ACROSS-FI: Attribute-Based Access Control with Distributed Policies for Future Internet Testbeds

Edelberto Franco Silva
Institute of Computing
Fluminense Federal University (UFF)
MídiaCom Laboratory
Niterói, RJ, Brazil
Email: edelberto@midiacom.uff.br

Natalia Fernandes Castro
Dept. of Telecommunications Engineering
Fluminense Federal University (UFF)
MídiaCom Laboratory
Niterói, RJ, Brazil
Email: natalia@midiacom.uff.br

Débora C. Muchaluat Saade
Institute of Computing
Fluminense Federal University (UFF)
MídiaCom Laboratory
Niterói, RJ, Brazil
Email: debora@midiacom.uff.br

***Abstract*—Interests in access control authorization methods for distributed resources have been growing as more shared resources environments and resource federations have been made available, both in academy and in industry. Different proposals aiming at creating a granular and scalable access control in those distributed environments have been presented in the literature. The standardization of access control models based on roles and attributes are examples of that effort. However, none of the existing proposals or standards present a complete authentication and authorization framework that can be adapted for different distributed environments. This work presents an authentication and authorization framework based on policies and attribute aggregation for controlling access into Future Internet (FI) distributed testbeds. A generic solution for attribute-based access control in Future Internet testbeds federation is implemented and evaluated, providing a generic interface to allow communication between the FI resource federation and our access control proposal. Based on user and resource's attributes, policies are dynamically applied to control which resources a user may require. This work has been validated in an experimental identity management laboratory (GIdLab) enabling the use of identity management services offered in an academic identity federation and in an experimental environment for the Future Internet.**

Keywords*—future internet; authorization; authentication; attribute-based access control.

I. INTRODUCTION

Identity Management (IdM) is the set of processes and technologies used for guaranteeing the identity of an entity. IdM ensures the quality of identity information such as identifiers, credentials, and attributes and uses it for authentication, authorization, and accounting processes [1].

Authentication procedures focus on confirming the identity of an entity, that is, checking that an entity is who it claims to be. Authorization mechanisms define the access rights to resources associated to an identity. Authorization procedures describe these access rights to ensure that they are obeyed. Finally, accounting refers to track network resource consumption by users for capacity planning and billing.

In recent years, the use of academic authentication and authorization (A&A) federations to control access to resources became popular [2][3]. In Brazil, for instance, academic researchers access scientific publication repositories using identities of the CAFe academic federation [4]. Hence, there is no need to duplicate user information in local databases.

The Federated Identity Management (FIM) is the basis of this work, when users from many institutions can access services provided by other partner institutions. A federated and distributed identity service depends on the ability of any service provider to trust the credentials provided to them by other entities. In this scenario, IdM appears as a strong requirement for establishing the trust environment among participants, as to share tools or resources among each other.

Important examples of such environments are the initiatives for experimental facilities for the Future Internet (FI) research [5][6]. New network architectural proposals depend on exhaustive tests before they are implemented in the real world. Thus, various experimental facilities, or testbeds, were developed [7][8]. Researchers, however, realized that interconnecting those testbeds is a requirement in order to carry out real experiments in geographically dispersed scenarios. This brings up many management challenges, because communication and access control agreements are necessary. The need to specify an IdM architecture in this context draws attention.

There are some proposals for federating FI testbeds. Among them, we highlight the Slice-Based Federation Architecture (SFA) [9], which is currently in use in testbeds such as OneLab, FIBRE Project (*Future Internet testbeds experimentation between BRazil and Europe*) [10], and PlanetLab. In SFA-based FI testbeds, users supply their credentials to get access authorization to a set of resources located in different institutions, such as a set of computers and a minimal specified bandwidth. Although SFA is the most important initiative to create a federation of FI testbeds, it presents open issues related to A&A. Briefly, this occurs because its proposal is focused on interconnecting resources through a *resource federation*. The A&A ends up in background, composed only of a simple authentication mechanism based on X.509 certificates and static profiles.

To illustrate our proposal a component architecture is shown in Figure 1. On top the identity federation is responsible for authenticating users. In the middle all components of a federated resource environment are depicted, with an attribute provider, an access control component, a credential translation

 ISBN: 978-1-61208-398-8

component (necessary to translate the credential from the identity federation to the testbed federation, which is presented in [11]), a service provider and the resource federation (i.e., FI testbeds or islands).

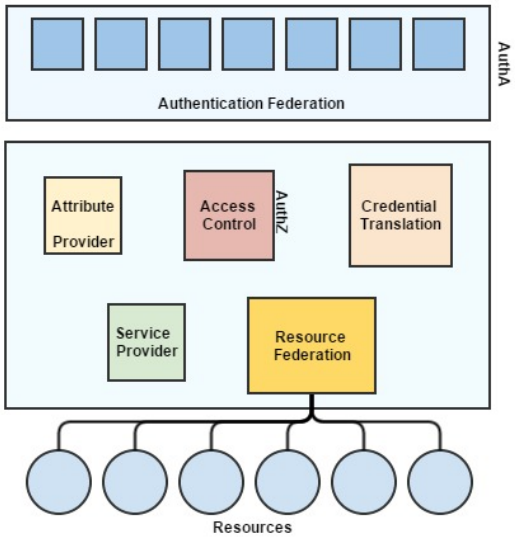

Figure 1. Proposed component architecture for authentication and authorization.

In this work, we propose a new authorization method for SFA-based testbeds. Our proposal integrates A&A federations based on Shibboleth [12] and a authorization framework based on Extensible Access Control Markup Language (XACML) [13]. Shibboleth implements the Security Assertion Markup Language (SAML) standard [14] and also supports Attribute-Based Access Control (ABAC), which has become a standard in 2014 [15]. Using ABAC, it is possible to implement more granular and dynamic access policies. Moreover, Shibboleth is used by the Brazilian academic federation, named CAFe, and also by eduGAIN. Our proposal allows the user to allocate resources in testbed federations based on attributes arising from an identity federation. We propose a generic framework for ABAC using an aggregate attribute mechanism that associates points for user attributes and resource attributes. Our goal is to use the access control proposal in the FIBRE testbed, which is an initiative of federated testbeds between Brazil and Europe, using CAFe and eduGAIN for authentication.

We implemented the proposed A&A architecture using a real experimentation laboratory called GIdLab. GIdLab provides a mirror of the CAFe federation, which serves as an experimental environment for new applications that use the federation. GIdLab also offers virtual machines, in which we configure some virtual testbeds and all ABAC infrastructure. This implementation allowed us to validate the proposal and to evaluate security features, comparing it to other proposals.

The rest of the article is organized as follows. Section II discusses related work. Section III shows an essential background of technologies and concepts necessary to understand the proposal. Section IV details our proposal and Section V presents current results. In Section VI, conclusions and future works are described.

II. Related Work

There are many initiatives to federate testbeds, such as GENI (Global Environment for Network Innovations), OneLab and FED4FIRE [5]–[8][16].

A recent initiative for creation of testbeds in Brazil and Europe is the FIBRE Project [10]. FIBRE proposes the construction of a network for large-scale experimentation, which includes wired and wireless environments, through the interconnection of small testbeds, called islands, in various parts of Brazil and Europe. Thus, FIBRE is strongly grounded in building a federated environment. Although these proposals are strongly based on the resource federation, using tools such as SFA, they present open issues related to identity management. These projects integrate testbeds using different control and management frameworks, each of them using a different user database and different authentication and access control methods. Tools such as SFA do not provide a proper A&A federation architecture to integrate such different environments.

Related work, in general, proposes the introduction of a standardized model (such as RBAC [17], ABAC [15]) for resource distributed environments such as grid computing, and more recently, cloud computing. The area where there is more related work is undoubtedly grid computating. We can cite works as [18][19], on which role-based access control models (RBAC) are applied. More recent works in cloud computing use ABAC for access control, such as [20]. However, we must emphasize the need to know how access control in these environments has been employed, but each distributed resource environment has its particularities.

In this paper, we present the first proposal for policy and Attribute-Based Access Control in FI testbeds, different of GENI ABAC proposal (the other – and only – similar proposal), when attributes are used to restrict and delegate access [21], introducing a new way to represent the resources, attributes and policies in this enviroment.

III. Background

This section presents an introduction of technologies and concepts needed to understand the solution proposed by this work.

A. SAML and Shibboleth

The Security Assertion Markup Language (SAML) standard [14] presents a set of specifications to define an infrastructure for dynamic exchange of security information between partners (e.g., institutions). SAML defines the roles of entities, “assertions” and transport protocols supported. Assertions use an XML format [22] for describing data, which represents the authorization of a user at a given time for instance. There are two main types of entities that compose an Authentication and Authorization (A&A) federation environment: Identity Provider (IdP is responsible for storing and providing information about users and their authentication and the Service Provider (SP) is responsible for offering one or more services (or resources). Shibboleth [12] implements SAML and allows

 ISBN: 978-1-61208-398-8

web applications to enjoy the facilities provided by the model of federated identity, such as the concept of Single Sign-On (SSO).

B. CAFe

Federated Academic Community (CAFe) is the Brazilian academic federation, encompassing education and research organizations. Through CAFe, a user keeps all his information at his home organization and can access services offered by institutions participating in the federation through SSO. CAFe uses standards and software solutions already available and adopted by other federations, such as Shibboleth. Besides maintaining the usual set of privacy policies, CAFe also comprises a set of tools for populating an Lightweight Directory Access Protocol (LDAP) repository with data from different corporate databases. Integrated to eduGAIN, the CAFe federation participates in the network of trust of GÉANT academic federation. In the FIBRE project context, CAFe is being proposed as the main means of authentication [11] for Brazilian users.

C. FIBRE project

The FIBRE project [10] is a partnership between Brazilian and European institutions in order to create a large-scale network virtualization testbed. Topologically, FIBRE can be seen as the union of a large European island and a large Brazilian island, which consists of several small islands, located in different universities and research centers.

In FIBRE, there are several control frameworks. To control OpenFlow equipment [23][6], the experimenter uses the OFELIA Control Framework (OCF) [24]. To control wireless equipment, FIBRE provides the Control and Management Framework (OMF) [25]. Moreover, FIBRE also has islands based on ProtoGENI, which is a control framework developed for the GENI project [26]. The idea is that FIBRE can provide different control interfaces and can aggregate an increasing number of islands.

D. XACML

XACML (eXtensible Access Control Markup Language) [13] is an XML-based standard language for declaring security policies by OASIS (*Organization for the Advancement of Structured Information Standards*), aiming at ensuring interoperability between authorization systems. Moreover, it is a language to declare access control policies, defining a format for request and response messages [13].

ABAC uses the XACML architecture, working with the same entities. For example, PEP (Policy Enforcement Point), PDP (Policy Decision Point) and PAP (Policy Administration Point), where PEP is responsible for translating requests and responses and PDP for deciding if any policy (defined in PAP) is applied.

E. Access Control Mechanisms

Access control (in this work, access control and authorization have the same meaning) is a fundamental mechanism for protecting a resource from unauthorized access or respecting security requirements. Specifically, an access control policy defines the conditions to which access to resources can be granted and to whom. With the increasing complexity of computing systems, access control methods have evolved from Mandatory Access Control (MAC) [27], Discretionary Access Control MAC (DAC) [28], Role-Based Access Control (RBAC) [17], to Attribute-Based Access Control (ABAC) [15]. In this work, ABAC is the focus of access control applied to resource federation for FI testbeds.

In [15], ABAC is an access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions.

IV. ACROSS-FI Proposal

This section presents the ACROSS-FI proposal. At first, an attribute aggregator is proposed and validated, using an attribute provider to store application-specific user attributes. Then, a mechanism to generalize attribute values of both users and resources is introduced. Finally, the proposal of access control in the FI testbed environment is presented.

A. Attribute Aggregation

An attribute provider is necessary to store application-specific complementary attributes for a given user. Additional attributes are those employed only in a specific context, such as a trial project in networks. In the FI testbed scenario, many additional attributes can be necessary to access network resources, on the other hand, they are not necessary in other federation services. So, storing those additional attributes is a responsibility of the service provider (i.e., FI's testbeds), not the Identity Federation (e.g., CAFe).

Attribute aggregation models were studied [29][30], and in a nutshell, these papers introduce two models, when the user is responsible (behalf) to aggregate all distributed attributes (at different IdPs) or, alternatively, the SP is responsible to proceed with this aggregation. In this work we decided to develop a particular solution where the aggregation of attributes is implemented with the help of an attribute aggregator and one extra attribute provider, once our enviroment has particular characteristics as specifics attributes for specifics testbeds. We will see a similar approach on *attribute aggregation performed by linking service* presented by [29], when the SP is responsible to link all attribute's source. However, additional attributes stored in the attribute provider should not identify the user to which they are associated. Thus, a single and opaque ID was created in order to link the academic federation user with his extra attributes without identifying him, protecting him from malicious attacks. In this case, malicious attack can be a user modifying its attributes (or of other user) to obtain more privileges than he really should. With an opaque ID, this weakness is solved.

The attribute aggregation proposal is shown in Figure 2, where steps 1 and 2 are the process of user authentication at his home identity provider (IdP) in CAFe federation. Then, CAFe returns the user attributes in step 3 to the service provider (SP), which in turn forwards them to the attribute aggregator. An opaque attribute is sent to the attribute provider that returns only the user additional attributes without the knowledge of

 ISBN: 978-1-61208-398-8

which user that opaque attribute refers to, as shown in step 5. Additional attributes are kept in a local LDAP (IdP of Attribute Provider). In the end, the Attribute Aggregator gathers all attributes.

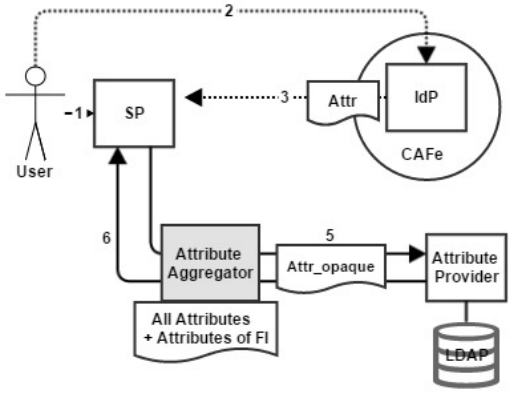

Figure 2. Attribute Aggregation Proposal.

The following equations show how the unique and opaque attribute to identify each user is generated:

$$\delta \leftarrow Attr_u(uid) \cup Attr_u(uidNumber) \quad (1)$$

$$Attr_U(opaque) \leftarrow hash(\delta) \quad (2)$$

Figure 3. Results of attribute aggregation process.

As an example for $uid \rightarrow esilva@uff$ with $uidNumber \rightarrow 1223$, concatenating these two attributes in an MD5 hash, we have the result $af2ec12ce73cc910358ddb400f4abb74$, which corresponds to the user ID at the Atribute Provider. It is noteworthy that only to validate the model a simple MD5 hash was used. Other modern cryptographic hashes, such as SHA-2, SHA-3, etc., should be used in a real environment.

Results of Attribute Aggregation. Briefly, the user proceeds with all steps involved in Shibboleth authentication. After this, Figure 3 shows all user attributes, the ones that came from his home IdP and additional attributes that came from the Attribute Provider (highlighted in red). They refer to specific attributes of the FI environment, i.e., *Shib-fibre-userEnable* (if user is active in FI testbeds), *Shib-fibre-omfAdmin* (if user is an administrator of OMF testbeds) and the opaque attribute, *Attr_opaque* (the user ID at the Attribute Provider).

B. A Generic Access Control Based on Attribute Scores

This work proposes a new method to generalize attribute values of both users and resources. This generic approach is applied on ABAC scenarios. At first, attributes are associated to points and those points are summed to determine a user level. Attribute points are predetermined by a global administrator (the global administrator of the FI environment). Algorithm 4 explains the procedure of computing a user attribute score. All possible attributes are contained in a list called $All\_Attributes$, where each attribute has a weight $Weight(Atribute)$. A simple normalization of attribute scores is applied (forcing the score to range from 0 to 1).

Data: User attributes.
Result: Score (Total of points).
1 **for** *Attribute in All_Attributes* **do**
2 **if** *Attribute.content* $\subset$ *User_List[Attribute]* **then**
3 $Total \leftarrow Total + Attribute.Point * Weight(Atribute)$;
4 **end**
5 **end**

Figure 4. Attribute Score.

When a user is associated to a level, a generalization can be used, because the policy access control does not need to know exactly which attributes a user has. User levels are used to define global and local access control policies. Global access control policies are defined by a FI testbed federation administrator. Local policies are defined by a FI testbed island administrator.

To illustrate the proposal of generalization based on attribute scores, one example is given in Table I. In this example, the maximum value is equal to 80 and the minimum is 0, when normalized ranges between [0-1], as follows:

$$\left(z_i^k\right)_N = \frac{z_i^k - z_{min}^k}{z_{max}^k - z_{min}^k}$$

where the result is a normalized number assuming the max and min attribute scores and the computed user score z_i^k.

TABLE I. AN EXAMPLE OF ATTRIBUTE SCORE.

An example of attribute score.					
Attribute	**value**	**points**	**weight**	**score**	**normalized**
brEduAffiliationType	student	10	3	30	
omfAdmin	TRUE	10	2	20	
institution	uff	8	1	8	
			Total	**58**	**0.725**

As shown in Table I, that user has score of 0.725 points. In the proposed model, it is assumed that the global administrator

 ISBN: 978-1-61208-398-8

will determine a number of levels L and score thresholds for each level. Thus, for a score $l_i < X \leq l_{i+1}$, the user will be on N_i level, where $1 \leq i \leq L$. So, in Table II the global administrator sets 3 levels, where the example user is associated to level 2.

TABLE II. AN EXAMPLE OF LEVEL DEFINITION BASED ON SCORES.

Level Definition	
Score	**Level**
$0 \leq X \leq 0.5$	01
$0.5 < X \leq 0.75$	02
$0.75 < X \leq 1$	03

TABLE III. ACCESS CONTROL POLICIES BASED ON SCORES FOR VIRTUAL MACHINES.

Access Control policies based on scores for virtual machines	
VMs	**Level**
$0 \leq X \leq 5$	1
$0 \leq X \leq 15$	2
$0 \leq X \leq 20$	3

The island (local testbed resources in one institution) administrator sets how many resources a user under a certain level can request. For example, Table III shows that the example user can request up to 15 virtual machines.

V. ACROSS-FI VALIDATION

A. Scenario

In this section, we explain how ACROSS-FI modules are interconnected. Figure 5 shows all components involved, from the authentication to authorization. It is possible to see a blue box on the top, where the authentication process occurs. Red boxes represent the authorization, with attribute aggregation and ABAC solution. It is also possible to see an XML document configured by a global administrator, concerning the creation of user levels used in authorization (Tables I and II).

Our case study is the FIBRE project. Based on Figure 5, the main steps, taken beginning from the federated authentication up to authorization to use resources protected by distributed access policies, can be seen, considering both local and global policies.

Thus, in **step 1**, the user accesses the service provider (SP) that will forward (**step 2**) to authentication, either through CAFe or FIBRE federated LDAP. The FIBRE federated LDAP is a tree that interconnects both Brazilian and European institutions that do not integrate CAFe, enabling a federated access to other users participating in the project. Such steps are traditionally used to create an SAML session [14] from the user to the SP access, redirecting through WAYF (Where Are You From) to its home IdP to proceed the authentication and exchange the user attributes.

In **step 3**, the authenticated user requests the list of resources available to the SFA federation. In this step, SFA is responsible to communicate with the SM (Slice Manager) having a global view of all AMs (Aggregate Managers) (**step 4**), which have direct contact with the island testbed resources. Thus, available resources are listed by a type of XML files, called RSpecs (Resource Specification) and returned to the user in **step 5**. Thereafter, the user may request the resources.

Step 6 is responsible to send through the SP the attributes to attribute aggregator, and the attribute aggregator is responsible to generate an opaque attribute, which identifies the user in the attribute provider, so that additional attributes of IF can be recovered without identifying the user directly to the IdP CAFe federation (**steps 7 and 8**).

Then, the SP receives all attributes from the attribute aggregator, in **step 9**, and forwards these attributes and the RSpec (identifying the requested testbed resources) in **step 10** to the PEP. The PEP then computes the user attribute score indicating a user level (see Section IV-B). In **step 11**, the PEP performs the conversion of RSpec files and score generated to an XACML request.

In **step 12**, the XACML request generated is sent to each FIBRE island, (the island's PIP, **step 13**, will check for additional attributes – optional). Then, in **step 14**, XACML policies that the island administrator previously registered through the PAP are returned to the PDP (**step 15**). At that time, a global policy is also checked through **step 16** and policy-combining algorithms presented by XACML are used, returning to the PDP (**step 17**) the decision. In **step 18**, the response is returned to the PEP that converts to RSpec and forwards it to the SP (**step 19**), stating if the user can or cannot allocate the requested resources.

B. Results

To validate the proposal, the GIdLab experimental laboratory was used, where a mirror of CAFe is available and all other proposed components. All modules, including the attribute aggregator and credential translation were developed. Other necessary features, such as how the SP communicates with SFA federation and the ABAC control access were also implemented.

As we saw in Section IV-A, the attribute aggregator was proposed and validated. Similarly, credential translation was also discussed and implemented in [11]. The proposal of attribute scores presented in Section IV-B was validated at GIdLab using the Sun's XACML implementation and three different virtual machines, one for PEP and PDP and two others to simulate the testbeds. Thus, after checking the user level and the RSpec, a number of resources (e.g., VMs) were requested, and the island's PAP checks if the user is allowed to allocate that number of requested resources. When the XACML response was received by the PDP, a global policy was verified too, and only after these steps the user received an RSpec with available resources.

VI. CONCLUSION AND FUTURE WORK

This work is motivated by the need of access control mechanisms in environments for evaluation of Future Internet proposals. In this context, federations for authentication and authorization can be used to facilitate the shared use of testbed resources for researchers belonging from different institutions.

Our main contributions are: 1) attribute aggregation model proposed and validated; 2) an ABAC model based on user scores and levels to associate dynamically users and resources

 ISBN: 978-1-61208-398-8

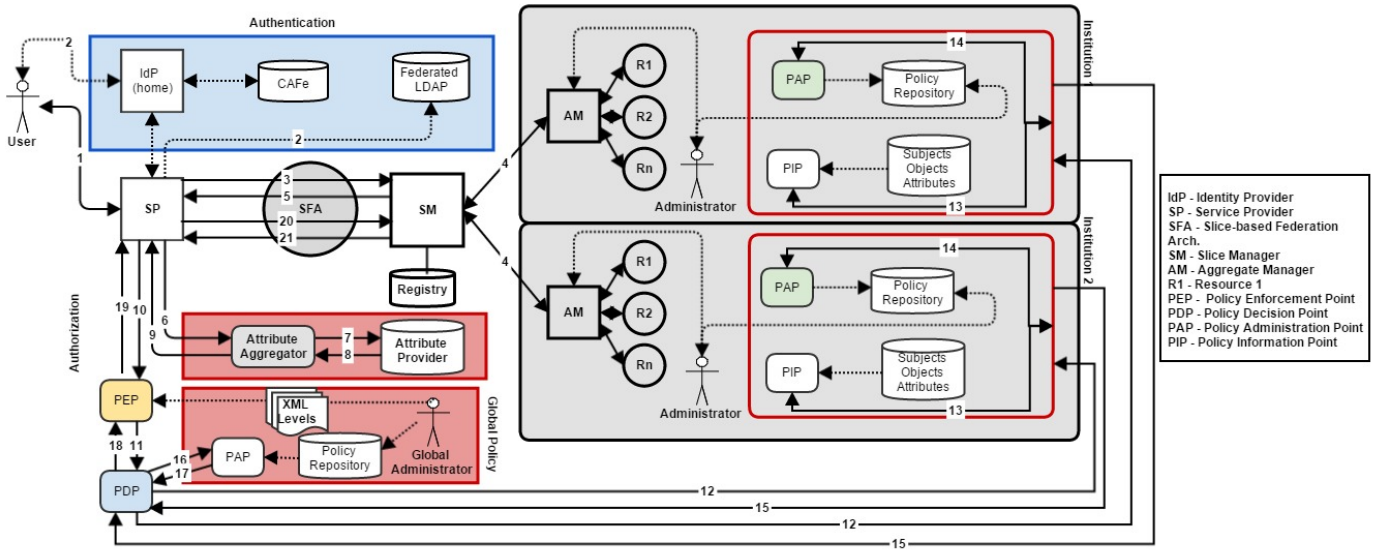

Figure 5. ACROSS-FI Scenario.

proposed and validated; 3) implementation of an integrated authentication and authorization solution for FI testbed environments validated in GIdLab.

As future work, we intend to generalize the proposed A&A solution to the concept of virtual organizations, where a subset of users from different home institutions may use services and share resources from other institutions. We also intend to develop configuration tools to facilitate the definition of attribute points and user levels and policies.

ACKNOWLEDGMENT

We thank RNP (GIdLab), CAPES, CNPq and FIBRE project for supporting this research.

REFERENCES

[1] J. Jensen, "Federated identity management challenges," in Availability, Reliability and Security (ARES), 2012 Seventh International Conference on, 2012, pp. 230–235.

[2] R. Dhungana, A. Mohammad, A. Sharma, and I. Schoen, "Identity management framework for cloud networking infrastructure," in Innovations in Information Technology (IIT), 2013 9th International Conference on, 2013, pp. 13–17.

[3] J. Leskinen, "Evaluation criteria for future identity management," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, pp. 801–806.

[4] RNP, "CAFe - Federated Academic Community," http://portal.rnp.br/web/servicos/cafe-en, Feb. 2015.

[5] P. Stuckmann and R. Zimmermann, "European research on future internet design," Wireless Communications, IEEE, vol. 16, no. 5, 2009, pp. 14–22.

[6] R. Riggio, F. De Pellegrini, E. Salvadori, M. Gerola, and R. Corin, "Progressive virtual topology embedding in openflow networks," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on, 2013, pp. 1122–1128.

[7] S. Jeong and A. Bavier, "Geni federation scenarios and requirements," Tech. Rep., Jul. 2010.

[8] A. Falk, "Federation in geni - draft proposal - comments invited," in GENI Engineering Conferences - GEC11, Jul. 2011.

[9] L. Peterson, R. Ricci, A. Falk, and J. Chase, "Slice-based facility architecture," Tech. Rep., Jul. 2010.

[10] S. S. et. al, "FIBRE project: Brazil and Europe unite forces and testbeds for the Internet of the future," in Proceedings of TridentCom 2012, Jun. 2012.

[11] E. Silva, N. Fernandes, N. Rodriguez, and D. Muchaluat-Saade, "Credential translations in future internet testbeds federation," in 6th IEEE/IFIP Workshop on Management of the Future Internet (ManFI 2014)/NOMS, May 2014, pp. 1–6.

[12] T. Scavo and S. Cantor, "Shibboleth architecture," Tech. Rep., Jan. 2005. [Online]. Available: http://shibboleth.internet2.edu/docs/draft-mace-shibboleth-tech-overview-latest.pdf

[13] T. Moses. eXtensible Access Control Markup Language TC v2.0 (XACML). OASIS. [Online]. Available: http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf [retrieved: Feb., 2005]

[14] OASIS, Security Assertion Markup Language (SAML) v2.0, Std., 2005.

[15] V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to attribute based access control (abac) definition and considerations," NIST Special Publication, vol. 800, 2014, p. 162.

[16] Future Internet Research & Experimentation, http://cordis.europa.eu/fp7/ict/fire/, March, 2015.

[17] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, Aug. 2001, pp. 224–274. [Online]. Available: http://doi.acm.org.ez24.periodicos.capes.gov.br/10.1145/501978.501980

[18] B. et. al, "Identity Federation and Attribute-based Authorization through the Globus Toolkit, Shibboleth, Gridshib, and MyProxy," in 5th Annual PKI R&D Workshop, Apr. 2006.

[19] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," Int. J. High Perform. Comput. Appl., vol. 15, no. 3, Aug. 2001, pp. 200–222.

[20] Y. Zhu, D. Huang, C. Hu, and X. Wang, "From rbac to abac: Constructing flexible data access control for cloud storage services," Services Computing, IEEE Transactions on, vol. PP, no. 99, 2014, pp. 1–1.

[21] M. Berman and M. Brinn, "Progress and challenges in worldwide federation of future internet and distributed cloud testbeds," in Science and Technology Conference (Modern Networking Technologies) (MoNeTeC), 2014 First International, Oct 2014, pp. 1–6.

[22] W3C, "Extensible Markup Language (XML) 1.0 (Fifth Edition)," Feb. 2015. [Online]. Available: http://www.w3.org/TR/REC-xml/

 ISBN: 978-1-61208-398-8

[23] M. et. al, “Openflow: enabling innovation in campus networks,” SIGCOMM Computer Communication Review, vol. 38, no. 2, Mar. 2008, pp. 69–74.

[24] A. Köpsel and H. Woesner, “Ofelia: pan-european test facility for openflow experimentation,” in Proceedings of the 4th European conference on Towards a service-based internet, ser. ServiceWave’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 311–312.

[25] T. Rakotoarivelo, M. Ott, G. Jourjon, and I. Seskar, “OMF: a control and management framework for networking testbeds,” SIGOPS Oper. Syst. Rev., vol. 43, no. 4, Jan. 2010, pp. 54–59.

[26] ProtoGeni ClearingHouse, http://www.protogeni.net/wiki/ClearingHouse Desc, March, 2015.

[27] R. S. Sandhu, “Lattice-based access control models,” Computer, vol. 26, no. 11, Nov. 1993, pp. 9–19.

[28] R. Sandhu and P. Samarati, “Access control: principle and practice,” Communications Magazine, IEEE, vol. 32, no. 9, Sept 1994, pp. 40–48.

[29] D. Chadwick and G. Inman, “Attribute aggregation in federated identity management,” Computer, vol. 42, no. 5, May 2009, pp. 33–40.

[30] ——, “The trusted attribute aggregation service (TAAS) - providing an attribute aggregation layer for federated identity management,” in Availability, Reliability and Security (ARES), 2013 Eighth International Conference on, Sept 2013, pp. 285–290.

 ISBN: 978-1-61208-398-8