World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 7, No. 1, 1-6, 2017

Impact of Security Issues in Cloud Computing Towards Businesses

Bader Methqal AlFawwaz
Department of Computer Information Systems
Al al-Bayt University, Jordan

Abstract—Cloud computing structures allow businesses to save expenses by subcontracting computer related activities on-demand. However, customers of cloud computing facilities presently have no sources for authenticating privacy and reliability of their confidential data. Cloud servers are skillful of managing large quantities of shapeless data to support recognizing, improving and then making new planned business prospects. Company's administrators recognize that appropriate and precise information can turn out to be enhanced business performance. These days' cloud tools are dominant in enlightening the qualitative and quantitative worth of the confidential data presented to executives of the organizations. In this paper, we debate that apprehensions about the privacy and reliability of their data and other electronic material are a main restrictive factor for company's desire to adapt cloud-computing facilities. The concept of passing over confidential information to a third party is troublesome, this ultimately means that the customers need to be attentive in accepting the threats of data breaks in this novel situation. The methodology of this paper is based on literature analysis. For results, researcher has studied published work on cloud computing security and how these issues leading companies having loss in business. Further, this research presents a thorough study of the cloud computing safety problems and experiments concentrating on the cloud computing categories and the service supply kinds. The research is helpful for those company managers, owners, policy makers and decision makers, which are mostly dependent on the cloud services while taking decisions.

Keywords-Cloud Services; Cloud Business; Cloud Computing; Cloud Security.

I. Introduction

Cloud computing is among the latest developments in the world of computing technology. It involves the use of shared information technology resources stored within a network [1].

Prior to the development of cloud computing technology, the storage of data and necessary applications have been done on personal computers or servers. The disadvantages associated with the personal storage of data and application inspired motivation for the development of cloud computing. As the name suggest, cloud computing makes use of a single network resource, for hosting multiple users interested in using common resources such as computers applications. The development of cloud computing technology is arguably a procedural occurrence. The development of different computing technologies based on the concept of data sharing and resources allocation inspired the development of virtual servers. Such servers are not necessarily stored in user's computers, but are remotely located in 'cloud' format. The storage of data is thus no longer dependent of highly performing hardware for continued functionality. However, the latter remains necessary for optimized performance of the different users connected to the particular network. Security issues remain a major challenge after the development of cloud computing the related technologies. Where sharing of resources is the common approach to the implementation of the concerned technologies, the vulnerability associated with such sharing options create a loophole for the execution of online attacks. The benefits associated with cloud computing are innumerable, however, implementation of necessary security measures remains equally important. The methodology of this paper is conceptual analysis of published work on cloud computing, security and the difference in approach to computing, introduced through cloud computing. Further there is review of published literature, with interest in making an analysis of security issues surrounding the use of cloud computing. This methodology is based on a substantive review of the literature mainly on the cloud computing and the security issues in the context of worldwide. The existing state of knowledge through literature review reveals the relevant concepts, methods and technique about the particular investigation. The discussion of the paper center around the gaps identified in the course of literature review. The conclusion features a summary of the different elements discussed in the paper, with recommendations on the subjects at the end.

II. Literature Review

Data breaches ranks among the leading threats with respect to cloud computing [2]. The breach of data involves the unwarranted access to personal information and data for individuals connected to a cloud-computing network. In such a case, the data in question is usually not encrypted and revealed to third parties with the intent of compromising the same [3]. According to [2], the loss of personal gadgets or devices such as phones or laptops, through theft, can give attackers the opportunity to access personal information. Once the attacker has gained entry into an identified cloud-computing network, he can manipulate the system and steal vital information. On a larger scale, the attack can infiltrate to other users connected to the network, considering that cloud computing necessarily involves the sharing of resources and at times, computational data. As [3] continues to note, the effects of data breaches go beyond the loss of personal information to include loss of data for entire organizations. Where attackers gain access into a network sharing vital data on the management of a company, they are able to delete, compromise or steals the concerned information, all of which remain detrimental to the running of the concerned organization. As the authors note, the prevention of data breaches forms an integral area in security considerations for cloud computing security. Hence, ensuring data security at the personal level and the same at the organizational level goes a long way in ensuring that cloud computing remains effective in empowering individuals as well as business interactions.

Data Loss is an additional security issue associated with the world of cloud computing. [4] notes the impact on individuals as well as organizations, associated with the loss of vital data. The author notes specific instances in history, where large organizations lost user's data in one or several ways. Where the loss of data involves a single individual, the impact is less significant with respect to the running operation of the business environment. However, the situation gains significance where the loss of concerned data is from a large organization entitled to the protection of many user's personal information [4]. The author proceeds to propose different ways through which individuals as well as corporations can protect themselves against the accidental or manipulated loss of vital data. [5] introduce a different dimension to the discussion, where they argue on the importance of data recovery in the case of loss. Whereas cloud computing is a necessarily new field in the course of computational technology, the safeguarding of important data and ensuring the recovery of the same in the event of loss remains an issue of concern [5]. The recovery of different types of data requires different lengths of time and resources for the accomplishment of the same. Hence, creating awareness for the users of a particular network is essential in ensuring that the concerned members fully understand the measure of risk they are exposed to in the course of using cloud-computing environments.

[6] highlights the importance of security in the use of cloud computing through the use of secure interfaces. Users connected to a cloud-computing network make use of administrative interfaces as gateways of accessing the resources available therein. Where a single user makes use of a compromised interface for logging-in to a cloud-computing network, they expose the entire network to risk. As [6] continue to note, the use of secure gateways for the access of cloud computing resources is important in ensuring the same remains available and secure to other users of the network. One of the main approaches in ensuring that interfaces remain free from corruption is through education of the concerned users. Where an interface is corrupted and likely to provide an intrusive point for an attacker, knowledge on how to handle the point of weakness on the concerned interface is of high importance. The arguments surrounding the integrity of interfaces is developed in the work of [7]. The author explores qualities of secure software and the impact of the same with regards to the efficient running of businesses. Interfaces connected to cloud computing environments provide access points for different individuals connected to the networks to gain access into the same. Further, modification of elements is made on the concerned interface, affecting portion of, or entire parts of a cloud-computing network [7]. The integration of proper authentication measures and filtering procedures remains the best approaches in ensuring that interfaces maintain their integrity and maintain a high 'uptime guarantee'.

Account traffic hijacking is the additional form of security threat with respect to cloud computing [8]. [9] notes that account traffic hijacking attacks are not a new concept in the world of computing. He cites that such attacks have existed for a prolonged period of time in the past. However, in the wake of cloud computing, the impact associated with such attacks is far devastating. Where an attacker gains access into an encrypted service, they are able to intercept additional information sent over the network. The concerned attacker uses credentials associated with a single user, connected to the cloud network. Such credentials have the example of usernames and passwords necessary for gaining access to user account. Once into the system, the attacker is able to divert traffic to an illegitimate destination, which more often than not is a clone of the original site. The systematic procedure used by attackers in the execution of account traffic hijacking escapes most users, where the redirection to alternative websites goes unnoticed. However, to the keen user, redirection to an illegitimate destination is easily noted. The Information Systems Control and Audit Associations (ISACA) [10] advances the argument in noting the adverse effects associated with account hijacking attacks in cloud computing. The sensitivity associated with cloud computing and vulnerability to insecurity issues creates the need for much care and caution. An attacker with access to a cloud network can lurk within the particular network for a prolonged period of time, all. One they acquire the necessary information for attack execution; they have the advantage of carrying-out a network-wide attack with little possibility of their efforts being hampered [10]. Ensuring high-level encryption services and educating account holders of the importance of ensuring privacy of their account information rank among the most effective ways of preventing attacks.

Denial of service attack is another form of security concern issue in the area of cloud computing. In this particular case, the intrusion of attackers into a network result in the exhaustion of the network with numerous server requests. The result of the requests is the denial of access to vital information and applications over the network. [11] notes that Denial of Service

Attacks necessarily aim at denying the users of a particular network, access to the resources available at the specific cloud-computing environment. Attackers send continues requests at an identified server. The specified server is essentially used for the storage of data and other vital resources available for the users of the network. Where the server is burdened with requests set for mandatory feedback; it shuts down and remains unavailable for the intended users. Whereas the cost associated with Denial of Service Attacks has in the past incurred costs on individuals as well as network services providers, the effects of the same are far worse with respect to cloud computing. Where an organization makes use of shared resources in a cloud environment, it risks the ability to continue with work in the case of such as attack necessary resources such as application required to attend to the needs of clients remains unavailable. In such a case, a company is likely to record high losses that might kick the same out of business. As [11] continues to note, increased bandwidth usage and strain on storage space are some of the resources exploited in the case of a denial of Service Attack.

Malicious employees can also initiate attacks in a cloud-computing environment. Where retrenched workers retain access to an organization's cloud computing environment, they can execute changes that have the potential to affect the entire company's operations. [12] note that malicious attackers can broadly be categorized into two groups – insiders and outsiders. Employees to an organization with malicious intentions in the infringement of company data are categorized under internal attackers. Whereas attacks generally result in the compromise or loss of data, internal attacks have far-reaching devastating effects associated with the compromise of data. The same is arguably, so considering that employee to the organization have access to important company information and can alter the same without the possibility of correction or recovery. The position of an employee in an organization further influences their potential in affecting highly confidential information [13]. Where an administrator of a cloud-computing interface corrupts information associated with a company, the particular efforts have considerably irreversible damages. Hence, the association of the company with credible and highly dependable individuals goes a long way in ensuring that the company remains protected against damage or loss of information due to malicious employees.

Shared technology vulnerabilities is further classified under noteworthy cloud computing attacks. The same is concerned with the exposure of data and resources in cloud computing to danger as a result of shared privileges. Cloud computing revolves around sharing resources between different organizations. Hence, a particular type of resources can be under the utilization of different companies at different times of a particular timeline. Where the use of an application provides a loophole for an attack, the attacker gains access to all resources within the network. Hence, encryption of services and available resources in a cloud environment plays an important role in the prevention of attacks. The ability of a cloud computing to isolated different parts of the environment in the case of an attack remains one of the most effective strategies in the course of cloud computing. The isolated area is not able to host an attacker targeting the entire system. Consequently, repair to the system is also manageable and easy executed. Further, the dedicated use of cloud computing resources is a measure necessary for ensuring that attacks are kept at bay. Individual companies and organizations retain exclusive right to access of cloud computing resources in a dedicated environment. Though the cost of maintaining and running such facilities are fairly higher, the advantages associated with the same remain evident to the concerned users.

III. Cloud computing impact on businesses

A. Security issues in Cloud Computing and Impact in Business

The different types of attacks in cloud computing have varying levels of impact on the operations of a business and the potential to interrupt the same. Hence, different levels of attention and consideration is afforded the attacks existing in an identified context. Essentially, the main concern with respect to the use of cloud computing in business is the loss of compromise of data. Whereas each of the different attacks leads to the loss or compromise of client information, the prevention of each remains a contextualized approach. Denial of service attacks is arguably among the leading security threats in corporate engagements. Such attacks cast a strain on the dedicated cloud computing resources of an organization and thus leading to additional costs. Ideally, cloud computing operates through dedication of storage space and computing bandwidth to connected users. Where such resources are under attack in the course of denial of service, the effectiveness of the network to the particular users remains hampered. [11] notes that Denial of Service Attacks lead to additional costs in the maintenance of the cloud-computing network associated with a particular organization. The figure below gives an illustration of the execution procedure of a Denial of Service Attack.

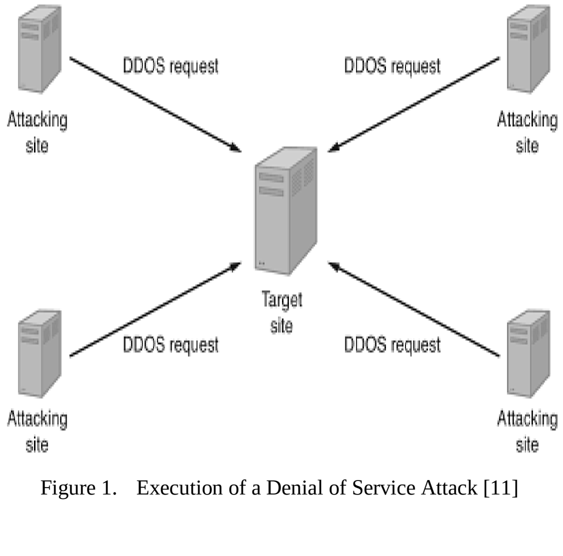

Figure 1. Execution of a Denial of Service Attack [11]

Further, malicious employees and their breach of confidentiality leads to negative impact on the associated firm. Competitors in the market against a firm that makes use of cloud computing gain advantage over an entity in the case employee's breach of confidentiality agreement. The sale of vital information and contacts under the ownership of the company can be some of the reasons behind employee’s breach of confidentiality [13]. The loss of company data and confidential information through leakage from employee’s accounts for the loss of data in a way beyond the other security threats on cloud computing platforms. One of the challenges associated with malicious employees as a security threat executed against a company has to do with the depth of breach on security of a company. It might require a lengthy period of time for the associate company to effectively determine the extent to which data is breached and exposed. Hence, the corporation of employees and their continued support in the course of using cloud computing remains of central importance in securely engaging in business within such and related environments. Frequent updating of access information and credentials after the retrenchment of workers is one of the security measures likely to safeguard against loss of data. The appointment of trustworthy personnel as managers of sensitive credentials is an additional measure in the prevention of attacks.

In addition, authentication procedures and software are essential in providing protection against account traffic hijacking. Where an account traffic hijacking attack is initiated successfully, clients to an intended site and products are lost to the imposter’s interfaces and sites. The development of cloud computing established the importance associated with administration interfaces as gateways to accessing cloud networks. In the presence of potential attacks on cloud environments, the institution of secure environments for access of the particular networks is highly essential [9]. The employment of secure socket layers as encryption measures for the security of administration interfaces is an effective measure. Encrypted information is only availed to individual with access to a network and the associated resources. Further site authentication services give assurance to the user that they are connected to the legitimate and intended site, and not a clone of the original. Such authentication services are provided by third party firms at additional costs. However, the benefits associated with retaining the trust and confidence of customers creates the need for additional investment in security measures.

B. Types of Cloud Computing

The different types of cloud computing include Private, Public, Community or Hybrid cloud options [14][15]. The different cloud environments and options have different advantages and attend to varying organizational needs. Hence, the choice of a given cloud computing type is dependent on the needs of the organization coupled with the efficiency of the adapted technology for the delivery of the necessary results. Private cloud environments allow access to selected individuals as well as corporate entities. Thus, the strain and exposure of such utilities and resources to the needs of the public remains checked [16]. The firms and individuals with access to private clouds incur higher costs with regards to maintenance of the same in business interactions. Some of the corporate needs associated with the adoption of private clouds in computing include the need for a high up-time guarantee on the available resources. The assured availability of resources in a cloud environment contributes significantly to the productivity and efficiency of employees in the organization.

Public clouds in computing are the other type of cloud computing technology. In the case of public cloud environments, sharing of information and the available resources is rather open and accessible to the public, in comparison to the limited nature in the private network. The cloud computing services in a public network are provided by a third party with interest in the communal sharing of information and resources within the network [17]. Though the public environment and openness involved in information and resources sharing does not favor the transmission and storage of confidential information, it favors alternative business and personal interactions. Resources such as email applications and sharing of non-sensitive data can be carried out at the public cloud-computing environment without fears of security breaches and leakage of the stored information.

Community cloud environments allow a group of organizations to share the cloud resources such as security requirements and policies. This type of cloud is implemented in the government sector (G-Cloud).

Additionally, hybrid cloud computing environments is the additional type insofar as cloud-computing technology is concerned. Hybrid clouds merge the properties of the private and public cloud technologies, to deliver appropriate services and resources to the concerned users [18]. Large companies and organizations with the need to tap from the benefits of both private and public networks make use of the hybrid approach in cloud computing. Whereas the associated cost is reduced compared to other options such as the private cloud, the security considerations associated with adoption of the same in organizational dealings remains evidently beneficial.

The challenge associated with making choice of an appropriate cloud computing technology has to do with projecting the short-term as well as long-term goals of the organization. Managers and policy makers have the role of identifying the necessary resources for the accomplishment of projected needs and company’s objectives. However, with a clear strategic framework for the organization in question, and the required resources for the execution of the intended tasks, organizational leaders are able to make informed and consequently effective choices with respect to types of cloud computing.

C. Service delivery types in cloud computing

Service providers in cloud computing make use of different service models for the delivery of the cloud services to the intended subscribers. Cloud-computing service delivery types include platform as a Service [PaaS], Infrastructure as a Service [IaaS], Software as a Service [SaaS], and Unified Communications as a Service [UCaaS] [14]. The different service delivery types involve the dissemination of appropriate application and resources necessary in meeting the needs and demands of the consumer. The adoption of a given service delivery type over another is wholly dependent on the needs of consumers and the objectives of the concerned firms.

The Software as a Service delivery [SaaS] type involves the sale or provision of cloud software resources at levy or free of charge. The availability of software at the cloud environment either at a fee or free is dependent on the needs of the service provider. Where the provider has a fair control of consumer share in the market, they are able to offer the concerned services for free while at the same time banking on other avenues of income generation [19]. Such avenues include sale of advertisement space and dedicated cloud resources. Arguably, dealings in software as a service rest at the top of the chain, where additional building blocks feature at the bottom of the framework. The choice of an organization on whether to invest in the purchase of Software services from a cloud computing service provider is largely dependent on the needs of the organization and the nature of business concerned with the firm. Where the concerned organization requires fast and optimized performance in the case of cloud-computing software, the use of internal resources would remain more advantageous compared to hired cloud computing resources.

Further, Platform as a Service is the additional technology associated with cloud computing. In the particular environment, service providers offer users the ability to develop applications and software for use at the Software as a Service environment. Service providers thus give developers the opportunity to save on costs associated with the purchase of necessary hardware and application platforms for the development of the appropriate technologies. Services at the Platform as a Service level are additionally either provided for free of levied as per agreement with the concerned developer. Investment in development platforms would prove rather expensive and thus unaffordable for most clients and developers of such and related systems [20]. However, the availability of the same in cloud format, as hosted in networks owned by service providers, creates the opportunity to collaborate as well as share ideas on platform development over the same network. Alternatively, users have the choice of investing on the necessary software and hardware for the creation of desirable platforms which are necessary in hosting appropriate software applications at the cloud or local network environment.

Infrastructure as a Service is an additional component in cloud computing. The same involves the sale of virtual storage space and hardware for the storage of company-specific information. In such a case, the client firms do not need to purchase hardware for use in the storage of data and other necessary information. On the contrary, such firms hire space on virtual servers and storage hardware as provided by service providers [19][20]. The advantages as well as disadvantages associated with the use of virtual storage space creates the opportunity for evaluation, where the concerned firm is able to determine whether or not it requires to hire virtual storage space. Hardware used in the course of virtual storage is owned and managed by service providers, who offer portions of the available bandwidth and space to the target consumers. The purchase of storage space is largely dependent on the needs of the organization placing the request and the long-term application of the organization’s objectives. Infrastructure as a Service ranks among the most popular service delivery packages in the course of cloud computing. Numerous firm make the choice of hiring virtual storage space from third-party entities, who ensure the provision of such services round the clock. Virtual storage of information is closely related with data security and responsibility over the backup of data stored in a cloud environment.

IV. SUMMARY

In consideration of the speed at which the cloud-computing world has recorded innovation and development of advanced technologies, the need for advanced security systems is ever pressing. Cloud technology is a relatively new concept but the security issues surrounding its operations have roots in the historical timeline of computing. Hence, several considerations for the future of cloud technologies will move a long way in ensuring that the same is able to serve the needs of the concerned members of public. Among the leading measures is the development of advanced security systems in cloud and related environments. Such security measures should integrate approaches that completely wade off earlier challenges associated the integrity of cloud computing systems and technologies. Security concerns such as Denial of Service and Account traffic hijacking necessarily needs elimination. Such systems with the ability of detecting and eliminating current security threats are only capable through extensive research and advanced work in technology.

Further, the entrance of new competitors into the cloud computing technology market will ensure that monopolies are not established. Whereas the delivery of cloud services is dependent of agreement with the concerned users, the rise and establishment of a monopoly in the concerned line of business is likely to hamper the quality of products and services offered in the particular environment. In the current market involving cloud technologies, the early adopters of the same technology are arguably the global leaders in the same. Hence, the need for legislation that allows other firms an opportunity to practice in the particular market environments. Where competition is discouraged, the cost associated with such facilities and services will unnecessarily remain high, leaving the concerned client with the need to incur high cost for the acquisition of desirable services.

Lastly, less focus on development of high-performance hardware and more time and resources spent on development of virtual environment is set to yield better results in the current state of cloud technology development; firms have the advantage of avoiding pressure for investment in the latest hardware infrastructure. The necessary equipment for the execution of tasks is available in virtual environments, where users with low-performance hardware are able to tap into the capabilities of hardware provided by their service providers. The pooling of resources and shared applications while at the same time earning from the sale of server space enables service providers to provide high-performance equipment at affordable levies.

V. Conclusion

Evidently, cloud computing is among the latest significant developments in the world of computing. Whereas the movement of different organizations towards the adoption of cloud computing remains slow, the same is a reality which every business entity will have entitlement to address. Thus, sooner or later, every firm with the intention of having relevance in business engagements into the future will have the mandate of ensuring integration of cloud computing services in their operations. The choice and employment of each of the service delivery types will be dependent on the needs of the concerned firm and willingness to take risks with data security. The latter is an important aspect for consideration in cloud computing, where security breaches result in the corruption or loss of valuable data and resources. The current different types of security attacks in cloud computing offer a glimpse of the challenges associated with the world of cloud computing. Ironically, the numerous advantages associated with the adoption of cloud technologies are matched against the advanced forms of security threats that have emerged to compete against the same.

References

[1] Almudawi, N. A. (2016) 'Cloud Computing Privacy Concerns in Social Networks', International Journal of Computer (IJC), Vol 22, No 1, pp 29-36.

[2] Buyya, R. , Broberg, J. and Goscinski, A (2011) 'Cloud Computing Principles and Paradigms', A John Wiley & Sons Inc, Hoboken, New Jersey.

[3] Srinivasan, S (2014) Cloud computing basics. New York: Springer.

[4] Williams, M. I (2010) A quick start guide to cloud computing: Moving your business into the cloud. London: Kogan Page.

[5] Ivanov, I., Sinderen, M. J., Leymann, F., and Shan, T (2013) Cloud Computing and Services Science: Second International Conference, CLOSER 2012, Porto, Portugal, April 18-21, 2012, revised selected papers. Cham: Springer.

[6] Wang, L. Ranjan, R. Chen, J. and Benatallah, B (2012) 'Cloud Computing: Methodology, Systems, and Applications', CRC Press, Taylor and Francis Group.

[7] Paul, M (2012) 'The 7 qualities of highly secure software', Boca Raton, FL: CRC Press, Taylor and Francis Group.

[8] Usman. M., Jan. A and He. A (2016) 'Cryptography-based Secure Data Storage and Sharing Using HEVC and Public Clouds', Elsevier Information sciences, accepted, 2016.

[9] Halpert, B (2011) 'Auditing cloud computing: A security and privacy guide', Hoboken, N.J: John Wiley & Sons.

[10] ISACA (Information Systems Audit and Control Association) (2011) 'IT control objectives for cloud computing: Controls and assurance in the cloud', Rolling Meadows, USA.

[11] Jamsa, K (2013) 'Cloud computing: SaaS, PaaS, IaaS, virtualization, business models, mobile, security and more. Burlington', MA: Jones & Bartlett Learning.

[12] Das, S. K., Kant, K., and Zhang, N (2012) 'Handbook on securing cyber-physical critical infrastructure', Waltham, MA: Morgan Kaufmann.

[13] Park, J. J., Chao, H., Obaidat M. S, and Kim. J (2011) 'Computer science and convergence: CSA 2011 & WCC 2011', Proceedings. Dordrecht, New York: Springer.

[14] Jayalekshmi MB, Krishnaveni SH (2015) 'A Study of Data Storage Security Issues in Cloud Computing', Indian Journal of Science and Technology. 2015 Sep; 8(24)

[15] Sumit Goyal (2014) 'Public vs Private vs Hybrid vs Community - Cloud Computing: A Critical Review', I.J. Computer Network and Information Security, 2014, 3, 20-29

[16] Nick. A and Lee. G (2010) 'Cloud Computing Principles, Systems and Applications', London: Springer, 2010

[17] Buyya. R, Vecchiola. C, and Selvi. S. T (2013) 'Mastering Cloud Computing: Foundations and Applications Programming', Morgan Kaufmann. .

[18] Dhamdhere, S. N (2013) 'Cloud computing and virtualization technologies in libraries'. Hershey, PA: IGI Global.

[19] Grandinetti, L., Pisacane, O., and Sheikhalishahi, M (2014) 'Pervasive cloud computing technologies: Future outlooks and interdisciplinary perspectives', Hershey PA: IGI Global.

[20] Moumtzoglou, A., and Kastania, A (2014) 'Cloud computing applications for quality health care delivery', Hershey, PA: IGI Global, 2014.