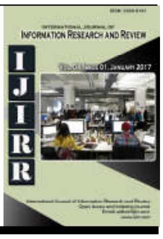
IJIRR

International Journal of Information Research and Review
Vol. 04, Issue, 01, pp. 3511-3516, January, 2017



Research Article

USERS PERCEPTION ON THE PUBLIC CLOUD SECURITY RISK AND DATA MONETIZATION

[1,*]Emmanuel Guzmán Rodríguez, [2]Enrique Medina Sánchez and [3]Ángel Ojeda Castro

[1]Doctorate Student School of Business and Entrepreneurship, Universidad del Turabo, Puerto Rico
[2]Doctorate Student School of Business and Entrepreneurship, Universidad del Turabo, Puerto Rico
[3]Associate Professor, Management Information Systems, Universidad del Turabo, Puerto Rico

ARTICLE INFO

Article History:

Received 14th October, 2016
Received in revised form
22nd November, 2016
Accepted 25th December, 2016
Published online January, 30th 2017

Keywords:

Public Cloud Security Risk,
Cloud Monetization,
User Trust,
Prospect Theory.

ABSTRACT

The subject of interest is that individuals and small businesses have a security uncertainty about how the public cloud manage their information.The objective is to close the knowledge gap of what, why, how, where and who is responsible for the cloud security uncertainty.Thefirst research criteria is to explain the public cloud security dilemma in its architecture and infrastructure; then, explain why and where the public cloud has security problem; and third, use trust and the original prospect theory to understandwhy individuals and small businesses use the PC. The latter is the research innovation which provide new knowledge on user's perception. The resultsare important as it was foundthe public cloud is a business model that monetizes its user's data, and the perceived security uncertainty is a confidentiality problem.The literature review on cloud monetization is scarce, the current trend of cloud providers is to breach users' confidentiality to monetize their data. This researchclears the public cloud security uncertainty perceived by individuals and small businesses. It also provides new insights on how to predictconsumer's behavior in decisions with different levels of risk, and provides a detailed description of where is the security uncertainty of the public cloud.

INTRODUCTION

On this section the research provides a brief summary on what is cloud computing, its contribution to society, and what types of cloud products and services are offered. The research contribution differs from other cloud security articles as its objective is to identify why the public cloud has a perceived security uncertainty; rather than discuss cloud vulnerabilities, exploits, and weaknesses. The first part of theliterature reviewintends to instill new knowledge about where, how, why and who is the cause for the perceived PC security uncertainty. Then provide a theoretical analysis on consumer's perceptionmoderated with trust and the prospect theory. The public cloud popularityrelieson its information system access without geographical nor physical constrains (Dihal, et al. 2013); and (Syal and Goswami 2012). Cloud computing is a new business modelthatoffers a broadband service thatrentscomputer hardware as a mobile resource (Dihal et al. 2013); and (Syal and Goswami 2012). Its expected role is to provide secure, quick, convenient data storage and net computing service delivered online (Zhang, Xu, Duan, Gong, Lu and Yang, 2015). The PC innovation is not the use of virtual computer, nor the access to computer hardware from another geographical location.

Cloud computing originality is the liaison between computer hardware as software with mobile intelligence devices with broadband services that enable worldwide access for a fraction of the cost to buy, program and maintain an information system infrastructure. Cloud service providers offer the deployment of five different types of clouds and four online services. The five type of cloud deployments are the private cloud, hybrid cloud, virtual cloud, community cloud and public cloud(Prantosh, Bhaskar and Rajesh 2015); (Syal and Goswami 2012); and(Vilkomir 2012). Private clouds maintain the benefits of cloud computing, but it is a personal or private enterprise architecture; hence, better security but requires upfront capital investment (Syal and Goswami 2012). Hybrid cloud is the use of cloud benefits through a third party, but the data is always within the customer's storage hardware (Syal and Goswami 2012). Virtual cloud computing is a layer above the private and public cloud which provides security and information process customization (Syal and Goswami 2012). Community cloud is a set of organizations that share the architecture of physically owned devices to create and maintain an online information system. The previous cloud deployments require upfront capital investment, only the public cloud provides a free cloud architecture through an open network. With the deployment of the clouds, service providers also offer online services as software as a service (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS) and testing as a service (TaaS) (Padilla, Milton and Johnson 2015); (Syal and

****Corresponding author: Emmanuel Guzmán Rodríguez,***
School of Business and Entrepreneurship, Universidad del Turabo, Gurabo, Puerto Rico

Goswami 2012); and (Vilkomir 2012). Cloud service providers negotiate a contractual obligation with the customer, known as the service level agreement. SLA does not apply for public cloud, as the user must accept the provider's conditions to connect with the open access platform. Individuals and small businesses accept provider's conditions as theirfinite economic resource constrain their ability to build and manage an information infrastructure(Quedraogo, et al. 2015). The importance and the social-economic contribution of the public cloud is that itbypasses business to business and business to customer economic barriers with their open access platforms and rent of online services at reasonable prices.The present problem of the PC is the uncertainty of its security environment, and how the providers manage its customer's data.

Research Problem

Public cloud service providers have a transparency problem, which results in a perceived unknown risk of its expected role. Based on Zhang et al. (2015) the PC role is to maintain customer data confidential, integral and accessible. Data integrity and accessibility are not perceived at risk, as the cloudsafeguards its user's data in different storage devices worldwide. Based on multiple articles the perceived uncertain risk seems related with the cloud architecture and its security environment (Quedraogo et al. 2015);(Yunchuan, et al. 2014); and (Santosh and Goudar 2012). PC security uncertainty has a worldwide momentum, it has serious security challenges which include regulating legal issues and customer confidentiality (Fateminezhad and Mohammad 2016); (Rastogi, Gloria and Hendler 2015); (Quedraogo et al. 2015); (Kesan, Hayes and Bashir 2013); (Brooks, Robinson and McKnight 2012); and (Sehgal et al. 2011). Even though the cloud has multiple challenges, the researchfocuseson what is the security uncertainty of the PC architecture.

Research Contribution

Based on the literature review it was revealedthat the public cloud architecture providesinsight on the customer confidentiality problem. Theliterature review aims to discuss the public cloud architecture as it will provide useful information to understand how the cloud providers interact with its user's data. The objective of the research is to identify the cloud security uncertainty in its architecture and infrastructure. For this article the criteria on security uncertainty is limited to customer confidentiality, integrity and accessibility. The second objectiveaimsto provide comprehensible information that clears the cloud security uncertainty.And theoriginal contribution of this researchis the use of Trust and Prospect Theory to explain customer'sperception on why they continue to use the public cloud.

LITERATURE REVIEW

The Security Concern of the Public Cloud Architecture

The environment of apublic cloud information system is managed and controlled by the provider (Srinivasan 2013). Since the confidentiality, integrity and availability of user's data is in the management of a third party, it is on the customer's best interest to discuss thecloud architecture. The public cloud structure is composed of seven components: the application, the Data, the Middleware or Operating System, the virtualization of computer resources, the hardware and the physical network (Rastogi et al. 2015). SaaS is the monetary term for rented cloud applications. Open source SaaS are referred as public cloud applications, and are the users interface or the first step toward managing an individual or businesses information. The middleware or PaaS is the deployment of a virtual platform. Its role links cloud customer's application with physical or virtual hardware resources, these include but are not limited to storage, ram, and computer processing resources available at the cloud. The term virtualized hardware is the source or the core of the cloud concept. It is technology resources at the user's disposal with the only requirement of internet access. Lastly, the network component represents the physical infrastructure of the virtualized hardware resource.

It is important to examine if thepublic cloud can maintain user's information confidential, integral and available. To tackle the previous interrogatives the paper researchedhow the cloud communication works. The PC processes information from two stand pointsFront End and Back End. The first focuses on the client, the user or the application that access the cloud services; while the Back End are the cloud service providers, farm servers, and the middleware (Syal and Goswami 2012). The public cloud has a Back End architecture security uncertainty for customer data confidentiality (Syal and Goswami 2012). This research is not limited on user's confidentiality, we add user's data availability and integrity as subjects of interest in the cloud infrastructure.Forthe cloud, availability is not a problem. The problem or uncertainty are on its integrity and confidentiality. Information integrity is related with the cloud providers methods to increase hardware efficiencies; because, the overuse of hardware resources can result on system failure as an increase in thermal nodes affect the infrastructure reliability (Sasikala and Suresh 2016) and (Rajadarshini and Alageswaran 2016).

Thermal nodes are measured in terms that represent heat created by a device processing information; hence, the reliability of the cloud infrastructure is associated with the methods used to process information. Cloud computing architecture can process information in clusters or in grid networks (Brooks, Robinson and McKnight 2012). A cloud architecture which processes information in clusters is related to a centralized infrastructure; and is associated with a higher hard-drive error rate (Yunchuan et al. 2014). As an alternative, cloud providers can choose to process information with a grid computing infrastructure. It is a decentralized network that divides the information load on a diversity of devices that processes the data parallel to each other maximizing the on-demand technological resources (Brooks et al. 2012).The literature review on grid computing mentions cloud providers are moving to centralized databases; because, it maximizes the infrastructure reliability, efficiency, and the providersbottom line (Sasikala and Suresh 2016);and(Rajadarshini and Alageswaran 2016). The term efficiency is based on the infrastructure economic cost rather than user's data transfer. A lower amount of thermal nodes results in a decrease in electric consumption, hence lower expenses.Cloud efficiency and reliability are different terms, yet, areviewed as how the hardware of its infrastructure is used to process and maintain data integrity.

The problem is the concept of reliability from the cloud provider is driven by their bottom line. Moving to a centralized infrastructure that processes data in clusters is a business decision that aims to decrease electric expenses. The problem of this strategy is that a higher hard-drive error rate was associated with clustering networks and not with the reduction of thermal nodes or the control of roomtemperature (Yunchuan et al. 2014). The benefit of a centralized network in a single location is that it enhances the provider's capacity to create a secure environment. Based on the previous discussion, cloud providers have an economic function for reliability, integrity and confidentiality. Where the economic investment of each, affects the other. To increase reliability of cloud infrastructure, grid computing is recommended, but this strategy actually results in a higher risk for user confidentiality; because, grid computing is the use of multiple physical devices in different locations as hardware resources. Data integrity and accessibility are the objectives of the cloud, and works by backing up the data in multiple devices in different locations. A centralized cloud requires more economic resources to guarantee the data integrity, accessibility and devices reliability. To create or improve the cloud security environment requires a significant investment. Public cloud providers do not possess the cash flow to create and maintain a centralized cloud that is always accessible, reliable and secure.

A secure environment needs to provide information confidentiality and maintain its integrity, these security concepts share the requirement that only authorized personnel can have access to the information (Veeralakshmi and Latha 2016). Based on the cloud literature review, encryption is the common denominator to ensure users confidentiality and integrity. Encryption is an algorithm with the purpose to codify the bits that identify a document into unrecognized bits. The flaw is that encryptions require a key, which is used as an index to encrypt and decrypt the bits. Data stored in the cloud is under the control of third parties, plus the cloud can provide the technology resources to assimilate a super computer that can decipher the key to decrypt documents. The security uncertainty in the cloud is a serious problem, because its implementation cannot guarantee users confidentiality. Users and cloud providers can only build security obstacles rather than security walls, because the information is accessible for those who have the resources to obtain authorization.

Data encryption is used by the minority, and the reality is that users of the public cloud delegate their security responsibility to the cloud providers. A good security environment is not enough to maintain confidentiality, because hackers are constantly innovating. Hardware and software vulnerabilities as a conjunction can provide hackers a route to trigger an exploit to access the physical host of a virtual computer (Manavati, et al. 2014). The cloud provides free data integrity and accessibility in exchange for the sale of customer information to third parties. Cloud providers are challenged to maintain a secure virtual framework from outside malicious attacks, and inside malpractices. Cloud computing is vulnerable to traditional attacks, because the infrastructure is not new and is accessible worldwide. The cloud is also vulnerable to zero day exploit that may compromise cloud information confidentiality. These attacks success rates are related with unknown vulnerabilities on the hardware and software.

Centralized cloud providers can minimize outside threats, as a result of maintaining the data within a single location. This is impossible with a decentralized cloud; because, the security protocols arethe responsibility of multiple parties that depend on limited economic resources to maintain an updated security framework. From the customer perspective, this can result on profiling users consumption and assigning protocols, which limit their demand on resources (Sasikala and Suresh 2016);and(Rajadarshini and Alageswaran 2016). The public cloud architecture has an architecture problem in which third parties have access to customer information through the data controller (Rastogi et al. 2015). The public cloud is a worldwide network with different information system environments; hence, public cloud user security depends on unknown third party protocols (Aleem and Sprott 2013). The public cloud business model has multiple security vulnerabilities, and their role as information storage is attractive for hackers who also live by selling user information (Rastogi et al. 2015); (Kesan, Hayes and Bashir 2013); (Fateminezhad and Mohammad 2016); (Quedraogo et al. 2015); (Rastogi et al. 2015); and (Sehgal, et al. 2011).

Data Monetization in the Public Cloud

To monetize a product or service, first it is required to create a saleable value that meetssomeone's needs (Reopel, et al. 2004). Based on Wixom (2014) and Najjarand Kettinger (2013) data monetization can be defined as an exchange of useful data as a product for an asset; and/or a service to develop a company's data into a monetized product. The cloud has created an important and useful technological resource, yet the saleable value is not the cloud but the stored data from its users.The strategy of the public cloud to collect data is not new, but with today's technology it is a useful and attractive open source resource. Big data is a business intangible asset, capable ofgenerating an additional economic resource by monetizing its data (Woerner and Wixom 2015).

The public cloud business model moves towardscreating value out of its user's cloud, hencedata confidentiality is not taken into consideration (Najjar and Kettinger 2013). PC providers possess a big data pool with a possible value, but it requires to be analyzed and minedin search ofsaleable information. In open source technology,it is common that a mutual agreementis inexistent as the users are required to accept the terms in order to have access to the resources. This method to force customers to the terms of use,is a legal loophole were the providers offer a needed or desired technological resource in exchange to collect, mine, and sale its user's data. Since 2009 there is an increasing trend of business innovation towardscollecting and monetizing data (Woerner and Wixom 2015). On Woerner& Wixom (2015) article they mention that businesses are giving more importance to the data that surrounds a product than to the product itself. The method of the public cloud to collect data is in its architecture. The public cloud business model and architecture provides accessibility and data integrity but it is not focused toward user's confidentiality. The public cloud income or economic source for its sustainability is through the sale of data(Rastogi et al. 2015); and (Kesan et al. 2013). The public cloud is a big data pool, mined by third parties for advertisement purposes (Rastogi et al.). Based on Rastogi et al. the data controller is the architectural component that compromisesuser's confidentiality.Also, the SaaS and PaaS architectural components provide access to third parties that can mine and analyze the information, including the use ofidentifier artificial intelligence algorithm (Rastogi et al.);and(Kesan et al.).This business model will eventually evolve so that in the future people may have or want to pay for their own privacy, as the application of the business model of data monetization continues to become more and more habitual. Businesses have continuously researched, estimated and handled uncertainty based on probability. The cloud security uncertainty is difficult to research, estimate and handle; because, there are multiple unknown parties involved in the use and analysis of user's data. Another problem is that manager's decisions reside in an economic perspective, as the cloud is also a for profit business they may allow a certain risk that represents an acceptable financial loss. Before individuals and small businesses incorporate the public cloud computing, they need to consider the security, the benefits and if the value received overcomes the risks (Brooks, Robinson and McKnight 2012). The next section discusses why users of the public cloud computing accept the confidentiality risk.

Users Trust on the Public Cloud Providers

For this research trust is defined as the willingness to take a risk on a third party in return for an expected outcome (Huang and Nicol 2013). It seems users of the public cloud accept the uncertain risk in exchange for the expected technological resources. The unknown risk has been identified asuser's confidentiality risk that extends to third parties that participate in data monetization (Holt and Macic 2015); and (Rastogi et al. 2015). Customersare not informed that the public cloud shares their information; hence, when information is uncertain, decisions are taken based on benefits rather than risks (Kahneman and Tversky 1979). The public cloud success on monetizing their consumer's data may reside in limiting the available information of how they generate economic resources. The public cloud risk is not limited to their user's confidentiality as theenvironment is shrouded with security uncertainty, lack of public information, and unclear data control (Khan and Malluhi 2010). To minimize cloud security attacks, it requires to build and maintain an up to date secure environment that monitors and controlsuser's interaction. The solution to increase the security is not the problem, but the economic resources required can threaten the cloud provider's sustainability. Public cloud providers are a business model and having a negative bottom line is not their purpose. The dilemma is between user's interests on confidentiality and a secure environment, against cloud providers' bottom line. The monetization of its consumer's data is considered as a breach of trust (Najjar and Kettinger 2013);yet, it seems that users of the public cloud are willing to accept the risk in exchange for the cloud technological resources of accessibility and data integrity. It seems public cloud providers nurture trust and amend the trust breach by guaranteeing users expectation (Michael 2009). Huang and Nicol (2013) explain that user's acceptability towards data monetization can be the result of trusting the cloud for guaranteeing its performance on accessibility and data integrity. The next section uses the Prospect Theory of Kahneman and Tversky (1979) to explain why the users of the public cloud are willing to risk their confidentiality.

Users Prospect on the Public Cloud

This research takes a different approach from (Tversky and Kahneman 1992); (Gilboa and Schmeidler 1989); and (Gilboa 1987) which they advance the prospect theory from an economics perspective. For this paper the original prospect theory is ideal, as the term acceptable prospect is compatible with the business model of data monetization. The sustainability of the public cloud is through the transfer of data. It is the general acceptable prospect and certain need between companies and users in search to maximize their technological resources. The prospect theory can provide insights on the reasoning of cloud customers. From the customer'sperspective, the public cloud provides accessibility and data integrity, the uncertain risk is the probability of stolen, distributed, mined or even lossof information. The probability of losing data within the cloud is minimized by creating backups, but this increases the probability of having the information stolen. The concept of the PC is a normal decision for small businesses, because their objective is to maximize the bottom line rather than customer confidentiality (Willcocks, Venters and Whitley 2013).

PC is very popular for individuals as their interests is towards accessibility to their information at all times. On (Kahneman and Tversky 1979) article, the prospect theory explains that an individual desires or preferences overweight the axiom of the utility theory when there is not a certain outcome. The weight of the decision making process is in the individual desires or preferences. When a certain outcome is not provided, an acceptable prospect is chosen. Otherwise they gamble on the choice with the highest outcome, and they become risk seekers when negative outcomes are the only choices. Also, people are willing to gamble in the first step of a sequential process if there is an acceptable prospect of receiving the expected outcome (Kahneman and Tversky). The article of the prospect theory does not provide what is the percentage for an acceptable prospect. A limitation of Kahnemanand Tversky research is that no significant percentage was researched, which can influenceindividual's decision between the utility theory and prospect theory. The article discusses that users always prefer expected outcomes, if probabilities are the only choices. Also,an acceptable prospect needs a 90% or higher, otherwise decisions are based on the outcome with the highest return.

An acceptable prospect is when it is able to incorporate itself into a given structure, and its usefulness transcends the owner's equity (Kahneman and Tversky 1979). KahnemanandTverskyexplain that decisions with a probable risk does not always follow the economic axiom, but the prospect postulate. Decisions are made on the user's desire or preferences of the expected outcome. In this research the prospect axiom is not economic, but the open technological resource that meets user desires and preferences. The public cloud business model provides a desired expected outcome, an open source and online technological resources. Individuals and small businesses will continue to use the public cloud because it is an acceptable prospect and provides a guaranteed outcome that meets their desires or preferences. The problem of the public cloud is that usersassess risk toward data accessibility and integrity, and donot take into consideration their confidentiality.

This perception provides the opportunity for a business model that generates assets through data monetization. The public cloud guarantees an acceptable prospect in exchange to collect, store, mine, and sell its users data. A private cloud can provide data confidentiality, but as KahnemanandTversky (1979) discuss between a certain loss and no loss, users will choose to gamble when negativeoutcomesare provided. Users of the public cloud prefer open source resources at the risk of their confidentiality.

Illustration 1.0 Customer Perception of their Data Monetization in the Cloud

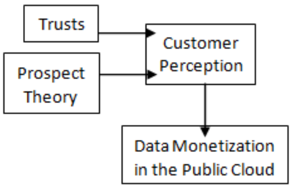


Illustration created by the authors, 2016

The research contribution is limited as it does not survey if customer perception changesafter given information about a confidentiality breach and data monetization. Interestingly the literature review provides insights that customer perception is not influenced by the cloud business model, but their desires and preferences. From a critical analysis, the original prospect theory does have a theoretical relevance in this paper, but to support its application it requires a survey to identify if user's behavior will change after knowing about the cloud business model. Trust and the Prospect Theory share a common explanation in which PC users take into consideration the expected outcome based on their desires and preferences when the risk is uncertain. Also, future studies should research if consumer's decision making process is weighted on the expected outcome rather than a given risk. For example: if PC consumers are informed about their data monetization, and confidentiality breach, will they be willing to continue using the PC services;if they do, then this provides new knowledge that desires and preferences are dominant in consumer's decisions.

Research Discussion and Conclusion

It seems that users of the public cloud are willing to take risks when there is limited or unknown information about the uncertainty; hence, they are willing to trust a product or service based on their perception of the expected outcome. In search to explain why users of the public cloud accept the uncertain risk, the prospect theory of Kahneman and Tversky (1979) was applied. The result was that perception is also important and is operationalized into consumer's desires and preferences on the expected outcomes. This provides insights that consumers decisions are based on their desires and preferences on a subject. When Trust was applied, it was found that under uncertain risk they are willing to trust the provider if the expected outcome is guaranteed. Users seem to accept a higher risk to lose or gamble toward a higher probable benefit. They are not assessing the loss of the risk, but the benefit of the risk. From the losing perspective users prefer a probable outcome than a certain loss, and always choose the lowest economic loss even if it has a higher probability.

An important limitation of the research contribution is that it does not apply a questionnaire that can obtain users perception before and after knowing about their confidentiality risk and that their data is monetized. The questionnaire results can support the theoretical application of the authors, and support a new theoretical axiom that consumer's decision making process is based on their desires and preferences. It is recommended that cloud computing add a defined security architecture and analysis of communication protocols (Brooks, Robinson and McKnight 2012). Cloud computing challenges are the unreliability of end-devices, security enforcement, user's privacy, and business model transparency. The business model of the public cloud is data monetization. To maintain its sustainability, it requires to bypass and avoid government privacy laws. The literature review on data monetization in the cloud is scarce, and it is a current business model with serious confidentiality problems.

REFERENCES

Aleem, Azeem, and Christopher Ryan Sprott. 2013. "Let me in the cloud: analysis of the benefit and risk assessment of cloud platform." *Journal of Financial Crime* (Emerald Group Publishing Limited) 20 (1): 6-24. doi:10.1108/13590791311287337.

Brooks, Tyson, Jerry Robinson, and Lee McKnight. 2012. "Conceptualizing a Secure Wireless Cloud." *International Journal of Cloud Computing and Services Science* (Institute of Advanced Engineering and Science) 1 (3): 89-114.

Dihal, Soebhaash, Harry Bouwman, Mark de Reuver, Martjin Warnier, and Christer Carlsson. 2013. "Mobile cloud computing: state of the art and outlook." (Emerald Group Publishing Limited) 15 (1): 4-16. doi:10.1108/14636691311296174.

Fateminezhad, Ali, and Soltanaghaei Reza Mohammad. 2016. "An Overview of Cloud Computing and Its Related Security Issues." *Journal of Current Research in Science* S (1): 410-414.

Gilboa, Itzhak. 1987. "Expected Utility with Purely Subjective Non-Additive Probabilities." *Journal of Mathematical Economics* (North-Holland) 16: 65-88.

Gilboa, Itzhak, and David Schmeidler. 1989. "MAXMIN Expected Utility with Non-Unique Prior." *Journal of Mathematical Economics* (Research Gate) 18: 141-153.

Hashizume, Keiko, David G Rosado, Eduardo F Medina, and Eduardo B Fernandez. 2013. "An analysis of security issues for cloud computing." *Journal of Internet Services and Applications* (Springer Open Journal) 4 (5). http://www.jisajournal.com/content/4/1/5.

Holt, Jennifer, and Steven Macic. 2015. "The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union." *Journal of Information Policy* (Penn State University Press) 5: 155-178. http://www.jstor.org/stable/10.5325/jinfopoli.5.2015.0155.

Huang, Jingwei, and David M Nicol. 2013. "Trust mechanism for cloud computing." *Journal of Cloud Computing Advances, Systems and Applications* 2 (9). doi:10.1186/2192-113X-2-9.

Kahneman, Daniel, and Amos Tversky. 1979. "Prospect Theory: An Analysis of Decision under Risk." *Journal of Econometric Society* (The Econometric Society) 47 (2): 263-292. http://www.jstor.org/stable/1914185.

Kesan, Jay P, Carol M Hayes, and Massoda N Bashir. 2013. "Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency." *Washington & Lee Law Review* 70 (1): 365. http://scholarlycommons.law.wlu.edu/wlulr/vol70/iss1/6.

Khan, Khaled M, and Qutaibah Malluhi. 2010. "Establishing Trust in Cloud Computing." *Cloud Computing Journal* (IEEE Computer Society).

Manavati, Mihir, Patrick Colp, Bill Aiello, and Andrew Warfield. 2014. "Users' trust in cloud systems is undermined by the lack of transparency in existing security policies." *Journal of Association for Computing Machinery* 57 (5). doi:10.1145/2593686.

Michael, B. 2009. "In clouds shall we trust?" *IEEE Security and Privacy* 7 (5). doi:10.1109/MSP.2009.124.

Najjar, M, and M Kettinger. 2013. "Data Monetization: Lesson from a Retailer's Journey." *Management of Information Systems* 12 (4): 213-225.

Padilla, Roland S, Simon K Milton, and Lester W Johnson. 2015. "Components of service value in business-to-business Cloud Computing." *Journal of Cloud Computing: Advances, Systems and Applications* (Springer Open Journal) 4 (15). doi:doi 10.1186/s13677-015-0040-x.

Parker, J. 2012. "Lost in the Cloud: Protecting End-User Privacy in Federal Cloud Computing Contratcs." *Public Contract Law Journal* 41 (2): 385-409.

Prantosh, Paul Kr, Karn Bhaskar, and R Rajesh. 2015. "Cloud Computing and its Deployment Model: A Short Review." *International Journal of Applied Science and Engineer* (New Delhi Publishers) 3 (1): 29-36. doi:Doi: 10.5958/2322-0465.2015.00005.2.

Quedraogo, Moussa, Severine Mignon, Herve Cholez, Steven Furnell, and Eric Dubois. 2015. "Security Transparency: the next frontier for security research in the cloud." *Journal of Cloud Computing* (Springer Open Journal) 4 (12). doi:doi: 10.1186/s13677-015-0037-5.

Rai, A, and S Sharma. 20113. "Privacy Issues Regarding Personal Data In Cloud Computing." *Journal of Advanced Research in Computer Science* 4.

Rajadarshini, M, and R Alageswaran. 2016. "Optimal Double Renting Scheme Based Dynamic Virtual Machine Provisioning and Allocation for Improving QoS and Profit Maximization." *Advances in Natural and Applied Sciences* 10 (10): 281-288.

Rastogi, Nidhi, Marie Joan Kristine Gloria, and James Hendler. 2015. "Security and Privacy of Performing Data Analytics in the Cloud: A Three-way Handshake." *Journal of Information Policy* (Penn State University Press) 5: 129-154. http://www.jstor.org/stable/10.5325/jinfopoli.5.2015.0129.

Reopel, Robert G, Michael R, Jeanne Mey Sun, and Stephen M Tanny. 2004. "Turning value into money." *The Journal of Business Strategy* (Emerald Group Publishing Limited) 25 (4): 25-30. doi:DOI 10.1108/02756660410547368.

Santosh, Kumar, and R. H Goudar. 2012. "Cloud Computing-Research Issues, Challenges, Architecture, Platforms and Applications: A Survey." *International Journal of Future Computer and Communication* 1 (4): 356-360. doi:10.7763/IJFCC.2012.V1.95.

Sasikala, S, and S Suresh. 2016. "An Adaptive Approach for Efficient Energy Saving Technique in Enterprise Cloud Data Centers." *Advances in Natural and Applied Sciences* 10 (6): 164-169.

Sehgal, Naresh K, Sohum Sohoni, Ying Xiong, David Fritz, Wira Mulia, and John M Acken. 2011. "A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing." *IETE Technical Review* 28 (4).

Srinivasan, S. 2013. "Is Security Realistic in Cloud Computing?" *Journal of International Technology and Information Management* 22 (4).

Syal, Subina, and Menka Goswami. 2012. "Effective Cloud Computing: Innovations and Challenges." *International Journal of Management Research and Review* (IJMRR) 2 (10): 1800-1809.

Tversky, Amos, and Daniel Kahneman. 1992. "Advances in Prospect Theory: Cumulative Representation of Uncertainty." *Journal of Risk and Uncertainty* (Kluwer Academic Publishers) 5: 297-323.

Veeralakshmi, Ponnuramu, and Tamilselvan Latha. 2016. "Secured Storage for Dynamic Data in Cloud." *Informatica* 40: 53-61.

Vilkomir, Sergiy. 2012. "Cloud Testing: A State of the Art Review." *International Journal of Information & Security* (ProCon Ltd) 28 (2): 213-222.

Willcocks, Leslie P, Will Venters, and Edgar A Whitley. 2013. "Industry Insight Cloud sourcing and innovation: slow train coming? A composite research study." *Strategic Outsourcing: An International Journal* (Emeral Group Publishing Limited) 6 (2): 184-202. doi:Doi: 10.1108/S0-04-2013-0004.

Wixom, Barbara H. 2014. "Data Monetization in Action." *Center for IS Research Briefing XIV.* Center for Information Systems Research .

Woerner, S, and B Wixom. 2015. "Big Data: extending the business strategy toolbox." *Journal of Technology* 30: 60-62. doi:10.1057/jit.2014.31.

Yunchuan, Sun, Zhang Junsheng, Xiong Yongping, and Zhu Guangyu. 2014. "Data Security and Privacy in Cloud Computing." *International Journal of Distributed Sensor* (Hindawi Publishing Corporation) 2014. http://dx.doi.org/10.1155/2014/190903.

Zhang, Weishan, Liang Xu, Pengcheng Duan, Wenjuan Gong, Qinghua Lu, and Su Yang. 2015. "A video cloud platform combing online and offline cloud computing technologies." *Personal and Ubiquitous Computing* 19: 1099-1110. doi:Doi: 10.1007/s00779-015-0879-3.

****