Cloud Computing in Healthcare and Privacy

COM S 559, Dr. Wensheng Zhang

Term Project Report

Yu-Pin Liang

Abstract:

There are many advantages for healthcare professionals turning toward cloud computing. Many institutions have replaced the traditional system with more novelty cloud computing services in recent years. However, a feasible method for storing personal health records on a cloud server without any data privacy concerns has raised a critical issue. Moreover, cloud providers need to deal with helping healthcare services exchange information with the highest security approach. Recent technology provides some alternative approaches for cloud services to protect sensitive data.

Research Goal: Review (1) the challenge for healthcare organizations to shift from the paper-based medical record to the electronic medical system, (2) the challenge for healthcare organizations to utilize electronic records by deploying Cloud Computing, and (3) how sensitive data can be protected in Cloud Computing

Keywords: electronic health record (EHR), cloud computing, privacy, Neural Network

Problem description

1. Introduction and Background

1.1 Traditional Medical Record to Novel Electronic Health Records (EHR)

Healthcare is now progressively transferring medical record types from traditional handwritten hard paper copies to the novel EHR manner. Maintaining paper-based records is time-consuming with low flexibility (Institute of Medicine (U.S.). Committee on Improving the Patient Record., Dick, Steen, & Detmer, 1997). Moreover, remotely accessing a patient's health record from another location was almost impossible in the past time. By using EHR, healthcare can structurally manage data by reducing the search time for medical personnel and improving the overall medical quality. Physicians can browse all the medical records of a specific patient and help make medical decisions without knowing (Stausberg, Koch, Ingenerf, & Betzler, 2003). EHR brings significant benefits to both sides of healthcare providers and patients. In this

stage, most of the EHR systems are still stored and built in the local-based database system without any Cloud involvement. Data can be accessed and exchanged locally and transferred by an authorized user (Office of the National Coordinator for Health Information Technology & Human, 2015). However, there are some barriers to adopting the EHR in each organization, including (Ajami & Arab-Chadegani, 2013) financial risk, software-related problems, hardware-related issues, unfamiliar programming, and data-related technical errors. These are significant reasons for an organization being unwilling to replace the paper-based system with EHR or slow replacements.

1.2 Cloud and Electronic Health Records (EHR)

Nowadays, people are trying to access medical records in real time everywhere. The record should include not only basic personal medical information but also detailed and high-quality information. Cloud computing has become more prominent in recent years. Cloud computing helps medical institutions manage data and improve the adoption of electronic health records (EHR) (Kanagaraj & Sumathi, 2011). Cloud service is also capable of providing solutions for barriers that healthcare may have, and developers can solve the technical issues—users' routine changes to upload the data to the Cloud without concerning the system's sustainability. For example, Cloud service is more affordable to maintain compared to searching for professionals to manage and find out the technical issues. Furthermore, the Cloud can create multidisciplinary cooperation and enhance data integration. There are three different distribution models for cloud computing services (Cervone, 2010; Han, 2010).

- Software as a Service (SaaS) - The applications (e.g., EHRs) are hosted by a cloud service developer and made available to clients over a network, typically the Internet.
- Platform as a Service (PaaS) - The development tools (e.g., O.S. systems) are provided in the Cloud and accessed through a browser. With PaaS, developers can build web

applications without installing any tools on their computers and then deploy those applications without specialized administrative skills.

- Infrastructure as a Service (IaaS) - The cloud user outsources the equipment to support operations, including storage, hardware, servers, and networking components. The cloud service provider owns the equipment and is responsible for housing, running, and maintaining it (e.g., Amazon EC2). The client typically pays on a per-user basis

The U.S. National Institute of Standards and Technology (NIST) listed four models for deploying cloud computing (Mell & Grance, 2011).

- Private Cloud - A proprietary network or a data center supplies hosted services to a particular group.
- Public Cloud - A cloud service provider makes resources (applications and storage) available to the general public over the Internet.
- Community Cloud - The cloud infrastructure is shared by several organizations and supports a specific community with common concerns (e.g., mission, security requirements, policy, and compliance considerations).
- Hybrid Cloud - An organization provides and manages resources within its data center and has others provided externally, such as Microsoft HealthVault.

According to the previous reviews study (Griebel et al., 2015), which investigated what domains are for healthcare using data with Could in 102 articles, 34 studies were related to Telemedicine/Teleconsultation, 15 studies were related to Medical Imaging, 15 studies were related to Public health and patients' self-management, 13 studies were related to the Hospital management/clinical information systems, seven studies were related to the Therapy, eight studies were related to the Secondary use of data. Cloud computing can even help save patient lives in emergency circumstances by quickly evaluating and diagnosing patients'

electrocardiography (Fujita et al., 2013). Based on the pieces of evidence, Cloud computing was shown to have high demands and can be utilized in many aspects. Amazon's Web Service (AWS) is the first agent to collect healthcare information from healthcare data storage applications and store it in Amazon S3 infrastructure (Seh et al., 2020).

1.3 Challenges of Deploying Cloud in Healthcare Data

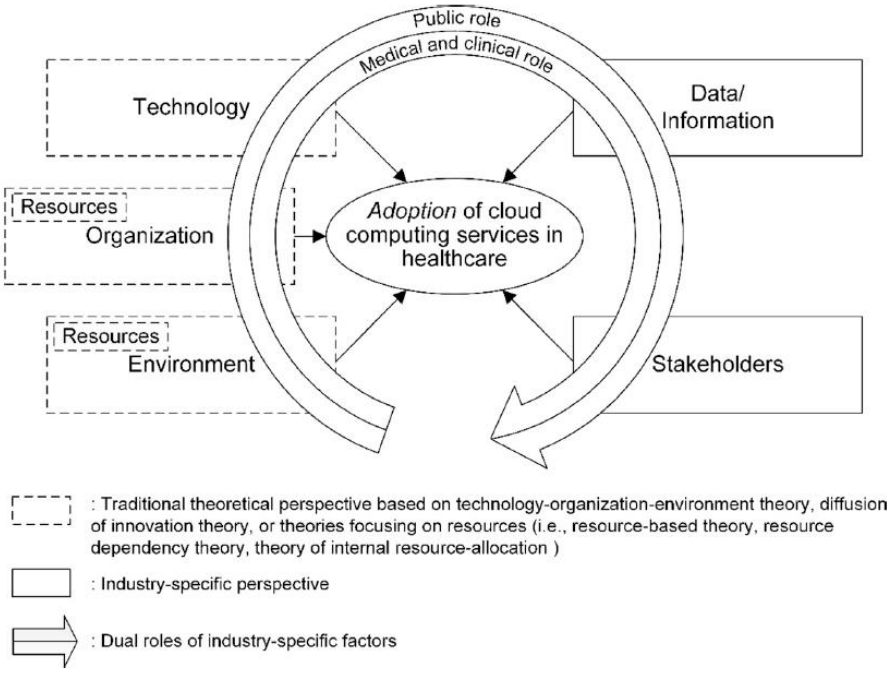
However, there are some challenges in applying cloud services to patients' sensitive information. The insufficiency of the user's trust and lack of good regulations for adopting cloud services still need to be solved. Previous studies indicated that the challenges for users trusting the cloud service include service availability, data lock-in, data confidentiality and audibility, data transfer bottlenecks, performance unpredictability, scalable storage, bugs in large-scale distributed systems, scaling quickly, reputation fate sharing, and software licensing (A. et al., 2011). Data jurisdiction, data interoperability, and some legal issues are also potential significant concerns resulting from the U.S. Health Insurance Portability and Accountability Act (HIPAA) restricts companies from disclosing personal health data to non-affiliated third parties unless specific contractual arrangements have been put in place (M. H. Kuo, Kushniruk, & Borycki, 2011). Also, from an interview-based study, interviewees commonly showed concern about uploading sensitive data to the Cloud, and most of the subjects preferred local storage over the Cloud (Ion, Sachdeva, Kumaraguru, & Čapkun, 2011).

2. Solutions for Privacy issues in the Cloud

2.1 A Theoretical Framework and Architecture

Moreover, Gao et al. (F. Gao, Thiebes, & Sunyaev, 2016) examined the previous studies by fitting into the H, O, T model, which was human organization fit (HO-fit), human technology fit (HT-fit), organization technology fit (OT-fit), and irrelevant. On the other hand,

Gao and Sunyaev (Fangjian Gao & Sunyaev, 2019) raised a conceptual framework of determinant factors for cloud computing adoption in healthcare contexts and proposed future research suggestions.



(Fangjian Gao & Sunyaev, 2019)

2.2 A Feasible and Practical Framework

Khan et al. proposed a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs) (Khan, Ali, Abbas, & Haldar, 2014). Authors secured the inter-sensor communication by multibiometric-based key generation scheme in WBANs. All the sensitive data were only stored in the private Cloud of the institution. The result indicated that the frameworks not only protected the sensitive data but also with a highly efficient key generation mechanism. Kundalwal et al. (Kundalwal, Singh, & Chatterjee, 2018) provided a security framework based on the ruleset to protect the data, and only registered users were available to access the sensitive data. The ruleset-based framework combining a data perturbation technique also protects data being attacked. Fabian et al. (Fabian, Ermakova, & Junghanns, 2015) proposed a novel inter-organizational data sharing with an attribute-based

encryption model and assumed Clouds were semi-trusted. By selective access authorization and cryptographic secret sharing, data can be split into multiple Clouds and weaken the Cloud provider's ability to own the data. Li et al. (Li, Yu, Cao, & Lou, 2011) also proposed an attributed-based hierarchies framework combined with the Authorized Private Keyword Search (APKS) to reduce privacy exposure. Overall, attributed-based encryption is still the standard and primary approach for data security in the Cloud. All the studies above provided practical approaches to help Cloud developers enhance data security in the Cloud.

2.3 Neural Network and Cloud Security

Abdelsalam et al. (Abdelsalam, Krishnan, Huang, & Sandhu, 2018) proposed a Convolutional Neural Network (CNN) model to determine the malware in IaaS. The author applied both two-dimensional and three-dimensional convolutional neural networks with a substantial amount of the input data from the mean of the hypervisor for each of the processes. As a result, the three-dimensional convolutional neural networks can better identify the malware with an overall accuracy of 90% compared to the two-dimensional convolutional neural networks with an overall accuracy of 79%. Ong et al. (Ong, Qiao, Routray, & Raphael, 2017) proposed a context-aware DLP (Data Loss Prevention) system. They trained an LSTM model to detect sensitive content in almost real-time. Not only by detecting sensitive information using a passive method which is sorting the context by dictionary-based, but the LSTM model could also provide an active identification process of the sensitive data by using the contexed-aware strategy. As a result, the LSTM could detect sensitive information in an overall less than 100 milliseconds, which meant almost being recognized in real-time. Zhang et al. proposed (Zhang et al., 2021) a model to deal with the conflict between the data owner and the model owner. The model SGX (Citadel) could achieve the goal for both the data owner and the model owner side with the model scalable ability by zero-sum masking to prevent data and model leakage. The result showed that the performance of this new model has, in general,

1.7 times slowed down compared to the existing model. The strength of this study is that they successfully deployed a new model to keep data privacy and model privacy, especially since this was also the first work in dealing with this kind of conflict.

reference

Abdelsalam, M., Krishnan, R., Huang, Y., & Sandhu, R. (2018, 2-7 July 2018). *Malware Detection in Cloud Infrastructures Using Convolutional Neural Networks.* Paper presented at the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD).

Ajami, S., & Arab-Chadegani, R. (2013). Barriers to implementing Electronic Health Records (EHRs). *Mater Sociomed, 25*(3), 213-215. doi:10.5455/msm.2013.25.213-215

Cervone, H. F. (2010). An overview of virtual and Cloud computing. *OCLC Systems & Services: International digital library perspectives*.

Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems, 48*, 132-150. doi:https://doi.org/10.1016/j.is.2014.05.004

Fujita, H., Uchimura, Y., Waki, K., Omae, K., Takeuchi, I., & Ohe, K. (2013). Development and clinical study of mobile 12-lead electrocardiography based on cloud computing for cardiac emergency. *Stud Health Technol Inform, 192*, 1077.

Gao, F., & Sunyaev, A. (2019). Context matters A review of the determinant factors in the decision to adopt cloud computing in healthcare. *International Journal of Information Management, 48*, 120-138. doi:https://doi.org/10.1016/j.ijinfomgt.2019.02.002

Gao, F., Thiebes, S., & Sunyaev, A. (2016, 5-8 Jan. 2016). *Exploring Cloudy Collaboration in Healthcare: An Evaluation Framework of Cloud Computing Services for Hospitals.* Paper presented at the 2016 49th Hawaii International Conference on System Sciences (HICSS).

Griebel, L., Prokosch, H.-U., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., . . . Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC Med Inform Decis Mak, 15*, 17-17. doi:10.1186/s12911-015-0145-7

Han, Y. (2010). On the clouds: a new way of computing. *information technology and libraries, 29*(2), 87-92.

Institute of Medicine (U.S.). Committee on Improving the Patient Record., Dick, R. S., Steen, E. B., & Detmer, D. E. (1997). *The computer-based patient record: an essential technology for health care* (Rev. ed.). Washington, D.C.: National Academy Press.

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011). *Home is safer than the Cloud! Privacy concerns for consumer cloud storage*. Paper presented at the Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania. https://doi.org/10.1145/2078827.2078845

Kanagaraj, G., & Sumathi, A. C. (2011, 8-9 Dec. 2011). *Proposal of an open-source Cloud computing system for exchanging medical images of a Hospital Information System.* Paper presented at the 3rd International Conference on Trendz in Information Sciences & Computing (TISC2011).

Khan, F. A., Ali, A., Abbas, H., & Haldar, N. A. H. (2014). A Cloud-based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks. *Procedia Computer Science, 34*, 511-517. doi:https://doi.org/10.1016/j.procs.2014.07.058

Kundalwal, M. K., Singh, A., & Chatterjee, K. (2018, 12-13 Oct. 2018). *A Privacy Framework in Cloud Computing for Healthcare Data.* Paper presented at the 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN).

Kuo, A. M. (2011). Opportunities and challenges of cloud computing to improve health care services. *Journal of medical Internet research, 13*(3), e67. doi:10.2196/jmir.1867

Kuo, M. H., Kushniruk, A., & Borycki, E. (2011). Can Cloud computing benefit health services? - a SWOT analysis. *Stud Health Technol Inform, 169*, 379-383.

Li, M., Yu, S., Cao, N., & Lou, W. (2011, 20-24 June 2011). *Authorized Private Keyword Search over Encrypted Data in Cloud Computing.* Paper presented at the 2011 31st International Conference on Distributed Computing Systems.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Office of the National Coordinator for Health Information Technology, D. o. H., & Human, S. (2015). 2015 Edition Health Information Technology (Health I.T.) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health I.T. Certification Program Modifications. Final rule. *Fed Regist, 80*(200), 62601-62759.

Ong, Y. J., Qiao, M., Routray, R., & Raphael, R. (2017, 25-30 June 2017). *Context-Aware Data Loss Prevention for Cloud Storage Services.* Paper presented at the 2017 IEEE 10th International Conference on Cloud Computing (CLOUD).

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel), 8*(2), 133. doi:10.3390/healthcare8020133

Stausberg, J., Koch, D., Ingenerf, J., & Betzler, M. (2003). Comparing paper-based with electronic patient records: lessons learned during a study on diagnosis and procedure codes. *J Am Med Inform Assoc, 10*(5), 470-477. doi:10.1197/jamia.M1290

Zhang, C., Xia, J., Yang, B., Puyang, H., Wang, W., Chen, R., . . . Yan, F. (2021). *Citadel: Protecting Data Privacy and Model Confidentiality for Collaborative Learning*. Paper presented at the Proceedings of the ACM Symposium on Cloud Computing, Seattle, WA, USA. https://doi.org/10.1145/3472883.3486998