Dimensions Of Security Threats In Cloud Computing: A Case Study

Mathew Nicho, University of Dubai, UAE
Mahmoud Hendy, University of Dubai, UAE

ABSTRACT

Even though cloud computing, as a model, is not new, organizations are increasingly implementing it because of its large-scale computation and data storage, flexible scalability, relative reliability, and cost economy of services. However, despite its rapid adoption in some sectors and domains, it is evident from research and statistics, that security-related threats are the most noticeable barrier to its widespread adoption. To investigate the reasons behind these threats, the authors used available literature to identify and aggregate information about IS security threats in cloud computing. Based on this information, the authors explored the dimensions of the nature of threat by interviewing a cloud computing practitioner in an organization that uses both the private and public cloud deployment models. From these findings, the authors found that IS security threats in cloud computing must be defined at different levels; namely, at the business and technical level, as well as from a generic and cloud-specific threat perspective. Based on their findings, the authors developed the Cloud Computing Threat Matrix (CCTM) which provides a two-dimensional definition of threat that enables cloud users to fully comprehend the concerns so that they can make relevant decisions while availing cloud computing services.

Keywords: Cloud Computing; Security; Cloud Security Issues Taxonomy; Threat Matrix

INTRODUCTION

Because a cloud is a collection of inter-connected and virtualized computers (Buyya et al., 2008), the main enabling technology for cloud computing is virtualization. The basic concept of cloud is based on the premise that instead of having selected information systems (IS) resources, such as software and data stored locally on a user's or organization's computer systems, these resources can be stored on Internet servers, called "clouds," and accessed anytime, anywhere as a paid service on the Internet. Cloud computing has the potential to bring significant benefits to small- and medium-sized businesses by reducing the costs of investment in information communication technology (ICT) infrastructure because it enables the use of services, such as computation, software, data access, and storage by end-users, without the need to know the physical location and configuration of the system that delivers the services (Mujinga & Chipangura, 2011). However, it has been stated that organizations adopt cloud computing projects and systems cautiously while maximizing benefits and minimizing risks (Lawler, Joseph, & Howell-Barber, 2012). Cloud computing is expected to play a vital role in reshaping the enterprise architecture and transitioning it toward a service-oriented architecture (SOA) which provides a convenient way of deploying software as a service using web technology (Pathak et al., 2012). Although this provides new opportunities for cloud computing, such as virtualization, vendor flexibility, elasticity (scalability), and cost economies (Srinivasamurthy & Liu, 2010), it also exposes a lot of issues and challenges. According to numerous studies (Shen & Tong, 2010a; Wood, 2012) and statistical surveys by academia and professionals, a serious challenge exists in the security of cloud systems.

Cloud computing is a very complex model and, as such, different perspectives of security issues exist. Researchers believe that if the dimensions of security issues are identified, then mitigation of these threats at different levels will lead to safer and greater adoption of the cloud. This paper is positioned from both a technological and a business perspective, focusing on cloud security issues (see Table 1).

Table 1: Classification of Topics in Cloud Computing (Yang & Tate, 2012)

Topics	Subtopics
Technological Issues	Cloud Performance, Data Management, Data Centre Management, Software Development, Service Management, Security
Business Issues	Cost, Pricing, Legal Issues, Ethical Issues, Trust, Privacy, Adoption
Conceptualising Cloud Computing	Foundational/Introductions, Predictions
Domains and Applications	e-Science, e-Government, Education, Open Source, Mobile Computing, Other Domains

The next section discusses the different perspectives of cloud computing, followed by the identification and aggregation of reported security issues. The final section presents an analysis of the results of the case study, followed by a presentation of dimensions of the IS security cloud model.

PERSPECTIVES ON CLOUD COMPUTING

Although academia and practitioners agree on the core concept of cloud computing, the term has been defined from different perspectives. Cloud computing has been defined as an on-demand access model of delivering hardware and software as services over the Internet in different ways of deployment models and service models (Srinivasamurthy & Liu, 2010). According to the National Institute of Standards and Technology (NIST), cloud computing is defined as the management and provision of resources, software, applications, and information as services over the cloud (Internet) on-demand (Mell & Grance, 2009). NIST's definition of cloud computing further classifies it as having five essential characteristics, three service models, and four deployment models.

- **Essential Characteristics:** On-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service
- **Service Models:** Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)
- **Deployment Models:** Private, community, public, and hybrid cloud

Depending on the relationship between the provider and the consumer, the cloud platform can be deployed on the basis of four models; namely, private, public, community, and hybrid cloud (Dillon, Wu, & Chang, 2010a; Mell & Grance, 2009; Yang & Tate, 2012). In this respect, a private cloud is owned by a single organization or entity, whereas in a public cloud, the provider owns the infrastructure and the consumers pay for the services. On the other hand, a community cloud is a collaborative effort in which the infrastructure is shared between several organizations from a specific community and a hybrid cloud is a combination of different cloud infrastructure models. Although the deployment model differentiates the types of cloud infrastructures, the services they provide can be categorized as SaaS, PaaS, data storage as a service (DaaS), and IaaS. In SaaS, the consumers host their applications on the cloud; in PaaS, the consumers can develop their own applications; in DaaS, the consumers store the data on the cloud; and in IaaS, the consumers use the entire IT. In this paper, the authors examine the issues related to the cloud deployment model and the services, in general. Although these two dimensions of the cloud have been effective for classifying the cloud computing model, in general, Craig-Wood (2010) added another dimension (essential characteristics) and integrated these three to provide a three-dimensional view.

Another definition by Mansukhani and Zia (2011) describes cloud computing as a method for delivering information services that provides flexible use of servers, scalability, and management services, along with a unique combination of capabilities that include scalable and dynamic infrastructure, global/remote access, precision usage controls and pricing, and standard platform and support services, IT, and management. The three definitions thus present the core concept of cloud computing, which is to provide access to relevant components of IS with value-added features over the Internet for public or private use.

Issues in Cloud Computing

Statistical Trends

While there is a growing tendency toward the adoption of cloud computing by organizations, statistical analyses (Figure 1) of the challenges show an alarming trend in terms of security. International Data Corporation conducted a study of 244 IT executives, and out of the nine points raised, security was highlighted as the most serious concern by approximately 87.5% of the respondents (Balding, 2009).

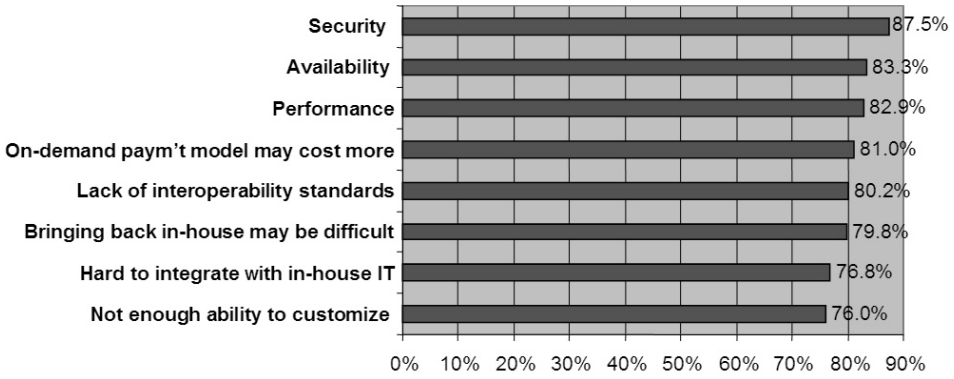

Figure 1: Challenges and Issues in Adopting Cloud Computing (Balding, 2009)

The results reveal that correspondingly, these respondents look for security attributes while choosing a cloud environment. This was substantiated by another survey (Figure 2) which reported that security was the most critical attribute that customers look for before choosing cloud computing.

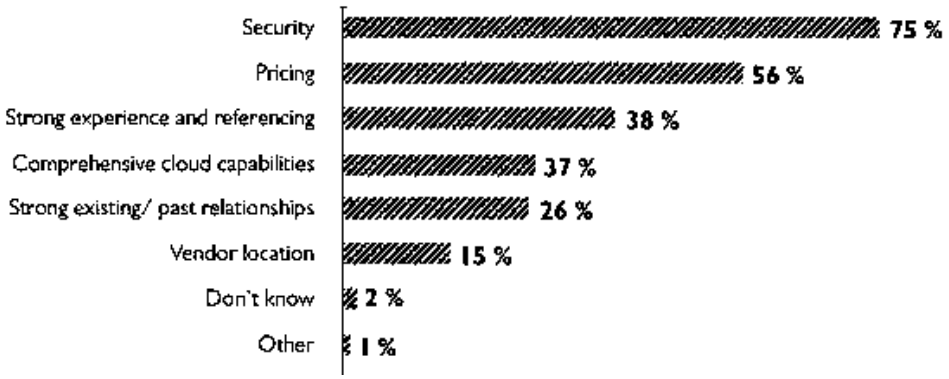

Figure 2: Attributes Respondents Look For in A Cloud Provider (Wipro Technologies, 2012)

Examining the specifics of security in cloud computing, a survey by Sophos Security revealed that attackers extended their reach to more platforms, from social networks and cloud services to Android-based mobile devices (Sophos Ltd., 2013). A Cisco survey, which included 1,300 IT professionals in 13 countries concerning challenges in adopting cloud computing, stated that during the cloud migration process, data protection security (72%) was cited as the most challenging obstacle to a successful implementation, followed by the availability and reliability of cloud applications (67%), device-based security (66%), visibility and control of applications across the wide area network (WAN) (60%), and overall application performance (60%) (Cicso, 2012). The survey also reported that if given the choice of only being able to move one application to the cloud, most respondents would choose storage, followed by Enterprise Resource Planning (comprising of applications to manage human resources (HR), customer relationship management, supply chain management, and project management systems), email and collaboration solutions (Figure 3). From the statistical analyses, the authors can observe that security is the most critical feature/attribute among other attributes in adapting cloud computing.

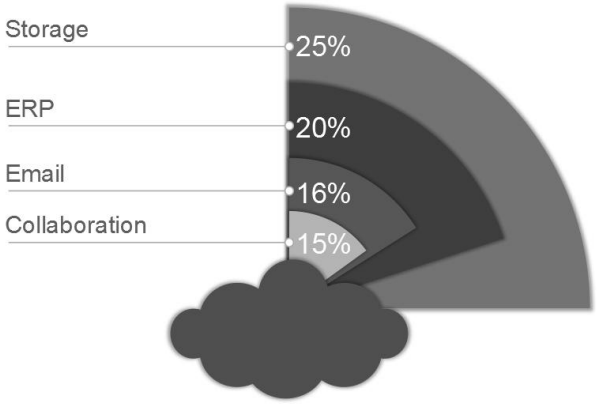

Figure 3: Services Accessed by Cloud Users (Cicso, 2012)

IS Security Issues in the Cloud

Statistical analyses present the magnitude of threats. In this section, the authors explore this further to determine the specific nature of threats facing organizations that migrate to the cloud. The authors have stated that cost-effectiveness offered by cloud computing has led to a growth in cloud interest, but data security remains the main concern (Mujinga & Chipangura, 2011). The virtualized architecture of cloud computing offers various benefits to the cloud user, but because the security of the cloud is a shared responsibility between the cloud user and the cloud provider (Mansukhani & Zia, 2011), security issues can originate from the cloud user or the provider. In this paper, the authors describe their research on the security issues facing the cloud user from the cloud provider. To focus further on the nature of security issues in cloud computing, when the NIST definition of cloud computing was analyzed, it was found that a public cloud is the predominant cloud computing deployment model (Dillon, Wu, & Chang, 2010b).

Security in the cloud has become a critical issue because of the widespread usage of distributed systems and network computing (Shen & Tong, 2010b). Hence, security in the cloud environment emerged as the most significant barrier to faster and more widespread adoption of cloud computing (Chen, Paxson, & Katz, 2010). IS security issues and threats in cloud computing have been researched from various perspectives. Srinivasamurthy and Liu (2010) listed the top seven security threats and Subashini and Kavitha (2011) examined the security issues from a cloud platform perspective (SaaS, PaaS, and IaaS). Zissis and Lekkas (2012) classified the threats from the perspectives of service-level, user, and security requirements. Ramgovind, Eloff, and Smith (2010) looked at the different types of concerns from a requirements perspective; namely; risk assessment, IS requirements, policies and guidelines, service-level agreements (SLAs), data protection, governance, monitor, and control. To view the threats from a broader perspective, the authors aggregated and identified 41 threats facing cloud users (see Table 2) to provide a more comprehensive view of cloud security.

Even though the numerous issues in cloud computing have been researched from various perspectives, a precise definition of threats is lacking in this domain, thus making it difficult for practitioners to focus on the exact nature of these threats. The listed threats include various combinations such as vulnerabilities (e.g., SQL injection flaws, access control weakness), generic threats (e.g., natural disasters, misuse of infrastructure), and technical threats (e.g., cookie manipulation, hidden field manipulation). Hence, a meaningful overview of threats is required to classify threats specific to the different dimensions of cloud computing. For example, if the authors take the cloud deployment model, the nature and gravity of threats differ between the various cloud deployment and service models, as there are several critical security challenges for the commercial public cloud (Ren, Wang, & Wang, 2012). Furthermore, a public cloud poses a major risk, whereas a private cloud seems to have lesser impact (Subashini & Kavitha, 2011). Likewise, the service models (SaaS, PaaS, and IaaS) also place a different level of security requirement in the cloud environment (ibid).

Table 2: IS Security Threats in the Cloud Computing Domain

No.	Threats	Dimitrios Zissis & Dimitrios Lekkas	S. Subashini & V. Kavitha	Shilpashree Srinivasamurthy & David Q. Liu
1	Interception	X		
2	Modification of data at rest and in transit	X		
3	Privacy Breach	X		
4	Impersonation	X		
5	Session Hijacking	X		X
6	Traffic Flow Analysis	X		
7	Exposure in Network	X		
8	Defacement	X		
9	DDOS	X		
10	Disrupting Communications	X		
11	Programming Flaws	X		
12	Software Modification	X		
13	Software Interruption (deletion)	X		
14	Network Attacks	X		
15	Connection Flooding	X		
16	Hardware Interruption	X		
17	Hardware Theft	X		
18	Hardware Modification	X		
19	Misuse of Infrastructure	X		
20	Natural Disasters	X		
21	Data Security	X	X	X
22	Network Security		X	
23	Data Locality		X	
24	Data Integrity		X	
25	Data Segregation		X	
26	Data Access		X	
27	Authentication and Authorization		X	
28	Hidden Field Manipulation		X	
29	Access Control Weaknesses		X	
30	Cookie Manipulation		X	
31	SQL Injection Flaws		X	
32	Session Management		X	
33	Identity Management and Sign-on Process		X	
34	Virtualization Vulnerability		X	X
35	Insecure Storage Configuration		X	
36	Intrusion of Data		X	
37	Insufficient Transport Layer Protection		X	
38	Abuse and Nefarious Use of Cloud Computing			X
39	Insecure Application Programming Interfaces			X
40	Malicious Insiders			X
41	Unknown Risk Profile			X

Cloud computing has been classified on the basis of research (Yang & Tate, 2012) and definition (Mell & Grance, 2009). From a security perspective, cloud computing has been classified on the basis of service model, user, and security requirements (Zissis and Lekkas, 2012), and Subashini and Kavitha (2011) provided a two-dimensional complexity of security in cloud environment. Therefore, because of the limited research in classifying cloud security issues, a comprehensive classification of the type of cloud security threats based on deployment and service level models is lacking. The predominance of security issues in cloud computing, coupled with the lack of categorization of these issues, directs us to the exploratory research question, *What are the different dimensions of IS security threats in cloud computing?*

RESEARCH METHODOLOGY

This study is exploratory in nature and, as such, the authors chose a case study research approach. Furthermore, a case study is regarded as a "common way to do qualitative enquiry" (Stake, 2003, p. 443) and "investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 1994, p. 13). Because the listed threats may not be comprehensive and need to be explored further, it was deemed imperative to conduct exploratory research through interviews. In addition, to appropriately define these threats, they must be correlated into their respective categories. This necessitates delving deep into this domain, thus justifying the chosen methodology. In order to explore these issues further and to map the issues into their respective categories to validate the taxonomy, the authors decided to conduct an interview with an IT manager who handles cloud computing in an organization.

ANALYSIS

Organizations that use any two of the cloud deployment models were sourced and contacted. Out of the few organizations contacted, only one organization agreed to the request for an interview. It is a media company in the United Arab Emirates that utilizes both a private and a public cloud for its IS requirements. Regarding the company's IT infrastructure, 70% of its servers are virtualized. The respondent is the IT Manager of the organization. He is an ISO 27000, ISO 20000, and ISO 22301 Certified Lead Auditor. He is also an ITIL Expert, with CGEIT Certification, IT Governance Certified in COBIT 4.1, a Cloud Computing Associate, and TOGAF 9.1 professional with 23 years of experience in the IT industry. Because he deals with the cloud service, the authors found it appropriate to interview him. The respondent was shown the 41 threats and was asked to comment on the nature and dimensions of threats that his company faces in cloud computing. The responses were digitally recorded and transcribed and exported into NVIVO and the nodes were extracted on the basis of existing and new themes. From the analysis of the nodes, the following major themes emerged:

- Reasons for the company to go for cloud computing
- Definition of threats in cloud computing
- NIST classification of cloud computing
- Process of analyzing IS security cloud Issues
- Evaluation of threat identified from the literature
- Threats in cloud computing—technical perspective
- Threats in cloud computing—business perspective

Drivers for Cloud Computing

There are major drivers for the company to choose cloud computing. It deploys and uses both a public and a private cloud. For the private cloud, the two major drivers were to improve business continuity for which they have a target of 99.99% (which is independent of the hardware) and to reduce the operational cost by utilizing the disaster recovery site.

For the public cloud, which is hosted outside the country, the major drivers were the high bandwidth available from the external service provider and the huge amount of audio and video data (being a media company) that needs to be accessed. The company uses SaaS service for live streaming and for the video-on-demand portal, because the local internet service provider cannot support the high bandwidth. Hence, here the use of a public cloud is out of necessity rather than choice.

Definition of Threat

The respondent stated that IT personnel tend to look into threats from "different points of view" because of the different perspectives of the definition of threats and, thus, they tend to highly disagree on the number of existing threats (commonalities). In addition, he mentioned that the threats, vulnerabilities and risks, do not exist in siloes but overlap with each other, and currently there is no common agreement on what is regarded as threats in cloud computing.

According to the respondent, the differing points of views are due to the vulnerabilities and risks (referring to the listed threats). He also stated that these threats need to be specified to better understand their nature and, consequently, redefine the threat paradigm.

NIST Classification of Cloud Computing

According to the respondent, threats in cloud computing cannot be classified according to the service or deployment model because categorizing threats on the basis of SaaS, PaaS, or IaaS is not relevant. Hence, the threats need to be looked at from a business or customer perspective rather than the technology used. The cloud itself is defined as SaaS, PaaS, and IaaS, because there are public, private, hybrid, and community deployment models. It is very difficult to classify threats according to these service levels and deployment models because, in a single cloud environment, you might have a PaaS, with a private deployment model with a partial public environment, and accordingly it might be considered as hybrid. Therefore, threats overlap within these levels and models.

- *Cloud Deployment Model:* Perceiving security issues from a cloud deployment model, the respondent stated that he only considers a public and private cloud when it comes to security because a hybrid and community cloud has elements of both a public and private cloud and the inclusion of a hybrid and community cloud may distort the classification. Technically speaking, "There is nothing called hybrid cloud as it is a combination", and for a community cloud, the only factor is the "type of community, and this does not make it technically different for threat perspective."
- *Service Levels:* From a security perspective, customers (in this case, organizations that avail of cloud service) do not care whether it is Saas, PaaS, or IaaS or private or public because as a customer, they look at security and not technology, as each vendor will have its own types of threats. According to the respondent, categorizing threats on the basis of SaaS, PaaS, or IaaS is not relevant because the threats need to be perceived from a business or customer perspective, rather than a technology perspective.

Process of Analyzing IS Security Cloud Issues

The respondent suggested that the process of cloud computing threat analysis (Figure 4) has six stages. The first considers the requirements in terms of the cloud service in which the company has to decide the nature of the service it requires from the cloud. Second, the company must examine the cloud offering and match the requirement with the offering. The third stage involves undertaking a business impact analysis study because the business impact and risk assessment mechanisms are highly considered in the case of the cloud concept. The fourth stage is the risk analysis which involves a series of substeps; namely, identifying the assets/services, differentiating/categorizing the assets from the business perspective, valuation of the assets, and linking these to the infrastructure. The fifth stage involves exploring the vulnerabilities, which subsequently aids in identifying the threats (sixth stage).

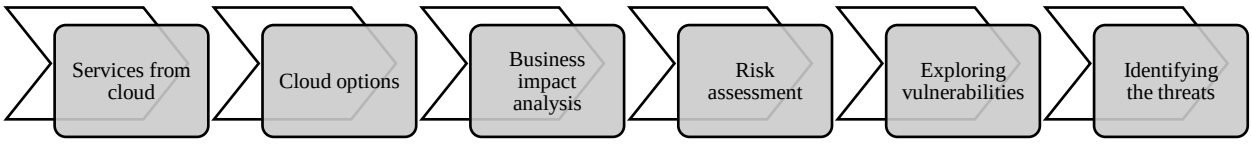

Figure 4: Process of Identifying Threats in Cloud Computing

Threats Identified from the Literature

Regarding the threats sourced from the literature, the respondent believes that there is no agreement on the definition of threats. He also thinks the list is not specific where some vulnerabilities and risks have been identified as threats. In addition, he believes the threats need to be more defined from a contextual perspective. The respondent does not agree on the listed threats, as he stated that the threat is much more than those listed in the literature and it is not feasible to list all the threats.

Threats in Cloud Computing—Technical Perspective

Regarding the technical threats, the respondent stated that the list was not sufficiently exhaustive, and if he were to consider all of the risks, threats, and vulnerabilities from a technical perspective, he could probably add approximately 500 different items. The respondent also stated that some threats are common to all public and online services, such as distributed denial of service (DDoS) attacks and thus, they are not specific only to the cloud. Hence, some of the identified threats are not specific to cloud computing. In addition, he believes that a more generic term needs to be used for DDoS in a cloud environment, which is 'service discontinuity' because this term will have much more vulnerabilities than DoS. According to him, "For example, there are more than ten types of DDoS attacks and you do not want to go deep into that and your job is to make sure the continuity of the connection", which is defining threat from a business perspective. Illustrating the case of a SQL injection attack, he said that he "may not have a SQL server on the cloud or the database at all, on that particular service that I am having on the cloud." Moreover, DDoS attacks are common to all public and online services, and thus, they are not specific to the cloud only. Therefore, the types of threats in cloud computing need to be redefined because the above 41 threats are not the concern of the company, but to the cloud service provider.

Regarding preventing the listed threats, the respondent suggested three options to reduce the threats:

- The use of intrusion prevention and firewalls
- The use of encryption technology in both communication and hardware
- Infrastructure update and patching, which are crucial for private cloud security

Threats in Cloud Computing—Business Perspective

According to the respondent, the threats have to be considered from the business perspective because it is driven by business requirements as new threats in cloud computing emerge when viewed from a business perspective. Moreover, there are situations where the threat from an IT perspective is not regarded as a threat from a business perspective. Considering threats from a business perspective is more important than the technical perspective because if a company selects a vendor to provide a cloud service (SaaS—public cloud), it will be more concerned about the vendor reputation, the business model it uses, the revenue, and continuity in the business, rather than the technical issues. When the threats are viewed from the business perspective of the organization, this focuses the threats from the business impact analysis from which the company drives its priorities, which eventually give rise to the risks assessment and then the threats. Some of the threats from a business perspective are explained below

- *Physical Security:* The example given is based on the theft of equipment where the respondent said that the location of the datacenter needs risk assessment where the vulnerabilities have to be identified to arrive at the threats. In the case of Japan, the threat is natural disaster (earthquake), whereas in India, Europe, or other countries/areas, the local competitor can use the cloud with the same provider who also provides cloud services for a UAE company and that leads to threat of a cloud provider insider to manipulate the data or steal it in favor of the competitor.
- *Service Discontinuity:* Internet connection is a threat because this is the core basis of a virtual service. Moreover, if one considers a threat, such as a DDoS attack, in a cloud environment, the more generic term is service discontinuity, because this term will encompass more vulnerabilities than DoS. This is because there are more than ten types of DDoS attacks and it makes no sense to analyze the nature of DDoS attack, as the IT manager's job is to ensure continuity of the connection. This again is defining threat from a business perspective.
- *Cost of Connection:* This can be a threat and a bottleneck while choosing the bandwidth, which will affect the service response in the cloud environment.
- *Cloud Service Provider's Changing Profile:* Company profile of the vendor is an important aspect. For example, if a company links with a specific vendor—a small cloud provider—and eventually if it is going to be acquired by another company, then the company profile will be a major aspect to consider. Also important is the continuity of the service. For example, the respondent said that when his company develops its own applications on certain platforms (PaaS), and if it builds its business applications on

Sharepoint, then the business profile of Microsoft is of much concern. If the company changes the platform, it is more concerned about the risk of losing certain features that it is currently using.

- *Confidentiality of Information:* If the company uses SaaS and uses the email service with Google (to reduce the cost) and in the future considers the information in emails as very sensitive, then cost will become secondary because the company will consider moving the email from Google to the company cloud. Here again, the threat is based on confidentiality of information. Before listing the threat, one has to understand the value of the information that needs to be protected because the threat depends on the value of the information. A business perspective of threat is important because of the threat level. Here again, the threat to sensitive information is much more than it is to irrelevant information because hackers are not interested in information that is of no value.
- *Compliance Aspect of The Cloud Service Provider:* If the company is using IaaS, then the priority is to examine the compliance of the provider in relation to ISO 27000 because the company has to worry more about the internal operations of the vendor, as it depends on the vendor's infrastructure. Hence, the company must ensure that the vendor has implemented ISO 27001 with all the relevant controls. SLAs, compliance with IT controls in ISO 27000, and frameworks such as Cobit, play a vital role in deciding the cloud provider.
- *Internal Threat:* In a private cloud, looking at the threats is irrelevant because a single entity is responsible for the security, regardless of the service or platform used. In the case of a private cloud, regardless of it being SaaS, PaaS, or IaaS, it is the responsibility of the company to maintain security under the same business umbrella. Here, it is irrelevant to view threats from a SaaS, PaaS, or IaaS perspective because the cloud user views the entire package implemented across the organization. According to the respondent, the user needs to undertake risk assessment by examining the service catalog and relating his service catalog to the business risk assessment from the business perspective, which is crucial for each and every service. For example, email might be critical to one organization but not be critical to another one.
- *Change of Vendor:* This happens if the customer wants to move from one provider to another. In this case, the threat arises if the company does not have the option to move from one vendor to another.
- *Business Impact:* The impact of loss of data for business is a major threat. For example, a customer relationship management database might be sensitive for a cloud provider serving a government or for an online business that contains financial information of customers. This is a case of business impact.
- *Threat Transference:* Sometimes a business may accept the risk on the basis of an SLA. There was an instance in the respondent's organization, where the IT department proposed a redundant link between the headquarters and the disaster recovery site, to which management refused, saying that it is the responsibility of the ISP (Etisalat) and the company accepted the risk because the company has a solid SLA with Etisalat, who is providing the link, which is the concern of Etisalat rather than the organization. Thus, this is a case of threat transference.
- *Business Continuity:* Business continuity in the case of failover and a backup plan in the case of disaster recovery should also be considered as a threat in the cloud environment.

Dimensions of Threat

From the analysis of the responses, it was observed that IS security threats in cloud computing must be considered from both a business and a technical perspective. Threats that are perceived to be technical in nature can be viewed from a business perspective in cloud computing. Some threats (technical as well as business) are common to the entire IS, in general, whereas others are specific only to cloud computing. Furthermore, threats overlap with each of the two dimensions such that threats can be business as well as technical in nature. Likewise, the common threats in one scenario can be specific to another scenario. Hence, taking this into consideration, the threats can be positioned at any coordinates of the two dimensions to denote the relative weight of each of the four quadrants. Incorporating the various dimensions of threats, the ensuring model, which the authors termed the Cloud Computing Thread Matrix, is presented in Figure 5.

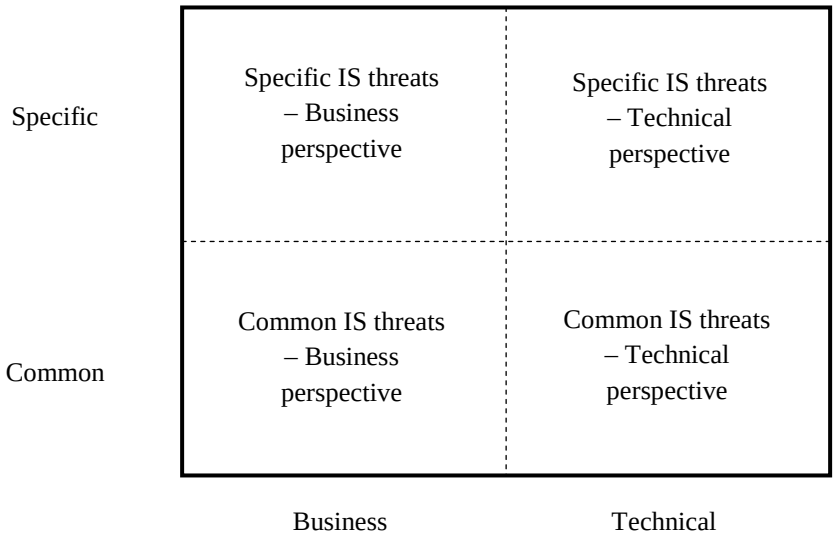

Figure 5: Cloud Computing Threat Matrix—Dimensions of IS Security Threats in Cloud Computing

CONCLUSION

The growth of cloud computing as a new way of delivering diversified computing resources using different service models and technologies with value-added benefits to its users is not without its threats. Despite its positive characteristics, it also brings new security issues and challenges, which can, if unchecked, hinder the effective utilization of IS resources. Although numerous threats have been listed in the literature, in this study the authors developed a two-dimensional matrix for categorizing and positioning the IS security threats in cloud computing to provide an accurate definition of threats from the different perspectives.

This study is not without its limitations, which highlights several directions for further research. First, additional studies in different contexts (business sectors and organizational size) are needed to generalize the findings. Second, further research could explore a list of threats and map them (along with the existing threats from the literature) into the four quadrants to validate this model. Third, the threats could be quantified by placing a value of 0.0 to 9.0, with the x axis and y axis as coordinates to position the threats in its respective quadrants. Finally, more intensive research can add a third dimension.

AUTHOR INFORMATION

Mathew Nicho is an assistant professor and Director of the MSc program at the College of Information Technology of the University of Dubai. He holds a master's degree and a PhD from Auckland University of Technology, New Zealand. He researches and publishes in the area of information security, IT governance, audit, and assurance. His work has appeared in international journals, books, and referred conference proceedings. E-mail: mathewnicho@gmail.com (Corresponding author)

Mahmoud El Hendy is a master's student (MSc in Information Systems Management) at the University of Dubai, Dubai, UAE. He has worked in a different organization in the IT sectors as Systems Administrator, Web developer, and IT consultant. His areas of interests are mainly cloud computing and IT security. He is certified in ethical hacking and is currently working at the University of Dubai.

REFERENCES

1. Balding, C. (2009). New IDC IT Cloud Services Survey: Top Benefits and Challenges. Retrieved December, 2012, from http://cloudsecurity.org/blog/2008/10/14/biggest-cloud-challenge-security.html

2. Chen, Y., Paxson, V., & Katz, R. H. (2010). What's New About Cloud Computing Security? (Vol. 20, pp. 2010-2015). Berkeley: University of California.
3. Cicso. (2012). Cisco Global Cloud Networking Survey. Retrieved December, 2012, from http://www.cisco.com/en/US/solutions/ns1015/2012_Cisco_Global_Cloud_Networking_Survey_Results.pdf
4. Craig-Wood, K. (2010). Definition of Cloud Computing, Incorporating NIST and G-Cloud Views. http://www.katescomment.com/definition-of-cloud-computing-nist-g-cloud/
5. Dillon, T., Wu, C., & Chang, E. (2010a). Cloud Computing: Issues and Challenges. Paper presented at the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA) Perth, Australia.
6. Dillon, T., Wu, C., & Chang, E. (2010b). Cloud Computing: Issues and Challenges. Paper presented at the 24th IEEE International Conference on Advanced Information Networking and Applications, Perth, Australia.
7. Lawler, J., Joseph, A., & Howell-Barber, H. (2012). A Case Study of Determinants of an Effective Cloud Computing Strategy. *Review of Business Information Systems, 16*(3), 145-156.
8. Mansukhani, B., & Zia, T. A. (2011). An Empirical Study of Challenges in Managing the Security in Cloud Computing. Paper presented at the 9th Australian Information Security Management Conference, Perth Western Australia.
9. Mell, P., & Grance, T. (2009). Draft NIST Working Definition of Cloud Computing. Referenced on June. 3rd. Gaithersburg: NIST.
10. Mujinga, M., & Chipangura, B. (2011). Cloud Computing Concerns in Developing Economies. Paper presented at the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia.
11. Pathak, B., Rajesh, S., Jain, S., Saxena, A., Mahajan, R., & Joshi, R. (2012). Private Cloud Initiatives Using Bioinformatics Resources and Applications Facility (BRAF). *International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2*(6), 25-34.
12. Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The Management of Security in Cloud Computing. Paper presented at the Information Security for South Africa (ISSA), Johannesburg.
13. Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *IEEE Internet Computing, 16*(1), 69-73.
14. Shen, Z., & Tong, Q. (2010a). *The Security of Cloud Computing System enabled by Trusted Computing Technology*. Paper presented at the 2010 2nd International Conference on Signal Processing Systems (ICSPS), Dalian, China.
15. Shen, Z., & Tong, Q. (2010b). The Security of Cloud Computing System Enabled by Trusted Computing Technology. Paper presented at the 2nd International Conference on Signal Processing Systems (ICSPS) Dalian, China.
16. Sophos Ltd. (2013). Sophos Security Threat Report 2013. Retrieved April, 2013, from http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf
17. Srinivasamurthy, S., & Liu, D. Q. (2010). Survey on Cloud Computing Security–Technical Report Department of Computer Science, Indiana University Purdue University Fort Wayne. Fort Wayne: Indiana University Purdue University.
18. Stake, R. E. (2003). Qualitative Case Studies. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage Handbook of Qualitative Research* (443 p.). California: Sage Publications.
19. 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.
20. Wipro Technologies. (2012). Cloud Potential the Opportunity to Invent and Reinvent Business. Retrieved December, 2012, from http://www.wipro.com/Documents/insights/Cloud_Potential.pdf
21. Wood, K. (2012). Exploring Security Issues in Cloud Computing. Paper presented at the UK Academy for Information Systems Conference, New College, Oxford, UK.
22. Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems, 31*(1), 2.
23. Yin, R. K. (1994). *Case Study Research: Design and Methods* (2nd ed.). Thousand Oaks: Sage Publications, Inc.

24. Zissis, D., & Lekkas, D. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems, 28*, 583-592.

