Guidelines for Secure Cloud-Based Personal Health Records

Avuya Mxoli
Nelson Mandela University Port Elizabeth, Eastern Cape, Council for Scientific and Industrial Research, Gauteng, Pretoria
Email: amxoli@csir.co.za

Nicky Mostert
Nelson Mandela University, Port Elizabeth, Eastern Cape
Email: nicky.mostert-phipps@mandela.ac.za

Mariana Gerber
Nelson Mandela University, Port Elizabeth, Eastern Cape
Email: mariana.gerber@mandela.ac.za

Abstract— **Traditionally, health records have been stored in paper folders at the physician's consulting rooms – or at the patient's home. With the rise of technology there have been many offerings of ways to store health records in a safer and better way by using Personal Health Records (PHRs). Web-based PHRs are stored in various ways including the use of Cloud computing. This brings numerous benefits including accessibility and efficiency but there are also privacy and security concerns. This paper proposes guidelines that can assist PHR providers in choosing a Cloud Service Provider that will store PHRs in a secure manner.**

I. Introduction

A PERSONAL HEALTH RECORD (PHR) is a tool, usually web-based, that allows individuals to capture, share, store and process their medical records in one central place [1]–[3]. The PHR is typically owned, created and managed by the individual; and it allows him to have a life-long summary of all of his health information in one convenient place. Such a system allows individuals to better manage their health; and it is especially useful for individuals with chronic conditions, such as diabetes and hypertension, or with diseases such as cancer, tuberculosis or HIV/AIDS [4].

A PHR typically allows an individual to record information on past and current illnesses, allergies, immunisations, medication, procedures, test results and more [5], [6].

Individuals are able to provide their healthcare provider with a detailed summary of their medical history gained from their PHRs. This often accelerates the diagnosis process and ultimately the healing process.

As PHRs are web-based, there are numerous ways in which the data can be stored on the internet; and cloud computing is one of them [7]. Cloud computing can succinctly be defined as a broad array of pay-as-you-go applications delivered as a service over the internet, as well as the hardware and software used in the various data centres that provide such services [8], [9].

Because of the various advantages associated with cloud computing, PHR providers are increasingly leaning towards using the cloud as their storage facility [10].

Due to security and privacy issues associated with cloud computing, PHRs stored in the cloud are exposed to increased risks increased risks [11]. The data stored in a PHR can typically be divided into two categories, namely: personally identifiable information (PII) and healthcare data. PII consists of information that can be used to identify, locate or contact an individual, e.g. name, address, telephone number, etc. Healthcare data are composed of medical files about the individual, such as scans, X-rays, and other types of medical images and videos [12]. This type of information is highly sensitive and should be treated as such.

Providers of products and services via cloud computing facilities should therefore be provided with information that would assist them to choose a cloud service provider (CSP) that is secure and trustworthy. There is a lack of guidance to assist PHR providers in making an informed choice when selecting a CSP, to ensure that their customers' data are kept private and secure. The primary objective of this research project is thus to propose guidelines to assist PHR providers in making an informed choice when selecting a CSP to ensure that their customers' data remain private and secure.

II. Methods

A systematic literature review was conducted to identify security and privacy risks of which PHR providers should be aware of when storing data in the cloud. A subsequent systematic literature review identified control measures that could be used to mitigate the identified risks. This assisted the researcher to develop appropriate guidelines.

Guidelines for secure cloud-based PHRs were formulated, based on the identified security and privacy risks, as well as the control measures that could be taken to manage these risks. The formulation of these guidelines employed argumentation and reasoning, based on the results of the systematic literature review. Elite interviews were also conducted, in order to further refine and validate the guidelines.

The elite interviews focused on the quality, utility, and the efficacy of the guidelines for secure cloud-based PHRs. The evaluation of quality, utility and efficacy are in line with recommendations from Hevner, March, Park, and Ram (in [13]. The authors state that utility is based on the usefulness, simplicity, understanding and practical usage of an artifact. Quality is based on evaluating whether the artifact is presented in a satisfactory manner. Finally, efficacy focuses on determining whether the artifact adopted will meet the required standard. The aspects raised during the interviews

were addressed and incorporated to finalize the risks and guidelines, as presented in this manuscript.

III. RESULTS

The following privacy and security risks which PHR providers should be aware of when storing data in the cloud were identified through the literature review: [11], [14]–[26]:

- Malicious insiders
- Third-party access
- Multi-tenancy
- Software intrusions
- Physical intrusions
- Poor encryption key management
- Temporary outages
- Prolonged and permanent outages
- Data lock-in
- Denial of Service (DoS)

In the sections that follow, guidelines to assist PHR providers in making an informed choice when selecting a CSP to ensure that their customers' data remain private and secure are presented. The information security risks relating to cloud-based PHRs, as well as the control measures that could be used to mitigate the identified risks are presented. Based on the identified risks and control measures from the ISO 27799:2008, ISO 27017:2015 and ISO 17090:2008 standards, guidelines were developed and validated through elite interviews, in order to assist PHR providers in making an informed choice when selecting a CSP to ensure that their customers' data remains private and secure.

A. *Guideline: Control Access to PHR Data*

Risk addressed: Malicious insiders
Control measures:

- Access control policy (7.8.1.2)*
- Access to Networks and Network Services (9.1.2) $
- Roles and responsibilities; Screening; terms and conditions of employment (7.5.1)*
- Management responsibilities: Information security awareness, education and training; Disciplinary process (7.5.2)*
- Terminating responsibilities and return of assets; Removal of access rights (7.5.3)*
- Audit logging (7.7.10.2) *
- Protection of log information (7.7.10.4)*
- User registration and deregistration (9.2.1) $
- Information access restriction (9.4.1) $

Source: [14]

B. *Guideline: Assess risk involved with third parties*

Risk addressed: Third-party access
Control measures:

- Assessment of risks related to external parties (7.3.3.1)*
- Addressing security in third-party agreements (7.3.3.3)*
- User access provisioning (9.2.2) $
- Management of privileged access rights (9.2.3) $
- Health information exchange policies, and procedures and exchange agreements (7.7.8.1)*

Source: [19], [22]

C. *Guideline: Separate customer data*

Risk addressed: Multi-tenancy
Control measures:

- Separation of development, test and operational facilities (7.7.1.4)*, (12.1.4) $
- Segregation in networks (13.1.3) $

Source: [20], [22]

D. *Guideline: Prevent malicious code infections*

Risk addressed: Software intrusions
Control measures:

- Controls against malicious code (7.7.4.1)*
- Controls against malware (12.2.1) $

Source: [21], [23]

E. *Guideline: Store PHR data in secure data centres*

Risk addressed: Physical intrusion
Control measures:

- Physical security perimeter (7.6.1.1)*, (11.1.1) $
- Physical entry controls (11.1.2) $

Source: [24]

F. *Guideline: Adopt strong private key management techniques*

Risk addressed: Poor encryption key management
Control measures:

- Policy on use of cryptographic controls (10.1.1) $
- Key management (10.1.2) $
- Private key backup (7.6.2.5) #
- Method of destroying private key (7.6.2.11) #
- Avoid loss, disclosure or unauthorised use of private keys. If any occurs, report immediately (7.9.6.4) #

Source: [11], [27]

G. *Guideline: Ensure business continuity*

Risk addressed: Temporary outages
Control measures:

- Security of network services (7.7.6.2)*
- Alignment of security management for virtual and physical networks (CLD.13.1.4) $
- Administrator's operational security (CLD.12.1.5) $

Source: [11], [15], [28]

H. Guideline: Backup and encrypt PHR data

Risk addressed: Prolonged and permanent outages
Control measures:

- Health information backup (7.7.5)*
- Information backup (12.3.1) $

Source: [16]

I. Guideline: Enforce technical interoperability

Risk addressed: Data lock-in
Control measures:

- Compliance with security policies, standards and technical compliance (7.12.3)*

Source: [17], [18]

J. Guideline: Respond to information security incidents

Risk addressed: Denial of Service (DoS)
Control measures:

- Reporting information security events and weaknesses (7.10.1)*, (16.1.2)$
- Responding to information security incidents (16.1.5) $

Source: [11], [17], [22]

* denotes the use of the ISO 27799:2008 standard
$ denotes the use of the ISO 27017:2015 standard
# denotes the use of the ISO 17090:2008 standard

IV. DISCUSSION

The sections that follow describe the aspects that PHR providers should look for when selecting a CSP to ensure that their customers' data remains private and secure.

A. Control Access to PHR Data

The malicious insider threat is very common in the cloud environment; and there is usually a lack of transparency on the hiring process of the CSP. There is no clarity on their hiring standards and practices; and this creates an opportunity for an opponent to gain access to sensitive information [14]. The main guideline that has been identified to limit this risk is to control access to PHR data, which implies that the PHR provider should ensure that the CSP adheres to the following:

- In order to govern access to personal health information, an access control policy should be in place. It should be predefined, according to the roles with associated authorities, which are consistent, but limited to the needs of that particular role (7.8.1.2)*.
- Prior to employment, staff members should be given roles and responsibilities in the job description. A screening process should also be conducted to verify identity, living address, previous employment, as well as the terms and conditions of employment (7.5.1)*.
- During employment, staff members should be assigned responsibilities, offered information security awareness and training, and be informed of the disciplinary process (7.5.2)*.
- Upon termination or change of employment, access rights must be revoked (7.5.3)*.
- Systems that process personal health information should create a secure audit record every time a user accesses, creates, updates or archives personal health information via the system (7.7.10.2)*.
- Audit logs shall be secure and tamper-proof. The access to system audit tools and audit trails shall be secure to prevent misuse or compromise (7.7.10.4)*.
- The CSP should provide user registration and deregistration functions for the customers of the PHR provider. The specifications of how these functions work should also be provided to the PHR provider (9.2.1) $.
- The CSP should provide access controls that allow PHR providers to restrict access to their cloud services, their cloud service functions and the PHR provider's data maintained in the service (9.4.1) $.

The control below states what the PHR provider should do:

- The PHR provider's access control policy, which provides guidance on the use of network services, should specify the requirements for user access to each separate cloud service that is provided by the CSP (9.1.2) $.

Implementing this guideline would ensure that the confidentiality of a PHR is preserved. Employees of the CSP would be governed by a control policy that would clearly state the role of each employee and the type of access he/she has. This would also protect the integrity of the data, because any employee who makes changes to the data without having the proper access rights would be held liable. Employees who are no longer with the CSP should have their access rights revoked; so as to prevent them from tampering with the availability, auditability and privacy of the PHR data.

B. Assess the Risks Involved With Third Parties

Adding more administrators to cloud systems increases the risk of unauthorised access [29]. Third parties may pose a threat to the users of cloud services if they aim to use in a negative way the access that the CSP has granted them. Other risks involved with third parties include maintaining data confidentiality and integrity [19]. The guideline that has been identified to limit this risk is to assess the risks involved with third parties, which implies that the PHR provider should ensure that the CSP adheres to the following:

- Conduct a risk assessment to weigh the risks that may be brought by third parties to the systems and the data. Security controls must subsequently be

implemented, according to the identified level of risk and to the technologies used (7.3.3.1)*.

- When a third party is granted access to process personal health information, there must be formal contracts that specify the confidential nature and value of the personal health information; the security measures that must be implemented and complied with; limitations to access these services by third parties; and the penalty that would apply – should any of these security measures be breached (7.3.3.3)*.
- Support third-party identity and access management technologies for the cloud services and associated administration interfaces (9.2.2) [$].
- Provide sufficient authentication techniques for authenticating the PHR provider's administrators to the administrative capabilities of a cloud service, according to the identified risks (e.g. enable the use of third-party multi-factor authentication mechanisms) (9.2.3) [$].
- Information exchange agreements that specify the minimum set of controls to be implemented must also be formulated (7.7.8.1)*.

Third parties that have access to PHR data can be controlled in terms of the risks they could impose, should they perform malicious acts. The confidentiality, integrity, availability, auditability and privacy of PHRs can be maintained; if the risks that come with third parties are well-assessed and managed in time.

C. Separate Customer Data

The lack of compartmentalisation of resources in cloud computing allows users to access other users' personal information [20]. Multi-tenancy also makes it difficult to monitor and log the processes of virtual machines in the cloud [29]. The guideline that has been identified to deal with this risk is to separate customer data. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Development, testing and operational environments should be separated physically or virtually so as to reduce the risks of unauthorized access or changes to the operational environment (7.7.1.4)*, (12.1.4) [$].

In addition to this, the PHR provider should:

- Define its requirements for the segregation of networks in order to achieve tenant isolation in the shared environment of a cloud service, and to ensure that the CSP meets these requirements (13.1.3) [$].

In order for PHRs to have confidentiality, integrity, availability and privacy, customer data should be separated.

D. Prevent Malicious Code Infections

It is difficult to eliminate software intrusions in the cloud; and this raises concerns for prospective cloud customers. Malware also compromises the integrity of software in the cloud; because it can modify the victim's software somehow [21]. The guideline that has been identified to deal with this risk is to prevent malicious code infections. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Proper prevention, detection and response controls that are used to protect systems against malicious software must be adopted; and appropriate user awareness and training must be implemented (7.7.4.1)*.
- Detection, prevention and recovery controls to protect against malware should be implemented, in conjunction with the appropriate user awareness (12.2.1) [$].

When PHRs are protected from software intrusions by preventing, detecting and properly responding to malicious code infections, the confidentiality, availability and privacy of PHRs would be preserved.

E. Store PHR Data in Secure Data Centers

The data centres that CSPs use to store the PHR data may be at risk of being attacked physically through the risk of physical intrusion, which would result in hardware theft, unauthorised access to servers, or the loss of access to data [24]. The guideline that has been identified to limit this risk is to store the PHR data in secure data centres. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Security perimeters should be defined and used to protect areas that contain information that is either sensitive or critical (11.1.1) [$]. There should be physical entry controls; offices should be secured; there should be protection against external and environmental threats; and public access, delivery and loading areas should be secure enough to prevent the loss of personal health information. These are all ways to prevent the public from getting too close to IT equipment. Software or equipment used to support a healthcare application that contains personal health information should not be removed from the site, or relocated within the organization – without authorized permission from the organization (7.6.1.1)*.
- Secure areas should be protected by appropriate entry controls, to ensure that only people with authorized access are allowed entry (11.1.2) [$].

The confidentiality, integrity, availability and privacy of PHRs would be protected if the data centres used to store PHR data are kept secure from external and environmental threats.

F. Adopt Strong Private Key Management Techniques

Some systems allow users to generate their own decryption keys, and to distribute them to authorised parties [11]. This may lead to poor encryption key management; since it becomes a challenge if the user loses the keys or discloses

them to malicious parties [25]. For the purpose of the identified control measures, encryption keys are – from this point onwards – referred to as private keys; and the party responsible for keeping the keys is known as the certificate holder. The guideline that has been identified to deal with this risk is to adopt strong private key management techniques. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Provide information to the PHR provider on the circumstances in which it uses cryptography to protect the information it processes. The CSP should also let the PHR provider know whether it can offer them any capabilities that allow the PHR provider to perform its own cryptographic protection (10.1.1) [$].
- It is recommended that the certificate holder creates a backup of the private keys, where possible. This backup would be held in the environment of the certificate holder; and it would be entirely in his/her control (7.6.2.5) [#].
- When the private key is no longer in use, all its copies in computer memory and shared disk space must be securely destroyed by overwriting multiple times (7.6.2.11) [#].
- A certificate holder must ensure that he/she makes every effort to avoid the loss, disclosure or unauthorized use of the private keys. If there is any actual or suspected loss, disclosure or other compromise of the private key, the certificate holder must immediately notify the certification authority (7.9.6.4) [#].

In addition to the controls above, the PHR provider should:

- Not allow the CSP to store and manage the encryption keys for cryptographic operations, when it uses its own key management, or a separate distinct key management service (10.1.2) [$].

When encryption keys are managed and disposed of properly, the confidentiality, availability and privacy of PHR data can be ensured.

G.Ensure Business Continuity

It is vital that systems that process health information in the cloud should be available continuously without any interruptions [11]. Outages are not exclusive to cloud environments; but they are prominent there because of the interconnectedness of their services [30]. A temporary outage could be caused by a natural disaster, vulnerability exploits and deliberate attacks [15]. Health organisations recognise business continuity management as a requirement; and this includes disaster recovery [31]. The guideline that has been identified to limit this risk is to ensure business continuity. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Carefully consider what impact the loss of network service availability would have on clinical practice (7.7.6.2)*.
- In a cloud computing environment, the inconsistency of network policies can cause system outages. The CSP should define and document an information security policy for the physical network (CLD.13.1.4) [$].

In addition to the controls above, the PHR provider should:

- Create a document that contains procedures for critical operations, where failure can cause irreparable damage to assets in the cloud computing environment. This document should specify that a supervisor should monitor such operations (CLD.12.1.5) [$].

In case a PHR goes offline, or is unavailable for any reason, business continuity should be ensured by considering the impact that this would have, and taking measures to avoid such.

H.Backup and Encrypt PHR Data

When the cloud that is used for storage, experiences prolonged and permanent outages, it has a negative impact on the customer who relies on the data. It is important for a CSP to have a plan for how the data would be recovered; and to ensure that it is still accessible [16]. The guideline that has been identified to limit this risk is to back up and encrypt PHR data. This implies that the PHR provider should ensure that the CSP adheres to the following:

- In order to make sure that personal health information would be available in the future; it should be backed up and stored in a physically secure environment (7.7.5)*.

In addition to the above control, the PHR provider should:

- Request the specifications of the backup capability in a case where the CSP provides backup capabilities as part of the cloud service (12.3.1) [$].

PHR data should be backed up and encrypted to ensure their availability.

I. Enforce Technical Interoperability

It is possible for customer data to experience data lock-in in the cloud – due to a number of reasons – such as the provider going out of business [17]. The lack of interoperability between cloud services prohibits customers from utilising multiple providers at the same time [18]. The guideline that has been identified to deal with this risk is to enforce technical interoperability. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Systems that process personal health information need to be technically interoperable; since many of them typically consist of different interoperating systems (7.12.3)*.

In addition to the above control, the PHR provider should:

- Consider using the hybrid cloud approach. This is a private cloud that is linked to one or more external cloud services that are managed centrally and provisioned as a single unit [32]. This can be used to mitigate data lock-in where the public cloud can be used to capture the extra tasks that cannot be easily run in the data center – due to temporary heavy workloads [33].

It is vital for PHRs to be interoperable with other health systems, in order for them to be deemed useful.

J. Respond to Information Security Incidents

Denial of Service (DoS) poses numerous threats in the cloud computing environment [17]. By attacking one server, the attacker may affect the availability of other services as well [29]. This threat is intensified in a health system that becomes unavailable, especially in an emergency situation [11]. The guideline that has been identified to limit this risk is to respond to information security incidents. This implies that the PHR provider should ensure that the CSP adheres to the following:

- Report security incidents. These include corruption or unintentional disclosure of personal health information, or the loss of availability of health information systems, where such a loss affects the patient's care in an undesirable manner (7.10.1)*. Have mechanisms in place that allow the PHR provider to report an information security event to the CSP. The CSP should also report any information security event to the PHR provider, and also keep track of the status of the reported information security event (16.1.2) [$].
- Respond to information security incidents. This involves the collection of evidence as soon as possible after the incident has occurred; conducting information security forensic analysis; ensuring that all involved response activities are properly logged for later analysis; dealing with information security weaknesses that led to, or contributed to, the incident (16.1.5) [$].

For PHRs to be kept available all the time, security incidents should be reported to the PHR providers; so that they can provide other means to keep the PHR accessible. Action also needs to be taken, in order to properly respond to and avoid the incident from recurring.

V. CONCLUSION

Health is one of the most important factors that one has to manage, as part of one's daily living. Using paper records to store and manage past and current illnesses has proven to be a challenge when it comes to accessibility and storage. The introduction of PHRs is one way of simplifying health management

PHRs can be stored locally on a web server or via cloud computing. Cloud computing introduces numerous benefits for the storage and processing of information. Storing PHRs in the cloud environment is beneficial for both the PHR users and the PHR providers. PHR users get extensive access to their health data, as long as there is an internet connection. They get to use the resources as needed, which promotes great scalability. PHR providers get to cut operational costs because they transfer all the IT infrastructure and maintenance costs to the CSP.

As much as cloud computing brings all these added benefits to PHRs, it comes with serious security concerns, which is what led to this study. Cloud computing involves many uncertainties that should be considered before any kind of business decides to migrate to the cloud.

The main problem addressed in this study is that there is a lack of guidance to assist PHR providers in making an informed choice when selecting a CSP, to ensure their customers' data are kept private and secure. The primary objective of the study was thus to propose guidelines to assist PHR providers in making an informed choice when selecting a CSP to ensure their customers' data remain private and secure.

This research aimed at assisting a PHR provider in making sure that they select a CSP that adheres to the technical aspects addressed in the guidelines. The Cloud Security Alliance (CSA) (2016) states that insufficient due diligence in selecting a CSP is a security concern for cloud adoption. Providing these guidelines could, therefore, ensure that PHR providers perform due diligence. They can also aid in the better use of cloud facilities, as well as those of PHRs, by potentially diminishing some of the risks associated with offering cloud-based PHRs.

VI. REFERENCES

[1] D. Kaelber, A. Jha, D. Johnston, B. Middleton, and D. Bates, "A research agenda for personal health records (PHRs)," *J. Am. Med. Informatics Assoc.*, vol. 15, no. 6, pp. 729–736, 2008.

[2] A. Sunyaev, A. Kaletsch, C. Mauro, and H. Krcmar, "Security Analysis of the German Electronic Health Card ' S Peripheral Parts," in *International Conference on Enterprise Information Systems*, 2009, pp. 19–26.

[3] C. Pagliari, D. Detmer, and P. Singleton, "Potential of electronic personal health records," *Bmj*, vol. 335, no. 7615, pp. 330–333, 2007.

[4] N. Archer, U. Fevrier-Thomas, C. Lokker, K. a McKibbon, and S. E. Straus, "Personal health records: a scoping review.," *J. Am. Med. Inform. Assoc.*, vol. 18, no. 4, pp. 515–522, 2011.

[5] H. Neal, "EHR vs. EMR, What's the Difference," 2008. [Online]. Available: http://profitable-practice.softwareadvice.com/ehr-vs-emr-whats-the-difference/. [Accessed: 29-May-2013].

[6] J. Woollen *et al.*, "Patient Experiences Using an Inpatient Personal Health Record," *Appl. Clin. Inform.*, vol. 7, no. 2, pp. 446–460, 2016.

[7] L. C. Osterhaus, "Cloud Computing and Health Information," *U I SLIS J.*, vol. 19, pp. 1–7, 2010.

[8] F. Sabahi, “Cloud computing security threats and responses,” *2011 IEEE 3rd Int. Conf. Commun. Softw. Networks*, pp. 245–249, 2011.
[9] J. Geelan, “Twenty-One experts define Cloud computing,” 2009. [Online]. Available: http://www.vertualization.sys-con.com/node/612375?page=0,0. [Accessed: 18-Feb-2014].
[10] R. Kalaiselvi, K. Kousalya, R. Varshaa, and M. Suganya, “Enhanced secure sharing of personal health records in cloud computing,” *Gazi Univ. J. Sci.*, vol. 29, no. 3, pp. 583–591, 2016.
[11] E. AbuKhousa, N. Mohamed, and J. Al-Jaroodi, “e-Health Cloud: Opportunities and Challenges,” *Futur. Internet*, vol. 4, no. 3, pp. 621–645, Jul. 2012.
[12] H. Elmogazy and O. Bamasak, “Towards healthcare data security in cloud computing,” *8th Int. Conf. Internet Technol. Secur. Trans.*, pp. 363–368, 2013.
[13] J. R. Venable, “Design science research post Hevner et al.: Criteria, standards, guidelines, and expectations,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6105 LNCS, pp. 109–123, 2010.
[14] A. Behl, “Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation,” *Proc. 2011 World Congr. Inf. Commun. Technol. WICT 2011*, pp. 217–222, 2011.
[15] C. Onwubiko, B. P. Rimal, E. Choi, and I. Lumb, “Cloud Computing,” *Comput. Commun.*, vol. 77, pp. 271–288, 2010.
[16] W. Jansen and T. Grance, “Guidelines on Security and Privacy in Public Cloud Computing,” *Director*, vol. 144, no. 7, 2011.
[17] M. Carroll, A. Van Der Merwe, and P. Kotzé, “Secure Cloud Computing: Benefits, Risks and Controls,” *Inf. Secur. South Africa*, pp. 1–9, 2011.
[18] T. Dillon, C. W. C. Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” *Adv. Inf. Netw. Appl. (AINA), 2010 24th IEEE Int. Conf.*, pp. 27–33, 2010.
[19] S. Sengupta, V. Kaulgud, and V. S. Sharma, “Cloud Computing Security--Trends and Research Directions,” *2011 IEEE World Congr. Serv.*, pp. 524–531, 2011.
[20] A. Mishra, R. Mathur, S. Jain, and J. Rathore, “Cloud Computing Security,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 1, no. 1, pp. 36–39, 2011.
[21] Z. Mahmood and R. Hill, *Computer Communications and Networks*. 2011.
[22] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, 2013.
[23] J. Wei, C. Pu, C. Rozas, A. Rajan, and F. Zhu, “Modelling the runtime integrity of Cloud servers: A scoped invariant perspective,” in *Privacy and security of Cloud Computing*, London: Springer, 2013, pp. 212–232.
[24] A. Hutchings, R. G. Smith, and L. James, “Cloud computing for small business: Criminal and security threats and prevention measures,” no. 456, 2013.
[25] A. M. Kuo, “Opportunities and challenges of cloud computing to improve health care services,” *J Med Internet Res*, vol. 13, no. 3, p. e67, 2011.
[26] G. Fernández-Cardeñosa, I. De La Torre-Díez, M. López-Coronado, and J. J. P. C. Rodrigues, “Analysis of cloud-based solutions on EHRs systems in different scenarios,” *J. Med. Syst.*, vol. 36, no. 6, pp. 3777–3782, 2012.
[27] A. M. Kuo, “Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model,” *J. Med. Internet Res.*, vol. 13, no. 3, 2011.
[28] I. de la Torre-Díez, S. González, and M. López-Coronado, “EHR systems in the Spanish Public Health National System: the lack of interoperability between primary and specialty care.,” *J. Med. Syst.*, vol. 37, no. 1, p. 9914, Feb. 2013.
[29] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, “A survey on security issues and solutions at different layers of Cloud computing,” *J. Supercomput.*, vol. 63, no. 2, pp. 561–592, 2013.
[30] Y. Sharma, B. Javadi, W. Si, and D. Sun, “Reliability and energy efficiency in cloud computing systems: Survey and taxonomy,” *J. Netw. Comput. Appl.*, vol. 74, pp. 66–85, 2016.
[31] International Organization for Standardization, “Health informatics — Information security management in health using ISO/IEC 27002,” Switzeralnd, 2008.
[32] S. Ramgovind, M. M. Eloff, and E. Smith, “The management of security in Cloud computing,” *Inf. Secur. South Africa (ISSA), 2010*, 2010.
[33] M. Armbrust *et al.*, “A view of Cloud Computing,” *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.