The University of Western Australia

CITS5503 - Cloud Computing

Cloud Computing: a Review

Michael Stewart

October 25, 2015

Contents

1 Introduction

Cloud computing has become a popular topic recently thanks to the rising demand for computing resources. Cloud computing has been defined as

> "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [3]

It provides a wide range of benefits, including removing the cost that results from assembling servers in-house, as well as the ability to provision computing resources on demand. On the other hand, there are several risks associated with cloud computing, which mostly relate to security and privacy. This paper explores the service models and hosting options available, and outlines the benefits and risks associated with cloud computing. We aim to determine whether it is beneficial for a company to move applications and data to the cloud, or to continue to use their own infrastructure.

1.1 Background

Cloud computing emerged as a result of the growing need for large-scale applications. The "cloud" may be thought of as a series of shared computing resources, which are typically made available to customers on a pay-as-you-go basis. The technology has been made possible by a range of computing innovations, including virtualisation, load balancing, web service architecture, and the advent of Web 2.0 [24].

The foundation of cloud computing is the data centre, which contains a large number of servers running the cloud [22]. Cloud computing providers may have many data centres located across the world in order to provide faster and more effective service to their customers. The servers within each data centre run virtualisation software, allowing each server to act as more than one computing node. They are also networked, enabling the sharing of resources. Customers may connect to these servers remotely via technologies such as Secure Shell (ssh) and utilise the cloud's resources for their own purposes.

1.2 Service models

Cloud computing features three primary service models, each offering a different level of control and set of capabilities to the end user. These service models are depicted in Figure 1.

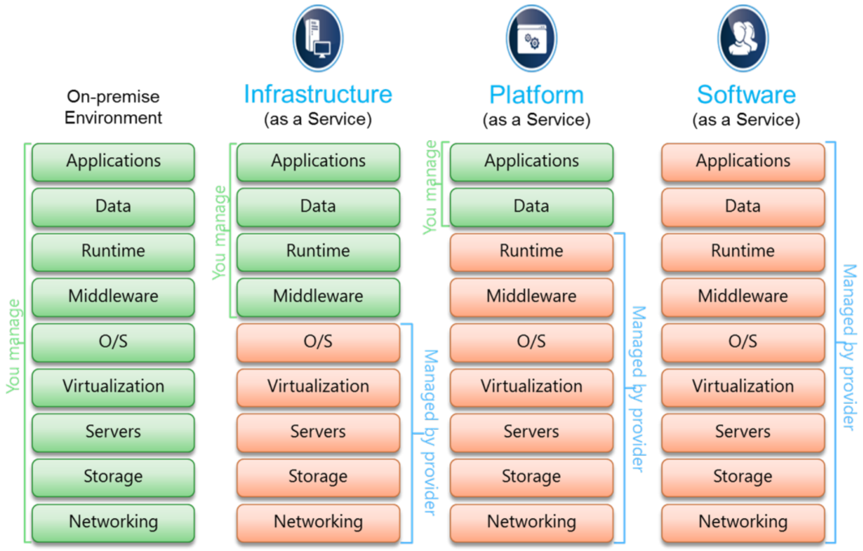

Figure 1: The three service models of cloud computing[1].

[1] *Simple Talk.* https://www.simple-talk.com/cloud/development/a-comprehensive-introduction-to-cloud-computing/

1.2.1 Infrastructure as a Service

Infrastructure as a Service (IaaS) offers the most developmental control to its end users, as providers of IaaS typically only provision the networking, hardware, virtualisation and operating system. This means that users of IaaS may deploy and run arbitrary software and have full control over their applications [17]. It is therefore the most appropriate choice for a company that is looking to host its data and/or infrastructure externally. There are several highly-popular IaaS providers available, the most popular of which being Amazon Web Services[2].

1.2.2 Platform as a Service

Platform as a Service (PaaS) provides its users with the ability to run their own software on a pre-built application-hosting environment [17]. It is often used for the hosting of web and enterprise applications [6]. The key benefits of the PaaS model are reduced costs and deployment time as a result of its users not being required to set up their applications' runtime environment. This also results in reduced maintenance time and system complexity. Popular PaaS providers include Google App Engine, as well as the aforementioned Amazon Web Services, which provides a mixture of both IaaS and PaaS [9].

1.2.3 Software as a Service

The final cloud service model, *Software as a Service* (SaaS), allows customers to use applications the provider is running on a cloud infrastructure [17]. These applications are typically interacted with using a web browser or program interface. This model does not offer any infrastructure control to the end user, but instead is utilised for purposes such as email clients and payroll processing software. SaaS offers even greater benefits than PaaS with regards to time and cost saving, and has a more mature business model [6]. It also allows for small companies to access software that was previously only available to large corporations. Examples of

[2] Clouds360. *http://www.clouds360.com/iaas.php*

popular SaaS products include Google Apps and Salesforce.

1.3 Deployment options

There are several deployment options available to cloud computing customers. Each option requires a differing level of commitment and skills in order to remain a viable hosting solution [17]. These deployment options are discussed in the following section.

1.3.1 Public cloud

Public clouds involve the provisioning of cloud infrastructure for use by the general public. The infrastructure and computational resources are owned by the cloud provider, and are situated in their data centres [12]. Computing resources may be shared by multiple clients, leading to potential security risks that may only be resolved by the cloud provider [3]. Despite being the most ubiquitous deployment option, utilising the public cloud still requires the consumer to possess IT skills in order to access the cloud remotely. Public cloud is typically used for purposes such as web applications and other publicly-accessible software.

1.3.2 Private cloud

Private clouds, as opposed to public clouds, offer a computing environment for one single organisation [12]. Private clouds may be operated internally or externally by a cloud provider. Allowing a provider to manage an organisation's private cloud allows the organisation to utilise the provider's extensive resources when required [3]. It is typically more expensive to run a private cloud on-site due to the large costs associated with setting up or converting a data centre and hiring skilled IT professionals to maintain it.

1.3.3 Hybrid cloud

Hybrid clouds involve the combination of two or more cloud infrastructures. For example, they may consist of a public and private cloud. Each cloud may communicate with other clouds owned by the consumer, allowing for application and data portability [17]. One common usage of a hybrid cloud is to store sensitive data on a private cloud and connect that data to an application hosted on a public cloud[3]. Hybrid clouds also see usage for the purpose of "cloud bursting", which involves hosting an application on a private cloud and referring users to the same application hosted on a public cloud in the event of increasing capacity demands. This allows an organisation to only utilise the elasticity of public cloud resources when required, allowing them to save money on computing resources [19].

1.3.4 Community cloud

Community clouds are used by groups that share similar interests, such as security requirements and policies [11, 15]. In a similar manner to private clouds, the cloud may be managed by one group member, or managed externally by a cloud provider. Developing a community cloud allows organisations to save money by sharing the costs between other similar organisations [4]. Also, community clouds are useful for testing products before they are placed on to the public cloud environment[4].

[3] *TechRadar.* http://www.techradar.com/news/internet/cloud-services/hybrid-cloud-is-it-right-for-your-business–1261343

[4] *Data Centre Knowledge.* http://www.datacenterknowledge.com/archives/2014/10/13/explaining-community-cloud/

2 Benefits

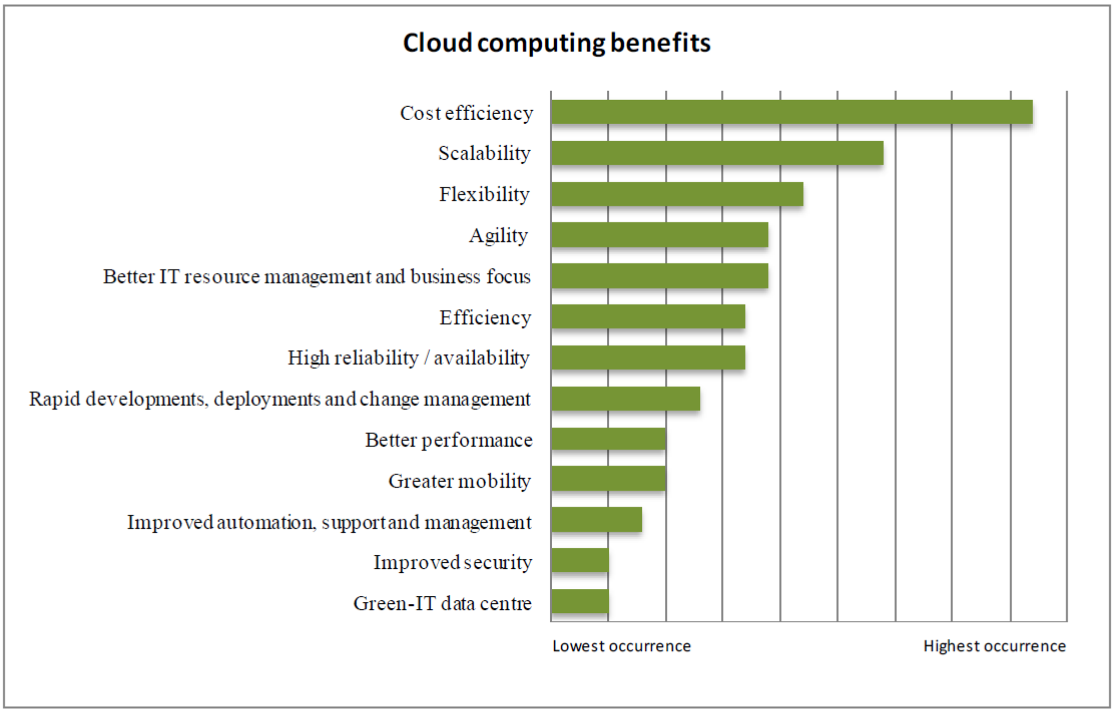

Figure 2: The benefits of cloud computing, in order of most citations within literature [5].

There are numerous benefits associated with moving to a cloud-based solution. Some of the most widely-accepted benefits are shown in Figure 2 and discussed in the following section.

2.1 Cost efficiency

Cost efficiency is the most obvious benefit of cloud computing. Each cloud service model provides a number of ways to reduce costs to its consumers. PaaS, for example, allows its consumers to save time and money on developing and deploying applications [3]. SaaS, on the other hand, allows for dramatically-reduced license management overheads by enabling consumers to employ a single license on multiple computers when required, rather than over-provisioning the license.

According to Microsoft, 89% of a company's IT budget is spent on maintenance and infrastructure [16]. Consumers hosting their data externally on the cloud do not need to set up or convert a data centre for their own needs, meaning they can utilise their IT budget for other important purposes. Using cloud computing also eliminates the cost of power, cooling and floor space [5]. This benefit is perhaps most useful to start-up companies, who no longer need to spent substantial amounts to build their own data centres thanks to the advent of cloud computing [2]. Migrating to an externally-hosted cloud typically incurs a low up-front cost, dependent on the level of employee training and cloud-based software required.

2.2 Scalability

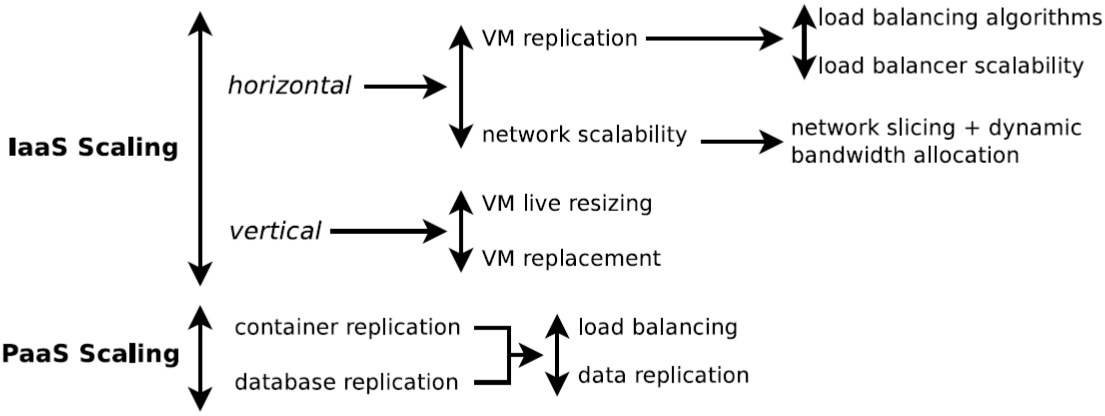

Figure 3: The ways in which cloud computing infrastructure scales [23].

Cloud computing provides its users with on-demand self-service, meaning they may automatically provision computing capabilities when required [15]. No interaction with the service provider is required, allowing for rapid resource expansion when necessary. Conversely, a company may scale down their computing resources when they are no longer required, in order to save costs. As shown in Figure 3, cloud computing scales both horizontally and vertically, as a result of technologies such as virtualisation and load balancing.

Scalability also exists at the software level. For example, PaaS application development frameworks are designed to scale and operate during high fluctuations of user demand [3]. These systems are able to handle very high request rates and are built this way in order to handle the traffic of the applications they are hosting [23]. This is often made possible by using a combination of three software-level mechanisms: distributed caching, NoSQL databases, and database clustering.

2.3 Performance

Cloud computing enables its users to access high-peforming computing resources that would otherwise be unavailable without spending large amounts of time and money on setting up servers. Amazon Web Services, for example, offers computing instances known as "C4", which feature up to 36 vCPUs and 60GB of RAM[5]. These instances may be used for high performance computing tasks, which were previously only possible with an on-site supercomputer. Cloud computing also facilitates greater performance in regular computing tasks. For example, load balancing enables applications to maintain their performance even when experiencing heavy traffic [23].

2.4 Reliability

Cloud providers are generally able to provide uninterrupted services to their users, and rarely have outages nowadays [11]. According to Leavitt [13], "a system run by a large service provider that has many resources and redundant equipment should offer more availability than an infrastructure run in-house by a small or even midsize company". Outages are usually repaired very quickly – Amazon EC2, for example, had a total downtime of just 2.41 hours across the entire year of

[5] *Amazon Web Services.* http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/c4-instances.html

2014[6]. Because any outages are fixed by cloud providers, public cloud or external private cloud users do not have to worry about investing time and effort into fixing outages themselves.

3 Risks

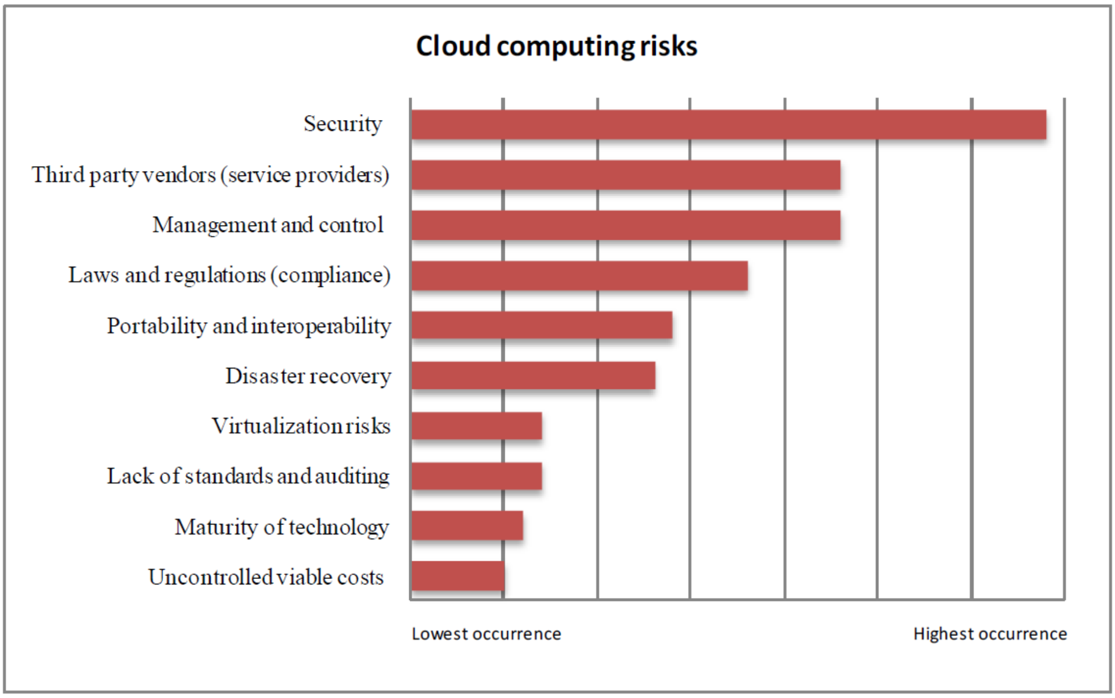

Figure 4: The risks of cloud computing, in order of most citations within literature [5].

Despite its many benefits, there are a number of reasons as to why a company may decide to avoid cloud computing and opt for an in-house computing infrastructure solution. The majority of these reasons relate to privacy and security concerns, as well as the issues surrounding data sovereignty when storing data at an external cloud provider's off-shore data centres. There are a number of other

[6] *Enterprise Tech.* http://www.enterprisetech.com/2015/01/06/aws-rates-highest-cloud-reliability/

risks associated with cloud computing, such data corruption and infrastructure failure [20]. The most widely-accepted risks associated with cloud computing are shown in Figure 4. The following section outlines some of these risks in greater detail and provides several means for mitigating these risks.

3.1 Security

Security concerns are the most notable risk associated with cloud computing [5]. Many security issues relating to cloud computing are due to the complexity of cloud infrastructure. The increased system complexity of a cloud platform requires a higher level of skill and effort to maintain in order to keep the platform secure [12]. The need for diligent maintenance is due to the vulnerability that results from the high number of interactions between components in the system. If not properly maintained, the system could face substantial security problems such as unauthorised access and destruction of data. Security risks may be reduced by maximising security prior to outsourcing data to a cloud provider [14].

3.2 Privacy

Transitioning to a cloud computing platform introduces privacy concerns, as the cloud consumer's data is handed to a third-party vendor. It can be difficult for a company using the cloud to ascertain the data privacy of its users due its distributed nature [3]. Another privacy concern associated with cloud computing is data leakage, whereby security flaws allow sensitive data to be obtained by unauthorised users [5]. The shared multi-tenant environment of external cloud computing also introduces potential threats, as vulnerabilities in the virtualisation of hardware may be exploited by attackers to gain access to sensitive data [12].

The issues relating to the privacy of cloud computing may be mitigated in a number of ways. Firstly, companies may select a cloud provider that promises not to retain data in the event that they leave the market [1]. Secondly, cloud consumers may require their cloud providers limit access to their data to essential personnel only, and conduct background checks of those personnel [18]. This helps to prevent the leakage of sensitive data. Finally, Carroll et al. [5] recommend cloud consumers conduct regular third-party audits to monitor their cloud service provider's compliance to the terms originally agreed upon. This ensures that the cloud consumer's data is managed appropriately.

3.3 Lack of control

The lack of data control companies face when using the services of an external cloud provider is another issue associated with cloud computing. When using a public or externally-hosted private cloud, companies must relinquish control of their computations and data to a third party [10]. There is often no point of contact when dealing with cloud providers, and cloud users must trust providers to cooperate and maintain their responsibilities such as continuous monitoring and maintenance [12].

The lack of any party's full control over cloud infrastructure introduces ethical issues. For example, it is often difficult to place the blame on any party in the event of problems such as data loss [21]. A company may also face issues when terminating their service with a cloud provider. The process of transferring data from one cloud provider to another can be very long and difficult [8], and companies that depend on one particular cloud provider may be too reliant on that provider to switch to another (a concept known as vendor lock-in). These risks may be mitigated by selecting a reliable and popular cloud provider such as Amazon Web Services[7], which may remove the need to change providers.

3.4 Data sovereignty

The global distribution of cloud data centres introduces concerns related to data sovereignty. Simply put, data sovereignty is the concept that data is subject to the

[7] *Amazon Web Services.* aws.amazon.com.

laws of the territory in which it is located[8]. There are many regulations in place that concern data, such as the Health Information Protection and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA) of 2002, and the USA PATRIOT Act [3]. The latter allows the United States government to sieze any piece of information stored in a US data centre, without the data owner's knowledge [7]. Cloud consumers should therefore be aware of the laws of the territory where their data is stored, and consider storing private data locally in order to avoid such complications.

4 Evaluation

There are several ways an organisation may move its computing infrastructure to the cloud. As highlighted in Section 1.2, there are three primary service models of cloud computing, each with its own purpose. Companies that wish to host their own applications may use IaaS and enjoy the benefits of vast scalability and low up-front costs. They may also use PaaS to save time on deployment and reduce the need for skilled IT workers to handle low-level programming. SaaS may be used for company applications, allowing businesses to save money on licenses and use popular, reliable software. The purpose of each cloud service model is well-defined, so the most difficult decision for companies considering moving to the cloud is whether to deploy applications and host data on a public, private, hybrid or community cloud, or to keep their own infrastructure.

While the ideal IT infrastructure for a company is highly dependent on that company's needs, we believe it is important to ensure that private data remains on internal servers, and does not reside on an externally-hosted cloud. This avoids the issues surrounding the multi-tenant environment, which, as discussed in Section 3.2, can allow hackers to obtain data by exploiting software vulnerabilities. It also ensures that data does not leave the company's servers and is therefore not subject to foreign laws and regulations. We recommend consumers store sensitive data in an internally-hosted private cloud or community cloud in order to avoid

[8] *What is?*. http://whatis.techtarget.com/definition/data-sovereignty

these types of problems. This results in increased set-up costs, but helps to avoid the aforementioned privacy and security risks.

We believe that it is highly advantageous to move publically-available applications to an externally-hosted public cloud. As mentioned previously, the scalability of the cloud is incredibly beneficial, as it allows consumers to be confident that their applications will remain highly available. When experiencing user growth or unexpectedly high amounts of traffic, consumers may simply provision more computing resources to handle demand. Also, hosting applications on a public cloud removes the cloud consumer's need for skilled IT workers to conduct low-level maintenance. Maintenance can be left to the cloud providers, who typically have very reliable service level agreements.

5 Conclusion

In conclusion, this paper has explored the concepts behind cloud computing. It has also described the three service models of cloud computing, as well as the various cloud deployment options available. We have discussed the benefits and risks associated with the technology, and have come to the conclusion that companies should avoid hosting sensitive data on externally-hosted clouds. However, we believe the benefits of cloud computing vastly outweigh the drawbacks in the realm of application deployment, and recommend companies host their applications on the public cloud. Ultimately, cloud computing has greatly changed the IT options available to companies and should be strongly considered as a viable IT infrastructure solution.

References

[1] Ethics opinion on cloud computing. *Florida Bar News*, 40(4):25–27, 2013.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. *Communications of the ACM*, 53(4):50–58, 2010.

[3] Lee Badger, Tim Grance, Robert Patt-Corner, and Jeff Voas. *Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology.* CreateSpace Independent Publishing Platform, 2012.

[4] Fabrizio Baiardi and Daniele Sgandurra. Securing a community cloud. In *Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International Conference on*, pages 32–41. IEEE, 2010.

[5] Mariana Carroll, Alta Van Der Merwe, and Paula Kotze. Secure cloud computing: Benefits, risks and controls. In *Information Security South Africa (ISSA), 2011*, pages 1–9. IEEE, 2011.

[6] William Y Chang, Hosame Abu-Amara, and Jessica Feng Sanford. *Transforming enterprise cloud services.* Springer Science & Business Media, 2010.

[7] Primavera De Filippi and Smari McCarthy. Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, 3(2), 2012.

[8] Robert L Devereaux and Michael C Gottlieb. Record keeping in the cloud: Ethical considerations. *Professional Psychology: Research and Practice*, 43(6):627, 2012.

[9] Eugene Gorelik. *Cloud computing models.* PhD thesis, Massachusetts Institute of Technology, 2013.

[10] Andreas Haeberlen. A case for the accountable cloud. *ACM SIGOPS Operating Systems Review*, 44(2):52–57, 2010.

[11] Yaju Jadeja and Kavan Modi. Cloud computing-concepts, architecture and challenges. In *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, pages 877–880. IEEE, 2012.

[12] Wayne Jansen, Timothy Grance, et al. Guidelines on security and privacy in public cloud computing. *NIST special publication*, 800:144, 2011.

[13] Neal Leavitt. Is cloud computing really ready for prime time? *Computer*, (1):15–20, 2009.

[14] Dan C Marinescu. *Cloud computing: Theory and practice.* Newnes, 2013.

[15] Chris May. Seeing into the cloud: How to mitigate potential ethic and security issues. *The Federal Lawyer*, 60:69–76, 2013.

[16] Andrew McAfee. What every ceo needs to know about the cloud. *Harvard Business Review*, 89(11):124–132, 2011.

[17] Peter Mell and Tim Grance. The nist definition of cloud computing. 2011.

[18] Richard Mosher. Cloud computing risks. *ISSA Journal, July Issue*, pages 34–38, 2011.

[19] Srijith K Nair, Sakshi Porwal, Theo Dimitrakos, Ana Juan Ferrer, Johan Tordsson, Tabassum Sharif, Craig Sheridan, Muttukrishnan Rajarajan, and Afnan Ullah Khan. Towards secure cloud bursting, brokerage and aggregation. In *Web Services (ECOWS), 2010 IEEE 8th European Conference on*, pages 189–196. IEEE, 2010.

[20] Scott Paquette, Paul T Jaeger, and Susan C Wilson. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 27(3):245–253, 2010.

[21] Job Timmermans, Bernd Carsten Stahl, Veikko Ikonen, and Engin Bozdag. The ethics of cloud computing: A conceptual review. 2010.

[22] Wei-Tek Tsai, Xin Sun, and Janaka Balasooriya. Service-oriented cloud computing architecture. In *Information Technology: New Generations (ITNG), 2010 Seventh International Conference on*, pages 684–689. IEEE, 2010.

[23] Luis M Vaquero, Luis Rodero-Merino, and Rajkumar Buyya. Dynamically scaling applications in the cloud. *ACM SIGCOMM Computer Communication Review*, 41(1):45–52, 2011.

[24] Lizhe Wang, Gregor Von Laszewski, Andrew Younge, Xi He, Marcel Kunze, Jie Tao, and Cheng Fu. Cloud computing: a perspective study. *New Generation Computing*, 28(2):137–146, 2010.