Cybersecurity threats in cloud computing

Julian Jang-Jaccard
CSIRO Computational Informatics (CCI)

Surya Nepal
CSIRO Computational Informatics (CCI)

Y Jay Guo
CSIRO Computational Informatics (CCI)

Recently we have witnessed the emergence of cloud computing as a new computing model that offers resources (e.g., compute, storage, network, etc.) as general utilities to be leased and released on-demand by users through the Internet. Given its innovative nature and reliance on the Internet, the cloud inherently comes with a number of vulnerabilities that increase the space for cyber attacks. This paper aims to provide an overview of major potential risks to privacy and security in the cloud. Various emerging threats and attack methods are discussed, and some speculative future research directions are presented.

Introduction

With the rapid development of processing and storage technologies and the success of the Internet, computing resources have become cheaper, more powerful, and more ubiquitously available than ever before. This technological trend has enabled the realisation of a new computing paradigm, *cloud computing*, in which resources (e.g. compute, storage, network, etc.) are provided as general utilities that can be leased and released by users through the Internet in an on-demand fashion. Cloud computing is revolutionising IT services and holds great potential to increase their affordability and availability. Users, whether large enterprises, small businesses or individuals, are drawn towards the cloud's promises of agility, reduced capital costs and enhanced IT resources (Dahbur et al. 2011). Corporations are shifting from providing their own IT infrastructure to utilising the services provided by the cloud for their information technology needs. The effectiveness and efficiency of moving data and applications to the cloud continue to attract users. Applications such as DropBox[i] (Drago et al. 2012) and iCloud[ii] for storing data or Gmail[iii] and Live mail[iv] to handle emails are being widely used today.

Given its innovative nature and reliance on the Internet, cloud computing raises a number of issues related to its resilience in terms of Cybersecurity. It is generally acknowledged that there are significant risks associated with privacy, security, and trust for cloud-based services (Nepal & Pathan 2014, Jansen 2011, Jansen & Grance 2011). There is a need to understand

 http://doi.org/10.7790/ajtde.v1n1.4

these risks as well as to build technologies to address them. Our focus in this article is to discuss the emerging threats to cloud services and present some potential future research directions.

The rest of the article is structured as follows. The next section provides a brief overview of cloud computing, which is followed by the discussion on the privacy, security, and trust issues related to cloud computing. We then outline major emerging threats and attack methods, followed by a discussion of future research directions.

Cloud Computing Overview

Though cloud computing has emerged as a new computing model in recent times, the main idea behind it is not new. The term 'cloud' has been used in various contexts such as describing large ATM networks in the 1990s (Zhang et al. 2010). However, it was after Google's CEO Eric Schmidt used the word to describe the business model of providing services across the Internet in 2006 that the term really started to gain popularity (Zhang et al. 2010). Since then, the term cloud computing has been used mainly as a marketing term in a variety of contexts to represent many different ideas. This has resulted in a fair amount of scepticism and confusion. In this paper, we use the definition of cloud computing provided by the National Institute of Standards and Technology (NIST) as

> "*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*". (NIST 2009)

Essential Characteristics

Cloud computing provides unique characteristics that are different from traditional approaches. These characteristics arise from the objectives of using clouds seamlessly and transparently. The five key characteristics of cloud computing defined by NIST (NIST 2009) include:

- *On-demand self-service* means users can request and manage resources such as storage or processing power automatically without human intervention.
- *Ubiquitous network access* enables computing resources to be delivered over the Internet and can be used by a variety of applications in heterogeneous platforms.
- *Resource pooling* means users can draw computing resources from a resource pool. The result is that the physical computing resources become 'invisible' to consumers.
- *Rapid elasticity* allows consumers to scale up and down the resources based on their needs, such as scaled up at the time of heavy loads and usage spikes.

 http://doi.org/10.7790/ajtde.v1n1.4

- *Measured Service*, also often called as Pay As You Go (PAYG), enables the cloud to be offered as a utility which users pay for on a consumption basis.

Service Models

In addition to the above five essential characteristics, the cloud community have extensively used the following three service models to categorise the cloud services (Buyya et al. 2009):

- *Software as a Service (SaaS)*. Cloud providers deliver applications hosted on the cloud infrastructure as internet-based on-demand services for end users, without requiring the installation of these applications on the users' computers. Examples of SaaS include *SalesForce.com*[v] and Google Apps such as *Google Mail*[vi] and *Google Docs*[vii].
- *Platform as a Service (PaaS)*. PaaS provides a programming environment such as OS, hardware and network so that users can install software or develop their own applications. *Google AppEngine*[viii] and *Microsoft Windows Azure*[ix] are the most well-known PaaS.
- *Infrastructure as a Service* (IaaS). IaaS provides a set of virtualised infrastructural components such as processing units, networks and storage. Users can build and run their own OS, software and applications. *Amazon EC2*[x] is the most recognised IaaS platform.

These three services sit on top of one another, IaaS at the bottom and SaaS at the top, and form the layers of cloud computing.

Deployment Models

More recently, four cloud deployment models have been defined to deliver cloud services to users:

- *Private cloud*. In this model, computing resources are used and controlled by a private enterprise, i.e., resource access is limited to the users that belong to the organisation that owns the cloud.
- *Public cloud*. In this model, computing resources are dynamically provisioned over the Internet via web applications/web services.
- *Community cloud*. In this model, a number of organisations with similar interests and requirements share the cloud infrastructure. The cloud infrastructure could be hosted by a third-party vendor or within one of the organisations in the community.
- *Hybrid cloud*. In this model, the cloud infrastructure is a combination of two or more clouds (private, community or public) described above. This model is becoming

 http://doi.org/10.7790/ajtde.v1n1.4

popular as it enables organisations to increase their core competencies by outsourcing peripheral business functions onto the public cloud while controlling core activities on-premises through a private cloud.

Security, Privacy, and Trust in the Cloud

In the following, we discuss security, privacy, and trust issues from four different perspectives: infrastructure, data, users, and providers. The discussion starts with the potential vulnerabilities in the cloud infrastructure, which is followed by a discussion on how to safeguard cloud data. We then discuss the user access management mechanisms, such as authentication, authorisation and identity management. Finally, we discuss the compliance issues for cloud providers including the requirements to follow standard policies, rules and regulations across multiple jurisdictions.

Cloud Infrastructure

Security starts from ensuring that the set of system components is inherently secure and resilient from adversaries' infiltration attempts. In addition, the programs run in those system components must have a set of appropriate security mechanisms in place to safeguard the cloud users' data from any potential misuse. We examine a number of unique technologies that are adopted by the cloud to make this possible.

Virtualisation is an important enabling technology provided at the IaaS layer that helps abstract the cloud infrastructure and resources to be made available to different users as isolated Virtual Machines (VMs) (Takabi et al. 2010). A hyper-visor or VM monitor is a piece of platform-virtualisation software that lets multiple operating systems run on a host computer concurrently. This underlying virtualisation enables an architectural feature called *multi tenancy,* whereby a single instance of software serves multiple client organisations (Zissis & Lekkas 2012). The software running on the cloud is designed to virtually partition its data and configuration so that each client organisation works with a customised virtual application instance.

Although the multi-tenancy model provides a means to generate virtualised resources for sharing, the notion of using a shared infrastructure could be a huge concern (Takabi et al. 2010). Without strong isolation, virtualised cloud resources, such as VMs, storage, and networks, are in a danger of being misused by adversaries (Takabi et al. 2010). Java Virtual Machine (JVM) and process level isolation techniques, originally proposed in Czajkowski (2000), are being increasingly used (Takabi et al. 2010). Newer platforms like Apex (Fisher 2007) from *Force.com* use components and meta-data that are shared across cloud users. They provide strong session management, object scoping and data filtering mechanisms

 http://doi.org/10.7790/ajtde.v1n1.4

(Sengupta et al. 2011). Trusted virtual machine monitors like Terra (Garfinkel et al. 2003) allow strong isolation at VM layer.

The PaaS layer provides a set of Application Programming Interfaces (APIs) that cloud users utilise to manage and interact with cloud services. The security and availability of general cloud services is dependent upon the security of these basic APIs. Appropriate security controls are mandatory requirements to enforce that only authorised cloud users can access service interfaces and make calls to authorised APIs with the right permissions. Moreover, there is a need for the isolation of APIs in memory to maintain the isolation between different users of the same service. Protocols such as mutual authentication (TPM 2011), WS-Security (OASIS 2006a; Jensen et al. 2009), and OAuth[xi] can be used to enforce authentication and authorisation on calls to APIs.

In the SaaS layer, web applications represent the dominant deployment model that enables the cloud users to access cloud services. Web applications represent 75% of the total reported vulnerabilities over the last three years (Almorsy et al. 2012). Thus, SaaS applications should be continuously validated and scanned for vulnerabilities, and provide automated mitigation (Yadav et al. 2013). Specific vulnerabilities of major web applications are related to the browser's front-end component. Among them are client-side data manipulation vulnerabilities, where adversaries exploit user components by completely altering legitimate users' input (Grobauer et al. 2011). Security mis-configuration is also very critical with multi-tenancy operations, where each tenant has its own security configurations that may conflict with others, leading to security holes (Yadav et al. 2013).

The National Vulnerability Database[xii] and the Common Weaknesses Enumeration[xiii] publish the most recent web vulnerabilities. NIST has been conducting a security analysis tools assessment project (NIST 2013). A part of this project is to specify a set of weaknesses that any source code security analysis approach should support, including Structured Query Language (SQL) Injection (Halfond & Orso 2005) and Cross Site Scripting (XSS) (Kirda et al. 2006).

In addition to the concerns at each layer of the cloud service models described above, the architecture dependency between different layers yields some serious security concerns (Yadav et al. 2013). The cloud computing model depends on a deep stack of inter-dependent layers where the functionality of a higher layer depends on the lower layers. The IaaS model covers cloud physical infrastructure and virtualisation. The platform interfaces and APIs in the PaaS layer depend on the virtualisation of resources delivered by the IaaS. The SaaS layer depends on a layer of platforms to host the services and a layer of virtualisation to optimise resource utilisation when delivering services to multi-tenants. Furthermore, any breach to

any cloud object created individually or the combination of IaaS/PaaS/SaaS will impact the security of the whole cloud platform.

Cloud Data

Specific threats to data in the cloud include theft, misuse (especially for purposes different from those originally notified to and agreed by the users) or unauthorised resale (Pearson & Benameur 2010). In addition, there is no guarantee that a cloud service provider has mechanisms in place to ensure cloud users can get access to all their data, or that cloud providers comply with a request for deletion of their data (Subashini & Kavitha 2011). It can also be difficult to get data back from the cloud and avoid vendor lock-in. In this section, we describe a number of issues related to data protection and privacy concerns prevalent in cloud computing (Svantesson & Clarke 2010).

The simple form of data protection from unauthorised data accesses is to use strong data encryption mechanisms like Advanced Encryption Standard (AES) (FIPS 2001) and Data Encryption Standard (DES) (FIPS 1999) where the whole data is encrypted with a private key and decrypted by a public key through the Public Key Infrastructure (PKI) (IETF 1995). This form of encrypted data in the cloud is good for storage or archiving but is rather costly to process. However, a new form of encryption proposed by Liu and Wang (Liu 2012; Liu & Wang 2012) from CSIRO enables the encrypted data to be processed in the public cloud without decrypting it. These encryption mechanisms generate a large number of keys and they need to be well managed. Key management is considered to be data security's Achilles heel (Sengupta et al. 2011). Virtual file system, called *TrustStore*, is another technique developed at CSIRO which allows sensitive data to be stored in the cloud and provides the secure service for the management of keys (Yao et al. 2010).

As the data in the cloud is fully controlled by the provider, there is a risk that data may be subject to unauthorised resale and may suffer from vendor lock-in. For example, to increase the revenue of the company, a cloud service provider may sell customers' data. However, this type of secondary data usage may violate customers' privacy. Data anonymisation is a technique employed by many providers to de-identify individual records, for example these include k-anonymisation (Zhong et al. 2005) and differential privacy (Dwork 2006). Such techniques protect privacy of customers while still being used for analysis. There may also be doubt about what will happen to data kept by a cloud provider when it becomes bankrupt or is acquired by another company (Pearson & Benameur 2010). To approach the issue, the standardisation of a set of data interfaces and transformation logic can be helpful as data can be moved around in case one cloud provider fails for any reason.

Data deletion is another data privacy concern. Cloud providers ensure availability by replicating data in multiple data centres. It is difficult to guarantee that no copy of the data or its backups is stored or processed, or that all these copies of data are deleted (Pearson & Benameur 2010). The matter becomes worse if the data is spread over or moved across different legal jurisdictions (Hooper et al. 2013). A new technique called Provable Data Possession (PDP) generates a probabilistic proof of data integrity based on only a small portion of the file (Ateniese et al. 2007). Similarly, there is research around Proof of Retrievability (PoR) to give users assurance that, once data is stored in a public cloud, it will be eventually retrievable (Shacham & Waters 2008). Proof carrying codes (Mahajan 2007) is another mechanism through which the cloud provider can verify user applications through formal proofs.

Cloud Users

Access management is another fundamental cloud security concern. In the cloud, access management is complex, as multiple users access the resources from a shared pool which is allocated dynamically on demand. There are also multi-level access points in different cloud service models. In addition, accesses to the shared computing resources are made over the Internet using various client applications with heterogeneous platforms. This in fact expands the opportunities for attack if no appropriate access protection mechanisms are in place.

Traditionally, an individual accessing a pool of resources is centrally managed by an enterprise by mapping the individual to a directory structure like Lightweight Directory Access Protocol (LDAP) (IETF 2006) and Activity Directory (Iseminger 1999), based on roles and access rights. In the cloud, synchronising such access control lists is a challenging issue as the volume of users can spike at anytime (Sengupta et al. 2011). This can be an especially difficult issue to solve as PaaS and SaaS have complex hierarchies, and establishing dynamic fine-grained access capabilities is not always straightforward. However, Service Provisioning Markup Language (SPML) (OASIS 2006b) can enable a faster user account provisioning and de-provisioning.

It is also found that user authentication in cloud is more error-prone and difficult, as the cloud exposes resources over the Internet. The resources can be accessed through

(a) web browsers (HTTP/HTTPS) using web applications supported in SaaS layer;

(b) web services and APIs, such as SOAP (W3C 2000), REST (Fielding 2000) and RPC protocols in PaaS, and

(c) remote connections made through Virtual Private Networks (VPN) and FTP in IaaS layer in the case of VMs and storage services.

 http://doi.org/10.7790/ajtde.v1n1.4

Security controls should target vulnerabilities related to these protocols, such as Man-In-The-Middle attack, to protect data transferred between the cloud platform and cloud users (Yadav et al. 2013).

In addition, cloud services are increasingly being accessed through web browsers and thin mobile devices running new sets of applications such as HTML-5 (W3C 2013). The utilisation of web browsers and mobile devices opens up even more opportunities for attack when their vulnerabilities are exploited (Grobauer et al. 2011). This has pushed enterprises to use VPN while communicating to the cloud. The Cloud Security Alliance (CSA) recommends cloud providers to offer stronger authentication mechanisms and also (optionally) allow users to use third-party identity management and single sign-on platforms like Microsoft Passport (Choo 2006). Online open identity management communities like OpenID[xiv] and OAuth[xv] provide standardised identity management mechanisms. They enable cloud providers to define their own set of integration solutions.

There is a growing concern in federated identity management in the use of community cloud. One of the major concerns is the lack of a set of common security token services and identity providers (Sengupta et al. 2011). Security Assertion Markup Language (SAML) (OASIS 2005) provides management infrastructure based on x.509 certificates. The ongoing Web Services standardisation work in WS-federation (OASIS 2009) has tried to provide some help in this aspect. However, these approaches are based on an assumption of strong trust relations being in place. This assumption does not work in the cloud where the collaboration is established in a transient fashion, i.e., dynamic and context-based short-term benefits. There is a need to develop more flexible cases of identity federation (Sengupta et al. 2011).

Cloud Providers

Cloud computing, at this stage, lacks interoperability and security management standards (Takabi et al. 2010, Popovic & Hocenski 2010). There is no standardised communication mechanism between and within cloud providers. Furthermore, there is no standard data export format, which makes it difficult for cloud users to leave a cloud provider. The lack of standards also makes it difficult to establish security frameworks for such heterogeneous environments and forces people for the moment to rely on common security best practices, which have been reported with a number of vulnerabilities (Grobauer et al. 2011).

Various forms of compliance are in practice in cloud computing. A few examples include industry initiatives on compliance like accounting (Sarbanes-Oxley, Basel), health information privacy (HIPAA) (Annas 2003) and credit card data safety (PCI) (Shaw 2009). Similarly standards around outsourcing auditing (SAS70) (Nickell & Denyer 2007) also govern cloud based outsourcing vendors. US Federal and other international laws such as the

Electronic Communication Privacy Act (ECPA) (Hernandez 1988) can be a concern for data privacy in the cloud. The transparency of data location is an important issue to be resolved for cloud computing if it wants a wider acceptance (Sengupta et al. 2011). In reality, different geographical data locations may come under different jurisdictions, each with its own set of laws that govern data privacy and security. It is not clear which party is responsible for ensuring that legal requirements for personal information are observed, appropriate data handling standards are set and followed, and whether they can effectively audit third-party compliance (CSA 2013).

Emerging Threats and Attack Methods

The cloud services and data hosted in the cloud can come under attack from two different sources: internal and external. External attacks come from cyber criminals who are not part of the cloud environments. Internal attacks come from insider threats (i.e., employees of cloud providers) and users misusing the cloud resources. We describe the main threats in both categories below.

Botnets and Denial of Service (DoS)

Bots (short for "robots") are malware programs covertly installed on a user's machine that allow an unauthorised user to remotely control the compromised computer for a variety of malicious purposes (DHS 2009). Botnets are networks of machines that have been compromised by bot malware so that they are under the control of an adversary. Among the various forms of malware, botnets are emerging as the most serious threat to cloud security as they provide a distributed platform for major illegal activities in the cloud (CSA 2013; DHS 2009).

A cloud is a large collection of computers or processors, memory, storage space, applications and other computing resources connected to the web. Cyber criminals may seek out the security vulnerabilities in the cloud to capture these resources for their own benefit using botnets. For example, a spam operation might use a botnet to blast out millions of messages, or unscrupulous businesses could use a botnet to knock down a competitor's website (CSA 2013). Botnets can also be used to crack open password-protected or encrypted information by using the combined resources of the botnet to conduct 'brute force' attacks.

Denial of Service (DoS) has been a threat to the Internet for years, but it becomes more problematic in the cloud computing environment when customers are dependent on the 24/7 availability of one or more cloud services. DoS forces the victim cloud service to consume large amounts of finite system resources such as processor power, memory, disk space or network bandwidth. This causes an intolerable system slowdown for legitimate

 http://doi.org/10.7790/ajtde.v1n1.4

service users. Eventually, the attack will prevent cloud users from being able to access their data or their applications. At worst, users may be billed for computer cycles and disk spaces they did not use but which were occupied by bots on their behalf.

Malicious Insiders

Previous research on cyber security has focused on protecting valuable resources from attacks by outsiders. However, the Cloud Security Alliance report shows that a large amount of security and privacy breaches in clouds is due to insider attacks (CSA 2013). Lack of control for the data kept in the cloud is contributing to the increasing rates of insider threats as the control of data is solely left under the provider's single management domain (Hunker & Probst 2011). There is often no visibility in the employee hiring standards and practices for cloud providers that contribute to the increasing incidents of insider threats (Cappelli et al. 2012). Without any barring, a third-party vendor for the provider can exploit this vulnerability to tap into sensitive data and sell it to a competitor of the victim organisation.

General Vulnerabilities

Web browsers are one of the most commonly used applications to allow cloud users to access various services offered by cloud providers. Like any other software, web browsers contain vulnerabilities. A well-known vulnerability is the Cross-Site Scripting (XSS). XSS enables attackers to inject malicious script into web pages. When unsuspecting users view the web pages, the malicious code is executed to perform malicious activities on the user's computer.

Cyber criminals are expanding their battleground from desktops to other platforms, including mobile phones, tablet computers and Voice over Internet Protocol (VoIP) (Goode 2002). Recently, malwares created specifically for mobile platforms are on the rise, as reported in annual security trend reports from Georgia Tech[xvi] and Symantec[xvii]. It is a major concern that cyber criminals will be drawn to the VoIP medium to engage in voice fraud, data theft and other scams.

There are virtually no limits to the creativity of adversaries in spreading malware when social engineering is involved. For example, an adversary, often under a false pretence, would befriend a naive user over a social network and lure the user into deliberately executing malicious code on the victim's machine (Chen et al. 2010). Cloud services are no exception from such attacks as the cloud entices attackers due to the large amount of sensitive data it holds.

Future Research Directions

We have so far discussed the main characteristics of cloud computing, the major security, privacy, and trust concerns in the cloud and the emerging threats and attack methods. We next describe what we believe are the major future research directions in this area.

Privacy-Preserving Model

The cloud involves the collaboration among multiple parties both at the user and provider levels. It is important to preserve privacy while exchanging information among these multiple entities. Research around secure multi-party computation (Fung et al 2010) seeks to create a randomised bit-level partition scheme. Using this scheme, the random data does not reveal any useful information even if it is aggregated by third parties. A number of privacy preserving techniques have been also developed in recent times (Wang 2010). These privacy-preserving models and research are increasingly becoming important in the cloud environments.

Data-Centric Security

Data in the cloud typically resides in a shared environment, but the data owner should have full control over who has the right to use the data and what they are allowed to do with it. To provide this capability, a standards-based data-centric security approach is an essential element that basically shifts data protection away from traditional systems and applications (Sengupta et al. 2011). The traditional approach encrypts the entire data, which is too expensive as much data in the cloud contains rich media content. One way of achieving data-centric security would be to use policy-based or role-based access controls. These access controls then can be defined in a language like Extensible Access Control Markup Language (XACML) (OASIS 2013) to govern context-based access rules. With the use of a standard like XACML, any access request to the data can be verified through an assertion or by checking with a central server.

Trust Management

Trust management and policy integration are active areas of research in cloud computing as the outsourcing model of the cloud forces users to have significant trust in their provider's technical competence (Pearson a& Benameur 2010). In cloud computing environments, the interactions between different service domains are also dynamic, transient, and intensive. Thus, development of a trust framework has been proposed to allow efficient capturing of a generic set of parameters required for establishing trust and to manage evolving trust (Zhang & Joshi 2009). The cloud's policy integration is another active area of research to address

challenges such as semantic heterogeneity, secure interoperability, and policy-evolution management (Pearson & Benameur 2010). Furthermore, customers' behaviours can evolve rapidly, thereby affecting established trust values. This suggests a need for an integrated, trust-based, secure interoperation framework that helps to establish, negotiate, and maintain trust to adaptively support policy integration (Zhang et al. 2010).

Data Provenance

Provenance technique is another notable mechanism that has been emerging and provides an ability to trace the lifetime changes and transformation of data (DHS 2009). With the complexity of the cloud infrastructure, it is becoming important to know who created a piece of data, who modified it and how, and so on. The provenance aims to provide good knowledge about the sources and intermediate processors of the data (DHS 2009). This is to assess the data's trustworthiness and reliability in the decision-making process. Provenance information could be used for various purposes such as trace-back, auditing, and history-based access control.

Trustworthy Systems

The term 'trustworthy systems' has been defined by the Department of Homeland Security (DHS) in the US as a long-term goal to indicate a computing system that is inherently secure, available and reliable, despite environmental disruptions, human user and operator errors, and attacks by hostile parties (DHS 2009). Towards this goal, Sheldon & Vishik (2010) advocate the requirements for secure hardware and software combinations as essential building blocks towards trustworthy systems. In this proposal, systems and devices share their provable and standard trust information confirming their trustworthiness. Trusted Platform Modules (TPM) offer a remote server attestation mechanism to attest users to a host and host to users to tackle the concerns of un-trusted execution environments (TPM 2011).

Conclusion

Cyber attacks have been on the rise in recent times. The effect of cyber attacks in cloud is severe. For example, the denial of service attacks on cloud data services may not only disrupt the services and keep the genuine customers out of enterprise services, but also increase the costs due to the underlying pay-as-you-go model. There is no way cloud service providers can vouch that a service request is genuine or the result of a cyber attack. Thus, the cloud service providers should not only be able to detect and prevent the cyber attacks on the services deployed on their clouds, but also should establish clear guidelines on how to resolve the disputes arising from such attacks. It is thus clear that some of the challenges

 http://doi.org/10.7790/ajtde.v1n1.4

related to cloud security, privacy and trust go beyond the technological solutions. We need to look at the social and legal aspects of the cloud data services.

To thwart potential cyber attacks, the cloud system should consider security, privacy, and trust as an essential requirement at the design time. However, there are a number of conflicting application requirements that require balancing acts. For example, balancing between data provenance (reveal enough information to trust the data and its source) and privacy (hide enough information not to identify individuals in the data) itself is a significant challenge in clouds. Other issues related to data security in cloud that need further research include seamless data migration among cloud providers, secured and privacy preserving big data analytics, interoperability among cloud service providers, strong user authentication, users' control of their own data including secure deletion, etc.

References

Almorsy, M., Grundy, J., & Ibrahim, A. S. 2012. Supporting automated vulnerability analysis using formalized vulnerability signatures. *In Proceedings of the 27th IEEE/ACM International Conference on Automated Software Engineering,* pp.100-109

Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. 2007. Provable data possession at untrusted stores. *In Proceedings of the 14th ACM conference on Computer and communications security*, pp. 598-609. http://doi.org/10.1145/1315245.1315318

Annas, G. J. 2003. HIPAA regulations-a new era of medical-record privacy?.*New England Journal of Medicine*, *348*(15), 1486-1490. http://doi.org/10.1056/NEJMlim035027

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25(6), 599-616. http://doi.org/10.1016/j.future.2008.12.001

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. 2012. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional

Chen, Y., Paxson, V., & Katz, R. H. 2010. What's new about cloud computing security. University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010), 2010-5.

Choo, K. K. R. 2006. Issue report on business adoption of Microsoft Passport. *Information management & computer security*, *14*(3), 218-234. http://doi.org/10.1108/09685220610670387

Czajkowski, G. 2000. Application isolation in the Java virtual machine. In *ACM SIGPLAN Notices,* 35(10), 354-366. http://doi.org/10.1145/354222.353195

CSA. 2013. The Notorious Nine Cloud Computing Top Threats in 2013. Cloud Security Alliance. [Internet]. Accessed 15 July 2013. Available from: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

DHS. 2009. Roadmap for Cybersecurity Research. Department of Homeland Security. [Internet]. Accessed 15 July 2013. Available from: www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

Dahbur, K., Mohammad, B., & Tarakji, A. B. 2011. A survey of risks, threats and vulnerabilities in cloud computing. In *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications,* pp. 1-6.

Drago, I., Mellia, M., M Munafo, M., Sperotto, A., Sadre, R., & Pras, A. (2012, November). Inside dropbox: understanding personal cloud storage services. In *Proceedings of the 2012 ACM conference on Internet measurement conference*, pp. 481-494. http://doi.org/10.1145/354222.353195

Dwork, C. 2006. Differential privacy. In *Automata, languages and programming,* pp. 1-12

Kirda, E., Kruegel, C., Vigna, G., & Jovanovic, N. 2006. Noxes: a client-side solution for mitigating cross-site scripting attacks. In *Proceedings of the 2006 ACM Symposium on Applied Computing* , pp. 330-337. http://doi.org/10.1145/1141277.1141357

FIPS. 2001. Advanced encryption Standard (AES). Federal Information Processing Standards Publication 197.[Internet]. Accessed 22 August 2013. Available from: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS. 1999. Data Encryption Standard (DES). Federal Information Processing Standards Publication 46-3.[Internet]. Accessed 22 August 2013. Available from: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

Fielding, R. 2000. Representational state transfer. Architectural Styles and the Design of Network-based Software Architecture, Doctoral dissertation, University of California, Irvine

Fisher, S. 2007. The architecture of the apex platform, salesforce. com's platform for building on-demand applications. In *Software Engineering-Companion, 2007. ICSE 2007 Companion*. pp. 3-3.

Fung, B., Wang, K., Chen, R., & Yu, P. S. 2010. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (CSUR)*, 42(4), No.14

Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., & Boneh, D. 2003. Terra: A virtual machine-based platform for trusted computing. In *ACM SIGOPS Operating Systems Review*, 37(5), 193-206. http://doi.org/10.1145/1165389.945464

Grobauer, B., Walloschek, T., & Stocker, E. 2011. Understanding cloud computing vulnerabilities. *IEEE Security & Privacy*, 9(2), 50-57. http://doi.org/10.1109/MSP.2010.115

Goode, B. 2002. Voice over Internet protocol (VoIP). *Proceedings of the IEEE,90*(9), 1495-1517. http://doi.org/10.1109/JPROC.2002.802005

Halfond W. G. J., & Orso A. 2005. AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks. In *Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering* (ASE '05). ACM, New York, NY, USA, 174-183.

Hernandez, R. T. 1988. ECPA and online computer privacy. *Fed. Comm. LJ,41*, 17.

Hunker, J., & Probst, C. W. 2011. Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), 4-27

Hooper, C., Martini, B., & Choo, K. K. R. 2013. Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, *29*(2), 152-163. http://doi.org/10.1016/j.clsr.2013.01.006

IETF. 1995. Public-Key Infrastructure (X.509). Internet Engineering Task Force (IETF) pkix charter. [Internet]. Accessed 22 August 2013. Available from: http://datatracker.ietf.org/wg/pkix/charter/

IETF. 2006. Lightweight Directory Access Protocol (LDAP). Internet Engineering Task Force (IETF) RFC 4511. [Internet]. Accessed 22 August 2013. Available from: http://tools.ietf.org/html/rfc4511

Iseminger, D. 1999. *Active Directory Services for Microsoft Windows 2000*. Microsoft Press.

Jansen, W. A. 2011. Cloud hooks: Security and privacy issues in cloud computing. In *2011 44th Hawaii International Conference on System Sciences (HICSS,)*pp. 1-10.

Jansen, W., & Grance, T. 2011. Guidelines on security and privacy in public cloud computing. NIST special publication, 800-144.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. 2009. On technical security issues in cloud computing. In *IEEE International Conference on Cloud Computing,* pp. 109-116

Liu, D. 2012. Homomorphic encryption for database querying. Australian Provisional Patent 2012902653, 2012

Liu, D., & Wang, S. 2012. Programmable order-preserving secure index for encrypted database query. In *IEEE 5th International Conference on Cloud Computing*, pp. 502-509

Mahajan, M. 2007. Proof Carrying Code. *INFOCOMP Journal of Computer Science*, 6, 100-109

Nepal, S., & Pathan, M. 2014. Security, Privacy and Trust in Cloud Systems. Springer. http://doi.org/10.1007/978-3-642-38586-5

Nickell, C. G., & Denyer, C. 2007. An introduction to SAS 70 audits. *Benefits Law Journal*, *20*(1), 58-68.

NIST. 2009. The NIST definition of Cloud Computing, version 15. National Institute of Standards and Technology (NIST), Information Technology Laboratory. [Internet]. Accessed 15 July 2013. Available from: http://www.csrc.nist.gov

NIST. 2013. Software Assurance Metrics And Tool Evaluation (SAMATE). National Institute of Standards and Technology (NIST), Information Technology Laboratory. [Internet]. Accessed 15 July 2013. Available from: http://samate.nist.gov/Main_Page.html

OASIS. 2005. Security Assertion Markup Language (SAML) v2.0. Organization for the Advancement of Structured Information Standards (OASIS). [Internet]. Accessed 22 August 2013. Available from: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

OASIS. 2006a. Web Services Security Language (WS-Security). Organization for the Advancement of Structured Information Standards (OASIS). [Internet]. Accessed 15 July 2013. Available from: https://www.oasis-open.org/standards#wssv1.1

OASIS. 2006b. Service Provisioning Markup Language (SPML). Organization for the Advancement of Structured Information Standards (OASIS). [Internet]. Accessed 15 July 2013. Available from: https://www.oasis-open.org/news/pr/service-provisioning-markup-language-spml-ratified-as-oasis-standard

OASIS. 2009. Web Services Federation Language (WS-Federation) Version 1.2. Organization for the Advancement of Structured Information Standards (OASIS). [Internet]. Accessed 22 August 2013. Available from: http://docs.oasis-open.org/wsfed/federation/v1.2/ws-federation.html

OASIS. 2013. Extensible Access Control Markup Language (XACML) v3.0. Organization for the Advancement of Structured Information Standards (OASIS). [Internet]. Accessed 22 August 2013. Available from: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Pearson, S., & Benameur, A. 2010. Privacy, security and trust issues arising from cloud computing. In IEEE Second International Conference on Cloud Computing Technology and Science, pp. 693-702

Popovic, K., & Hocenski, Z. 2010. Cloud computing security issues and challenges. In *2010 proceedings of the 33rd international convention MIPRO,* pp. 344-349.

Sengupta, S., Kaulgud, V., & Sharma, V. S. 2011. Cloud Computing Security-Trends and Research Directions. In *2011 IEEE World Congress on Services (SERVICES)*, pp. 524-531. http://doi.org/10.1109/SERVICES.2011.20

Shaw, A. 2009. Data breach: from notification to prevention using PCI DSS. *Colum. JL & Soc. Probs.*, *43*, 517

Sheldon, F. T., & Vishik, C. 2010. Moving toward trustworthy systems: R&D Essentials. *Computer*, 43(9), 31-40. http://doi.org/10.1109/MC.2010.261

Shacham, H., & Waters, B. 2008. Compact proofs of retrievability. In *Advances in Cryptology-ASIACRYPT,* pp. 90-107

Subashini, S., & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1-11. http://doi.org/10.1016/j.jnca.2010.07.006

Svantesson, D., & Clarke, R. 2010. Privacy and consumer risks in cloud computing. *Computer Law & Security Review*, *26*(4), 391-397. http://doi.org/10.1016/j.clsr.2010.05.005

Takabi, H., Joshi, J. B., & Ahn, G. J. 2010. Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, 8(6), 24-31. http://doi.org/10.1109/MSP.2010.186

TPM. 2011. Tusted Platform Module (TPM) Main Specifications v1.2. [Internet]. Accessed 22 August 2013. Available from http://www.trustedcomputinggroup.org/resources/tpm_main_specification

Wang, H. 2010. Privacy-preserving data sharing in cloud computing. *Journal of Computer Science and Technology*, 25(3), 401-414. http://doi.org/10.1007/s11390-010-9333-1

W3C. 2000. Simple object access protocol (SOAP) 1.1. W3C Note 08 May 2000 [Internet]. Accessed 22 August 2013. Available from: http://www.w3.org/TR/2000/NOTE-SOAP-20000508/

W3C. 2013. Hypertext Markup Language Version 5. (HTML-5), Editor's Draft 15 July 2013. W3C. [Internet]. Accessed 15 July 2013. Available from: http://www.w3.org/html/wg/drafts/html/master/

Yao, J., Chen, S., Nepal, S., Levy, D., & Zic, J. 2010. Truststore: making amazon s3 trustworthy with services composition. *In Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, pp. 600-605

Yadav, P., Mishra, P., Sharma, T., & Sharma. V. 2013. Security Issues In Cloud Computing And Associated Mitigation Techniques. *International Journal of Innovative Research and Development,* 2(5), 495-513

Zhang, Y., & Joshi, J. 2009. *Access control and trust management for emerging multidomain environments*. Emerald Group Publishing

Zhang, Q., Cheng, L., & Boutaba, R. 2010. Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, 1(1), 7-18. http://doi.org/10.1007/s13174-010-0007-6

Sdata. In *Proceedings of the twenty-fourth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*. pp. 139-147

Zissis, D., & Lekkas, D. 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592. http://doi.org/10.1016/j.future.2010.12.006

Endnotes

i www.dropbox.com

ii www.apple.com/au/icloud

iii mail.google.com

iv mail.live.com

v www.salesforce.com

vi mail.google.com

vii docs.google.com

viii appengine.google.com

ix www.windowsazure.com

x aws.amazon.com/ec2

xi oauth.net

xii nvd.nist.gov

xiii cwe.mitre.org

xiv openid.net

xv oauth.net

xvi https://www.gtisc.gatech.edu/

xvii http://www.symantec.com/security_response/publications

Cite this article as: Jang-Jaccard, Julian; Nepal, Surya; Guo, Y. Jay. 2013. 'Cybersecurity threats in cloud computing'. *Australian Journal of Telecommunications and the Digital Economy* 1 (1): pp.4.1 – 4.17. DOI: 10.7790/ajtde.v1n1.4 At: http://telsoc.org/journal