doi: 10.17234/INFUTURE.2015.15 Preliminary communication

Legal Compliance and Technical Capability for Privacy-sensitive Data Protection in the Cloud

Eun G. Park
McGill University, Canada
eun.park@mcgill.ca

Summary

This study aims to investigate if both the legal compliance and technical capability are sufficient to protect privacy-sensitive data and records at privacy-sensitive institutions in the cloud. The study examines the applicability of current legal requirements in Canada, the United States and Europe to the cloud environments. We also conduct a case study to test the implementation of current privacy-preserving techniques to protect privacy information at selected government agencies or health institutions.

Keywords: privacy, security, cloud computing, security assessment

Introduction

Many privacy-preserving techniques have been developed to address the privacy issues in different data sharing scenarios that are used in the field related to records and data management (Fung et al., 2010; Mohammed et al., 2013; Park, 2014). The emergence of cloud computing has significantly improved the potential of sharing records and data. However, the major obstacle to adopting this technology in the public sector is a lack of trust in sufficient security and privacy protection. Research has shown that simply removing explicit identification information of patients, participants or citizens, including the person's name, social insurance number, telephone number, and address, is insufficient for privacy protection. Therefore, there is a need to assess the privacy-preserving techniques and tools that are available and popular in the field and test how well these techniques can actually help protect privacy and security to records managers at the real settings (e.g. privacy and security sensitive institutions, such as government agencies or health institutions). Government agencies hold a large amount of citizens' data with their privacy information on the data (e.g. social insurance number, etc.). Health agencies also create, use and house a large amount of patients' data with their health information, such as blood type, disease, drug, etc. These institutions tend to be more sensitive with privacy information in their data sets. It is important to examine whether legal requirements as minimum requirements that are based on government privacy guidelines are satisfactory from a viewpoint of records management in implementing privacy-preserving techniques and tools at different institutional settings in re-

ality. In addition, there is a pressing need to examine at what extent these techniques and tools can actually help reduce security and privacy risks in records and data management practices in the cloud at the institutional contexts.

Objectives of the Study

The objectives of this study are: (1) to identify the security and privacy challenges of hosting person-specific information on cloud; (2) to evaluate the state-of-the-arts privacy-preserving techniques and their applicability to the cloud environment; and (3) to study the readiness of the health and government agencies of the technological shift to the cloud.

Method

To answer the first objective, this study examines the current legal guidelines of privacy management in Canada, the United States and Europe, especially, new laws and guidelines on the cloud and draw the privacy preserving and security criteria that are driven by literature review. This study takes a close look at the (e.g. Personal Information Protection and Electronic Document Act (PIPEDA), Privacy Act of 1974, Health Insurance Portability and Accountability Act (HIPAA) and Privacy Act of 1974 and does a comparative analysis of the three acts' requirements on privacy protection. In addition, new acts, notices or polices related to the cloud are examined to identify how to apply to the cloud environments in Canada, the United States, and Europe (e.g. Privacy Impact Assessments for Personal Information Banks, Information Sharing Agreements for personal information sharing, Office of the Privacy Commissioner of Canada, Information Breach Protocol, etc.).

To answer the second objective, this study examines whether the available security and privacy-preserving techniques and tools can meet the criteria at the practical sites, especially government and health agencies in Canada or the United States. The security and privacy-preserving techniques and tools to review include the following four approaches: single provider and single release, sequential release, collaborative data integration, RFID trajectory data release, etc. In addition, we developed one security technique to be applicable to the cloud environment.

Further, we plan to conduct a case study at government agencies or health agencies or government to examine whether the legal requirements and technical capability are met at the chosen sites. Based on the findings at the chosen agencies, this study plans to make suggestions on how to manage security and privacy risks in records and data management at government agencies or health institutions in Canada.

Progress to Date and Expectations

This study is in progress. To date, laws and cases on the applicability to the cloud have been reviewed. Literature review on the applicability of laws and regulations to the cloud are in progress. Further, based on the literature review, the privacy preserving and security criteria will be developed and the popular privacy-preserving and security techniques have being in progress of review. To test the privacy preserving and security criteria, we are contacting a couple of sites for having access to their data and plan to conduct a case study at the chosen sites. We plan to complete this study by the end of 2015.

Acknowledgements

This study is part of InterPARES Trust project.

References

Fung, B. C. M., Wang, K., Fu, A. W.-C., and Yu, P. S.. Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques, ser. Data Mining and Knowledge Discovery. 376 pages, Chapman & Hall/CRC, August 2010.

Mohammed, N., Jiang, X., Chen, R., Fung, B. C. M., and Ohno-Machado. L. Privacy-preserving heterogeneous health data sharing. Journal of the American Medical Informatics Association (JAMIA), 20(3):462-469, May 2013. BMJ.

Park, E. G. 2014. InterPARES Trust 2nd International Symposium, October 17, 2014: A Privacy-preserving Approach for Records Management in Cloud Computing. Victoria, BC: University of Victoria Library.