Journal of Electronic Commerce Research, VOL 12, NO 4, 2011

THE IMPACT OF SECURITY AND SCALABILITY OF CLOUD SERVICE ON SUPPLY CHAIN PERFORMANCE

Olatunde A. Durowoju
NorwichBusinessSchool, University of East Anglia
Norwich, NR4 7JT, UK
O.Durowoju@uea.ac.uk

Hing Kai Chan
NorwichBusinessSchool, University of East Anglia
Norwich, NR4 7JT, UK
H.Chan@uea.ac.uk

Xiaojun Wang
School of Economics, Finance and Management, University of Bristol
Bristol, BS8 1TN, UK
Xiaojun.wang@bristol.ac.uk

ABSTRACT

Cloud computing introduces flexibility in the way an organization conducts its business. On the other hand, it is advisable for organizations to select cloud service partners based on how prepared they are owing to the uncertainties present in the cloud. This study is a conceptual research which investigates the impact of some of these uncertainties and flexibilities embellished in the cloud. First, we look at the assessment of security and how it can impact the supply chain operations using entropy as an assessment tool. Based on queuing theory, we look at how scalability can moderate the relationship between cloud service and the purported benefits. We aim to show that cloud service can only prove beneficial to supply partners under a highly secured, highly scalable computing environment and hope to lend credence to the need for system thinking as well as strategic thinking when making cloud service adoption decisions.

Keywords: cloud service, security concerns, scalability, supply chain management

1. Introduction

The internet has been employed in multidimensional and multifaceted ways in various supply chains. Lancioni et al [2003] found there to be an increase in the use of the internet by organizations to leverage supply chain management applications. The significance of the internet owes to its ubiquity and provisioning of real time communication. Irrespective of the type of supply chain, the internet has proven to be limitless in the purpose it can serve provided its use had been carefully or strategically planned [Wang et al., 2004]. Its use has ranged from communication information exchange to more operational related functions such as order filling, purchasing, production scheduling, customer service, human resource management etc. [Chen and Meixell, 2003]. Leveraging Information Technology (IT) can be costly and has deterred small to medium scale organizations from using it. This in part has led to the emergence and justification for the somewhat new IT concept called 'cloud computing'.

Cloud services bring flexibility, configurability, cost effectiveness, low implementation cost to IT and by extension, Supply Chain Management (SCM). Many IT experts and academics have reported a plethora of benefits an organization stands to gain if and when they avail themselves to this opportunity. In the same vein there has been a series of counter argument about the purported benefits of joining the cloud. However, as is common to most IT initiatives, a careful analysis of how it will affect one's internal and external business environment must be undertaken before adopting the strategy, otherwise it can be the bane of a business existence. Top amongst these counter arguments are the issues of security [Subashini and Kavitha, 2011] and ability to scale up or down computing resources as needed without making service unavailable [Armbrust, 2010].

Most of these reports, although anecdotal, have been viewed from the cloud provider's perspective. There has been paucity of report on how these issues affect cloud users (in this case supply chain members), which have been mostly studied at an organization level. There is yet to be an academic research on how these issues affect the

operations of an entire supply network. This study proposes an approach, which incorporates a system thinking perspective, to investigate how some of these issues, especially security and scalability, affect businesses at an organizational level and supply chain level. By looking at the impact of these variables on supply chain performance, the research posits that this will inform an appropriate cloud computing adoption strategy to suit the overall organization and supply chain management goal.

Security is conceptualized as one of the uncertainties present in the cloud. It is defined here as the level of defence against IT threats as evidenced by the probability of breach occurrence. To remove any form of ambiguity, a breach is defined as the incidence or occurrence of a particular IT threat[1] compromising the integrity, confidentiality or availability of information needed for daily operations. Studies which have investigated the impact of security breach have been largely qualitative and confined to individual organization. These studies are quite subjective and lack consistency. There is no quantitative study in literature that has investigated the impact of IT threat-type incidences on the supply chain using purely objective approach. This study will fill this important gap by conducting a quantitative assessment of risks to information security and provide knowledge on how the incidence of these threats may affect the operations of the supply chain.

One of the flexibilities that the cloud purports to offer is the ability to increase or decrease computing power as required by the user. This is referred to as scalability. Scalability is defined here as the ease of ensuring just the right amount of computing power is available to the cloud user at any point in time. While it is intuitive that the inability to be flexible in terms of dynamically scaling computing resources will result in poor performance of the cloud-enabled business, it is not evidenced from literature how this will affect other organizations linked to the business. This study proposes a way of assessing this impact.

This research intends to be an opening contribution to the quantitative study on the impact of cloud computing features (such as scalability) and uncertainties (security risk[2]) on supply chain management. We offer a methodology with which cloud users can assess cloud partners based on their security level and their resource scaling power.

2. Literature Review

2.1. Cloud Computing and Cloud Service

The emerging trend of enabling IT systems on the platform of cloud computing has been a subject of discuss in recent years. There have been several discussions in the literature as to the suitability and flexibility of cloud computing strategy. Many have offered various definitions of the concept. Some define it according to its functionality while others have looked at its applicability. At the most basic definition, cloud computing entails using computing resources such as computer applications and programmes over the internet as opposed to license-and-install on the desktop [Buttell, 2010]. It is easier to understand the concept and how it can be successfully adopted when we define it according to its functionality as well as its applicability. A purely functional definition of cloud computing is that it is a way of accessing hardware or software resources, or a combination of both, anywhere in the world by an organization or an individual via the internet [Amir, 2009, Armbrust et al. , 2010, Smith, 2009]. These resources are shared amongst many users, abstracted, available on demand, scalable, and configurable [Marston et al. , 2011]. The service provided by cloud computing is referred to as cloud service in this paper.

Although this is not an entirely new concept, its unique feature where resources are pulled as opposed to being pushed makes it a more promising concept than its predecessors; time sharing in the 1960s and application hosting in the 1980s [Amir, 2009, Cusumano, 2010]. However there exists a need to examine its impact on business operations and treat it as a strategic tool rather than merely 'the new way of computing'. As like many other IT concept, its adoption must be duly informed, otherwise it may spell disaster for whosoever rushes into it. A good understanding of the internal and external business environment coupled with an understanding of the pertinent concerns over moving to the cloud would be the bedrock of successful adoption of cloud service.

Its applicability would entail seeing this concept being delivered over different service configurations. There are three basic service configurations also known as cloud service models which are Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In SaaS, the cloud user buys the right to use a working application hosted by an external provider via the internet. The PaaS model involves the use of an externally provided infrastructure to host the application, while IaaS model requires the use of servers provided externally for raw computing, storage and network transfers [Durkee, 2010, Subashini and Kavitha, 2011]. We can also look at the scope of the service whether it is purely open to the public (Public Cloud) or restricted to certain

[1] An event or action that can potentially inflict harm or damage to the functioning of an IT system.

[2] The chance of a threat (in this case Information Technology (IT) security breach) occurring having either a negative or positive impact on a firm or supply chain.

users (Private Cloud) or a combination of both (Hybrid Cloud). Some have argued that the cloud concept cannot be anything short of public access since cloud by definition entails external providers in an open computing environment [Orange and Cohen, 2009, Ryan, 2011]. Although private clouds purports to have tighter security and boast greater reliability, they are argued to be quite costly and lack the financial incentive to encourage small to medium firms to adopt [Orange and Cohen, 2009]. This in principle defies the concept of the cloud. Therefore for the purpose of this research, public cloud has been opted to use in the definition of cloud computing. We however accept the definition offered by [Seccombe et al., 2009] describing cloud computing as "the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption."

The discussions on cloud computing have been multifaceted and multivariate. At an anecdotal level, several articles have discussed the benefits of adopting cloud computing [Buttell, 2010, Kefer, 2010, Marston et al. , 2011, Smith, 2009] and others have raised numerous concerns [Cusumano, 2010, Durkee, 2010, Ryan, 2011, Smith, 2010, Smith, 2009] while some have suggested important factors to consider in selecting cloud service providers [Cakebread, 2010, Pendergraft, 2010]. Some conceptual studies have been done on a range of its application which is viewed from the service provider's perspective and from the user's perspective. However not many research has been done on the dynamics of cloud computing and how it affects the supply chain. A recent study by Marston et al. [2011] is one of the very few studies that have looked at cloud computing from the business perspective. However they have only reinforced the prevalence of these concerns and offered recommendations to practitioners. There still exists a need to understand, using real evidence and not anecdotes, how these issues affect an organization that adopts cloud computing strategy. Our research intends to fill this gap and provide real evidence to examine the impact of these issues on the performance of supply chains adopting the concept.

2.2. Benefits of Cloud Computing and Service

The key driver of cloud computing is the internet. Service providers and cloud users are linked together by the internet. It is the vehicle upon which service is provided. Nugent and Raisinghani [2002] found that more people are interconnected than in previous years and this trend will continue due to advancement in technology and internet growth. At an organizational level, Lancioni et al. [2003] found that in 2001 the internet is being applied in the areas of purchasing/procurement; inventory management; transportation; order processing; customer service; production scheduling; and vendor relations, with procurement, transportation, and customer service having the most internet usage and has established that . However it is clear from literature that exchange of information drives business efficiency and effectiveness [Chan and Chan, 2010].

Cloud computing have several benefits over traditional IT models reported in literature. Cloud services bring flexibility, configurability, cost effectiveness, low implementation cost to IT and SCM. Primarily it offers a cost advantage to firms especially the small to medium scale enterprises who otherwise cannot afford the huge financial commitment required for deploying typical cutting edge enterprise-level IT such as Enterprise Resource Planning (ERP) systems, [Marston et al., 2011]. This is achieved through the metering system based on the notion of "pay as you go".

Various hardware and/or software resources can be combined, separated and recombined by organizations as they so please. Thus an organization might purchase specific software components from Oracle, SAP, Apple or any other software provider and link them together via the cloud to create a business solution [Amir, 2009]. This configurability in the cloud makes it a more attractive solution to many businesses than other IT models such as stand-alone web services. Another benefit is the scalability feature that it has. As demand for computing changes, the necessary computing power can be dynamically increased or decreased to meet the change in demand. Thus organizations can pay for what is needed and get rid of unnecessary resources. All of these make computing in the cloud very attractive and facilitate flexibility in the way business is conducted. This concept has been extended to manufacturing where product design, manufacturing, testing, management, and all other stages of a product life cycle are encapsulated into cloud services and managed centrally [Xu, 2012]. This is similar in principle to (but not the same as) distributed manufacturing. Other benefits includes taking away associated costs of IT such as; system upgrades; recruiting and training IT staff; equipment delivery and installation; or modification of IT facility, from the Cloud user [Smith, 2009]. It also helps to prevent the loss that would otherwise be incurred when an organization is unsuccessful in deploying an expensive in-house information system (IS). This is because its flexible feature makes it possible to change from one cloud service provider to another without any major cost to the user. If a service provider does not deliver an agreed level of quality of service (QoS), the service user may change to another provider offering a better or even cheaper service. These advantageous features of Cloud computing can help organizations or supply chains to be lean, agile or le-agile, responding effectively to demand.

Li et al. [2006] surmised that the advantage of using Inter-organizational Information Systems (IOISs) does not only come from efficient transaction processing and improved monitoring and information processing capacity as previous studies indicate, but also from sharing and improved access to key business information. Several studies in the literature has shown that sharing information is important in supply chains however, the derived benefits only come under the right conditions of: right information being shared at the right time in the right format by the right entities within the right environment [Huang and Lin, 2010]. Information quality plays a pivotal role in the success of collaborative practices, and this is due to quality factors such as timeliness, accuracy, relevance and added value of the shared information [Frank, 2010].

2.3. Concerns for Cloud Service Adoption

As there are benefits for adopting cloud service, so are there concerns. These concerns come under the broad headings of security [Hitchings, 1995, Kim et al. , 2011, Rees et al. , 2011, Ryan, 2011, Subashini and Kavitha, 2011, Ulrich and Oliver, 2008, Warren, 2000, Whitman, 2003], QoS [Durkee, 2010], service availability [Armbrust et al. , 2010, Smith, 2009, Son and Kim, 2004], data liberality (which we also termed here as migrability) [Armbrust et al. , 2010, Fitzpatrick and Lueck, 2010] and scalability (which refers to ease and speed of provisioning and de-provisioning) [2010, Dutta and VanderMeer, 2011, Marston et al. , 2011]. Top amongst these concerns are security and scalability.

Security concerns as it relates to information sharing are privacy, protection of proprietary information, preservation of the quality of information. As security breach comes in various forms, the quality of information or even the accessibility to information can be compromised. This may result in delayed transmission which might reduce the relevance or value of the information, or altogether jeopardize the accuracy of the shared information. It is clear from the recent Sony's PlayStation Network (PSN) security breach incidence that organizations need to understand the impact security incidences will have on their operations by performing a pre-assessment of threats they are exposed to. Some experts opined that Sony was not prepared for such an attack and did not respond to the breach adequately and did not warn their consumers soon enough [Newman, 2011, Pollack, 2011]. It is therefore presumable that perhaps if Sony had made an adequate assessment of the impact of hacking incidence before it occurred; it would have formulated the right mix of risk prevention, mitigation and recovery strategies in the event of an attack. A recent survey done by PricewaterhouseCoopers in conjunction with Infosecurity Europe, under the auspices of the Department for Business Innovation and Skills (BIS), called The Information Security Breach Survey (ISBS) 2010 reported some security breaches experienced by various organizations. These include: Systems failure or data corruption; Infection by viruses or malicious software; Theft or fraud involving computers; other incidents caused by staff; attacks by unauthorised outsider including hacking attempts [Potter and Beard, 2010]. These breaches can be grouped under internal-based, external-based or platform-based. The internal based security breaches are those resulting from deliberate or in deliberate actions of staff and members of the organization. External –based breaches include those perpetrated by outsiders who are not members or staff of the business. This security breach can be worm; virus or malicious software attack. It can also be password sniffing/cracking software; spoofing (either IP spoofing or web spoofing) attack, denial of service attack (email bomb attack or Ping O'Death), or direct attack (hacking) [Warren, 2000]. Lastly the Platform-based incidences are caused by the service provider. Examples of this include; systems failure or data corruption resulting from poor resource management or over committing computing resources [Durkee, 2010], policy violations or physical damage or theft of the resources. A survey done by Verizon Risk team joined by United States Secret Service (USSS) revealed that 70% of data breach was caused by external agents, 48% by insiders and 11% implicated business partners [Baker et al. , 2010].

Rees et al. [2011] described three types of losses an organization faces when they experience data breach: damage to a company's image, regulatory fines e.g. fines paid to Health Insurance Portability and Accountability Act (HIPAA) due to non-compliance to regulation, and production losses as a result of disruption in production's IT support. The average cost of the worst incidence of security breach in 2010 was between £280k and £690k for large organizations (>250 staff) and between £27.5k and £55k for small organizations (<50 staff) [Potter and Beard, 2010]. According to *Tom Pisello, the CEO of Orlando-based Alinean* which specializes in ROI consultancy, historical data reveals that the most costly breaches are data destruction or damage and theft or disclosure with the average cost of responding to it and resolving it take more than 120 hours of IT staff time and an estimated cost of $350k [Pisello, 2004]. The onus of ensuring adequate security falls on the cloud user, the cloud provider and any third party security provider [Armbrust et al. , 2010].

Financial impact of security risk has been studied by multiplying the probability of a breach occurring by a pre-assessed cost impact it will have on the organization when it occurs. There are two kinds of probabilities, the objective and the subjective probabilities [Horton, 2004]. Objective interpretation of probability is that they are real and can be estimated using historical data, statistical analysis, experimentation or a combination of these [Haimes, 1998] while the subjective counterpart suggests that they are human beliefs and are specified by humans to

characterize their uncertainty [Horton, 2004]. Over the years, security has been assessed mostly by using subjective probability. These have been used in IT-related security incidence studies: objective probability [Rees et al., 2011] and subjective probability [Bellefeuille, 2005, Whitman, 2003]. The suitability of each has been propagated by their respective proponents. This study takes the objectivist perspective to probability as there is a good degree of rationality to it which the subjectivist perspective lacks [Keynes, 1921]. However, the uncertainty in objectively estimating the probability of incidence (P) and pre-empting the impact a breach will have on the operations of the organization makes security risk assessment all the more difficult. It is clear from the recent Sony PlayStation Network security breach incidence that things change, and that very quickly. Sony never imagined that things could go so wrong as they previously estimated a profit of $855 million for the fiscal year which changed to a loss of $3.14 billion after the Tsunami and hacking incidence [Charette, 2011]. This uncertainty need to be addressed in order to accurately capture security risk. Since the incidence of a breach cannot be known with certainty, we propose the use of Entropy Theory to capture the unpredictability of breach incidence as well as the probability of incidence. Entropy according to Shannon [1948] is a quantitative measure of uncertainty. Uncertainty refers to the changeable nature of the number of times threat incidence occur and the unpredictability of whether or not it will occur.

The second main concern is the scalability. Similar in principle to the management of an application system under varying amount of work load to ensure that the performance of the system is not affected by surges in demand for the application, organizations should be able to increase or decrease computing power without adverse delay. Demand varies dynamically by time periods in the day, days of the week, months of the year, and these variations affect the performance of the organization in meeting these changes in demand. The ability in terms of capacity to manage these variations results in three states: under-provision, on-provision, and over-provision. Under provision exists when resources are not sufficient to cater for surges in demand. On-provision occurs when the resource level is just enough to satisfy the increased demand, while over-provision is a state where the resources available or in use are more than necessary to meet the increased demand. The latter is ideal in meeting any variation in demand but not ideal from a resource utilization point of view. However there is a need to optimize the utilization of resources while satisfying demand. In other words, as demand increases, resources should be increased to meet the demand *pari passu*, and as demand decreases, use of resources should be decreased to have just the right of amount of resources to meet the demand. In theory, a state of on-provision should be maintained at any point in time and at all times. This is one of the promises of cloud computing called scalability. Scalability is the ability to maintain a good level of on-provisioning at all times by dynamically adjusting computing resources to match the demand for it.

As is the pattern for most firms, technology adoption is preferably done in a stepwise manner so as to be able to discontinue its use when it is proving ineffective in delivering the anticipated benefits without any major impact on the firm's operations. Cloud computing offers this benefit and therefore the ease of increasing or reducing computing power and quickness at which this can be done at the level of automation is very important. The more time is spent trying to increase the level of resource provisioning to cater for sudden increase in demand, the longer the delay in completing the task and hence, higher risk of loss of business [Armbrust et al. , 2010, Dutta and VanderMeer, 2011]. An inactive computer consumes two-third of the energy consumed by an active computer [Armbrust et al. , 2010] and service providers are frantically considering ways to optimize server and VM utilization. A number of studies have looked at the performance of servers under different configurations and scheduling schemes. According to Yang et al. [2006] using a singer server for provisioning user request would mean that the server requires upgrading each time demand for it increases beyond its capacity and this can be complex and costly. Ng et al. [2003] proposed that an alternative solution would be to have several servers that provides for a scalable server class which handles provisioning by allocating additional server when required. Gautam [2002] studied the optimal number and location of proxy servers to minimize cost subject to delay throughput and demand constraint. At a more specific level, Son and Kim [2004] examined the optimal number of servers of a particular server class in an online transaction processing client/server environment. Dutta and VanderMeer [2011] described why existing cost-optimal allocation strategies cannot be directly applied to a middleware virtualization. This argument is applicable to cloud services as servers could be located at different locations and used to provision any resource requirements of the users. These studies have predominantly viewed performance from the perspective of the service provider and highlighted the trickledown effect on users. However, there is need in academic literature to understand, in practice, how these server performances affect the business operations of a client.

Although a huge concern to most users is availability of service, this problem mostly rise from issues with security breach or inability to provision for needed resources. With the assumption that service is being provided regularly, the next concerns would be the safety or protection of one's data, application, or transactions being done in the cloud. Another similar concern is being able to dispose of any unnecessary computing resource or quick provisioning of extra resources as demand increases. For this reason, this research will focus on studying the impact of security and scalability of cloud service on supply chain performance.

2.4. The Supply Chain Scenario

If we consider a scenario where a supply chain contains the retailer, distributor, manufacturer and supplier and we know that information about demand flows from the retailer through the chain to the manufacturer, which uses this information to place order to its supplier. Depending on the level of integration, partners can access this information once they have access to the internet and plan their operations effectively in a timely manner. If we assume that the system which the retailer uses in capturing demand is enabled on the cloud and the demand or customer information is saved on the cloud. Intuitively we know that once this system is compromised due to the fact that the cloud provider experienced security attack that makes service unavailable, the other parties in the supply chain would be denied the advantage of knowing demand as it occurs or even denied access to real demand information because the data has been corrupted. Consequently, they may result into using forecasted demand to place their orders with their suppliers and cannot take advantage of having timely demand information. Bourland et al. [1996] revealed that a supplier could reduce inventories and its associated costs or improve the reliability of deliveries to its customers given more accurate demand information. Although cloud computing promises low cost in sharing timely demand information in the supply chain when compared to traditional computing, this promise comes with an increased risk.

On the other hand if a system, enabled in the cloud, with a customer interface, which allows a customer to place order to the retailer or manufacturer directly, becomes unavailable due to security breach, or crashes due to a sudden increase in the number of customers accessing the interface at the same time. The organization or supply chain might lose that customer depending on the severity of the incidence. Severity here means the type of security breach and the number of repeated occurrence. According to Hoffman and Lowitt [2008], retaining one's customers is critical to survival of an organization, let alone growth. If we assume, hypothetically, that a web service where customers are able to place their orders online is compromised and has become inaccessible to customers. This in effect will result in the customers defecting to use services provided by competitors. The customers are classified into two categories which are the 'loyal customers' (which are those accustomed to the use the service and regularly patronize it) and the 'likely customers' (which are trying the service for the first time and are looking for a reliable service to stick to). From Capraro et al. [2003] and Hennig-Thurau and Klee [1997] we understand that loyal customers are still likely to purchase from vendors despite incessant dissatisfaction. However, a research conducted by Accenture revealed that 70% of US retail customers are loyal customers and that 85 percent of these "loyal" customers are willing to shop elsewhere if properly enticed [Hoffman and Lowitt, 2008]. In other words, there is an 85% chance they could defect. Inaccessibility to service might be the defecting factor which would cause 'loyal customers' to defect and 'likely customers' to permanently defect. The breached organization would then have to spend more money on promotional packages, among other things, to win back customers.

3. Proposed Research Framework

The research model is shown in Figure 1. In selecting cloud service providers, users tend to use price as the major criteria for selection [Durkee, 2010]. This, although tempting, can be greatly misleading. There are other factors that may make what appears to be a somewhat profitable investment to become the bane of existence. These factors, as they are also the features of cloud service, are to be given due considerations before selecting a cloud partner. The important factors amongst these are security and scalability. While cloud computing is a flexible way of computing, security and scalability plays an important role in moderating the level of benefit, if any, derivable from adopting it.

Security breach can cause disruption in business processes and may ultimately lead to loss of business [Loch, et al., 1992]. This becomes a greater problem when the source of the security breach is unknown. This can cause the system to crash preventing suppliers and other Supply chain members from having access to the service, hence disrupting the flow of transaction leading to loss of money amongst other intangible yet crucial losses. Depending on the form of attack, the magnitude of the impact of such failure can be colossal and highly detrimental to SC performance. It becomes worse when two or more breaches occur concomitantly. A classic example is the recent breach in Sony's PlayStation Network (PSN) which resulted in unavailabilityof service for weeks and cost the business billions of dollars [Osawa 2011]. It is also understood from the Bullwhip effect described in Lee et al. [2004] that there is a distortion in order information in the supply chain and this increases as you go upstream leading to variation between order and sales. Since breach in security may result in disruption of information flow and lead to increased variance between order and sales, this study therefore hypothesize that:

H1: *Security moderates the benefit Cloud computing offers to an organization and its supply chain partners*

While cloud computing offers the flexibility of increasing or reducing computing power, the ease and quickness at which this can be done at the level of automation is very important [Durkee, 2010]. The need for this is apparent from the Animoto story [Armbrust, 2010]. Animoto had to increase the number of servers provisioned by Facebook

from 50 to 3,500 in three days due to a surge in demand. They were registering 20,000 new users every hour at peak period within the said three days. If there had not been facilities to ensure quick provisioning, their website would have crashed due to overload and Animoto would have lost out on new users and the old users may have defected. Scalability can be quantified by the amount of usage of extra resources which are automatically commissioned with the increase in demand and charged on a pay-per-consumption basis [Misra and Mondal, 2011]. "Time is money", which is always a concern for organizations because the more the time it takes to reduce unneeded resources, the more the organization spends for the unwarranted resources. This in a way defies the whole concept of pay-as-you-go because in theory you are paying for unwanted resources. In fact, the actual importance of scalability lies in the time that resources are made available which could have a profound impact on the supply chain performance such as time to market and customer satisfaction. Because understanding the impact of delay in this context would help an organization judge and decide the minimum scalability power, we propose the following:

H2: *Ability to dynamically scale (Scalability) cloud resources moderates the benefits embellished in the cloud.*

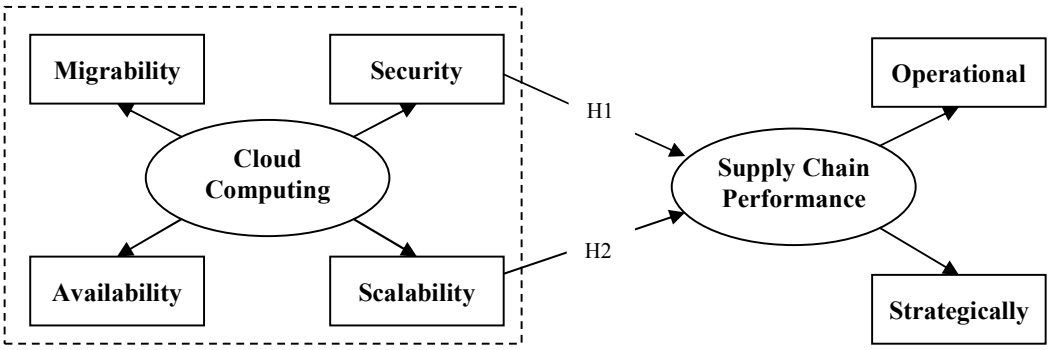

Figure 1: Research Model

4. Research Approach

In this section we would explain the underlying concept of the proposed methodology. Based on the research model, the study is defined into three stages. Each stage reveals the underlying concept for studying each of the variables. At the first stage, the study demonstrates how entropy can be used in security level assessment. The second stage looks at how scalability (scaling power) can be assessed. The third stage reveals how the impact of security and scalability on supply chain can be investigated using discrete event simulation.

4.1. Security

To assess security, every threat a system or subsystem is exposed to is first identified and their probability of incidence is calculated from historical data or statistical data. These threats are then assessed using information entropy. This system is further broken down into subsystems to evaluate the level of uncertainty or disturbance each subsystem poses to the entire system. These subsystems can be classified depending on the agent responsible as internal-based (supply chain members), external-based (the environment) and platform-based (service provider) threats. To demonstrate how entropy theory can be used, we evaluate security threats using probability values derived from the survey conducted by Whitman [2003] and work out the level of entropy each threat introduce into the system. It follows that the more the overall entropy, the lower the level of security of that system, hence the more susceptible it is to attack. The argument is that since complexity of a system (characterized by the uncertainty of a system) can be measured using entropy approach [Frizelle and Woodcock, 1995, Martínez-Olvera, 2008], and the little is known about a random variable the more the entropy of that variable, hence the level of entropy of a security breach can be determined once the probability of occurrence is known [Airoldi et al. , 2011]. Frizelle and Efstathiou [2002] explained that high entropy can impede flow by introducing obstacles that makes supply chain operations less predictable. By inference, security breaches introduce obstacles to the flow of operation and the predictability of these breaches can help evaluate the level of chaos they introduce into the system. Airoldi, et al. [2011] demonstrated that using entropy approach in estimating risk was very effective. The mathematical definition of entropy as prescribed by Shannon [1948] is a quantitative measure of uncertainty [Martínez-Olvera, 2008, Sivadasan et al., 2002]:

$$H(S) = -\sum_{i=1}^{n} Pi \log_2 Pi \qquad (1)$$

$H(S)$ is the entropy level of the system, defined here as the expected amount of information needed to describe the state of the system S , and P_i is the probability of breach type, i (i=1,...., n) occurring, where $P_i \geq 0$
Sivadasan et al. [2002] proposed two models for determining operational complexity under two conditions. However since this study is not operational complexity but is in fact security breach assessment, the names of these two models have been changed to reflect the study in question. First is complexity associated with knowing whether the system is "in control" or "not in control" which they denoted by the "in or not in control operational complexity index," OCI (S^{INC}), which in this study is called 'Chance Entropy' (CE). This is shown in equation (2), where P is the probability of being in control. CE is a measure of the amount of information needed to describe the "in-control" or "not in control" state of the system i.e the unpredictability of whether a breach will occur or not. The closer the probability of incidence is to 0.5, the closer the CE value is to one.

$$CE = -P\log_2 P - (1-P)\log_2(1-P) \quad (2)$$

Second is the complexity associated with out-of-control states, given that the system is not in control i.e. a breach has occurred. This they denoted by the "not in control operational complexity index," OCI (S^{NC}) which we now call the 'Risk Entropy' (RE). This is shown in equation (3), where $P_{i/j}$ is the conditional probability computed over the "not in control" state with states i (i=1,..., n) at nodes j (j=1,..., M). This index is a measure of the amount of information needed to monitor the extent to which the system is not in control i.e. the probability of a breach occurring.

$$RE = -(1-P)\sum_{j=1}^{M}\sum_{i=1}^{n} P_{i/j}\ \log_2 P_{i/j} \quad (3)$$

State 'i' here represents the breach with
i=1 representing Act of Human Error or failure;
i=2 representing compromises to intellectual properties and so on, as shown in the Table 1.
Nodes 'j' here represents the number of attacks per month frequency groups with:
j=1 representing greater than 100 attacks
j=2 representing 50-100 attacks
j=3 representing 10-50 attacks
j=4 representing less than 10 attacks
j=5 representing no attack at all.
According to Sivadasan et al. [2002], the sum of equation (2) and (3) is the total operational complexity which we now call 'Total Entropy' (TE). It follows that the higher the value of the entropy indices, the lower the security level of the system in managing the particular breach, hence the greater the associated information needed to manage the system and vice versa. To illustrate this concept, the threat rate provided in Whitman [2003] were plugged into equation (2) and (3) and the corresponding entropy indices were calculated and is shown in Table 3. From this we see that deliberate software attack has the largest TE of 1.91 while the lowest is deliberate acts of information extortion with TE of 0.46. This is because both of these security breaches are two occurring extremes with the former occurring 83.4% of the time and the latter occurring 9.4% of the time. Therefore more information would be needed to monitor the system to prevent deliberate software attack than deliberate acts of information extortion. However, we see that the total entropy score for 'Acts of Human error or failure' is same for 'technological software failures or errors' although the probability of incidence might suggest the former to be higher than the latter. This is so because the chance entropy of the latter (0.88) is higher than that of the former (0.74). The interaction of the two indices (CE and RE) to produce the total entropy gives a rather clearer picture of the uncertainty that each breach represent. Comparing these entropy values to the ranking scores provided in the Whitman study revealed some correlation between the two and the top three breaches with the highest TE values in this study were the same as the top three most significant breaches reported in the Whitman's study. The breach with the least TE score was 'Deliberate Acts of Information Extortion' which also had the least weighted ranking according to Whitman [2003]. While it is not very evident from the discussion above that entropy corresponds to the level of impact, a further investigation into the correlation between entropy scores and impact on the organization or

supply chain is advocated. A way to evaluate the impact security threats have on the supply chain is explained in section 4.3.

Table 1: Breach Entropy of the Whitman's 2003 study.

i	Breach Type (threat)	Prob. of incidence	CE	RE	TE	Whitman's Weighted Ranking
1	Act of Human Error or Failure	0.79	0.74	0.90	1.64	1101
2	Compromises to Intellectual Property	0.43	0.99	0.22	1.20	495
3	Deliberate Acts of Espionage or Trespass	0.31	0.90	0.15	1.04	1044
4	Deliberate Acts of Information Extortion	0.09	0.45	0.01	0.46	225
5	Deliberate Acts of Sabotage or Vandalism	0.35	0.94	0.16	1.10	963
6	Deliberate Acts of Theft	0.46	0.99	0.28	1.27	695
7	Deliberate Software Attacks	0.83	0.65	1.26	1.91	2178
8	Forces of Nature	0.38	0.95	0.17	1.13	611
9	Quality of Service Deviations from Service Providers	0.53	1.00	0.39	1.38	434
10	Technical Hardware Failures or Errors	0.66	0.93	0.61	1.53	942
11	Technical Software Failures or Errors	0.70	0.88	0.76	1.64	1130
12	Technological Obsolescence	0.40	0.97	0.24	1.21	428
	Overall				15.51	

4.2. Scalability

The relative ease with which an organization can increase or decrease computing power is an important flexibility index. In essence, the ability to quickly scale up or down computing power saves time and money and ultimately reduces the impact of data centre or server farms on the environment.To understand the impact of scalability it is important to measure the impact of some of its elements, delay in allocation or de-allocation of resources during sudden changes in demand and network delay under various band widths (resource capacity). Computer processes have such characteristics that makes it easy to be modelled by a Poisson process and the exponential distribution [Son and Kim, 2004], and most Cloud computing services are typical of client/server system. The structure shown in Figure 2 reveals the four typical client/server process structures as explained in [Son and Kim, 2004]. In the figure, (a) represents One server per client; (b) oneserver, one scheduler; (c) multiple server classes, one scheduler; (d) multiple server classes,multiple schedulers. For our research, we model both options (b) and (c) and replace 'clients' with 'client request' with requests coming from a single organization. Model (b) describes a situation where a single server is used for provisioning all similar requests sent by an organization by the use of a scheduler. Model (c) depicts a scenario where a scheduler provisions for all client requests by distributing between multiple identical servers, which is often the case in practice. The third option Model (d), which is not a subject of this research would be a more complex scenario where an organization has more than one type of request requiring different types of servers (for example both application server and database server).

Although modern server/client computing can be modelled as a M/M/c/k queuing system typical of a multithreaded process which has one arrival entrance; one finite waiting queue, k; one departure exit; and can execute multiple jobs simultaneously at a go, it can still be modelled as M/M/c queuing system with an infinite queue as proven by Son and Kim [2004]. In this study 'k' represents the maximum capacity of a server, that is, the maximum amount of load it can take at once. If the load experienced goes beyond the maximum capacity, then the server crashes and service becomes unavailable. Therefore we assume that the inter-arrival time is exponentially distributed with a forgetfulness property [Adan and Resing, 2002, Martínez-Olvera, 2008]and the queue discipline is First-In-First-Out [Jouini et al. , 2009]. We also assume that the system is a non-loss system where the requests arriving do not leave the queue but wait to be provisioned for [Singer and Donoso, 2008, Son and Kim, 2004]. Therefore Model (b) would follow an M/M/1/k queuing system translated as one server with an exponential arrival and service rate with a limited queuing capacity, k, while Model (c) would follow an M/M/c queuing system with multiple numbers of servers, c. We posit that model (c) would perform better than model (b). The easier it is to increase or decrease computing power, the better the performance of the system and hence the more the benefit to the organization or supply chain.

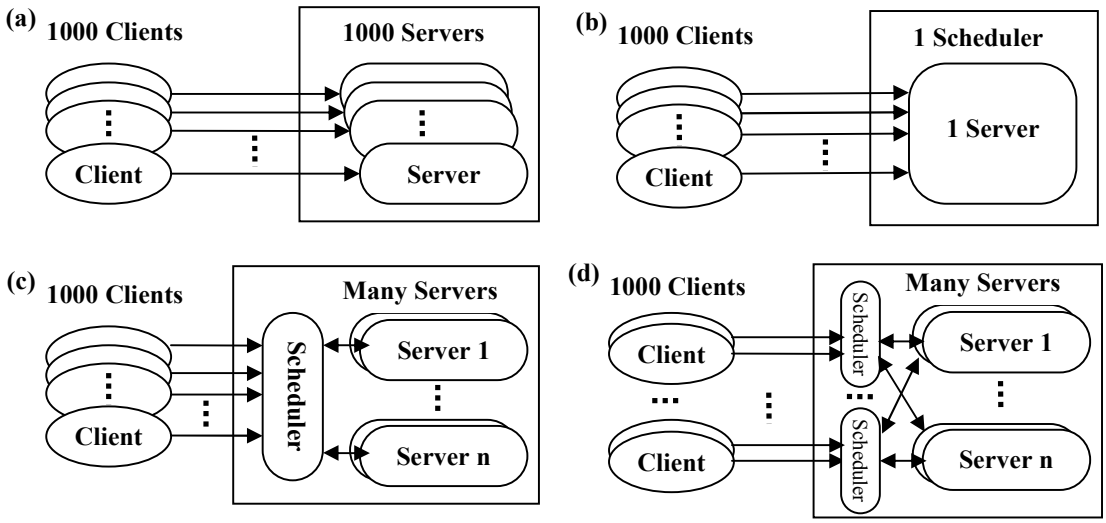

Figure 2:Four different client/server process structures (adapted from Son and Kim, 2004).

To evaluate the models we determine the probability of delay, Π_W, (that a request has to wait before being provisioned for) and waiting time, W, (amount of time taken for requests to be provisioned for after arrival). It is generally known in literature that waiting time, W, of an M/M/c system can be calculated using equation (4) [Adan and Resing 2002, Singer and Donoso, 2008, Son and Kim, 2004]:

$$W = \frac{1}{\mu} + \frac{\left(\frac{\lambda}{\mu}\right)^c \mu}{(c-1)!\,(c\mu-\lambda)^2} \times \left[\sum_{n=0}^{c-1} \frac{1}{n!}\left(\frac{\lambda}{\mu}\right)^n + \frac{1}{c!}\left(\frac{\lambda}{\mu}\right)^c \left(\frac{c\mu}{c\mu-\lambda}\right)\right]^{-1} \quad (4)$$

where:
λ is the actual arrival rate of request
μ is the service rate
c is the number of servers
n is the number of requests in the system
Adan and Resing [2002] proposed equation (5) to compute the probability of delay where ρ is the occupation rate per server and is calculated as $\rho = \lambda/c\mu$

$$\Pi_W = \frac{(c\rho)^c}{c!}(1-\rho)\left[\sum_{n=0}^{c-1}\frac{(c\rho)^n}{n!} + \frac{(c\rho)^c}{c!}\right]^{-1} \quad (5)$$

As proven by Burke [1968], the distribution of departure rate of an M/M/c queue system with infinite queue is same with that of the mean arrival rate of the system. Consequently the client/server computing can be transformed into a serial two stage tandem network of schedulers and servers with negligible error as shown in [Son and Kim, 2004]. Therefore the two performance characteristics can be computed for the scheduler to understand the impact of quick provisioning, and for the server to understand the impact of delay.

We see from the Table 2, extracted from Adan and Resing [2002], that for a constant occupation rate and service rate, the probability of delay slowly decreases as the number of schedulers (servers) increases, while the mean waiting time reduces quickly. Using discrete event simulation, these parameters can be varied to evaluate the performance of the aforementioned models.

Table 2: Performance characteristics for the M/M/c with $\mu = 1$ and $\rho = 0.9$ [Adan and Resing, 2002]

Number of servers, c	Probability of delay, Π_W	Waiting time, W
1	0.9	9.0
2	0.85	4.26
5	0.76	1.53
10	0.67	0.67
20	0.55	0.28

4.3. Discrete Event Simulations

Discrete event simulations (DES) are a powerful tool used in mimicking the dynamics of a real system as it evolves over time [Ingalls, 2008, Law, 2007]. A multiagent approach where each tier of the supply chain has at least one agent (or member as it is sometimes called) making decisions is quite representative of the real world situation, hence making it the approach of choice [Swaminathan et al., 1998]. This has been used extensively in literature because of its promising advantages. It has been described as an effective and practical tool in evaluating and analyzing, in great details, supply chain design and management alternatives [Swaminathan et al., 1998]. It can prove to be more credible than most analytical approaches being that it requires fewer simplifying assumptions and as a result captures more of the true characteristics of the system under study [Lau et al., 2004, Shannon, 1998]. It has been used in supply chain studies to understand impact of different variables on supply chain performance such as information sharing [Chan and Chan, 2009, Lau et al., 2002, Lau et al., 2004, Yang et al., 2009], integration [Chan and Zhang, 2011, Wang et al., 2008, Zhang et al., 2006] and inventory management [Jammernegg and Reiner, 2007, Lau et al., 2008, Schwartz et al., 2006, Southard and Swenseth, 2008], to mention a few.

This study focuses on information sharing as breach in information security is conceptualized as a disruption in the flow of information. Munoz and Clements [2008] using DES of the beer distribution game studied the disruption in information flow and how this affects the supply chain from a revenue costing approach. They found thatthere is a direct relationship between lost sales revenue and delay in information and that several levels of delay will result into loss of sales revenue. We surmise that the impact of each threat on each organization within the supply chain can be modeled according to the amount of disruption of service (delay) they perpetrate and applied to an appropriate simulation model (like those described in Lau et al., 2004 or Munoz and Clements, 2008] to investigate how performance measures such as inventory holding cost, backlog cost, ordering cost, production setup cost and order fill rate are affected. The impact on the supply chain can be measured in terms of the supply chain cost which is the addition of inventory holding cost, ordering cost, backlog cost and production cost. Another supply chain measure could be the total order fulfillment time. In the same light the impact of scalability on supply chain performance can be modeled according to the delay in provisioning and these delays can be applied to a simulation model as described above.

5. Conclusion and Future Research Directions

Cloud computing is expected to become an important and viable step in the evolution of information technology. However, despite its early success, cloud computing carries some limitations due to the lack of maturity typical of new technologies.Whatever the achieved level of flexibility, there are other factors such as security, scalability and service availability that greatly affect the obtained performance. This study looks at the impact of two moderating variables, security and scalability, on the performance of cloud enabled business functions of an organization. It is the first to use entropy as an assessment tool to understand how security level can be assessed and used in comparing amongst cloud providers based on their security history. Based on queuing theory, the second stage looks at why scalability is an important consideration in selecting cloud partners and how it can be evaluated.

This research serve to provide exploratory evidence that understanding the issues surrounding cloud computing adoption should come from a system thinking perspective of what the emergent effect these factors would have on the performance of an organization or supply chain network. Further, the research offers an approach which helps managers to assess the security level of any given cloud provider based on security breach data. This assessment would also serve as a risk assessment tool which can inform any risk prevention and recovery strategy decision to be made by managers. We believe that once an organization is aware of the singular as well as the combined impact of each type of security breach in quantitative terms, an organization can then understandably make informed information security decision. Furthermore, the evidence on the emergent impact would help managers develop an effective cloud computing strategy. We hope that our attempt to look at the phenomenon through a business perspective sheds more light on some of the issues surrounding cloud computing, and more importantly encourage the discussions on the various issues identified in the study.

While this paper has proposed and presented a research framework to evaluate the impact of the security and scalability on the supply chain performance, the next research direction is to build discrete event simulation models for each variable and run them under different scenarios to evaluate the impact of the variables on the operational benefits of adopting the cloud computing concept and how this on the long run relates to strategic benefits for the supply chain. The entropy score for each threat can be compared to the output values of the impact study to verify a correlation between the two. A good correlation would imply that entropy can be used as an assessment tool in predicting the level of impact security threats would have on the supply chain or the organization. In addition, as the impact of the security and scalability on the benefit from cloud computing was studied separately, further research will be examining the emergent effect of both security and scalability on the strategic as well as operational benefits of using cloud computing.

REFERENCES

Adan, I., and J. Resing, "Queuing Theory," *Department of Mathematics and Computing Science, Eindhoven University of Technology*, 2002.

Airoldi, E. M., X. Bai, and B. A. Malin, "An Entropy Approach to Disclosure Risk Assessment: Lessons from Real Applications and Simulated Domains," *Decision Support Systems* Vol. 51, no. 1: 10-20, 2011.

Amir, M. S., "It's Written in the Cloud: The Hype and Promise of Cloud Computing," *Journal of Enterprise Information Management* Vol. 23, no. 2: 131-34, 2009.

Armbrust, M., "A View of Cloud Computing," *Communications of the ACM* Vol. 53, no. 4: 50-58, 2010.

Baker, W., M. Goudie, A. Hutton, C. D. Hylender, J. Niemantsverdriet, C. Novak, D. Ostertag, C. Porter, M. Rosen, B. Sartin, and P. Tippett, "2010 Data Breach Investigations Report." In *Verizon RISK Team in cooperation with the United States Secret Service* 2010.

Bellefeuille, C. L., "Quantifying and Managing the Risk of Information Security Breaches to the Supply Chain." Massachusetts Institute of Technology, 2005.

Bourland, K. E., S. G. Powell, and D. F. Pyke, "Exploiting Timely Demand Information to Reduce Inventories," *European Journal of Operational Research* Vol. 92, no. 2: 239-53, 1996.

Burke, P. J., "The Output Process of a Stationary M/M/S Queueing System," *The Annals of Mathematical Statistics* Vol. 39, no. 4: 1144-52, 1968.

Buttell, A. E., "6 Reasons to Switch to Cloud Computing," *Journal of Financial Planning*: 6-7, 2010.

Cakebread, S., "Don't Get Lost in the Cloud," *Baseline*, no. 104: 16-16, 2010.

Capraro, A. J., S. Broniarczyk, and R. K. Srivastava, "Factors Influencing the Likelihood of Customer Defection: The Role of Consumer Knowledge," *Journal of the Academy of Marketing Science* Vol. 31, no. 2: 164-75, 2003.

Chan, F. T. S., and T. Zhang, "The Impact of Collaborative Transportation Management on Supply Chain Performance: A Simulation Approach," *Expert Systems with Applications* Vol. 38, no. 3: 2319-29, 2011.

Chan, H. K., and F. T. S. Chan, "Comparative Study of Adaptability and Flexibility in Distributed Manufacturing Supply Chains," *Decis. Support Syst.* Vol. 48, no. 2: 331-41, 2010.

Chan, H. K., and F. T. S. Chan, "Effect of Information Sharing in Supply Chains with Flexibility," *International Journal of Production Research* Vol. 47: 213-32, 2009.

Charette, R., "Sony Playstation Breach Costs Estimated to Be $171 Million " In *The Risk Factor*: ieee spectrum, 2011.

Chen, M. and M. J. Meixell, "Web Services Enabled Procurement in the Extended Enterprise: An Architectural Design and Implementation," *Journal of Electronic Commerce Research* Vol. 4, no. 4: 140-55, 2003.

Cusumano, M., "Technology Strategy and Management: Cloud Computing and Saas as New Computing Platforms," *Communications of the ACM* Vol. 53, no. 4: 27-29, 2010.

Durkee, D., "Why Cloud Computing Will Never Be Free," *Communications of the ACM* Vol. 53, no. 5: 62-69, 2010.

Dutta, K. and D. VanderMeer, "Cost-Based Decision-Making in Middleware Virtualization Environments," *European Journal of Operational Research* Vol. 210, no. 2: 344-57, 2011.

Fitzpatrick, B. W and J.J. Lueck, "The Case against Data Lock-In," *Queue* Vol. 8, no. 10: 20-26, 2010.

Frank, W., "Collaborative Supply Chain Practices and Performance: Exploring the Key Role of Information Quality," *Supply Chain Management: An International Journal* Vol. 15, no. 6: 463-73Supply, 2010.

Frizelle, G. and J. Efstathiou, "Seminar Notes on 'Measuring Complex Systems'," *London School of Economics*, 2002.

Frizelle, G. and E. Woodcock, "Measuring Complexity as an Aid to Developing Operational Strategy," *International Journal of Operations & Production Management* Vol. 15, no. 5: 26-39Internat, 1995.

Gautam, N., "Performance Analysis and Optimization of Web Proxy Servers and Mirror Sites," *European Journal of Operational Research* Vol. 142, no. 2: 396-418, 2002.

Haimes, Y.Y., Risk Modeling, Assessment, and Management, New Jersey: John Wiley & Sons, 1998.

Hennig-Thurau, Thorsten, and Alexander Klee, "The Impact of Customer Satisfaction and Relationship Quality on Customer Retention: A Critical Reassessment and Model Development.," *Psychology and Marketing* Vol. 14, no. 8: 737-64, 1997.

Hitchings, J., "Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology," *Computers & Security* Vol. 14, no. 5: 377-83, 1995.

Hoffman, J. L., and E. M. Lowitt. "Reducing the Risk of Customer Defection." *Institute for High Performance Business* 2008.

Horton, G. A., "Defining Risk," *Financial Analyst Journal* Vol. 60, no. 6: 19-25, 2004.

Huang, C. and S. Lin, "Sharing Knowledge in a Supply Chain Using the Semantic Web," *Expert Systems with Applications* Vol. 37, no. 4: 3145-61, 2010.

Ingalls, R. G., "Introduction to Simulation." Paper presented at the Proceedings of the 2008 Winter Simulation Conference, Miami, FL, USA 2008.

Jammernegg, W., and G. Reiner, "Performance Improvement of Supply Chain Processes by Coordinated Inventory and Capacity Management," *International Journal of Production Economics* Vol. 108, no. 1-2: 183-90, 2007.

Jouini, O., Y. Dallery, and Z. Aksin, "Queueing Models for Full-Flexible Multi-Class Call Centers with Real-Time Anticipated Delays," *International Journal of Production Economics* Vol. 120, no. 2: 389-99, 2009.

Kefer, G., "Cloud Technology: Transforming Your Global Sourcing Operations," *Retail Merchandiser* Vol. 50, no. 5: /Oct2010,-7, 2010.

Keynes, J. M., A Treatise on Probability, London: Macmillan, 1921.

Kim, W., O. Jeong, C. Kim, and J. So, "The Dark Side of the Internet: Attacks, Costs and Responses," *Information Systems* Vol. 36, no. 3: 675-705, 2011.

Lancioni, R. A., M. F. Smith, and H. J. Schau, "Strategic Internet Application Trends in Supply Chain Management," *Industrial Marketing Management* Vol. 32, no. 3: 211-17, 2003.

Lau, J. S. K., G. Q. Huang, and K. L. Mak, "Web-Based Simulation Portal for Investigating Impacts of Sharing Production Information on Supply Chain Dynamics from the Perspective of Inventory Allocation," *Integrated Manufacturing Systems* Vol. 13, no. 5: 345-58Integra, 2002.

Lau, J. S. K., G. Q. Huang, and K. L. Mak, "Impact of Information Sharing on Inventory Replenishment in Divergent Supply Chains," *International Journal of Production Research* Vol. 42, no. 05: 919-41, 2004.

Lau, R. S. M., J. Xie, and X. Zhao, "Effects of Inventory Policy on Supply Chain Performance: A Simulation Study of Critical Decision Parameters," *Computers & Industrial Engineering* Vol. 55, no. 3: 620-33, 2008.

Law, A. M., Simulation Modelling and Analysis, Ed. Kenneth E Case and Philip M Wolfe, 4th ed, Industrial Engineering and Management Science, New York: McGraw-Hill companies, 2007.

Lee, H. L., V. Padmanabhan, and S. Whang, "Information Distortion in a Supply Chain: The Bullwhip Effect," *Management Science* Vol. 50, no. 12: 1875-86, 2004.

Li, J., R. Sikora, M. J. Shaw, and G. W. Tan, "A Strategic Analysis of Inter Organizational Information Sharing," *Decision Support Systems* Vol. 42, no. 1: 251-66, 2006.

Marston, S., Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, "Cloud Computing -- the Business Perspective," *Decision Support Systems* Vol. 51, no. 1: 176-89, 2011.

Martínez-Olvera, C., "Entropy as an Assessment Tool of Supply Chain Information Sharing," *European Journal of Operational Research* Vol. 185, no. 1: 405-17, 2008.

Misra, S. C., and A. Mondal, "Identification of a Company's Suitability for the Adoption of Cloud Computing and Modelling Its Corresponding Return on Investment," *Mathematical and Computer Modelling* Vol. 53, no. 3-4: 504-21, 2011.

Munoz, A., and M. D. Clements, "Disruptions in Information Flow: A Revenue Costing Supply Chain Dilemma," *J. Theor. Appl. Electron. Commer. Res.* Vol. 3, no. 1: 30-40, 2008.

Newman, J., "Experts on Psn Hack: Sony Could Have Done More." In *Security*: PCWorld Communications Inc., 2011.

Ng, B., F. W. B. Li, R. W. H. Lau, A. Si, and A. Siu, "A Performance Study on Multi-Server Dve Systems," *Information Sciences* Vol. 154, no. 1-2: 85-93, 2003.

Nugent, J. H. and M. S. Raisinghani, "The Information Technology and Telecommunications (or E-Business) Security Imperative: Important Issues and Drivers," *Journal of Electronic Commerce Research* Vol. 3, no. 1: 1-14, 2002.

Osawa, J.. " As Sony counts Hacking Costs, Analyst See Billion-Dollar Repair Bill," *The Wall Street Journal* [online] Available:http://online.wsj.com/article/SB10001424052748703859304576307664174667924.html

Orange, E. and A. M. Cohen, "Mining Information from the Data Clouds," *The Futurist* 17-22, 2009.

Pendergraft, L., "Tensteps for Evaluating and Selecting Software and Service Providers," *Information Management (15352897)* Vol. 44, no. 1: 40-44, 2010.

Pisello, T., "Is There a Business Case for It Security?" In *Security Management*. Alexandria, Virginia: ASIS International, 2004.

Pollack, D., "Sony Breach Now a Class Action." In *idexperts Blog*: idexperts, 2011.

Potter, C. and A. Beard. "Information Security Breach Survey 2010." In *Information Security Breach Survey* 2010.

Rees, L. P., J. K. Deane, T. R. Rakes, and W. H. Baker, "Decision Support for Cybersecurity Risk Planning," *Decision Support Systems* Vol. In Press, Corrected Proof, 2011.

Ryan, M. D., "Cloud Computing Privacy Concerns on Our Doorstep," *Communications of the ACM* Vol. 54, no. 1: 36-38, 2011.

Schwartz, J. D., W. Wang, and D. E. Rivera, "Simulation-Based Optimization of Process Control Policies for Inventory Management in Supply Chains," *Automatica* Vol. 42, no. 8: 1311-20, 2006.

Seccombe, A., A. Hutton, A. Meisel, A. Windel, A. Mohammed, A. Licciardi, A. Chuvakin, A. Chetal, A. Hedge, B. Monday, B. Cohen, B. Barman, B. O'Higgins, C. Espiritu, C. Hoff, C. Watson, D. Jackson, D. Lingenfelter, D. Mortman, D. Sherry, D. Tyson, D. Hurst, D. Blumenthal, D. Yoran, E. Dahan, E. Peterson, E. Hayden, F. Gilbert, G. Engh-Hellesvik, G. Hess, G. Eschelbeck, G. Bhat, G. Brunette, G. Kane, G. Tipps, H. Harel, J. Tiller, J. Pawluk, J. Reich, J. Spivey, J. Ritter, J. Laundrup, J. Garcia, J. Arlen, J. Hietala, J. Cupano, J. McDonald, J. Stein, J. Wallace, J. Weise, J. Arnold, J. Callas, J. Stein, J. Foster, K. Lossau, K. Worstell, L. Newcombe, L. Morales, M. S. Prasad, M. Johnson, M. Reiter, M. Sutton, M. Kavis, N. Bukhari, P. Fusco, P. Sullivan, P. Gregory, P. McLaughlin, P. Cox, R. Broom, R. Barr, R. Mogull, R. Austin, R. Zhao, S. Chugh, S. Giordano, S. Matsumoto, S. Morrison, S. Catlett, S. Loureiro, S. Khiyara, S. Chaput, S.

Lakshminarayanan, S. Nair, S. Kumaraswamy, T. Singh, T. Forsheit, V. Williams, W. Axelrod, W. Pauley, W. Streitberger, W.Ko, and Y. Wilson, Cloud Security Alliance - Security Guidance for Critical Areas of Focus in Cloud Computing, Edited by Glenn Brunette and Rich Mogull, 2009.

Shannon, C. E., "A Mathematical Theory of Communication," *The Bell System Technical Journal* Vol. 27: 379-423, 623-56, 1948.

Shannon, R. E. "Introduction to the Art and Science of Simulation." In *Proceedings of the 30th conference on Winter simulation*, 7-14. Washington, D.C., United States: IEEE Computer Society Press, 1998.

Singer, M. and P. Donoso, "Assessing an Ambulance Service with Queuing Theory," *Computers & Operations Research* Vol. 35, no. 8: 2549-60, 2008.

Sivadasan, S., J. Efstathiou, G. Frizelle, R. Shirazi, and A. Calinescu, "An Information-Theoretic Methodology for Measuring the Operational Complexity of Supplier-Customer Systems," *International Journal of Operations & Production Management* Vol. 22, no. 1: 80-102Interna, 2002.

Smith, R., "Computing Beyond the Firewall," *Research Technology Management* Vol. 53, no. 3: 64-65, 2010.

Smith, R., "Computing in the Cloud," *Research Technology Management* Vol. 52, no. 5: 68, 2009.

Son, J. H. and M. H. Kim, "An Analysis of the Optimal Number of Servers in Distributed Client/Server Environments," *Decision Support Systems* Vol. 36, no. 3: 297-312, 2004.

Southard, P. B. and S. R. Swenseth, "Evaluating Vendor-Managed Inventory (Vmi) in Non-Traditional Environments Using Simulation," *International Journal of Production Economics* Vol. 116, no. 2: 275-87, 2008.

Subashini, S., and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," *Journal of Network and Computer Applications* Vol. 34, no. 1: 1-11, 2011.

Swaminathan, J. M., S. F. Smith, and N. M. Sadeh, "Modeling Supply Chain Dynamics: A Multiagent Approach*," *Decision Sciences* Vol. 29, no. 3: 607-32, 1998.

Ulrich, F. and P. Oliver, "Management of Security Risks a Controlling Model for Banking Companies," *International Handbooks Information System*, 2008.

Wang, M., J. Liu, H. Wang, W. K. Cheung, and X. Xie, "On-Demand E-Supply Chain Integration: A Multi-Agent Constraint-Based Approach," *Expert Systems with Applications* Vol. 34, no. 4: 2683-92, 2008.

Wang, W.Y.C, C.W. Chang, and M.S.H. Heng, "The Levels of Information Technology Adoption, Business Network, and a Strategic Position Model for Evaluating Supply Chain Integration," *Journal of Electronic Commerce Research* Vol. 5, no. 2: 85-98, 2004.

Warren, M., "Cyber Attacks against Supply Chain Management Systems: A Short Note," *International Journal of Physical Distribution & Logistics Management* Vol. 30, no. 7/8: 710, 2000.

Whitman, M. E., "Enemy at the Gate: Threats to Information Security," *Commun. ACM* Vol. 46, no. 8: 91-95, 2003.

Xu, Xun, "From Cloud Computing to Cloud Manufacturing," *Robotics and Computer-Integrated Manufacturing* Vol. 28, no. 1: 75-86, 2012.

Yang, Jianhua, Di Jin, Ye Li, Kai-Steffen Hielscher, and Reinhard German, "Modeling and Simulation of Performance Analysis for a Cluster-Based Web Server," *Simulation Modelling Practice and Theory* Vol. 14, no. 2: 188-200, 2006.

Yang, Taho, Yuan-Feng Wen, and Fang-Fang Wang, "Evaluation of Robustness of Supply Chain Information-Sharing Strategies Using a Hybrid Taguchi and Multiple Criteria Decision-Making Method," *International Journal of Production Economics* Vol. In Press, Corrected Proof, 2009.

Zhang, David Zhengwen, Anthony Ikechukwu Anosike, Ming Kim Lim, and Oluwaremilekun Mowanuola Akanle, "An Agent-Based Approach for E-Manufacturing and Supply Chain Integration," *Computers & Industrial Engineering* Vol. 51, no. 2: 343-60, 2006.