Security metrics management for cloud service providers

In 1961, John McCarthy, an American computer and cognitive scientist, was the first to suggest publicly the idea of computer time-sharing technology that might allow that computing capabilities and specific applications could be sold as a service in a future time. That future is now. Information and Communication Technologies (ICT) development in recent years has made possible this technology through the concept of *Cloud Computing*.

Cloud Computing arises to satisfy the increasing computing needs from companies and users. This model of cloud provides them on-demand access to high computing capabilities, storage services or software tools without needing to own infrastructure. As a result, the number of companies that have decided to adopt cloud services is growing today.

However, that trend of cloud services entails some risk and security problems, especially with privacy management and data loss, that companies want to avoid. Those security problems are analysed by different organizations, and one of these is the Cloud Security Alliance (CSA), a non-profit organization that promotes the research into best practices for *Cloud Computing* security and provides education and guidance to companies who implements these services.

Regarding these practices, CSA provides risk assessment tools, such as CAI Questionnaire, which help companies to select cloud service provider (CSP). CAIQ (*Consensus Assessment Initiative Questionnaire*) is a document provided by CSA for cloud customers and auditors to assess the security of a cloud provider. This document includes a survey with questions about security controls, which define the service of a cloud provider.

These security controls are defined by CSA based on all the security requirements that users and companies need to adopt a cloud solution. CAI Questionnaires are included in a registry created by CSA called STAR (*Security, Trust & Assurance*

Registry). This registry contains a list of CPS's and their assessment documents. Also, cloud providers are classified by different certification levels.

The objective of this Final Project is the development of a tool that makes this cloud service assessment easy for the customer by automatic processing of CAIQ documents from several providers. That tool is divided in two parts, as shown in Figure 1:

- An engine that manages and analyses data security metrics of cloud services providers and a Web service to access that data.

- A Web application that allows to compare the services' metrics from different CSPs using the Web service to access the data.

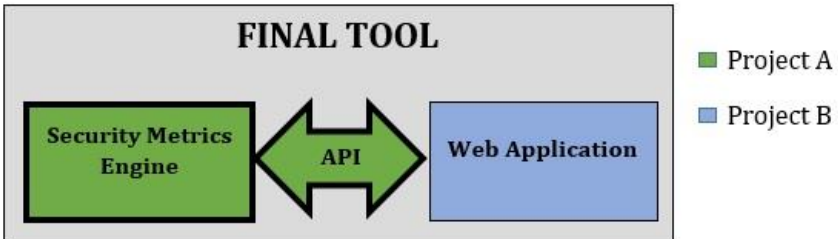

Figure 1. Tool structure.

This Final Project is focused on developing the security metrics engine and API matching the Project A, which together with the Web application of Project B composes the final tool.

The structure of the developed system is composed of following three blocks (Figure 2):

- A Java program that parses CAI Questionnaire metadata into a JSON (*JavaScript Object Notation*) format, introducing metrics for each security control.

- A documental database, which stores JSON metadata from parser program.

- A Web server that integrates a Web service to allow the access to metadata by external applications using REST (*Representational State Transfer*).

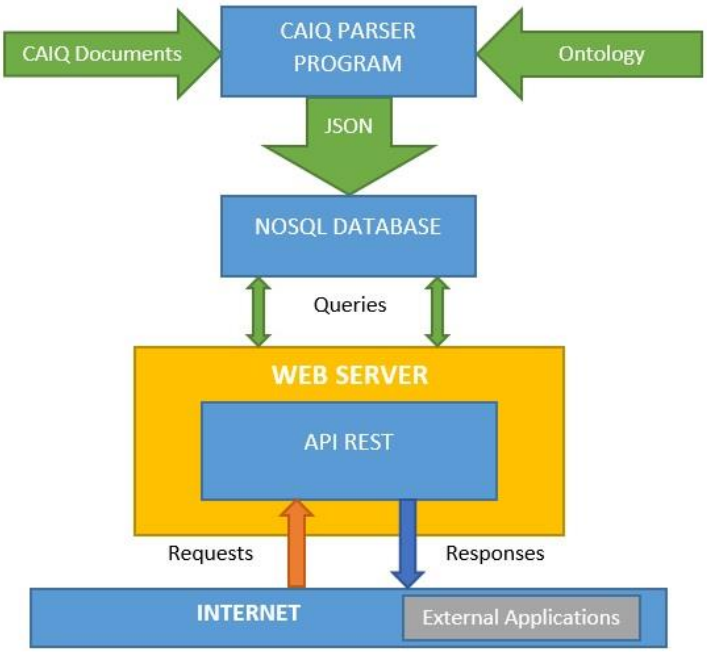

Figure 2. System architecture.

Firstly, the parser program processes the information of contained in CAI Questionnaire, an Excel document (.xlsx) whose internal structure is defined by the Office Open XML format. The Office Open XML specification includes a markup format based on XML for Excel documents, called SpreadsheetML. This format establishes that Excel documents are ZIP files that encapsulate XML files hierarchy. In this way, the program processes CAIQ as an XML file and parses into a JSON format following a particular structure.

The structure of JSON parsed objects is defined by an ontology previously elaborated (see Figure 3). This ontology is developed based on categories in which the information of the CAIQ metadata is classified.

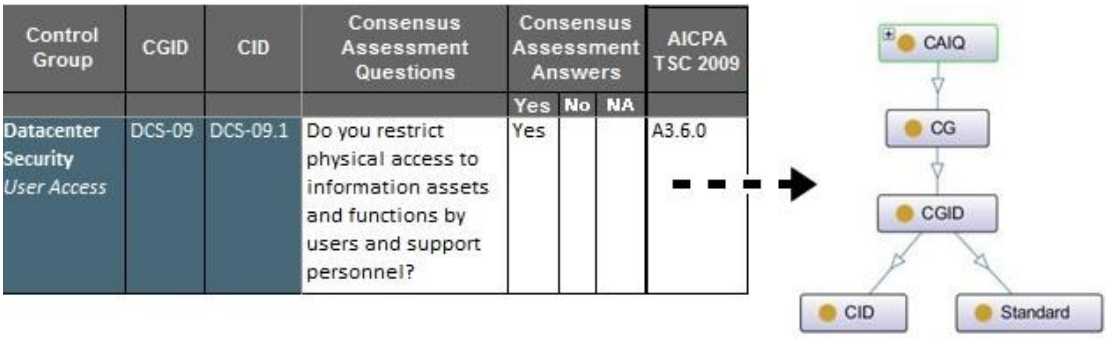

Figure 3. Ontology structure of CAIQ.

CAIQ is composed by 4 categories: CID, which defines a specific security control; CGID, which defines the control groups; CG, which indicates the security domain; and Standard, which matches the rest of the industry standards.

In this block, metrics of each security control (CID) are implemented according to the questionnaire answers provided by CSPs. These answers indicate if a control is applied by cloud provider (Table 1).

Consensus Assessment Answer	Metric Value
Yes	1
No	0
Not Applicable	The CID is ignored

Table 1. Security metrics assignation.

The metrics of the others categories are calculated through aggregation of control values. Also, a selection of available cloud providers is necessary, based on document format, different CAIQ versions and internal structure of CAIQ metadata. Of all providers registered in CSA STAR, the following CSPs are selected (Table 2):

CSP
Adallom
Aryaka
Capriza
Caretower
DataNoah
Devellocus
EDC Corporation
Everbridge
HKT
iLand
New World Telecommunications Ltd

OneLogin
Peer1
Perfecto Mobile
Zscaler

Table 2. List of selected CSP.

Secondly, parsed JSON metadata are stored in a documental database, in this case MongoDB, which receives custom queries from the Web server and gives it the required information.

Finally, the last block of the developed system implements the Web service with a well-defined API. The Web service is implemented using an Apache Web server where the application that represents the API is deployed.

The Web service is defined by several resources that may be requested by external applications. This specifies an external API in REST format to perform requests. Each of these requests allow to access to different information about cloud providers' metadata. There are main four available requests defined:

- The first request allows to the user to get the list of cloud providers stored in the system, returning CSPs identifiers and URL of logo images.

- The second request returns the list of categories or criteria names, according to three details levels, so this request can be divided in three sub-requests. Depending on the detail level (high, medium or low), it can be returned the names of criteria by CID, CGID or CG.

- The third request returns the security metrics of available cloud providers. As well as the previous case, this request can be return three different information depending on the detail level.

- The last request allows accessing the complete CAIQ metadata from a cloud provider as additional information.

Furthermore, it is used a RESTful Web services that have so many advantages, because it allows the use of JSON format in the responses and provides an easy access to resources through its URIs (*Universal Resource Identifier*). Figure 4 shows the selected URIs for the implemented resources:

Figure 4. API resources URIs.

To sum up, the security metrics management system developed in this project, joined with the Web application of the complementary project, may result a very useful tool to help cloud consumers and companies in the process of cloud adoption.