Chapter 76
Cloud-Based Identity and Identity Meta-Data:
Secure and Control of Data in Globalization Era

Grzegorz Spyra
Edinburgh Napier University, UK

Peter Cruickshank
Edinburgh Napier University, UK

William J Buchanan
Edinburgh Napier University, UK

Elias Ekonomou
Edinburgh Napier University, UK

ABSTRACT

This paper proposes a new identity, and its underlying meta-data, model. The approach enables secure spanning of identity meta-data across many boundaries such as health-care, financial and educational institutions, including all others that store and process sensitive personal data. It introduces the new concepts of Compound Personal Record (CPR) and Compound Identifiable Data (CID) ontology, which aim to move toward own your own data model. The CID model ensures authenticity of identity meta-data; high availability via unified Cloud-hosted XML data structure; and privacy through encryption, obfuscation and anonymity applied to Ontology-based XML distributed content. Additionally CID via XML ontologies is enabled for identity federation. The paper also suggests that access over sensitive data should be strictly governed through an access control model with granular policy enforcement on the service side. This includes the involvement of relevant access control model entities, which are enabled to authorize an ad-hoc break-glass data access, which should give high accountability for data access attempts.

INTRODUCTION

Current technology and business trends are moving organizations, institutions and enterprises into the cloud, although many are aware of the risks, exemplified by the recent events which show that even highly protected personal data can be seized for processing, without the data owner's consent and knowledge (Kroes, 2013).

DOI: 10.4018/978-1-5225-0159-6.ch076

The risks increase: the latest leaks (January, 2014) by Edward Snowden show that the USA's National Secure Agency (NSA) is involved in an on-going project called Penetrating Hard Targets (PHT), which aims to develop a super quantum computer enabling US government to decrypt information (Rich & Gellman, 2014). As this technology will inevitably become widespread over time, the conclusion has to be that any Cloud-based model or system that will process or store personal data will require not only multiple safeguards to protect the confidentiality, but also should deliver high accountability enforced by governments where personal data is protected by law.

Cloud-based services can often provide data security that delivers data protection sufficient to secure the data from outsider threats, but they cannot protect it from rogue Cloud Service Provider (CSP) employees (Mowbray, Pearson, & Shen, 2010). Currently, personal data stored by schools, hospitals and other organizations often does not meet baseline safeguards required to hold such data and is often not ready for Cloud-computing era (Hölbl, 2011).

In health care, medical organizations store and process sensitive personal information, and also need access to sensitive data (X. Chen, 2004) to save their patients life at any time, without technological and jurisdictional constraints (OECD, 2013b). Unfortunately, access to such data is mostly restricted to one institution or very often a single building.

In this paper, we define personal data as a piece of information that identifies an individual directly or indirectly (OECD, 2013a).

Even when personal data is stored and processed within secure and well-defined boundaries, problems can arise because there is no oversight by the data owner (i.e., the patient): there are strong indications that Personal Health Records (PHR) owners would also like to have full access to their own information (e.g., Buchanan et al., 2013), and also to be able to control the rights of access to the records. PHRs and even more so the Electronic Health Record (EHR) which aggregate them need a platform that will allow secure data exchange (Zhang & Liu, 2010) preserving privacy across Cloud-based systems (Li, Yu, Zheng, Ren, & Lou, 2012).

Similar problems can be found in educational institutions where pupil (Buchanan, Lewis, Fan, & Uthmani, 2012) or student information cannot be shared due to legal and technological limitations, despite the data owner's expectations. In order to give people full ownership of their data and to enable institutions; organizations and enterprises around the world to securely share sensitive information security professional, as well as governments, we must deliver tools, platforms and knowledge base applicable to modern environments (Zhou, Varadharajan, & Hitchens, 2014).

In this paper, we will focus on the possibilities for an up-to-date identity meta-data model that could be designed to be ready for globally established secure data processing, cloud hosting and extensive authentication. With this model, owners would have control over their own data (or be able to delegate it to identified affiliated people) starting from their birth.

This work builds on a number of projects including within health and social care, the UK Technology Strategy Board- (TSB) funded project with Chelsea and Westminster Hospital in London which focused on creating an e-Health Cloud within a hospital environment (Fan, 2011 and Fan, 2012). This used a novel method of defining the ownership of the data, and providing a rights infrastructure for the citizen (or patient) to define the rights of access to their data. This work has since been extended within a number of projects including the TSB Trusted Service project, which has focused on integrating both digital and human trust, to provide a fully integrated and holistic care infrastructure, which integrates primary and secondary health care with assisted living (Ekonomou, 2011; L, 2012).