Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

ELSEVIER

Computers & Security

Sticky policies approach within cloud computing

Grzegorz Spyra, William J. Buchanan *, Elias Ekonomou

The Cyber Academy, Edinburgh Napier University, Edinburgh, UK

ARTICLE INFO

Article history:
Received 11 May 2017
Received in revised form 1 July 2017
Accepted 5 July 2017
Available online 10 July 2017

Keywords:
IRM
Sticky policies
IBE
Cloud security
XACML
Cryptography

ABSTRACT

This paper discusses a secure document sharing approach, which addresses confidentiality, integrity and authenticity concerns related to cloud-based data sharing. This research is focused on a secure construct that would integrate with other cloud ready standards and products for data protection. Sticky policies, recently considered as one of the preferred cloud data protection techniques, are here combined with standardized OOXML data package. The defined model leverages the Identity Based Encryption (IBE) scheme to attach sticky policies to the data. This paper also shows several security features and functions that are suitable for secure data sharing in the cloud. Technologies used for proposed construction are not new, therefore only their unique combination with AES key derived from XACML sticky policy via IBE and OOXML wrapper constitutes novelty of this research.

1. Introduction

Cloud service providers (CSPs) are offering services that in large organizations and enterprises were previously delivered only on-premises. This introduced completely new challenges for potential CSP customers. Major security organizations offered tough security standards that CSP have to comply with and standards that customers from governmental, financial and public sectors have to implement (Luna et al., 2015). Security standards compliance however is a regulatory form of information security practice not a safeguard that can actually protect the data.

To compete with new technological challenges, many data protection services that were previously only delivered within strict security boundaries are offered as a cloud service. One of the major threats is related to data encryption. It has been shown that currently used cryptographic schemes with common setup could be broken with an emerging quantum technology (Chen et al., 2016). Quantum computing has been hanging as sword of Damocles over the cloud security for a decade. No data could be safe but its governance could be improved. Another possible threat is related to Big Data where simple machine learning and business intelligence as a service becomes a way to efficiently process large amounts of anonymized or encrypted personal data. Extracted anonymized data becomes highly sensitive due to fact that illegitimate data analysis applied on a large scale could have a potentially serious social impact (Reimsbach-Kounatze, 2015). Without right dedicated information security techniques for cloud, it is rather hard to protect information. Nevertheless, different security techniques having various vulnerabilities could serve better if properly chosen for the right purpose.

CSPs protecting data at rest on per-database basis can leverage database encryption. Recently Microsoft researchers published results around a new efficient homomorphic encryption what could be a solution for a medical data (Dowlin et al., 2015) that has to be processed in a secure manner without

* *Corresponding author.*
E-mail address: w.buchanan@napier.ac.uk (W.J. Buchanan).

http://dx.doi.org/10.1016/j.cose.2017.07.005

divulging underlying information. On the other side, just a few months earlier, another group of Microsoft researchers proved that database CryptDB encryption, previously acknowledged as a secure data protection technique can be broken with a single trick (Naveed et al., 2015). It might be just a matter of time until homomorphic encryption becomes vulnerable to a new type of attack. Database encryption approach is highly efficient from indexing perspective, however single vulnerability may compromise entire database security and divulge vast amount of sensitive information.

On the other hand, Information Rights Management (IRM) approach applies security on per data piece or data-in-motion basis. CSPs offering IRM as a service encrypt every single document or message separately therefore risk that entire data repository is compromised due to a single vulnerability is reduced. IRM seems to be a relevant and an easy solution for document and message exchange; although to deliver both security and performance, it involves at least two cryptographic methods where keys management becomes complex. There is still a lack of cloud standards and just a few products that makes data exchange between parties homogeneous therefore hard. IRM providers considered new security countermeasures (i.e. Microsoft), to improve keys protection, enabled on-premises Hardware Security Module (HSM) support (Sergey et al., 2015) for its flag, cloud-based IRM product MS Rights Management Services (RMS) Online. IRM itself does not provide functionality for data indexing and its applications without prior data extractions and anonymisation are limited in comparison to DB encryption. However still large organizations and enterprises as well as small businesses and individuals store and exchange sensitive information using unprotected documents and single plain text messages. IRM is not suitable for many applications, although it is very efficient when it comes to constrained data exchange where two or more parties share a data in asynchronous manner.

In regards to frameworks for cloud data sharing, data hosted and protected by one cloud service provider cannot be securely transferred outside of a single CSP security boundary. Such a migration would require either data to be re-encrypted before migration or cloud providers would have to exchange cryptographic master keys. Cloud data hosting very often is based on storing data by homogeneous application in a public Internet space; what bends initial cloud service principals. Theoretically cloud provider should offer a transparent service that could be dynamically transferred or seized by other cloud service provider without loss of actual service quality and data availability (Leimbach et al., 2014). Using IRM with properly designed infrastructure of distributed trust authorities (TA) could address problem of data sharing and data migration between CSPs and other data sharing parties.

The solution presented here is built on top of existing open standards mainly authentication and authorization framework that have been developed over years and that have been used for various global implementations. Security Assertion Markup Language (SAML) authentication standard developed by The Organization for the Advancement of Structured Information Standards (OASIS) (Cantor et al., 2005) is not discussed further in this paper but it is worth mentioning in regards to actual future implementation. SAML authenticates identity across different organizations and cloud providers. For authorization this research applied an existing eXtensible Access Control Markup Language (XACML) policy framework (Saldhana et al., 2013), which can enforce Discretionary Access Control (DAC) rights and leverage non-DAC roles like in Role-based Access Control (RBAC) systems (Anderson, 2004) or can be combined with modern risk assessment engine (Gasparini, 2013) to control access using dynamic risk calculations. Most of the modern access control techniques can be combined with XACML policy including dynamic membership and rights revocation. Document data format used in this research is based on Office Open XML (OOXML) an open standard (Apple et al, 2006), which defines the XML schemas with conforming vocabularies for word-processing, spreadsheet and presentation documents, as well as the documents packaging. Finally both the XACML-based sticky policy and the data are bound together using Identity Based Encryption (Boneh and Franklin, 2003), a cryptographic primitive that protects the data's confidentiality and integrity as well as sticky policy authenticity.

Section 2 shows other works this research refers to and other papers that discuss secure data sharing in the cloud and sticky policies as a cloud enabler. Section 3 describes Identity Based Cryptography and shows its applications for discussed sticky policies model. Section 4 explains Identity Based Encryption with other entities i.e. sticky policy used for key construction. Section 5 shows IBE security proof that applies to sticky policies model. Section 6 discusses integrity and non-repudiation. Section 7 shows how sticky policies can protect the data and what safeguards they bring.

2. Related work

Many research projects aim to deliver new data protection safeguards sufficient to protect highly sensitive personal data such as medical or governmental records (Jain and Farkas, 2013; Le et al., 2012; Abbas and Khan, 2014; Li et al., 2012).

Sticky policy is not a new data protection model, it was first discussed in Karjoth et al. (2002), went through various transformation and has been used for many successful Information Rights Management (IRM) implementations. Existing IRM systems Microsoft Rights Management Services (RMS) Online product (Sergey et al., 2015) or Oracle Information Rights Management (IRM) (Martin and Peet, 2010) and other same as sticky policies model attach policy to the data. These are products that have been already evaluated on a larger scale, although none of these products are based on any open standard that could be compatible in the cloud, and actually only RMS was adapted for the cloud use. RMS IRM construct uses eXtensible rights Markup Language (XrML), the rights expression language that was designed for closed environments (Microsoft Corporation, 2008) where cloud implementation was not considered. XrML (ContentGuard, 2001) and XACML (Saldhana et al., 2013) are very similar; however the semantics used to express access rights are different. Both define tuples where subject is permitted to perform specific activity defined by predicate against access object. In XrML, a condition is a functional equivalent of XACML obligations, although what give XACML advantages are complex expressions and predicates with negative and deny assertions. Note that XrML supports only positive assertion.