Information security risk measures for Cloud-based Personal Health Records

Avuya Mxoli[1+2], Mariana Gerber[1] and Nicky Mostert-Phipps[1]

[1]School of Information and Communication Technology
Nelson Mandela Metropolitan University
Port Elizabeth, South Africa
[2]Smart Systems
Council for Scientific and Industrial Research
Pretoria, South Africa

Abstract—**Personal Health Records (PHRs) provide a convenient way for individuals to better manage their health. With the advancement in technology, they can be stored via Cloud Computing. These are pay-per-use applications offered as a service over the Internet. Similar to other Internet-based technologies, Cloud Computing poses security risks. This paper aims to formulate the implications of Cloud Computing risks on personal health information. A qualitative content analysis was used to analyse literature on Cloud Computing risks to emphasise its implications from a personal health information perspective. Access management, security issues, legal issues and loss of data are some of the risks that negatively impact the storing of PHRs in the Cloud. These can be mitigated by ensuring that only authorized parties are granted access; ensuring that users do not gain access to other users' data and that data remains encrypted; Cloud providers should comply to audits in order to make sure that proper regulations are followed in securing data in the Cloud; and making backups in case of data loss. Using Cloud-based PHRs can improve healthcare. Cloud Providers should work together with PHR providers in order to make sure PHR users can reap these benefits without being too concerned about the associated risks.**

Keywords—Cloud Computing; personal health records; information security risks; privacy; legislation

I. BACKGROUND

A Personal Health Record (PHR) is usually a web-based tool that allows individuals to capture, share, store and process their medical records in one central place [1], [2], [3]. The PHR is typically created, owned, and maintained by the individual and stores a summary of the individual's health information in one convenient place. It allows the individual to better manage his/her health especially if the individual has been diagnosed with a chronic condition such as diabetes and hypertension or diseases such as cancer, tuberculosis, or HIV/AIDS [4]. Depending on functionality, some PHRs allow individuals to set reminders for taking medications and schedule appointments with healthcare providers. They provide the option to make notes of symptoms, track pain and record side effects of medication. PHRs allow an individual to record medical information such as past and current illnesses, allergies, immunizations, medication, procedures, test results, and more [5], [6].

Some offer a variety of reliable health information, which can aid the individual in improving and better managing their health and that of their loved ones [6]. If an individual is being taken care of by a caregiver or family members, some PHRs allow those individuals to have access to some of the person's medical information. This promotes a better collaboration between the individual and those taking care of him.

PHRs enable individuals to provide their healthcare provider with a detailed summary of their medical history. Some allow health care providers to make notes on the individual's condition. Besides speeding up the diagnosis process and eventually the healing process, it could improve continuity of care by providing other healthcare providers with a clear description of the individual's health status based on what other healthcare providers discovered or observed [7]. Consulting with multiple healthcare providers may reduce the chances of having duplicate tests done if an individual uses a PHR [8]. Individuals may also use a PHR at home to monitor chronic diseases [7]. When forwarding PHRs to doctors or caregivers, timely advice and encouragement could be provided to individuals while they are at home recovering.

Web-based PHRs could be stored using Cloud Computing storage facilities [9]. Cloud Computing can 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 datacenters that provide the services [10], [11].

Cloud Computing has gained recognition; to such an extent that PHR providers are willing to shift their storage and applications to the Cloud [9]. It has also been claimed that Cloud Computing is set to see immense global investment in many sectors, including health care [12]. There are many ways that patients and healthcare providers can benefit from using the Cloud to access, store and manage PHRs [13], [14], [15], [16], [11], [7]. These include:

The financial assistance of the South African National Research Foundation (NRF) towards this research is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

- Reduced cost
- Improved continuity of care
- Interoperability
- Ease of use
- Scalability

Regardless of the many advantages that Cloud-based PHRs offer, the problem is that it also poses security and privacy risks to individuals' PHRs, which typically contain sensitive health information. This paper focuses on the implications of Cloud-based PHRs, by identifying risks to privacy and security of PHRs stored in the Cloud and proposes mechanisms to address these.

II. METHODS

For this research study, a literature study, in combination with a qualitative content analysis was used to identify and analyze relevant literature sources. A literature review was conducted to identify Information Security risks related to Cloud-based PHRs. The identified risks were further analyzed according to Confidentiality, Integrity and Availability as seen on Table 1. Based on this analysis, measures to address these risks were identified. Content analysis is one of the many qualitative methods used to analyze textual data. It focuses on detail and depth rather than measurement [17]. For the purpose of this study, this research method was found to be appropriate.

The next section discusses some Information Security risks and their implications on Cloud-based PHRs, followed by potential ways to address these.

III. INFORMATION SECURITY RISKS RELATING TO CLOUD-BASED PHRS

Health information on its own needs to be protected due to privacy issues; this is amplified when it comes to storing it in the Cloud because of the security and privacy risks that it is exposed to [14]. In general, for PHR's within the Cloud Computing environment, there are concerns around privacy and security. Below are some of these risks. These risks can be grouped according to two categories i.e. unauthorized access and loss of data.

Unauthorized access:

- Malicious insiders: The Cloud provider's staff members who have authorized access to a user's data may misuse it to perform malicious attacks on the users' PHR data [18].
- Physical intrusion: Cloud storage facilities are at a risk of being accessed by intruders which may compromise PHR data stored there [19].
- Third party access: A Cloud provider may decide to outsource the storage of some of their users' data to external parties [20]. This increases the fear of unauthorized access to the user's PHR data [21].
- Multi-tenancy: Different users share memory, networking capabilities etc. in Cloud Computing. This puts users' data at risks of being accessed by malicious attackers posing as PHR owners [22].
- Poor encryption key management: Some systems allow users to generate their own decryption keys and distribute them to authorized parties [14]. This becomes a challenge if the user loses the keys or discloses them to malicious parties [12].
- Software intrusions: A user's PHR may be attacked by malware which can compromise their sensitive information such as login details [23].

Loss of data:

- Data lock-in: It is possible that a PHR provider may want to change Cloud providers due to different reasons. Cloud Computing makes this difficult because most Cloud infrastructures have little capability on data, application and service interoperability [12].
- Systems unavailability: In the Cloud environment there is a possibility of systems unavailability and this can be a major issue in an emergency situation where an individual needs their PHR data [14].
- Temporary outages: Cloud services can and do experience temporary outages which last for hours [24].
- Prolonged and permanent outages: It is possible for a Cloud provider to experience serious problems such as bankruptcy or facility loss. This affects service for extended periods or even leads to a complete shutdown [25].
- Denial of Service (DoS): This involves "saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner" [25]. The attacker is not targeting the information but rather it aims at denying genuine rights to others [26].

The following section categorizes the above mentioned risks according to some aspects of Information Security that can be affected by them.

IV. RISK CATEGORIES

Data security is one of the most recognized problems in Cloud Computing [27], [28]. Information Security may be defined as "something that ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability)" [29]. It involves three aspects: confidentiality, integrity and availability (CIA):

- Confidentiality: refers to who has access or authority to access certain information.

- Integrity: refers to the modification of assets by authorized parties and these can be data, hardware or software.
- Availability: refers to whether the data is available when needed by authorized parties.

Table 1 illustrates the classification of the above mentioned risks according to the aspects of CIA. The definition of each identified risk was analyzed to determine the implication of risk according to the aspects to which it most closely relates. Some risks were associated with having implications to more than one aspect.

TABLE I. PHR-RELATED CLOUD COMPUTING RISKS

RISK	Category		
	Confidentiality	***Integrity***	***Availability***
Unauthorized access			
Malicious insiders	✓	✓	✓
Physical intrusion	✓		✓
Third party access	✓	✓	
Multi-tenancy	✓	✓	✓
Poor encryption key management	✓	✓	✓
Software intrusions	✓	✓	✓
Loss of data			
Data lock-in	✓	✓	✓
Systems unavailability			✓
Temporary outages			✓
Prolonged and permanent outages			✓
Denial of Service (DoS)			✓

V. ADDRESSING INFORMATION SECURITY RISK FOR CLOUD-BASED PHRS

This section discusses potential measures that can be taken in order to mitigate the risks mentioned in the Information Security risks relating to PHRs section according the categories mentioned in the one above. The ISO 27799:2008 standard for information security management in health was consulted to identify some of the measures.

A. Unauthorized Access

The following sub-section includes a discussion on addressing risks that may compromise access to an individual's Cloud-based PHR. The risks that fall under this sub-section are malicious insiders, physical intrusion, third-party access, multi-tenancy, poor encryption key management and software intrusions as illustrated on Table 1. Suggestions from various authors are mentioned below [30], [31], [21], [32], [25], [33], [34]:

Personal health information should be uniformly classified as confidential. The following characteristics of information assets need to be considered. Confidentiality of personal health information is:

- Often largely subjective, rather than objective.
- Context-dependent i.e. when used in a different context, information can be confidential whereas in another it may not be.
- Prone to shift over the lifetime of individual's health record. Some issues that are considered confidential currently may not have been considered as confidential in another lifetime.

Because of these characteristics, all personal health information should be subject to suitable protection at all times. Confidentiality, can be compromised if the PHR data is somehow leaked or there is a misapplication of network rights. All health systems used to process personal health information should, therefore, inform users of the confidentiality of the personal health information accessible from such systems, e.g. at start-up or log-in. Hard copy output from the systems should be labeled as confidential (7.4.2.2.). There must be an agreement in place that specifies the confidential nature of the information. It must be applicable to all personnel that have access to the health information (7.3.2.3.). Ways to prevent confidentiality breach include network security controls; network authentication services and data encryption services.

Identity and access management (IAM) can be used to ensure that only the users with the legitimate identity can gain access. Organizations that process personal health information must control access to the information. Users of health information systems should only access personal health information when there is a healthcare relationship between the user and data subject; the user is carrying out activities on behalf of the data subject; or when there is a need for specific data to support this activity (7.8.1.). Identity is crucial to any system that is security conscious. It grants users, services, servers and any other entities access to the system. IAM focuses on Authorization, Authentication and Auditing (AAA) of the users accessing Cloud services. Access to health information systems that contain personal health information must be subject to a formal user registration process. This will ensure that the level of authentication required by the claimed user identity is consistent with the level(s) of access that will be granted to the user. These details must be periodically reviewed to ensure that they are complete, accurate and that the access is still required (7.8.2.1.). This preserves the confidentiality of the system and the data contained therein. Health information systems that process personal health information must authenticate users and should do that by means of authentication that involves at least two factors (7.8.5.1.). Apart from authentication, user privileges should exist and be monitored in order to restrict access to sensitive parts of a system or consumer's data. Role-based access control, workgroup-based access control and discretionary access control can help to ensure confidentiality and integrity (7.8.2.2.). Organizations that process personal health information should clearly define and assign information security responsibilities. They should also have an

Information Security Management Forum (ISMF) that will ensure that there is clear direction and visible management support for initiatives which involve the security of health information (7.3.2.1.). Special consideration, however, should be given in cases where a user may need to access personal health information in an emergency situation where the subject of care may be unable to grant the access (7.8.2.4.). Health information systems processing personal health information must provide personally identifying information that will assist health professionals in confirming that the electronic health record retrieved belongs to the subject of care under treatment (7.9.2.5.).

Integrity, when it comes to information stored in the Cloud, requires that three principles are met i.e.

- Unauthorized personnel or processes cannot make modifications.
- Authorized personnel or processes cannot make unauthorized modifications.
- The data is internally and externally consistent meaning the data stored internally matches all its sub-entities as well as the one stored externally.

Firewall services, communications security management and intrusion detection systems may be used to preserve information integrity. Health information systems that contain personal health information should create a secure audit record every time a user accesses, creates, updates or archives personal health information via the system. The audit log should uniquely identify the user, data subject; identify the action performed by the user and note time and note of such an action. When personal health information has been updated, the original document as well as its audit log should be retained (7.7.10.2.). The integrity of the information contained in the PHR can be maintained by conducting these logs. There should be a segregation of duties and responsibilities in order to reduce chances for unauthorized modification or misuse of personal health information (7.7.1.3.). The availability of PHR data can be compromised if the above mentioned CIA aspects because once confidentiality and integrity are compromised it means a third party gained unauthorized access and by modifying the data they can influence its availability. One way that loss of availability can occur is if an employee changes the name of a file then there will be no way to access it if they do not share this information. Some of the elements that can be used to ensure availability include backups and redundant disk systems; acceptable logins and operating process performance; and reliable and interoperable security processes and network security mechanisms. Below are suggestions that relate specifically to the risks and ISO 27799:2008 controls that relate to each risks are discussed.

I. Malicious insiders

Malicious insiders pose a serious threat to consumer data as they can use a higher level of access to gain access to confidential information about the consumer. They can use this information without the knowledge of the consumer and they can also compromise its availability. An important requirement for Cloud providers is that they monitor their administrators in terms of what they access and a background check should also be conducted. An access control policy must be in place in order to govern access to personal health information. 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 (7.5.1.), staff members should be given roles and responsibilities in the job description; there should be a screening process to verify identity, living address, previous employment; terms and conditions of employment. During employment (7.5.2.), staff members should be assigned responsibilities; get information security awareness and training; be informed of the disciplinary process. Upon termination or change of employment (7.5.3.), access rights must be revoked. Consumers should then ask their Cloud providers to give them specific details about the people they hire and exactly what kind of privileged access they have over their data. Consumers should demand more transparency from the Cloud providers, in terms of the security and management process including compliance reporting and breach notification.

II. Physical Intrusion

There should also be a physical security perimeter in order to control access to facilities that contain personal health information; there should be physical entry controls; offices should be secured; rooms and facilities should be secured; protection against external and environmental threats should exist; public access, delivery and loading areas should be secure enough not to expose personal health information. These are all there in order to ensure that the public do not get too close IT equipment. Equipment or software used to support a healthcare application that contains personal health information should not be removed from the site or relocated within the organization without authorization by the organization (7.6.).

III. Software intrusion

Appropriate prevention, detection and response controls to protect against malicious software must be adopted and appropriate user awareness training should be implemented (7.7.4.1.). Cloud services have intrusion detection systems (IDSs), intrusion prevention systems (IPSs), virtual private networks (VPNs) and multifactor authentication. These systems set off alerts about detected intrusions then a system administrator or the actual system takes appropriate action.

IV. Third party access

A risk assessment must be carried out by organizations responsible for processing health information to weigh the risks that third parties might pose to the systems and data they contain. Security controls must then be implemented according to the identified level of risk and to the technologies used (7.3.3.1.). In cases where 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, security measures that must be implemented and/complied with,

limitations to access these services by third-parties, the service levels to be achieved in services rendered, the arrangements for compliance auditing of the third-parties, and the penalties that will apply should any of these not be honored (7.3.3.3.). Information exchange agreements that specify the minimum set of controls to be implemented must also be used (7.7.8.1.).

V. Multi-tenancy

Development, test and operation facilities should be separated (physically or virtually) (7.7.1.4.). Compartmentalization should be enforced in order to ensure that consumers may not access other consumers' information due to multi-tenancy. "Policies, application deployment, and data access and protection should be taken into account to provide a secure multi-tenant environment" says [35].

VI. Poor encryption key management

Encryption is considered as the main solution to obtaining confidentiality for data, processes and communications. It is one of the solutions to ensuring security in the Cloud. If applied, it is recommended that it be performed at multiple locations, within the data center, or between private and public Clouds and so on. Consumers are also advised to encrypt their data separately before uploading it.

B. Loss of data

This sub-section covers possible measures that can be taken to mitigate risks that relate to data lock-in, systems unavailability, temporary outages, prolonged and permanent outages and Denial of Service (DoS). These risks all relate to the Availability aspect of CIA. Even though it is highly unlikely for Cloud providers to go broke or get acquired and consumed by a larger company, consumers should make sure that their data will remain available [32]. Organizations that process personal health information should carefully assess what impact the loss of network service availability will have on clinical practice (7.7.6.2.) [33]. Below are a few suggestions on how to ensure that data is not lost in the Cloud gathered from [36], [37], [38], [39], [4], [40], [33]:

All personal health information must be backed up and stored in a physically secure environment in order to preserve its future availability. Encryption should be used to preserve confidentiality (7.7.5.). Business continuity management which includes disaster recovery is increasingly recognized as a requirement for health organizations (7.11). In case of a disaster occurring, whether it is of natural or human origin, data in the Cloud should be regularly backed up for recovery. Using the virtualization software, virtual servers can be copied which can provide backups and quick reallocation of computing resources without downtime. Cloud providers can back up their consumer data across a number of Clouds. This will help in the recovery process if one Cloud service fails. The Cloud security alliance [4] proposes that consumers get into a contractual agreement with their Cloud providers which will state the Cloud provider's backup and retention strategies. One of the ways to mitigate data lock-in is the standardization of Application Programming Interfaces (APIs) so that a developer can be able to deploy services and data across many Cloud providers. This will provide a backup in such a way that if there is a failure with one provider, there will still be other copies available. Organizations that process personal health information should report security incidents. These include corruption or unintentional disclosure of personal health information or loss of availability of health information systems, where such a loss undesirably affects patient care (7.10.1.).

Table II summarizes the ISO 27799:2008 controls that can be used to address the specific risks as described above.

TABLE II. PHR-RELATED CLOUD COMPUTING RISKS WITH POTENTIAL ISO CONTROLS

Risk	**Category**		
	Confidentiality	***Integrity***	***Availability***
	ISO 27799:2008 Controls		
Unauthorized access			
Malicious insiders	7.3.2.1. 7.3.2.3. 7.4.2.1. 7.4.2.2. 7.5. 7.7.1.3. 7.7.8.1. 7.7.10.2. 7.8.1. 7.8.1.2. 7.8.2.1. 7.8.2.2. 7.8.5.1.	7.3.2.1. 7.5. 7.7. 7.8.2.2. 7.8.5.1.	7.3.2.1. 7.7.1.3.
Physical intrusion	7.6.		7.6.
Third party access	7.3.2.3. 7.3.3.1. 7.3.3.3. 7.4.2.1. 7.4.2.2. 7.7.8.1. 7.7.10.2. 7.8.1. 7.8.1.2. 7.8.2.1. 7.8.2.2. 7.8.2.4. 7.8.5.1. 7.9.2.5.	7.3.3.1. 7.3.3.3. 7.8.2.2. 7.8.2.4. 7.8.5.1.	

Multi-tenancy	7.7.1.4.	7.7. 1.4.	7.7.1.4.
Poor encryption key management			
Software intrusions	7.7.4.1.	7.7. 4.1.	7.7.4.1.
Loss of data			
Data lock-in			7.7.5.
Systems unavailability			7.7.5. 7.7.6.2. 7.10.1. 7.11.
Temporary outages			7.7.5. 7.7.6.2. 7.10.1. 7.11.
Prolonged and permanent outages			7.7.5. 7.7.6.2. 7.10.1. 7.11.
Denial of Service (DoS)			7.7.5. 7.7.6.2. 7.10.1. 7.11.

VI. Conclusion

As much as Cloud-based PHRs introduce advantages, Cloud Computing poses security and privacy risks to an individual's PHR. This paper focused on the implications of Information Security risks on Cloud-based PHRs. Literature sources were used to highlight the risks that Cloud Computing poses on Cloud-based PHRs as well as potential mechanism to address these risks. Legislation proves to be very significant in enforcing compliance from Cloud providers to protect the data that they store for their consumers. Future research includes developing an approach that will address information security legislation relating to Cloud-based PHRs.

References

[1] D C Kaelber, A K Jha, D Johnston, B Middleton, and D W Bates, "A reserach agenda for personal health records," J Am Med InformAssoc, vol. 15, pp. 729-736, 2008.

[2] C Pagliari, D Detmer, and P Singleton, "Potential of electronic personal health records," BMJ, vol. 335, no. 330, pp. 330-333, 2007.

[3] A Sunyaev, D Chornyi, C Mauro, and H Krcmar, "The evaluation framework for personal health records: Microsoft HealthVault vs. Google Health," in System Sciences (HICSS), 2010 43rd Hawaii International Conference, Honolulu, 2010, pp. 1-10.

[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. 8, no. 4, pp. 515-522, 2011.

[5] H Neal. (2008, November) EHR vs PHR- What's the difference? [Online]. http://profitable-practice.softwareadvice.com/ehr-vs-emr-whats-the-difference/. Access Date: 29 May 2013).

[6] P C Tang, J S Ash, D W Bates, J M Overhange, and D Z Sands, "Personal health records:definitions,benefits, and strategies for overcoming barriers," J AM Med Inform Assoc, vol. 13, no. 2, pp. 121-126, 2006.

[7] The Workgroup on the NHII of the NCVHS, "Personal health records and personal health record systems," Washington,D.C., 2006.

[8] M I Kim and K B Johnson, "Personal health records: Evaluation of Functionality and Utility," Journal of the American Medical Informatics Association, vol. 9, no. 2, pp. 171-180, 2002.

[9] L Ming, Y Shucheng, R Kui, and L Weinjing, "Securing Personal Health Records in CloudComputing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings," in Security and privacy in communication networks.: Springer Berlin Heidelberg, 2010, pp. 89-106.

[10] F Sabahi, "Cloud computing security threats and responses," in Communicayion software and networks (ICCSN),2011 IEEE 3rd International Conference, 2011, pp. 245-249.

[11] J Geelan. (2009, January) Twenty-one experts define cloud computing. [Online]. http://virtualization.sys-con.com/node/612375. Access Date: 18 February 2014).

[12] A Kuo, "Opportunities and Challenges of Cloud Computing to Improve Health Care Services Cloud Computing : A New Economic Computing Model," Journal of Medical Internet Research, vol. 13, no. 3, pp. 622-645, 2011.

[13] S Marston, Z Li, S Bandyopadhyay, J Zhang, and A Ghalsasi, "Cloud computing-the business perspective," Decision support systems, vol. 51, no. 1, pp. 176-189, 2011.

[14] E Abukhousa, N Mohamed, and J Al-Jaroodi, "e-Health Cloud: Opportunities and Challenges.," Future Internet, vol. 4, no. 3, pp. 621-645, 2012.

[15] S Zhang, S Zhang, X Chen , and X Huo, "Cloud computing research and development trend," in 2010 second Internation Conference on Future Networks, Sanya, 2010, pp. 93-97.

[16] M E Bégin et al., "An EGEE comparative study: Grids and Clouds-Evolution or Revolution," 2008.

[17] J Forman and L Damschroder, "Qualititative methods," in Empirical methods for bioethics: A primer, 11th ed., L Jacoby and L A Siminoff, Eds. Oxford: Elsevier, 2008.

[18] A Behl, "Emerging Security Challenges in Cloud Computing: An insight to cloud security challenges and their mitigation," in Information and Communication Technologies (WICT), Mumbai, 2011, pp. 217-222.

[19] A Hutchings, S G Russell, and J Lachlan, "Cloud computing for small businesses: criminal and security threats and prevention measures," Trends and issues in Crime and Criminal Justice, no. 456, pp. 1-8, 2013.

[20] D Zissis and D Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, 2012.

[21] C Modi, D Patel, B Borisaniya, A Patel, and M Rajarajan, "A survey on security issues and solutions at different layers of Cloud computing," The Journal of Supercomputing, vol. 63, no. 2, pp. 561-592, 2013.

[22] A Mishra, R Mathur, S Jain, and J S Rathore, "Cloud computing security," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 1, no. 1, pp. 36-39, 2013.

[23] J Wei, C Pu, C V Rozas, A Rajan, and F Zhu, "Modelling the runtime integrity of Cloud servers: A scoped invariant perspective," in Privacy and security of Cloud Computing, S Pearson and G Yee, Eds. London: Springer, 2013, pp. 212-232.

[24] N Leavitt, "Is Cloud Computing Really Ready for Prime Time?," Computer, vol. 42, no. 1, pp. 15-20, 2009.

[25] W A Jansen, "Cloud hooks: security and privacy issues in Cloud computing," in System sciences (HICSS),2011 44th Hawaii INternational Conference, 2011, pp. 1-10.

[26] K T Win, W Susilo, and Y Mu, "Personal Health Record Systems and Their Security Protection," Journal of Medical Systems, vol. 30, no. 4, pp. 309-315, 2006.

[27] A Sarwar, M Naeem, and A Khan, "A Review of Trust Aspects in Cloud Computing Security," International Journal of Cloud Computing and Services Sciences, vol. 2, no. 2, pp. 116-122, 2013.

[28] D Jamil and H Zaki, "Cloud computing security," Internationa Journal of Engineering Science and Technology, vol. 3, no. 4, pp. 3478-3483, 2011.

[29] ISACA, "COBIT 5 for Information Security," ISACA, USA, Preview version 2012.

[30] A Bouayad, A Blilat, N El Houda Mejhed, and M El Ghazi, "Cloud computing:security challenges," in Information Science and Technology (CIST), 2012 Colloquium, 2012, pp. 26-31.

[31] G Kulkarni, J Gambir, T Patil, and A Dongare, "A security aspect in Cloud Computing," in Software Engineering and Service Science (ICSESS), 2012 IEEE 3rd International Conference, 2012, pp. 547-550.

[32] J. Brodkin. (2009, July) Network World. [Online]. www.networkworld.com/news/2008/070208-cloud.html?page=1. Access Date: 20 February,2014).

[33] International Organization for Standardization, "Health informatics — Information security management in health using ISO/IEC 27002," Switzerland, eStandard ISO 27799:2008(E), 2008.

[34] C Lo, C Huang, and J Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," in Parallel processiong workshops,2010 39th International conference, San Diego, 2010, pp. 280-284.

[35] H Takabi, J B Joshi, and A Gail-Joon, "SecureCloud:Towards a comprehensive framework for cloud computing environments," in Computer Software and Applications Conference Workshop (COMPSACW),2010 IEEE 34th Annual, 2010, pp. 393-398.

[36] J M Kizza, "Cloud computing and related security issues," in Guide to computer network security. London: Springer London, 2013, pp. 465-489.

[37] S Subashini and V Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[38] K Popovic and Z Hocenski, "Cloud computing security issues and challenges," in MIPRO,2010 Proceedings of the 33rd International Convention, 2010, pp. 344-349.

[39] M A AlZain, E Pardede, B Soh, and J A Thom, "Cloud computing security: from single to multi-clouds," in System Science (HICSS), 2012 45th Hawaii International Conference, 2012, pp. 5490-5499.

[40] M Armbrust et al., "A view of Cloud Computing," Communications of the CAM, vol. 53, no. 4, pp. 50-58, 2010.