Integrating privacy into an architecture for learning analytics

Author: George Ciordas-Hertel
German Institute for International Educational Research
ciordas@dipf.de

ABSTRACT: With the installation of the General Data Protection Regulation (GDPR) of the European Union each learning analytics architecture in place need to face specific privacy concerns. One of these concerns regards the right of the user to object to the collection of his personal data. In this hackathon a mechanism could be set in place which applies this right to a Learning Record Store (LRS).

Keywords: learning analytics, architecture, xAPI, privacy, GDPR

1. INTRODUCTION

The General Data Protection Regulation (GDPR) [2] of the European Union (EU) is intended to strengthen data protection for all European citizens. With this regulation the EU wants to give the people more control over how their personal data is used. The GDPR will be enforced in May 2018. Each learning analytics architecture in place will then need to face these privacy concerns. There are multiple challenges to face within such architecture [3]. A typical learning analytics system comprises multiple data sources which provide facts to a Learning Record Store (LRS). These facts could be xAPI statements resulting out of different types of activities the users do [1]. Considering "The right to object" of user to the collection of their personal data, the LRS needs to provide a mechanism to reject those facts.

2. CHALLENGE

A challenge the GDPR imposes on learning analytics architecture is that the facts which are getting pushed by multiple other systems need to be filtered with regard to the privacy settings of each individual user. As the GDPR describes a general right to object, giving the user a possibility to object more differential by activities, might allow us to still do analytics on parts of the personal data. Therefore a system with multiple components is necessary. One component is providing the privacy settings through a common API. Another component is the LRS which will be receiving and storing the facts. As you may see in figure 1, this LRS needs to be extended by a privacy guard which is responsible for the filtering based on the privacy settings. The purpose of this hackathon project is to design and implement a privacy filter mechanism for a learning analytics framework.

Research Questions:

- How to efficiently synchronize the privacy settings between software components?
- How to efficiently filter xAPI statements based on more or less generic privacy settings?

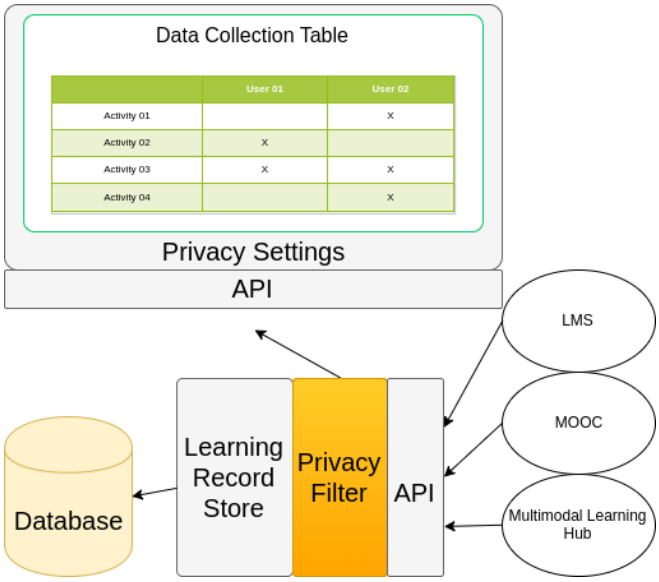

Figure 1: The privacy filter rejects facts arising from activities send by multiple sources based on the privacy settings of the users.

3. LOGISTICS

A system stub developed in Java EE 7 is available. The components are communicating with REST services sending JSON objects. The privacy component has a connection to a MySQL database. The LRS has a connection to a MongoDB. The whole system can be deployed on each development machine with a Docker setup. xAPI Statements could be send to the LRS from a separate system test component which afterward checks if the xAPI Statements where filtered out or not.

REFERENCES

[1] A. Berg and M. Scheffel and H. Drachsler and S. Ternier and M. Specht (2016). *Dutch Cooking with xAPI Recipes: The Good, the Bad, and the Consistent.* Proceedings of the 2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT).

[2] European Commission. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[3] Hoel, Tore and Griffiths, Dai and Chen, Weiqin (2017). *The Influence of Data Protection and Privacy Frameworks on the Design of Learning Analytics Systems.* Proceedings of the Seventh International Learning Analytics Knowledge Conference.