Distributed, Highly-Scalable, Sticky Policies Implementation for Healthcare

Grzegorz Spyra , William J Buchanan,
Elias Ekonomou
Centre for Distributed Computing Networks and Security
Edinburgh Napier University,
g.spyra@napier.ac.uk
w.buchanan@napier.ac.uk
e.ekonomou@napier.ac.uk

This paper outlines some of the key functional characteristics required for the creation of secure identity and identity meta-data framework hosted in the cloud. Many information infrastructures are moving to the cloud, and thus require increased protection for not only malicious outsiders, but seek for new safeguards that will protect the information independently from the Cloud Service Provider security features.

Infection, Informatics, Healthcare Improvement, Antimicrobial, Outcomes.

1. INTRODUCTION

This paper outlines some of the key functional characteristics required for the creation of secure identity and identity meta-data framework hosted in the cloud. Many information infrastructures are moving to the cloud, and thus require increased protection for not only malicious outsiders, but seek for new safeguards that will protect the information independently from the Cloud Service Provider (CSP) security features [1].

Any solution should address:

● Sharing and Data Protection Act.

Whilst the solution should address major personal and sensitive personal data protection concerns, they should also combine well-established open standards to deliver an easily adaptable model for e-Health, especially for simplicity and to support modern data sharing services, whilst respecting the Data Protection Act (DPA) principles.

● Personal Identifiable Information (PII).

This includes any personal information that cannot flow without governance [2]. Access to such information requires the data owner's consent [3]. In order to deliver cloud services that would respect legal aspects of data protection, the data sharing system require a move to digital identity centric models.

● Level of Assurance (LoA).

This guaranties a defined quality of digital identity [4]. It is an essential criteria on whether a person can access data in the cloud, or not. Furthermore the data independently from native CSP security system has to enforce restrictions by carrying the necessary decision rules with it.

● Location and consistent access issues.

Information, once released into the cloud, may be stored at several locations, across several jurisdictions and can be hosted by various cloud services. These may not necessarily share the information required to take legitimate access control decisions.

2. BACKGROUND & RELATED WORK

Some projects focus on creating a framework capable of hosting Big Data in the Cloud. Building a platform for electronic health systems is a challenging task, due to the need to support legacy systems which may be using various database types. Such data repositories cannot be simply migrated to cloud services.

The Microsoft HealthVault project defines in detail, several data schemas that can represent legacy medical database structures. eXtensible Markup Language (XML) data format used by Microsoft to represent data stored in native medical systems is easy to integrate with modern systems. Data schemas covered by Microsoft HealthVault can be effectively adapted for specific medical institutions.

Some have also used XML solutions to support legacy systems in health-care, education industry and so on [5, 6].

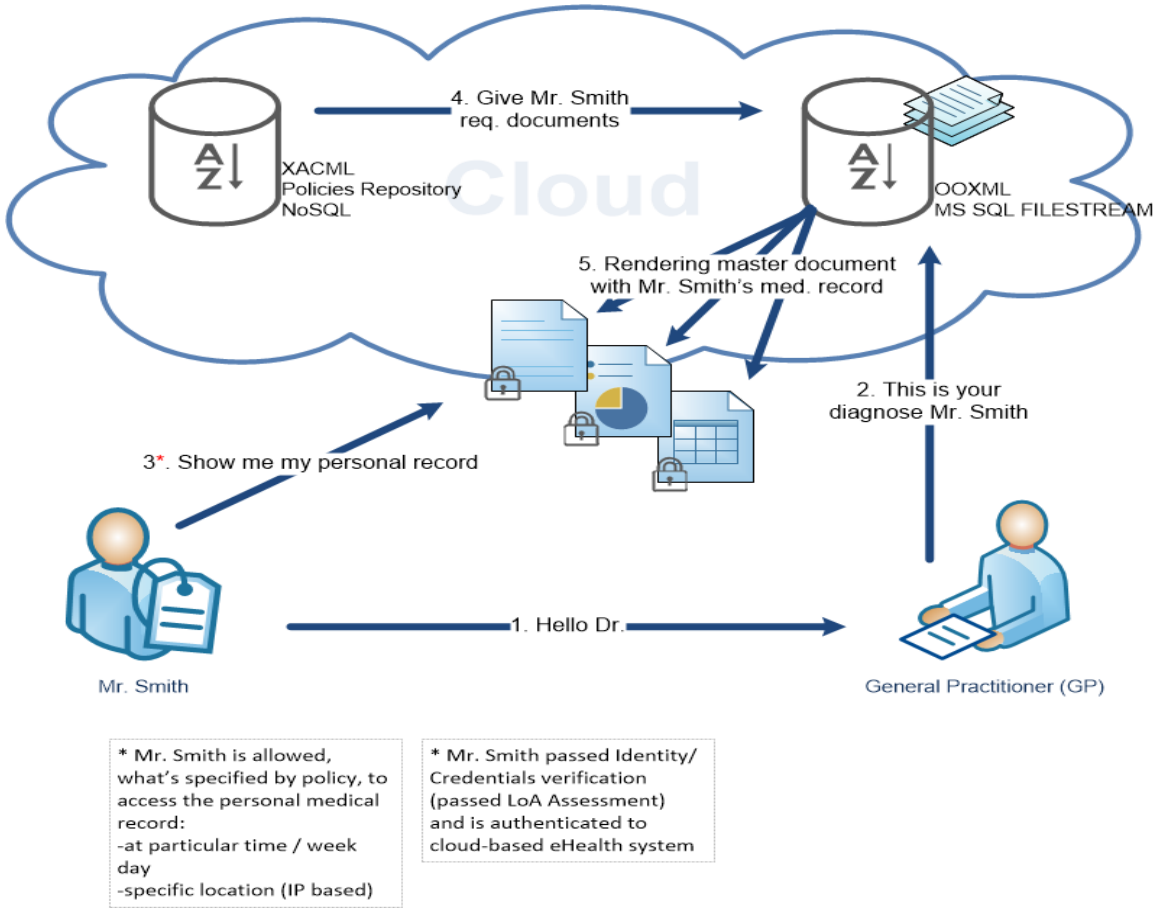

Figure 1: *Sticky-policies granularly control access over patient's medical record*

3. IDENTITY META-DATA

To build a digital identity-oriented system, where a person ─ an identity owner ─ is responsible and accountable for owning the data as well as data access, we need to look at the various steps of the processes starting from person *identification*, through to *authentication* (AuthN); *authorization* (AuthZ); and *accounting.*

These systems need to efficiently find relevant pieces of information among a large volume of other records. Highly efficient identity-centric framework can for example utilize JSON (JavaScript Object Notation) framework [7], which is based mostly on open standards but is efficiently utilized in commercial implementations.

3.1 Sticky Policy

Sticky policies group rules define *who* can access the, *when, where and how*. Unlike other access control models, the policy is *'attached'* to the data.

Sticky policy added to a patient medical report (see Figure 1) would cover a data owner consent and define the rights to process that data. This access control model would secure Personal Identifiable Information (PII) with high accountability: where each personal data access attempt is a subject of extensive auditing [8]. Furthermore, the complete implementation of the sticky policy model supports several security auditing functions. Any security breach or a data leakage incident is reported by sticky policies framework and can be tracked ─ with potential legal consequences ─ as policies can be combined to technically enforce the Data Protection Act (DPA) principles. Data-owners pre-selected, approved policies follow data released into the Cloud and specify how the sticky policy can be interpreted by the Trust Authority (TA) [9]. Information about the TA is attached to the policy and is passed to the Service Provider (SP) (i.e. eHealth system).

An XML schema that can store sticky-policy definition can be integrated into identity meta-data. Furthermore, some authors successfully integrated eXtensible Access Control Mark-up Language (XACML) representing sticky policy with Office Open XML (OOXML) document representing any information related to identity owner. XACML is a Sticky-policies based standard from OASIS, where the policy model defines tuple relationships where subject performs particular action against object.

3.2 OOXML policy wrapper Framework

The OOXML standard is mostly build on top of XML files, which reference each other to form a single document. XML files can be supplemented with other reach files to deliver graphic, multimedia and other elements. OOXML data format can deliver data integrity using internal elements hashing, while confidentiality can be assured by ZIP wrapper password protection and content encryption.

These techniques are sufficient to protect content that does not leave corporate network. However, when leaked, this built-in protection may not be sufficient for personal data. Cloud-based identity meta-data sharing solution ─ in order to utilize OOXML standard ─ would require additional safeguards from service providers. By hosting and secure delivery of *'information piece'* rather than the entire data document, data structured using this XML-based standard can be well protected.

3.3 Framework

This work focuses on the solution that can be used by medical institutions as a part of an e-Health programme. Implemented as a simple data-hosting platform, this approach can be leveraged for all types of enterprises and organizations that seek for secure data hosting in the cloud. The complete work is based on thorough field research around technologies capable of securing personal data in the cloud. That includes XML schemas and ontologies, data anonymization and obfuscation, selected cryptographic techniques, AuthZ, AuthN and Office Open XML (OOXML) standard. Work includes high level design details as well as basic evaluation framework and testing results.

4. SUMMARY

The combination of XACML, Security Assertion Markup Language (SAML), OOXML and optionally Identity-Based Encryption (IBE) delivers functionality for Cloud-based access control framework where Personal Identifiable Information can be securely stored in a public cloud space (see Figure 1). These technologies support several best security practices for access control systems [10].

We suggest that systems suitable for medical institutions, organizations and enterprises should provide such security functionality as: break-glass temporary access granted, based on policy owned by subject, dynamic access key-revocation, as well as key-lease, for a constraint period of time [9, 11].

5. REFERENCES

[1] Mowbray, M., Pearson, S., & Shen, Y. (2010). Enhancing privacy in cloud computing via policy-based obfuscation. The Journal of Supercomputing, 61(2), 267-291.

[2] Zhou, L., Varadharajan, V., & Hitchens, M. (2014). Cryptographic Role-Based Access Control for Secure Cloud Data Storage Systems. In S. Nepal & M. Pathan (Eds.), Security, Privacy and Trust in Cloud Systems (pp. 313-344). Berlin, Heidelberg: Springer Berlin Heidelberg.

[3] Kroes, N. How we're boosting trust in the cloud, post PRISM - European Commission.

[4] Burr, W. E., Dodson, D. F., & Polk, W. T. (2006). Electronic Authentication Guideline. NIST Special Publication 800-63. Version 1.0.2 (April 2006)

[5] Jain, A., & Farkas, C. Ontology-Based Authorization Model for XML Data in Distributed Systems. In Digital Rights Management (pp. 210-236). IGI Global.

[6] Le, X. H.; Doll, T.; Barbosu, M.; Luque, A. & Wang, D. An enhancement of the Role-Based Access Control model to facilitate information access management in context of team collaboration and workflow Journal of Biomedical Informatics, 2012, 45, 1084 – 110

[7] Jones, M.B. A JSON-Based Identity Protocol Suite. Information Standards Quarterly, 26 (3), 2014

[8] Mont, M. C.; Pearson, S. & Bramhall, P. Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services Proceedings of the 14th International Workshop on Database and Expert Systems Applications, IEEE Computer Society, 2003.

[9] Pearson, S., Mont, M. C., & Kounga, G. (2011). Enhancing Accountability in the Cloud via Sticky Policies. Secure and Trust Computing, Data Management, and Applications Communications in Computer and Information Science, 187, 146-155.

[10] Hommel, W. (2005). Using XACML for Privacy Control in SAML-Based Identity Federations. In J. Dittmann, S. Katzenbeisser, & A. Uhl (Eds.), Lecture Notes in Computer Science (Vol. 3677, pp. 160-169). Munich: Springer Berlin Heidelberg.

[11] Simone Fischer-Hübner, Penny Duquenoy, Marit Hansen, Ronald Leenes, G. Z. (2011). Privacy and Identity Management for Life. (S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang, Eds.) (6th ed., p. 352). Helsingborg, Sweden: Springer Berlin Heidelberg.