Asian Journal of Information Technology 16 (1): 53-60, 2017
ISSN: 1682-3915

Analysis of Cloud Computing Security Issues in Small Business Environments in Northern Territory

[1]Christopher Sudjana, [2]Kazi Naimul Bari, [1]Sami Azam,
[1]Kheng Cher Yeo and [1]Bharanidharan Shanmugum
[1]School of Engineering and Information Technology,
[2]School of Law, Education, Business and Arts,
Charles Darwin University, Casuarina, Australia

Abstract: Cloud computing is a relatively matured concept and its adoption into business still remains slow. Uncertainties risen from lack of promotion and support of cloud services result in missed opportunities for the public. The purpose of the study is to identify the security issues in cloud computing for small local businesses in Northern Territory, Australia. This study recommends information packages and financial support for cloud clients. These mitigate rash and uninformed decisions and certain security risks. It appears that there is a lack of certified professionals who work in the cloud. Most cloud personnel are gathered from other disciplines of the IT industry to fulfil cloud roles. To combat this, official accreditation and incentives are required not only to create needed professionals but also to retain them. Through education and support, cloud computing can manage its place in the world and also able to gain momentum in small business.

Key words: Cloud issues, cloud solutions, cloud security alliance, certification, small business, gartner, risk

INTRODUCTION

The cloud environment is an ever-changing and evolving part of the IT industry. As such, the security front is always adapting to mitigate harm. However, it is an irrefutable fact that no security is perfect. The aim of this study is to investigate the many security issues, threats and associated solutions; if any. All of the above facet aid in raising awareness of risks in the cloud for users to defend against them. Analysis of research materials are used to ascertain any notable gaps in the cloud security discussion. The demand is growing rapidly for the types of services that provide to small businesses via cloud computing (Hutchings *et al*., 2013; Gupta *et al*., 2013). Through the use of small businesses in the Northern Territory (NT), Australia; analysis is placed in context to address cloud issues in this manner. From this, ideas to improve cloud security towards identified issues are proposed. The application of this knowledge will be used to strengthen the area of cloud computing in the regional areas of Australia.

Cloud computing overview: Cloud computing is an emerging technology which brings numerous benefits with its use. In lieu of this, there are many issues which surround its existence. Security issues in particular which has always been at the forefront for IT technologies. To safeguard against these threats, awareness must be raised of their existence to ensure the growing use of cloud computing into the IT world. From this understanding solutions can be proposed to counteract the impeding possibility of security breaches. In a dynamic and often erratic environment, the battle in the cloud is an endless struggle.

Security in the cloud: It is a well-known fact that data traversing the internet is not always secure. That is to say, there are no assurances to the safety and integrity of the data being sent or received. Thus, data security that consists of compliance, privacy, trust and legal matters becomes a common fear that often leads to hesitation when employing cloud computing system (Sun *et al*., 2014; Timmermans *et al*., 2010). In that sense when entrusting information, data and services to a third party, it is a matter of mutual trust which carries considerable risk. Data ownership plays a vital role in cloud computing (Ahmed and Hossain, 2014). Some of the issues including who owns what is stored on servers and storage media? Is it the service provider or the client? It is important to communicate with providers to know their policies and regulations (Chilcott, 2011). On that note, a client's data may be stored on the same device as data from other clients. Though the data is encrypted, the security risk of which the circumstances present can potentially ruin

Corresponding Author: Christopher Sudjana, School of Engineering and Information Technology, Charles Darwin University, Casuarina, Australia

businesses. This is a security risk concerning segregation of data where unauthorised access is a possibility.

Most security issues are associated with the service provider themselves. The benefits which the service provider bestows upon a client are great but it is based on volatile trust. Healthy relationships between provider and client do not remove the possibility of corruption and self-gain. The underlying risk is that if one suspects the service provider of foul play, it may not result in any judiciary action. Cloud computing is still not matured as such the legal implications surrounding it are somewhat blurred and not entirely set. Hence, cloud computing is considered a hellish agenda for law practitioners. To make matters worse, the organisation's concerns may not even warrant any investigative action through legal means.

Generic cloud security issues: The Cloud Security Alliance (CSA) is renowned as being an organisation leading the front in safeguarding the cloud. According to the official 'top threats to cloud computing v1.0" created in 2010; there are seven main issues to remain wary of (CSA, 2010). The threats listed are not based on severity and are the product of subjective opinions by the contributing collaborators of the CSA document. CSA has also proposed corresponding solutions to each of the issues they describe.

Abuse and nefarious use of cloud computing: This risk mostly concerns the end user or the client side of cloud computing. Providers of iaas offer their customers the "illusion" of unlimited computing, networking and storage capacity. Anyone with a valid credit card can register for these services, some providers even going as far as to offer free trials for a limited duration. In many cases the registration process can be defined as "frictionless". Meaning the registration form consists of only small number of steps and does not require too many details. Black-hat hackers, spammers and other criminals take advantage of the anonymity to perform their illicit acts without constraints and relatively low chances of being caught (CSA, 2010).

The future concerns related to the cloud computing involve hacker's persistence and intuitiveness (CSA, 2010). Criminals take advantage of the advances of technology to forward their own gains. Improve their methods and avoid detection through the coverage of anonymity brought on by weak registration systems.

Insecure interfaces and APIs: Software interfaces and API sets are generally provided to consumers by service providers to manage and interact with corresponding cloud services. "Provisioning, management, orchestration and monitoring are all performed using these interfaces" (Mell and Grance, 2011). The security of these APIs affects the security and availability of general cloud computing services. They include several authentication and access controls, encryption and activity monitoring within the service. The security surrounding this is designed to safeguard against accidental and malicious incidents. Organisations and third parties often develop these APIs to enhance customer service with value. It adds a sense of complexity to the API with new layers. However, this also places organisations at risk as they may be asked to surrender their credentials to "enable their agency" (Mell and Grance, 2011). By relying on weak interfaces and API sets, an organisation is confronted with various security issues. These issues often relate to the accountability, availability, integrity and confidentiality (CSA, 2016).

Malicious insiders: The human element combined with ambition and personal gain is a volatile mix harmful to organisations and consumers alike. The magnitude of this threat is increased due to the convergence of IT services and customers under a single domain. General transparency of the provider's processes and procedure also add to the increase in threat severity. An example would be the with holding of certain information and details to the consumer. This may include how employees access organisation assets both physical and virtual and how policy is maintained through the management of employees. More often than not, there is little "visibility into the hiring of cloud employees" (Mell and Grance, 2011). This can lead to "attractive opportunities" for any party who wish to take advantage (Mell and Grance, 2011). Such groups could range from typical black hat hackers to organised crime, even corporate espionage and federally sponsored intrusion is possible. It is found that insider-attack is another threat for cloud computing (Ahmed and Hossain, 2014). According to CSA, malicious insider includes current or former employee, business partner or contractor who might affect the safety and integrity of the business information (CSA, 2016). Among those, the most dangerous malicious insider to an organisation is the employees themselves. This is due to their knowledge of how the business operates; the existence of certain assets as well as the access they have. The world is slowly transitioning into the cloud. Thus, the human element becomes ever more important to alleviate the negative impact of this threat.

Shared technology issues: This threat typically affects Infrastructure as a Service (IaaS). By sharing infrastructure, IaaS providers provision their services in a scalable way. The underlying components of this service infrastructure do not offer "strong isolation

properties for a multi-tenant architecture" (CSA, 2010). This problem was addressed by what is known as virtualisation hypervisors. Hypervisors mediate the access between guest operating systems and the physical computing resources. Even with these there still exists a notable flaw. Guest operating systems still manage to gain inappropriate high levels of access and control of the underlying platform. A recommended defence against this issue is to focus on storage and network security "enforcement and monitoring" (CSA, 2010). Moreover, "strong compartmentalisation" should be implemented to ensure individual customers do not interfere with other tenants of the cloud. This means they should not be able to access other tenant's data, network traffic, etc.

Attackers focus on how to affect the operations of other cloud customers. The goal is to gain unauthorised access to data. Attacks spring from the fact that disc partitions, CPU caches, GPUs and other shared elements were never designed for supporting the "strong compartmentalisation" (CSA, 2010). Overall, shared elements in the cloud are at risk from interfering with one another. The collective data can be exploited rather easily.

Data loss of leakage: Data loss and leakage are one of the greatest concerns for anyone. There is a multitude of ways data can be compromised. These can include altered, deleted, lack of backups, use of unreliable storage media, loss of encrypted key, etc (CSA, 2016). An obvious threat is unauthorised access to sensitive data. Any incident made by this threat can impact morale and trust from customers, employees and business partners. Depending on the data which is leaked or lost, there may be financial, competitive and even legal ramifications. It is believed that this threat increases due to the following reasons:

- "The number of interactions between risks and challenges are unique to the cloud" (CSA, 2010)
- "More dangerous because of the architectural or operational characteristics of the cloud environment" (CSA, 2010)

Account or service hijacking: The issue of "hijacking" accounts and services is very common and renowned throughout the world. Common incidents include fraud, phishing and the exploitation of vulnerabilities in software and infrastructure (CSA, 2016). The primary objective of committers of this threat is the possession of sensitive information. This includes credentials and information which holds any potential financial benefit. With such information, an attacker can use the new found access to infiltrate areas which would be much harder to enter. In addition, whilst using the authority of a guise an attacker can launch consecutive attacks. Once in, one could spy on activities and transactions, manipulate data, falsify information and redirect stolen information to a third party. Information which is redirected is generally used for more nefarious purposes. Organisations need to be wary of this threat at all times. Its potential to compromise integrity, confidentiality and availability of services is too great to ignore. An organisation should devise plans to deal with this threat to avoid overwhelming damages and possible legal implications.

Unknown risk profile: A defining characteristic of cloud computing is the reduction in hardware and software ownership. This has many benefits like decreased costs. However, there are underlying "contradictory" security concerns (CSA, 2010). This is mainly due to parties who begin to lose track of security and focus on the anticipated benefits of cloud deployment. There are various factors that one should consider to create a realistic idea of their security stance. According to CSA (2010), lists the following:

- Version of software
- Code updates
- Security practices
- Vulnerability profiles
- Intrusion attempts
- Security design
- Who infrastructure is being shared with
- Network intrusion logs
- Redirection attempts and/or successes

Gartner security issues: Gartner produces many documents concerning the management and security of information and information technology. They have identified seven main areas of consideration and concern, consumers should be aware of before adopting the cloud (Brodkin, 2008).

Privileged user access: There are high levels of inherent risk involved when sensitive data is processed from outside the organisation. This is due to the fact that third party services generally bypass "physical, logical and personnel controls" that IT oriented people keep in mind (Brodkin, 2008). It is wise to gather as much information about service providers before conducting business. Know how data is being controlled and stored and the access controls in place to ensure privacy is maintained.

Regulatory compliance: Even though data is in the possession of a service provider, the overall responsibility of data integrity and security falls onto the customer. Traditionally, service providers were required to undergo external audits and security certifications. There are often organisations who do not comply with recognised standards and regulations. Providers who refuse to "undergo such scrutiny are signalling to customers that they can only use them for the most trivial of functions" (Brodkin, 2008). It also raises suspicion of illicit activity that the provider may be involved in if any.

Data location: Since, data exists in the cloud, its physical location could potentially be anywhere in the world. It is unnerving to customers not knowing where data is stored and what could be happening to that data. Therefore, providers need to ensure the transparency of data location that enables to build customer trust regarding data security. Though, location transparency is one of the major advantageous of cloud computing, it poses security threat as well (Ahmed and Hossain, 2014). It is important to communicate with providers to ensure that they will abide by legal jurisdictions and policies. These include contractual agreements stating they will commit to privacy requirements on behalf of their respective customers (Brodkin, 2008).

Data segregation: Generally when data exists in the cloud, its storage is shared with data from other consumers. It is found that encryption is effective but cannot completely protect data from unauthorised activity (Brodkin, 2008). Gartner advises people to ascertain how data is segregated while it is at rest. Providers of cloud computing services should provide explicit details as well as reassuring evidence that data encryption are in place. These encryption systems should be designed and tested by knowledgeable and experienced specialists. Gartner states that incidents involving encryption can result in unusable data. As well as this, encryption can affect data availability in general (Brodkin, 2008).

Recovery: Cloud computing service providers have the obligation to tell their customers how data is managed during a disaster event. Can the provider ensure that no data will be lost and remains uncorrupted? Can the provider promise to be able to perform a complete restoration? These are questions a customer must ask to be able to lower the chances of such an event affecting them. Gartner states that service providers who does not "replicate data and application infrastructure across multiple sites is vulnerable to total failure" (Brodkin, 2008).

Investigative support: Most people can take legal action towards several different incidents of the IT industry. However, it is very difficult to do this for cloud computing issues. Gartner states that cloud services are difficult to investigate, practically impossible (Brodkin, 2008). It is very difficult to gather confronting evidence to support claims against service providers who may have committed such acts. The grey areas in cloud computing incidents leave legal representatives worse for fear.

Long-term viability: The probability of this risk is relatively low. This risk concerns the service provider's existence in the market. In other words, if the current provider business is took over by another company, then how to put safety against data security that might prevent misuse of data by new owner. The underlying issue here is the changing of hands. Will data still be safe in the possession of a new party? Will the data be available to you and if so will you be able to get it all back? Customers should ask potential service providers how they can get their data back and under what conditions. Again this is an unlikely occurrence but consumers should be wary of it all the same.

Small business: Though, small business has significant impact on Australian economy, there is no unique definition for small business established by the regulatory body in Australia. Small businesses account for more than a third of production and half of the employment in non-financial private sector. Different regulatory bodies try to define small business based on different criteria such as loan size, number of employees, revenue and balance sheet indicators that derived from the law they administer. Australian Bureau of Statistics (ABS) defines small business in terms of number of employees. ABS describes business which operates with <20 employees as small business. On the other hand, ATO explains that an organization having less than $2 million turnover annually is called small business (ASIC, 2016).

Small business and cloud computing: The benefits to adapt cloud computing in small business are enormous. That includes security and privacy, reduction on cost, sharing and collaboration, reliability and ease of use and convenience (Devasena, 2014; Albakri *et al*., 2014). To provide relevance to the context, a local IT business and cloud provider offered input on the matter of cloud security. Much of the contribution from interview confirmed the research undertaken. It was revealed that the most popular service delivered to local small businesses was infrastructure followed by software. This

involves allowing businesses access to ICT infrastructure whist removing recurring capital costs (Devasena, 2014). The director of technology agreed with the idea that the best way to manage a threat is to be aware and educated about it. "You can't manage it if you don't know what it is" (darwin business representative). As a rapidly changing and evolving environment, it pays to be proactive. Only through putting the best effort in can one get the best results. This includes requisitioning the best technology and creating effective policies and practices. As a business and service provider customer satisfaction is a priority. Reassuring the customer that security can be tailored and delivered according to their needs is a responsibility. Communication is crucial with customers. Most of the time customers will not know what they want or fully understand their needs. It is this stage which is crucial in truly mitigating any risks that are associated. The recount detailed how an interstate business was forced to change their cloud provider due to contract discrepancies. The unnamed business was presented with a service contract very similar to many other providers. However this was not delivered to a high standard. To summarize, the provider utilised cheap and inexpensive technologies to provide the service.

The security risks that businesses face are essentially all that have been detailed in this project thus far. Common risks like hacking, malicious code, data loss or unauthorised manipulation are all considered. To confront these risks, common approaches like firewalls, encryption and redundancy are implemented. In terms of redundancy, this should be done to compensate for all manner of possibility. Extra generators, servers, routers, connection lines data centres and data. All of these in place ensure continuity and availability of services. To be able to ensure security in the cloud, one must cater for the physical and the logical risks. Equipment concerning cloud computing is undoubtedly expensive and hence having physical obstacles for offenders is a necessity. Surveillance, guards, locks and the like are but examples.

Improvements for the small business: From the summary of interview, suggestions are provided to improve the security situation. It is also found that there is a shortage of professionals in the NT and that IT businesses often have to hire from other states (darwin business representative). It is imperative to try and create incentives for professionals to stay in the NT. Having more accreditations for professionals would definitely improve the security situation.

MATERIALS AND METHODS

For the purpose of studying security issues in the cloud both primary and secondary data are used in this study. As a secondary data, literature from different journal articles, government websites and IT specialist company websites have taken into account whereas an interview and questionnaire survey was conducted in Northern Territory to obtain primary data for this research. An IT firm's specialist interview was taken from Northern Territory and used for the study purpose. The questionnaire was developed based on the security issues discussed in literature.

RESULTS AND DISCUSSION

Even though cloud computing is still considered a 'buzz word' and in its infancy, so much has been done already. In short, most if not all issues in the cloud derive from areas preceding it. Ideas about privacy and protecting data and how important security is have been emphasised several times over. Many of the suggestions and recommendations come from large organisations or collectives with extensive experience and knowledge. Hence they suggest constructing policy or a technical solution which appear to relate to parties similar to themselves.

Of all of the research material collected thus far, few hint at education as a strategic option. The most likely reason is that it is something so fundamentally simple that it is considered obvious. An assumption that people will actively seek the knowledge they need. However, this alone does not help create proficient individuals within the industry. The IT industry currently has many people who utilise the cloud. There are few who exist and work in the cloud. Those who do; come from several other disciplines of the IT industry and adopt cloud roles. From current research there is yet to be an actual certification for professionals in the cloud. Owing to the fact that IT is becoming a critical part of the world, establishing professions seems a logical course of action.

As mentioned, the cloud is still young and has not been adopted or fully understood. The Northern Territory is no exception. Few businesses use the cloud and its advantages. The main reason being that not many businesses have need of it. However, for those that do, it cannot be said that security is implemented at its best. The main reason people are often hesitant about considering cloud is fear. It is still a large unknown. Even if one were to make use of it, it does not mean they can afford to implement a series of security measures on their side. To elaborate, the providers may offer their security services but that may not extend as far as the client side of the environment. As of yet there are no groups providing security assistance exclusively for such consumers. It may not be necessary now but it would best to be prepared for impending risk.

From the research material that has been accumulated thus far, the following can be stated. The vast majority of material which has been published highlights many threats and risks. The most proposed course of action is usually a technical one. What has been seen lacking in these documents is something fundamental and logical. A pre-emptive and proactive course of action generally begins with 'knowing thy enemy'. It is often an aspect people tend to overlook as they focus on how to react to specific threats as quickly as possible.

Another recommendation comes from the idea that the cost to improve security is undeniably expensive. This problem mainly concerns consumers as opposed to providers. The need to assist those who wish to improve security can have underlying benefits. This may not necessarily be achieved through monetary means.

Cloud computing certification: As of yet, a certification for a professional who works extensively and exclusively in the cloud is yet to be established. Though cloud computing takes aspects from several branches of IT; the cloud is still an entity unto itself. The growing 'buzz word' is vastly gaining ground in the industry as more organisations find intrigue in deploying in the cloud. Due to this, there is a foreseeable rise in the need for personnel who possess the desired skill set to thrive effectively in the cloud.

The establishment of an official certification for cloud professionals is needed. This can be provided at certain levels or areas of focus. Currently people who work in the cloud usually enter the environment with background pertaining to a certain IT discipline. Depending on the business, a training program may follow. This training may cover fundamentals of the cloud as sufficient knowledge to function within the organisation. The position at the business will most likely determine the extent of training or exposure an individual may have. Being proactive to remain aware of the cloud is encouraged. To learn as one goes can be effective in its own right. However, due to the evident growth in technology and need for IT professionals; especially in the NT; official certification is direly needed. The roles of the cloud are gradually becoming specialised. Only certified people with specialisation can fill in these roles. The main challenge to implement this is the recognition and support of institutions that understand its importance. From there, setting standards and expectations as to the capabilities and potential these professionals will have need to be considered. Material pertaining to the course and its structure are also important factors. In regards to the NT though, there is a renowned issue concerning professionals. It has been a long standing problem that specialists and experienced professionals often leave for 'better prospects'. The fact of the matter is that many people do not see much incentive in staying in a relatively small and remote area. By providing clear career paths and positions which appear fulfilling, this issue can be greatly mitigated.

Cloud consumer assistance programs: The main reason cloud consumers turn to the cloud is that it is an affordable option. In a 'make-or-buy' situation, most circumstances dictate that 'buying' is inherently the cheaper choice. Resorting to a cheaper option would suggest that other outlooks may be out of reach. Not to say that security exists at a poor level. The ability to safeguard against greater threats may not be possible. To function with cloud services, the necessities are expected. Thus, logical firewalls, anti-virus applications, adequate IT knowledge and physical security are the few names. The need for more sophisticated security measures may not be as dire in initial stages. However, if operational expansion is on the rise then more security is required to compensate.

Essentially cloud users like small business and groups require assistance. This can be provided in a manner of ways. The extended benefits of pursuing this venture involve promoting business. If there is assistance to integrate IT assets and protect them, then more parties are more willing to take part in such business.

Equipment and security packages: The cost of specialised security software and hardware is costly to say the least. Local business (darwin business representative) revealed that a new physical firewall was valued at close to A$100 000. Though most people would not require such equipment, it is an example of how difficult it can be to acquire quality security assets. To alleviate this dilemma, a program or funding of some kind needs to be implemented. A means of aiding interested parties in obtaining quality security to improve security capability. Financial backing is necessary to realise this. Thus far, it cannot be seen as to what organisation may endorse this plan other than the government. In addition, the venture will only proceed if the benefits are substantial. The following factors are most likely to influence the decision:

- The cloud gaining popularity as cloud gains presence in the NT more security is required to protect what exists in the cloud
- Technology growth technology develops exponentially and often spontaneously. The integration of IT assets and the increase of data per annum will see more use of cloud infrastructure services to fill the void

- Security asset costs advancements in technologies will lower the prices of existing tools and hence will favour benefit over cost in such decisions

Published and distributed guidelines: Another method to assist NT businesses is to distribute or make available a set of guidelines or information packages. The related document would include details of how to best defend against certain threats in the cloud environment. The term 'guidelines' is being used because; different parties have different approaches to different problems. A set of guidelines which describe what can be considered sufficient security. This description would account for the type of business. For instance its scale, industry and primary uses of IT or information and reflects predefined business archetypes. It may also highlight what are the most likely threats for that businesses cloud implementation. The document may be a booklet or a handout of some kind via and to cloud providers.

The information packages mentioned earlier can be simple or very technical and elaborate. Similar to the 'guidelines' mentioned above, these packages are more descriptive and content heavy. Such information packages will be made available to those who wish to increase knowledge pertaining to cloud security risks. This may be done via physical documents or paid sessions via consultants. Simple versions highlight certain security risks and provide an overview of existing solutions. More sophisticated versions will suggest more technical solutions be more descriptive and can be more specific. That is, if a certain risk arises there is a process provided or a specific action to take that proves most effective for that issue. The main challenges to implement this include the following:

- Finding a group to produce content
- Getting it distributed
- Promoting its existence and use
- Keeping it relevant through updates. Frequency of updates is also a consideration

CONCLUSION

The research has shown that issues within the cloud can be described as old problems within a new context. Most publications thus far have proposed technical and policy based solutions to mitigate risk and impact. Privacy, data protection, service availability and assurance are what concerns cloud users most. These have been elaborated and reiterated upon countless times. Few hint on the idea of education as a strategic option. Analysis shows that the gradual migration into the cloud environment will increase the demand of specialists in this field. As the roles of cloud become more specialised, recognition of professionals is needed. Thus an official certification is recommended. On another note, the security from NT cloud providers appears adequate but the same cannot be said for all consumers.

RECOMMENDATIONS

Aiding in the acquisition of security assets for businesses in need helps maintain a benchmark for security as a whole. By applying these recommendations, the IT sector of the NT can expect to improve cloud security. This also reassures that cloud is a safe and supported venture and will encourage the adoption of cloud technology for interested parties. Education, understanding and collaboration are the keys to improving the security state of the cloud in darwin. The research here can benefit others in the world so that this technology can reach higher potential comfortably under security.

Initially, a survey was conducted in local small businesses in Northern Territory to identify the security issues encountered in cloud computing and provide some recommendation on how to deal with those security problems in future. In regards to further work about cloud computing, communication with various institutions in Australia is recommended so that future study can be conducted in developing a frame work or model that may include any new parameters along with existing issues discussed in this paper to mitigate the security risk in the cloud. Request time to question the viability of ideas discussed in this paper and respective party interests. Such parties include ICT industries, government agencies, universities and business farms. Discuss whether any other recommendations are necessary, relevant and if there are alternatives. Further research can also be done by placing above recommendation in practice to see whether the local businesses overcome the security issues in cloud computing or not and that the underlying benefits outweigh the costs.

ACKNOWLEDGEMENT

Researchers are thankful to Charles Darwin University for providing the funding support and necessary facilities for the preparation of the research.

REFERENCES

ASIC., 2016. Small business-what is small business. Australian Securities and Investments Commission, Sydney, Australia.

Ahmed, M. and M.A. Hossain, 2014. Cloud computing and security issues in the cloud. Int. J. Network Secur. Applic., 6: 25-36.

Albakri, S.H., B. Shanmugam, G.N. Samy, N.B. Idris and A. Ahmed, 2014. Cloud computing adoption challenges. Adv. Sci. Lett., 20: 546-548.

Brodkin, J., 2008. Gartner: Seven Cloud-Computing Security Risks. Network World Inc, Framingham, Massachusetts,.

CSA., 2010. Top threats to cloud computing. Cloud Security Alliance, Singapore.

CSA., 2016. Top threats to cloud computing. Cloud Security Alliance, Singapore.

Chilcott, B., 2011. Cloud computing policy and guidelines. Department of Corporate and Information Services, Australia, Oceania.

Devasena, C.L., 2014. Impact study of cloud computing on business development. Oper. Res. Appl. Intl. J., 1: 1-7.

Gupta, P., A. Seetharaman and J.R. Raj, 2013. The usage and adoption of cloud computing by small and medium businesses. Int. J. Inf. Manage., 33: 861-874.

Hutchings, A., R.G. Smith and L. James, 2013. Cloud computing for small business: Criminal and security threats and prevention measures. Trends Issues Crime Criminal Justice, 456: 1-8.

Mell, P. and T. Grance, 2011. The NIST definition of cloud computing. National Institute of Standards and Technology, Gaithersburg, Maryland. http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Sun, Y., J. Zhang, Y. Xiong and G. Zhu, 2014. Data security and privacy in cloud computing. Int. J. Distrib. Sensor Networks, 2014: 1-9.

Timmermans, J., B.C. Stahl, V. Ikonen and E. Bozdag, 2010. The ethics of cloud computing: A conceptual review. Proceedings of the 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom), 30 November-3 December, 2010, IEEE, Delft, Netherlands, ISBN:978-1-4244-9405-7, pp: 614-620.