A Metric-Based Approach to Assess Risk for "On Cloud" Federated Identity Management

Patricia Arias-Cabarcos · Florina Almenárez-Mendoza · Andrés Marín-López · Daniel Díaz-Sánchez · Rosa Sánchez-Guerrero

Abstract The cloud computing paradigm is set to become the next explosive revolution on the Internet, but its adoption is still hindered by security problems. One of the fundamental issues is the need for better access control and identity management systems. In this context, Federated Identity Management (FIM) is identified by researchers and experts as an important security enabler, since it will play a vital role in allowing the global scalability that is required for the successful implantation of cloud technologies. However, current FIM frameworks are limited by the complexity of the underlying trust models that need to be put in place before inter-domain cooperation. Thus, the establishment of dynamic federations between the different cloud actors is still a major research challenge that remains unsolved. Here we show that risk evaluation must be considered as a key enabler in evidence-based trust management to foster collaboration between cloud providers that belong to unknown administrative domains in a secure manner. In this paper, we analyze the Federated Identity Management process and propose a taxonomy that helps in the classification of the involved risks in order to mitigate vulnerabilities and threats when decisions about collaboration are made. Moreover, a set of new metrics is

P. Arias-Cabarcos (✉) · F. Almenárez-Mendoza · A. Marín-López · D. Díaz-Sánchez · R. Sánchez-Guerrero
Department of Telematics Engineering, University Carlos III of Madrid, Avda. de la Universidad, 30, 28911 Leganés, Madrid, Spain
e-mail: ariasp@it.uc3m.es

F. Almenárez-Mendoza
e-mail: florina@it.uc3m.es

A. Marín-López
e-mail: amarin@it.uc3m.es

D. Díaz-Sánchez
e-mail: dds@it.uc3m.es

R. Sánchez-Guerrero
e-mail: rmsguerr@it.uc3m.es

defined to allow a novel form of risk quantification in these environments. Other contributions of the paper include the definition of a generic hierarchical risk aggregation system, and a descriptive use-case where the risk computation framework is applied to enhance cloud-based service provisioning.

Keywords Trust management · Cloud computing · Risk assessment metrics · SAML · Federation

1 Motivation

The cloud computing paradigm is set to become the next explosive revolution on the Internet. According to the definition of this model [1], resources are provisioned as a service over the network, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). Furthermore, four different deployment models are contemplated: private, community, public, and hybrid clouds. Based on this paradigm, users will enjoy on-demand network access to a shared pool of configurable computing resources, such as networks, storage, services or applications that can be rapidly provisioned and released with minimal management effort. But, despite all these envisaged benefits, the adoption of cloud computing is still hindered by security problems, as it has been widely emphasized in several recent research works [2–4].

Among all these security issues, this paper treats the challenges posed by identity management in the cloud [5], focusing on risk assessment. It is easy to see that cloud environments involve multi-provider and multi-service scenarios. In this context, new applications are likely to combine data from multiple cloud-based sources, belonging to different domains, each of which has its own access control mechanisms. Thus, it is desirable that users in one domain are able to access applications hosted in another cloud—or domain—as long as a trust relationship exists between the two cloud environments. Therefore, functionalities to manage the flow of user identity (i.e., authentication, authorization and attribute data) across clouds or domains are required. For this reason, a robust identity management must be put in place for cloud deployment and interaction in a usable and secure way. More specifically, federated identity management (FIM) is identified by researchers and experts as an important security enabler, since it will play a vital role to allow the global scalability that is required for the successful implantation of cloud technologies. This topic has gained momentum and, in fact, several standardization organisms and research initiatives involved in cloud computing have recently included identity federation as an indispensable mechanism in its use-cases documents and whitepapers [6–8]. Furthermore, the “Open Cloud Manifesto” states that clouds have to dynamically scale up and down [9]. However, the main drawback is that current FIM systems lack mechanisms to achieve dynamic federation, which is still an open challenge that requires further investigation. We previously identified this requirement in [10, 11] and we argue that risk assessment must be incorporated in evidence-based trust management to allow agile cloud

interaction without requiring static pre-configuration and to make dynamic federation possible.

With these ideas in mind, we propose a novel taxonomy to identify risks in federated identity management. Federation is one of the basic principles of cloud computing [12] because this paradigm of computing requires strong integration, cooperation and collaboration among different clouds. Furthermore, we also introduce a set of metrics to make quantification possible, since this is currently one of the more complex tasks in risk assessment. The proposed taxonomy aims to raise the attention of the community and to serve as a foundation to identify and investigate new metrics in FIM. Other contributions of the paper include the definition of a hierarchical risk aggregation framework, and a descriptive use-case scenario where our risk computation technique is applied to enhance cloud-based service provisioning.

The remainder of the article is structured as follows: Sect. 2 provides background knowledge regarding risk and identity management. Next, in Sects. 3 and 4, we present a categorization of risks in FIM, and explain how to derive metrics for its quantification. In Sect. 5, the proposed aggregation system is explained, followed by an application scenario in cloud computing described in Sect. 6. Finally, Sect. 7 highlights the main related works, and Sect. 8 gives the principal conclusions and future works.

2 Background Knowledge

2.1 On Risk

Due to the omnipresent character of risk, there are many definitions of the term depending on specific applications and contexts. Despite the ambiguity of the word and the lack of global consensus on the meaning, a good definition to understand the concept could be the following: "the possibility of loss or injury" [13]; that is, the probability of occurrence of undesirable outcomes. Mathematically, the most common formula to formalize risk in quantitative terms is (1):

$$R = P \times I \tag{1}$$

that reflects that risk (R) is proportional to both the probability of an undesirable event occurring (P) and the impact of this event (I). Usually the risk is composed by a series of risks, each one referred to a possible negative output, as shown in (2):

$$TR = \sum_{i} R_i \quad i = 1, \ldots, N \tag{2}$$

So, the total risk (TR) associated to a transaction is the combination of the risk values of all the possible undesired events (R_i). The main recurrent issue in the risk literature is quantification. The fundamental problem lies in the calculation of the two magnitudes that contribute to risk. Thus, determining the rate of occurrence is often complicated since statistical information is not available on all kinds of past incidents. Furthermore, evaluating the impact of the consequences is also hard.

It seems to be easier in areas related to economy, because the impact is proportionally related to the investments, but the task of asset evaluation in other fields gets relatively complex since resources other than money are hard to measure.

The first step for quantification is to collect data and extract significant numerical values, the metrics, that could be used later together with statistics and probability theory to conform a risk model. But metrology in Information Technology (IT) is still emerging [14].

Here we define a taxonomy with the aim to help the risk metric identification process in FIM. It constitutes a first effort to start quantification, following the maxim of "If you cannot measure (or model) it, you cannot improve it."

2.2 On Federated Identity Management

Federated Identity Management (or FIM) refers to the technologies, standards and use-cases that serve to enable the portability of identity information across otherwise autonomous security domains [15]. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly and without the need for completely redundant user administration.

The main actors in a FIM scenario are (1) the Identity Provider (IdP), which vouches for the identity of a user and issues authentication, authorization and/or attribute tokens about her; (2) the Service Provider (SP), which provides services to the end user and relies on the identity tokens generated by the IdP; and (3) the User, that interacts (usually via a user agent, e.g., web browser) with both SPs and IdPs.

In the particular context of cloud computing, the SPs are the cloud service providers (which provide anything as a Service, i.e., XaaS); and the IdPs are those entities that act as authoritative sources of identity data for users. Federation of identities maintained by the multiple cloud SPs is crucial to allow flexible cloud-based service composition and application integration. In fact, federation protocols are currently used commercially by companies and government agencies to provide cloud Single Sign-On (SSO) connections and security solutions to hybrid cloud computing environments.

For scalability reasons, trust relationships between the involved actors[1] should be created on-demand instead of being statically defined previous to interaction, which is the method currently used in FIM. However, there is a high uncertainty component when deciding whether to cooperate or not with unknown parties. Thus, every actor that participates in a FIM system has to make decisions that imply dealing with some form of risk. An IdP may ask itself if it is secure to collaborate with a particular unknown SP. Similarly, an SP will have to decide if it is secure to accept authentication statements or other identity data issued by a specific IdP. And finally, it is crucial that users are aware of the transactions regarding their identity. In fact, they should be provided with some kind of risk information to determine if they should reveal their personal data to an SP or IdP.

[1] The term actors are used in accordance with definitions in [6].

On the other hand, there are some subtleties inherently related to the term *federation* in Identity Management scenarios that must be first clarified to properly understand the proposed taxonomy. So, the verb *federate*, as defined in the Merriam Webster Dictionary, means "To link or bind two or more entities together." In the context of our research, there are two possible senses in which the word federation (and its variants) can be employed and still be consistent with the former definition. According to it, we can talk about (a) *federation*, meaning the act of establishing a relationship between providers; and (b) *identity federation*, that exists when there is an agreement between various providers on a set of identifiers and/or attributes that are used to refer to a subject (i.e., the user). Thus, an *identity federation* is not possible if providers are not *federated*. But a provider federation depends on the identity framework being used; it could be a trivial process, as occurs with OpenID [16], where no trust model is required to cooperate; or an extremely complex task, as happens with Security Assertion Markup Language (SAML) [17] or Liberty Alliance protocols [18], where contractual frameworks must be statically established to set up a Circle of Trust (CoT).

So, once the shades in the meaning of the word *federation* have been clarified, the principal division of the taxonomy can be understood.

3 Risk in FIM: A Taxonomy

Based on the reasoning in the previous section, we argue that Federated Identity Management consists of two different phases that should be analyzed separately to evaluate risks.

1. *Pre-federation Phase* (or federation between providers). This phase consists of the establishment of a relationship between providers, which means deciding on protocols to interoperate, agreeing on common rules and policies, etc. Definitely, pre-federation can be understood as a *Bootstraping Phase* that allows parties to gather information about each other and to initiate cooperation.
2. *Post-federation Phase* (or transactions between federated providers). This phase contemplates the transactions between two federated entities (e.g., requesting user attributes or accepting authentication claims). So, at this point, we have basic information to support our decisions. At least, the deciding entity will count with all the data derived from the *Bootstrap Phase* and, if more interaction has taken place, it will also maintain a history of transactions. This stage can be viewed as the *Evolution Phase*, since entities progressively construct and consolidate their relationships, which fulfills the dynamic and subjective nature of trust.

The decisions to make and the applicable information are different in each phase; and so are the faced risks. In pre-federation, an entity will presumably have to decide whether to establish a relationship for further cooperation with another entity. The sources of information to compute a risk metric could be, for example, the entity metadata [19], pre-configured relationships, policies, and the Service Level Agreements (SLAs) being negotiated. On the other hand, metrics in the

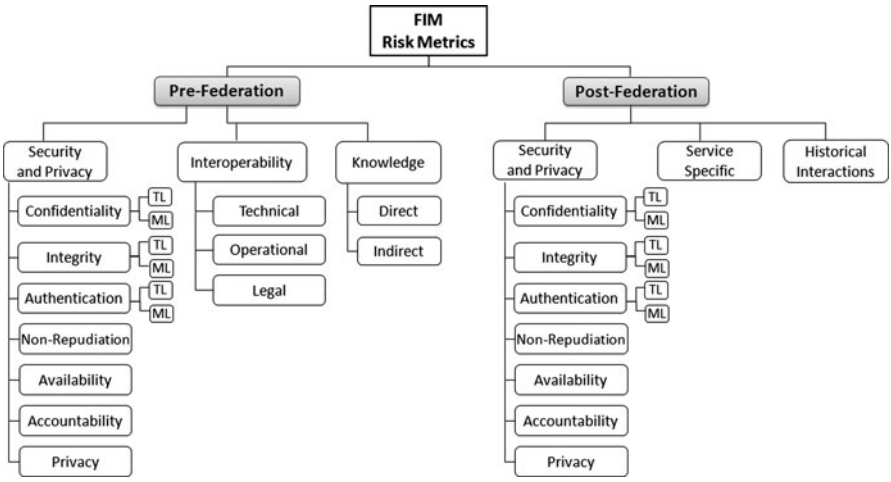

Fig. 1 Taxonomy for risk metric categorization in federated IDM

Post-Federation Phase can be calculated from the information available in the assertions and protocols in use, the characteristics of the specific service transaction in process, and also, by leveraging the risk metrics from the previous phase. The distinction of these two fundamental phases in FIM constitutes the first level (L1) of the proposed taxonomy, whose complete schematic is depicted in Fig. 1. In the following subsections, we explain the different risk categories related to each phase that are shown in the picture.

3.1 Pre-federation Risks

In order to establish a federation between providers, a set of agreements must be put in place so a trust relationship can be created. For this purpose, there is not a standard or common fixed set of minimum requirements. Instead, every deployment follows its own rules based on the federation framework in use. After thoroughly analyzing FIM specifications, best practices and recommendations [20] and reviewing public data about how current federation deployments were established [21], it can be concluded that the whole set of aspects to be considered before creating a federation are oriented to achieve security and privacy objectives, to establish operational rules and policies for legal compliance, as well as to define the technical configuration required for communication. The taxonomy proposed here aims to cover all these aspects in order to be generic enough to abstract all the federation frameworks. According to this, we divide the next level (L2) of classification in the pre-federation phase into three main blocks or categories; *Security and Privacy Risks*, *Knowledge Risks*, and *Interoperability Risks*. Next, each of these classes is explained in more detail.

The first class, *Security and Privacy Risks*, encompasses those risk metrics related to the security and privacy features that are supported by an entity that wants to establish a federation, located at level L3 in the taxonomy:

- *Confidentiality* Disclosing information only to the intended and authorized recipients;
- *Integrity* Guarding against improper information modification or destruction;
- *Authentication* Confirming something (or someone) as authentic, verifying the validity of the claims made by or about the so called subject;
- *Non-Repudiation* Providing evidence that one party involved in a transaction sent or received a message, so it cannot be denied;
- *Availability* Ensuring that a system is operational and that it is accessible to those who need to use it, so the business purposes can be met; loss of availability is often referred to as "denial-of-service";
- *Accountability* The ability to associate a consequence with a past action of an individual. It is required that the individual can be linked to an action or event for which he/she is to be held accountable;
- *Privacy* Appropriate use and protection of information; meaning seclusion and selective disclosure of data according to law and policies. Privacy is sometimes related to anonymity, defined as the wish to remain unnoticed or unidentified in the public domain.

Each of the above basic security services or "CIA" (i.e., Confidentiality, Integrity and Authentication) depends on the cryptographic characteristics of both the data exchanged at the *message level* (ML) and at the *transport layer level* (TL). In this regard, most of the FIM protocols strongly recommend the use of secure communication protocols, such as Secure Sockets Layer (SSL) [17, 22]. Thus, it is required to evaluate the quality of the security services that can be provided at the message level and also with regard to the communication nature. For example, a FIM transaction with encrypted assertions that are also transmitted over a secure SSL connection would incur in less risks than if the communication channel is not secured. This requirement is also reflected in the taxonomy, as a sub-classification (at level L4) to be evaluated for each basic security service.

The second subclass under pre-federation, called *Knowledge Risks*, involves those factors related to the previous information that is known about the other entity. These metrics aid in the quantification of the initial trust level that is assigned, being a point of relation between trust and risk. Since each party has to decide whether to engage in a relation with the other party for future cooperation, it is reasonable to gather information about its trustworthiness.

In order to capture the different types of relationships, Knowledge metrics are sub-classified into Direct and Indirect. The Direct Knowledge metrics are related to pre-configured relationships (e.g., digital certificates or business agreements); whereas Indirect Knowledge refers to that information that can be inferred from direct relationships in other contexts or obtained from external sources [23]. Consequently, the risk level will vary according to the existing knowledge, because it is indirectly proportional to the uncertainty.

Finally, the last differentiation to allocate risk contributing factors in pre-federation is named *Interoperability Risks*, which encompasses those issues related to interworking between entities. Interoperability can be decomposed in three different domains, located at level L3 in the taxonomy: *Technical, Operational* and

Legal. The Technical category is required since there are many different technologies for FIM. Furthermore, inside a specific framework there can be different implementations. For example, two SAML enabled entities could not interoperate if they do not support a set of common *Profiles*. Thus, metrics are required in order to measure the technical compatibility of the systems. Apart from technology related interoperability, it is also important to evaluate if the policies of each entity are compatible to a certain degree. In this sense and on one hand, entities should measure the interoperability regarding operational policies. On the other hand, legal compliance and applicable jurisdictions should also be addressed, so cooperation is also interoperable at the regulatory level. Therefore, if cooperation implies risk of violating an entity policy, it should be avoided. Thus, the interoperability metrics are computed based on the information gathered from Metadata, SLAs, and policies of the other entity before deciding on interaction.

3.2 Post-federation Risks

After a federation between providers has been established, transactions to exchange user identity data can be performed between them. In this phase, risk must be evaluated on a per-transaction basis. As shown in Fig. 1, Post-Federation Risk metrics can be categorized in three main classes; *Security and Privacy Risks*, *Service Specific Risks* and *Historical Interaction Risks*.

In post-federation transactions it is relevant to measure how the security features are fulfilled in order to know how they contribute to the total risk. Thus, the same classification of *Security and Privacy Risks* made for pre-federation applies here. The difference is that the Security and Privacy metrics taken in post-federation are related to the current transaction, and so they are used to decide whether or not to transact in the measured conditions. However, metrics in the pre-federation phase are used to determine the global support of security features and decide whether to federate or not.

Apart from the Security and Privacy related metrics, we consider a further distinction in order to include *Service Specific Risks* and ensure completeness. This category allows the risk model to be tailored for different types of services. Services differ in characteristics such as required personal information, value of the resources owned by the SP, importance of data availability and so forth. All these issues must be considered by every member involved in a service transaction in order to create a risk context and decide about proceeding with the transaction or not.

Finally, there is also a *Historical Interactions Risks* category to consider those risk metrics related to the information and knowledge about the other entity involved in the transaction. In this phase, in contrast to the pre-federation case, there is another source to compute knowledge related metrics: the history of transactions. As more transactions are performed, the entities will have a better direct knowledge about the behavior of other entities. In addition, indirect knowledge could be obtained in anomalous situations. Consequently, the involved risk level can be tuned accordingly.

All the above distinctions are captured in the schematic of the taxonomy depicted in Fig. 1. To summarize, the taxonomy is organized into two major classes:

pre-federation and post-federation. These taxonomic classes are further divided into the subclasses representing Security and Privacy Risks, Knowledge Risks, Interoperability Risks, Service Specific Risks and Historical Interactions Risks. Finally, the last levels contemplate the different dimensions in which every risk can be evaluated. The taxonomy in Fig. 1 should be adopted by every entity in the system to enrich its intelligence and independence and to be capable of making well-informed decisions.

The classification compiles the characteristics of FIM systems and makes risk decomposition in small subsets possible. Besides, it is generic enough to be applicable to every federation framework (SAML, Liberty Alliance, OpenID, etc.), since the provided abstraction levels allow to cover all the common features, as well as the specific ones.

4 Risk Quantification: A Metric-Based Approach

In the following, we explain how to identify risk metrics using the taxonomy in Fig. 1. For this purpose, we assume an SAML-based federated system. The main goal is to identify independent terms that contribute to the computation of the overall risk, as illustrated in formula (2), although other methods might be used [24].

The first step is to choose a terminal node in the taxonomy tree, e.g., *Post-Fed* → *Security and Privacy* → *Confidentiality* → *TL*. For this selected category, the possible threats can be derived. In this case, if no confidentiality is provided at the transport level, the system could be subjected to eavesdropping attacks or privacy violations. So, transport confidentiality yields a contribution to the feasibility of the mentioned threats. However, the final risk will be affected by other components, such as the confidentiality at the message level. Once we are aware of the related risks, we can define a way to quantify relevant facts that relate to them. In this example, the value of the confidentiality at the transport level can be assigned depending on the cryptographic strength of the encryption algorithms supported by the entity willing to federate. Thus, we finally came up with the semantic definition of the metric, as shown in Table 1.

Following this strategy, we can identify more metrics. Another example is the Level of Assurance or LOA (see Table 2). It is usually defined as the degree of confidence in identifying an entity to which a credential was issued, and the degree of confidence that the entity using the credential, is indeed the entity that the credential was issued to. For example, the National Institute of Standards and Technology (NIST) [25] defines four discrete levels that are associated with the

Table 1 Definition of the confidentiality-transport level metric

Metric	Confidentiality—transport level ($CONF_{TL}$)
Definition	Measures confidentiality of information exchanged at transport level, depending on the encryption algorithm (e.g., based on strength, key size)
Considerations	Inversely proportional to risk. *Source*: Entity Metadata [19]

Table 2 Definition of the level of assurance (LOA) metric

Metric	Level of assurance (LOA)
Definition	The LOA measures the degree of confidence in identifying an entity to whom a credential was issued
Considerations	Inversely proportional to risk. *Source*: can be obtained from the SAML Authentication Assertion, either directly [26] or by calculating it from the Authentication Context [27]

strength of the authentication methods. This way, simple password challenge-response is categorized as LOA level 1, and hard cryptographic tokens are considered level 4. The LOA, which falls into the *Post-Fed* → *ServiceSpec* category, is a clear example of an existing concept that fits into the taxonomy and can be used as a risk metric in FIM. Thus, the value expressed by the LOA metric can be used by providers to decide whether an individual should be granted access to specific protected resources or if a higher LOA is required.

The purpose of the taxonomy is to serve as a reference framework to better understand the process of federation and identify the different aspects that need to be taken into account when building trust and analyzing the possible risks. There are existing defined metrics that are applicable to FIM infrastructures, and new tailored ones can be created for specific service necessities. So far, the set of basic metrics that we have derived from the taxonomy and that can be incorporated in the risk aggregation system described in Sect. 5 are summarized in Table 3.

The degree in these metrics represents the probability value (P) in formula (1). So in a first approach, we consider the impact (I) as a constant estimated value for each interaction applied according to the sensitivity of the services and resources that potentially could be affected.

So far, we have provided a semantic high-level definition of the metrics, and assigned a linguistic scale to each one in the next section. However, we do not specify how to calculate the numeric values to be mapped in these scales.

5 Hierarchical Risk Aggregation

5.1 Architecture

Apart from serving as a basis for deriving risk metrics, the taxonomy can be used to define an aggregation model for risk calculation. Its hierarchical structure makes it suitable to be the foundation of a hierarchical aggregation system. This is an important advantage since multicriteria decision making (MCDM) mechanisms and related mathematical techniques (such as *Analytic Hierarchy Process* (AHP) [28]) rely on the decomposition of problems into a hierarchy of more easily comprehended sub-problems, each of which can be analyzed independently.

Thus, with the aim to apply the defined taxonomy to compute the total risk in the different phases of FIM, we have designed a generic hierarchical aggregation system that is comprised of the following elements:

Table 3 Basic set of metrics for risk quantification in FIM

Category (L2)	Metric name	Description
Security and privacy	$CONF_{TL}$, $CONF_{ML}$	Measure confidentiality degree of information exchanged at transport level and message level, respectively
	INT_{TL}, INT_{ML}	Measure integrity degree of information exchanged at transport level and message level, respectively
	$AUTH_{TL}$, $AUTH_{ML}$	Measure authentication degree of information exchanged at transport level and message level, respectively
	NON-REP	Measures the degree of non-repudiation
	ACC	Measures the degree of accountability
	AV	Measures the degree of availability
	LOP	Level of protection measures the degree of data protection that either an IdP or a SP provides for identity information entrusted to them by a user
Interoperability	$INTEROP_T$	Measures the degree of technical interoperability between the involved parties
	$INTEROP_O$	Measures the degree of interoperability between the operational policies of the involved parties
	$INTEROP_L$	Measures the degree of interoperability between the legal policies of the involved parties
Knowledge	$KNOW_D$	Measures the degree of direct knowledge about the other party
	$KNOW_I$	Measures the degree of indirect knowledge about the other party
Service specific	SLOs, LOA	Service Level Objectives (SLOs) define characteristics of a service in precise, measurable terms (each service should define its own specific metrics, e.g., throughput, bandwidth)
		Level of Assurance (LOA) measures the degree of confidence in identifying an entity to whom a credential was issued
Historical interactions	HINT	Measures the posteriori probability of interactions

- *Input Source Data* The input data that will be employed to extract appropriate metrics for risk calculation. The model contemplates external data sources, such as messages and SLAs, as well as internal data sources, such as trust lists or local policies.
- *Risk Metric Extractor* This component processes the input data and derives the low level risk metrics that will be subsequently used to compute the final risk value.
- *Aggregation Engines* These modules are in charge of taking separate risk contributing factors and applying an aggregation function to combine them in a single value. The system contains an aggregation engine per each category in the taxonomy.

We adopt the following notation: each element in the taxonomy is called a risk category (e.g., Security and Privacy Risks, Knowledge Risks…) and the risk value associated to a specific category is calculated by combining the risk values associated to its sub-categories that are located in a lower level. According to these

definitions, Fig. 1 and formula (3) illustrate the basic building blocks of the hierarchical aggregation model. Essentially, the risk associated to category i at level j (R_i^j) is obtained by aggregating the k contributory factors that are a sub-category of i in the immediate lower level (R_k^{j+1}), and each of those can be further partitioned into these lower level contributory factors:

$$R_i^j = Agg(R_k^{j+1}), \quad k = 1, \ldots, N \quad k \forall \text{subcategory}(i) \tag{3}$$

The aggregation function (Agg) may be selected according to the policies of the entity that calculates risk. Next, we particularize the hierarchical risk system by applying a specific aggregation technique in order to show how risk computation is performed.

5.2 Particularizing the System: The Fuzzy Aggregation Case

Aggregation refers to the fusion of several input values into a single and meaningful output value, and aggregation operators are the mathematical objects to achieve this task. Since aggregation is an indispensable tool of the majority of engineering, economic, social and other sciences, extensive research has been conducted in the field [29].

On the other hand, it is remarkable the applicability of fuzzy logic [30] and related aggregation functions in fields where uncertainty and imprecision play a relevant role. In order to aggregate fuzzy sets, there are also numerous specific operators that have been proposed in the literature, e.g., fuzzy t-norms (intersection, minimum, product) and fuzzy s-norms (union, maximum, summation). The selection of an aggregation operator will depend on the context where it is applied. In [31], detailed discussions on the election of appropriate operators are presented.

In our case, we will use fuzzy techniques to perform aggregation in the context of the presented hierarchical risk system. The application of fuzzy logic to risk seems appropriate, since this kind of analysis is subjective and related to uncertain and incomplete information.

So, in order to construct a fuzzy inference system (FIS), the following steps are performed (1) *Fuzzification*, that is comprised of the definition of the input and output parameters and their associated levels or linguistic labels; (2) Definition of *If–Then Rules* that will be used for reasoning about input values and obtain the output; and (3) *Deffuzification*, that refers to the calculation of a single output number after the rules are applied.

It is worth noting that due to the hierarchical nature of the proposed risk aggregation system, different fuzzy inference systems are used to aggregate individual risk categories at each level in the taxonomy. Next, these blocks, which we have previously termed *aggregation engines*, are cascade interconnected in order to obtain the final global output.

Thus, for calculating the total risk in the pre-federation phase, we start by defining a first FIS, the *Confidentiality Aggregation Engine*, with the input variables Confidentiality at transport level and Confidentiality at message level (based on metrics $CONF_{TL}$, $CONF_{ML}$), and output variable Confidentiality Risk. Similarly,

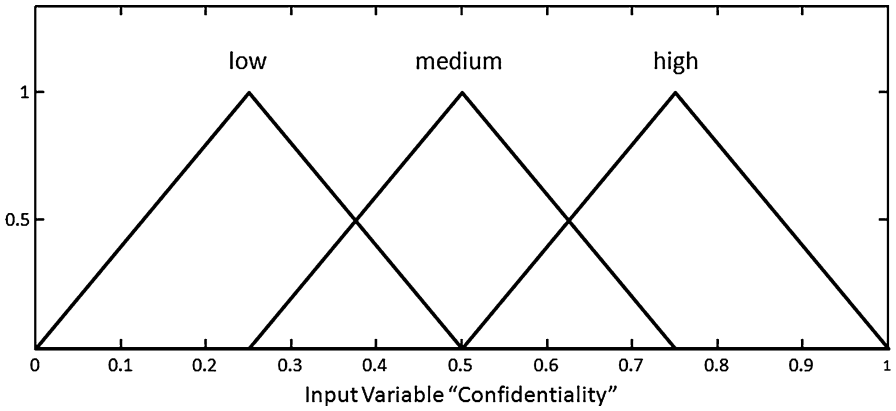

Fig. 2 Fuzzy linguistic scales for confidentiality variables. Similarly, a three level scale is also used in the rest of input and output variables of the system

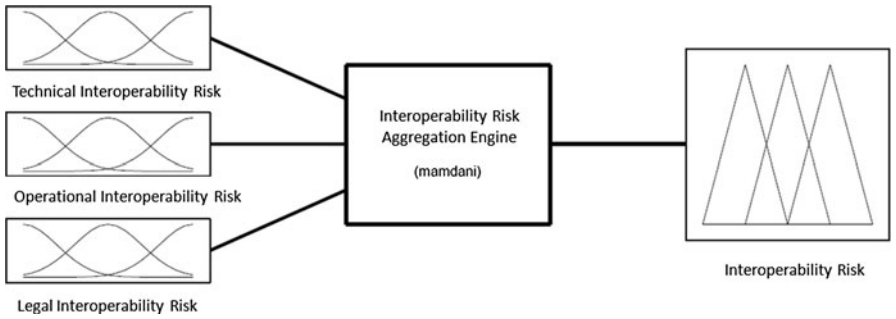

Fig. 3 Fuzzy-based aggregation engine to compute the Interoperability Risk value

the rest of FIS systems are created at the taxonomy Level L3 by using the metrics defined in Sect. 4 as inputs. The outputs are used to feed the FIS systems at Level L2: *Security and Privacy Aggregation Engine, Interoperability Aggregation Engine* and *Knowledge Aggregation Engine*. And finally, the total pre-federation risk at Level L1 is obtained by applying *if–then rules* to the Security and Privacy, as well as the Interoperability and Knowledge outputs in Level L2.

As depicted in Fig. 2 we use three linguistic levels in the *fuzzification* procedures (Low, Medium and High) both for input and output variables. However, both the granularity of the scale, as well as the scoring system and mapping between metrics and linguistic values, are to be defined by each party according to its necessities. Figure 3 shows the logical model of one of the aggregator blocks, the *Interoperability Aggregation Engine*, with the different input variables and the output of the module.

As shown in Fig. 3, in order to obtain the final Interoperability Risk value, the three input variables must be combined. And this combination is done based on a set of predefined rules in the following form:

```
IF Technical Interoperability Risk IS {High, Medium, Low} AND
Operational Interoperability Risk IS {High, Medium, Low} AND
Legal Interoperability Risk IS {High, Medium, Low} THEN Interop-
erability Risk IS {High, Medium, Low}
```

Similarly, a whole set of *if–then* rules must be defined for the rest of the aggregation engines. Thus, each entity has to describe its own rules in a policy document, so that they can be automatically extracted and applied by the aggregator engines. Finally, after applying the rules, the linguistic risk output is translated into a numerical value (*deffuzification*) in order to be used in decision making by comparing this number with internal pre-established risk thresholds in the system.

Although we have only described the system for pre-federation risk computing, the case for post-federation is equivalent.

In the following section, we show how the proposed technique for risk assessment is applied in a dynamic cloud federation use-case to demonstrate the scope of application.

6 Application Scenario

In order to illustrate the applicability of our proposal, we present an example scenario where risk-based decision making is used to allow dynamic cooperation between previously unknown cloud providers. It shows how the application of risk assessment allows a smooth and seamless experience to the end users.

We start from the use-case described in [6] where Alice, who is subscribed to her own cloud storage provider (CSP), has created various files there that contain personal data, one of which is her curriculum vitae (CV). Alice wishes to let Bob, her friend, read her CV file so she needs to delegate 'read access' to him. But Bob is not a subscriber to this particular cloud service provider, and has no wish to register for yet another set of credentials for accessing yet another service.

However, Bob does have an account with an IdP that is part of the same federation as the cloud storage provider, and is trusted to correctly authenticate Bob. For this use-case to be possible they rely on the assumption that "Federated IDM is already in place."

At this point, it is obvious that if the IdP belongs to the same federation of the cloud storage provider because previous contracts and arrangements have been put in place, there will be no problems. However, taking into account the multi-provider and multi-service nature of cloud computing environments, it is reasonable to think that both providers may be completely unknown.

In this case, a mechanism to allow a dynamic federation to be created on-demand and driven by user needs is highly desirable. This is the problem we solve with this proposal.

Let us now assume that the IdP and the CSP are unknown to each other. For this particular example and for the sake of simplicity, let us also assume that both providers are interoperable at every level: they are able to use the SAML FIM protocol, they have indirect knowledge via digital certificates and their policies say

that the only requirements to cooperate are related to the security of the communication; more specifically, to the CIA metrics (i.e., confidentiality, integrity, authentication.)

Thus, the new operation flow for dynamic federation introducing risk assessment is comprised of the following steps:

1. Bob sends a Service Request to the cloud storage provider (CSP) in order to access Alice's CV.
2. The CSP discovers that Bob is not a registered user and that he prefers to be authenticated by his IdP. But, since the CSP and the IdP are unknown to each other, they will first evaluate the involved risks to decide on cooperation.
3. Thus, the pre-federation risk is computed at the SP using the proposed hierarchical aggregation system based on internal data, such as local policies, and also using gathered external data regarding Bob's IdP (SLAs, metadata, reputation data, etc.) In this particular example, the CSP only takes into account the Security and Privacy Risk to make a decision, and its local policy says that just Confidentiality, Authentication and Integrity Risks must be taken into account. In Fig. 4, an example of SAML Metadata is shown that can be used as input source data for the risk metric extractor to get the required metrics. This Metadata document includes information regarding the cryptographic algorithms supported by the entity to be used when signing and encrypting messages. From this input data, the CIA metrics are derived and then mapped to linguistic risk variables in the scale {Low, Medium, High}.

Assuming, again for simplicity, that only message level metrics are required, aggregation will take place at the Security and Privacy Risk Aggregation Engine. Regarding the logic *if–then rules* that are executed in aggregation, let us suppose that the provider has decided to adopt the conservative risk approach that the aggregated risk is always the maximum of the single contributing risks. Accordingly, Table 4 summarizes the knowledge base used for the rules in the Security and Privacy Risk Aggregation engine:

Thus, according to the set of defined *if–then rules*, Fig. 5 shows the risk surfaces for the Security and Privacy Risk category obtained by combining all possible input values in the lower level. As stated before, since we are assuming a conservative policy, we can observe for example, that it is enough that one of the inputs is High in order to determine that the output risk is High.

4. If the final risk value is assumable according to internal thresholds, then the CSP assigns an initial trust to the IdP and a Federation Request is sent.
5. Since trust must be bilateral in a federation, the IdP would also evaluate the risks regarding possible cooperation with the CSP, in order to establish trust and decide on a federation.
6. If the calculated pre-federation risk is assumable by the IdP, then the federation is completed and transactions between providers can be performed. The storage provider will now accept authentication assertions about Bob, issued by the IdP, so the users are capable to collaborate, and the files can be shared.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                  xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport"
                  entityID="https://serviceprovider.example.com/SAML">
    <Extensions>
        <alg:DigestMethod
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
        <alg:DigestMethod
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha256"/>
        <alg:SignatureMethod MinKeySize="256" MaxKeySize="511"
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
        <alg:SignatureMethod MinKeySize="2048" MaxKeySize="4096"
            Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
    </Extensions>
    <SPSSODescriptor
            protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor>
            <ds:KeyInfo>...RSA key elided...</ds:KeyInfo>
            <EncryptionMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
            <EncryptionMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
            <EncryptionMethod
                Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
        </KeyDescriptor>
    ...
    </SPSSODescriptor>
...
</EntityDescriptor>
```

Fig. 4 Example of partial metadata instance (taken from [32]) for a provider that supports a number of signature and digest algorithms

Table 4 Knowledge base used by the *if–then* rules in the security and privacy risk aggregation engine

Confidentiality risk	Security and privacy risks			Integrity risk
High	*High*	*High*	*High*	High
High	*High*	*High*	*High*	Medium
High	*High*	*High*	*High*	Low
Medium	*High*	*High*	*High*	High
Medium	*High*	*Medium*	*Medium*	Medium
Medium	*High*	*Medium*	*Medium*	Low
Low	*High*	*High*	*High*	High
Low	*High*	*Medium*	*Medium*	Medium
Low	*High*	*Medium*	*Low*	Low
Authentication risk	High	Medium	Low	

The table shows the final output value of the security and privacy risk for all possible combinations of the three input variables (highlighted in italic)

Thus, the presented application scenario clearly illustrates how risk evaluation contributes to enhance the current landscape in Cloud Identity Federation and makes global scalability possible.

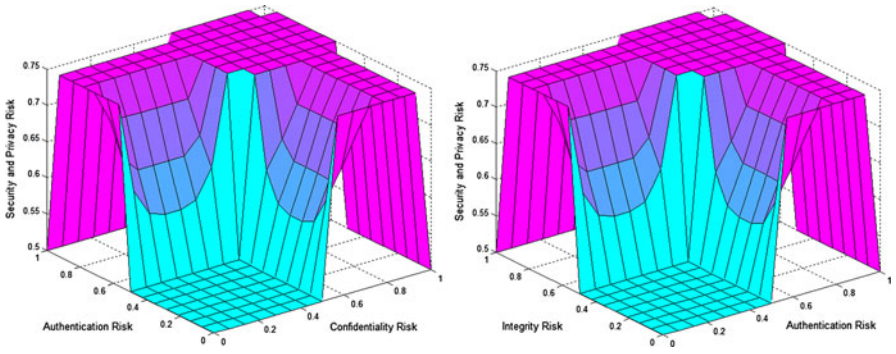

Fig. 5 Security and privacy risk surface for *Left*: all possible combinations of confidentiality and authentication risk values; *Right*: all possible combinations of integrity and authentication risk values

7 Related Work

Due to the increasing interest in the cloud computing paradigm, security is becoming an important concern for researchers since it constitutes the main barrier to adoption. Security surveys and recommendations are presented in [2, 33, 34]. Between the main security open issues, appropriate access control and identity management systems are frequently referred to as key required mechanisms for data protection in the cloud. In [35], the authors consider that the existing trusted third party (TTP) protocols may provide at least part of the security solution for cloud services, which supports the idea of using Single Sign-on models based on FIM technologies, such as SAML, Liberty Alliance, OpenID, WS-FED [36], or OAuth [37]. Furthermore, [5, 38] also identify that the federation of identities maintained by the multiple cloud service providers is critical for cloud-based service composition and application integration. Both works emphasize that the trust relation setup between cloud providers should be automatically established in order to reach a more scalable and flexible model that can meet cloud computing demands.

For these reasons, there is a growing body of work dealing with various cloud computing identity issues. The European Network and Information Security Agency (ENISA) published a series of guidelines regarding security [39], identifying "building trust on the cloud" as an immediate and interesting research direction. The National Institute of Standards and Technology (NIST) [40] and the Cloud Security Alliance (CSA) [41] are working on document drafts about security recommendations for the cloud, both considering identity and trust as key issues. Also, many other standardization organisms and research initiatives have recently included identity federation as an indispensable mechanism in its use-cases documents and whitepapers [6–8]. Apart from these emerging initiatives, current related work consists basically of recommendations and surveys regarding how to address identity management and trust issues in the cloud [5, 42–44].

However, there are still few concrete proposals and the existing ones tackle only a subset of the identity, trust and risk problems. Between the most relevant [45],

explores the concept of federation between clouds, but they assume that previous static trust relationships between providers exist based on Public Key Infrastructure (PKI) and digital certificates. There are also a few research papers considering identity management integration in the cloud landscape [46, 47], but they are still preliminary works on requirements analyses or high level architectures.

To summarize, most of the papers on the topic that can be found in the literature simply state that risk should be taken into account in the decision making processes for the establishment of federated trust relationships. Nevertheless, works defining how to assess risk are scarce and the nature of the current proposals is mainly qualitative.

As far as our work is concerned in [10], we made a comparative analysis of the underlying trust models in the current identity federation frameworks, which led us to assert that dynamic secure federation is not possible nowadays. Thus, we made a first proposal that consisted of adding new components and protocols so that entities could gather information and make dynamic decisions in real time.

Since then, increasing interest has developed around the possibility of ad-hoc dynamic federations, which can be derived from the recent specification released by the European Telecommunications Standards Institute (ETSI) [48].

In [11], we extend the generic trust management model called PTM (Pervasive Trust Management) [49]—that was focused on limited devices—to include risk management, online reputations, and SLA (Service Level Agreement) negotiations. The proposal here, based on this previous research, it is focused on federated infrastructures and is the unique work on risk management in the different phases of a federation. We have extended our ideas based on the understanding that risk assessment is vital when making decisions in uncertain environments. The methodology and initial metrics presented in this paper will be used to implement a risk calculation module and complete a prototype entity capable of engaging in dynamic federations.

8 Conclusions and Future Work

In order to overcome the limitations of the current static features of FIM systems and contribute to allow the global scalability required for the success of cloud computing, it is required to define new trust models that allow the dynamic creation of federations. So, since risk evaluation is a vital component for this purpose, it must be considered as a key enabler to foster collaboration between previously unknown parties. The work presented here contains several unique contributions. First, we provide a novel taxonomy that reflects Federated Identity Management as a two-phased procedure, encompassing both bootstrap and evolution stages. This innovative distinction will help in the identification of risks involved at each phase and can be used as a central piece to define risk metrics that are relevant for quantification. Second, a set of initial metrics has been introduced that are useful to compute risk. Furthermore, a hierarchical aggregation system has been proposed and an illustrative application of risk computation in cloud computing scenarios has been described.

In future work, our main goal is to derive a more extensive set of metrics and provide not only a semantic description but also the detailed numerical values. The whole risk model based on these metrics will be used as part of the decision making procedures in dynamic federated environments. Thus, the derived risk calculation module will be used, together with the extensions proposed in [10], to complete a prototype entity capable of engaging in dynamic federations.

Acknowledgments This work was supported in part by the Spanish Ministry of Science and Innovation under the project CONSEQUENCE (TEC2010-20572-C02-01). The authors would like to *thank* the *anonymous reviewers* for their valuable comments and suggestions to improve the quality of this paper.

References

1. Mell, P., Grance, T.: The NIST definition of cloud computing. National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2009). Accessed 15 June 2012
2. Jensen, M., Schwenk, J., Gruschka, N., Iacono, L.L.: On technical security issues in cloud computing. In: Proceedings of the IEEE International Conference on Cloud Computing, pp. 109–116. Bangalore, India (2009)
3. Harauz, J., Kaufman, L.M., Potter, B.: Data security in the world of cloud computing. IEEE Secur. Priv. **7**(4), 61–64 (2009)
4. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
5. Gopalakrishnan, A.: Cloud computing identity management. SETLabs Brief **7**(7), 45–55 (2009)
6. Hardjono, T., Rutkowski, M. (eds.): Identity in the Cloud—Use Cases Version 1.0, Draft Version 0.1q. http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.pdf (2011). Accessed 15 June 2012
7. Cloud Computing Use Case Discussion Group: Cloud computing use cases, Tech. Rep. Version 4.0. http://bit.ly/gjxdL7 (2010). Accessed 15 June 2012
8. Cloud Computing Use Case Discussion Group: Moving to the Cloud, Version 1.0. http://bit.ly/fuAkKF (2010). Accessed 15 June 2012
9. Open Cloud Manifesto: Open Cloud Manifesto. http://www.opencloudmanifesto.org/ (2009). Accessed 15 June 2012
10. Arias, P., Almenárez, F., Marín, A., Díaz., D.: Enabling SAML for dynamic identity federation management. In.: Proceedings of Wireless and Mobile Networking Conference, pp. 173–184. Gdansk, Poland (2009)
11. Cabarcos, P.A.: Risk assessment for better identity management in pervasive environments. In: Proceedings of IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 389–390 (2011)
12. Buyya, R., Broberg, J., Goscinski, A.: Cloud Computing: Principles and Paradigms. Wiley, New York, NY, USA (2011)
13. Boehm, B.W.: Software risk management: principles and practices. IEEE Softw. **8**(1), 32–42 (1991)
14. Jansen, W.: Directions in security metrics research. National Institute of Standards and Technology (NIST) Interagency Report, NISTIR 7564 (2009)
15. Maler, E., Reed, D.: The venn of identity: options and issues in federated identity management. IEEE Secur. Priv. **6**(2), 16–23 (2008)
16. OpenID: OpenID Authentication 2.0. http://openid.net/specs/openid-authentication-2_0.html (2007). Accessed 15 June 2012
17. Cantor, S., Kemp, J., Philpott, R., Maler, E.: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005
18. Liberty Alliance: Liberty Alliance ID-FF 1.2 Specifications. http://www.projectliberty.org. Accessed 15 June 2012
19. Cantor, S., Moreh, J., Philpott, R. Maler, E. (eds.): Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, March 2005
20. Kantara Initiative. http://kantarainitiative.org/. Accessed 15 June 2012

21. Terena TF-EMC2: REFEDs Federation Survey. https://refeds.terena.org/index.php/Federations. Accessed 15 June 2012
22. Hirsch, F., Philpott, R., Maler, E. (eds.): Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard (2005)
23. Gómez, F., Girao, J., Martínez, G.: TRIMS, a Privacy-aware Trust and Reputation Model for Identity Management Systems. Comput. Netw. Special Issue Manag. Emerg. Comput. Environ. **54**(16), 2899–2912 (2010)
24. Díaz-Sánchez, D., Marín López, A., Almenárez Mendoza, F., Campo Vázquez, C., García-Rubio, C.: Context awareness in network selection for dynamic environments. Telecommun. Syst. **36**(1), 49–60 (2007)
25. Burr, W.E., Dodson, D.F., Polk, W.T.: NIST Special Publication 800-63 Version 1.0.2, Electronic Authentication Guidelines. National Institute of Standards and Technology (NIST) (2006)
26. Tiffany, E., Madsen, P., Cantor, S. (eds.): Level of Assurance Authentication Context Profiles for SAML 2.0. Working Draft 01 (2008)
27. Kemp, J., Cantor, S., Mishra, P., Philpott, R., Maler, E. (eds.): Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard (2005)
28. Saaty, T.L.: How to make a decision: the analytic hierarchy process. Eur. J. Oper. Res. **48**(1), 9–26 (1990)
29. Calvo, T., Kolesárová, A., Komorníková, M., Mesiar, R.: Aggregation operators: properties, classes and construction methods. In: Calvo, T., Mayor, G., Mesiar, R. (eds.) Aggregation Operators. New Trends and Applications, pp. 3–104. Physica-Verlag, Heidelberg (2001)
30. Zadeh, L.A.: Fuzzy sets. Inform. Control **8**(3), 338–353 (1965)
31. Klir, G.J., Yuan, B.: Fuzzy Sets and Fuzzy Logic—Theory and Applications. Prentice-Hall, Inc., Englewood Cliffs, NJ, USA (1995)
32. Cantor, S. (ed.): SAML V2.0 Metadata Profile for Algorithm Support Version 1.0. OASIS Committee Draft (2010)
33. Bernstein, D., Vij, D.: Intercloud security considerations. In: Proceedings of the IEEE 2nd International Conference on Cloud Computing Technology and Science, pp. 537–544. Indianapolis, Indiana, USA (2010)
34. Almulla, S.A., Yeun, C.Y.: Cloud computing security management. In: Proceedings of 2nd International Conference on Engineering Systems Management and Its Applications, pp. 1–7. Sharjah, United Arab Emirates (2010)
35. Rimal, B.P., Jukan, A., Katsaros, D., Goeleven, Y.: Architectural requirements for cloud computing systems: an enterprise cloud approach. J. Comput. **9**(1), 3–26 (2011)
36. Goodner, M., Nadalin, A. (eds.): Web Services Federation Language (WS-Federation) Version 1.2, OASIS Web Services Federation (WSFED) TC (2009)
37. Hammer-Lahav, E. (ed.): The OAuth 1.0 Protocol. http://tools.ietf.org/html/draft-hammer-oauth-10 (2010). Accessed 15 June 2012
38. Sengupta, S., Kaulgud, V., Sharma, V.S.: Cloud computing security—trends and research directions. In: Proceedings of the 7th IEEE World Congress on Services, pp. 524–531. Washington DC, USA (2011)
39. Catteddu, D., Hogben, G.: Cloud computing: benefits, risks and recommendations for Information security. Technical Report, European Network and Information Security Agency (2009)
40. Jansen, W., Grance, T.: Guidelines on Security and Privacy in Public Cloud Computing. Information Technology Laboratory. National Institute of Standards and Technology (NIST). http://csrc.nist.gov/publications (2011). Accessed 15 June 2012
41. The Cloud Security Alliance (CSA): security guidance for critical areas of focus in cloud computing v3.0. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf (2011). Accessed 15 June 2012
42. Habib, S.M., Ries, S., Muhlhauser, M.: Cloud computing landscape and research challenges regarding trust and reputation. In: Proceedings of the Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing, pp. 410–415. Xi'an, China (2010)
43. Palson Kennedy, R., Gopal, T.V.: Assessing the risks and opportunities of cloud computing—defining identity management systems and maturity models. In: Proceedings of the IEEE 2nd International Conference on Trendz in Information Sciences & Computing, pp. 138–142. Chennai, India (2010)
44. Pearson, S., Benameur, A.: Privacy, security and trust issues arising from cloud computing. In: Proceedings of the IEEE 2nd International Conference on Cloud Computing Technology and Science, pp. 693–702. Indianapolis, USA (2010)

45. Casola, V., Rak, M., Villano, U.: Identity federation in cloud computing. In: Proceedings of the IEEE 6th International Conference on Information Assurance and Security, pp. 253–259. Atlanta, USA (2010)
46. Celesti, A., Tusa, F., Villari, F.M., Puliafito, A.: Security and cloud computing: intercloud identity management infrastructure. In: Proceedings of the 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, pp. 253–259. Larissa, Greece (2010)
47. Ates, M., Ravet, S., Ahmat, A.M., Fayolle, J.: An identity-centric internet: identity in the cloud, identity as a service and other delights. In: Proceedings of the 6th International Conference on Availability, Reliability and Security, pp. 555–560. Vienna, Austria (2011)
48. ETSI GS INS-004V 1.1.1, Group specification: identity and access management for networks and services; Dynamic federation negotiation and trust management in IdM systems (2010-11)
49. Almenarez, F., Marín, A., Díaz, D., Cortés, A., Campo, C., García, C.: Trust management for multimedia P2P applications in autonomic networking. Ad Hoc Netw. **9**(4), 687–697 (2011)

Author Biographies

Patricia Arias Cabarcos received her Telecommunication Engineering degree in 2008 and MSc degree in Telematics in 2009, both from University Carlos III of Madrid. She is currently pursuing a PhD focused on the problem of identity management in open environments, with special attention to risk analysis and underlying trust models.

Florina Almenárez Mendoza received her Computer Science degree in 1999 from University Autónoma of Bucaramanga, her PhD degree from the University Carlos III of Madrid in 2006, and is currently an Associate Professor at UC3M. Her research interests include trust and reputation management models, identity management and federation, security architectures in ubiquitous computing, and SIM-based applications.

Andrés Marín López received a Telecommunication Engineering degree and PhD from the Technical University of Madrid in 1992 and 1996 respectively. He lectures in Computer Networks and Ubiquitous Computing in the University Carlos III of Madrid, as an Associate Professor. His research interests include ubiquitous computing: limited devices, trust, security services, and security in NGN.

Daniel Díaz-Sánchez received a Telecommunication Engineering degree from University Carlos III of Madrid in 2002. He graduated as Master Telematics Engineering (2004) and obtained his PhD (2008) from UC3M. He currently works as an Associate Professor at Universidad Carlos III. His research topic is distributed authentication, authorization and content protection activities, and identity management.

Rosa Sánchez Guerrero received a Telecommunication Engineering degree from University Carlos III of Madrid in 2009 and she obtained the MSc degree in Telematics in 2011. Currently, she works as researcher within the PerLab research group in the UC3M. Her research topics include the problem of identity management, security and privacy in healthcare.