A Generalized Threat Taxonomy for Cloud Computing

Monjur Ahmed
School of Computer and Mathematical Sciences
Auckland University of Technology
New Zealand.
E-mail: monjur.ahmed@aut.ac.nz

Alan T Litchfield
School of Computer and Mathematical Sciences
Auckland University of Technology
New Zealand.
E-mail: alan.litchfield@aut.ac.nz

Shakil Ahmed
School of Computer and Mathematical Sciences
Auckland University of Technology
New Zealand.
E-mail: shakil.ahmed@aut.ac.nz

Abstract

This paper presents a genre-based, generalized threat taxonomy for cloud computing. Cloud computing provides numerous possibilities and challenges but the nature of cloud computing exposes the resources of a cloud architecture to a wide range of threats. Presently, many potential threats, represented as security concerns, are known in a general sense but they are not classified specifically in relation to cloud services delivery. Therefore security concerns need identification and assessment and presented in a consistent and hierarchical form. We posit that to approach the issue in this way allows for more effective enforcement and therefore better resilience in a cloud architecture. We further posit that failure to effectively identify threats will lead to lower levels of trust, effectiveness and performance. The generalized threat taxonomy provides researchers with a framework through which risk factors and threats may be identified; and related against an overall picture of threat patterns.

Keywords

Cloud Computing, Security, Threat Taxonomy, Trust, Vulnerabilities.

1. INTRODUCTION

Cloud computing has recently reached a level of general acceptance and is used as a means for deploying computing resources (Dahbur, Mohammad & Tarakji, 2011). Cloud computing is often delivered on a rental basis, implying that resources are exposed to the outside world and therefore open to attack from third parties. While the customers of a cloud computing service have little to worry about with infrastructure management (Akande, April & Belle, 2013), security threats are a major concern (Jaeger, Lin & Grimes, 2008). Therefore, security management is a key requirement in cloud computing (Gonzalez, Miers, Redıgolo, Simplıcio, Carvalho, Naslund & Pourzandi, 2012) and so it is important to explore and realize threats in a cloud computing environment.

A cloud based infrastructure implies an adaptation of a distributed network to support operations. Any distributed network is prone to security issues where the failure of any element may open the whole network to security threats (Garcia-Morchon, Kuptsov, Gurtov & Wehrle, 2013). Network security challenges are a common problem for which security in computer networks remain a challenge (Yang & Lui, 2014). This suggests that cloud computing needs to give special attention to security and that challenges need to be defined and identified. In this paper we present a generalized threat taxonomy for cloud computing. A genre-based, high level categorization of threat families are taken into account for the threat taxonomy instead of specific threats. The taxonomy is developed by applying the intuitive methodology outlined by Nickerson, Varshney and Muntermann (2013).

The motivation to develop a threat taxonomy arises from a need to present threats in a rational form. To do this, we take a genre based approach rather than identifying specific threats. This ensures that any new threat that emerges satisfies general categories instead of developing a new taxonomy for each type of threat.

First we discuss existing viewpoints on cloud threat taxonomy, then we present a generalized threat taxonomy and rationale. To justify the taxonomy, we consider five recent case studies that illustrate breaches and then the case studies are related to the taxonomy.

2. CLOUD THREAT TAXONOMY

This taxonomy is founded on the epistemological foundations of existing research. For example, Gonzalez et al. (2012) propose three viewpoints for considering threats: architecture, compliance and privacy. The security taxonomy for cloud computing proposed by Hashemi and Ardanaki (2012) considers four major categories: infrastructure, application, platform and administration. They then denote specific threats under each category. Grobauer, Walloschek and Stocker (2011) do not discuss a cloud threat taxonomy in a traditional structured approach, instead the authors concentrate on generic threats that are linked to cloud computing. The cloud computing threats listed by Lee (2012) categorises risks: responsibility ambiguity, protection inconsistency, evolutional risks, supplier lock-in, business discontinuity, license risks, bylaw conflicts, bad integration, hypervisor isolation failure, service unavailability, data unreliability, abuse of rights of the cloud service provider, shared environment and use of insecure APIs.

Chou (2013) describes how the risks of the cloud model are to be considered from its deployment model as well as traditional network threats and data loss perspectives. The major threat categories proposed are resource abuse, data breaches and security attacks. Höfer and Karagiannis (2011) propose a tree-based taxonomy for cloud services that can be used to identify associated threats in each type of service.

Addressing management issues, Cardoso and Simões (2012) note costs, benchmarks, change management, legislation, SLA, lack of interoperability, information retrieval, information localization, standardization, single point of failure, service availability and security issues as the major category of challenges for cloud computing. However, Rimal, Choi and Lumb (2010) argue that all kinds of taxonomy for cloud computing are developed from a vendor perspective with little or no concern for the consumer or enterprise IT perspective.

Soares, Fernandes, Gomes, Freire and Inácio (2014) identify eight major threat categories for cloud computing: security issues identified by organizations, deployment and service delivery model security, software-related security issues, data storage and computational security issues, virtualization security issues, networking, web and hardware resource security issues, access and trust security issues. Singh and Shrivastava (2012) describe a threat taxonomy based on classes of participant in a cloud-based architecture: service users, service instances and cloud providers. The threats are further classified as six root categories: service-to-user, user-to-service, cloud-to-service, service-to-cloud, cloud-to-user and user-to-cloud.

Finally, Chraibi, Harroud and Maach (2013) address the technical aspects of cloud architectures to describe cloud security as five major categories: hardware components, virtual machine manager, guest operating systems, applications network and governance.

We have taken these factors into account and assimilated them into a more generalised taxonomy that incorporates the factors along with artefacts that are produced for use in the cloud.

3. CASE STUDIES

This section presents six cases of where cloud services have been breached or taken offline. To justify the elements, the case studies are then mapped to the taxonomy.

3.1 Case study 1 – Apple iCloud Breach

Apple’s iCloud is a consumer level service that is often used to back up a user’s phones’ images, music, data and so on (Apple, 2014). During Labour Day weekend in 2014, celebrity photos that were obtained from Apple’s iCloud service were published by purported hackers (PCWorld, 2014). The hackers had gained unauthorized access to the contents of user accounts through the application of brute force password cracking. TechTimes (2014) and The Wall Street Journal (2014) report that Apple denied there was a security breach and categorised the event as a targeted attack. TechTimes (2014) adds that Apple reported the attack as having been focussed some on specific user accounts (those of the celebrities) and that access was gained by the hackers working out the username, password and security question, therefore Apple says this is not an architecture wide breach on iCloud.

3.2 Case study 2 – Sony Attack and Amazon Cloud

In April 2011, the online entertainment system of Sony Corp was attacked. It is claimed that Amazon's cloud based web servers are used to launch the attack (Bloomberg, 2014). "Hackers using an alias signed up to rent a server through Amazon's EC2 service and launched the attack from there... The development sheds light on how hackers used the so-called cloud to carry out the second-biggest online theft of personal information to date. The incursion, which compromised the personal accounts of more than 100 million Sony customers, was "a very carefully planned, very professional, highly sophisticated criminal cyber attack," Sony has said… The hackers didn't break into the Amazon servers... Rather, they signed up for the service just as a legitimate company would, using fake information." (Bloomberg, 2011)

Bloomberg (2011) states that Amazon is left open for anyone to use anonymously by opening an account. It is claimed that using cloud based web services has helped the hackers achieve anonymity. Besides, using a clpoud based architecture for password cracking by makes the cloud an attractive target (Bloomberg, 2011).

3.3 Case study 3 – JP Morgan cloud server hack

In 2014, 80 million JP Morgan account holders have their records accessed in a cloud related breach (CNN, 2014). Personal information like names, addresses, email addresses and phone numbers of 76 million users and 7 million small businesses are accessed by the hackers. The bank claims that no account related information, account number user IDs or dates of birth is exposed to the hackers. The bank claims no unusual customer fraud is observed in the incident. Any user accessing the service, including websites and smartphone apps, are affected. Despite there being no evidence of fraudulent activity, JP Morgan stresses that the accessed information can still be abused by selling it to spammers (CNN, 2014). Computerworld (2014) reports that this incident as a cyber-attack though no "unusual" fraud is detected.

3.4 Case study 4 – Dropbox

The cloud storage provider Dropbox faces a cloud attack in mid-2011. The incident is described as a security nightmare scenario. The website is exposed and unprotected with a large number of customers' sensitive personal data. The cloud storage provider serves 25 million customers who use the service to store their documents, photos, videos or other files. The system was unprotected for four hours and during the period visitors could gain access to any account by using any password. The company traded security for use of use by encrypting and decrypting data on its own servers and instead of using complex encryption keys users are provided with a simpler method for logging in with just a password (CNN, 2011).

3.5 Case study 5 – SnapChat

The chat and photo sharing application SnapChat is claimed to have its cloud servers hacked in October, 2014. The service provider's phone app and/or its servers have supposedly been hacked. The service provider denies the claim and points to a third party vendor that reverse engineered an API to access and store users' materials from the SnapChat server. Further, the third party app makes users non-compliant with SnapChat terms and conditions. Thus SnapChat users are victims of the third party and SnapChat servers have not been hacked (TheRegister.co.uk, 2014).

3.6 Case study 6 – Spark

Spark, the largest telecom vendor in New Zealand, experiences a major shutdown of its cloud servers in September 2014. This resulted in service unavailability of the vendor's broadband service. The incident is the consequence of a cyber-attack. It is believed that the attack is the work of international cyber criminals who have installed malware onto users' computers. The malware code provides the capability to launch a denial of service attack. The attack generated high volumes traffic to the vendor's servers and resulted in service unavailability. The service provider clarifies that this is not a fault with its own network infrastructure but rather the issue affects the client terminals or platforms (Stuff.co.nz, 2014).

4. GENERALIZED THREAT TAXONOMY

The difficulty in distinguishing cloud and non-cloud threats in a cloud computing environment lies in the conceptual nature of 'cloud computing'. The term refers to a generalized and holistic application of remote computing resources, either hard or soft, and as an encapsulating layer for all the technologies and approaches required for a tangible distributed, virtualized and homogenized computing environment. This implies that the challenges and threats that need to be considered for cloud computing do not essentially have to be cloud specific, or the security challenges that are purely cloud related. Since many kinds of technology can be used within the context of cloud computing, a generalized threat taxonomy is required to ensure that no security concerns are left out of the scope in strategic surveillance planning for a cloud computing architecture.

The genre-based generalized threat taxonomy for cloud computing (Figure 1) is defined as a high level categorization of the family of threats rather than providing low level detailing of actualized threats within each genre (such as those described in section 2). The holistic view of the generalized threat taxonomy ensures that major trends in security concerns are taken into account to potentially identify threats from facets out of which cloud computing security challenges may arise. If specific threats are considered and a categorization of threats are done with no hierarchical order then the threat taxonomy may not maintain internal coherence. Thus, the generalized threat taxonomy is hierarchical.

Both qualitative and quantitative aspects of a computing environment may be applied in a cloud computing scenario where *soft* and *hard* factors of the parties involved in cloud computing are accounted for. The parties considered are cloud providers, cloud users and intermediary providers (for example, Internet or public infrastructure discussed later in this section).

Cloud computing illustrates a computing approach that includes any kind of system and social setting, including socio-technical systems. Consequently both technological and human factors (for example regulations, policy, and user competence) are part of the greater picture from which challenges and security concerns for cloud computing may emerge. The social context includes social engineering, competence and compliance. Social engineering is an emerging threat in Internet and cloud computing (Krombholz, Hobel, Huber & Weippl, 2013) and that introduces security threats to confidentiality, integrity and authenticity of personal and confidential data (Thornburgh, 2004). Robling and Muller (2009) define social engineering as activities that manipulate people to gain unfair access to confidential and sensitive data. This in turn presents additional factors such as low levels of competence or lack of compliance that may provide opportunities for practices that facilitate social engineering attacks.

The hierarchical categorization of the generalized threat taxonomy has ‘hard’ technological factors and ‘soft’ human factors as root categories. The proposed taxonomy is depicted in figure 1.

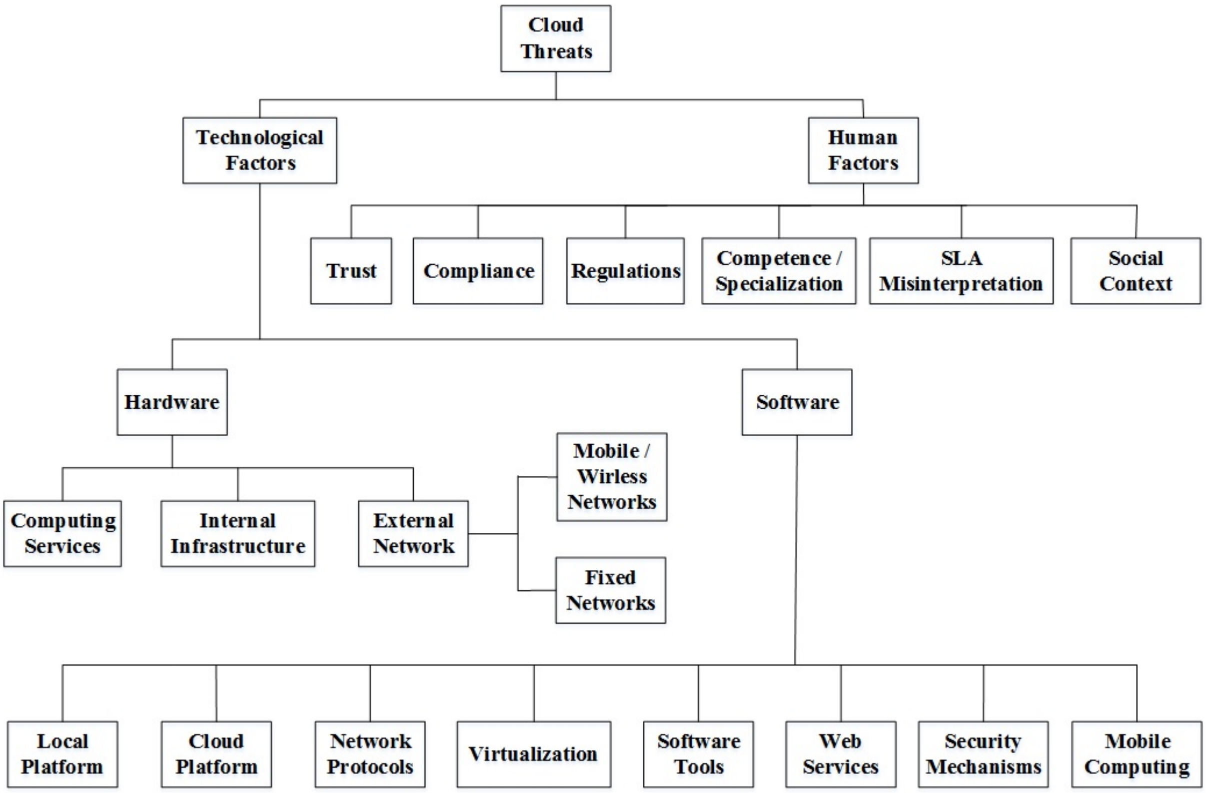

Figure 1: Generalized, genre-based threat taxonomy for Cloud Computing

4.1 Human Factors

Human factors in this context can be thought of as the human-centric actions in a cloud infrastructure that may potentially introduce security risks in that respective cloud architecture. For example, a lack of effective governmental regulations may hinder cloud services development in a region or a lack of integrity of the application of regulations may lead to unethical exploitation of cloud services. Other human factors associated with cloud threats include social engineering, poor levels of computer literacy or security awareness of cloud users, insufficient trust, and poor compliance to regulations and standards. For example, in the SnapChat case, users installed the third party app in order to get around the terms and conditions specified by SnapChat and to capture and store images. Ideally, SnapChat does not retain image data after a short time but the reality is that data are transferre through a network and so it exists on servers. The third party app effectively intercepted the data stream. Additionally, in the Spark case, the company blamed users who had downloaded and installed malware by opening infected email attachments. Often the users had no idea of what they had done.

Any single cloud breach may incorporate a number of threats in the taxonomy. For example, the JP Morgan case introduces a concern that users' personal information are stolen and while no further abuse is found, there is the potential for subsequent damages to occur when data are sold to criminals. Whether the reason is technological (computing services, cloud platform, virtualization, web service) or human factor (competence, social context) the issue of trust as a threat for the organization is highlighted.

Service License Agreement (SLA) design and management are related to cloud security issues (Srinivasan, Sarukesi, Rodrigues, Manoj & Revathy, 2012). SLA misinterpretation is a major factor when issues arise, for example blindly accepting an SLA or not understanding the legal implications of the SLA by the end users provides opportunites for security breaches to manifest. SLA misinterpretation may be associated with the unexpected consequences of actions and therefore situations that are not in line with business strategy. Thus the consequences can present risks and threats to the business and monitoring SLA's is important (Emeakaroha, Netto, Calheiros, Brandic, Buyya & Rose 2012). While Sun, Singh and Hussain (2012) say that the SLA provides assurance against security risks from SLA violation we add that SLA provisioning is important, we also say that sufficient research is required because violation is linked to security threats (Casalicchio and Silvestri, 2013).

Gonzalez et al. (2012) and Guo, Sun, Chang, Sun & Wang (2011) say that trust is linked to security concerns and that as a concept, it comes from the social sciences. Khan and Mullahi (2010) say that a user keeps trust with a cloud provider through consistent practices of control, ownership and security. Trust is normally held by the cloud services consumer and so the choice for the consumer is whether to place their trust in the provider. This is a matter of perception and is not technology dependent. Also, the strength of trust for cloud service providers in any region is largely dependent on the integrity, scope and dependability of relevant regulations and policies set and enforced by regulatory authorities. While cloud services consumers are required to have trust in cloud providers when they store their personal data (Roberts & Al-Hamdani, 2011), security and trust management remain as one of the major challenges in cloud computing (Noor, Sheng, Zeadally & Yu, 2013). The opportunity to breach the defenses of a service provider presents a new threat, that is loss of trust. Case study four, the DropBox example, provides an illustration of how trust can be affected from the lowering of the perception of the integrity of a cloud architecture from a breach. This case study is also provides a view about lack of competence when designing the security mechanism or forecasting potential threats.

Of the six cases presented, some incidents are not attacks on cloud architecture. In several cases, it is not easy to identify those responsible for the attack. This may reflect a lack of regulation or compliance of standards in cloud service provisioning and management. Apple is one such example, the claim is made that specific user accounts are targeted and accessed using brute force techniques, thus not all Apple users were affected. Apple provides robust security but in this case, it is the users' weak passwords, lack of vigilance, for example, not locking the phone or leaving an unlocked phone unattended.

Either the fault lies with human or technological factors. If there is no architecture-wide attack, then users may have just cause to blame the cloud service provider. However, this may link to a misinterpretation of the SLA, despite of the fact that such incidents may emerge as a consequence of human factors such as competence and social context.

4.2 Technological Factors

Technological factors refers to threats that fall outside the human factor categories, which generally means threats associated with technological practices and deployment. Technological factors are subdivided into hardware and software related threats. The hardware related threats normally arise from the cloud infrastructure and the network (for example the Internet) through which cloud resources are accessed. Software based threats emerge from operating environments, tools, applications or services available. These include both the cloud providers' servers and the services consumers' devices. Thus software and platforms (for example operating systems and Virtual Machine management systems) are the major sources of software based threats.

The Internet is a significant factor in cloud computing because it is the primary means of access to remote cloud based resources. Internet protocols have their own set of vulnerabilities that the cloud computing inherits due to its heavy reliance on Internet technology (Grobauer, Walloschek & Stocker, 2011). When it comes to software based security concerns, virtualization comes into focus because virtualization is widely used in cloud server deployment and comes with known vulnerabilities (Perez-Botero, Szefer & Lee, 2013). Therefore virtualization is identified as a threat category.

Web based services are a popular means of accessing computing functions. Since web based sessions can have numerous known security challenges, web services are noted as a threat. This is something that Spark experiences on a daily basis but the case referred to provides an example of how a targetted attack can overcome services. Additionally, Grobauer, Walloschek and Stocker (2011) argue that virtualization, web services, and application and cryptography are associated with either intrinsic or prevalent vulnerabilities. The Sony incident brings not only technological factors into context, but also human factors where one organization becomes vulnerable while using the cloud architecture provided by another.

As a consequence of the ingenuity of those who would breach the security of systems, an equally wide range of security mechanisms have been established over time. For example, cryptography is incorporated as part of security mechanisms in computing applications to prevent security breaches (Fan & Huang, 2013). Additionally, mobile computing is now widely used as a service (Chow, Jakobsson, Masuoka, Molina, Niu, Shi & Song, 2010) both with and without cloud based services. The SnapChat example provides stark evidence of what goes wrong when lax security is employed, albeit in this case that the third party software developer acted outside the terms and conditions of the company. With the concept of Bring Your Own Device (BYOD), mobile computing is experiencing increased integration in cloud computing environments (Krombholz et al., 2013). Thus, mobile computing specific threats need to be addressed.

Hardware based security concerns normally emerge from infrastructure and its maintenance. Various computing and maintenance services for example, unless a robust monitoring system is in place that includes incident response and routine maintenance, then the opportunity is provided for a person (insider or outsider) to attempt an intrusion. Also, the internal infrastructure of a cloud architecture presents a number of potential security weaknesses. For example, failure or malfunctioning of hardware may lead to overall inconsistency in the infrastructure. The external network always provides a threat simply because it is a ‘public place’ where security is not guaranteed. However, norms associated with the real life analogy of the public place do not apply in the case of computer and communication networks because external computing and communication networks do not necessarily adhere to political boundaries. So the robustness of the ‘public place’ is determined by collective global standards. In the case of mobile computing, these issues are highlighted where the public infrastructure is the usual means for connectivity.

6. CONCLUSION

Cloud computing provides opportunities and challenges as it is increasingly embedded into computing operations. Opportunities progressively reveal themselves and as they emerge, so do challenges and so it is important to acknowledge and contextualize challenges. If security concerns in cloud computing are not addressed sufficiently, the consequences may be severe. A top down generalized threat taxonomy for cloud computing provides the context for identifying, acknowledging and addressing threats. Such a taxonomy ensures safer cloud computing practice and that major trends are not left out of scope when developing a robust and integrated surveillance strategy.

REFERENCES

Akande, A.O., April, N.A. and Belle, J.V. 2013. “Management Issues with Cloud Computing”, *ACM ICCC’13,* December 1–2, Wuhan, China, pp. 119-124.

Apple, 2014. “iCloud: What is iCloud”. Retrieved 24 September 2014, from http://support.apple.com/kb/ph2608

Bloomberg, 2011. “Amazon.com Server Said to Have Been Used in Sony Attack”. Retrieved 24 September 2014, from http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackers-using-amazon-com-server.html

Bloomberg, 2011. “Sony Network Breach Shows Amazon Cloud’s Appeal for Hackers”. Retrieved 25 September 2014, from http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html

Cardoso, A. and Simões, P. 2012. “Cloud Computing: Concepts, Technologies and Challenges”, *ViNOrg 2011, CCIS 248,* Springer-Verlag Berlin Heidelberg, pp. 127–136.

Casalicchio, E. and Silvestri, L. 2013. “Mechanisms for SLA provisioning in cloud-based service providers”, *Computer Networks* (57), pp. 795–810.

Chou, T. 2013. “Security Threats on Cloud Computing Vulnerabilities”, *International Journal of Computer Science & Information Technology*, (5:3), pp. 79-88, DOI : 10.5121/ijcsit.2013.5306.

Chow, R., Jakobsson, M., Masuoka, R., Molina, J., Niu, Y., Shi, E. and Song, Z. 2010. “Authentication in the Clouds: A Framework and its Application to Mobile Users”, *ACM CCSW’10*, October 8, 2010, Chicago, Illinois, USA. pp. 1-6.

Chraibi, M., Harroud, H., and Maach, A. 2013. “Classification of Security Issues and Solutions in Cloud Environments”, *ACM iiWAS2013*, 2-4 December, 2013, Vienna, Austria.

CNN, 2014. “JPMorgan: 76 million customers hacked.” Retrieved 06 October 2014, from http://money.cnn.com/2014/10/02/technology/security/jpmorgan-hack/

CNN, 2011. Dropbox's password nightmare highlights cloud risks. Retrieved 07 October 2014, from http://money.cnn.com/2011/06/22/technology/dropbox_passwords/

Computerworld, 2014. “JPMorgan Chase breach affected 83 million customers.” Retrieved 06 October 2014, from http://www.computerworld.co.nz/article/556581/jpmorgan-chase-breach-affected-83-million-customers

Dahbur, K., Mohammad, B. and Tarakji, A.B. 2011. “A Survey of Risks, Threats and Vulnerabilities in Cloud Computing”, *ACM ISWSA’11*, April 18–20, Amman, Jordan.

Emeakaroha, V.C., Netto, M.A.S., Calheiros, R.N., Brandic, I., Buyya, R. and Rose, C.A.F. 2012. “Towards autonomic detection of SLA violations in Cloud infrastructures”, *Future Generation Computer Systems* (28), pp. 1017–1029.

Fan C. and Huang, S. 2013. “Controllable privacy preserving search based on symmetric predicate encryption in cloud storage”, *Future Generation Computer Systems* (29), pp. 1716–1724.

Garcia-Morchon, O., Kuptsov, D., Gurtov, A. and Wehrle, K. 2013. “Cooperative security in distributed networks”, *Computer Communications* (36), pp. 1284–1297.

Gonzalez, N., Miers, C., Redıgolo, F., Simplıcio, M., Carvalho, T., Naslund, M. and Pourzandi, M. 2012. “A quantitative analysis of current security concerns and solutions for cloud computing”, *Journal of Cloud Computing: Advances, Systems and Applications* (1:11), pp. 1-18.

Grobauer, B., Walloschek, T. and Stocker, E. 2011. “Understanding Cloud Computing Vulnerabilities”, *IEEE Security and Privacy*, March/April, 2011, pp. 50-57.

Guo, Q., Sun, D., Chang, G., Sun, L. and Wang, X. 2011. “Modeling and Evaluation of Trust in Cloud Computing Environments”, *3rd International Conference on Advanced Computer Control (ICACC 2011)*, pp. 112-116.

Hashemi, S.M. and Ardakani, M.R.M., 2012. “Taxonomy of the Security Aspects of Cloud Computing Systems – A Survey”, *International Journal of Applied Information Systems*, (4:1), pp. 21-28.

Höfer, C.N. and Karagiannis, G. 2011. “Cloud computing services: taxonomy and comparison”, *Journal of Internet Service Applications* (2), pp. 81–94, DOI 10.1007/s13174-011-0027-x.

Jaeger, P.T., Lin, J. and Grimes, J.M. 2008. “Cloud Computing and Information Policy: Computing in a Policy Cloud?”, *Journal of Information Technology & Politics* (5:3), pp. 269-283, DOI: 10.1080/19331680802425479.

Khan, K.M. and Malluhi, Q. 2010. “Establishing Trust in Cloud Computing”, *IT Pro*, September/October 2010. pp. 20-26.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E. 2013. “Social Engineering Attacks on the Knowledge Worker”, *ACM SIN ’13*, November 26-28, Aksaray, Turkey. Pp. 28-35. http://dx.doi.org/10.1145/2523514.2523596.

Lee, K. 2012. “Security Threats in Cloud Computing Environments”, *International Journal of Security and Its Applications* (6:4), pp. 25-32.

Nickerson, R.C., Varshney, U. and Muntermann, J. 2013. “A method for taxonomy development and its application in information systems”, *European Journal of Information Systems* (22), pp. 336–359.

Noor, T.H., Sheng, Q.Z., Zeadally, S. and Yu, J. 2013. “Trust Management of Services in Cloud Environments: Obstacles and Solutions”, *ACM Computing Surveys* (46:1), Article 12, pp. 12:1-12:30.

PCWorld, 2014. “Don’t blame iCloud yet for hacked celebrity nudes”. Retrieved 24 September 2014, from http://www.pcworld.com/article/2601081/dont-blame-icloud-yet-for-hacked-celebrity-nudes.html

Perez-Botero, D., Szefer, J. and Lee, R.B. 2013. “Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers”, *ACM, CloudComputing’13*, May 8, Hangzhou, China, pp. 3-10.

Rimal, B.P., Choi, E. and Lumb, I. 2010. *“Cloud Computing: Principles, Systems and Applications”*, Computer Communications and Networks, Chapter-2, Springer-Verlag London Limited, DOI 10.1007/978-1-84996-241-4_2.

Roberts, J.C. and Al-Hamdani, W. 2011. “Who Can You Trust in the Cloud? A Review of Security Issues within Cloud Computing”, *ACM Information Security Curriculum Development Conference 2011*, October 7-9, Kennesaw, GA, USA, pp. 15-19.

Robling, G. and Muller, M. 2009. “Social Engineering: A Serious Underestimated Problem”, *ACM ITiCSE’09*, July 6–8, Paris, France, pp. 384-387.

Singh, A. and Shrivastava, M. 2012. “Overview of Attacks on Cloud Computing”. *International Journal of Engineering and Innovative Technology* (1: 4), pp. 321-323.

Soares, L.F.B., Fernandes, D.A.B., Gomes, J.V., Freire, M.M. and Inácio, P.R.M. 2014. *“Cloud Security: State of the Art”*, Security, Privacy and Trust in Cloud Systems, (3), Springer-Verlag Berlin Heidelberg, DOI: 10.1007/978-3-642-38586-5_1.

Srinivasan, M.K., Sarukesi, K., Rodrigues, P., Manoj, S.M. and Revathy, P. 2012. “State-of-the-art Cloud Computing Security Taxonomies - A classification of security challenges in the present cloud computing environment”, *ACM ICACCI '12,* August 03 – 05, Chennai, India, pp. 470-476.

Staff.co.nz. 2014. “Spark broadband still down for many.” Retrieved 13 October 2014, from http://www.stuff.co.nz/business/10468128/Spark-broadband-still-down-for-many

Sun, L., Singh, J. and Hussain, O.K. 2012. “Service Level Agreement (SLA) Assurance for Cloud Services: A Survey from a Transactional Risk Perspective”, *ACM MoMM2012*, 3-5 December, Bali, Indonesia, pp. 263-266.

TechTimes, 2014. “Apple denies iCloud, Find My iPhone security breach: Only very targeted attacks”. Retrieved 25 September 2014, from http://www.techtimes.com/articles/14717/20140907/apple-denies-icloud-find-my-iphone-security-breach-only-very-targeted-attacks.htm

The Wall Street Journal, 2014. “Apple Denies iCloud Breach”. Retrieved 24 September 2014, from http://online.wsj.com/articles/apple-celebrity-accounts-compromised-by-very-targeted-attack-1409683803

TheRegister.co.uk, 2014. “Slap for SnapChat web app in SNAP mishap flap: '200,000' snaps sapped” Retrieved 10 October, 2014, from http://www.theregister.co.uk/2014/10/10/new_photo_hack_claim_200000_snapchat_photos/

Thornburgh, T. 2004. “Social Engineering: The “Dark Art”, *ACM InfoSecCD Conference’04*, October 8, Kennesaw, GA, USA, pp. 133-135.

Yang, Z. and Lui, J.C.S. 2014. “Security adoption and influence of cyber-insurance markets in heterogeneous networks”, *Performance Evaluation* (74), pp. 1–17.

COPYRIGHT