Reliance on Cryptography of Cloud Computing in Healthcare Information Management, Lessons for Ghana Health Service.

Jonathan Kissi*, Baozhen Dai (PhD)*, Benedicta A.Clemency **, Grace Amoah-Anomah**

*Jiangsu University, School of Management, Department of Health Policy and Management, 301 Xuefu Road, Zhenjiang 212013, China.

**University of Winneba, Center for Distance Education, Winneba-Ghana.

ORCID ID: 0000-0003-2942-5654, 0000-0001-9881-531X, 0000-0003-1079-1291, 0000-0002-7790-250X

Research Paper Received: 20.05.2018 Revised: 10.09.2018 Accepted: 27.09.2018

Abstract - Cloud Computing is considered as the next logical step in emerging technology as a prosperous platform for resource outsourcing, information sharing in Physician-Patient relationship and for research development. The fast drift of Ghana's healthcare facilities into cloud computing for finding treatment to humanity's major illnesses has called for a pragmatic understanding of cloud computing and its areas of security deterrence techniques. Studies in cryptographic discipline of Ghana's healthcare requires a working understanding of the areas of security challengs in cloud computing by Healthcare Administrators, Health Information Officers and their Service Providers. Healthcare data leaked outside to unauthorized users tarnishes the image of the individual, healthcare facility and the Ghanaian populace. This paradigm shift requires a strong and efficient security system among healthcare facilities on their patients data to avoid the erosion of trust. Our review is motivated by these contemporary technologies to explore the adoptions, utilization, identification of areas of security challenges and the provision of adequate security challenges strategies in cloud computing innovations in healthcare. Much emphasis were placed on the following areas: network, interfaces, data, virtualization, legal, compliance and governance, as these are the main areas of security challenges identified when using this innovation. Relevant literatures were discussed to highlight their prominent findings. The contributions presented in this review are relevant in providing a practical understanding and adequate solutions for preventing of security challenges of cloud computing in healthcare and in other disciplines as well.

Keywords- Security; Technology; Cloud; Infrastructures; Healthcare

1 Introduction

The expression "cloud" is an allegory of internet which is being credited to Google's CEO (Eric Schmidt),who was said to have christen this novel Information Technology (IT) service model "cloud computing" at a conference in the year 2006 [1,2]. Cloud computing is deemed as 5th generation information technology architecture. The various narratives of computing began from Mainframes Computers (1970), Client-Server Architecture (1980), Web Services (1990), Service Oriented Architectures (2000) and Cloud Computing (2006 to date) [3,4]. The emergence of this new innovation brought in its wake doubts to many renowned ICT expert's including Richard Stallman (founder, Free Software Foundation) and Larry Ellison (founder, Oracle software) about its use and importance in the current global economy[1,5]. Notwithstanding this, Adueni et al., (2016) and Basu et al., (2012) empathizes that the new cloud computing has gain many market and very constructive in its operations as acknowledge by the users. The fast migration drift of many organisations like healthcare organisations, health insurance organisations, pharmaceuticals and medical research organisations, banking organisations, education institutions etc, into cloud computing calls for a high, strong and dependable cloud system[1,5]. Consequently, the

increasing nature of cloud Customers has resulted in the formation of inter-cloud networks systems among Cloud Service Providers (CSP) [6]. This helps the Cloud Service Provider's recover easily in an event of system hack, data breach, system failure or natural disasters. Apparently, this paradigm calls for strong and efficient security management among cloud service providers and their individual customers in accelerating the erosion of trust in multiple organisations for inter-cloud users [1].

Studies by Kruse, Smith, Vanderlinden & Nealand,(2017) and Acheampong,(2012) elaborates on the progression in technology as an agent for many effective and efficient innovations. These innovations when implemented well will help prevent some causes of morbidity and mortality rate in the Ghana Health Service community and Physician's work will be reduced considerably [7,8]. Studies by Samaras & Samaras, (2016) and Ahuja, Mani and Zambrano (2012) depicts clearly of some healthcare industries such as pharmaceutical and medical research organization using electronic commerce to find solutions to treatment of humanity's major illnesses. This has also motivated patients to test and experience the advantages of this new novelty [9,10].

As elucidated in the works of Adueni et al, (2017), patient care and quality of care has always proved futile in the Ghanaian community [3]. There is no harmonization of the delivery process between healthcare providers in the hospitals and other health centres and even from one region to the other, leaving the patient isolated within the delivery chain [3]. Most health facilities in the country are using standalone Electronic Health Records system (EHR) in their operations [3,11]. The information on patients' healthcare delivery has not been managed well, because the data resides only in that particular point of care [3,8]. The fanaticism of health service practitioners in performing a collative work on patients in a distributed cloud computing environment is lost in the health service delivery operations of GHS. This is due to the absence of a common integrated cloud database platform which can be accessible via World Wide Web not considering the location of the Physician to facilitate such processes [3,8]. In addition this deficiency results in data duplication, delays in referrals, information disintegration, scarcity and inappropriateness of healthcare report [3].

In this review article we will discuss the various services of cloud computing and the contributions of cloud computing in healthcare's provision. Much emphasis will be place on the recognition of security areas of challenges that healthcare institutions in the Ghana Health Service willing to adopt needs to know. This is because the health service information are mainly information of individuals in the society and when not protected well will tarnish the image of the individuals involved especially in cases where chronic diseases like HIV, high fever and mental retardations are involved.

The complicated nature of inter-clouds systems with its interoperability, orchestration designs and models call for consistent security management because the cloud environment is dynamic [10]. Cloud Service Providers can alter the information from the service connection point to be accessed by its cloud system users. This occurs in an event of a system failure or a natural disaster and in such situations, strong agreement must be established between any evolving parties [5,12]. In addition this has highlighted our review to place much emphasis on providing recommendations to the areas of security challenges realised in cloud computing especially in the healthcare service industry. In exploring these occurrences, some extracted examples on extant literature on the use of cloud computing by such industries in health service provision have been discussed.

2 Methodology

We conducted a structured literature review to identify how cloud computing is used in the health service industry with it accompanying importance, the current areas of security challenges and how they can be prevented. Articles used for the review were mainly obtained from Google Scholar as the indexing database, as well as the following electronic journal databases Science Direct, Web of Science, Engineering village, Springer Link and Elsevier.

2.1 Screening and Identification of literature

We classified the search for literature into two broad categories: (i) 'cloud computing adoption in healthcare and its importance (ii) areas of security challenges and deterrence techniques in healthcare settings. An article was included in the research if it satisfied the following criteria: (1) original and peer-reviewed research, (2) qualitative, quantitative or mixed methods research, (3) A research which its content consists of the adoption and importance of cloud computing in healthcare. (4) A research aimed at investigating on the areas that contributes to security challenges and recommended procedures to avert it. We sifted all titles and abstracts for relevant literatures. Studies that were not relevant to the evaluation criteria were discarded while divergent argument were determine by the researchers. Using the inclusion criteria, all articles that did not meet the set criteria were excluded. The Figure 1 depicts the study selection flow process.

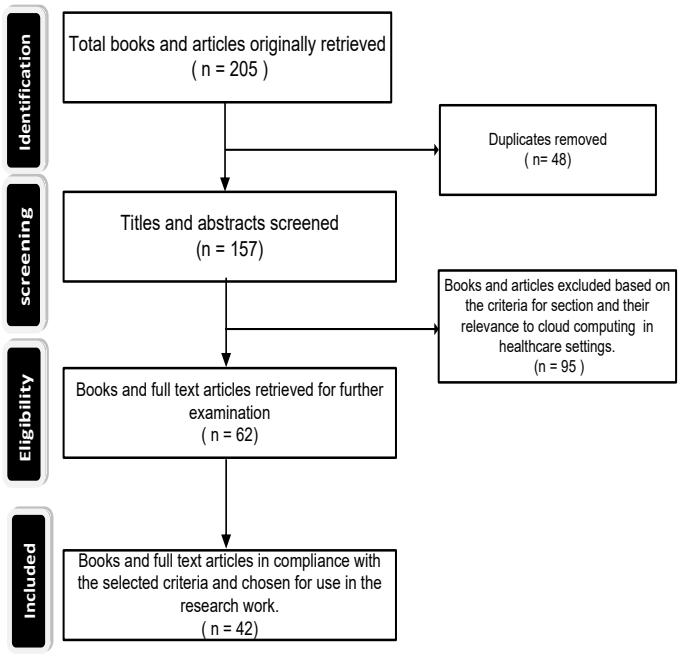

Fig. 1: The process flow of literature search.

2.2 Selection of literatures.

Through the search for literature in the electronic databases above, a total of 205 books and articles were originally retrieved but some literature were in other languages which the researchers were unfamiliar with and rejected them. 157 books and articles were chosen after reading their topics and abstracts in the English language. 62 books and articles were retrieved for further examination. Finally, 42 studies published between 1999 and 2018 met all the inclusion criteria. We concluded on the following statistics for the materials use: 28 (66.67%) on cloud computing in healthcare and its importance, and 14 (33.33%) areas of security challenges and deterrence techniques in healthcare settings. This implies that several works has been undertaken on cloud computing in health service organisations but little has been done on the areas of security challenges and its safeguard techniques necessary for ensuring strong security. This Review therefore focuses much on how to develop the necessary security techniques needed in cloud computing in protecting its data. The table 1.0 shows the classification of articles for the review process.

3 The Concept of Cloud Computing.

The National Institute of Standards and Technology (NIST) describes this concept as a model for enabling convenient, on-demand, ubiquitous, and network access to several pool of configurable computing resources. These resources can be released and rapidly provisioned with nominal management attempt or service provider interaction [12]. These resources may include servers, workstations, networks devices, applications system, storage devices and application services [1]. Under this cloud computing innovations, there is no data centre infrastructure burden to the organisation (healthcare) that generate their data but rather the whole process is largely dependent on Cloud Service Providers (CSP).

The CSP provides services on the demands of their end users. These services are mainly provided via the public internet or private (Virtual Private Network) or by a hybrid network [14]. Studies by some researchers imply that cloud computing model encompasses five indispensable characteristics which include: measured service, on-demand self-service, broad network access, rapid elasticity and resource pooling [15]. - four deployment models which includes public, private, hybrid, and community models (Rami) [16] and three service models [12] .

Table 1.0: classification of articles for the review process.

Categories	Areas	References
Cloud Computing in Healthcare and its importance.	Definitions and components of Cloud Computing	[1,12,13,14,15,16,17,18]
	Application areas of Cloud Computing in Healthcare	[14,19,20,21]
	Precursors of ICT in Healthcare Cloud Computing	[22,23,24,25,26]
	Benefit of Cloud Computing in Healthcare	[4,6,10,13,18,21,26,27]
Areas of security challenges and deterance techiques in using cloud computing in Healthcare	Network Security	[35,36,37]
	Virtualization	[17,34,37]
	Interface	[25,38,39]
	Data Security	[7,9,23,37,39]
	Legal Issues	[37,38,40]
	Compliances	[33,35,37,40]
	Governance	[37,40,41,42]

Each of these services provided by the Cloud Provider runs on different infrastructure platforms. Meanwhile there are three main types of infrastructure platforms. The functions rendered on each platform have been simplified below from the reviews of the following researchers [5,12,17], these include:

3.1 Infrastructure as a Service – (IaaS)

This infrastructure is often managed by the Administrators of the cloud. Their activities are done remotely into the applications using virtual computers, storage device and web servers. The most recognized vendors under this platform include Joyent, GoGrid's Cloud Servers and Amazon EC2.

3.2 Platform as a Service – (PaaS)

This platform is used to manage activities such as database administration, operating system management, web services which are done by expert in teams under the traditional client-server architecture environment. These operations are being performed remotely by cloud services. Among the prominent market leaders under this platform includes Microsoft's Azure, Amazon's web services, Google's App Engine and force.com (salesforce.com). This platform is remotely managed by the Developers.

3.3 Software as a Service – (SaaS)

This platform is patronized by the End-Users of the cloud services. Maintaining and installing of system and application software's are done remotely using the internet on this platform. The platform renders an application functionality that ranges from productivity application like PowerPoint application, picture maker, spreadsheet application, word processing, Google App (Mail, Translator, and Converter etc), Microsoft Office Live, WebEx, Salesforce.com and Yahoo mail etc. to programmes like Enterprise Resource Management (ERM) and Customer Relation Management (CRM).

Fig 2 below shows the collections of Cloud Service Providers.

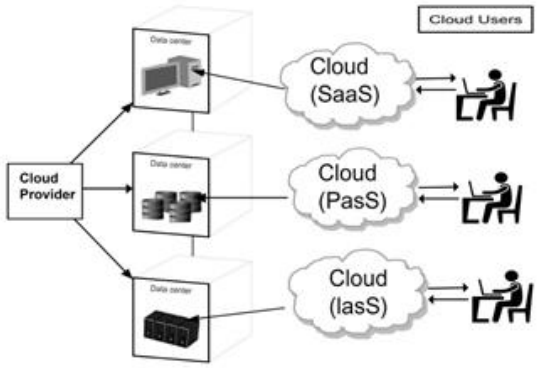

Fig 2: Cloud Service Providers at the various service platforms.

Studies conducted by some researchers shows the four deployment models in the cloud computing to be consisting of:

- Public cloud: The accessibility of the cloud infrastructure is unrestricted to the public and is operated by any firm selling cloud services. [5,12,18].
- Private cloud: The cloud infrastructure is accessible to the requested organization only. It may be managed by an internal or external third party or by the healthcare data management team. [12,14,18].

- Community cloud: This is a private cloud that is collectively used by several customers with similar security features, on it applications and data. [12,14,18].
- Hybrid cloud: This cloud combines several clouds computing model into a hybrid model; it can use the public cloud to host its data and private cloud for data retrieval. [12,14,18].

  The figure below shows the visual models of cloud computing definition

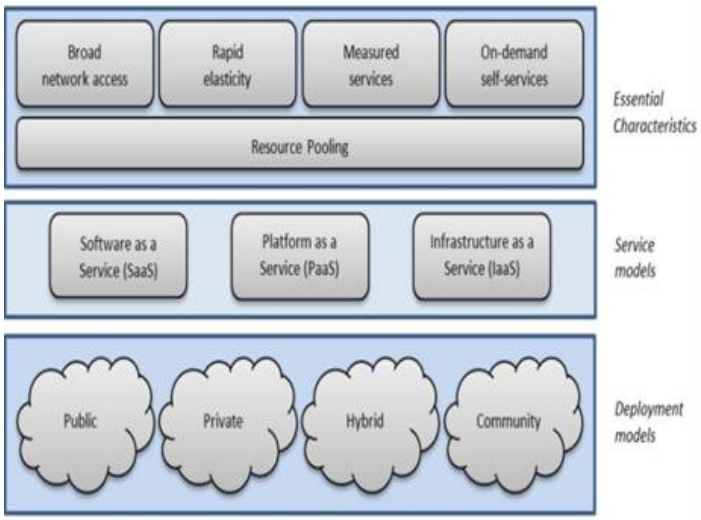

Fig 3: The visual models of cloud computing definition (source: NIST, 2017)

4 Application areas of cloud computing in healthcare organisations

Amron et al., (2017) emphasized that the paucity of healthcare personnel's and resources like healthcare Physicians, Clinicians, Community health workers, Public Health Administrators etc. [19] are being tightened so as to come to terms with the increasing demand by the rising populations [20]. The life growth expectancy of many people have left many advance countries an ageing population which needs medical care at a time when resources are limited [20]. Some researchers states that the current situation is prompting many health providers to look for more contemporary innovation technologies, which will be cost effective [21]. The search and easy of accessibility to medical information solutions to address this growing frightening situation is on the high side [14]. This review shows that cloud computing has the potency in developing solutions required for addressing such economic crisis. A research study by Sultan & Sultan, (2012) portrays that the alarming situation has gingered some advocators of ICT into cloud computing in healthcare. This includes ICT giants like IBM, Microsoft and Google who have invested much in developing cloud medical record services for healthcare provider partners. Large and magnificent data centres have been developed by these precursors of ICT to help fight the underlying economic misfortune [5].

4.1 IBM Version of Cloud Computing in Healthcare

Studies by Sultan, (2011) and IBM, (2011) shows how the healthcare industry is changing towards information centric care delivery model. This is supported by a collaborative workflow of information sharing and cooperation between the patient and their individual medical practitioners.

The cloud computing system is proficient, with the elasticity to respond to the needs and the latest medical breakthroughs [22]. The research works by Yan, Rong, & Zhao, (2009) also supports that services delivered by cloud computing has evolved to broaden a wide variety of healthcare processes and services. The patient will receive safer, convenient, less costly and better care and services [23] because of constant interaction with their medical practitioners. The patients will be nearer to their physician assistants, specialists, pharmacists, care coordinators and nurses regardless of their geographical location for real time service. This will provide a better and core team work among the health facilitators [24].

According to IBM (2011) cloud technology will help collaboration and team-based care delivery of applications based on the clinical information set[23]. This will help transform the available, current and clinical knowledge to support care provider decisions[23,24]. Chadwick & Casenove, (2011) also added their voice that the IBM cloud computing will also help to deliver a comprehensive, integrated and care focused value creation rather than consumption [25]. This implies that the integrated new services on a single platform will be based on a comprehensive and longitudinal view for patients irrespective of where or by whom the care was delivered as enshrined in the studies by Sultan & Sultan, (2012).

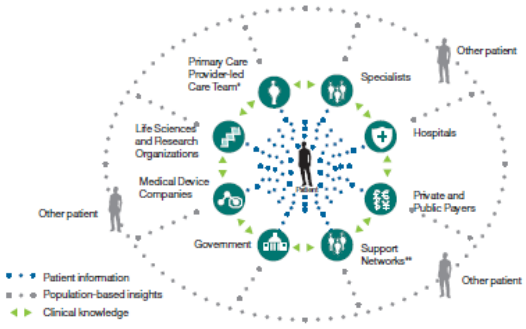

Fig 4 : An example of how cloud could enable healthcare in the future (source: IBM, 2011).

4.2 Dell Version of Cloud Computing in Healthcare

Yan et al., (2009) describes Dell partnership with 'Practice Fusion' a SaaS provider to offer a package for Small to Medium Medical Enterprises (SMMEs) on the cloud-based Electronic Medical Records system [23]. The works of Jain, (2012), highlight that the partnership has attracted EMR systems in United States of America, in many health delivery organizations [24]. The cloud base technology has also infused Obama's administration of Health Information Technology for Economic and Clinical Health (HITECH) Act to move from a paper based system to an automated system [25] and has provided American's citizen with EMR systems.

Sultan & Sultan, (2012) elaborated on the influence of the cloud computing and its usefulness in the Electronic Medical Records system (EMR) [21]. Their study also describes the advent of the cloud computing as a blessing in the National Insurance Authority (NIA) which enables patients to uniformly access their health insurance benefits [1]. In some developed countries like the UK, USA, Australia, the system has reduced the numbers of turnout visits to medical centres because most repeated prescriptions and consultations are done via the internet [21].

4.3 Microsoft and Google Version of Cloud Computing in Healthcare

In a study conducted by Kabachinski (2011), Microsoft has worked in partnership with Kaiser Permanente to enlarge its capability of Microsoft Health Vault applications [26]. Google Health also uses cloud services to get personal health records from Cleveland Clinic's MyChart program [26]. Its main focus is to store health and fitness information in a centralized location and shared easily across healthcare entities including patients [25]. Yan et al.,(2009) recommended that, this partnership will help healthcare organizations and patients to get better access to information and services which will result to improved health outcomes, increased cost savings and reduced medical errors [23].

5 Benefits of Cloud Computing to Health Service Organizations.

Studies by some researchers reveal that cloud computing technology has the propensity of providing several and diverse advantage to the healthcare industry and its stakeholders (Health Administrators/Physicians/ Clinicians), Customers (Patients) and the general healthcare community. Some of these advantages have been shown in this review.

As expounded in the works of Basu et al.(2012) and Williams, et al. (2014), the application of the cloud computing in medical services helps to increase the quality of service for the patients and increase collaboration between Physicians and Clinicians, healthcare organizations as well as healthcare companies like pharmaceuticals and insurance companies [6,27].

Ahuja et al. (2012) also wires the point that the combined approach enables healthcare services to interoperate among them internally and externally. This aids to offer a faster and efficient response which helps to improve the quality of service for Patients through sharing of information across healthcare organizations [10].

As shown in the study conducted by Chen, Paxson, & Katz, (2010), clients' information in clinics, chip centres, hospitals, pharmacies, imaging centres and insurance companies are easily and efficiently shared among the health center. This may include information such as, prescription, test results, patients' medical records, X-rays, physicians' references, referral notes, facilitating insurance approval, physician's availability, scheduling physicians' appointments, etc. These services can be utilized by authorized entities regardless of their physical location [13]. According to Sultan & Sultan (2012), the cloud

architecture has the prospects of providing large data storage location to the health service administrator which will enable them to store all the Clients data. The huge cost on buying internal Severs, higher specification machines and building of datacentre by the health service organisation will cease because of the space provided by the CSP depends on the financial capability of the health service administrators [21]. Cloud computing will assist in minimizing several ICT burdens from the healthcare organisation. All the ICT processes will be migrated to the remote cloud-computing infrastructure where such processes will be performed and stored [4].

Studies by Kabachinski, (2011) shows that the coordination and dissemination of medical process as well as reducing of investment on ICT infrastructure or maintenance costs will be greatly enhanced which will lead to a better healthcare environment [26]. Cloud computing technology will help Healthcare Administrators to deploy their required software onto the cloud and shared among themselves easily in a couple of minutes [27]. Medicals and Insurances bills of clients can also be paid via the internet. Studies by most researchers presuppose that Patients can book appointment on line with their Physicians without necessarily being physically present to form queues and waste precious time at the health facilities. Patients are also being put on monitoring devices and monitored by their Physicians on their health conditions in the comfort of their homes [4,18,21].

6 Cloud computing adoption at London's Chelsea and Westminster Hospital.

Research studies by (N.Sultan, 2014) shows the prototype of healthcare cloud computing as DAKAR. DAKAR(Data Capture and Auto Identification Reference) was the first e-health cloud model in Europe as stated by [1] and its providers were Flexiant an SME software developer. The developers were very instrumental in helping Napier University at Edinburgh (and its partners) in the implementation of UK-funded DAKAR project at the London's Chelsea and Westminster Hospital. The project addresses the most common e-health application requirements such as authentication, data capture, data confidentiality, data integrity, authorization, and audit trail. The DAKAR system runs efficiently on a cloud platform as a service infrastructure that provides the tools for smoothing the progress of the integration, development and deployment of an e-health solution [1,21]. DAKAR runs on the infrastructure as a service platform for its efficiency and has being in operation a number of years.

Williams, Olatunji & Olayinka, (2014) describes DAKAR to consist of three layers; the top layers that consist of a data bucket which holds patients' data and offers long-term persistence. This supports the creation, updating, reading and deletion of patients data [27]. The middle layer which is a Single Point of Contact (SPoC) is used to meet the authorization requirement [21, 27] and the third layer controls the security and confidentiality mechanism for data integrity, confidentiality, reliability and authentication requirements [1,21]. It also consists of a simulator that provides an interface to capture dummy patients' data. Clients who have attended DAKAR hospital ones in their life can spool their data from the DAKAR system via the World Wide Web. Physicians and Clinicians refers to the DAKAR system for continuation of care for both old and new patients and this makes work easier [1,21,27]. Patients can be monitored online by their Physicians to know their health conditions especially diabetics and hypertensive patients and can interact with their physicians daily without going to the hospital through the web portal in the system [1,21,27]. Fig 5 below shows the flow of data in an e-health system at Chelsea and Westminster hospital.

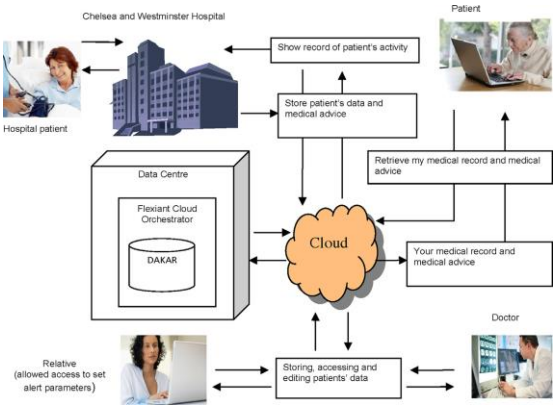

Fig. 5. Data flows in a e-health system at Chelsea and Westminster hospital (Adopted from : Nabil Sultan, 2014)

7 The State of ICT Systems in Ghana

Cline & Haynes, (2001) laments on Information Technologies (IT) prospects for improving healthcare systems in developed and under developed countries and Ghana is not an exception [28]. This can be confirmed in several pilot projects across the developed countries, which can be cited in the works of Sultan & Sultan (2012). The presence of modern equipment in healthcare has attributed to the several initiatives intended at improving the performance of health service professionals, efficiency of healthcare management systems and proper diagnosis to healthcare clients [29].

Ghana as a developing country is in the part of the world where major activities are influenced by ICT to help disseminate information via electronic media[11]. Ghana has patronised ICT innovations for the thirty years in most activities and has several agencies like the Ministry of Communications(MoC),National Communications Authority (NCA), and National Information Technology Agency (NITA), whose functions include but not limited to supervising the general policies of ICT and internet networks use in the country [8].

Studies by Bossert, (2002) elucidate the presence of several private internet service providers in the country. They provide internet services to institutions running online activities [11]. Several of the government activities have been automated and operate under the cloud computing technology infrastructure: The National Health Insurance Scheme (NHIS), National Identification Authority (NIA), Commercial and Rural Banks, Immigration Services, Passport services etc. all operate on the cloud computing environment. This medium helps to disseminate information online to their clients not considering locations [8].

Kowal et al., (2012) explains that the Information and Communication Technology for Accelerated Development (ICTAD) Policy in Ghana is focused on improving the socio-economic status of citizens including their healthcare [29]. Notwithstanding this, is the presence of the Health Sector ICT policy and e-health policy for in the country. The ambition of the e-health plan is to tie together the potential of ICT's to develop the healthcare status of the Ghanaian populace [11].

Admittedly, Achampong (2012), emphasized that despite the high rich benefit in ICT that Ghanaians are currently experiencing, there exist still the absence of a common podium for healthcare information system among the numerous hospitals in the country as elaborated in its ICTAD policy [8].

8 The Healthcare Systems in Ghana (case study)

The Ghanaian populace is about 29,272,464 (0.39% of the total world population)as at January 2018 and with 4 teaching hospitals, 1 university hospital, 9 regional hospitals, 348 community/ urban hospitals, and 5361 chip centers [30,31].

The Ghana Health Service (GHS) is the largest sector under the Ministry of Health (MOH) and is authorized through its Directorates and healthcare facilities to provide rehabilitative, preventive and curative health services [30,31]. It is also to ensure continuous contact and seamless referral system that enables continuity of healthcare services to every Ghanaian [8]. GHS annual reports always indicates the high rate of mortality every year which is ascribed to lack of real live healthcare information sharing among the healthcare professional [3,8] as compared to the developed countries where healthcare information sharing is at its best and the utilizations of technology in healthcare institution is on the mount [8].

The Ghana Health Service Report 2016 showed that although there was a reduced mortality rate from 19.6% to 18% compared to the prior year 2015, it is not statistically satisfactory as elaborated in the ICTAD policy. The constituents for the first top five causes of death were, cerebrovascular accident, pneumonia, septicaemia shock and HIV [30,31]. There were 499 Hospitals and 5361 chip centres and none of these facilities are interconnected for easy sharing of patient data. The independent operational activities of the facilities made the Doctor to population ratio stood 1:8000. These figures indicate that there are more works to be done in the health service sector with the introduction of an integrated cloud based computing technology to lessen the burdens on the Doctors [30,31].

A study by Acheampong, (2012) supports the idea that the expansion of technology has introduce

many effective and efficient technologies which when implemented well, will help prevent the afore-mentioned causes of sickness leading to deaths and Physician's work will reduce proportionately [8].

In addition, the works of Adueni et al, (2016) reveals that, despite the numerous healthcare facilities, patient care and quality of care has always proved ineffective in the Ghanaian community [3]. There are little harmonisations in the delivery process between healthcare providers in the hospitals and Chips centres and even from one region to the other, leaving the patient isolated within the delivery chain [3]. There are also some healthcare facilities in the country using standalone Electronic Health Records system (EHR) in their operations [3,11]. The information on patients' healthcare delivery is inappropriately managed, because the data resides only in that particular point of care [3,8,11]. There are no collaborative works on patients care from one health facility to the other unless under special cases where the patient is referred from the hospital and in such cases, the manual way of referring and caring for patients data are used. Studies by Adueni et al, (2017) communicates that referred patient are sometimes allowed to send their folders to the next point of care[3]. The fanaticism of health service professionals to collectively work on patient in a distributed cloud environment is very limited in the health service operations of the GHS. Occasionally, telephone communications and other social media platforms like whatsapps, facebook, tango, skype are used by Physicians to establish connection between the receiving and referring healthcare facilities [32]. This is due to the nonexistence of a national integrated cloud database platform, which can be accessed through the hypertext transfers protocols and not necessarily considering the site of the Physician to foster such processes [3,8]. Patients transferred from one health facility to another wait in queues before attended to, which demoralise some patients from attending the next facility and restore to over the counter medication [3,8].

The research by Nyanator et al., (1999), also implies that the nonexistence of an integrated national cloud database in the operations of the Ghanaian healthcare industry results in data duplication, delays in referrals, information disintegration, scarcity and inappropriateness of healthcare report [32].

The Health Service report indicates that GHS has the likelihood of enjoying the rich healthcare benefit when it implements an integrated national cloud database system. This will link all the information of healthcare clients in the country unto a common database platform [3]. The information on the system can be accessed by health institutions or by the patients regardless of their location through the internet. This system will give real and live information on each patient health conditions which will aid Physicians to make judgements on patients who have been transferred from one health facility to the other easily [3,8]. There are several importance that Ghana Health Service will gain when it moves its customers (Physician/Patients) data to the clouds and this has been stated explicitly clear in this literature. Notwithstanding this potential benefit of cloud computing, there are some areas of security concerns for the healthcare organisations (GHS) in moving their data to the clouds [33,34] and this has been discussed below with its deterrence solutions in this literature.

9 Areas of Security Challenge's identified and Recommended solutions in Cloud Computing.

As spelt out in the works by Zissis & Lekkas (2012), there exist numerous Cloud Providers with different cryptographic policies. Cryptography is an indispensable technique for protecting information into an unreadable format and later converted back into plain text between any two parties [34]. This strategy is done to prevent malicious attacks or intruders from intercepting the information. CSP compete among themselves with the introduction of strong security controls on their platforms. It therefore calls for integration of common security technologies, protocols and typologies to exist among inter-cloud systems without changing the security authorization, authentication and policy processes [35]. Cloud Customers seek to have a high security technique against their information from the Cloud Providers [36] but the Cloud Customers are unaware of which security managing functions and preferences are needed between the inter-cloud elements [37]. The current dynamic interactions

and coexistence of the varied technologies should be provided [35]. A well-established security management approach has to be built among these inter-cloud systems for their customers to eradicate the erosion of their data leakage [33].

This review work seeks to identify the areas of security challenges in cloud computing and recommends adequate deterrence management solutions to Heath Information Officer's, Cloud Service Providers and their inter-cloud systems. These identified areas of security challenges and recommendation must be scrutinized vigorously and understood well by the Ghana Health Service Administrators before engaging in any Service Level Agreement with their Cloud Service Providers. These areas include:

9.1 Network Security

The security risk regarding the network devices, configurations and network communications have high tendencies of being hacked by intruders. These intruders can be averted by the extension of the healthcare internal networks and access to the customers (Physicians or Patients) by extending the local strategies to resources remotely. Studies by, Jensen et al., (2009), Gonzalez et al., (2011), and Yang & Chen, (2010) shows the various types and available network security threats [35,36,37]. To maintain a trusted network security, our review has proposed these security techniques that ought to be implemented:

To begin with is by firewalling: The prevention of Denial-of-Service (DoS), passive and active attacks in the health service organization should be protected by implementing strong internal firewalls, proxy servers that will intercept messages that leaves and enters the network by hiding the network address, application gateways that will allow only certain applications to run remotely outside the network and packet filters that will agree or deny data based on system defined criteria.

Security configuration: These are configurations performed on high security devices, technologies, systems and protocols in the health service system which guides the system efficiently without causing any compromise to its performance and success.

Virtual Private Network (VPN) mechanisms are needed in shielding the transfer of healthcare information from the attackers' against spoofing, side-channel and sniffing. These activities are done by huge data resource sharing, virtual machines and distributed architecture.

9.2 Virtualization

This consists of protocols for mitigation of virtualized security risks. The protocols may consist of changes in security administration and control, physical security, network security, management, monitoring and logical access. Research studies from Rimal, Choi, & Lumb, (2009), Yang & Chen, (2010) and Zissis & Lekkas, (2012) shows how virtualization occurs [17,34,37]. The following are the strategies this review proposes to be implemented against virtualization:

Firstly, isolation: The idea of isolation is referred to fine-grained assets, like storage, memory and computational resources. All virtual machines and resources allow malicious entities to utilize data leaks.

Secondly, Cross-Virtual Machine attacks: This includes attempts to speeds traffic rates in facilitating the chances of stealing encryption and decryption keys and speeds virtual machine placement attacks.

Last but not the least is, Hypervisor vulnerabilities: The hypervisor is a software component of virtualization, which needs constant and thorough studies to be conversant with the security procedures.

And lastly, Data leakage: Isolation of controls and hypervisor vulnerabilities to seep out information from virtualized infrastructures, acquiring responsive healthcare data and impacting negatively on the integrity and confidentiality of the data.

9.3 Interfaces

This elaborates on potentate matters concerning the administrative interfaces, user interfaces, and application programming interfaces for controlling and using the clouds environment by the health service industry. Studies from Chadwick & Casenove, (2011), Han, (2011), and Haufe &

Colomo-palacios, (2016), shows the various interfaces [25,38,39] . This can be address by identifying the following:

First and foremost, administrative interface: This interface allows recourses to be controlled remotely in the various service levels. This may include the handling of application tools like, access control and configuration on (Saas), coding, development, testing and deployment on (Paas) and virtual management on the (Iaas).

In addition is user interface: This interface provides both the Developers and End-Users of cloud system the necessary methods to interact and adapt to strategies that protects the system.

Lastly, Application Programming Interfaces: This interface is employed for accessing virtualized processes, systems, devices and resources from the cloud. It is mostly performed on the (Iaas) and (Paas) platforms.

9.4 Data Security

The fortification of Customers (Physicians and Patients) data from active and passive attacks, from illegal access, annihilation and unwanted interruption through controlling the data's integrity, availability and confidentiality calls for a strong data security protection system. The research works by Yan et al., (2009), Samaras & Samaras, (2016), Haufe & Colomo-palacios, (2016) Kruse, Smith, Vanderlinden, & Nealand, (2017) and Yang & Chen, (2010) shows the consequences of data breach [7,9,23,37,39]. Our review seeks to propose the following mechanisms that ought to be implemented to prevent the data security breach in cloud computing:

To begin with is cryptography: This involves the exchanging of encryption and decryption keys required by state, industry and federation.

Secondly, disposal: The complete annihilation of data, including log references, deletion and hiding of backup registries from present locations are essential in clod environment.

Lastly, redundancy: Information technology core processes and functions are used to avoid data loss.

9.5 Legal Issues

Healthcare data transmitted to the cloud can easily be accessed by both active and passive attacks through the hypertext transfer protocol links. The healthcare organization data becomes open to the public based on the cloud architecture modules. Attacks can invade from any geographical location. Studies by Nicanfar et al., (2016), Han, (2011) and Yang & Chen, (2010), shows the relative judicial legislation and law [37,38,40]. Our studies seek to propose the following that ought to be comprehensively followed. This may include

Firstly, legislation: Juridical and law enforcement matters connected to new concepts in cloud computing as introduced and in line with the catchment areas laws.

Secondly, data location: Healthcare Customer (Physicians and Patients) data are held in several catchment locations depending on how the geographic locations are affected, directly or indirectly, or by subpoena law-enforcement processes.

Thirdly, E-discovery: Different law-enforcement measures exist in different geographical locations. Data disclosure and confiscation of hardware devices are crucial during data investigation.

9.6 Compliance

Health service organizations need to guarantee the security, confidentiality and integrity of their (Physicians and Patients) data in the cloud. The CSP have to conform to the security standards regardless of the geographical location of their applications systems, services and data. Research studies by Brodkin, (2008), Brandic et al., (2010), Nicanfar et al., (2016) and Yang & Chen, (2010), seeks to show that the following standards must be mutually agreed by both healthcare Administrators and the Service Providers that provide the services [33,35,37,40]:

To start with is service conformity: The contractual responsibility and service requirements are to be delivered by the Service Providers based upon on their basic service and customer needs of the health service Administrators.

Secondly, Service Level Agreements (SLA): The mutual agreement that should exist between

Healthcare Administrators and Service Providers to guarantee the basic security policies, procedures and guidelines of services are adhered to.

Moreover is Systems Audit: System audit should be holistically and vigorously performed among the Service Providers and their customers (Healthcare Administrators). This will ensure effective and efficient service delivery. The Customers should be allowed to verify the security and availability assessments on all their services. Independent, efficient and transparent strategies are necessary for service conditions analysis.

Lastly is Loss of Service: An all-inclusive risk management systems, disaster recovery plans and policy recommendations should be implemented to recover the healthcare organization from being hacked in an event a disaster occurs. Routine disaster recovery drills and testing should be very vital among health service organizations.

9.7 Governance

The authorization and execution of security control tools and techniques bestowed by the health service organization is to check that only authorized users have privilege right and grant to the information and applications. Risk of exposure to the healthcare data and network are high when hosted in the public clouds. From the works of Sadeghi, Schneider, & Winandy, (2010), Pearson, (2009), Nicanfar et al., (2016) and Yang & Chen, (2010) [37,40,41,42], our review shows that access rights ought to be carefully assigned to authorize users and periodic review should be carried on them. This could be achieved through:

Data control: secure and relevant data security protocols and configurations are to be strictly emphasized because moving data to the cloud implies losing direct control over data files, data redundancy and file systems.

Security control: insufficient documentation and clarity, misunderstanding of procedures and standards on (SLA) leads to security gaps. This creates loss of governance over guidelines, procedures and security policies to be guided by.

10 Conclusion

A protected cloud computing environment depends on several security solutions working harmoniously together. Security of the cloud infrastructure lies on suitable cryptography and trusted cloud techniques that have been employed by the CSP. Healthcare Administrators (Ghana Health Service) should not lose sight of cloud securities by virtue of the rich benefit that it provides. The current review identifies the following as benefits associated with cloud computing; reduced cost, scalability, flexibility, availability, health information sharing, remote monitoring and a platform for research and development. Healthcare organisations ought not to lose control over their data after sending them to CSP for migration to the clouds. The protocols, standards and format directly affecting the attempts to migrate different service providers with their SLA's must to be complied with.

Our review work has emphatically highlighted on several areas of security challenges and policies that should be implemented to safeguard the information asset in the healthcare organisation when moving data to the cloud. It can be iterated that the health information of an individual leaked outside to unauthorized users tarnishes the image of such individual and the healthcare facility. This review work has also focused on several security threats areas in cloud computing as a guide for healthcare organisation willing to adopt its use (Ghana Health Service). These included the securities areas of concerns that if mishandled can cause more impairment to the cloud system like: network security, interfaces, data security, virtualization, legal issues, compliance and governance while providing adequate prevention solution to such areas identified.

For the trust of clients to be maintained in health service organizations, security should be considered as indispensable part of the cloud computing system. It is the considered view of this review that GHS adopts the private cloud service model solely for its operations. Private cloud service model will brace the security, privacy and promote efficient service delivery. Moreover, the identity management, reporting of security incidents and access controls of the cloud service providers should be evaluated well before

healthcare administrators select a cloud service provider for their services. In addition, the consistent and continuous use of ICT in the operations of GHS should be enforced in all health facilities to increase the quality of care and professionalism in a service delivery chain. Furthermore, a shared integrated platform should also be created to fortify the existing collaboration workforce among the Physicians, Patients and the health service facilities. This will aid in sharing computing resources and health care resources more easily and very quick.

In contrast, our current studies did not consider much on the interoperability devices that ought to be used by the CSP and the legal implication on the breach of the SLA's between the parties involved. This review recommends further studies that tackle the above stated areas of concerns in protecting data of clients in other disciplines.

Funding information

This work was funded by National Nature Science Foundation of China (71774069), 2014 "Six Talent Peaks" Project of Jiangsu Province (2014-JY-004).

References

[1] Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information Management*, *34*(2), 177–184. https://doi.org/10.1016/j.ijinfomgt.2013.12.011

[2] Regalado, A. 2010, "Who coined the term 'Cloud Computing'?", *The Business Technology Forum*, http://www.thebusinesstechnologyforum.com/2011/10/who-coined-the-term-cloud-computing/ (Accessed on: 4 December, 2017).

[3] Isaac Akuamoah-Boateng Adueni, J. B. Hayfron-Acquah, J. K. P. (2016). Developing a Common Cloud Platform to Manage Ghana ' s Healthcare System . Case Study of Ghana Health Service (GHS). Journal of Communications Technology, Electronics and Computer Science, Issue 4, 2016 ISSN 2457-905X, 4(4), 6–10.

[4] Al-Rashedi, A. A. (2014). E-Government Based on Cloud Computing and Service- Oriented Architecture. *International Journal of Computer and Electrical Engineering*, *6*(3), 201–206. https://doi.org/10.7763/IJCEE.2014.V6.822

[5] Sultan, N. A. (2011). Reaching for the "cloud": How SMEs can manage. *International Journal of Information Management*, *31*(3), 272–278. https://doi.org/10.1016/j.ijinfomgt.2010.08.001

[6] Basu, S., Andrews, J., Kishore, S., Panjabi, R., & Stuckler, D. (2012). Comparative performance of private and public healthcare systems in low- and middle-income countries: A systematic review. *PLoS Medicine*, *9*(6), 19. https://doi.org/10.1371/journal.pmed.1001244

[7] Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security Techniques for the Electronic Health Records. https://doi.org/10.1007/s10916-017-0778-4

[8] Achampong, E. K. (2012). The State of Information and Communication Technology and Health Informatics in Ghana. Online Journal of Public Health Informatics, 4(2), 1–13. https://doi.org/10.5210/ojphi.v4i2.4191

[9] Samaras, E. A., & Samaras, G. M. (2016). Confronting systemic challenges in interoperable medical device safety, security & usability. *Journal of Biomedical Informatics*, *63*, 226–234. https://doi.org/10.1016/j.jbi.2016.08.024

[10] Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A Survey of the State of Cloud Computing in Healthcare. *Network and Communication Technologies*, *1*(2), 12–19. https://doi.org/10.5539/nct.v1n2p12

[11] Bossert, T. J. (2002). Decentralization of health systems in Ghana, Zambia, Uganda and the Philippines: a comparative analysis of decision space. *Health Policy and Planning*, *17*(1), 14–31. https://doi.org/10.1093/heapol/17.1.14

[12] Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology, Information Technology Laboratory*, *145*, 7. https://doi.org/10.1136/emj.2010.096966

[13] Katz, R., Goldstein P. & Yanosky. R. 2010. "Cloud Computing in Higher". http://net.educause.edu/section_params/conf/CCW10/higherd.pdf.

[14] Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud computing: A survey. *Journal of Cloud Computing*, *1*(1), 1–18. https://doi.org/10.1186/2192-113X-1-19

[15] Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2017). Current State of Cloud Computing Adoption - An Empirical Study in Major Public Sector Organizations of Saudi Arabia (KSA). *Procedia Computer Science*, *110*, 378–385. https://doi.org/10.1016/j.procs.2017.06.080.

[16] Ramireddy, S., Raghu, T. S., Chakraborthy, R., & Rao, H. R. (2010). Privacy and Security Practices in the Arena of Cloud Computing.

[17] Kissi, J., Dai, B., Boamah, K. K. B., Owusu-Marfo, J., & Asare, I. (2018). Integrated Cloud Based Platform for

Managıng Employees Pensıon Schemes; Case of Ghana. *Australian Journal of Economics and Management Sciences*, *8*(1).

[18] West, B. C. (2014). Factors that Influence Application Migration to Cloud Computing in Government Organizations: a Conjoint Approach, 1–90. Retrieved from http://scholarworks.gsu.edu/bus_admin_diss/40

[19] Amron, M. T., Ibrahim, R., & Chuprat, S. (2017). A Review on Cloud Computing Acceptance Factors. *Procedia Computer Science*, *124*, 639–646. https://doi.org/10.1016/j.procs.2017.12.200

[20] Abouelmehdi, K., Beni-hssane, A., Khaloufi, H., & Nationale, E. (2017). ScienceDirect Big data security and privacy in healthcare : A Review Big data security and privacy in healthcare:*Procedia Computer Science*, *113*, 73–80. https://doi.org/10.1016/j.procs.2017.08.292.

[21] Sultan, N., & Sultan, Z. (2012). The application of utility ICT in healthcare management and life science research: A new market for a disruptive innovation. *The European Academy of Management Conference EURAM*, (JUNE 2012), 6–8.

[22] Marketing, C. (2011). Cloud Computing : Building a New Foundation for Healthcare. *White Paper*, 12. Retrieved from http://www-05.ibm.com/de/healthcare/literature/cloud-new-foundation-for-hv.pdf

[23] Yan, L., Rong, C., & Zhao, G. (2009). Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based. *Cloud Computing*, *5931*, 167–177. https://doi.org/10.1007/978-3-642-10665-1_15

[24] Jain, P. (2012). Security Issues and their Solution in Cloud Computing. *International Journal of Computing & Business Research ISSN (Online*, 2229–6166.

[25] Chadwick, D. W., & Casenove, M. (2011). Security APIs for my private cloud: Granting access to anyone, from anywhere at any time. *Proceedings - 2011 3rd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2011*, 792–798. https://doi.org/10.1109/CloudCom.2011.122

[26] Kabachinski, J. (2011). What's the forecast for cloud computing in healthcare? *Biomedical Instrumentation and Technology*, *45*(2), 146–150. https://doi.org/10.2345/0899-8205-45.2.146

[27] Williams, S. O., Olatunji, O. M., & Olayinka, O. O. (2014). Cloud Based Framework for Efficient Management of Research Data, 1–6

[28] Cline, R. J., & Haynes, K. M. (2001). Consumer health information seeking on the Internet: the state of the art. *Health Education Research*, *16*(6), 671–692. https://doi.org/10.1093/her/16.6.671

[29] Kowal, P., Chatterji, S., Naidoo, N., Biritwum, R., Fan, W., Ridaura, R. L., … Newell, M. L. (2012). Data resource profile: The world health organization study on global ageing and adult health (SAGE). *International Journal of Epidemiology*, *41*(6), 1639–1649. https://doi.org/10.1093/ije/dys210

[30] Ghana Health Service 2016 Annual Report, (June, 2017).

[31] District Health Information Management System, 2018.

[32] Nyanator, F., Kutzin, J., & Nyonator, F. (1999). Health for some? The effects of user fees in the Volta Region of Ghana. *Health Policy and Planning*, *14*(4), 329–341.

[33] Brandic, I., Dustdar, S., Anstett, T., Schumm, D., Leymann, F., & Konrad, R. (2010). Compliant Cloud Computing (C3): Architecture and language support for user-driven compliance management in Clouds. *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, (i), 244–251. https://doi.org/10.1109/CLOUD.2010.42

[34] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

[35] Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. Lo. (2009). On technical security issues in cloud computing. *CLOUD 2009 - 2009 IEEE International Conference on Cloud Computing*, 109–116. https://doi.org/10.1109/CLOUD.2009.60

[36] Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M., Naslund, M., & Pourzandi, M. (2011). A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing. *2011 IEEE Third International Conference on Cloud Computing Technology and Science*,231–238. https://doi.org/10.1109/CloudCom.2011.39.

[37] Jadeja, Y., & Modi, K. (2012). Cloud computing - Concepts, architecture and challenges. *2012 International Conference on Computing, Electronics and Electrical Technologies, ICCEET 2012*,877–880. https://doi.org/10.1109/ICCEET.2012.6203873

[38] Han, Y. (2011). Cloud Computing: Case Studies and Total Costs of Ownership. *Information Technology & Libraries*, *30*(December), 198–206. https://doi.org/Article

[39] Haufe, K., & Colomo-palacios, R. (2016). Security Management Standards : A Mapping. *Procedia - Procedia Computer Science*, *100*(1877),755–761. https://doi.org/10.1016/j.procs.2016.09.221

[40] Nicanfar, H., Liu, Q., TalebiFard, P., Cai, W., Leung, V. C. M., Mello, F. L. De, Alliance, C. S. (2016). State-of-The-Art of cloud computing cyber-security. *Proceedings of 2015 IEEE World Conference on Complex Systems, WCCS*

2015, *3*(4),0–176. https://doi.org/10.1109/ICoCS.2015.7483283

[41] Sadeghi, A. R., Schneider, T., & Winandy, M. (2010). Token-based cloud computing: Secure outsourcing of data and arbitrary computations with lower latency. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6101 LNCS*, 417–429. https://doi.org/10.1007/978-3-642-13869-0_30

[42] Pearson, S. (2009). Taking Account of Privacy when Designing Cloud Computing Services 2 . Why is it important to take privacy into. *Challenges of Cloud Computing, 2009. CLOUD'*,44–52. https://doi.org/10.1109/CLOUD.2009.5071532