International Journal of Information Management 47 (2019) 121–130

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Research Note

An integrated holistic model for an eHealth system: A national implementation approach and a new cloud-based security model

Salah Al-Sharhan[a,*], Esraa Omran[a], Kamran Lari[b]

[a] Computer Science Department, Gulf University for Science and Technology, Kuwait
[b] Faculty of Medicine, McGill University, Montreal, Canada

ARTICLE INFO

Keywords:
Holistic eHealth model
EHealth services
eHealth cloud
EHR security
Integrated eHealth framework

ABSTRACT

Although its structure and strategies are rapidly evolving, the impact of the eHealth on the healthcare services is evident. Implementing eHealth systems on a national level can drastically enhance the health practices and services provided to the patients and community. Hence, the engineering of a new model and a holistic framework for eHealth systems becomes a necessity in order to have an effective implementation of these systems. The vast and rapid development in computers, communication, and Internet technologies has significantly affected the contemporary health systems. However, the complexity of the healthcare environment, the abundance of information, the compatibility and the lack of unified eHealth framework creates real challenges to present efficient and attractive eHealth model that encompasses all these elements. Furthermore, the security of the health records and the secure access to the information add a new dimension of complexity. This work presents a new model and an integrated framework for an efficient implementation of eHealth systems at the national level. The proposed model and framework successfully incorporate all the success factors of efficient eHealth system along with a new security model to access the health records.

1. Introduction

eHealth, as defined by the World Health Organization (WHO), is "the use of Information and Communication Technologies (ICT)" for health (WHO, 2006). It is evident that implementing eHealth systems, such as Electronic Health Records (EHR), mobile health, telemedicine systems, and smart hospitals (Merilampi & Sirkka, 2016), has turned to be a cornerstone of enhancing the accessibility, responsiveness and the affordability of the health services (Cebul, Love, Jain, & Hebert, 2011; De Pietro & Francetic, 2018; Oderanti & Li, 2018). In addition, a proper implementation of eHealth systems can dramatically enhance and improve these services locally, regionally, and worldwide (Domínguez-Mayo et al., 2015). However, and similar to other national initiatives such as eLearing (Al-Sharhan & Al-Hunaiyyan, 2012; Al-Sharhan, Al-Hunaiyyan, & Al-sharah, 2010) and egovernment (Turban, Whiteside, King, & Outland, 2017), a successful development of an efficient eHealth system becomes a real challenge (Stroetmann, 2014) as it incorporates different fields, requires interdisciplinary experiences and requires a stringent security model to protect patients information. Hence, an integrated efficient national eHealth model and an implementation framework that incorporates an efficient security model are required to ensure the effective delivery of eHealth services and the required quality of services. Furthermore, the holistic approach must streamline of a generalized acceptance behavior of citizens and ensure the predicting of citizens' preferences and expectations of the healthcare services (Dwivedi, Shareef, Simintiras, Lal, & Weerakkody, 2016).

It is evident that the utilization of the ICT can change the healthcare environment, information accessibility to electronic medical record (EMR), smart hospitals and its emerging technologies Thakare and Khire (2014), communicating with colleagues and third parties using telemedicine Eadie et al. (2014) and Mobile devices and medical imaging Perera and Chakrabarti (2013) are some examples to name in this regard. In addition to information accessibility, such utilization can also enhance the quality of health services and their impact. For example, Cebul et al., have shown that in the United States of America, the meaningful use of EMR could improve the quality of diabetes care of patients regardless their health insurance Cebul et al. (2011).

Despite its obvious benefits that are widely recognized by several international success stories, the current implementation frameworks do not provide a comprehensive and holistic approach form the view of the adopters, implementers and practitioners. It is evident now that developing an integrated framework to implement eHealth systems on a national level forms a real challenge (Van Gemert-Pijnen et al., 2011) identified the potential and limitations of eHealth frameworks proposed

* Corresponding author.
E-mail addresses: alsharhans@gust.edu.kw (S. Al-Sharhan), hussein.i@gust.edu.kw (E. Omran), kamran.lari@mmikuwait.com (K. Lari).

https://doi.org/10.1016/j.ijinfomgt.2018.12.009
Received 1 July 2017; Received in revised form 19 December 2018; Accepted 21 December 2018

between 1999 and 2009. In that study, 16 eHealth frameworks were identified as holistic approaches towards the development and the implementation of eHealth systems. Due to these difficulties and limitations, several international organizations attempted to present a conceptual eHealth framework. For example, the World Health Organization (WHO) proposed a framework that was made up of several components or building blocks (WHO & ITU, 2012). Another conceptual framework for eHealth infrastructure is proposed by the International Society for Telemedicine and eHealth (ISfTeH) (Kwankam, 2012). The proposed framework aims at achieving a maximum positive impact on a country's healthcare sector. In Alberts, Fogwill, Botra, and Cretty (2014), an ICT platform is proposed to develop an eHealth system that enables the integration of heterogeneous health information, the orchestration of eHealth and mHealth services and easy deployment of mobile services.

The complications of eHealth implementation are driven by technical, cultural, managerial, financial and competencies barriers (Almuayqil, 2017). Therefore, this paper proposes a new eHealth model that incorporates all the success factors and a comprehensive layered-based implementation framework for the national eHealth implementation with a new security model of Electronic Health Records (EHR). The proposed framework is designed based on independent layered architecture to improving eHealth output. The proposed model and framework are based on a practical experience as it was developed by the authors to be implemented at the national level in Kuwait. The foundation of the model and framework development is the Capability Maturity Model Integration framework which consists of best practices that covering the product life cycle from conception through delivery and maintenance. To achieve the aim of this paper, the following objectives are developed:

- To develop the success factors of the eHealth implementation.
- To develop a model that incorporates all the success factors and a framework for the eHealth implementation.
- To develop a new EHR security model.

The remainder of this paper is organized as follows: In Section 2, the challenges confronted by the national eHealth initiatives are depicted. In Section 3, a new eHealth model for the national implementation is presented along with all its success factors, and Section 4 presents the implementation framework. The new security model is presented in Section 5. Section 6 describes the implementation of the new system, its testing cases and the results and the discussion. The conclusion of the paper is presented in Section 7.

2. eHealth challenges

Worldwide, several countries have launched eHealth initiatives on a national level. However, despite the governmental support, many initiatives have been subject to slow implementations, change resistance, increasing budget deficits and in some other cases, negative impacts on the quality of services. The challenges of eHealth implementation are a common phenomenon with a similar range of problems being widely reported (Murray et al., 2011). One of the main challenges is the high cost of eHealth implementation, which usually requires high budget and investments of infrastructure, hardware, health solutions, outsourcing and providing the professionals. This may result in a considerable accumulated cost for healthcare organizations. Another dimension of the problem is the high cost of eHealth systems maintenance and the sustainability of the investments due to the rapid change and development in the technologies and ICT field. A major challenge that faces the national implementation of eHealth initiatives is the heterogeneity of the health environment. In many health organizations, one can easily identify a large number of different technologies, protocols, management styles, and data resources. In addition to that, the geographical heterogeneity where most of the health components and premises are scattered in wide geographical and, sometimes, rural areas. The third dimension of challenges lies in the absence of a unified foundation to implement the national eHealth projects. In addition, there is no well-established governance system to guide the implementation and operation of eHealth projects. Furthermore, the security of patients data (Omran, Grandison, & Al Sharhan, 2015) and the lack of unified standards are real concerns for eHealth adopters. For example, the data protection standards, e.g., HIPPA and HITECH are at different levels across countries (AbuKhousa, Mohamed, & Al-Jaroodi, 2012).

3. A new eHealth model and framework

It is known that many countries are not very successful in benefiting and adopting eHealth initiatives due to the lack of understanding the issues related to eHealth's components compatibility, neglecting the eHealth synergy and lack of support of eHealth integration effort (Carvalho, Rocha, Vasconcelos, & Abreu, 2018; Wang, Chen, & Benitez-Amado, 2015). Hence, a holistic model and framework are required to ensure the success the theses national initiatives.

The national eHealth initiatives consist of several interrelated components. The relationship between all the different components of an eHealth initiative is strongly coupled. Hence, a tight coordination during the implementation phase is required in a concurrent manner in order to effectively deliver a successful initiative. In addition, the work stream is highly dependent upon the success of other components. This section presents construction of a new eHealth *model* and implementation *framework*. The main objective here is to overcome some challenges and limitations of the existing frameworks. Several elements are incorporated in the proposed model, and a layered-architecture implementation framework, as explained in the next section, is constructed based on the proposed model. The proposed model is essential in order to understand the different elements, governance, enablers and drivers, and the different roles of stakeholders. It takes into consideration all the success factors for efficient and effective eHealth implementation. The model is depicted in Fig. 1.

The proposed model incorporates all factors of success which ensure efficient and successful implementation. For example, in countries like Kuwait and the GCCs, cultural considerations are a must to have a successful implementation. In addition, it is known that Introducing eHealth technologies needs careful coordination and communication among healthcare professionals, patients, end users, and other stakeholders (Van Gemert-Pijnen et al., 2011). Hence, one can easily realize the importance of the change management component in the model. Another example is the project management and the Program Management Office (PMO); the precise coordination between the different components from a project management perspective is of a vital importance to ensure the success of implementation (Van Gemert-Pijnen et al., 2011).

3.1. The main components of the proposed model

The proposed model considers the three levels of management; namely the strategic or governance, tactic and operational levels and is formed of the following components:

- Strategic Level:
  - National vision and mission.
  - National strategy with all key players parties.
- Tactic Level:
  - Regularity level that deals with the eHealth polices, procedures, and processes.
  - The Management level that deals with organizational assets of health sector and all its related factors.
- Operational Level:
  - ICT readiness on national level: This component deals with

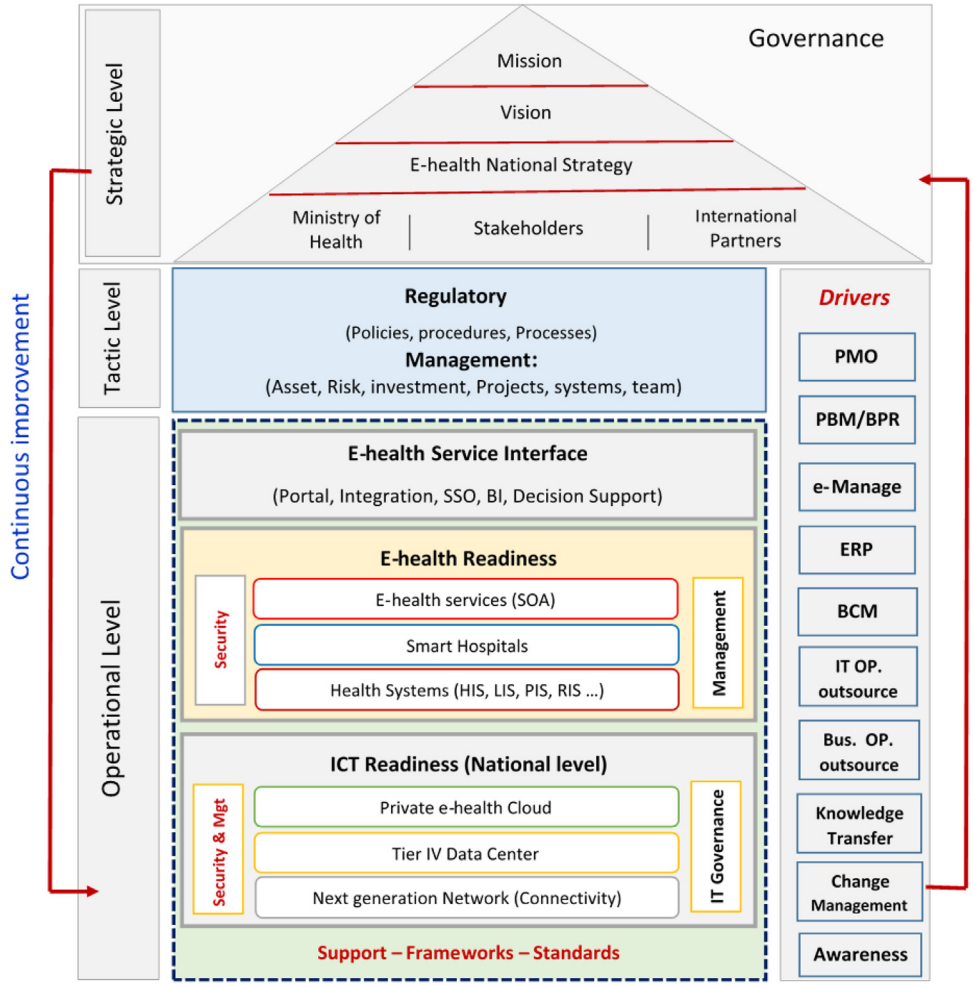


Fig. 1. The proposed holistic eHealth model.

preparing he ICT infrastructure in terms of preparing the next generation network (connectivity), the national data centers, and the eHealth cloud.
- eHealth readiness: this components concentrates on preparing the smart hospitals, eHealth services and other health solutions such as HIS, LIS, PIS and RIS.
- eHealth service interface: this component provides unified interface and access to eHealth system. It incorporates and integrates the national eHealth portal with health solutions, Business Intelligence (BI) solutions along with the decision support systems.

4. eHealth implementation framework

The proposed framework as depicted in Fig. 2 follows a general layered architecture that is composed of different integrated layers; namely, Infrastructure Layer, eHealth Cloud Layer, smart Hospital Layer, Healthcare Solutions Layer, Portal and Decision Making Layer. Additionally, several Drivers/Enablers are incorporated into the framework in order to ensure effective implementation.

4.1. Framework architecture

The following are the components of the integrated implementation framework:

4.1.1. National infrastructure

An effective national eHealth implementation requires reliable and solid ICT infrastructure of which based on the latest technologies. Hence, any eHealth implantation in the upcoming few years must benefit from the next generation networking infrastructure where speeds increase from 10 Gbps to 40 Gbps and eventually 100 Gbps. Here, different optical technologies and cabling infrastructures are required for connecting all the hospitals, clinics, and health premises in one unified, high-speed fiber-optic network. In addition, future eHealth initiatives must take advantage of the emerging green ICT infrastructure (Riaz, Gutiérrez, & Pedersen, 2009) and the integrated ICT infrastructure in complex urban systems (Adepetu, Arnautovic, Svetinovic, & de Weck, 2014). These new trends of integrated infrastructures can provide reliable infrastructure on the national level without major financial challenges.

Supporting the mission of critical eHealth systems and being able to quickly and cost efficiently adapt the emerging technologies are critical functions of a well-built IT network infrastructure. Furthermore, the backbone of this infrastructure must be secure, robust and adaptable structured architecture (Amin, 2014; Olsen et al., 2015). Through the Infrastructure component of the implementation framework, the structured cabling system will ensure increased data speeds, allow for IP services, provide a full connectivity between the eHealth cloud component, and all the health premises, and a full wireless coverage within hospitals and other health premises, and standardize the health network across the country.

4.1.2. eHealth private cloud

Cloud computing introduces a system that can provide distributed, rapidly provisioned and configurable computing resources which are a

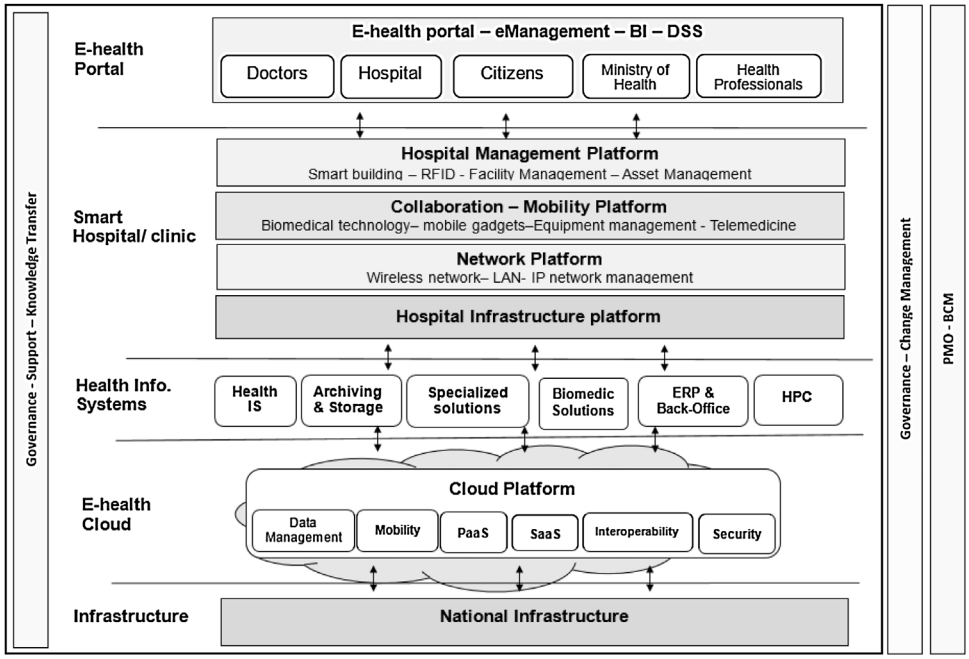


Fig. 2. The layered architecture implementation framework.

rapid elastic and measured (Mell & Grance, 2009). Public cloud computing is the delivery of on-demand computing resources over the Internet on a request-and-serve basis. Private cloud computing, on the other side, can utilize smaller private access networks. Hence, it will be the best approach to implement a national initiative since it relies on sharing computing resources rather than having local servers or data centers in each hospital to run different health applications. Recent years have witnessed several emerging eHealth based on cloud computing as an efficient solution to face the cost challenges of individual solutions (Moumtzoglou, 2014). The reader may refer to Ahuja, Mani, and Zambrano (2012) and Hu and Bai (2014) for the different trends of cloud computing in healthcare. In the proposed model of eHealth, the suggested cloud computing is based on a private eHealth cloud implementation that mainly provides the following orchestrated services:

1. Cloud-based applications – or Software as Service (SaaS) – runs on the Central cloud that is connected to users' computers via Kuwait fiber networks. These networks connect all the hospitals, primary clinics and health premises to the cloud. The cloud will provide the hospitals and other stakeholders with a wide spectrum of healthcare systems, e.g., the Health Information System (HIS), Lab Information System (LIS), Pharmacy Information System (PIS), and Radiology Information System (RIS). Patients and physicians can access these services using the Internet, regardless of their physical location.
2. Platform as a Service provides (PaaS) – a cloud-based environment with everything required to support the complete life cycle for delivering the cloud-based health applications – without the cost and complexity of buying and managing underlying hardware and software or provisioning and hosting.
3. Infrastructure as a service (IaaS) provides all hospitals and clinics in Kuwait with on demand virtual computing resources, such as servers, storage networking to other components, and data center space on a requirements basis.

In addition, eHealth private cloud can provide 'storage as a Service' of which provides data resources as well as storage to entire health software. This may include a medical electronic record, an imaging storage, a health portfolio and lab tests information to name a few. A major characteristic of proposed storage as a service is the reliability and redundancy. This is based on the fact that the private eHealth cloud is built based on two reliable data centers and several disaster recoveries. This architecture provides distributed database design in order to possess a higher availability. Redundancy among these several databases and different views controls, to a large extent, the consistency of the data (He, Fan, & Li, 2013).

4.1.3. eHealth solutions

Hospital Information Systems (HIS) (Carvalho et al., 2018) are broken into two categories: Clinical Information Systems (CIS) and Nonclinical Information Systems (NCIS). The clinical information systems include, but not limited to, Electronic Health Records (EHR) (Gagnon et al., 2016), Picture Archiving and Communication System (PACS), Laboratory Information System (LIS), Pharmacy Information System (PIS) and Radiology Information System (RIS). It also includes other systems, e.g., the Nursing Information System (NIS) (Merilampi & Sirkka, 2016). The Nonclinical Information Systems (NCIS) include the Inventory control system, Financial accounting system, Budgeting Planning and Management, HR Management, Asset, and Facility Management and HSE systems. Furthermore, an efficient telemedicine solution is a must to provide complete eHealth services (Chandwani, De, & Dwivedi, 2018).

Electronic Health Record has been defined by the US Institute of Standards and Technology as "a longitudinal collection of patient-centric healthcare information available across providers, care settings and time. It is a central component of an integrated health information system" (NIST, 2004). EHRs can be used for the digital input, storage, display, retrieval, printing and sharing of information contained in a patient's health record. These systems are varied on multiple dimensions, including levels of sophistication, details, data source, time-frame and extent of integration. Typical EHR records may contain the patients' historical medical data, scanned documents and digital images and radiology images such as X-rays, magnetic resonance imaging (MRI) and nuclear medicine, to name a few. More detailed EHRs may include also nonclinical data. EHRs can, therefore, be used by a variety of end users such as clinicians, administrators, and patients themselves. EHRs can also have varying degrees of integrated function to assist in interfacing to other systems such digital PACS, prescribe (ePrescribing), and access to CDSSs.

4.2. Success factors of national eHealth

To guarantee the success of the national eHealth implementation, it is important to identify the factors impacting the eHealth implementation. Hence, a multidimensional identification process has been conducted to identify the success factors of the eHealth national implementation. Furthermore, this work aims at proposing a holistic framework for eHealth implementation as a project-based implementation approach. Therefore, the main dimension here is to integrate the eHealth success factors into knowledge-based and project-based implementation approach. In summary, these factors, also called drivers, are incorporated in the proposed holistic model as listed below:

1. Program Management Office (PMO) (Afzal & Gauthier, 2017).
2. Business Process Engineering/Re-engineering (Hassan, 2017).
3. Enterprise Resource Planning (ERP) (Falcini & Rinaldi, 2017).
4. Business Continuity Management (BCM) Haraty, Kaddoura, and Zekri (2018).
5. IT/Operation outsourcing Program and handling its related risks (Bahli & Rivard, 2017).
6. Leadership, Knowledge Transfer and Training (Brunner et al., 2018).
7. Governance system (Tonelli, de Souza Bermejo, Dos Santos, Zuppo, & Zambalde, 2017; Van de Pas et al., 2017)
8. Change Management Program (Aarakhia & Hollohan, 2017).
9. Awareness program.

The next section presents a new model of security to access the health information at the eHealth service interface level. The rest of the model's component will be discussed in details in a future work.

5. Electronic health records: a new security model

The current healthcare security and privacy technologies tend to be too complex to be implemented, as they do not provide a natural fit for the domain and do not provide the ability of true sharing and contribution between different institutions/hospitals. These institutions are quickly confronting security dangers and vulnerabilities once moved to the digital environment. This study has investigated other mechanisms that can decrease intricacy, increase overall system presentation, and be easily implemented. Although the role-based access control (RBAC) (Zhou, Varadharajan, & Hitchens, 2013) may be viewed as the best mechanism to use the ability to formalize model specifications needed, complex healthcare scenarios, which may include emergency or exception-based access, is currently beyond the capabilities of existing staff and available systems. Furthermore, the shortage of awareness and staff proficiency in the part of RBAC boosts the ambiguity of equally the technological viability of rising victorious RBAC-facilitated creations and the growth rate and the edge of time. It is evident that the lack of awareness is always harmful in the technical field. Therefore, the staff members and other professionals must be properly aware of the technicalities related to the RBAC system. Similarly, successful development of RBAC is necessary for retrieving relevantly, and quality assured outcomes in a proper way. Moreover, learning about the technicalities will also enhance the effectiveness of the system in professional settings. In this paper, the Chain Ontology-based method is used to overcome these concerns in RBAC method.

The literature suggests a number of main data access management methods such as Role Based Access Control (RBAC) with all its subversions, Hippocratic, eXtensible Access Control Markup Language (XACML) and Chain method. Below is a brief introduction of each method:

5.1. RBAC

The Role-Based Access Control (RBAC) (Zhou et al., 2013) is proposed to handle the concerns related to the Mandatory Access Control (MAC) and Discretionary Access Control (DAC), and address their limitations. In particular, RBAC simplifies the management of permissions by assigning privileges for operating on some resources to roles instead of assigning them to users. After that, each user assigned a specific role(s) depending on his/her current position, job requirements and responsibilities within the organization. The main advantage of RBAC in data access methods is its popularity where it is almost used everywhere in local data access management. The main disadvantage of the RBAC, on the other side, is the lack of knowledge and staff expertise that area which may increase the uncertainty of technical feasibility and successful implementation. This would increase the time, effort and cost of design and implementation. Another disadvantage of the RBAC rises when the database becomes complex and where there is a large number of roles to administer as well as large numbers of users. Due to these disadvantages, using RBAC in a cloud-based data access management will lead to problems related to the data security and management as the system lacks the scalability.

5.2. Hippocratic

RBAC is not specifically designed to protect privacy while Hippocratic databases (HDB), by contrast, are designed for data protection. The method works on the basis of purpose and inspired by the famous Hippocratic Oath. Legitimate purposes are specified and data access permissions are associated with these purposes. Re-architecting database systems are needed to include responsibility for the privacy of data (Agrawal, Kiernan, Srikant, & Xu, 2002; WHO, 2013). However, and with this strength, the Hippocratic method suffers from its complexity, which makes it more useful for local systems and not in a cloud-based environment where the number of users and purposes to access the data is huge (big data).

5.3. eXtensible Access Control Markup Language (XACML)

The XACML is a method that has been proposed by OASIS (Standard, 2005a, 2005b). It is a structured language for expressing access control policies and a query-response protocol for access requests and decisions. To address privacy concerns, OASIS defines a profile of XACML for the specification of privacy policies. In particular, the XACML's Privacy Profile defines standard variables to represent the purpose for which data was collected and the purpose for which data is requested, and shows how to create a constraint that requires these to be consistent. The main advantage of XACML in data access methods is its simplicity to develop the data access policy; however, the addition of the new data access policy to the cloud is not easy.

5.4. Chain-Based Access Control

The Chain-Based Access Control (ChBAC) (Omran, Grandison, Nelson, & Bokma, 2013) system has been developed based on the earlier idea of a chain of acts that have been suggested by Al-Fedaghi (2007). Fedaghi introduced the idea by changing the principle of data access control from purposes to chains of limited acts. He claimed that the management of attributes and users' purposes is a complicated issue. To simplify the mapping process, users are assigned to roles, and access purpose permissions are granted to roles associated with responsibilities or functionalities, but not directly to individual users. The chain of acts method consists of a set of seven limited acts: collecting, creating, storing, using, mining, processing, and disclosing personal information, which is distributed amongst the different groups of roles. These acts define the policy and purpose for which a certain group of roles accesses the database. It also includes the actions that the user can apply on the database.

5.5. Type of the problem

The problem can be summarized as straining authorized and unauthorized consumers and then categorizing authorized consumers using ontology into classes of users that could contact assured groups of information. While fresh users contact the system and mature users no longer have the right to use the structure, the significance of having a trustworthy, stretchy attitude that can manage with all the anticipated and unanticipated troubles become vital. In addition, the structure will provide such flexibility and security to a huge repository of data that is available in the cloud.

5.6. The proposed solution

A new method is necessary that integrates the principles of cloud computing with the Chain technique beside ontology for modeling solitude strategies in a structure of the database. Unlike Role Based Access Control (RBAC), Chain does not need to have extensive, complex policies for every grouping of roles. As an alternative, a set of seven imperfect actions like Creating, Processing, Disclosing, Storing, Collecting, Using and Mining are dispersed amongst the unlike assembly of roles. These actions are the strategy and rationale of why such assembly of functions is contacting the database and at the same moment, it comprises the acts that the user could pertain to the database. The cloud will solve the problem of the availability while the Chain method offers an uncomplicated plan resolution with numerous circumstances, strategies, and hierarchies, while the ontology provides the dynamicity (the aptitude to inform the database which is according to the known limitations from the ontology GUI) which is not accessible in existing conventional accessing database supervision procedures. Fig. 3 depicts the overall system design and Table 1 presents a comparison between the conventional RBAC method and the proposed Chain-Ontology based method.

As shown in Fig. 3, the overall system architecture consists of the following parts:

- A Virtual Private Cloud (VPC) is an on-demand configurable pool of shared computing resources allocated within the AWS cloud environment, supplying a confident level of separation among the diverse Kuwaiti hospitals.
- Elastic Load Balancing automatically allocates incoming traffic across multiple EC2 instances. Each hospital should create a load balancer and register instances with the load balancer in one or more Availability Zones. The load balancer serves as a single point of contact for clients. This enables the hospitals to increase the availability of their application. Hospitals can add and remove EC2 instances from the load balancer according to their needs, without disrupting the overall flow of information.
- A VPN (Virtual Private Network) gateway is a network device that connects two or more devices or networks together which provides better security especially after applying the ontology-chain based principles.
- The circled components in the design are where the developed chain ontology-based system will be applied.

5.7. The Proposed Security Model

The Proposed Security Model is depicted in 4 shows how the security model works. First, each user will be assigned a number of chains of acts (out of the 7 acts presented in Section 5.6 above). Next, he/she will be assigned a role that is connected to the given chains (e.g., a doctor with create, process, and store patient data). Then he will have a session to use/apply his acts on the data by giving access permission that has been created using Resource Description Framework (RDF), which is a standard model for data interchange on the Web. It has features that can effectively enhance the data merging regardless the differences in their underlying schemas. Furthermore, the RDF supports the independent evolution of schemas over the time. This will forbid disclosing unneeded (extra information). As the doctor as a role will have a session to collect information about patients who have an appointment with him only or an emergency case and he will not be able to access information about other patients who have medical records at the hospital.

Fig. 5 describes an overview of the basic structure of the ontology developed for the proposed security system, the Classes (such as SystemUser, Context, Record, …) the subclasses (Doctor, Nurse, MedicalRecord, …), and the relations (hasPatient, hasApplicablePolicy, …) that have been used in the RDF relationships. An example that has been used in the experiments is a Doctor (Sub Class) from a MedicalStaff (Class) hasApplicableChain (relationship), hasPrerequisiteCondition (relationship) and hasPrerequisiteCondition (Relationship) to a MedicalRecord (Sub Class) from Record (Class).

RDF file generation: A separate module is used to generate RDF files from the database which has been included as part of the D2RQ

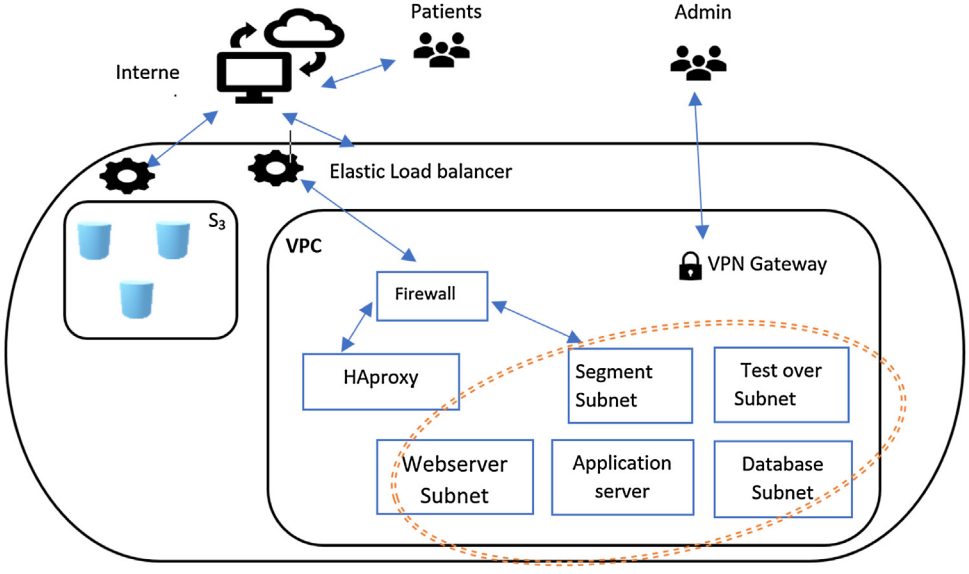


Fig. 3. Overall system design.

Table 1
Comparison between RBAC and Chain-Ontology Method.

Method	RBAC method	Chain-Ontology based method
Access right permission given by	Administrator	Administrator for the first time, and then system will do it automatically.
Content sensitivity	Not aware	Aware using ontology.
Need for expert database administrator	In need	No need, the ontology and limited acts will do the work.

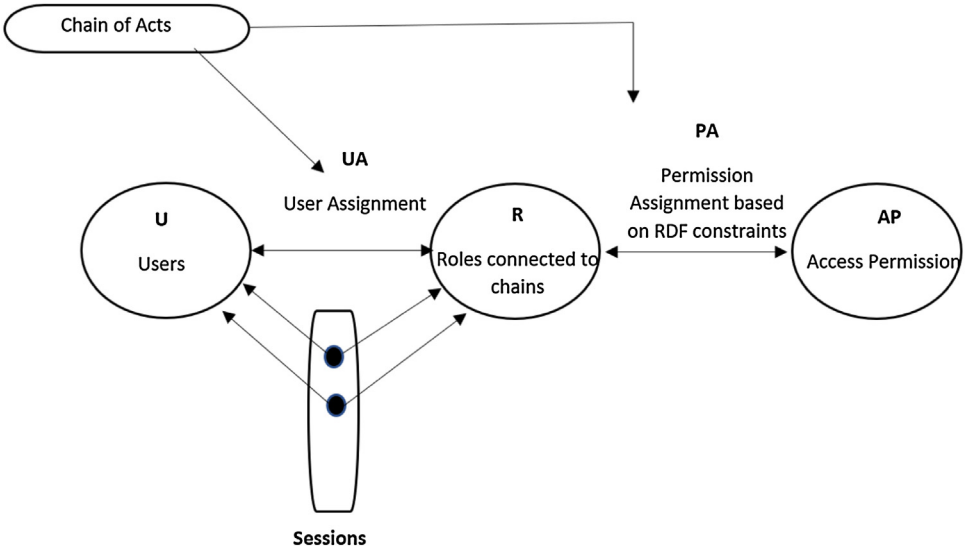


Fig. 4. The Proposed Security Model.

project. D2RQ provides a system to access relational databases as virtual, RDF graphs and has core java components for generating RDF files out of relational databases in all RDF file formats. For more details about the D2RQ project, the reader may refer to (project). For the proposed system, a dedicated class called **GenerateRDF.java** is used. It has a static method *updateRDF()* that generates the RDF (or update it) from the database connection.

Sparql query of rdf file using Jena: Jena library is used to connect to the generated RDF file from the last step and do all basic queries to find out data and related data using triples, in this project we have 12 different Sparql queries to obtain all sort of related data, from simple straightforward data to cross table related data. All sparql commands are separated into a function in a class-file named RetrieveFromRDF.java which creates a Jena model from the database.ttl file generated on the previous step, the code is straightforward Sparql code.

6. Implementation and experimentation results

The Public Healthcare System in Kuwait is currently suffering from being scattered and working in silos with a high demand for quality healthcare services. According to the World Health Survey in Kuwait (WHO, 2013), segments of the Kuwaiti population believe that healthcare system responsiveness, accessibility, and affordability could be improved. These factors, in tandem with technological advances, economic requirements and social and cultural changes, drive the need

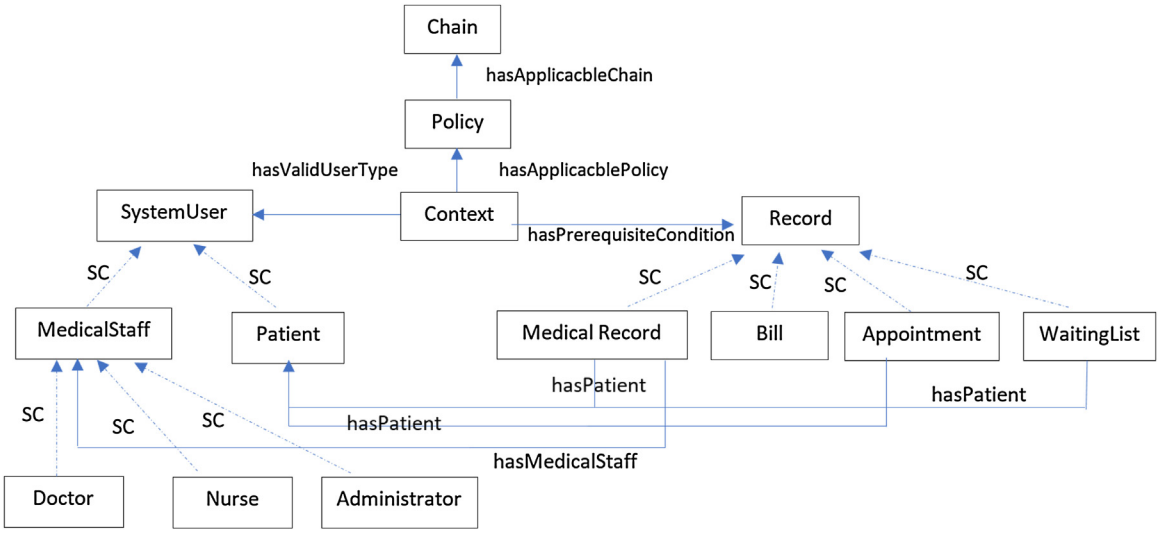


Fig. 5. Basic structure of the ontology.

for the Ministry of Health (MoH) to integrate information and communication technologies (ICT) into the public health sectors delivery system. Currently, the health information landscape of Kuwait is characterized by scattered information distributed across the different public and private hospitals. Significant challenges face any attempt to integrate, sharing, the information or to have unified health solutions. In particular, the MoH faces persistent barriers when undertaking critical functions, e.g., gathering, analyzing, managing and exchanging information in all areas of the sector from research to budget planning. In addition, no clear measures or key performance indicators (KPIs) can be harnessed to assess the system in its entirety. Hence, the implementation of the proposed national eHealth framework and the proposed access security model becomes essential to enhance the services and the accessibility of the records.

6.1. Tests and results

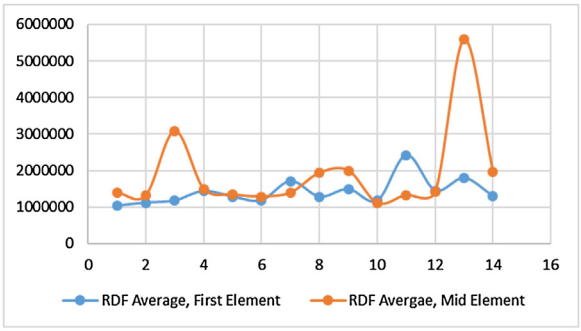
To prove the applicability of the proposed system in a real environment, we have implemented the system and conducted several test scenarios. In these tests, we have studied the performance of the proposed system and the classical RBAC system. The comparison was conducted on 7 data sets and different record locations. In the output of the tests, the figures and table, the name *Database* (DB) will be given to the traditional database with RBAC constraints and *RDF* for the developed system which uses a chain and RDF constraints to retrieve data. For all the generated data tests, we set the values of the episodes per patient to 5, the number of doctors' notes to 5, and the number of appointments per patient to 3. For each of the graphs presented, the test number is on the *x-axis* and the execution time (in nanoseconds) is on the *y-axis*. It should be noted that our performance numbers only account for the query information retrieval time, from inside the Web services, and does not include any client communication overhead. We also test the validity of the information retrieved using Web service clients; by using both the console and the full Graphical User Interface in Java. For example, Table 2 represent the data set 7 and its attributes and sample of the tests output on this data set.

The first case tests the time required to retrieve 100 patient records which represent the case of a small clinic. Fig. 6a and b compares the time required to retrieve the 100 patient records with 5 doctors in 5 different departments. In this simple case, the proposed RDF system outperforms the classical RBAC (DB).

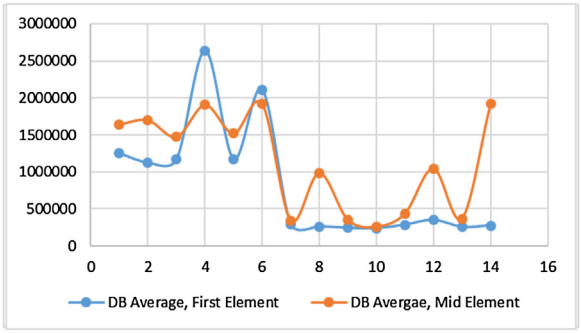
The second case compares the proposed RDF system to the classical RBAC in terms of retrieval time of 10,000 patient records, with 50 doctors in 20 different departments. Fig. 7a and b depicts the time required to retrieve the 10,000 patients records using the proposed system (RDF) and the RBAC (DB); respectively. Again, it is obvious that the proposed RDF system outperforms the classical RBAC (DB). The next section presents an overall comparison of the performance of the two methods using small, average and big data.

Table 2
Data set 7.

#	Attribute	Value
1	Patient count	27,000
2	Doctor count	200
3	Department count	20
4	Episodes per patient	5
5	Doctor instructions	5
6	Appointment per patient	3
7	Bill per patient	1
8	Nursing per patient	1
9	Prescription per patient	1
10	Surgery per patient	1
11	Vitals per patient	1
12	Total rows generated for test	513,220

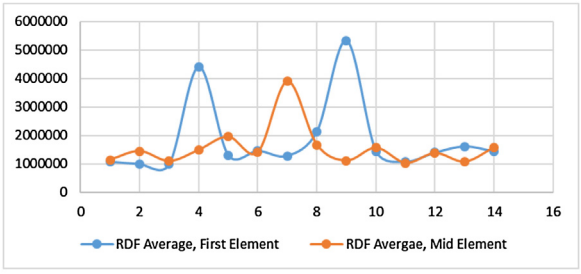


(a) First Element vs Mid Element RDF

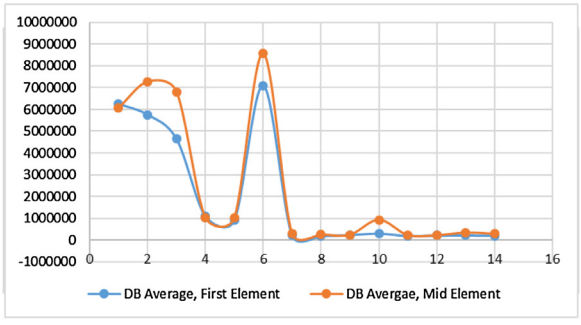


(b) First Element vs Mid Element DB

Fig. 6. Retrieving 100 patients, 5 doctors, 5 departments.



(a) First Element vs Mid Element RDF



(b) First Element vs Mid Element DB

Fig. 7. Retrieving 10,000 patients, 50 doctors and 20 departments.

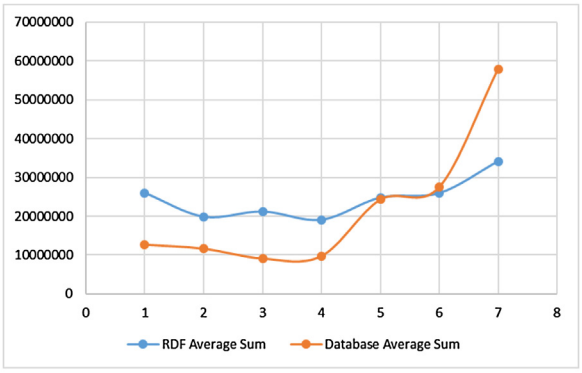
6.2. Overall comparison

In this section, we will sum all averages for each test and then compare the proposed RDF system and RBAC (DB) performance for the 7 tests. Table 3 shows the sum of all averages of all 7 tests.

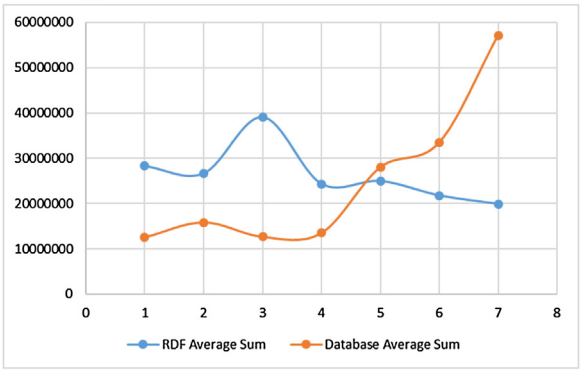
After that, the sum of all the averages was used to compare the proposed RDF system to the classical RBAC (DB). Fig. 8a shows the performance of the two systems for all the 7 datasets considering the first element retrieval time (nanosecond). Fig. 8b, on the other hand, compares the performance of the two systems for the 7 datasets

Table 3
Sum of all averages of all the 7 tests.

Set #	RDF first element	RDF mid element	DB first element	DB mid element
Set 1	26018523	28287497.33	12693475.33	12536107.33
Set 2	19883076.67	26669717.33	11663679.33	15850942.67
Set 3	21224181.33	39090070.67	9131463	12647647.67
Set 4	19099274.33	24362027.33	9767775.333	13503089.33
Set 5	24808447.67	24998869	24303821	28017009
Set 6	25954258.67	21813614	27533585.33	33472027.33
Set 7	34161658.33	19923364.67	57968616.33	57121866.67



(a) RDF vs DB Average Sum-First Element Tests



(b) RDF vs DB Average Sum-Mid Element Tests

Fig. 8. RDF vs. DB sum of averages performance.

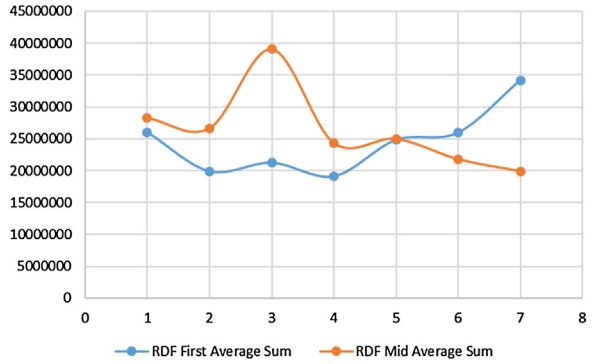


Fig. 9. RDF sum of averages performance for different elements.

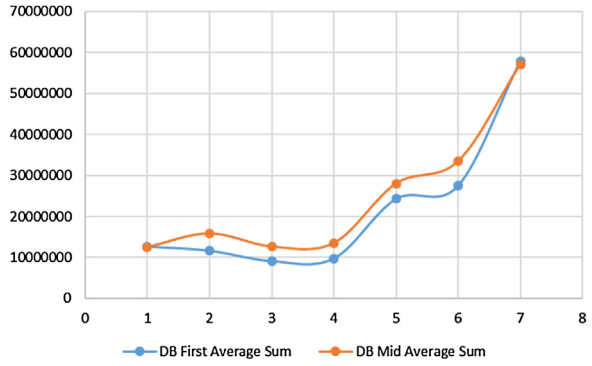


Fig. 10. DB sum of averages performance for different elements.

considering the mid element retrieval time.

In our tests, the sum of averages started to show that from Set 5 onwards, the sum of the average of all 14 queries have resulted in RDF performing better in data retrieval, which indicates that RDF queries may perform better in information retrieval from large data sizes (in our case 100,000 records and above). The retrieval time in DB increases linearly with the increase of the records number. This situation may lead to a denial of service in big data stored in the cloud for a whole country-above 4 million records.).

The next set of tests demonstrates the performance of the proposed RDF systems and the RBAC in terms of different record locations. Fig. 9 depicts the performance of the RDF system based on the sum of averages to compare the retrieval time for the first and mid elements. Fig. 10 shows the performance of the RBAC (DB) system for the same case. It is evident that accessing various elements is highly dependent on their location in the graph. For example, RDF retrieval of mid elements tends to be faster than accessing first elements, which is opposite to the classical RBAC system. In that system, accessing different elements in the database yields relatively very close results as shown in Fig. 10. As expected, accessing mid elements or elements with large IDs generally costs more than accessing elements that comes first in the database. Hence, it is clear that the newly developed method (chain ontology-based) suits the big data environment which is the case of a one eHealth cloud for the whole country.

7. Conclusion

This work introduces a new eHealth model for national implementation. It also aims to get the benefits of cloud computing, which is mainly the availability of the information, while preventing its disadvantages especially the lack of security and privacy as it introduces a new security model based on the chain ontology. In addition to the new eHealth model, the work introduces a new implementation framework where the objective is to overcome the challenges and limitations of existing frameworks. As the system integrates the idea of cloud computing with up to date methods and other layers, like the infrastructure and management layers, the proposed eHealth system is expected to have a great effect on the health sector. The rationale behind this perspective is that it will increase the quality of services by creating a better technological environment for information sharing between different healthcare institutions. Data or information security is of great importance, so it is highly preferable to incorporate the best technology and mediums. In this reference, cloud-based computing and information systems are into a leading era, and with the proposed security system, it will retrieve the required information faster and with higher

security.

References

Aarakhia, M., & Hollohan, K. (2017). The connecting south west ontario (cswo) benefits model: An approach for the collaborative capture of value of electronic health records and enabling technology. *Building Capacity for Health Informatics in the Future, 234*, 6–12.

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-health cloud: Opportunities and challenges. *Future Internet, 1*, 621–645.

Adepetu, A., Arnautovic, E., Svetinovic, D., & de Weck, O. (2014). Complex urban systems ICT infrastructure modeling: A sustainable city case study. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44*, 363–374.

Afzal, A., & Gauthier, J. B. (2017). *Project management and practitioners in the health sector: From the Quebec healthcare system perspective to pm literature review.* https://hal.archives-ouvertes.fr/hal-01579996.

Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2002). *Hippocratic databases. VLDB'02: Proceedings of the 28th international conference on very large databases*. Elsevier143–154.

Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. *Network and Communication Technologies, 1*, 12.

Al-Fedaghi, S. S. (2007). *Beyond purpose-based privacy access control. Proceedings of the eighteenth conference on Australasian database – Volume 63*. Australian Computer Society, Inc.23–32.

Al-Sharhan, S., & Al-Hunaiyyan, A. (2012). *Towards an effective integrated e-learning system: Implementation, quality assurance and competency models. 2012 seventh international conference on digital information management (ICDIM)*. IEEE274–279.

Al-Sharhan, S., Al-Hunaiyyan, A., & Al-sharah, H. (2010). *A new efficient blended e-learning model and framework for k12 and higher education: Design and implementation success factors. 2010 fifth international conference on digital information management (ICDIM)*. IEEE465–471.

Alberts, R., Fogwill, T., Botra, A., & Cretty, M. (2014). *An integrative ICT platform for ehealth. IST-Africa conference proceedings, 2014*. IEEE1–8.

Almuayqil, S. (2017). *Integrated framework of knowledge discovery and knowledge management for e-health in Saudi Arabia: Supporting citizens with diabetes mellitus*Staffordshire University Ph.D. Thesis.

Amin, S. M. (2014). *Robustness, resilience, and security of national critical infrastructure systems.* Wiley Handbook of Science and Technology for Homeland Security.

Bahli, B., & Rivard, S. (2017). *The information technology outsourcing risk: A transaction cost and agency theory-based perspective. Outsourcing and offshoring business services*. Springer53–77.

Brunner, M., McGregor, D., Keep, M., Janssen, A., Spallek, H., Quinn, D., et al. (2018). An ehealth capabilities framework for graduates and health professionals: Mixed-methods study. *Journal of Medical Internet Research, 20*.

Carvalho, J. V., Rocha, Á., Vasconcelos, J., & Abreu, A. (2018). A health data analytics maturity model for hospitals information systems. *International Journal of Information Management*.

Cebul, R. D., Love, T. E., Jain, A. K., & Hebert, C. J. (2011). Electronic health records and quality of diabetes care. *New England Journal of Medicine, 365*, 825–833.

Chandwani, R., De, R., & Dwivedi, Y. K. (2018). Telemedicine for low resource settings: Exploring the generative mechanisms. *Technological Forecasting and Social Change, 127*, 177–187.

De Pietro, C., & Francetic, I. (2018). E-health in switzerland: The laborious adoption of the federal law on electronic health records (ehr) and health information exchange (HIE) networks. *Health Policy, 122*, 69–74.

Domínguez-Mayo, F., Escalona, M., Mejías, M., Aragón, G., García-García, J., Torres, J., et al. (2015). A strategic study about quality characteristics in e-health systems based on a systematic literature review. *The Scientific World Journal,* 2015.

Dwivedi, Y. K., Shareef, M. A., Simintiras, A. C., Lal, B., & Weerakkody, V. (2016). A generalised adoption model for services: A cross-country comparison of mobile health (m-health). *Government Information Quarterly, 33*, 174–187.

Eadie, L., Heaney, D., Dowie, L., Glynn, L., Casey, M., Hayes, P., et al. (2014). Implementing transnational telemedicine solutions. *eTELEMED 2014, the sixth international conference on eHealth, telemedicine, and social medicine,* 68–73.

Falcini, F., & Rinaldi, G. (2017). *Medical records, ehealth and health it: What are the key points for the organizational benefits and for the improvements of the modern local health organisations? New perspectives in medical records*. Springer129–140.

Gagnon, M. P., Simonyan, D., Ghandour, E. K., Godin, G., Labrecque, M., Ouimet, M., et al. (2016). Factors influencing electronic health record adoption by physicians: A multilevel analysis. *International Journal of Information Management, 36*, 258–270.

Haraty, R. A., Kaddoura, S., & Zekri, A. S. (2018). Recovery of business intelligence systems: Towards guaranteed continuity of patient centric healthcare systems through a matrix-based recovery approach. *Telematics and Informatics, 35*, 801–814.

Hassan, M. M. (2017). An application of business process management to health care facilities. *The health care manager, 36*, 147–163.

He, C., Fan, X., & Li, Y. (2013). Toward ubiquitous healthcare services with a novel efficient cloud platform. *IEEE Transactions on Biomedical Engineering, 60*, 230–234.

Hu, Y., Bai, G., 2014. A systematic literature review of cloud computing in ehealth. arXiv preprint arXiv:1412.2494.

Kwankam, S. Y. (2012). Successful partnerships for international collaboration in e-health: The need for organized national infrastructures. *Bulletin of the World Health Organization, 90*, 395–397.

Mell, P., & Grance, T. (2009). *The NIST definition of cloud computing.* US Institute of Standards and Technology.

Merilampi, S., & Sirkka, A. (2016). *Introduction to smart eHealth and eCare technologies. Devices, circuits, and systems.* CRC Presshttps://books.google.com.kw/books?id=oCgNDgAAQBAJ.

Moumtzoglou, A. (2014). *Cloud computing applications for quality health care delivery.* IGI Global.

Murray, E., Burns, J., May, C., Finch, T., O'Donnell, C., Wallace, P., et al. (2011). Why is it difficult to implement e-health initiatives? A qualitative study. *Implementation Science, 6*, 2–11.

NIST (2004). *US institute of standards and technology.* Accessed 30.12.14 http://www.itl.nist.gov/div897/docs/EHR.html.

Oderanti, F. O., & Li, F. (2018). Commercialization of ehealth innovations in the market of the UK healthcare sector: A framework for a sustainable business model. *Psychology & Marketing, 35*, 120–137.

Olsen, R. L., Balachandran, K., Hald, S., Lopez, J. G., Pedersen, J. M., & Stevanovic, M. (2015). *Telecommunication networks. Intelligent monitoring, control, and security of critical infrastructure systems.* Springer67–100.

Omran, E., Grandison, T., & Al Sharhan, S. (2015). *Leveraging cloud services to spark innovation, privacy and security in Kuwait hospitals. 2015 fifth international conference on digital information processing and communications (ICDIPC)*. IEEE65–70.

Omran, E., Grandison, T., Nelson, D., & Bokma, A. (2013). A comparative analysis of chain-based access control and role-based access control in the healthcare domain. *International Journal of Information Security and Privacy (IJISP), 7*, 36–52.

Van de Pas, R., Hill, P. S., Hammonds, R., Ooms, G., Forman, L., Waris, A., et al. (2017). Global health governance in the sustainable development goals: Is it grounded in the right to health? *Global Challenges, 1*, 47–60.

Perera, C., & Chakrabarti, R. (2013). The utility of mhealth in medical imaging. *Journal of Mobile Technology in Medicine, 2*, 4–6.

project, D., http://www.d2rq.org. Freie University, Berlin (15.10.18).

Riaz, M. T., Gutiérrez, J. M., & Pedersen, J. M. (2009). *Strategies for the next generation green ICT infrastructure. 2nd international symposium on applied sciences in biomedical and communication technologies, 2009. ISABEL 2009*. IEEE1–3.

Standard, O., 2005. extensible access control markup language (xacml) version 2.0 (15.10.18).

Standard, O., 2005. Oasis open standards (15.10.18).

Stroetmann, K. A. (2014). *Health system efficiency and ehealth interoperability-how much interoperability do we need? New perspectives in information systems and technologies, Vol. 2*, Springer395–406.

Thakare, V., & Khire, G. (2014). Role of emerging technology for building smart hospital information system. *Procedia Economics and Finance, 11*, 583–588.

Tonelli, A. O., de Souza Bermejo, P. H., Dos Santos, P. A., Zuppo, L., & Zambalde, A. L. (2017). It governance in the public sector: A conceptual model. *Information Systems Frontiers, 19*, 593–610.

Turban, E., Whiteside, J., King, D., & Outland, J. (2017). *Innovative EC systems: From e-government to e-learning, knowledge management, e-health, and c2c commerce. Introduction to electronic commerce and social commerce*. Springer137–163.

Van Gemert-Pijnen, J. E., Nijland, N., van Limburg, M., Ossebaard, H. C., Kelders, S. M., Eysenbach, G., et al. (2011). A holistic framework to improve the uptake and impact of ehealth technologies. *Journal of medical Internet research, 13*.

Wang, Y., Chen, Y., & Benitez-Amado, J. (2015). How information technology influences environmental performance: Empirical evidence from china. *International Journal of Information Management, 35*, 160–170.

WHO (2006). *Building foundations for eHealth: Progress of member states: Report of the WHO global observatory for eHealth*(1st Edition). http://www.who.int/goe/publications.

WHO (2013). *World health survey in Kuwait: Main report – State of Kuwait ministry of health (MOH)* Available from: http://www.moh.gov.kw.

WHO, & ITU (2012). *National e-Health strategy toolkit* (1st Edition). World Health Organization and International Telecommunication Union – WHO publications.

Zhou, L., Varadharajan, V., & Hitchens, M. (2013). Achieving secure role-based access control on encrypted data in cloud storage. *IEEE Transactions on Information Forensics and Security, 8*, 1947–1960.