Review of e-Health Frameworks

Biraj Prajapati, Prof William J Buchanan, Richard Macfarlane, Adrian Smales, Greg Spyra
Edinburgh Napier University
10 Colinton Road, Edinburgh

In order to improve the quality of health care and widen the accessibility, health care providers are consistently looking to inject information and communication technology to the traditional health care system (Mair, et al., 2012). This process can be defined as e-health. World Health Organization (WHO) has defined E-Health as "the use of information and communications technologies (ICT) in support of health and health-related fields, including health-care, health surveillance, health literature, and health education, knowledge and research" (Blaya, et al., 2010). In other words, e-health can be defined as the use of information technology in order to make a progressive approach in the field of health care. This paper outlines some of the developments in the creation of e-Health framework, and which aim to create an integrate approach to e-Health. This includes the DACAR e-Health framework developed in collaboration between Imperial College, London and Edinburgh Napier University, and which was implemented within Chelsea and Westminster Hospital, London.

e-Health Framework, patient records, computer security

1. INTRODUCTION

The past decade has seen the constant growth on the study and research related to the implementation of e-health system and its evaluation. A study has found out that 56%-79% of internet users in US seek health information over the internet (Andreassen, et al., 2007). People from all around the world have started making a great use of technology for their healthcare system. Thus, the national health authorities around the world such as English NHS, German Telematic platform, danish sundhed.dk etc. have began to focus on different e-health services such as electronic patient record, electronic health cards and electroninc health portals (Andreassen, et al., 2007). Many innovative forms of electronic health care services have been evaluated over the past few years in order to analyse benefits, costs and potential consequences through it. There are also some certain requirements that an efficient and trustworthy e-health system should possess.

2. E-HEALTH SYSTEM REQUIREMENTS

Many surveys have been carried out around the world in relation to the requirements for use of technologies in the medical field and it was found out that security and privacy are the two most important requirements. Thus, it plays a vital role in successful implementation of e-health and other medical technologies. A survey found out that females and healthy adults require more security and privacy standards in comparison to the males and ailing elderly (Wilkowska & Ziefle, 2012). The sensitive data stored in an e-health system implies that an e-health system should always have proper security and privacy policy because the disclosure of any of the patient's data cound have a severe consequences. The leakage or the disclosure of the data may also result in legal penalties to the health system providers for violating the privacy laws.

Eysenbach (2001), in his paper, has put together 10 e's that characterizes an e-health. These 10 e's can also be classed as a requirement for the e-health system. According to Eysenbach (2001), an e-health should be efficient, evidence based and equitable. It should enhance the quality of care and also follow the patient-physician ethics. It should prioritise the education of health care workers via online sources and also enable the exchange of information in a uniform method. Finally, an e-health should also encourage relationship between patients and health professionals, resulting in the extension of scope of health care beyond the conventional boundaries (Eysenbach, 2001).

Although patient centric e-health system is the future for e-health system, there are lots of challenges that need overcoming if it is to be successfully implemented over the coming years (Ball & Lillis, 2001). It's not just the technical challenges that needs overcoming, but also the support and awareness for the patients, which would include consumer education, physican/ consumer communication, administrative efficiencies, clinical decision support and disease management (Ball & Lillis, 2001).

Along with all these requirements, it is also necessary that an e-health system complies with

laws related to the medical data sharing in a country. This would include the data protection act or a similar ethical act.

Availability of e-health services all the time has also been cited as one of the major requirements of an e-health system by AbuKhousa, et al. (2012). In an emergency situation, the loss or an unavailability of e-health system could result in severe consequences in patient's life, thus, it is necessary that the e-health system is available all the time (AbuKhousa, et al., 2012).

3. CURRENT STATE OF E-HEALTH

The injection of IT in the field of health care has become progressively important to many countries around the world in recent years. e-health has many advantages in terms of cost efficiency and improvement of personal health management. Thus, there has been a continuing global effort aiming to implement some form of e-health system.

Hsu, et al. (2005) carried out a longitudinal and population-based evaluation on the use of e-Health service in Northern California state of USA between 1999 and 2002, where over 3 million people utilised the e-health services provided by Kaiser Permanente-Northern California (KPNC), an integrated delivery system for e-health services. Their study involved e-health service members who used a web-based secure portal to request the appointments with their doctors and order the prescription drugs.

In order to utilize the service provided by KPNC, patients were required to register in this service by requesting a password protected account through the website. When that request was received, the IDS delivered a mail that had a randomly generated pin to the member's home address, who then could finalise the register using the pin and create a new personal password. This e-health system was mainly designed in order to facilitate the health records to the health worker and the patients had no access to their health records at all. Although this model found out that there was an increase in the number of users by more than 8% in the span of 3 years time, this model was only limited to the interest of health workers and the patients had a minimal role in it (Hsu, et al., 2005). Thus it was concluded that a lot of research was required in order to safely implement the e-health care system for the general public.

Canadian government began a plan to implement national e-health system in 2001, however, after 10 years when a qualititive study was performed on the progress, it was lagging behind many European countries in terms of implemention of national e-health care system, despite spending $1.6 billion. Lack of e-health policy was cited as one of the major reasons behind the failure of this plan, along with some of the approaches (Top-down) towards its implementation (Rozenblum, et al., 2011). Thus it was concluded that bottom-up, regional first approach was required for a successful implementation of an e-health technology.

Countries such as, Austria, Germany (German e-health card), and Taiwan (taiwan electronic medical record template) are conducting many different works in relation to authentication and access control for e-health. In case of German e-health card, every citizens are provided with the smart card which contains the general administrative information. The same card could be used in order to access the medical information. Every smartcard consists of cryptographic keys and functions in order to identify each patient uniquely. Taiwan electronic medical record contains a similar infrastructure which are based on smartcards, however, this model of Taiwan is more concentrated on easy information sharing (Lohr, et al., 2010).

Similarly, NHS scotland currently has its own e-health programme (2014-2020) that mainly aims to inject information and related technology with the intention of improving quality of patient care. The major strategic aims of this e-health programme includes supporting citizens to communicate and interact with NHS, manage their own health records, and improve the availability of the required information and tools for health workers in order to improve the quality of health care service. This programme also aims to facilitate everyone with digitally enabled information sharing solution, so that all the citizens and healthcare workers would be able to quickly access the information and required services, share the important information appropriately with the appropriate people and have an understanding on the information that is being shared, along with the confidence in its integrity, security and quality. Apart from accessing, sharing and controlling the information, it was also pointed out an e-health care system should be able to create an alert to trigger the people who are at risk. This programme is basically themed around placing people at the centre of health care and building partnerships between many health care bodies at local, regional and national level (Government, 2015).

At the current period though, health care systems of most developed countries face an uphill task to bring the improvement in the quality, efficency, security and safety of the citizens' medical data.

4. E-HEALTH FRAMEWORKS

Security and privacy of patients' medical and personal information is a major concern in healthcare domains and there is a great need of extensive work in regards to the privacy and secure access to the patients' records. There have been

many works carried out in the past in relation to the patients' data security and privacy in an e-health system.

Sharing of the data is an important aspect in a e-health system. In an ideal e-health system, selected doctors or health care workers should be able to access patients' data with the permission of patient. Russello, et al. (2008), in their paper, have suggested a workflow-based access control framework. In their framework, they have used the notion of workflow in order to capture the task one has to perform as the part of their duty, which would help to determine the required privilege. The model proposed by them is mostly based on the principle of granting least privilege in order to carry out their job (Russello, et al., 2008). In other words, an entity can have access to the resource for a certain length of time, only to perform their job, and once the work is completed, the access would be revoked. This model mainly follows the concept of role based access control for the health care system, and the decisions being made on the basis of the job performed by the entity. Even though Role base access control is considered as a state of art of the access control mechanism, this method is not flexible enough in order to cope with the demand that a health system or an e-health application presents in the current time.

Riedl, et al. (2008), in their paper, have introduced pseudonymization of information for privacy in e-health (PIPE) architecture in order to integrate primary and secondary usage of health data in an e-health system. Pseudonymization is a procedure in which a specifier replaces an identification data after being transformed into a specifier. This architecture provides an advanced concept for authorization, data sharing and data recovery, which would allow the restoration of access to the medical records even when the patient's security token is lost. (Riedl, et al., 2008) claim that this concept could be used as a foundation for the national electronic health record initiatives or even as an extension to any existant e-health applications. It is also claimed that in this system, patients are totally in control of their data that has maximum security, which was achieved by the application of encryption method. The use of different encryption key in order to secure the database has also been proposed in this architecture, whereas the integrity of data is maintained by making the use of Transport Layer Security or making the use of hash values (Riedl, et al., 2008).

Ford, et al. (2009) proposes the Secure Anonymised Information Linkage (SAIL) Databank system in order to ensure the secure data transportation and reliable record matchng method in order to facilitate precise linkage of data across the different medical datasets. This system accomplies with the data protection act 1998 and makes the use of deterministic encryption of the data in order to anonymise and prevent the identification of individuals. This system also ensures that the data access is performed in a controlled environment and is properly authorised. Moreover, this system also addresses the data disclosure risk in data views (Ford, et al., 2009).

The use of Model-Driven application level encryption has been proposed by (Ding & Klein, 2010) in order to maintain privacy in the medical data. Their model is based on the application's domain model, and generates the codes and configuration artifacts in order to control the encryption logic in the health system and modify database schema. The encryption is performed outside the database, thus, called application level encryption, which would allow flexibility in an e-health system. This model has also given special focus to the key management, giving special priority where the key is stored and who has the access to the keys. It is also argued in their paper that the use of randomly generated primary master key can be used in order to protect all the keys (Ding & Klein, 2010).

In order to provide the authentication and authorization for users to consume the services provided by e-health services, Han, et al. (2006) have proposed an authorization and authentication architecture for e-health services (A3AeHS) system that integrates both role based and attribute based method into the electronic health system. This model separates patients' general data from the sensitive record and creates an authorization policy according to the sensitivity of the data. The authorization policy is also based on the role of the entity in the system, e.g. a GP has an access to all the records of patient whereas a social worker will have access to only certain data. This model is similar to the WBAC model (Russello, et al., 2008) discussed previously, however, the attribute based access control and the proposal of multi-factor authentication system in order to access the data has made this model superior over WBAC model.

Similarly, Fan, et al. (2011) have proposed Data Capture and Auto Identification Reference (DACAR) platform for e-health in cloud computing in order to overcome the concerns related to security, large scale deployment, service integration, large scale deployment, and integration and confidentiality of the medical data. DACAR platform includes Single point of contact (SPoC) to provide authentication and authorisation functionalitites, rule based information sharing policy, and data buckets service in order to support the create, read, update and delete (CRUD) attribute which are hosted by cloud infrastructures. Some of the major issues that are addressed by DACAR are authentication, authorisation, data

persistence, data integrity, data confidentiality and audit trail. Apart from all these, DACAR also incude the functionalities for patient-centric e-health application, for eg: Early Warning Score(EWS) in order to react to any unusual data pattern (Fan, et al., 2011). DACAR platform also practices database-level encryption, using cryptographic signatures and kerberos authentication which ensures a great data security (Fan, et al., 2011).

Using DACAR platform, Ekonomou, et al. (2011), in their paper, have proposed a cloud based healthcare system which would integrate a formal health care system(DACAR) with an informal health care system (Microsoft Healthvault). This would enable the patients to share the health data on different health domain with their doctors, or someone who they prefer. They also claim that there is strong security and privacy of the medical data by following this practice, as the data security and privacy is ensured by both microsoft health vault and DACAR (Ekonomou, et al., 2011).

Similarly, Fengou, et al. (2013), in their paper, have proposed a framework that extends European Telecommunications Standards Institute (ETSI) architecture to deploy the standard services over next genertation IP networks (Fengou, et al., 2013). The collaboration of European Telecommunications standards, 3rd Generation Partnership Project and parlay group have defined the joint working group in the context of open service access and is responsible for developing and maintaining open service access specifications. These specifications define accessing the network functionalities by making the use of application programming interface(API). Fengou, et al. (2013), propose the use of ETSI/Parlay specifications in their e-health domain. In their framework, they have defined profile classes to categorise the users:

- Patients profile
- Healthcare professional profile
- Aid person's profile
- Operational domain's profile
- Group profile

In terms of security in the framework, low-weight hash functions along with the combination of key is used in order to generate a message authentication codes(MACs), which is used to authenticate the users and prevent the unauthorized data disclosure in order to maintain the data integrity (Fengou, et al., 2013). Similarly, this model also uses "*data integrity mechanism*", which was proposed by (Mantas, et al., 2009). In this method, data integrity is maintained by making the use of cryptographic smartcards, that contains secret keys, and MACs (Mantas, et al., 2009).

Lounis, et al. (2012) proposes a secure and scalable cloud-based architecture in order to deal with the challenges such as security and availability, created by the collection of health data with the means of medical sensor networks (Lounis, et al., 2012). They have claimed that the proposed mechanism for the data security is effective and flexible, as well as guarantees the confidentiality, integrity and access control to the medical data by making the use of combination of several cryptographic schemes. Their proposed framework considers two categories of users rather than five that was proposed by (Fengou, et al., 2013), i.e. patients and health professionals. Access control is achieved by making the use of attribute based encryption(ABE) in order to encrypt the data before storing it in database. There is a restriction to unauthorized access by using randomly generated symmetric key and security access policy which uses the combination of logical expressions through OR, AND or other operators. (Lounis, et al., 2012).

de Melo Silva, et al. (2014) have proposed the use of federated identity attributes for the secure storage and sharing of medical data in the cloud. They propose the use of SAML for the deployment of federated identity management. The collaborative networks between the institutions would enable the sharing of services between the users, and also enables the attribute management and facilitates single sign on. Like Lounis, et al. (2012), they too have proposed the use of attribute based encryption by providing users the cryptographic keys that would represent users true characters. They too, proposes the use of AND or OR operators and attributes to build a logical equation for security policies (de Melo Silva, et al., 2014).

The use of attribute based encryption is also supported by Li, et al. (2013), who proposes the use of individual secret key for every data owner(e.g. patient). It also supports the view of encryption of health record by using an encryption method, and implementation of role based access policy for users to access the data. They also claim that the security and access policy should be updated regularly, and there needs to be a provision of an audit trial to measure the effectiveness and security of data (Li, et al., 2013).

5. Conclusions

There are many e-Health frameworks proposed, each with key attributes, but there option requires a full review from experts, including those with a clinical and IT backgrounds. Without them, the sharing of information across disperate systems will be difficult, along with problems in sharing health entitites in differing systems. The development of DACAR within Chelsea and Westminster Hospital provides one such model, and where the patient has full control of their own data, and where data can be moved from one hosting provider to

another. This work has since progressed to a spin-out company (Symphonic Trust).

6. Bibliography

AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health cloud: opportunities and challenges. *Future Internet, 4*(3), 621-645.

Adams, C. (2011). Kerberos Authentication Protocol. In *Encyclopedia of Cryptography and Security* (pp. 674-675). Springer.

Al-Janabi, S. T., & Rasheed, M. A.-s. (2011). Public-key cryptography enabled kerberos authenticaiton. In *Developments in E-systems engineering (DeSE)* (pp. 209-214). IEEE.

Alliance, L. (2002). *Liberty alliance project*. Retrieved from http://www. projectliberty.org

Alsaleh, M., & Adams, C. (2006). Enhancing consumer privacy in the liberty alliance identity federation and web services frameworks. In *Privacy Enhancing Technologies* (pp. 59-77). Springer.

Al-Taee, M. A., Sungoor, A. H., Abood, S. N., & Philip, N. Y. (2013). Web-of-Things inspired e-Health platform for integrated diabetes care management. In *Applied Electrical Engineering and Computing Technologies (AEECT), 2013 IEEE Jordan Conference on* (pp. 1-6). IEEE.

Anderson, A. (2005). *A comparison of two privacy policy languages: EPAL and XACML*. Sun Microsystems, Inc. .

Anderson, J. G. (2007). Social, ethical and legal barriers to e-health. *International journal of medical informatics, 76*(5), 480-483.

Andreassen, H. K., Bujnowska-Fedak, M. M., Chronaki, C. E., Dumitru, R. C., Pudule, I., Santana, S., . . . Wynn, R. (2007). European citizens' use of E-health services: a study of seven countries. *BMC public health, 7*(1), 53.

Armando, A., Carbone, R., Compagna, L., Cuellar, J., & Tobarra, L. (2008). Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps. In *Proceedings of the 6th ACM workshop on Formal methods in security engineering* (pp. 1-10). ACM.

Armstrong, D., Kline-Rogers, E., Jani, S. M., Goldman, E. B., Fang, J., Mukherjee, D., . . . Eagle, K. A. (2005). Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome. *Archives of Internal Medicine, 165*(10), 1125-1129.

Ashley, P., Hada, S., Karjoth, G., Powers, C., & Schunter, M. (2003). Enterprise privacy authorization language (EPAL 1.2). *Submission to W3C*.

Ball, M. J., & Lillis, J. (2001). E-health: transforming the physician/patient relationship. *International journal of medical informatics, 61*(1), 1-10.

BBC. (2010). *Has new technology taken over our lives?* Retrieved 03 20, 2015, from http://www.bbc.co.uk/blogs/legacy/haveyoursay/2010/08/has_new_technology_taken_over.html

BeanSoftware. (2014). *Easy Intro to ASP.NET MVC*. Retrieved 02 2015, from http://www.beansoftware.com/ASP.NET-Tutorials/Intro-ASP.NET-MVC.aspx

Benhamou, P.-Y. (2011). Improving diabetes management with electronic health records and patients' health records. *Diabetes and metabolism, 37*, 53-56.

Bertino, E., Paci, F., Ferrini, R., & Shang, N. (2009). Privacy-preserving Digital Identity Management for Cloud Computing. *IEEE Data Eng. Bull., 32*(1), 21-27.

Blaya, J. A., Fraser, H. S., & Holt, B. (2010). E-health technologies show promise in developing countries. *Health Affairs, 29*(2), 244-251. Retrieved from http://content.healthaffairs.org/content/29/2/244.full#ref-1

Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006). Fourth-factor authentication: somebody you know. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 168-178). ACM.

Brostoff, S., Jennet , C., Malheiros, M., & Sasse, M. A. (2013, November). Federated Identity to Access e-Government Services: Are Citizens Ready for This? In *Proceedings of the 2013 ACM workshop on Digital Identity Management* (pp. 97-108). ACM.

Buchanan, W. J. (n.d.). Retrieved from http://billatnapier.com/unit03.pdf

Buchanan, W. J., Anderson, C., Smales, A., Varga, J., Burns, N., Uthmani, O., . . . Lawson, A. (n.d.). Who Would You Trust To Identify You In Accessing Your Health. In *Communications in Computer and Information Science.* Edinburgh: Springer.

Buecker, A., Filip, W., Hinton, H., Hippenstiel, H. P., Hollin, M., Neucom, R., . . . Westman, J. (2005). Federated Identity Management and Web Services Security. *IBM Redbook*.

Buecker, A., Filip, W., Hinton, H., Hippenstiel, H. P., Hollin, M., Neucom, R., . . . Westman, J. (2005, October). Federated identity management and web services security with IBM tivoli security solutions. Retrieved from http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf

Burr, W. E., Dodson, D. F., & Polk, W. T. (2006, April). *Electronic authentication guideline*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Centre for Retail Research. (n.d.). Retrieved from http://www.retailresearch.org/onlineretailing.php

Chadwick, D. W. (2009). Federated Identity Management. In A. Aldani, G. Barthe, & R. Gorrieri (Eds.), *Foundations of Security Analysis and Design V* (pp. 96-120). Berlin Heidelberg: Springer.

Cloud Computing Statistics. (n.d.). Retrieved 01 19, 2015, from http://siliconangle.com/blog/2014/01/27/20-cloud-computing-statistics-tc0114/

Dahbur, K., Mohammad, B., & Tarakji, A. B. (2011). A survey of risks, threats and vulnerabilities in cloud computing. In *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications* (p. 12). ACM.

Dansky, K. H., Thompson, D., & Sanner, T. (2006). A framework for evaluating eHealth research. *Evaluation and program planning, 29*(4), 397-404.

de Melo Silva, L., Araujo, R., da Silva, F. L., & Cerqueira, E. (2014). A new architecture for secure storage and sharing of health records in the cloud using federated identity attributes. In *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on* (pp. 194-199). IEEE.

Delfs, H., & Knebl, H. (2007). Symmetric-key encryption. In *Introduction to Cryptography* (pp. 11-31). Springer.

DiabetesUk. (2015). *Diabetes UK*. Retrieved 04 06, 2015, from http://www.diabetes.org.uk/Guide-to-diabetes/What-is-diabetes/

Ding, Y., & Klein, K. (2010). Model-driven application-level encryption for the privacy of e-health data. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on* (pp. 341-346). IEEE.

Dua, G., Gautam, N., Sharma, D., & Arora, A. (2013). Replay Attack Prevention in Kerberos Authentication Protocol Using Triple Password. *arXiv preprint arXiv:1304.3550*.

Ekonomou, E., Fan, L., Buchanan, W., & Thuemmler, C. (2011). An integrted cloud-based healthcare infrastructure. In *Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on* (pp. 532-536). IEEE.

El Maliki, T., & Seigneur, J.-M. (2007). A survey of user-centric identity management technologies. In *Emerging Security Information, Systems, and Technologies, 2007. SecureWare 2007. The International Conference on* (pp. 12-17). IEEE.

Eurostat. (2014). Retrieved 01 19, 2015, from Eurostat: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

Eysenbach, G. (2001). What is e-health? *Journal of medical Internet research, 3*(2).

Fan, L., Buchanan, W., Thummler, C., Lo, O., Khedim, A., Uthmani, O., . . . Bell, D. (2011). DACAR platfrm for eHealth services cloud. In *Cloud Computing (Cloud), 2011 IEEE International Conference on* (pp. 219-226). IEEE.

Fengou, M., Mantas, G., Lymberopoulos, D., Komninos, N., Fengos, S., & Lazarou, N. (2013). A new framework architecture for nexte generation e-health services. *Biomedical and Health Informatics, IEEE Journal of, 17*(1), 9-18.

Florencio, D., & Herley, C. (2007). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM.

Ford, D. V., Jones, K. H., Verplancke, J.-P., Lyons, R. A., John, G., Brown, G., . . . Couch, T. (2009). The SAIL Databank: building a national architecture for e-health research and evaluation. *BMC Health Services Research, 9*(1), 157.

Gaedke, M., Meinecke, J., & Nussbaumer, M. (2005). A modeling approach to federated identity and access management. In *Special interest tracks and posters of the 14th international conference on World Wide Web* (pp. 1156-1157). ACM.

Gao, H., Guo, X., Chen, X., Wang, L., & Liu, X. (2008). Yagp: Yet another graphical password strategy. In *Computer Security Applications Conference, 2008. ACSAC 2008. Annual* (pp. 121-129). IEEE.

Gomes, H., Cunha, J. P., & Zuquete, A. (2007). Authentication architecture for eHealth professionals. In *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS* (pp. 1583-1600). Springer.

Goodin, D. (2012, 12 10). *25-GPU cluster cracks every standard Windows password in <6 hours|Ars Technica*. Retrieved 02 13, 2015, from http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

Goodner, M., Hondo, M., Nadalin, A., McIntosh, M., & Schmidt, D. (2007). Understanding ws-federation. *Microsoft and IBM*.

Government, S. (2015, January). *e-health.* Retrieved 04 02, 2015, from http://www.ehealth.scot.nhs.uk/wp-content/uploads/Health-Social-Care-Information-Sharing-A-Strategic-Framework-2014-2020.pdf

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding cloud computing vulnerabilities. *Security & privacy, IEEE, 9*(2), 50-57.

Grossman, R. L. (2009). The case for cloud computing. *IT professional, 11*(2), 23-27.

Hall, R. E. (2012). *This Land of Strangers: The Relationship Crisis That Imperisl Home, Work, Politics, and Faith* (1 ed.). Austin, TX: Greenleaf Book Group Press.

Han, S., Skinner, G., Potdar, V., & Chang, E. (2006). A framework oof authentication and authorization for e-health services. In *Proceedings of the 3rd ACM workshop on Secure web services* (pp. 105-106). ACM.

Hardt, D. (2012). *The OAuth 2.0 authorization framework.*

Heck, C., Petry, D., & Marques, J. L. (2013). Development of an e-Health System to Detect Autonomic Neuropathy in Individuals with Diabetes. In *V Latin American Congress on Biomedical Engineering CLAIB 2011 May 16-21, 2011, Habana, Cuba* (pp. 1288-1291). Springer.

HIPAA. (2013). *Health Information Privacy*. Retrieved from http://www.hhs.gov/ocr/privacy

Hsu, J., Huang, J., Kinsman, J., Fireman, B., Miller, R., Selby, J., & Ortiz, E. (2005). Use of e-Health services between 1999 and 2002: a growing digital divide. *Journal of the American Medical Informatics Association, 12*(2), 164-171.

Inzucchi, S., Bergenstal, R., Buse, J., Diamant, M., Ferrannini, E., Nauck, M., . . . Matthews, D. (2012). Management of hyperglycaemia in type 2 diabetes: a patient-centered approach. Position statement of the American Diabetes Association (ADA) and the European Association for the Study of Diabetes (EASD). *Diabetologia, 55*(6), 1577-1596.

Jensen, J. (2011). Benefits of federated identity management- A survey from an integrated operations viewpoint. Berlin Heidelberg: Springer .

Jha, A. K., Doolan, D., Grandt, D., Scott, T., & Bates, D. W. (2008). The use of health information technology in seven nations. *International journal of medical informatics, 77*(22), 848-854.

Josang, A., Fabre, J., Hay, B., Dalziel, J., & Pope, S. (2005). Trust requirements in identity management. In *Proceedings of the 2005 Australasian workshop on Grid computing and e-research-Volume 44* (pp. 99-108). ACM.

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., . . . Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 523-537). IEEE.

Kumar, H., Kumar, S., Joseph, R., Kumar, D., Singh, S. K., Kumar, A., & Kumar, P. (2013). Rainbow table to crack password using MD5 hashing algorithm. In *Information & Communication Technologies (ICT), 2013 IEEE Conference on* (pp. 433-439). IEEE.

Kumari, A., & Kushwaha, D. S. (2011). Kerberos Style Authentication and Authorization through CTES Model for Distributed Systems. In *Computer Networks and Intelligent Computing* (pp. 457-462). Springer.

Landau, S., & Moore, T. (2012). Economic Tussles in Federated Identity Management. *First Monday, 17*(10).

Leandro, M. A., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2012). Multi-tenancy authorization system with federated identity for cloud-based environments using shibboleth. In *ICN 2012, The Eleventh International Conference on Networks* (pp. 88-93).

Leandro, M. A., Nascimento, T. J., dos Santos, D. R., Westphall, C. M., & Westphall, C. B. (2012). Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth. In *ICN 2012, The Eleventh International Conference on Networks* (pp. 88-93).

Li, C.-T., & Hwang, M.-S. (2010). An efficient biometrics-based remote user authentication scheme using smart cards. *Journal of Network and Computer Applications, 33*(1), 1-5.

Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *Parallel and Distributed Systems, IEEE Transactions on, 24*(1), 131-143.

Lohr, H., Sadeghi, A.-R., & Winandy, M. (2010). Securing the e-health cloud. In *Proceedings of the 1st ACM International Health Informatics Symposium* (pp. 220-229). ACM.

Lonea, A. M., Tianfield, H., & Popescu, D. E. (2013). Identity management for cloud computing. In *New Concepts and Applications in Soft Computing* (pp. 175-199). Springer.

Lounis, A., Hadjidj, A., Bouabdallah, A., & Challal, Y. (2012). Secure and scalable cloud-based architecture for e-health wireless sensor networks. In *Computer communications and networks (ICCCN), 2012 21st international conference on* (pp. 1-7). IEEE.

Madsen, P. (Ed.). (2005, December 5). Liberty Alliance project white paper: Liberty ID-WSF people service-Federated social identity. Retrieved March 2014, from

http://www.projectliberty.org/liberty/content/download/387/2720/file/Liberty_Federated_Social_Identity.pdf

Madsen, P., Koga, Y., & Takahashi, K. (2005, November). Federated Identity Management for Protecting Users from ID Theft. In *Proceedings of the 2005 workshop on Digital Identity Management* (pp. 77-83). ACM.

Mair, F. S., May, C., O'Donnell, C., Finch, T., Sullivan, F., & Murray, E. (2012). Factors that promote or inhibit the implementation of e-health systems: an explanatory systematic review. *Bulletin of the World Health Organization, 90*(5), 357-364.

Maler, E., & Reed, D. (2008). The Venn of Identity. *IEEE Security and Privacy, 6*(2), 16-23.

Mantas, G., Lymberopoulos, D., & Komninos, N. (2009). Integrity mechanism for ehealth tele-monitoring system in smart home environment. In *Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE* (pp. 3509-3512). IEEE.

Mazzoleni, P., Crispo, B., Sivasubramanian, S., & Bertino, E. (2008). XACML policy integration algorighms. *ACM Transactions on Information and system security (TISSEC), 11*(1), 4.

Mbanaso, U. M., Cooper, G., Chadwick, D. W., & Proctor, S. (2006). Privacy preserving trust authorization framework using XACML. In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks* (pp. 673-678). IEEE Computer Society.

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Mercuri, R. T. (2004). The HIPAA-potamus in health care data security. *Communications of the ACM, 47*(7), 25-28.

Microsoft. (2015). *ASP.NET*. Retrieved 02 2015, from http://www.asp.net/mvc

Morgan, R., Cantor, S., Carmody, S., Hoehn, W., & Klingenstein, K. (2004). Federated Security: The Shibboleth Approach. *Educause Quarterly, 27*(4), 12-17.

National strategy for Trusted Identities in Cyberspace. (2011, April). Retrieved October 20, 2014, from http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Ni, Q., Bertino, E., Lobo, J., Brodie, C., Karat, C.-M., Karat, J., & Trombeta, A. (2010). Privacy-aware role-based access control. *ACM Transactions on Information and System Security (TISSEC), 13*(3), 24.

Oladimeji, E. A., Chung, L., Jung, H. T., & Kim, J. (2011). Managing security and privacy in ubiquitous eHealth information interchange. In *Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication* (p. 26). ACM.

Parliament, B. (1998). *Data protection act of 1998.*

Peyton, L., Hu, J., Doshi, C., & Seguin, P. (2007). Addressing privacy in a federated identity management network for ehealth. In *Management of eBusiness, 2007. WCMeB 2007. Eighth World Congress on the* (p. 12). IEEE.

Riedl, B., Grascher, V., & Neubauer, T. (2008). A Secure e-Health Architecture based on the Appliance of Pseudonymization. *Journal of Software, 3*(2), 23-32.

Rimal, B. P., Choi, E., & Lumb, I. (2009). A taxonomy and survey of cloud computing systems. In *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on* (pp. 44-51). IEEE.

Rouse, M. (2011). *Model-View-Controller*. Retrieved 02 2015, from http://whatis.techtarget.com/definition/model-view-controller-MVC

Rozenblum, R., Jang, Y., Zimlichman, E., Salzberg, C., Tamblyn, M., Buckeridge, D., . . . Tamblyn, R. (2011). A qualitative study of Canada's experience with the implementation of electronic health information technology. *Canadian Medical Association Journal, 183*(5), 281-288.

Russello, G., Dong, C., & Dulay, N. (2008). A workflow-based access control framework for e-health applications. In *Advanced Information Networking and Applications-Workshops, 2008. AINAW 2008. 22nd International Conference on* (pp. 111-120). IEEE.

Sanchez, M., Lopez, G., Gomez-Skarmeta, A. F., & Canovas, O. (2008). using microsoft office infopath to generate XACML policies. In *E-Business and telecommunication networks* (pp. 134-145). Springer.

Shim, S. S., Bhalla, G., & Pendyala, V. (2005). Federated identity management. *Computer, 38*(12), 120-122.

Singh, S. P., & Maini, R. (2011). Comparison of data encryption algorithms. *International Journal of Computer Science and Communication, 2*(1), 125-127.

Spanakis, E. G., Chiarugi, F., Kouroubali, A., Spat, S., Beck, P., Asanin, S., . . . Thestrup, J. (2012). Diabetes management using modern information and communication technologies and new care models. *Interactive journal of medical research, 1*(2).

Sudha, M. (2012). Enhanced security framework to ensure data security in cloud computing using cryptography. *Advances in Computer Science and its Applications, 1*(1), 32-37.

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management, 30*(2), 109-116.

Sun, S.-T., & Beznosov, K. (2012). the devil is in the (implementation) details: an empirical analysis of oauth sso systems. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 378-390). ACM.

Thakur, J., & Kumar, N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering, 1*(2), 6-12.

Verma, O., Agarwal, R., Dafouti, D., & Tyagi, S. (2011). Peformance analysis of data encryption algorithms. In *Electronics Computer Technology (ICECT), 2011 3rd International Conference on* (pp. 399-403). IEEE.

Wang, Y.-y., Liu, J.-y., Xiao, F.-x., & Dan, J. (2009). A more efficient and secure dynamic ID-based remote user authentication scheme. *Computer communications, 32*(4), 583-585.

Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. *Health informatics journal, 18*(3), 191-201.

Wilson, E. V., & Lankton, N. K. (2004). Modeling patients' acceptance of provider-delivered e-health. *Journal of the American Medical Informatics Association, 11*(4), 241-248.

Yan, L., Rong, C., & Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In *Cloud Computing* (pp. 167-177). Springer.

Yang, G., Wong, D. S., Wang, H., & Deng, X. (2008). Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences, 74*(7), 1160-1172.