Cloud Computing: Technology, Security Issues and Solutions

Naim Ahmad
College of Computer Science
King Khalid University
Abha, Kingdom of Saudi Arabia
naimahmad@gmail.com

***Abstract*—The concept of cloud computing can be traced back to almost the middle of last century. Cloud paradigm offers scalable, portable, platform-independent, ubiquitous, shared resilient, sustainable, and near-utility computing. The cloud computing is implemented as a software-only solution or based on advanced hardware supported virtualization technology. This paper presents the fundamental technology behind the cloud computing. Cloud computing posit as a utopia to solve multitudes of challenges of the current time. But in practice security is a major road block to its widespread adoption. This paper discusses the security issues of the cloud computing. Further the paper illustrates upon the security solutions for the virtualization and web services, two major enabling technologies of cloud computing. It also explains the novel concept of integrating the multi-level security in all of the cloud offerings in contrast to the security-as-a-service concept. Finally paper mentions the important guidelines for the development of service level agreements.**

Keywords—Cloud Service Providers, Producers and Consumers; Cloud Computing Technology Framework; Hypervisor; Virtual Machine Monitors VMM; Virtual Machines VM; Cloud Security Issues; Multi-level Integrated Security; Service Level Agreements SLA.

I. INTRODUCTION

The cloud computing paradigm has characteristics envisioned since almost the middle of last century. It offers scalable or elastic computing on virtually complete range of computing devices, supporting all existing and archaic software technologies and tools, and served through disparate network hence making it platform independent, portable and ubiquitous. Similarly capability to serve on-demand, share and instant commissioning and de-commissioning of configurable computing resources causes it to be resilient, sustainable and near-utility computing. It offers services in three major categories Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [1]. SaaS refers to application software services, PaaS refers to application infrastructure services and IaaS refers to system infrastructure services. It is deployed under four schemes Private, Community, Public or Hybrid Cloud [1].

The cloud computing as institutionalized seems to bring the computing to common man's life such as every individual having a virtual desktop on the cloud. And as the resource hungry world is facing tough time to commit its resources on burgeoning needs of computing such as the concept of smart cities and its operations [2] and evolution of Big Data to mention some . And sustainability of information technology is being questioned all the more [3]. Cloud computing looks a silver bullet to meet range of challenges of the present world. Probably the only road block or hindrance to this panacea currently seems security threats or difficulty in achieving fully verified code.

The public cloud services market was at $175 billion in 2015 and is expected to grow at 16.5 percent in 2016 [4]. This shows the general acceptability towards the adoption of the public cloud. The benefits of cloud computing are multidimensional such as economic, operational, business and technological. Adoption motivations range from factors such as financial gains due to pay per use mechanism, no long time commitment to the service providers, performance and management ease of Information Communication Technology ICT resources, scalability due to datacenter integration, higher utilization of resources due to multi-tenant (sharing) environment and virtualization [5].

On the other hand several barriers to adoption of cloud are also present in the literature. The study [6] has presented the barriers after surveying 95 Spanish industrial Small and Medium Enterprises (SME). The first and foremost barrier happens to be the security with respect to the whole paradigm itself such as network attacks. The security concerns such as confidentiality, integrity and availability are of paramount importance to the cloud computing adopters. Data today holds the same position as material resources and is needed in all the digitized processed of the organizations without compromising the accuracy, privacy and ownership. Data is also required to fulfill the confidentiality and law requirements of individual nations. And in the multi-party and cross border ICT infrastructure data compliance assurance is a strong deterrent for the potential cloud adopters. Likewise the absence of strong business case having cost benefit analysis and difficulty in switching the service providers have been mentioned as barriers [6].

Therefore, where there are apparent benefits of public clouds, there also exists real concerns regarding the security, privacy and control of the data; availability, scalability, performance and cost-effectiveness of public cloud

978-1-5090-5814-3/17/$31.00 ©2017 IEEE

infrastructure; and due diligence of the public cloud service provider. This study aims at following objectives:

- The underlying technology of cloud computing and its institutionalization.
- The existing security threats in cloud computing.
- The security solutions adopted by the cloud computing community.

This paper is organized into five sections. First present section, Introduction, gives the basic concept of the cloud, its benefits and barriers to its adoption and the objectives of this study. Second section, Cloud Computing Technology, presents the important technological components that make cloud computing work and its implementation model. Third section, Cloud Computing security threats, delves into literature to identify the numerous security risks in the public cloud environment and present the security threat classification framework. Fourth section, Cloud Security Solution discusses important guidelines and frameworks to secure the virtualization and web services. This section also presents the novel concept of multi-level integrated cloud security concepts and important guidelines to design the document of service level agreements. Finally the fifth section concludes the study.

II. CLOUD COMPUTING TECHNOLOGY

The evolution of cloud computing can be traced back to the concept of virtualization and non-interference proposed in 1980s [7] or even to the later period of 1950s to the concept of virtual memory [8]. Virtualization in cloud computing context refers to hosting a unified and uniform view of disparate hardware resources to guest system and application software. The cloud computing rests on an important component called as Hypervisor that facilitates the hardware sharing through a masquerade known as virtualization. Generally speaking there are two types of hypervisors, also called as the virtual machine monitors (VMM). The type-1 or bare –mental hypervisor runs on top of hardware and manages different guest operating systems or virtual machines (VM). Whereas type-2 or hosted hypervisor runs on top of operating system and manages different VMs as processes. There are several hypervisor in the market such as Xen, VMware ESX and ESXi, Microsoft Hyper-V, Citix XenServer, Redhat KVM, Oracle VM Server etc.

The type-2 hypervisors run in the most privileged memory ring 0 whereas guest operating systems or VMs are deprivileged to run on higher memory rings such as 1 [8]. And VMM acts as host operating system for other guest operating systems and allocates the CPU resources, memory, hard-disk and bandwidth to each VM. Though achieving such software only virtualization requires the modification in the operating system code. This option more known as paravirtualization is only possible with open source operating systems. The other option is binary translation or patching and can be applied to other proprietary operating systems whose source code is not available.

Software only virtualization has several disadvantages such as memory ring aliasing and guest operating system failure due to incomplete context restoration to mention some [8]. Therefore hardware virtualization support such as root operation and non-root operation solves the problem of software only virtualization. In this scenario the VMM and guest operating system or VM both run in their intended memory rings. But the control is retained to the VMM by operating in the root-level in contrast to the VM which operate in non-root level. In this way there is no need of paravirtualization or binary translation (patching) and guest operating system can be used off-the-shelf.

The type-1 or bare metal hypervisors execute straight on the hardware unlike the type-2. They provide the virtualized hardware environment to other guest operating systems that run on top of them. They look more typical like an operating system and have the following components: core (boot and memory and scheduling manager), non-memory part (the bus manager, I/O interfaces, processor emulation, and on-the-fly code block translation) and management part (configuration, logging, and hot patch management) [7].

At the higher layer the concept of service oriented architecture (SOA) plays a vital role. Cloud computing services are presented in the form of web services and follow industry standards such as Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery and Integration (UDDI) [9]. And inside the cloud these services can be orchestrated and managed through SOA. Similarly on the client side to improve the functionality Rich Internet Application (RIA) are integrated on the client side in the web browsers or otherwise. And these RIAs make use of Asynchronous JavaScript XML (AJAX) [10]. With AJAX web applications can retrieve data from the server asynchronously without affecting the current screen of the user. Network is also an important entity that provides the link between cloud producer and consumer such as LAN/WAN, WLAN, Satellite, Mobile G3/G4 network etc. Fig. 1 depicts various important technological component of cloud computing.

Fig. 1 also presents several entities involved in the cloud computing paradigm such as Cloud Service Providers (CSP1), Cloud Service Producers (CSP2), Cloud Service Consumers (CSC) and Data Center Providers (DCP). It also presents some of the examples of services in different clusters of SaaS, PaaS and IaaS [11]. It also shows the different communication links between cloud producers and consumers. CSP1, CSP2 and DCP can be a single organization such as Google and DCP would be internal to the cloud. Or cloud may use the external DCPs with or without internal DCP. There are other players as well such as intermediaries, consultancies, industry standard organizations and governmental organizations among others as shown in the National Institute of Standards and Technology (NIST) conceptual reference model [12].

III. CLOUD COMPUTING SECURITY ISSUES

The cloud computing can be thought of as culmination of all sets of different information and communication technology (ICT) constituents working in tandem. In a simple case like purchasing 1 dollar soap from a web application hosted on

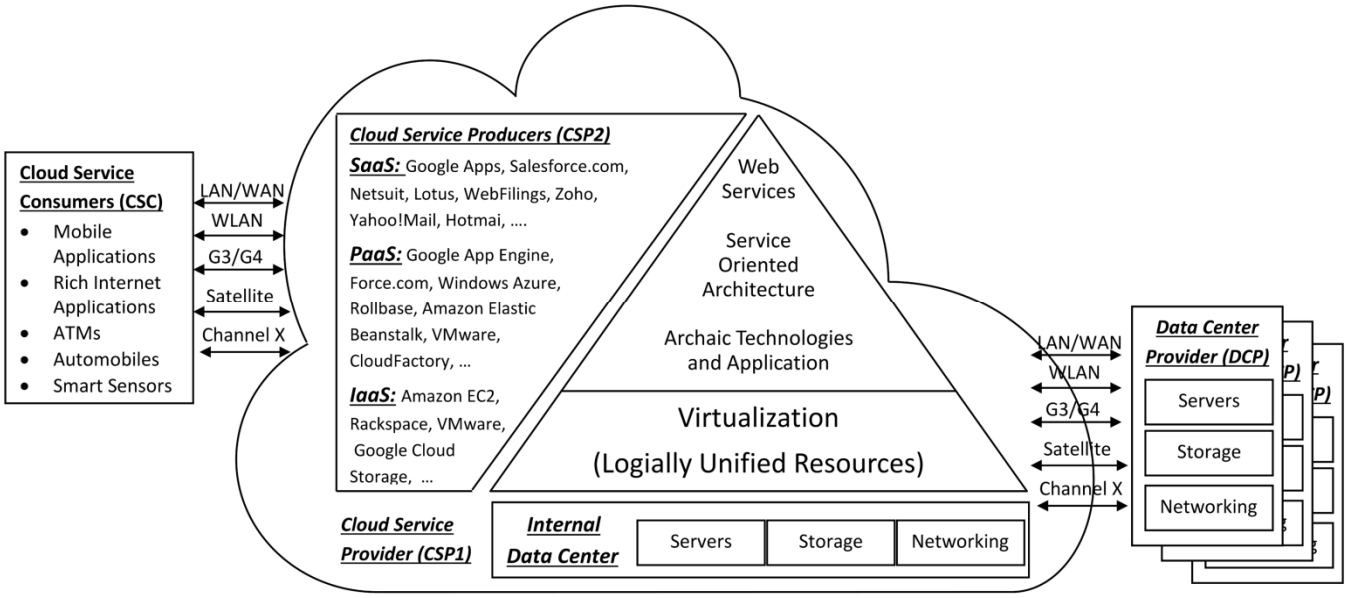

Fig. 1. Cloud Computing Technology Framework

cloud environment through a mobile device will make use of most expansive and global ICT infrastructure worth trillions of dollars. This simple transaction will go through hundreds of servers such as internet routing servers, database servers, mobile network servers, web servers, application servers, cloud servers etc. Similarly it will traverse through the virtual presence of multiple organizations such as product organization, cloud producer, cloud provider, financial organization etc. At the same time this simple transaction will be exposed to the multitude of threats present in this vast ICT infrastructure physically or virtually through malicious insiders and outsiders.

There are several studies in the literature that have identified security threats in the cloud computing paradigm. Some such studies [13]–[20] ranging from 2009 to 2016 have been selected to get the gist of the security concerns. The study of [13] have tried to categories these issues on the basis of cloud service models (SaaS, PaaS and IaaS). Similarly [14] has classified the security concerns on the basis of technology (communication and architecture) and business issues (conceptual and legal aspects). Whereas the study of [15] has presented threats in various general dimension of cloud computing. The study of [16] presents the security issues to be handled in service level agreements. And also emphasize upon the security threats to be addressed at various access points such as Server, Internet and Database. In addition to maintaining Data Privacy and Program access Security.

Looking at the importance of cloud computing various organizations such as NIST has put forth the guidelines for adopting cloud computing. It has categorized cloud security issues into 9 categories [17]. Similarly another important organization European Union Agency for Network and Information Security (ENISA) provides insights to SMEs on issues related to network and information security risks before they adopt cloud computing [18]. Last but not least, Cloud Security Alliance (CSA)'s Top Threat Working Group has recently published 12 most treacherous cloud threats based on survey from industry experts [19].

As the Web services and SOA are integral parts of cloud orchestration, the security in this domain is of paramount importance. The open web application security project (OWASP) has been issuing ten most critical web application security risks since 2003. In its present release of 2013 it has consolidated the top 10 list from over 500,000 vulnerabilities across hundreds of organizations and thousands of applications [20]. The review of these studies shows the cloud computing security issues range from physical ICT resources, internet, web applications, and data access and privacy, data centers on one hand to virtualization and cloud architecture, cloud deployment and service models, and service level agreements on the other hand. In essence first category is more pertinent to the traditional ICT infrastructure and second category is more concerned with the Cloud Computing domain.

Further to understand the vast range of security issues, it is important to have some logical and simple taxonomy. This paper presents this taxonomy based on simple content analysis and distinct themes of cloud computing. Table I gives the classification or taxonomy of security threat concerns into distinct domains and sub-domains. This classification serves as the guide in the security concern containment and resolution. There are five domains such as system virtualization, Application Programming, Data, Network and Communication, and Business and Legal Issues. Each of the five domains has further sub-domains such as Host and Guest Environment; Web Application and SOA; Hazards and Storage Issues; Internet, Intra Cloud, and Identity Management and Access Control; and Service Level Agreements, Governance, and Service Providers and Intermediaries respectively. Further it gives the items of security issue concern mapped into different domain and sub-domain. So the individual security threat can easily be tracked and resolved in the responsible entity.

TABLE I. TAXONOMY OR CLASSIFICATIO OF SECURITY THREATS IN THE CLOUD COMPUTING ENVIORNMENT [13]–[20]

Domain	Sub-Domain	Security Issue Concern
System Virtualization	Host Environment	Hypervisor Complexity; Attack Vectors; Virtualization Manager
	Guest Environment	VM image sharing, VM isolation, VM escape, VM migration, VM rollback and VM sprawl;
Application Programming	Web Application	Injection; Broken Authentication and Session Management; Cross-Site Scripting (XSS); Insecure Direct Object Reference; Sensitive Data Exposure; Missing Function Level Access Control; Cross-Site Request Forgery (CSR); Using Known Vulnerable Components; Invalidated Redirects and Forwards; Insecure APIs;
	Service Oriented Architecture	Machine-to-machine Service Oriented Architectures Applications; Cloud Application Architecture; Security Control APIs
Data	Hazards	Device theft/loss; Data Breaches; Ancillary Data; Database access security;
	Storage Issues	Data privacy, integrity, reliability, backup and recovery vulnerability; Improper media sanitization
Network and Communication	Internet	Denial-of-service; Man-in-the-middle; Eavesdropping; IP-spoofing based flooding; Masquerading; Account Hijacking; Advanced Persistent Threats (APTs); Client-Side and Server-Side Protection
	Intra Cloud	Shared communication infrastructure; Virtual network; Security miss-configurations; Incidence Reporting; Deployment Model; and Enterprise Service Bus (ESB); Malicious Insiders; Social Engineering Attacks
	Identity Management and Access Control	Weak Identity, Credential and Access Management; Authentication; Access Control; Management Graphical User Interface and API compromise;
Business and Legal Issues	Service Level Agreements	Accountability Problems; Business Services Continuity; Incident Response; Administrative or legal outages; Temporary, Prolonged and Permanent Outages; Data Ownership; Privileged user access; Long-term viability; Composite Services; Risk Management
	Governance	Data Location; Law and Regulations; Electronic Discovery; Foreign jurisdiction issues
	Service Providers and Intermediaries	Insufficient Due Diligence; Abuse and Nefarious Use of Cloud Services; Vendor lock-in; Overloads; Unexpected costs; Value Concentration

IV. CLOUD COMPUTING SECURITY SOLUTIONS

It is important to understand the different security threats posed by the core entities and their synergetic malignant effects in the cloud computing environment. Since the strength of the whole depends upon the strength of the weakest element. And cloud has to pass the litmus test of confidentiality, integrity and availability for its services before it can become integral part of organizations and communities. Another important criterion for any security solution to be viable in cloud environment is that it should be in line with the cloud philosophy such as scalable, portable, platform-independent, resilient, ubiquitous, sustainable, shared (multi-tenant) and near-utility computing. Among the wide range of security issues, System Virtualization and Application Programming are most important issues that need to be addressed before going on the cloud. Since security mechanisms in these core areas will restraint the threats in other dimensions. Similarly from the business perspective to mitigate the risks, service level agreement is an important document that needs to be stringently designed. As for the other traditional security challenges good old solution need to be adopted such as Redundancy, Backup and Recovery, and Cryptography.

A. System Virtualization

There are several security risks associated with guest virtualization such as hypervisors or VMMs and host virtualization such as Virtual Machines VMs. The challenges arise if the hypervisors are compromised by the getting the privileged access by some of the VM. Then this malignant VM can do malicious operation with other VMs in the muti-tenant environment. This happens when hackers find the loop holes in the hypervisors software. To counteract this situation Amazon Web Services uses dynamically varied customized versions of XEN HV [7]. Similarly VM operations such as image sharing (VM creation), migration and rollback are prone to security challenges [14]. Also the VM isolation and sprawl related security issues should be managed carefully.

CSA [21] gives the guidelines to secure the virtualization environment. It emphasis upon the utilization of the hypervisor's embedded APIs for the monitoring data traffic of VM. The CSP2 must update the security policy promptly. The data accessed by VMs must be encrypted by policy based key servers and the keys must be stored separate to data and VMs itself. VMs must include firewall, Hot and Network Intrusion Prevention System (HIPS and NIPS), and other traditional security tools. Whereas CSP1 should be responsible for the cleaning of backed up and failed over VMs during VM wiping operation. CSP1 must also maintain the record of VM isolation and notification mechanisms in case of breach of isolation.

B. Application Programming

Cloud computing relies heavily upon web applications or web services and SOA. OWASP's list of top most critical web application security risks is of great importance [20]. The study also mentions the exploitability, prevalence and delectability, and technical impact of each risk. Injection (Structured Query Language SQL, Operating System OS and Lightweight Directory Access Protocol (LDAP)), Insecure Direct Object Reference (DOR), Security Misconfiguration, Missing Function Level Access Control can easily be exploited. Similarly Broken Authentication and Session Management and Using Components with Known Vulnerabilities issues are widespread whereas Cross Site Scripting (XSS) issue is very widespread. The worst part is that XSS, Insecure DOR,

Security Misconfiguration, Cross-Site Request Forgery (CSRF) and Invalidated Redirects and Forwards are easily detectable by the attackers. But the positive side is that they can be fixed easily as well by proper testing and debugging. Similarly the technical impacts of Injection, Broken Authentication and Session Management, and Sensitive Data Exposure are of sever level. However the business impact of each risk is associated with the value of data and the extent of disruption.

OWSAP also has developed several resources to reduce the web application security risks. Among them are Application Security Verification Standard (ASVS) to assess the application security requirements; Developer's Guide and Prevention Cheat Sheet to design the security from the beginning; and Enterprise Security API (ESAPI) to develop the security APIs to produce secure web applications. Similarly Application Security Verification Standard (ASVS) can be used for the code verification. There are also some open source tools for code verification such as O2 and FindBugs. Finally the security and penetration testing tools such as WebScarab and Zip can be used to remove the security threats [20].

C. Multi-Level Integrated Security

There exits huge literature to deliberate and advocate the concept of security-as-a-service. But there are clear negative connotations to this idea that are very detrimental to the proliferation of the cloud computing. Firstly, it means that one has to pay directly for the security a major deterrent in time of scarce competitive resources. Secondly it implies the security is the luxury of effluents hurting the efforts to bridge the digital divide. Or the worst implications is that it sends the signal that without security-as-a- service subscription your resources are not safe, a very serious restraint for the potential adopters.

The correct approach would be to integrate the security features in all of the cloud offerings SaaS, PaaS or IaaS. And various levels of it can be defined such as normal, High or critical. Similarly security control APIs can be developed to enforce these levels. At the time of service subscription user must define the desired level based on the domain specific requirement. And during service configurations these can be enforced through the implementation of the various security control APIs. The cost of these endeavors can be first tried to be realized from the extra utilization of computing, storage and bandwidth or the increase in customer base. The other option, the less desirable, is through the direct billing on the subscription of these APIs. In either case security will remain the integrated concept in the cloud. Similarly the push security model should be followed from CSP1, CSP2 to CSC. Where almost all onus of security embedding should fall upon CSP1 and CSP2 in that order. And the CSC level users should be encouraged or enforced to security standard operating procedures through push models.

D. Service Level Agreements

This document holds a very important position in cloud computing to share the responsibilities to safeguard the interests of all parties involved. There are four parties directly involved in the execution of cloud computing environment: Cloud Service Providers (CSP1), Cloud Service Producer (CSP2), Cloud Service Consumers (CSC) and Data Center Providers (DCP). In addition to them there is involvement of several intermediaries such as security auditors, industry standard entities and governance organizations, governmental bodies etc.

This document should clearly divide the responsibilities of each stakeholder such as CSP1, CSP2, CSC and DCP in securing the individual interests. The fundamental criteria of performance such as confidentiality, integrity and availability of information assets should be meticulously and precisely defined. Additionally it should also lay down the clear guidelines for conflict resolution mechanism, authoritative governance organizations and dispute redressal jurisdictions. Similarly the ownership, security and privacy of the software artifacts and data should also be clearly defined. And in line with the philosophy of the cloud computing of instant provisioning and releasing of resources, the resources should be reclaimed in the usable form without any infringes by the individual parties in case of service discontinuation.

V. Conclusion

Cloud computing is surely culmination of almost previous half century efforts in the field of computing and endeavors to transform computing into utility service such as energy and water. It primarily rests upon three important technologies virtualization, web application and service oriented architecture, and rich internet applications on the client side. Nevertheless the whole paradigm of ICT comes into play, most importantly data centers and network.

This paper has shed some light on the founding technologies of cloud computing such as virtualization and web services/applications. Then the security challenges identified in the literature have been reviewed. These issues majorly circle around two major categories first ones are more traditional issues most importantly the web services and the others are concerned more with the implementation of cloud technology such as virtualization, cloud architecture, cloud deployment models, cloud service models and service level agreements. Further the classification model of security concerns have been provided to help in security issues containment and resolution. Then the security solutions and guidelines proposed by the CSA and OWASP in the area of virtualization and web services respectively along with technique of Amazon Web Services to safeguard the hypervisors have been mentioned.

This paper also presents the concept and importance of multi-level integrated cloud security in contrast to the famous security-as-a-service concept. And also emphasis up on the push model to implement security from CSP1, CSP2 to CSC. Additionally the important guiding principles to design the service level agreements have been discussed. Future work will focus on to develop the models to present different scenarios of cloud computing implementation instances and associated potential security risks. Subsequently the quantitative and qualitative assessment of benefits and security threats in different settings will be carried out. And will be followed by the demonstration of the solutions to mitigate the losses in different scenarios. Hence making it easier for potential cloud adopters to make informed decision to adopt cloud computing.

Cloud computing will surely would be more rewarding and lasting than grid computing or other related concepts due its simple implementation and abstract support for virtually every archaic technology. Therefore it is capable of using full potential of ICT to sustain itself. Further the concept is more important in the present time when world is experiencing the resource constraints to advance into the new future. And the sustainability and the smart cities a close synonym of the former are the norms of the day.

ACKNOWLEDGMENT

I am always thankful to the people who nurtured me throughout my career, family and friends for their moral support, and institutions for financial support.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology Draft (NIST) Special Publication 800-145*, 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[2] N. Ahmad and R. Mehmood, "Enterprise systems and performance of future city logistics," *Http://Dx.Doi.Org/10.1080/09537287.2016.1147098*, vol. 27, no. 6, pp. 500–513, 2016.

[3] N. Ahmad and R. Mehmood, "Enterprise systems: are we ready for future sustainable cities," *Supply Chain Manag. An Int. J.*, vol. 20, no. 3, pp. 264–283, 2015.

[4] Gartner, "Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016," 2016. [Online]. Available: http://www.gartner.com/newsroom/id/3188817.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Clearing the clouds away from the true potential and obstacles posed by this computing capability.," *Commun. ACM*, vol. 53, no. 4, pp. 50–59, 2010.

[6] S. Trigueros-Preciado, D. Pérez-González, and P. Solana-González, "Cloud computing in industrial SMEs: Identification of the barriers to its adoption and effects of its application," *Electron. Mark.*, vol. 23, no. 2, pp. 105–114, 2013.

[7] H. Orman, "Both Sides Now: Thinking about Cloud Security," *IEEE Internet Comput.*, vol. 20, no. 1, pp. 83–87, 2016.

[8] S. Campbell and M. Jeronim, "An Introduction to Virtualization," 2006.

[9] L. Wang, G. Von Laszewski, M. Kunze, and J. Tao, "Cloud computing : A Perspective study," *New Gener. Comput.*, vol. 28, no. 2, pp. 137–146, 2008.

[10] D. S. Linthicum, *Cloud computing and SOA convergence in your enterprise: a step-by-step guide*. Pearson Education, 2009.

[11] Gartener, "Cloud Computing as Gartener Sees it," in *Gartner's Application Architecture, Development & Integration Summit*, 2009.

[12] F. Lui, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badget, and D. Leaf, "NIST Cloud Computing Reference Architecture," *National Institute of Standards and Technology (NIST) Special Publication 500-292*, 2011. [Online]. Available: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=909505.

[13] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.

[14] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Inf. Sci. (Ny).*, vol. 305, pp. 357–383, 2015.

[15] M. Jouini and L. B. A. Rabai, "A Security Framework for Secure Cloud Computing Environments," *Int. J. Cloud Appl. Comput.*, vol. 6, no. 3, pp. 32–44, 2016.

[16] B. R. Kandukari, R. Paturi V, and A. Rakshit, "Cloud Security Issues," in *2009 Ieee International Conference on Services Computing*, 2009, pp. 517–520.

[17] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," *National Institute of Standards and Technology Draft (NIST) Draft Special Publication 800-144*, 2011. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf.

[18] M. A. C. Dekker and L. Dimitra, "Cloud Security Guide for SMEs," *European Union Agency for Network and Information Security*, 2015. [Online]. Available: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes.

[19] "The Treacherous 12: Cloud Computing Top Threats in 2016," *Cloud Security Alliance (CSA) Top Threats Working Group*, 2016. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf.

[20] OWASP Top 10, "The Ten Most Critical Web Application Security Risks," 2013.

[21] "Security guidance for critical areas of focus," *Cloud Security Alliance (CSA)*, 2011. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf.