environmental security, human resources security, business continuity management, compliance, and risk management (Srinivasan, 2012). In general, this framework encompasses every security incident associated with the cloud, thus, it is a well-organised strategy to assist organisations in ensuring the subtlety of the service level agreement defined by the cloud provider. ISO/IEC 27002 framework can also be implemented as a benchmarking blueprint to evaluate different CSPs.

To protect data from being compromised in terms of confidentiality, availability, or integrity, Zissis and Lekkas (2012) claim that hiring a Trusted Third Party in the cloud is a powerful strategy in this case. TTP is an entity that secures the connection between the client and the CSP who both trust the TTP. This added party, which has been underwritten and provided by technical, legal, financial, and structural means, to the infrastructure of cloud technology operates as cloud federations. It tests all critical communications between the parties based on created fraudulent digital contents. This third party works on trusted chains through called certificate paths, in order to deliver a web of trust establishing the methodology of a public key infrastructure (PKI). The former consequently results in strong authentication and authorisation, robust protection of data confidentiality and integrity, and non-repudiation (Zissis and Lekkas, 2012).

The need for more effective firewalls that can track data entering and leaving an organisation's network is, therefore, essential in the cloud to protect data from spiteful attacks (Jaeger, 2012). The firewall can be configured in groups to allow several classes of requests to have different rules such as web server group open port 80 (HTTP) and port 443 (HTTPS), application server group open port 8000 (application specific) to the web server group, and database group open port 3306 (MySQL) to the application group. In addition, an extra layer of security in this scheme is enriched by involving client's X.509 certificate and key to authorise changes in the firewall (Jamil and Zaki, 2011).

The notion of the mystery shopper implemented in any market by exposing dummy, trained, cooperative, confused or belligerent customers to investigate inconsistences in an organisation can be similarly applied in the cloud to inspect the cloud performance and to detect malware. Furthermore, cloud seeding act, which is another form of mystery shopping that intentionally puts malware into the cloud to observe its reaction, should be added to this practice to elaborate the results of the regular mystery shopper (Laplante, 2012).

There are several criteria to measure compliance with the service level agreement and information security standards; an organisation should decide which standard best fits its needs. These standards are the Sarbanes-Oxley Act of 2002, Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, ISO/IEC 27001, Internal Control from COSO, and ITIL (Cunningham, 2010).

Technically speaking, CSPs should ensure their cloud security by implementing the following: certification and encryption, strong authentication, private IP isolation, anti-virus software on every device, firewalls at every point, and safe internet skills awareness programmes for users (Hamouda and Glauert, 2012). Table 5 summarises the possible threats jeopardising data confidentiality, integrity, and availability and provides a key-solution for every threat.

Table 5 Threats and key-solutions for the cloud's data confidentiality, integrity, and availability

Threat	*Countermeasure*
Man in the middle	Certified SSL encryption
Network sniffing	Certified encryption methods
Port scanning	Firewalls and encryption methods
SQL injection	Implementing SQL filters, appropriate SQL privileges, the deletion of unneeded SQL procedures, and the restriction of integer numeric only (CRN Test Center, 2007)
Cross site scripting	Filters and cookies security methods Implementation
Unsecure browser	Implementing WS-security
XML signature wrapping	Implementing Xpath
Denial of service	Limiting privileges
Domain name system	Cryptographic signatures
Malware injection	Authenticity of received messages
Flooding	Using intrusion detection system
Lock ins	Well defined and discussed in the SLA

With respect to auditing obstacles in the cloud, organisations can use Statement on Standards for Attestation Engagement (SSAE 16) framework which is an updated version of SAS70. Statement on Auditing Standards (SAS 70) framework has been defined by AICPA that specified the requirements to audit outsourced operations. SSAE 16 aims to replace SAS 70 by providing a more in-depth range of options in the auditing process. After all, a broader framework for service organisations control (SOC) reports has been issued by the new SSAE 16 standard. SOC 1 report is created by assessing the controls followed by CSP that may affect the client's financial reports after engaging an independent auditor with the cloud provider. SOC 2 and SOC 3 provide assurance regarding security, confidentiality, integrity, availability, and privacy. Generally, SOC 2 reports expose more in-detail about the finding regarding the processing and controls at CSP's installations while SOC 3 reports are meant to be for broad use and public consumption (Nicolaou et al., 2012).

An external auditor should also assess the SLA between the client and the cloud provider to estimate the level of testing, monitoring, or controlling they are permitted to conduct. These assessments at least will lessen the difficulties auditors perform for cloud-based organisations (Nicolaou et al., 2012). Currently, there are some institutes that conduct courses in auditing the cloud such as The Institute of Internal Auditors, Lancelot Institute, MIS Training Institute, and Firebrand Training; the purpose of such courses is to assist auditors assessing agreement compliance, risks associated with cloud-based organisations, and best practices for auditing cloud-based organisations.

8 Conclusions

The advantages brought by the security in the cloud might sound bizarre but they are indeed true. In spite of the subjected security threats when moving IT infrastructure from in-house to the cloud, the cloud security presents a number of benefits to its clients.

These benefits include fault tolerance and reliability, low-cost tragedy recovery, hypervisor or centralised protection against system attacks, data partitioning and replication, and enhanced resilience. On the other hand, the obligatory trust of the cloud provider's security model, the governance loss of physical control, the governance loss of investigating proprietary implementations, and the inadequate extent for monitoring and auditing are considered cons brought by the cloud security (Hamouda and Glauert, 2012).

To conclude, cloud computing service, which provides worthy benefits on a pay-per-use basis, will propagate rapidly and definitely change the way organisations perform their jobs. Therefore, organisations should be well-informed about cloud computing technology before shifting toward it. Most importantly, they should assess and ensure the wholeness of the service level agreement with the CSP in order to avoid any incident that might lead the business to a tragedy. As a result of the high diffusion rate of the cloud computing service, CSPs must afford a high level of security to protect clients' data from confidentiality, integrity, availability, and auditing contraventions by implementing strong cryptographic technologies. In addition, they should unceasingly convoy new security threats to be prepared to encounter any breach because attackers never stop their malicious acts which lead to the vulnerability and invalidity of the current available solutions.

Acknowledgements

The author wishes to thank Professor Rhoda Joseph for her appreciated support and help and her valuable advices in finalising this paper. The author would also like to thank Susan Newell for her effort in revising this manuscript. The author would also like to thank the anonymous reviewers.

References

Business Software Alliance (2012) 'Cloud computing policy agenda for Europe' [online] http://www.bsa.org/country/~/media/files/policy/engb/bsaeuCloudagenda.ashx (accessed 1 November 2012).

Che Fauzi, A.A., Noraziah, A., Herawan, T. and Mohd Zin, N. (2012) 'On cloud computing security issues', in Pan, J.S. et al. (Eds.): *Intelligent Information and Database Systems*, pp.560–569 [online] http://dx.doi.org/10.1007/978-3-642-28490-8_58 (accessed 27 September 2012).

CRN Test Center (2012) '4 tips for stopping SQL injection attacks' [online] http://www.crn.com/news/security/index.htm (accessed 5 November 2012).

Cunningham, P. (2010) 'IT's responsibility for security, compliance in the cloud', *Information Management Journal*, Vol. 44, No. 5, pp.HT6–HT10.

Hamouda, S.K. and Glauert, J. (2012) 'Security, privacy and trust management issues for cloud computing', in Wang, L. et al. (Eds.): *Cloud Computing Methodology, Systems, and Applications*, pp.389–421, CRC Press, Boca Raton.

Huxford Jr., D.C. (2012) '6 steps for transitioning to the cloud', *Journal of Financial Planning*, Vol. 25, No. 3, pp.30–32.

Jaeger, J. (2012) 'Improving data security for cloud computing', *Compliance Week*, Vol. 9, No. 100, pp.47–60.

Jamil, D. and Zaki, H. (2011) 'Cloud computing security', *International Journal of Engineering Science and Technology*, Vol. 3, No. 4, pp.3478–3483.

Kalapatapu, A. and Sarkar, M. (2012) 'Cloud computing: an overview', in Wang, L. et al. (Eds.): *Cloud Computing Methodology, Systems, and Applications*, pp.3–29, CRC Press, Boca Raton.

Kerr, J. and Teng, K. (2012) 'Cloud computing: legal and privacy issues', *Journal of Legal Issues and Cases in Business*, Vol. 1, pp.1–11.

Laplante, P.A. (2012) 'Econ 101 for cloud enthusiasts', *IT Professional Magazine*, Vol. 14, No. 1, pp.12–15.

Miller, K.W. (2010) 'Ethical analysis in the cloud', *IT Professional Magazine*, Vol. 12, No. 6, pp.7–9.

Neroth, P. (n.d.) 'Euro legislation cloud threaten security of cloud data', *IEEE Xplore*, Vol. 15 [online] http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06156540 (accessed 1 November 2012).

Nicolaou, C.A., Nicolaou, A.I. and Nicolaou, G.D. (2012) 'Auditing in the cloud: challenges and opportunities', *The CPA Journal*, Vol. 82, No. 1, pp.66–70.

Qaisar, S. and Khawaja, K.F. (2012) 'Cloud computing: network/security threats and countermeasures', *Interdisciplinary Journal of Contemporary Research in Business*, Vol. 3, No. 9, pp.1323–1329.

Rose, C. (2011) 'A break in the cloud? The reality of cloud computing', *International Journal of Management and Information Systems*, Vol. 15, No. 4, pp.59–63.

Sinclair, J. (2010) 'Auditing in cloud computing' [online] http://www.slideshare.net/jonathansinclair86/Cloud-auditing (accessed 5 November 2012).

Srinivasan, M. (2012) 'Building a secure enterprise model for cloud computing environment', *Academy of Information and Management Sciences Journal*, Vol. 15, No. 1, pp.127–133.

Tsai, H., Siebenhaar, M., Miede, A., Huang, Y. and Steinmetz, R. (2012) 'Threat as a service? Virtualization's impact on cloud security', *IT Professional Magazine*, Vol. 14, No. 1, pp.32–37.

Wang, W.Y.C., Rashid, A. and Chuang, H. (2011) 'Toward the trend of cloud computing', *Journal of Electronic Commerce Research*, Vol. 12, No. 4, pp.238–242.

Wheatman, J. (2012) 'Data security monitoring in the cloud: challenges and solutions', 23 April, (ID: G00232645)], Gartner, Inc. (ccessed 27 September 2012).

Winterberg, B. (2012) 'How to stay safe when using the cloud', *Journal of Financial Planning*, Vol. 25, No. 7, pp.24–26.

Zissis, D. and Lekkas, D. (2012) 'Addressing cloud computing security issues', *Future Generation Computer Systems*, Vol. 28, No. 3, pp.583–592.