Computer Networks 122 (2017) 29–42

Contents lists available at ScienceDirect

Computer Networks

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

Cloud identity management: A survey on privacy strategies

Jorge Werner*, Carla Merkle Westphall, Carlos Becker Westphall

Post-graduate Program in Computer Science, Federal University of Santa Catarina, P.O. Box 476, 88040-970, Florianópolis, SC, Brazil

ARTICLE INFO

Article history:
Received 5 September 2016
Revised 23 February 2017
Accepted 7 April 2017
Available online 13 April 2017

Keywords:
Privacy
Identity management
Cloud computing

ABSTRACT

With the rise of cloud computing, thousands of users and multiple applications have sought to communicate with each other, exchanging sensitive data. Thus, for effectively managing applications and resources, the use of models and tools is essential for the secure management of identities and to avoid compromising data privacy. There are models and tools that address federated identity management, and it is important that they use privacy mechanisms to assist in compliance with current legislation. Therefore, this article aims to present a survey of privacy in cloud identity management, presenting and comparing main features and challenges described in the literature. At the end of this work there is a discussion of the use of privacy and future research directions.

1. Introduction

Cloud computing aims to improve the management of computing resources by combining concepts such as elasticity, on-demand use, and dynamic resource allocation [1,2]. The shared use of resources by different users and a very high amount of data and information, such as in *big data* applications, impose an additional level of confidence in service providers. In this context, the Identity Management (IdM) or Identity and Access Management (IAM) is increasingly being used to control identity data and to provide access control facilities. However, integration between cloud computing and identity management systems remains a challenge, especially regarding privacy issues [3].

There are some identity management tools with proper peculiarities [4,5], using different mechanisms to address privacy. However, even using IdM systems, leakage of user data, the distribution of unnecessary attributes, and a lack of control on the dissemination of personal data are recurrent in cloud environments [6–10]. Thus, to achieve cloud identity management and meet the current legislation, providers must protect the privacy of users, entities, data, and information throughout their lifecycle.

Our work establishes a relationship among identity management needs, privacy features, approaches, and challenges in the cloud environment. Models and techniques used to solve the privacy challenges in this context are described. Related work presents and proposes specific solutions, but sometimes they are not directed to dynamic environments and the cloud. In this paper we have identified the major privacy challenges to IdM in the cloud in the literature. The possible solutions, under development by our research works, are presented.

We think the success of cloud identity management systems are based on trust [9], an agreement on security mechanisms, the use of policies [8], and active user participation in choosing possible options [7]. The establishment of cloud identity federations, which are trust relationships, should consider trust metrics to construct the cloud dynamic federation environment [11]. An agreement on security options is used to combine privacy options among providers. Privacy and authorization policies should be transparent and granular in order to assist users in data dissemination and access control tasks. The user should have the opportunity to give consent about releasing his/her sensitive attributes, in a user-friendly and automated way.

This paper is organized as follows. Section 2 describes privacy in identity management in the cloud. Section 3 presents and compares IdM privacy techniques and models. Section 4 opens a discussion and proposes future research directions on key privacy requirements, identifying research challenges. In Section 5 we present some work in progress to answer the challenges. Finally, Section 6 concludes the paper.

2. Privacy in identity management in the cloud

Privacy refers to the ability of individuals to protect information about themselves (their own information) [10,12,13]. The exchange of sensitive data is intense in large-scale scenarios of cloud computing, with several federations, where multiple Identity Providers (IdP) and Service Providers (SP) work together to provide services. Therefore, identity management should provide models and privacy mechanisms in order to manage the sensitive data of its users.

* Corresponding author.
E-mail addresses: jorge@lrg.ufsc.br, jorge.werner@gmail.com (J. Werner).

http://dx.doi.org/10.1016/j.comnet.2017.04.030
1389-1286/

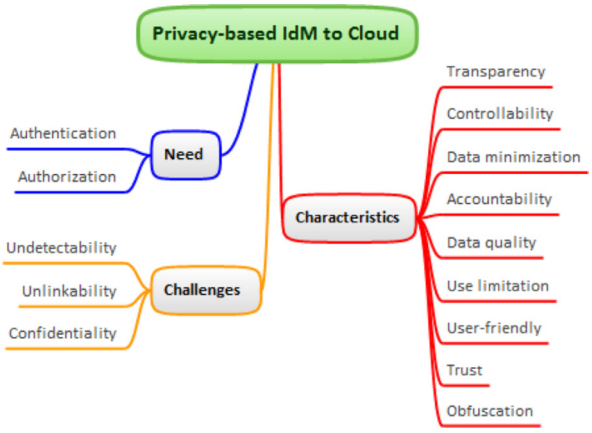


Fig. 1. A mind map about Privacy-based IdM to Cloud.

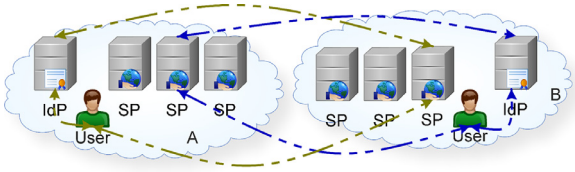


Fig. 2. Identity and Access Management (IAM) Systems.

Fig. 1 presents the components necessary to manage identities, the main IdM privacy challenges, and features in the cloud.

2.1. Identity management concepts

Identity management (IdM) is the process of creating, managing, and using identities, and the infrastructure that provides support for these processes. In IdM, each person or application is identified by a credential, which represents a set of attributes, issued by a reliable source [14,15]. A person could have a credential composed by his/her name and birth date. An application could have information such as a URL, identifier, and public key in its credential [3,16–18].

Cloud environments require IdM systems that can cooperate dynamically with each other by exchanging data and resources in a flexible way. User credentials can be created and validated in identity providers to be used by different cloud service providers.

In Identity and Access Management (IAM) systems, shown in Fig. 2, identity providers and service providers are usually IdM components dealing respectively with authentication and authorization [19] in the environment:

- ***Authentication*** – process of identity verification, to ensure that the individual is actually the person who he/she claims to be. Authentication is the proof of ownership of the identification attributes. This is a fundamental and necessary step before allowing anyone to perform an operation in a system. The authentication process is performed in the IdP, which stores the attributes of users. After authentication, the IdP sends a token or credential to the service provider;
- ***Authorization*** – provides different access decisions (for example, deny or allow) in different parts or operations of a computer system. The type of access is determined by the identity of the person and the type of operation or part of the system that needs to be accessed. The authorization process is usually carried out in SP, using credentials received from IdP. The SP should use authorization policies to decide on the release of the requested resource.

Besides offering greater security in identity manipulation, one advantage of using an identity management system is the ability to use Single Sign-On (SSO). With SSO, from a single authentication in the home domain or IdP, the user is able to use other services in the same domain or circle of trust. The possibility of closing all sessions of access, with a single logout process, is named Single Sign-off.

A circle of trust can establish a federation among identities and service providers. A federation can be defined as an association, agreement, and trust between two or more domains specifying how identity information will be exchanged and managed for cross-domain identification purposes [7,8,11]. This agreement also defines the use of common protocols and procedures (privacy control, data protection, standardized data formats, and cryptographic techniques). A federation enables SSO of users, providing access to resources in different administrative domains that participate in the federation [7,20].

Federated Identity Management systems (FIdM) are important for any online service in a public, private, or hybrid autonomous cooperation system [21] because it facilitates the sharing of resources between partners.

2.1.1. IdM Technologies

There are tools for creating federated environments. Some tools use SAML (Security Assertion Markup Language) to exchange data between IdPs and SPs such as Shibboleth [5], while others use JSON (JavaScript Object Notation) such as OpenID Connect protocol [4].

SAML is an XML-based security language specification and defines standard authentication, attribute, and authorization decision assertions, to be exchanged among identity and service providers. Shibboleth uses SAML and has future plans to add non-XML identity protocols [22].

The OpenID Connect is open source, has a standard protocol, has a native support for dynamic associations, and as it uses a lightweight message format (JSON), it fits mobile environments.

SAML federations are usually static, i.e., metadata should be placed in defined directories and some configuration data must be shared among IdPs and SPs in order to establish the federation. These metadata describe participants of the federation and are cryptographically signed by the federation manager [11,23].

OpenID Connect does not have the same type of federation as Shibboleth. While Shibboleth requires a strict notion of affiliation to an institution or group, OpenID Connect allows dynamic client registration when clients can register themselves automatically at a provider. Unfortunately, it means a provider will trust any client that asks and provides it with user information. Because of this facility, a dynamic federation can easily be defined [24]. There is work in progress to build OpenID Connect federations that use federation operators to build the identity trust [25].

2.2. Cloud IdM challenges

IAM systems have to scale to fit cloud environments. According to [6,24,26–30], the following major IAM functions are essential for successful and effective management of identities in the cloud:

- **Identity provisioning/deprovisioning** – provision and deprovision of identities to users in the cloud needs extended management to achieve correct and secure use of identities among providers. In the cloud, it is also necessary to have automated management for identities and provisioning privileges;
- **Authentication and federation** – users can authenticate in their home enterprises IdPs, using different authentication methods when there is a federation. Federation is a key feature to enable interaction in clouds and has challenges to manage

the identity lifecycle, authentication methods, federation standards, and token formats. A user-centric approach, when users have more control over their credentials among multiple service providers, is desirable in cloud environments. Authentication assertions can use SAML or JSON formats;

- **Authorization and attributes management** – authorization depends on the correct set of attributes information in order to make policy decisions. This is a challenge since different access control rules should be applied to sets of users in a multi-tenant cloud environment. It is necessary for the cloud service provider to have attributes information as well as authorization policies available. Notification about creation/removal of accounts/permissions and audit logs helps to control the use of cloud services, since much information needs to be shared among identity and service providers. The XACML (eXtensible Access Control Markup Language) can be used to represent the access control policy in a standard way. The development of privacy policies is another challenge.

The Cloud Security Alliance (CSA) and the Kantara initiative are now addressing the evolution of IAM aspects. The CSA is focusing on IAM for IoT (Internet of Things) [31]. The Kantara [32] is dealing with research about challenging topics for online services: digital identity, user-managed access, and privacy protection standards.

In [19] there are three ways listed to implement identity management in cloud environments: in-house, as a service, or bundled in service providers. When using the in-house option, identities are issued and managed by user enterprises. IdM delivered as an outsourced service, used by other enterprises and consumers, is called IDaaS (Identity as a Service). There are commercial IDaaSs available. An IDaaS provider can maintain a complete set of employee data or only pseudonyms of employees. In the third option, when IdM functions are bundled in service providers, each cloud service provider may implement a set of identity management functions independently. A different set of identities is required by user companies for each service provider.

According to our point of view [6,24,28], the dynamic nature of cloud computing raises new ways to establish trust relationship as a federation among cloud providers.

It is a challenge to have dynamic federation establishment when policy and privacy agreements should be performed. The dissemination of private data should be controlled, rather, with the user consent.

2.3. Privacy challenges and characteristics

The right to privacy encompasses the intimate sphere of the person who wants to control his/her personal data from the collection, storage, manipulation, and dissemination, without the interference of third parties [10,33–36].

According to the United Nations in its Declaration of Fundamental Rights, Article twelve [37], privacy is a fundamental right, everyone is entitled to privacy, and it must be guaranteed by legal means. In addition, the human rights council [37] declares that the rights that every citizen has in the offline environment should be extended to the digital environment.

Protecting the privacy of any computer system is a technical challenge. In a cloud environment this challenge is complicated by the distributed nature of clouds and possible lack of consumer awareness about where the data is stored and who has access to such data [38]. There should be the possibility of self-management of privacy due to legal claims so that the person can be responsible for his or her information [39].

Privacy is also a challenge in IdM since IdM systems share sensible identity attributes, called Personally Identifiable Information (PII) [14,15,40]. In IdM there is much concern about privacy, data protection, compliance with the rules, volume of information exchanged between different domains, dynamic exchange of information, execution of policies, consent from users, and control of credentials [41]. It is essential to comply with current legislation regarding the identity lifecycle while maintaining privacy in the exchange of data between different environments and providers.

In this way, identity management must meet the following challenges [42]:

- ***Undetectability*** – to hide transactions performed by the user, preventing the detection of the users actions in a given system;
- ***Unlinkability*** – to hide the connection between user identities and history of transactions (e.g., subjects, messages, events, actions [43]);
- ***Confidentiality*** – to enable the users control over the dissemination of their attributes.

The properties of undetectability, unlinkability, and confidentiality are related because they are concerned with defining actions or methods to deal with the parties involved in access to a range of private and sensitive data.

Privacy in the cloud environment must also involve mechanisms or specific characteristics that consider the dynamics of the environment. If privacy cannot be ensured in the cloud, users may not be willing to use these services [44].

In this section, we list the characteristics that we consider important for identity management in the cloud with an emphasis on user privacy. A survey of the characteristics sought to consider important points to ensure the privacy of sensitive user data used in identity management, considering the dynamic exchange of information in the elastic environment of cloud computing.

Current literature [45] does not exactly include privacy features for identity management in the cloud. Some authors treat only the features covered in their work, such as strong authentication [46]. Other authors address the privacy of data stored in the cloud environment [47], or identity management [48] without considering the cloud. Our selection of features seeks additional points of privacy of the standardized privacy principles [14,15,49]. Thus, a taxonomy was proposed as an extension of the privacy features presenting the different ways of treating privacy in IdM systems in the cloud. Fig. 3 represents the taxonomy relating the characteristics identified in the literature with the mechanisms identified in this work.

- **Transparency**: refers to the notification about the use of attributes. The environment shall be transparent and shall give notice to individuals about collection, use, disclosure, and modification of Personally Identifiable Information (PII). Transparency generally implies *advertence* or *consciousness*. The advertence provides alerts about the use of attributes or profiles, and consciousness promotes awareness by detailing information about the lifecycle of disseminated data;
- **Controllability**: refers to the options to enable the use of attributes, and is the effective control over data. An IT system must provide holders with effective means of data control over their personal data. It should involve the individual in the use of PII and, when possible, seek their individual consent to collect, use, disclose, and handle the personal data. Control is addressed by *selection* and/or *consent*. Selection means that the user chooses what data will be available to access the resource. When the users consent, they agree to the use of their data using pre-defined profiles of the system;
- **Minimization**: allows the user to forward only the information needed to access the resource. There should be a minimum spread of data within the cloud, especially in the access control process. The strategies for the minimization of disseminated attributes are linked to the control over the dissemination of data. The systems can allow the user a *control*, assigning

Fig. 3. A mind map: Taxonomy for Privacy-based IdM to Cloud.

to the user the possibility of selecting the attributes that must be disseminated, or, on the other hand, only allow the users *participation* in the dissemination of attributes, when the user can opt for minimization strategies in the dissemination of attributes;

- **Accountability**: represents auditing and tracking actions, in accordance with legal requirements. It is a way to dynamically trace the footsteps of data and users, using history and location of identity and linked attributes. Thus, it is possible to identify misuse and privacy breaches between different identity and service providers, enabling audit actions. Laws require identification and punishment of those involved in case of unauthorized access or malicious use of the data accessed. Current research projects seek *traceability* solutions, monitoring user data without compromising data privacy. The adoption of *policies* is also an alternative used to establish effective means to exchange specific audit rules;
- **Data quality**: refers to checking and validation of attributes. It is necessary to ensure the integrity of personally identifiable information, confirming and validating the data, so that the individuals privacy is preserved. Data may or may not be externally checked. The system can implement a verification about the veracity of the information, with a process that determines the degree of *validity* of the data. If not validated, the system assumes *confidence* in data, considering the existence of a reliable federation environment;
- **Use limitation**: only authorized entities should have access to personal data, ensuring the confidentiality of data. The limitation of use can be accomplished by *policies* and *obligations*. A policy, as a set of rules, can represent the reason or intention for using the data. An obligation is a directive that must be carried out before or after access is approved;
- **User-friendly**: refers to the ease of using applications with privacy features. Functions and related facilities to privacy must be friendly, that is, applications should provide sufficient help and simple interfaces to be used by less experienced users as well. The solution should include a user interface that lets users manage their different identities, check what data was released under what conditions, and to whom. Thus, the user can give informed consent and can view past transactions [50]. Basically, this item is linked to the ease of using the different strategies. Thus, how the component or technique is implemented is evaluated, and how it is made available to users with or without the addition of *extensions* (*add-ons*).
- **Trust**: refers to confidence verification using metrics such as reputation and risk. In an elastic and dynamic cloud environment where several providers communicate with different users, it is essential to create ways to keep or ensure the confidence among parties. Current studies seek to improve mechanisms to evaluate providers dynamically through *risk* and/or *reputation* measures;
- **Obfuscation**: refers to the use of techniques of *anonymity* or *pseudonyms*, important in federations where users have applications of different contexts. Users do not send their attributes to the provider and because of that, for example, potentially identifiable information such as the users IP address or location cannot be revealed. Different approaches are proposed in the literature using nicknames (anonymity or pseudonyms).

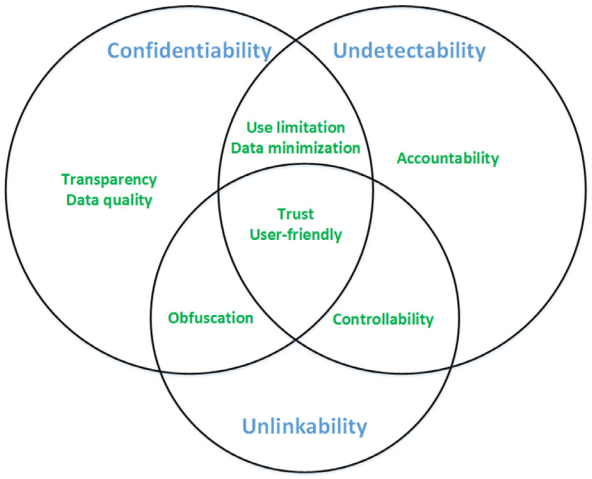


Fig. 4. IdM privacy–features versus properties.

In the literature there are various mechanisms and technologies used to ensure effective treatment of the privacy features presented, called Privacy-Enhancing Technologies (PETs). In this paper we emphasize a study on the necessary features for privacy in IdM systems, not necessarily involving mechanisms or technology used to ensure the functioning of the system with privacy.

In Fig. 4 we show the relationship among the privacy properties in IdM systems [42] and features grouped in this work. The relationship shows that it was possible to thoroughly address each privacy point.

3. Privacy in cloud IdM models and techniques

The issue of maintaining privacy in identity management systems in the cloud is our main question to be answered through this literature analysis. This section describes the main works related to IdM and privacy in the cloud.

The process used for the collection of works related to this research is presented in Section 3.1 through a systematic mapping. In Sections 3.2, 3.3 and 3.4 works are presented and discussed.

3.1. Systematic mapping

A systematic review to identify and analyze the most relevant proposals in the literature was carried out. To perform the study, we used principles proposed by [51] in its systematic mapping.

The work of [51] declares that a systematic mapping enables a broader view of the studies is aimed at data extraction, covering the development of the research question and an assessment of the quality of studies.

The main goal of this mapping is to identify the initiatives in scientific studies that address the privacy issue in cloud identity management. Thus, we would like to answer the following research questions:

- What is the necessary identity management model in cloud computing environments to ensure the privacy of entities?
- What are the best techniques to address the lack of privacy control in the interactions?
- How should an agreement among identity management federation partners be developed to address the lack of privacy in authorization and authentication procedures?

In order to answer the research questions, the search used the following keywords: *Identity Management, IDM, Privacy, Cloud Computing* and *Cloud*.

After applying keywords to the search, 198 research papers were located. For a more refined selection of studies a manual selection of papers was necessary considering some exclusion and inclusion criteria. The inclusion criteria were the title and summary analysis of publications considered relevant. The exclusion criteria were the content of each one of the selected publications; items that were not related to the subject of the search were removed. Finally, applying the inclusion and exclusion criteria, we selected scientific work that is highly relevant to the study.

Besides identifying studies to answer the research questions, we also aim at classifying approaches. This step is critical for the analysis of the results. Thus, the resulting mapping will serve as an indication of possible research directions .

3.2. IdM projects with privacy

In this section we describe some of the key projects that address privacy issues in identity management.

PRIME (Privacy and Identity Management for Europe) (2004 – 2008) – was a project funded by the European Union [52], developed between 2004 and 2008. The project aimed at developing a working prototype of an identity management system for enhanced privacy. This project was concerned with the spread of personal data and with secure interaction in order to keep track of peoples data [53].

PRIMELIFE (2008 – 2011) – The Primelife project [54] was a consortium of several companies (IBM, W3C, Microsoft and others) and institutions in Europe (University of Milano, University of Dresden and others). Primelife addressed the understanding of identity management issues for practical life, including privacy on the web and its applications, to develop friendly tools for identity management [55].

ABC4Trust (2010 – 2015) – ABC4Trust is a European Union (EU) funded research and development project advancing the federation and interchangeability of technologies supporting trustworthiness, and at the same time, privacy-preserving Attribute-based Credentials (Privacy-ABCs) [56]. The project had proposed anonymous credentials and the use of sticky policies. The access control model uses identification cards, which requires appropriate hardware for the entry of the participants.

GÉANT (2015 – 2016) – GÉANT is an association of members with operations managed through its legal entities in the Netherlands and the United Kingdom. GÉANT serves the research and education networking community in Europe, helping them to deliver innovative networks, technologies, and services for research and education. The current GN4-1 Research and Education Networking group has worked in research of the Identity & Trust Technologies for GÉANT Services (JRA3) [57]. They have, as a work item, the production of a proof-of-concept implementation of an OIDC (OpenID Connect) identity federation. The project is seeking a model of dynamic federation to integrate different existing federation technologies.

PRISMACLOUD (Privacy and Security Maintaining Services in the Cloud) (2015 – 2018) – PRISMACLOUD research has three main concerns: confidentiality of data, verifiability of features for the cloud, and privacy of users interacting within a cloud environment. The aim is to develop cryptographic tools that protect the security and privacy of user data during its lifecycle in the cloud. In particular, the project focuses on the development of secure and efficient storage solutions and privacy, preserving yet verifiable computing on authenticated data. To protect user privacy, the project proposes applying privacy enhancing technologies, for example, implementing data minimization strategies and efficient data anonymization. Three different use-cases from different application domains will be used to demonstrate and evaluate the potential of the project outcomes. The PRISMACLOUD project receives funding from the European Unions Horizon 2020 Research and Innovation program, Project ID: 644962 [58,59].

CREDENTIAL (Secure Cloud Identity Wallet) (2015 – 2018) – CREDENTIAL aims at developing friendly privacy means for storing and sharing personal data in the cloud. It also aims for identity and access management as a service system, supporting publicly certified identity data. The vision of CREDENTIAL is to develop solutions with cryptography to protect user data. The CREDENTIAL project receives funding from the European Unions Horizon 2020 Research and Innovation program, Project ID: 653454 [59,60].

Table 1 lists the main characteristics identified related to identity management and privacy in cloud computing environments from the projects found in the systematic review.

The relationship between the privacy features for IdM in the cloud and the taxonomy of the strategies addressed in each research project is presented. Research, while conceptually compre-

Table 1
Projects models versus privacy-based IdM characteristics to cloud.

Privacy-based IdM characteristics	Prime [53]	PrimeLife [55]	ABC4Trust [56]	Géant [57]	Prismacloud [58]	Credential [60]
Transparency	advertence	consciousness	consciousness	consciousness	consciousness	consciousness
Controllability	consent	selection	selection	consent	consent	consent
Minimization				control	control	control
Accountability				traceability	traceability	traceability
Data quality	confidence	confidence	confidence	confidence	confidence	confidence
Use limitation		policies	obligations			
User-friendly	with add-ons	with add-ons	with add-ons			
Trust		reputation	reputation			
Obfuscation		anonymity	anonymity	anonymity		

hensive, still requires a major practical evolution of standards, protocols, and agreements, as well as completely open systems.

The IBM company developed Identity Mixer (Idemix) as part of the PRIME architecture. Idemix uses pseudonyms, partial identities, and controlled attribute release, with strong privacy protection. PrimeLife produced a wide variety of results, including several small prototypes. Among the results is that the development of Idemix continued, because of the need for applications supporting libraries with anonymous credentials. PrimeLife has also developed PrimeLife Policy Language (PPL), offering an approach to privacy-enhanced access control and data handling. The ABC4Trust project advanced the research around attribute-based credentials preserving privacy. The project developed two pilot applications in real-life settings in Sweden and Greece. The Géant project worked for the standardization and collaboration among SAML Federations, OpenStack Clouds, and OIDC. The Prismacloud and Credential are projects in progress that already present some cryptographic tools such as homomorphic proxy and anonymous signature.

3.3. Privacy proposals in the cloud

In this section we present research that brings relevant mechanisms of privacy into cloud computing.

The intense exchange of data between different cloud providers can generate problems due to legal compliance and the trust of users. Research presented in [61] argues that the method to protect privacy in cloud computing must meet the intense dynamic data exchange. The related research proposes a new anonymous algorithm for cloud computing services. Data are only sent to the network after processing by the algorithm so that the data are spread with identifiers that do not reveal the true identity of the user. The anonymity mechanism proposed would be more efficient than traditional encryption technology because it is more flexible to use, not requiring the restoration of data or the use of cryptographic keys. The strategy uses a proposal for partial identifiers, for example, not identifying the exact user occupation, only to inform in a generic way. The proposal is defined by the authors as a *quasi-identifier*. This proposal is not focused on IdM systems, but can be adapted for use in systems in IdM, for example, as an anonymization technique.

Article [62] discusses an approach of agents to monitor the cloud computing environment, proposing an audit service (SaaaS, Security Audit as a Service), based on service level agreements for security (SSLA, Security Service Level Agreements). The proposal implements intelligent agents in various parts of the cloud environment. The agents monitor the environment, taking into account existing recommendations and standards (ISO 27001:2005, ITIL), which deal with privacy of an environment with appropriate audit trails, thus treating the traceability of actions.

The work proposed in [63] acts as an IaaS integrated security module and also as a TPM (Trusted Platform Module). The solution creates keys protected by hardware that are entered and monitored in order to ensure reliability in the operation of virtual machines. The work acts on privacy issues and confidentiality of data on different servers in the cloud, considering the whole life cycle of virtual machines.

Article [64] performs a broad discussion on trust in cloud environments by dividing the responsibility of accountability in layers using policy-based techniques. The environment is modeled in five abstraction layers, where each layer would be responsible for a number of related problems. For example, the policy layer and the laws and regulations layer would be responsible for treating personally identifiable information for the whole process involving the distribution, audit, forms of control, location, means of access, validity, care of the violation, and manipulation of data.

A dynamic security model providing different levels of security and privacy for cloud computing, as well as a model that meets the regulatory and reliable challenges is proposed by [65]. The work [65] proposes to solve the privacy problem in shared data using encryption mechanisms for public audit, data privacy, and privacy of identity. The engine is able to efficiently check the integrity of data shared without recovering the entire file. The authors provide mathematical and logical evidences, without a practical implementation of the suggested cloud environment.

3.4. Privacy proposals in IdM

A proposal to manage privacy based on customers is addressed by [66], reducing the amount of sensitive information sent to the cloud. The architecture provides a privacy manager focused on the client that must contain a minimum set of requirements: the minimization of data; the data use limitation; the purpose of using data; user-centered; and be transparent. The service provider should comply with laws and regulations. The work does not provide details and does not validate the proposal; only the system modules are presented.

The work proposed by [67] performs an extension in single federated authentication systems to provide privacy and identity management. The extension allows users to control and enforce their privacy requirements, and finally, the proposal was assessed with Colored Petri Nets. The work considers it important to meet the following privacy requirements: control of data, use limitation, data minimization, bargaining (agreement between the parties), data validation, warning about collecting data, and auditing. For that, privacy should be decided by the user; thus, there is a negotiator module coupled in environmental entities. The user defines which data will be used for authentication and authorization to access the application through a sensitive data protocol agreement, and may also use anonymity.

Article [36] proposes an approach for entity-centric IdM in the cloud, named IdM Wallet, which uses an active package scheme. The active bundle is a container that includes metadata, access control policies, personally identifiable information, and the virtual machine (a virtual machine manages and controls the program code enclosed in a bundle). Zero-knowledge proof is used for the authentication of an entity without revealing its identifier, i.e., an anonymous identification. With this proposal it is possible to use identity data in unreliable hosts and to minimize sensitive data on the network, providing only the necessary attributes for each service provider.

A model for cloud identity management infrastructure in federated scenarios called InterCloud, composed of hundreds of clouds, is described by [27]. The model considers it important to support various authentication technologies used by each cloud provider, and a single authentication for accessing resources within a security context. Thus, the work defines an authentication module that manages the process. The proposal uses SAML (Security Assertion Markup Language) messages, showing the steps of message exchanges. Basically, the proposal focuses on the interaction and trust among parties to achieve federated authentication.

Article [7] addresses the lack of transparency and control in exchange of user identification information between IdPs and SPs in federated environments. The idea is that the users can, before accessing the service, check which attributes related to their identity is being sent to the service provider, allowing them to select the attributes they want to share with the SP. To validate the model, an extension of Shibboleth IdP was developed, the module gives users better control over data IDs stored in the systems. Thus, the user would know which data are required by SP and could then choose to access the SP without sending any extra data.

Article [68] defends an approach based on sticky policies, that is, conditions and restrictions attached to data, describing how data should be treated, enabling compliance and enforcement of current requirements. The approach is broad but does not make clear the means to ensure the effective implementation of sticky policies after receiving data.

The work of [9] proposes a shared dynamic management solution with features on demand preserving user privacy. The approach defines a new SAMLv2 assertion, thus ensuring compatibility between different cloud providers. The privacy preference service provides an interface for setting user preferences on the processing of personal data and specifies options for the use and disclosure of confidential information. The system allows users to access cloud services and digital content, without necessarily revealing their true identity, thanks to the use of multiple identities, depending on the context. Thus, the architecture provides a structure for keeping user privacy and a degree of control to obtain a suitable degree of customization in different cloud services.

Chadwick et al. [8] presents an authorization infrastructure based on policies for cloud providers; users can define their own privacy policies. To forward the policy to the service provider, the data of users are stuck to their policies (sticky policies), allowing better management of user preferences. The infrastructure trusts that providers will comply with the policies based on previously established legal contracts. The structure also includes modules for policy manipulation and a strategy for conflict resolution. Finally, the article conducts performance tests that show a small overhead associated with multiple decision points.

Article [69] presents an approach to manage privacy preferences. The proposal provides users with predefined default privacy settings, which can be customized according to users' purposes, assisting users when selecting identifying attributes. The approach is adopted within the Primelife privacy project to provide user-friendly interfaces. Conceptually, the policy language can be divided into three parts: commitments (the purposes for which the data are requested), a set of rules, and credentials (ID validation). A prototype called "*send data?*", was developed, which is an extension of the browser, and enables the user to define the data to be disclosed to the SP. The authors themselves mention that the features provided by the PrimeLife Policy Language (PPL) are very powerful, but at the cost of added complexity for implementation.

Work [70] addresses privacy and security issues that users face when sending data to cloud providers. It was proposed as a way to define how much users trust a particular service provider, based on a confidence level, so the user could send data to the cloud, encrypting data or not. To validate the model, a package called Privacy Data Envelope (PDE) was developed to transport the data. The PDE could also carry data use policies, defining who, how, where, and when data can be used, and what actions can be performed with them.

Camenish et al. [71] proposes a unified language for privacy technologies, covering the entire lifecycle of privacy, including the issue, presentation, inspection, and revocation of identity. The authors argue that someone should reveal only data that is strictly necessary for requested operations. The proposal considers five entities: users, issuers, checkers, inspectors, and authorities of revocation, which carry out interactions according to the purpose of resource usage. The entities use different encryption mechanisms, such as pseudonyms for identification to avoid correlation attacks.

Article [47] proposes an authentication and authorization protocol that describes the main characteristics of anonymous communication in the cloud. The solution employs identities generated through anonymous certificates, then assigns anonymous identities for registered users, thus adding a layer of anonymity. The structure is flexible and provides various levels of anonymity, using more than just a certification authority to issue anonymous certificates. The protocol is designed so that the real identity is never used for the actual communication, so the process is transparent to the user. The protocol can be integrated with existing identity management systems, providing anonymity as a cloud service.

The work of [72] proposes a solution for a single access to the desired resource that generates an authorization voucher distributed in two parts. One part of this voucher is generated by the IdM and another by the cloud environment, which is then compared to allow or deny access. The solution tries to overcome network monitoring attacks, considering the high use of mobile devices. A double proof could validate access and increase security since the attackers would have difficulty both for the capture of these two vouchers and to relate the vouchers to the same identity.

The proposed architecture of [73] has a semantic authorization module to be used in cloud environments. The proposal has a knowledge base that stores the authorization rules and instances of the information model representing the virtual infrastructure being managed. Finally, the article shows that by using semantic rules and authorization process information it is possible to determine and evaluate the access required.

The work [74] describes an architecture named BlindIdM - a model that implements an identity management system as a service. The objective is to provide a cloud IdM service that can forward data blindly. The system allows the handling of personal information for access control, without the knowledge of providers about the real identity of users. The work uses the SAML 2.0 identity management protocol in conjunction with encryption technology.

The work presented by [75] combines the use of encryption, policy management, and notification about the confidence level of service providers. The approach addresses the lack of control that users have over their identification data when registering on federated identity providers. Users can define their attributes dissemination policies, choosing which PIIs are released. However, having user-centric management of dissemination policies can cause problems, since the majority of users do not have sufficient knowledge about policy creation and management.

The work [29] describes a new architecture for identity management, based on the dynamic nature of cloud environments. The architecture consists of authentication, identity management, and policy modules. Access control uses different models for authorization through a PMP (Policy Management Point) module, but the proposal does not make clear how to implement it. Finally, the proposal is validated through an experimental test using OpenStack, Keystone, and Apache JMeter, measuring the scalability of requests.

The work [76] presents an approach to protect sensitive data in a scenario of *Big Data*. The framework adopts sticky policy by using an encryption-based identifier to support sensitive data security policies. The security policy model is specified formally, with definitions of actions, objects, subjects, rules, and policies. Finally, the model is applied to a case study in s healthcare scenario.

In [77] is a proposal in which the sticky policies are used to ensure control of the data in a heterogeneous environment, considering different hardware and software. The proposal suggests the use of TPM (Trusted Platform Module) mechanisms so that confidence in the implementation of policies is guaranteed. The work uses a hash tree structure to ensure data integrity. Finally, a prototype is implemented to validate the proposal.

The work [78] deals with data storage in the cloud, ensuring the protection of sensitive data. The proposal extends the OOXML (Office Open XML) document format with XACML (eXtensible Access Control Markup Language), defining a sticky policy to ensure the integrity and reliability of information. Cryptography-based

Table 2
Proposed models versus privacy-based IdM characteristics to cloud.

Publications		Privacy-based IdM characteristics								
References	Year	Transparency	Controllability	Minimization	Accountability	Dataquality	Use limitation	User-friendly	Trust	Obfuscation
Mowbray [66]	2009	X	X	X		X	X			X
Suriadi [67]	2009	X	X	X	X	X	X			
Angin [36]	2010		X	X						X
Celesti [27]	2010								X	
Orawiwattanakul [7]	2010	X	X	X						
Pearson [68]	2011		X				X			
Sanchez [9]	2012	X	X		X		X		X	X
Chadwick [8]	2012	X	X						X	
Angulo [69]	2012	X	X					X		
Betge-Brezetz[70]	2013	X	X	X						
Camenisch [71]	2013	X								X
Khalid [47]	2013	X								X
Ahmad [72]	2014								X	
Bernabe [73]	2014	X	X	X						
Nunêz [74]	2014									X
Weingätner [75]	2014	X	X	X						
Faraji [29]	2014		X	X			X			
Li [76]	2015	X	X							
Brown [77]	2015	X	X							
Ferdous [11]	2015		X						X	
Sprya [78]	2016	X	X							
Weina [79]	2016		X					X		

identity (IBE) is used as an authentication mechanism to ensure the XACML policy.

The research described in [11] addresses the management of dynamic identity federations. The proposal allows users to create federations dynamically between two prior unknown organizations. The issue of trust is also a key component of the discussions. Trust means the way IdP and SP federate: *fully trusted* – entities have a legal contract between IdP and SP; *semi-trusted* – entities are the SPs that have been added dynamically to an IdP inside a federation by a user but without any contract between IdP and SP; *untrusted* – entities are the IdP and SP added dynamically without the presence of any contract. A proof of concept is discussed using SAML federations and use-cases demonstrate the ideas proposed.

The research described in [79] introduces OpenID Connect as an authentication and authorization service in cloud-based diagnostic imaging systems. The objective of this study is to offer solutions for secure sharing of medical images among diagnostic imaging repository, heterogeneous picture archiving, and communication systems as well as Web-based and mobile clients in the cloud ecosystem [79]. OpenID-Connect-as-a-service also provides a centralized authorization mechanism, allowing owners of resources to define access control policies to protect their distributed sensitive data, such as health insurance and mental health records [79].

Table 2 lists the main characteristics identified related to identity management and privacy in cloud computing environments, throughout works found in a systematic survey.

In Table 2, many studies dealing with the control of the identity lifecycle, addressing privacy mechanisms, were identified. Many papers [7,8,75] show improvements in privacy as control, transparency, and data minimization. The tendency is to seek improvements in IdM systems to deal with requirements of various laws [6].

However, these related works do not present a complete framework that provides privacy mechanisms in IdM systems, meeting the dynamic characteristics of federations in the cloud. A federated cloud environment should provide dynamic services to users. Similarly, users should have effective control over the dissemination of their data. Elastic changes in the scope of applications should be reflected throughout the dynamic environment. Providers must receive reliable data and users should receive confidence metrics about servers.

4. Challenges and directions for privacy-based IdM to cloud

The rapid adoption of cloud computing, managing thousands of users and resources, needs models and mechanisms to protect users data. The previous sections showed several mechanisms that assist in the treatment of privacy threats. In this section we foresee some challenges to be addressed by future research in identity management considering actual personal data management and compliance with recent legislation. The challenges, shown in Fig. 5, intend to fill the outstanding gaps regarding the privacy features described in Section 2.3.

Throughout the identity management process flow in the cloud, there are privacy gaps that can be improved. These gaps or challenges exist in a dynamic identity management environments establishment and operation: reliability assessment; privacy agreements; definition of interaction profiles; control over the data spread; and the definition of the agreed policies.

4.1. Reliability assessment

Many research works [6,9,24,27,72] address the evaluation of trust among entities to establish an identity federation. Thus, a refined evaluation of trust can assist entities in the dynamic establishment of the federation, helping users during access decision processes. Currently there is some related research that deals with an assessment of the reputation of the providers [8,9], where it is possible to have a metric that evaluates the honesty of the accessed provider.

In our opinion, it is important to search for other reliable evaluation metrics. For example, risk assessment [80] can be useful in identity management. The risk of access by certain devices (e.g., mobile device, mobile, tablet), or means of access (e.g., private or public), can be an important point for confidence-building in accessing resources or in spreading attributes for a particular provider.

4.2. Agreement of privacy options

An agreement of privacy options for identity management systems is an important task that can assist organizations in establishing a federation [9,11,24,81]. The environment must have prac-

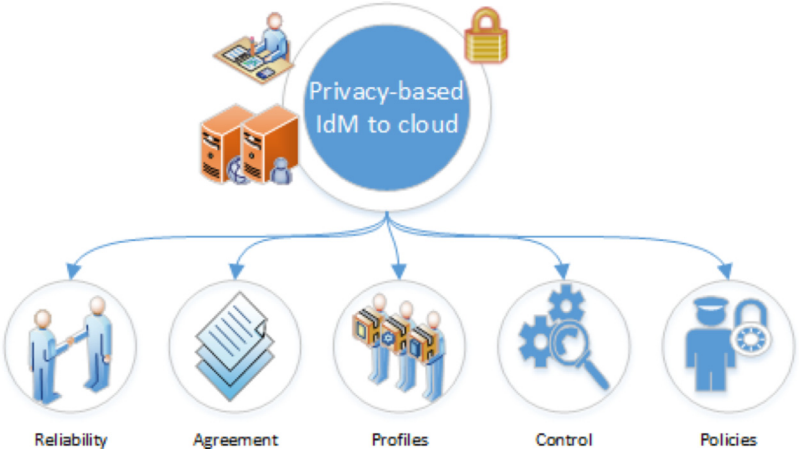


Fig. 5. Challenges and directions for privacy-based IdM to cloud computing.

tical and dynamic mechanisms to help the establishment of the cloud identity federation. Our proposal is to have an agreement of privacy options among identity and service providers in order to perform the federation process. Thus, there should exist a previous exchange of features and privacy criteria, agreed to by the providers. The interaction options should also include the possibility of having suppliers that do not address these privacy features, defining different forms of interaction. The communication agreement and use of different profiles should not be set statically, since this could hinder the process where thousands of service providers are interacting with each other.

The IdM systems should seek ways to interact in a dynamic and interoperable way. There must be integration mechanisms that allow communication between providers of different federations. Adaptations should guarantee environmental elasticity, without the user having to worry about the spread of data among providers.

4.3. Definition of interaction profiles

When we list characteristics about privacy in identity management, control and transparency in the dissemination of user data are some of the key points. These items can compose predefined standard profiles to assist users in data dissemination and access control decisions. A standard profile is a set of sensitive data or general attributes exchanged among interacting parties.

Some applications can have pre-established sets of profiles within the dynamic federation, according to the context [6,71,74,75]. Our research described in [6] proposes different standards of interaction profiles named: anonymous [71,74], pseudonym, partial attributes, and total attributes. In [75], the idea was to help users disseminate the least possible information to access the desired resource.

Using predefined profiles, it would be possible to access the resource with an anonymous user, without revealing any additional attribute or using an alias user, revealing only a nickname. It would also be possible to have only partial data dissemination according to the application context, automatically, for example, revealing payment information to the application that handles payment, and disseminating address data to the application that comes to delivery.

4.4. Grained control over the dissemination of data

The challenge addressed in this section deals with granular control [7,36,67,75] in the dissemination of personal attributes in different application contexts. The dynamic cloud environment requires fine control due to the wide range of applications that a single user can access. Section 4.3 discussed predefined templates to facilitate usability. However, mechanisms to enable granular control are needed to provide disclosure of partial attributes. So in specific contexts, the release of some individual attributes may be allowed. The partial dissemination of attributes allows the userowner of the attributes to choose and select which attributes can be disseminated at that time to the service provider.

In general, mechanisms should be improved to guarantee the validation of user attributes and the granular dispatch of attributes according to the application context. For example, the work of [75] allows the encryption of all user data stored in the identity provider, without evaluating the processing involved or the encryption method used. In our opinion, it would be useful to encrypt the attributes in a granular form to provide flexibility.

4.5. Ensure the implementation of policies

Policy definition can be a valuable mechanism to increase and ensure privacy. In cloud environments, where multiple providers are involved and are used elastically, the treatment of multiple access control policies may be essential [8,28]. Policies can behold legal policies, such as the regulations and laws of different countries; application policies, relating to the context and access profile; and data use policies, referring to the personal preferences of users.

It is essential that the application of different privacy policies [28] be guaranteed in an automated way, in the process of accessing a desired feature in the cloud. Thus, strategies to control access through policies must be guaranteed through an automated process. Some works [8] seek control over the implementation of policies, sticking policies, with user data.

The model of the authorization in the cloud must understand the multiple existing PDPs (Police Decision Point) and PEPs (Policy Enforcement Point) in different SPs and IdPs. Different access control models can be present, such as ABAC (Attribute-based Access Control), RBAC (Role-based Access Control), PBAC (Purpose-based Access Control), among others [29]. There are various privacy policy languages: EPAL (Enterprise Privacy Authorization Language), XACML (eXtensible Access Control Markup Language) and P2U (purpose-to-use) [82].

The application of policies in access control meets transparency requirements and control over the scattered data in the cloud among different service providers; such features are addressed in works such as [6,7]. The sticky policies [8] contribute to the effective control over the implementation of the policy. The compliance assessment about policies defined in the environment is a key challenge treated in various scientific research [8,28,67–69].

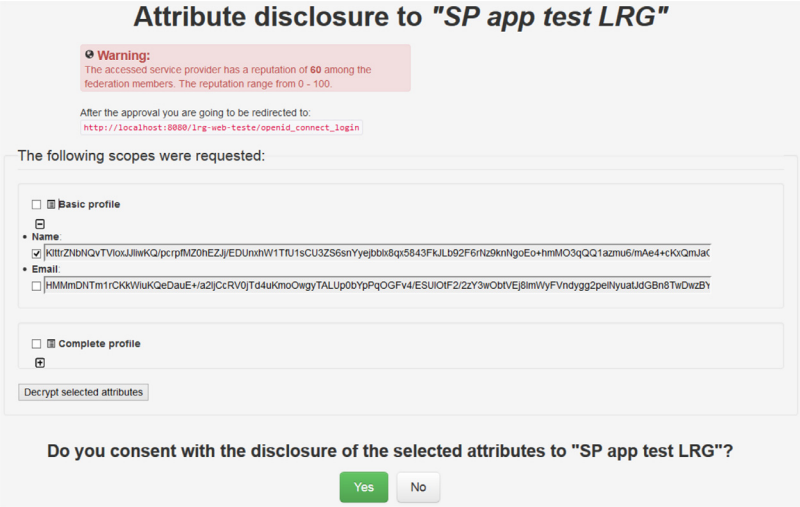


Fig. 6. Dissemination process extended [83].

5. Proposed solutions in progress

In this section we present some initial works that we are developing to solve the challenges listed in Section 4.

5.1. Sensitive data dissemination control

Users as owners of PIIs stored in IdPs have the right to effectively manage that data and have to be aware of any processing and disclosures.

The work [83] addresses privacy aspects found on IdPs of federated environments. On the one hand, it tackles the lack of control that users have over their PIIs stored in IdPs. On the other hand, it proposes improvements to add user support during the dissemination process, providing guidance to users, lowering the risks of unaware/unintentional data dissemination.

The proposal is that users encrypt their PII data before it is sent to IdPs. This way, users have more control over the data that is stored in IdPs, which prevents internal agents from using or disseminating PII data without prior consent and knowledge of the user [83].

Fig. 6 presents the dissemination page that was created, applying the proposal.

5.2. Privacy profiles on IdM

The work [6] presents an approach to address the issues involving privacy in the identity management systems around the PII. The proposal addresses three issues: the lack of PII control of users, the lack of models to assist users in data dissemination during the interaction, and the lack of user preference guarantees on the SP side. The work neither has changed the protocol nor the standard flow of interaction between the SP and IdP.

In this approach, the SP must support four minimum scopes, which are divided according to the profiles and access roles for each user: Anonymous Access, Access with Pseudonym, Partial Attributes Access, and Access with Total Attributes [6], as shown in Fig. 7.

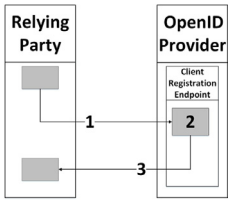


Fig. 8. Dynamic client registration flow [24].

5.3. Dynamic registering with privacy

The work [24] combines the concept of dynamic federation with privacy features proposed in [6]. The exchange of privacy scopes [6] is performed for a dynamic association between SP and IdP, improving the users privacy in dynamic federation solutions. This work uses the OpenID Connect (OIDC) to build the federation. The OIDC uses JSON (JavaScript Object Notation) Web Tokens instead of SAML, and unlike the SAML-based federations, the OpenID Connect has a good support for dynamic associations.

Fig. 8 shows the dynamic registering of Relying Party (RPs) in OIDC: in step 1, RP registration request; in step 2, RP registration; and, step 3, RP registration response.

```
{
 "openid_connect_protocol_supported_version": [
        "standard_openid_connect",
        "anonymous_openid_connect",
        "pseudonym_openid_connect",
        "partial_attribute_openid_connect",
        ]
}
```

Fig. 7. Scope choice in JSON format [6].

Fig. 9. Dissemination screen extended [28].

Table 3
Works in progress comparison.

	Paper			
Characteristics	Weingätner [83]	Werner [6]	Lucas [24]	Werner [28]
Transparency	X	X	X	X
Controllability	X		X	X
Minimization				X
Accountability				
Data quality	X			
Use limitation				
User-friendly		partial	partial	partial
Trust	X			X
Obfuscation				X

5.4. Model for IdM with privacy in cloud

The work [28] presents a privacy model for identity management systems in the cloud, considering a federated and dynamic environment [24], complying with the different laws and maintaining data privacy [6].

Fig. 9 shows the dissemination screen, presenting access scopes available. Users can choose among anonymous access, pseudonym access, access with partial attributes, or sending all of their attributes. The screen also displays a warning about the degree of trust of the provider registered dynamically in IdP. Thus, a better interaction is possible, allowing the control, transparency, and minimization of data sent [28].

6. Conclusion

This article presented a survey about privacy aspects in the cloud, describing characteristics in identity management and cloud environments. We also described and discussed privacy techniques that are in related works. We classified each one of the discussed works according to the presented characteristics. We presented and discussed the main challenges and directions to achieve privacy-based identity management in dynamic and elastic cloud systems. Finally, we presented the preliminary results to answer the privacy challenges, summarized in Table 3.

The initial results of our research combined the properties found in papers [8,9,70,75]. We encrypted users PIIs to prevent its use without users awareness and consent due to actions of curious/malicious entities [83].

Our proposal also addresses three issues: (1) the lack of PII control of users; (2) the lack of models to assist users in data dissemination during the interaction; and, (3) the lack of user preference guarantees on the SP side. Respectively, the users data are encrypted according to their needs; standardized models of interaction are available; and, finally, effective control of the operations on user data is also performed [6].

Our initial works combined the concept of dynamic federation with privacy features proposed in [6] and how to agree to these concepts dynamically. With that, our work differs from [11] and [81] by defining and applying theoretical and practical concepts of privacy in dynamic federations [24].

Finally, our initial works proposed an identity management model with privacy for cloud environments and demonstrated that the proposed solutions offer transparency, controllability, and minimization, contributing to our goals to reduce the risks of breaching privacy. Concepts related to cloud computing, identity management, and privacy were presented. We have also described the improvements developed in the framework to validate the IdM privacy approach. We used the framework called OIDC. The improvements that we implemented deal with dynamic environment interactions, using encryption and sticky policies [28].

Acknowledgment

The research is funded by the Brazilian Funding Authority for Studies and Projects (FINEP) under the Brazilian National Research Network in Security and Cryptography project (RENASIC) and conducted at the virtual laboratory of secure implementations (LATIM) at the Federal University of Santa Catarina (UFSC) in the Networks and Management laboratory (LRG).

References

[1] R. Buyya, C.S. Yeo, S. Venugopal, Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities, in: High Performance Computing and Communications, 2008. HPCC '08. 10th IEEE International Conference on, 2008, pp. 5–13, doi:10.1109/HPCC.2008.172.
[2] J. Werner, G.A. Geronimo, C.B. Westphall, F.L. Koch, R. Freitas, C.M. Westphall, Environment, services and network management for green clouds, CLEI Electron. J. 15 (2) (2012). URL http://www.clei.org/cleiej/paper.php?id=238
[3] M. Hansen, A. Schwartz, A. Cooper, Privacy and identity management, IEEE Secur. Privacy 6 (2) (2008) 38–45, doi:10.1109/MSP.2008.41.
[4] O. Foundation, Openid connect, 2016, Retrieved: June, 2016 URL http://openid.net/.
[5] Shibboleth, What's shibboleth?, 2016, Retrieved: July, 2016 URL https://shibboleth.net/about/.
[6] J. Werner, C.M. Westphall, R. Weingärtner, G.A. Geronimo, C.B. Westphall, An approach to idm with privacy in the cloud, in: Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015 IEEE International Conference on, 2015, pp. 168–175, doi:10.1109/CIT/IUCC/DASC/PICOM.2015.26.
[7] T. Orawiwattanakul, K. Yamaji, M. Nakamura, T. Kataoka, N. Sonehara, User-controlled privacy protection with attribute-filter mechanism for a federated sso environment using shibboleth, in: P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on, 2010, pp. 243–249, doi:10.1109/3PGCIC.2010.40.
[8] D.W. Chadwick, K. Fatema, A privacy preserving authorisation system for the cloud, J. Comput. Syst. Sci. 78 (5) (2012) 1359–1373, doi:10.1016/j.jcss.2011.12.019. {JCSS} Special Issue: Cloud Computing 2011.
[9] R. Sanchez, F. Almenares, P. Arias, D. Diaz-Sanchez, A. Marin, Enhancing privacy and dynamic federation in idm for consumer cloud computing, IEEE Trans. Consum. Electron. 58 (1) (2012) 95–103, doi:10.1109/TCE.2012.6170060.
[10] S. Gürses, J.M. del Alamo, Privacy engineering: shaping an emerging field of research and practice, IEEE Secur. Privacy 14 (2) (2016) 40–46, doi:10.1109/MSP.2016.37.
[11] S. Ferdous, R. Poet, Managing dynamic identity federations using security assertion markup language, J.Theor.Appl.Electron.Commerce Res. 10 (2015) 53–76. URL http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-18762015000200005&nrm=iso.
[12] C.E. Landwehr, Computer security, Int. J. Inf. Secur. 1 (1) (2001) 3–13, doi:10.1007/s102070100003.
[13] I. Goldberg, D. Wagner, E. Brewer, Privacy-enhancing technologies for the internet, in: Compcon '97. Proceedings, IEEE, 1997, pp. 103–109, doi:10.1109/CMPCON.1997.584680.
[14] ISO/IEC 24760-1:2011, Information technology – Security techniques – A framework for identity management., Technical Report, 2011a.
[15] ISO/IEC 29100:2011, Information technology – Security techniques – Privacy Framework., Technical Report, 2011b.
[16] A. Josang, S. Pope, User centric identity management, in: AusCERT Asia Pacific Information Technology ..., 2005, pp. 1–13.
[17] H. Lee, I. Jeun, H. Jung, Criteria for evaluating the privacy protection level of identity management services, in: 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 155–160, doi:10.1109/SECURWARE.2009.31.
[18] M. Hansen, P. Berlich, J. Camenisch, S. Clau, A. Pfitzmann, M. Waidner, Privacy-enhancing identity management, Inf. Secur. Tech. Rep. 9 (1) (2004) 35–44, doi:10.1016/S1363-4127(04)00014-7.

[19] E. Bertino, K. Takahashi, Identity Management: Concepts, Technologies, and Systems, Artech House, 2011.

[20] S. Singh, J. Sidhu, A survey of xml-based security standards for handling security requirements of grid and cloud, Int. J.Eng. Technol.(0975–4024) 5 (4) (2013).

[21] R. Baldoni, Federated identity management systems in e-government: the case of Italy, Electron. Government, Int. J. 9 (1) (2012) 64–84, doi:10.1504/EG.2012.044779.

[22] Shibboleth, Project roadmap, 2016, Retrieved: November, 2016 URL https://wiki.shibboleth.net/confluence/display/DEV/Project+Roadmap.

[23] D.R.D. Santos, T.J. Nascimento, C.M. Westphall, M.A.P. Leandro, C.B. Westphall, Privacy-preserving identity federations in the cloud: a proof of concept, Int. J. Secur. Netw. 9 (1) (2014) 1–11, doi:10.1504/IJSN.2014.059328.

[24] L.M. Bodnar, C.M. Westphall, J. Werner, C.B. Westphall, Towards privacy in identity management dynamic federations, in: ICN 2016, The Fifteenth International Conference on Networks, IARIA, Lisbon, Portugal, 2016, pp. 40–45.

[25] R. Hedberg, R. Gullikson, M.B. Jones, J. Bradley, Openid connect federation 1.0 - draft 01, 2016, URL https://openid.net/specs/openid-connect-federation-1_0.html.

[26] S. Kumaraswamy, S. Lakshminarayanan, M. Reiter, J. Stein, Y. Wilson, CSA - Domain 12: Guidance for Identity & Access Management V2.1, Technical Report, 2010. URL https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide-dom12-v2.10.pdf.

[27] A. Celesti, F. Tusa, M. Villari, A. Puliafito, Security and cloud computing: intercloud identity management infrastructure, in: Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on, 2010, pp. 263–265, doi:10.1109/WETICE.2010.49.

[28] J. Werner, C.M. Westphall, A model for identity management with privacy in the cloud, in: 2016 IEEE Symposium on Computers and Communication (ISCC), 2016, pp. 463–468, doi:10.1109/ISCC.2016.7543782.

[29] M. Faraji, J.M. Kang, H. Bannazadeh, A. Leon-Garcia, Identity access management for multi-tier cloud infrastructures, in: 2014 IEEE Network Operations and Management Symposium (NOMS), 2014, pp. 1–9, doi:10.1109/NOMS.2014.6838229.

[30] D.R.D. Santos, R. Marinho, G.R. Schmitt, C.M. Westphall, C.B. Westphall, A framework and risk assessment approaches for risk-based access control in the cloud, J. Netw. Comput. Appl. 74 (2016) 86–97, doi:10.1016/j.jnca.2016.08.013.

[31] C.I.W. Group, Identity and Access Management for the Internet of Things, Technical Report, 2016. URL https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf

[32] K. group, Kantara initiative, 2017, Retrieved: January, 2017 URL https://kantarainitiative.org/.

[33] D.J. Solove, A taxonomy of privacy, University Pennsylvania – Law Rev. 154 (3) (2006) 477–560.

[34] A.F. Westin, How the public views privacy and health research, Results of a National Survey Commissioned by the Institute of Medicine Committee on" Health Research and the Privacy of Health Information: The HIPPA Privacy Rule, 2007. 2011–1107.

[35] C. Diaz, S. Gürses, Understanding the landscape of privacy technologies, in: Extended Abstract of Invited Talk in Proceedings of the Information Security Summit, 2012, pp. 58–63.

[36] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, L.B. Othmane, L. Lilien, An entity-centric approach for privacy and identity management in cloud computing, in: Reliable Distributed Systems, 2010 29th IEEE Symposium on, 2010, pp. 177–183, doi:10.1109/SRDS.2010.28.

[37] U. Nations, The promotion, protection and enjoyment of human rights on the internet (2012). Retrieved: February, 2016 URL https://daccess-ods.un.org/TMP/208261.31105423.html.

[38] M.L. Badger, T. Grance, R. Patt-Corner, J.M. Voas, SP 800-146 – Cloud Computing Synopsis and Recommendations, Technical Report, Gaithersburg, MD, United States, 2012. Retrieved: February, 2016.

[39] D.J. Solove, Privacy self-management and the consent dilemma, Harvard Law Rev. 126 (7) (2013) 1880–1903.

[40] E. McCallister, T. Grance, K. Scarfone, SP 800-122 – Guide to protecting the confidentiality of personally identifiable information, Technical Report, 2010. Retrieved: February, 2016.

[41] J. Jensen, Federated identity management challenges, in: Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, 2012, pp. 230–235, doi:10.1109/ARES.2012.68.

[42] E. Birrell, F.B. Schneider, Federated identity management systems: a privacy-based characterization, IEEE Secur. Privacy 11 (5) (2013) 36–48, doi:10.1109/MSP.2013.114.

[43] A. Pfitzmann, M. Hansen, Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology, Technical Report, 2010. Retrieved: February, 2016 URL https://tools.ietf.org/id/draft-hansen-privacy-terminology-00.html.

[44] S.D.C. di Vimercati, S. Foresti, P. Samarati, Managing and accessing data in the cloud: privacy risks and approaches, in: 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2012, pp. 1–9, doi:10.1109/CRISIS.2012.6378956.

[45] A. Türk, F. PIZZETTI, The Future of Privacy - European Commission Article 29 Working Party WP168, Technical Report, 2009. Retrieved: February, 2016 URL http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009wp168_en.pdf.

[46] C.A. Ardagna, J. Camenisch, M. Kohlweiss, R. Leenes, G. Neven, B. Priem, P. Samarati, D. Sommer, M. Verdicchio, Exploiting cryptography for privacy-enhanced access control: a result of the prime project, J. Comput. Secur. 18 (1) (2010) 123–160. URL http://dl.acm.org/citation.cfm?id=1734234.1734236.

[47] J. Watada, L.C. Jain, R.J. Howlett, N. Mukai, K. Asakura, U. Khalid, A. Ghafoor, M. Irum, M.A. Shibli, 17th international conference in knowledge based and intelligent information and engineering systems - kes2013 cloud based secure and privacy enhanced authentication & authorization protocol, Procedia Comput. Sci. 22 (2013) 680–688, doi:10.1016/j.procs.2013.09.149.

[48] R. de Madrid, Estándares Internacionales sobre Protección de Datos Personales y Privacidad, Technical Report, 2009. Retrieved: February, 2016 URL http://www.privacyconference2009.org/media/Publicaciones/common/estandares_resolucion_madrid_es.pdf

[49] S. Pearson, Taking account of privacy when designing cloud computing services, in: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009, pp. 44–52, doi:10.1109/CLOUD.2009.5071532.

[50] S. Trabelsi, J. Sendor, Sticky policies for data control in the cloud, in: Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on, 2012, pp. 75–80, doi:10.1109/PST.2012.6297922.

[51] B.A. Kitchenham, Procedures for undertaking systematic reviews, Technical Report, Computer Science Department, Keele University, 2004. Retrieved: February, 2016.

[52] D. Sommer, M. Casassa Mont, S. Pearson, PRIME Architecture V3, Tech. Rep. D14.2.d, PRIME, 2008.

[53] Prime, Privacy and identity management for Europe, 2016, Retrieved: June, 2016 URL https://www.prime-project.eu/.

[54] S. Górniak, J. Elliott, M. Ford, D. Birch, Managing multiple electronic identities, Technical Report, ENISA - European Network and Information Security Agency, 2011.

[55] PrimeLife, Privacy and identity management for europe life, 2016, Retrieved: June, 2016 URL http://primelife.ercim.eu/.

[56] ABC4Trust, Abc4trust, 2016, Retrieved: May, 2016 URL https://abc4trust.eu/.

[57] GÉANT, Géant project, 2016, Retrieved: May, 2016 URL http://www.geant.org/.

[58] PRISMACLOUD, Prismacloud project - privacy and security maintaining services in the cloud, 2016, Retrieved: August, 2016 URL http://www.prismacloud.eu/.

[59] ERCIM, Ercim - the european research consortium for informatics and mathematics, 2016, Retrieved: August, 2016 URL http://ercim-news.ercim.eu/.

[60] CREDENTIAL, Credential project - secure cloud identity wallet, 2016, Retrieved: August, 2016 URL http://www.credential.eu/.

[61] J. Wang, Y. Zhao, S. Jiang, J. Le, Providing privacy preserving in cloud computing, in: 2009 International Conference on Test and Measurement, 2, 2009, pp. 213–216, doi:10.1109/ICTM.2009.5413073.

[62] F. Doelitzscher, C. Reich, M. Knahl, N. Clarke, An autonomous agent based incident detection system for cloud environments, in: Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on, 2011, pp. 197–204, doi:10.1109/CloudCom.2011.35.

[63] F. Rocha, S. Abreu, M. Correia, The final frontier: confidentiality and privacy in the cloud, Computer 44 (9) (2011) 44–50, doi:10.1109/MC.2011.223.

[64] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B.S. Lee, Trustcloud: A framework for accountability and trust in cloud computing, in: 2011 IEEE World Congress on Services, 2011, pp. 584–588, doi:10.1109/SERVICES.2011.91.

[65] B. Wang, B. Li, H. Li, Oruta: privacy-preserving public auditing for shared data in the cloud, IEEE Trans. Cloud Comput. 2 (1) (2014) 43–56, doi:10.1109/TCC.2014.2299807.

[66] M. Mowbray, S. Pearson, A client-based privacy manager for cloud computing, in: Proceedings of the Fourth International ICST Conference on COMmunication System softWAre and middlewaRE, in: COMSWARE '09, ACM, New York, NY, USA, 2009, pp. 5:1–5:8, doi:10.1145/1621890.1621897.

[67] S. Suriadi, E. Foo, A. Jøsang, A user-centric federated single sign-on system, J. Netw. Comput. Appl. 32 (2) (2009) 388–401, doi:10.1016/j.jnca.2008.02.016.

[68] S. Pearson, M. Casassa-Mont, Sticky policies: an approach for managing privacy across multiple parties, Computer 44 (9) (2011) 60–68, doi:10.1109/MC.2011.225.

[69] J. Angulo, S.F. Hübner, E. Wästlund, T. Pulls, Towards usable privacy policy display and management, Inf. Manage. Comput. Secur. 20 (1) (2012) 4–17, doi:10.1108/09685221211219155.

[70] S. Betgé-Brezetz, G.B. Kamga, M.P. Dupont, A. Guesmi, End-to-end privacy policy enforcement in cloud infrastructure, in: Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on, 2013, pp. 25–32, doi:10.1109/CloudNet.2013.6710554.

[71] J. Camenisch, M. Dubovitskaya, A. Lehmann, G. Neven, C. Paquin, F.-S. Preiss, Concepts and Languages for Privacy-Preserving Attribute-Based Authentication, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 34–52. 10.1007/978-3-642-37282-7_4.

[72] A. Ahmad, M.M. Hassan, A. Aziz, A multi-token authorization strategy for secure mobile cloud computing, in: Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2014 2nd IEEE International Conference on, 2014, pp. 136–141, doi:10.1109/MobileCloud.2014.21.

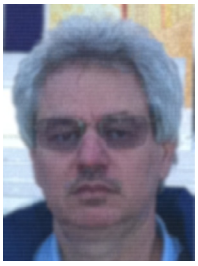
[73] J.B. Bernabe, J.M.M. Perez, J.M.A. Calero, F.J.G. Clemente, G.M. Perez, A.F.G. Skarmeta, Semantic-aware multi-tenancy authorization system for cloud architectures., Future Generation Comput. Syst. 32 (2014) 154–167, doi:10.1016/j.future.2012.05.011. Special Section: The Management of Cloud Systems, Special Section: Cyber-Physical Society and Special Section: Special Issue on Exploiting Semantic Technologies with Particularization on Linked Data over Grid and Cloud Architectures

[74] D. Nuñez, I. Agudo, Blindidm: a privacy-preserving approach for identity management as a service, Int. J. Inf. Secur. 13 (2) (2014) 199–215, doi:10.1007/s10207-014-0230-4.

[75] R. Weingärtner, C.M. Westphall, Enhancing privacy on identity providers, in: SECURWARE 2014, 2014 The Eighth International Conference on Emerging Security Information, Systems and Technologies, IARIA, Lisbon, Portugal, 2014, pp. 82–88.
[76] S. Li, T. Zhang, J. Gao, Y. Park, A sticky policy framework for big data security, in: Big Data Computing Service and Applications (BigDataService), 2015 IEEE First International Conference on, 2015, pp. 130–137, doi:10.1109/BigDataService.2015.71.
[77] J. Brown, D.M. Blough, Distributed enforcement of sticky policies with flexible trust, in: High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), 2015 IEEE 17th International Conference on, 2015, pp. 1202–1209, doi:10.1109/HPCC-CSS-ICESS.2015.235.
[78] G. Spyra, W.J. Buchanan, E. Ekonomou, Sticky policy enabled authenticated ooxml, in: SAI Computing Conference, 2016 IEEE 17th International Conference on, 2016, pp. 1–5. London, UK.
[79] W. Ma, K. Sartipi, H. Sharghigoorabi, D. Koff, P. Bak, Openid connect as a security service in cloud-based medical imaging systems, J. Med. Imaging 3 (2) (2016) 026501, doi:10.1117/1.JMI.3.2.026501.
[80] P.F. Silva, C.B. Westphall, C.M. Westphall, M.M. Mattos, Model for cloud computing risk analysis, in: ICN 2015, The Fourteenth International Conference on Networks, IARIA, Barcelona, Spain, 2015, pp. 140–146.
[81] P.A. Cabarcos, F. Almenárez, F. Gómez Mármol, A. Marín, To federate or not to federate: a reputation-based mechanism to dynamize cooperation in identity management, Wireless Pers. Commun. 75 (3) (2014) 1769–1786, doi:10.1007/s11277-013-1338-y.
[82] S. Sadki, H.E. Bakkali, An approach for privacy policies negotiation in mobile health-cloud environments, in: Cloud Technologies and Applications (CloudTech), 2015 International Conference on, 2015, pp. 1–6, doi:10.1109/CloudTech.2015.7336983.
[83] R. Weingärtner, Dissemination Control of Sensitive Data in Federated Environments, UFSC, Brazil, 2014 Master's thesis.

Jorge Werner is doing his PhD degree in Computer Science at Federal University of Santa Catarina. He has received his Master in Computer Science from Federal University of Santa Catarina (2011) and graduated from the Estacio de Sa University of Santa Catarina (2007) as Computer Network Technology.

Carla M. Westphall is a professor in the Department of Informatics and Statistics at the Federal University of Santa Catarina, Brazil. Her research interests include distributed security, identity management, and grid and cloud security. Westphall received her PhD in electrical engineering from the Federal University of Santa Catarina.



Carlos B. Westphall is a full professor in the Department of Informatics and Statistics at the Federal University of Santa Catarina, where he is the leader of the Networks and Management Laboratory. His research interests include network and service management, security, and cloud computing. He received his D.Sc. in computer science at Paul Sabatier University, France. He was the founder of LANOMS. In 2011 he was named an IARIA Fellow. He has served as Technical Program and/or Organizing Committee member (since 1994) of IFIP/IEEE IM, IEEE/IFIP NOMS, IEEE/IFIP DSOM, IEEE LANOMS, and IEEE APNOMS. He has been on the Board of Editors (since 1995) and Senior Technical Editor (since 2003) of the Journal of Network and Systems Management of Springer and an Editorial Board member (since 2004) of the Computer Networks Journal of Elsevier. He has also been an Associate Editor (since 2006) of the Journal of Communication and Information Systems of IEEE ComSoc/SBrT. Since 1993 he has been a member of IFIP TC6 Working Group 6.6 (Management of Networks and Distributed Systems), and since 2003 a member of the core team of the TeleManagementForum Universities Program (TMF UP). Since 2008 he has been Latin America International Academy, Research, and Industry Association (IARIA) Liaison Board Chair. He was a member (2004–2005 and 2006–2007) of the IEEE ComSoc Membership Programs Development Board. From May 2000 to May 2005 he acted as Secretary of the IEEE Committee on Network Operation and Management (CNOM). From May 2005 to May 2009 he acted as Vice- Chair of IEEE CNOM. He has been a member of IEEE CNOM since 1994.