Preface

The Internet, having its roots in telephone applications in the early 1990s, is often referred to as "The Cloud." By the turn of the millennium, the Internet was referred to as broadband, and the term "in the Cloud" was highly desired. Telephone utilities were investing in "The Cloud" for switching and routing the appropriate connections for phone calls, faxes, live feeds, and signals. Then, around the middle of the decade, Computational Cloud Services, called "Cloud Computing," was firmly in the vocabulary as a way to describe what the user was doing: accessing computing services in the cloud.

At the beginning of the decade, companies began building their Websites in such a way that users could utilize their services exclusively through the use of a browser. Shortly, through the use of more powerful technologies, "in the Cloud" applications became commonplace. By the middle of the decade, most leading corporations with a strong Web presence had reasonable and reliable operation of their services exclusively "in the Cloud."

The "Cloud" represents a fundamental change in the use of IT services, which involves a shift from owning and managing the IT system to accessing IT systems as a service. The term Cloud Services, a distinct terminology from outsourced IT hosting, comes from the fact that the Internet has often been depicted as a "Cloud." Cloud Services have been defined as the services that meet the following criteria (Soman, 2011):

- Consumers neither own the hardware on which data processing and storage happens nor the software that performs the data processing.
- Consumers have the ability to access and use the service at any time over the Internet.

As a result, the definition of Cloud Services is twofold. The first part pertains to the ownership of the actual hardware and software that is used to perform data storage and data processing, while the second part refers to the client's ability to access the service remotely when needed.

On the other hand, as definitions evolved, Cloud Computing denoted the influence of Cloud, and implied the user experience moving away from personal computers to a "Cloud" of computers. In this context, the National Institute of Standards and Technology (NIST) defined Cloud Computing as "a model for enabling ubiquitous, 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." (Mell & Grance, 2011). This cloud model is composed of five essential characteristics, three service models, and four deployment models (Mell & Grance, 2011). Essential characteristics, according to NIST, include

on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service (Mell & Grance, 2011)). Service Models include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), while deployment models include the Private Cloud, the Community Cloud, the Public Cloud, and the Hybrid Cloud.

Moreover, the research firm IDC described Cloud Computing as "an emerging IT development, deployment, and distribution model, enabling real-time delivery of products, services, and solutions over the Internet." It also defined Cloud Services as "Consumer and Business products, services, and solutions that are delivered and consumed in real-time over the Internet" (GensIDC, 2008). Finally, analyst firm Gartner defined Cloud Computing as "a model of computing in which scalable and flexible IT-enabled capabilities are delivered as a service to external customers using Internet technologies" (Gartner, 2009).

As far as healthcare is concerned, the trend appears to be irreversible. Software applications and information once in the realm of the local computer server are now in the sphere of the public Internet. Private health information once confined to local networks is migrating onto the Internet. Patients voluntarily grant access to their health records, while the collection and management of this data are entirely legal. Microsoft and Google are two notable examples of companies following the accelerating likelihood of placing once restricted and private health records, "in the Cloud." Their initiatives hold the attention timing and force convergence of events if we consider the "Transforming Healthcare through IT" and "Enabling Healthcare Reform using Information Technology" initiatives.

THE CHALLENGES

Cloud services amount to three developments that are relevant to an ethical analysis (Timmermans, et al., 2010):

1. The shifting of control from technology users to the third parties servicing the Cloud.
2. The storage of data in different physical locations across multiple servers around the world.
3. The interconnection of various services across the Cloud.

These developments complement with the limitations of current e-health systems (AbuKhousa & Najati, 2012):

- High cost of implementing and maintaining health information technology as it requires investments in software, hardware, technical infrastructure, IT professionals, and training.
- Fragmentation of health information technology and poor exchange of patient data since health information technology, in most cases, exists as separate small clinical or administrative systems within different departments of the healthcare provider's organization.
- Lack of regulations mandating the use and protection of electronic healthcare data capture and dissemination.
- Lack of a Health Cloud model and development standards playing a vital role in the analysis of the following ethical issues of cloud services (Timmermans, et al., 2010).

Control

Customers or users of a Cloud service relinquish control over computation and data (Haeberlen, 2010; Kandukuri & Rakshit, 2009; Grimes, Jaeger, & Lin, 2009). The loss of control can become problematic if something goes wrong. The risks associated with Cloud services are prohibited entry, data corruption, infrastructure failure, or unavailability/outing (Paquette, Jaeger, & Wilson, 2010). As a result, if something goes wrong it can be difficult to determine who has caused the problem (Haeberlen, 2010). Contributing to this is the fact that the boundary between what is part of one's own IT infrastructure and what lies outside it is blurred. Systems can extend the boundaries of various parties and meet the security perimeters that these parties have put in place. This process is called de-perimeterisation.

Problem of Many Hands

Cloud services typically make sense in "a Service-Oriented Architecture (SOA), where all functionality consists of services which can be aggregated into larger applications performing functions to end-users" (Soman, 2011).

Self-Determination

In a world of ubiquitous and unlimited data sharing and storage among organizations, self-determination is challenged. This not only raises privacy issues but also puts at stake the confidence and trust of in today's evolving information society (Cavoukian, 2008).

Accountability

Accountability requires detailed records of actions by its users in the Cloud. It is, therefore, important to consider what is being recorded and who the record is made available to, as there can be a tension between privacy and accountability (Pearson & Charlesworth, 2009). Moreover, in a de-parameterized world, not only the periphery of the organizations' IT infrastructure blurs but also the limits of the organization's accountability become less clear.

Ownership

Besides data actively stored in the Cloud by users, the Cloud also generates information to provide accountability, to improve the services provided, or other reasons such as running or security. Although identity-based systems will provide many benefits, unknown risks and threats are emerging. As Cavoukian (2008) states, "Identity fraud and theft are the diseases of the Information Age made possible by the surfeit of personal data in circulation, along with new forms of discrimination and social engineering made possible by asymmetries of data, information, and knowledge."

Function Creep

Data collected for specific purposes over time might be used for other purposes (function creep).

Monopoly and Lock-In

If only a handful of companies are able to achieve a dominant position in the market for Cloud services, this might lead to abuse or could be harmful otherwise to the interests of the users (Nelson, 2010).

Privacy

Companies providing Cloud services save terabytes of sensitive personal information, which is then stored in data centers in countries around the world. As a result, a key factor affecting the development and adoption of Cloud services is how these companies, and the countries in which they operate, address privacy issues (Nelson, 2010).

Privacy across (Cultural) Borders

Cloud services prepare for a dialogue between different cultures by providing the infrastructure to exchange, collaborate, and communicate across cultural borders. However, different opinions on privacy are further enhanced by cultural differences.

Cultural Imperialism and Dealing with Diversity

Cloud services may lead to increasing cultural homogenization, suppressing local cultures, due to the fact that large corporations, which dominate the Cloud, implement Western values into Cloud applications (Ess, 2008).

On the other hand, healthcare services are delivered by individuals with a variety of beliefs and values. Moreover, patients come from different economic and cultural backgrounds. As a result, the opportunities for misunderstanding are numerous.

In addition, Cloud Computing can significantly reduce IT costs and complexities but enhances resources utilization and faces various technical challenges:

- Most healthcare providers require high availability of the Health Cloud services.
- The Health Cloud requires unfailing reliability for the provided services.
- Huge numbers of medical records and images related to millions of people will be stored in Health Clouds. The data may be replicated for high reliability and better access at different locations and across large geographic distances.
- Scalability requires dynamic organization and reconfiguration as well as an automatic resizing of used virtualized hardware resources.
- Health Cloud services must be flexible to meet individual healthcare requirements; they also must be easily configurable to meet with different needs.
- Services for the Health Cloud can be provided from various Cloud service providers. As a result, a good level of interoperability facilitates easy migration among different available systems.
- It is crucial to offer Cloud services, which underpin appropriate and equitable access control and authentication mechanisms to protect the transfer data to and from clients and service providers.
- Health Cloud services amplify the main concerns in e-health systems (Goldman & Hudson, 2000; Kelly, 2002).

- Health Clouds increase the complexity of network maintainability compared to an individual e-health system.
- Health Clouds require significant changes to clinical and business processes and also to the organizational boundaries in the healthcare industry.
- There are still no clear regulations and guidelines for clinical, technical, and business practices of healthcare in the e-context.
- Ownership of data in the Health Clouds is a place with no clear guidelines.

Among all the challenges listed above, trust, privacy, and security emerge as the major concerns for the Cloud. Hence, several efforts in this area strive to provide solutions to address these concerns and improve the security and privacy of the Health Cloud.

Finally, there are open issues in delivering Cloud services:

- Policy enforcement within the Health Cloud could prove extremely difficult.
- It may only be possible to verify that data processing takes place somewhere within the Cloud, and not the specific places where this takes place.
- It may be difficult to determine the processors of data.
- It may be difficult to know the evolution of the Cloud service, as Cloud Computing is subject to a paradigm shift in user requirements from traditional approaches.

SEARCHING FOR A SOLUTION

The Health Cloud has the potential to support collaborative work among different healthcare sectors through connecting healthcare applications and integrating their high volume of information sources. Dispersed healthcare professionals and hospitals will be able to build networks, collaborate, and exchange information more efficiently. Overall, collecting patients' data in a central location as the Health Cloud results in many benefits:

- The ability to provide a unified patient medical record containing patient data from all patient encounters across all operators results in improving patient care.
- The ability to take advantage of the capabilities of Cloud Computing creates a collaborative economic environment. Moreover, the flexibility to only pay for actual resource utilization shares the overhead costs among the participants resulting in reduced cost.
- The ability to overcome shortage issues in terms of information technology infrastructure and healthcare professionals ameliorates the issue of resources scarcity.
- The storage of clinical data in the cloud enables health organizations supplying related entities with information on patient safety and the quality of care.
- The Health Cloud provides an integrated platform, which hosts an impressive information repository, which can be uniformly and globally accessed, affecting research.
- The Health Cloud increases the ability to monitor the spread of infectious diseases and/or other disease outbreaks.

- Decision makers can use the Health Cloud data for planning and budgeting for healthcare services.
- The Cloud serves as a broker between healthcare providers and healthcare payers streamlining financial operations.
- The Health Cloud facilitates clinical trials since health organizations could partner with pharmaceutical companies and medical research institutions for clinical trials on new medicines.
- The sharing of data allows for the creation of specialized registries targeted for specific types of patients such as cancer and diabetes registries.

Despite all the efforts, the Health Cloud is still in its infancy. However, the models so far proposed indicate the emergence of more comprehensive approaches that will satisfy the requirements of the healthcare professionals. Moreover, although several differences exist between Cloud Computing and multi-agent systems, some common problems can be identified, and various benefits can be obtained by their combined use. Until now, the research activities in the area of Cloud Computing are primarily focused on the efficient use of the computing infrastructure, service delivery, data storage, scalable virtualization techniques, and energy efficiency. Moreover, we could say that the main focus of Cloud Computing research is on the adept use of the infrastructure at reduced cost. On the contrary, research activities in the field of agents are more focused on the intelligent aspects of agents and their use for developing complex applications. In this context, the main problems are related to issues such as a complex system simulation, adaptive systems, software-intensive applications, distributed computational intelligence, and collective learning.

In spite of these differences, Cloud Computing and multi-agent systems share issues and research topics, and overlap in the need to be investigated. In particular, Cloud Computing can provide a powerful, reliable, predictable, and scalable computing infrastructure for the implementation of multi-agent systems. On the other side, software agents can be used as critical components for implementing intelligence in Cloud Computing systems making them more adjusting, adaptable, and self-directing in resource management, service provisioning, and in running extensive applications.

In this frame of reference, the Health Cloud will evolve from being a static repository of data into an active resource that health professionals rely on throughout their daily practice. With new capabilities for accessing online expert systems and applications, Cloud Intelligence will allow tapping into information, analysis, and contextual recommendations in more integrated ways. Virtual agents will migrate to personalized support and assistance that provides information and performs useful tasks.

ORGANIZATION OF THE BOOK

In chapter 1, Rahul Ghosh, Ioannis Papapanagiotou, and Keerthana Boloor provide a summary of research activities in a variety of healthcare related Cloud initiatives. They highlight the key areas of ongoing research and describe others that require attention. Their analysis and observations can be useful to healthcare Cloud professionals, and can motivate interested researchers to initiate new efforts for better healthcare services deployed on the Cloud. In chapter 2, Vahe Kazandjian explores the benefits and challenges of Cloud Computing to the amelioration of medical and healthcare services given the idiosyncrasies of medicine and healthcare. A special focus is given to the extent of readiness healthcare systems manifest to measuring their performance, sharing the findings with patients and communities, and the accountability these systems demonstrate for the promises, implicitly or explicitly, they made

about quality and safety of care. The implications of these promises in shaping patient expectations leading to patient and community evaluation of the healthcare services is the chapter's central theme. In chapter 3, Yiannis Koumpouros argues that the era of open data in healthcare is under way. The progress in technologies along with their adoption by the healthcare providers and the maturity of the citizens has brought the healthcare industry to the tipping point. An unprecedented amount of healthcare data is being generated, and this data comes from researchers, healthcare professionals and organizations, and patients. If we can harness this data, it can help us improve our understanding of disease and pinpoint new and improved therapies more efficiently than ever before. Big Data technologies are coming to market in a rapid way. The challenges, however, are still there due to fragmented systems and databases, semantic differences, legal barriers, and others. In chapter 4, Yang Li, Chao Wu, Li Guo, Chun-Hsiang Lee, and Yike Guo visualize the role Cloud Computing will play in the healthcare sector as spearheading a shift in focus from offering better healthcare services only to people with problems to helping everyone achieve a healthier lifestyle. They first discuss the existing and potential barriers followed by an in-depth demonstration of a service platform named Wiki-Health that takes advantage of Cloud Computing and Internet of Things for personal well-being data management. It is a social platform that is designed and implemented for data-driven and context-specific discovery of citizen communities in the areas of health, fitness, and well-being. At the end of the chapter, they analyse a case study to illustrate how the Wiki-Health platform can be used to serve a real world personal health training application. In chapter 5, Luciana Cardoso, Fernando Marins, Cesar Quintas, Filipe Portela, Manuel Santos, António Abelha, and José Machado present the Agency for Integration, Diffusion, and Archiving of medical information (AIDA), a multi-agent and service-based platform that ensures interoperability among healthcare information systems. In order to increase the performance of the platform, beyond the SWOT analysis they performed, they created a system to prevent failures that may occur in the platform database. The system was implemented in the Centro Hospitalar do Porto (one of the major Portuguese hospitals), and it is now possible to define critical workload periods of AIDA, improving high availability and load balancing. In chapter 6, Wassim Itan**i,** Ayman Kayssi, and Ali Chehab propose the design and implementation of an integrity-enforcement protocol for detecting malicious modification on Electronic Healthcare Records (EHRs) stored and processed in the Cloud. The proposed protocol leverages incremental cryptography premises and trusted computing building blocks to support secure integrity data structures that protect the medical records while: (1) complying with the specifications of regulatory policies and recommendations, (2) highly reducing the mobile client energy consumption, (3) considerably enhancing the performance of the applied cryptographic mechanisms on the mobile client as well as on the Cloud servers, and (4) efficiently supporting dynamic data operations on the EHRs. In chapter 7, Jonathan Sinclair, Benoit Hudzia, and Alan Stewart argue that an EHR is a modern specialisation of a Customer Relationship Management, which specifically focuses on the collection and exchange of electronic health information about individual patients between healthcare organisations. Electronic Heath Records systems hold personally identifiable information that falls under the category of sensitive personal data. As with all industries, the e-health industry sees potential in Cloud-based service offerings and the reduced infrastructure cost they imply, whilst realising the issues regarding security and privacy that may be encountered from outsourcing processing and storage to untrustworthy Cloud Service Providers (CSPs). In their chapter, they propose an approach to handle and audit data privacy requirements by leveraging a carefully designed architecture deployed for auditing data privacy in Cloud ecosystems. In chapter 8, Mauricio Paletta presents the current state and trends of Cloud Computing in healthcare,

as well as a detailed collaboration model based on intelligent agents focusing on the EHR sharing subject. This model for enabling effective service in cloud systems is based on recent research proposal, which defines a collaboration mechanism by means of Scout Movement. The chapter also includes details on the way in which services and service providers are clearly defined in this particular system. In chapter 9, Jalel Akaichi proposes a Cloud Computing location-based services system able to query points of interest, according to mobile users' preferences and contexts, under dynamic changes of locations. The contribution consists on providing software as a service, based on Delaunay Triangulation on road (DT_r), able to establish the Continuous k-Nearest Neighbors (CkNNs) on road, while taking into account the dynamic changes of locations from which queries, enhanced by users' preferences and contexts, are issued. The proposed software, implemented on a mobile Cloud and exploited by mobile physicians for healthcare institutions localization and selection, considerably improves the quality of services provided for patients in critical situations by permitting real time localization of adequate resources that may contribute to save patients' lives. In chapter 10, Piero Giacomelly argues that the Cloud infrastructure has been one of the latest technologies in the e-health sector. However, despite many research studies focusing on the privacy of the e-health data stored on the Cloud, the ways of exchanging e-health information between client and Cloud have not yet been fully addressed. Moving from this initial consideration, the chapter evaluates the possibility of using Message-Oriented Middleware (MOMS) for exchanging data between the Cloud storage and the remote device used in telemedicine and remote monitoring software. The evaluation is done using a Cloud testing environment, low bandwidth connection modem, and a simulation of 50 patients taking a ten-minute 3Lead EGC test. In chapter 11, Andreas Kliem proposes a novel approach that allows sharing medical devices among different operators. This means that each operator books a medical device as long as it delivers required data and is present in the operator's network. Besides cost-effectiveness, this approach can extend traditional Cloud-based e-health systems, usually designed to share Electronic Health Records, by sharing the devices that emit the data. This mitigates judicial constraints because only the data sources and not the data itself are shared and allows for more real-time access to mission-critical data. In chapter 12, Abraham Pouliakis, Aris Spathis, Christine Kottaridi, Antonia Mourtzikou, Marilena Stamouli, Stavros Archondakis, Efrossyni Karakitsou, and Petros Karakitsos analyze the application of Cloud Computing technology for the use in the everyday routine of BioLabs. Moreover, they provide a thorough bibliographical analysis of Cloud applications for research related to biology and biochemistry with emphasis on drug discovery, genomics, and artificial intelligence. In chapter 13, Abraham Pouliakis, Stavros Archondakis, Efrossyni Karakitsou, and Petros Karakitsos argue that using Cloud applications, infrastructure, storage services, and processing power, cytopathology laboratories can avoid huge spending on maintenance of costly applications and image storage and sharing. Cloud computing allows imaging flexibility and may be used for creating a virtual mobile office while security and privacy issues have to be addressed in order to ensure Cloud Computing wide implementation in the near future. In chapter 14, Roma Chauhan explains the need of the healthcare process re-engineering through the implementation of Software as a Service (SaaS). The chapter also highlights the potential and challenges of integrating SaaS-based Health Cloud in the healthcare industry. Finally, it discusses the different Healthcare Clouds and deployment models that can be preferred by the healthcare industry, illustrates SaaS-based solutions for the healthcare segment, and argues that Cloud-based healthcare and mobile healthcare can make health consultation convenient for the patients across the world. In chapter 15, Anastasius Moumtzoglou argues that although the notion of organizational culture is now routinely invoked in organizations and management literature,

it remains an elusive concept, but, in any case, it is clear that managing the culture is one path towards improving healthcare, and Cloud Computing introduces a dynamic system adaptation, affecting the quality of care.

Conclusively, *Cloud Computing Applications for Quality Healthcare Delivery* opens new avenues for understanding research initiatives for Healthcare Clouds, exemplifies big data, arguing that data should not just be meaningful but coordinated, explores interoperability and privacy in Healthcare Clouds, and presents ways of sharing medical information. Finally, it provides insight for Cloud Computing in bio labs and cytopathology, and explains that managing the culture is one path towards improving healthcare, and Cloud Computing introduces a dynamic system adaptation, affecting the quality of care.

Anastasius Moumtzoglou
Hellenic Society for Quality and Safety in Healthcare, Greece & P. & A. Kyriakou Children's Hospital, Greece

Anastasia Kastania
Athens University of Economics and Business, Greece

REFERENCES

AbuKhousa, E., & Najati, H. A. (2012). UAE-IHC: Steps towards integrated e-health environment in UAE. In *Proceedings of the 4th e-Health and Environment Conference in the Middle East*. Dubai, UAE: Academic Press.

Cavoukian, A. (2008). Privacy in the clouds. *Identity Journal,* 89-108.

Ess, C. (2008). Culture and global networks, hope for a global ethics? In J. van den Hoven, & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (pp. 195–225). New York: Cambridge University Press.

Gartner, Inc. (2009). Defining Gartner Highlights Five Attributes*highlights five attributes* of Cloud Computing*cloud computing*. Retrieved June 1, 2013, from http://www.gartner.com/it/page.jsp?newsroom/id=/1035013

Gens, F. (2008). Defining "Cloud Services" and "Cloud Computing". Retrieved June 1, 2013, from http://blogs.idc.com/ie/?p=190

Goldman, J., & Hudson, Z. (2000). Virtually exposed: Privacy and e-health. *Health Affairs*, *19*, 140–148. doi:10.1377/hlthaff.19.6.140 PMID:11192397

Grimes, J. M., Jaeger, P. T., & Lin, J. (2009). *Weathering the storm: The policy implications of cloud computing*. Retrieved June 1, 2013, from http://nora.lis.uiuc.edu/images/iConferences/CloudAbstract-13109FINAL.pdf

Haeberlen, A. (2010). A case for the accountable cloud. *SIGOPS Operating Systems Review*, *44*, 52–57. doi:10.1145/1773912.1773926

IDC. (2008). *IDC market analysis: IT spend on cloud services to grow to $42 billion / 25% of spend by 2012*. Retrieved June 1, 2013 from http://blogs.idc.com/ie/?p=190

Kandukuri, R., & Rakshit, A. (2009). Cloud Security Issues. In *Proceedings of the 2009 IEEE international Conference on Services Computing*, (pp. 517-520). Lincoln. NE: University of Nebraska Press.

Kelly, E. P., & Unsal, F. (2002). Health information privacy and e-healthcare. *International Journal of Healthcare Technology and Management*, *4*, 41–52. doi:10.1504/IJHTM.2002.001128

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. Gaithersburg, MD: NIST.

Nelson, M. R. (2010). The Cloud, the Crowd, and Public Policy. *Issues in Science and Technology*. Retrieved June 1, 2013, from http://www.issues.org/25.4/nelson.html

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253. doi:10.1016/j.giq.2010.01.002

Pearson, S., & Charlesworth, A. (2009). Accountability as a way forward for privacy protection in the cloud. In M. G. Jaatun, G. Zhao, & C. Rong (Eds.), *Cloud computing* (pp. 131–144). Berlin: Springer-Verlag. doi:10.1007/978-3-642-10665-1_12

Soman, A. K. (2011). *Cloud-based solutions for healthcare IT*. Science Publishers. doi:10.1201/b10737

Timmermans, J., Ikonen, V., Stahl, B. C., & Bozdag, E. (2010). The ethics of cloud computing: A conceptual review. In Proceedings of Cloud Computing Technology and Science (CloudCom), (pp. 614-620). IEEE Press.