Evaluating a Distributed Identity Provider Trusted Network with Delegated Authentications for Cloud Federation

Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito
Dept. of Mathematics, Faculty of Engineering, University of Messina
Contrada di Dio, S. Agata, 98166 Messina, Italy.
e-mail: {acelesti, ftusa, mvillari, apuliafito}@unime.it

***Abstract*—Federation offers an affordable opportunity for small and medium cloud providers to become as competitive as the biggest counterparts. However, in order to establish a federated cloud ecosystem, it is needed to rely on an efficient security infrastructure enabling authentication among clouds. Assuming a scalable federated cloud environment, the management of security can become very hard due to the number of authentications and trusted relationships that have to be established. Nowadays, the latest trend in authentication is the Identity Provider/Service Provider model. This paper aims to investigate a distributed IdP/SP infrastructure based on the concept of delegated authentications, evaluating its possible utilization in a federated cloud scenario.**

***Keywords*-Cloud Computing, Federation, Distributed IdPs, Trusted Network.**

I. INTRODUCTION

By now, the cloud ecosystem has been characterized by the steady rising of hundreds of independent and heterogeneous cloud providers, managed by private subjects which yield various services to their clients. Using this computing infrastructure it is possible to pursue new levels of efficiency in delivering Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) to clients (e.g., companies, organizations, end-users, and so on).

Despite such an ecosystem includes hundreds of independent, heterogeneous clouds, many business operators have predicted that the process toward interoperable federated Intracloud/Intercloud environments will begin in the near future [1], even involving standardization boards (i.e., IEEE [2]). Nowadays, small/medium cloud providers are becoming popular even though their virtualization infrastructures (i.e., deployed in their datacenters) cannot directly compete with the bigger counterparts, including mega-providers such as Amazon, Google, and Saleforce. The result is that frequently small/medium cloud providers have to exploit services of mega-providers in order to develop their business logic and their cloud-based services. This means that the role of market leader is intended to remain in the hands of bigger players in the near future. To this regard, a possible future alternative scenario is based on the concept of cooperating clouds constituting the federation. Federation has always had both political and historical implications: the term refers, in fact, to a type of system characterized by an aggregation of partially "self-governing" entities with a "central government". In a federation, each self-governing status of the component entities is typically independent and may not be altered by a unilateral decision of the "central government" [3]. Federation is also a concept which is adopted in many information systems. Considering small/medium independent self-governing cloud providers, federation means a cooperation enabling the sharing of part of their computational and storage resources with the purpose to provide new business opportunity. The advantage of a federated cloud scenario is twofold. On one hand, small/medium cloud providers, which rent resources to other providers, can optimize the use of their infrastructure, which often is under utilized, at the same time earning money for the use of their resources. On the other hand, external small/medium cloud providers can elastically scale their logical virtualization infrastructure, borrowing resources and paying other providers for their use. Therefore, cloud federation allows another form of pay-per-use economic model for ICT companies, universities, research centers and organizations that usually do not fully exploit the resources of their physical infrastructure. The benefits of cloud federation include provisioning of distributed cloud-based services, resource sharing, resource optimization and power saving [4].

However, several issues have to be faced from the point of view of security. Security is a wide topic in cloud computing and in this work we specifically focus on the establishment of trusted relationships between clouds, that can become very hard to be managed in scalable scenarios. Usually a trusted relationship among two or more systems is performed by means of authentication mechanisms.

In this paper, we discuss two possible authentication scenarios for the establishment of trust contexts between federated clouds: 1) Single Sign-On (SSO) Authentication using the traditional Identity Provider/Service Provider (IdP/SP) model; 2) Single Sign-On (SSO) authentication using a system of distributed Identity Providers (IdPs) with delegated authentications.

The paper is organized as follows: Section II describes the state of the art in authentication for distributed system, focusing on the IdP/SP model. In Section III, we analyze in detail the two authentication scenarios. A comparison between them is discussed in Section IV. Conclusions are summarized in Section V.

 ISBN: 978-1-61208-153-3

II. Related Works

A. Authentication Systems

With the term "authentication" we refer to any process by which it is possible to verify that someone is who claims to be. Username/password is the most widely used form of authentication. Another method is based on the private/public key cryptography. A stronger form of authentication is based on digital certificate [5], an electronic document which uses a digital signature to bind a public key with an identity described by information such as the name of a person or an organization.

Considering the evolving Internet scenarios, where entities need to access different services in a dynamic fashion, the requirement of interoperability among authentication technologies, also reducing the number of needed credentials and authentications is more and more compelling. To this regard, the latest trend in term authentication is represented by the Identity Provider/Service Provider (IdP/SP) model along with the Security Assertion Markup Language (SAML) [6], an XML-based standard that allows to exchange authentication and authorization data. The IdP/SP model allows to plan Single Sign-On (SSO) authentication scenarios when software/human entities can login once an IdP gaining the access to all SPs which rely on that target Idp.

Although SSO and SAML technologies are strictly related to the web context, some recent works are trying to employ the same approach on new scenarios where many entities that belong to different domains need to perform authentication [7], [8]. This is also the case of cloud federation [1], [9], where clouds cooperate together establishing trust contexts in order to provide new business opportunities. Recently, trust has been identified as a beneficial concept in large scale networks [10]. Considering trust relations when selecting service providers as partners leads to more efficient cooperation and composition of services [11].

SAML, offers the possibility of adding extensions in order to achieve dynamic federation in a generic way, regardless the specific scenario where it is applied. Considering federated cloud environments, in [12] it is discussed a new SAML profile named Cross-Cloud Authentication Agent SSO (CCAA-SSO) defining the steps needed for a secure cloud SSO authentication. However, the bottleneck of the IdP/SP model is represented by the presence of a central IdP per trust context. In order to overcome such a limitation, an approach [13] is proposed to minimize the dependence on central IdPs with a priori configuration, making entities more autonomous and capable of taking trust decisions. Another solution is exploiting the concept of delegation. Unfortunately, SAML natively lacks of delegation capabilities. Nevertheless, there are several works in Grid, Web Service, and Ubiquitous Computing environments where SAML is extended with the purpose to benefit of delegation capabilities [14], [15], [16].

B. Propagation of Trustiness

Scenario we are addressing can be defined as simplified context for trustiness in Cooperating Clouds, thus because Clouds may strongly leverage IdPs entities. Many works have been done in area of trustiness even in the propagation of trustiness. Of course our concept of delegation relies on some pre assumptions, those are: a) Each Cloud Provider uses well-know IdP (either its own or in the shared configuration). b) Each Cloud is able to decide if use/not-use the delegation against some specific IdPs (it may perform its filtering of IdPs existing in trustiness chains).

The complexity of evaluating the level of trust of a Subject insisting in the Internet determines to carefully face the topic, especially for large networks (i.e., Social Networks). Huang [17] developed a framework of trust propagation schemes evaluating them on a large trust network consisting of 800K trust scores expressed among 130K people. An interesting work has been conducted in [18] about the *Ontology of Trust* reporting a formal semantics and defining the concept of *Transitivity*. The authors highlighted that Trust Transitivity is not always an applicable concept at all. Chen et al [19] tried to determine a formula for expressing the trustiness. In particular they introduced the Mean operator (*Transitive mean degree*), that is the trust degree of a path (from source to destination considering the weights of edges existing in the between). It is calculated with the geometric or arithmetic mean of those weights of all edges along that path.

The security and trustiness in distributed environments are topics widely assessed. Our main aim is to investigate Clouds and adopt existing security solutions for overcoming issues related to the federation.

III. Authentication Between Clouds

Due to the high dynamism of federated cloud environments, a flexible method for building dynamic trust contexts should be provided.

According to [1], in this work, we assume that, regardless the adopted cloud middleware, the federation process is accomplished according to three different phases that is: Discovery, Match-Making and Authentication. In our solution a specific module named Cross-Cloud Federation Manager (CCFM) including three agents is able to perform such activities.

The *Discovery Agent (DA)* manages the discovery process of the resources and services made available by all the clouds belonging to the dynamic distributed environment. Once the clouds' service discovery has been performed, the *Match-Making Agent (MA)* will accomplish the task of choosing the more convenient cloud(s) wherewith to establish the federation according to requirements and policies. Finally, the *Authentication Agent (AA)* will perform the authentication with the selected clouds, creating a trust context, hence a federation. Once the security context has been created, a

 ISBN: 978-1-61208-153-3

cloud will be able to exploit resources and services offered by other federated cloud. In this Section, we focus on the authentication phase debating two different scenarios involving IdPs. In order to clarify the idea on using the IdP/SP model, we consider the following as a basic example: according to the IdP/SP terminology the AA of cloud A borrowing resources plays the role of "client", the AA of cloud B lending resources plays the role of "SP" (Relying Party), and IdP X plays the role of trust third party (Asserting Party) assuring to cloud B that cloud A is which claims to be. In order to allow cloud A to be authenticated by cloud B, it is needed that cloud A is enrolled in IdP X and that cloud B relies on IdP X. Once the authentication has been accomplished, cloud A will be able to log-in all clouds relying on IdP X without further authentications.

A. Traditional IdP/SP Scenario for Cloud Federation

Assuming an ecosystem with N clouds, the most obvious approach consists of using $M, M < N$ different IdPs. Basically, we can distinguish three main cases:

1) *Case 1.* $M = 1$. It is the simplest case. It consists of using a unique IdP for all federated clouds, thus enabling SSO authentications. In this way each cloud has to manage only one credential. However, this solution is out of place, because a unique central IdP would be a bottleneck for the whole authentication system.
2) *Case 2.* $M < N, M \neq 1$. It is the case in which a cloud, in order to perform authentications with the other $N-1$ clouds, has to perform an enrollment on M IdPs, thus managing M different credentials. For example, let us consider three different *IdPs X, Y, Z*, and clouds $1, 2, 3, 4, 5, 6, 7, 8, 9$. Clouds $1, 2, 3, 4$ rely on *IdP X*, clouds $5, 6, 7$ rely on *IdP Y*, and clouds $8, 9$ rely on *IdP Z*. In order to allow cloud 10 to be authenticated on all the other clouds, it has to perform enrollments on *IdP X, Y, and Z*, thus managing three credentials.
3) *Case 3.* $M = N - 1$. In this case each of the $N-1$ clouds rely on a different IdP. A cloud, in order to perform authentications with the other $N-1$ clouds, needs to perform enrollments on $N-1$ IdPs, thus managing $N-1$ different credentials.

In cases 2 and 3, if an IdP is corrupted, it will not affect the whole authentication system, however case 3 represents the worst case from the point of view of needed trust relationships, i.e, enrollments of clouds in IdPs. In this paper, we analyze this latter case. Considering a federation including N clouds, the number of trust relationships t_r needed to obtain the total overlay (i.e., each cloud is authenticated with each other) can be computed as:

$$t_r = N(N-1) \quad (1)$$

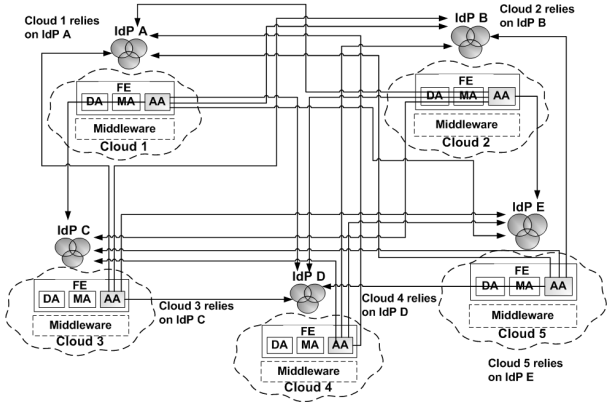

Figure 1. Authentication between clouds using the traditional IDP system where each cloud relies on a different IdP (worst case from the point of view of needed trust relationships).

In Figure 1, 5 clouds are depicted with their associated IdPs. Using eq. (1), $t_r = 5 * 4 = 20$. This means that the full overlay of the network can be reached after the establishment of 20 trust relationships (i.e., performed enrollments of clouds in IdPs). In Figure 1, the existence of a trust relationship is indicated by an arrow connecting the AA of the CCFM of each cloud with the corresponding IdP(s), where the cloud has an enrollment. For example, in order to allow cloud 1 to be authenticated in clouds 2, 3, 4, and 5, it as to perform enrollments in IdPs B, C, D, E. All the consideration we will assume in the following are based on the possibility of extending the SAML protocol as described in some recent works we have cited [13], [14], [15] and [16].

B. Distributed IdP Trusted Network (DIdP-TN) Scenario for Cloud Federation

As the authentication based on the traditional IdP system can imply high management costs especially in case 3, starting from the idea of delegation, we investigated an alternative authentication scenario able to reduce the number of required authentications in a federated cloud environment. We named such a system Distributed IdP Trusted Network (DIdP-TN). As depicted in Figure 2, the authentication system is based on the concept of delegation between IdPs. Cloud 1 has an enrollment on IdP A and therefore is able to perform a SSO authentication on cloud 2 and 3. As trusted relationships exist between IdP A, B, C, D, E, cloud 1 is also able to perform a SSO authentication on all the clouds of the federation. For example, as clouds 6, 7 rely on IdP E, cloud 1 is able to perform an authentication on cloud 7, because IdP E trusts IdP B and IdP B trusts IdP A. In this scenario, trust relationships have to be managed by the DIdP-TN and not by clouds themselves as in the traditional scenario. In this case the number of trust relationships t_r needed to obtain the full coverage of the network of clouds

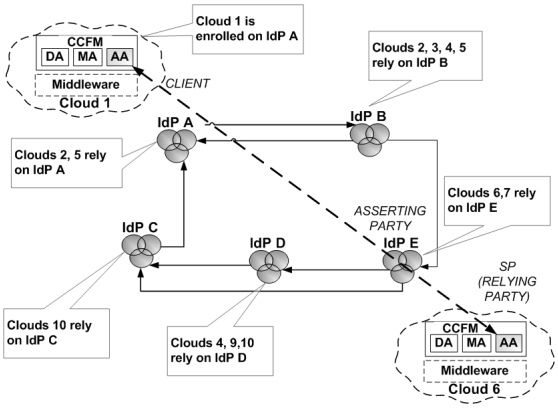

Figure 2. Authentication between clouds using the DIDP-TN system.

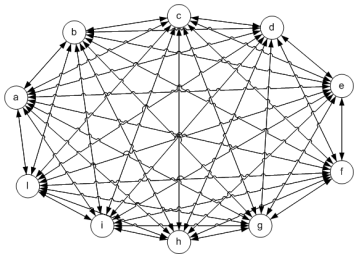

Figure 3. Example of digraph representing the traditional IDP-based authentication system for a federated cloud environment, where each cloud relies on a different IdP (worst case from the point of view of authentication management).

will be:

$$t_r \leq N(N-1) \quad (2)$$

IV. Evaluation of the DIdP-TN

In order to compare the DIDP-TN with a traditional IDP/SP authentication system for cloud federation, we modeled them using the graph theory and performed several experiments.

A. Modeling the two Authentication Systems

Let V and $E(V) = \{\{a,b\}$ *(for simplicity ab)* $|a,b \in V, a \neq b\}$ two finite sets. We define a pair $G = (V,E)$ with $E \subseteq E(V)$ the cyclic digraph (or directed graph) representing a cloud federation. The elements of V are vertices of G, and those of E the edges of G. Vertices a and b are adjacent if the edge $ab \in G$. The vertices set of the digraph G is denoted by V_G and its edge set by E_G. The number $\upsilon_G = |V_G|$ of vertices is called the *order* of G, and $\epsilon_G = |E_G|$ is the *size*. The E are oriented, that is, the edges are oriented: $E \subseteq V \times V$ where $ab \neq ba$. The digraph does not allow loops, that is, it is not allowed an edge aa. Let $e_i = v_i v_{i+1} \in G$ be edges of G for $i \in [1,k]$. The sequence $W_G = e_1 e_2 \dots e_k$ is a walk of length k from v_1 to v_k. Here e_i and e_{i+1} are compatible in the sense that e_1 is adjacent to e_{i+1} for all $i \in [1,k-1]$. We will write $a \to b$ if it exists at least one walk between a and b. We denote with $\omega_G = |W_G|$ the number of walks from a vertex a to a vertex b. A digraph will be named *complete* if $\forall a,b \in V_G$, a is adjacent with b. In this case, if $\upsilon_G = N$, it will be $\epsilon_G = N(N-1)$. Furthermore, a digraph will be named *connected*, if $\forall a,b \in V_G$ it exists at least one walk $a \to b$.

Let G_{IdP} a subgraph of the graph G, denoted by $G_{IdP} \subseteq G$, if $V_{IdP} \subseteq V_G$ and $E_{IdP} \subseteq E_G$. G_{IdP} represents the traditional IdP/SP authentication system in a federated cloud environment. G_{IdP} is built according to K events. An event represents the need of authentication of cloud a in cloud b, and each oriented edge $ab \in E$ represents a trust relationship, i.e., the enrollment of cloud a in the IDP on which cloud b relies, so that a will be read cloud and b IdP. Given an event with two equiprobable random vertices a,b, $a \neq b$, if a walk of length $k = 1$ exists, that is, if an edge ab exists, nothing is done; else an edge ab is created. Considering the set F with all the clouds belonging to the federation with $\upsilon_V = N$ each cloud $a \in F$, in order to be federated with the other $N-1$ clouds, must have a walk of length $l = 1$ toward all the other $N-1$ clouds of the federation. This implies that the digraph representing the federation has to be connected, so that $N(N-1)$ trust relationships (i.e., enrollments of cloud in IdPs) have to be performed. In this case, considering G_{IdP}, $\omega = \epsilon = N(N-1)$ is the number of needed trust relationships t_r in order that each clouds is able to be authenticated in each other. Figure 3 depicts an example of digraph representing the authentications in a federated clouds environment with total overlay using the traditional IDP-based system with $\upsilon = 10$ and $\omega = \epsilon = 90$.

Let $G_{DIdP-TN}$ a subgraph of the graph G, denoted by $G_{DIdP-TN} \subseteq G$, if $V_{DIdP-TN} \subseteq V_G$ and $E_{DIdP-TN} \subseteq E_G$. $G_{DIdP-TN}$ represents a DIdP-TN in a federated clouds environment. $G_{DIdP-TN}$ is built according to K events. An event represents the need to establish a trust relationship, i.e., an agreement between two IdPs, and each oriented edge $ab \in E$ represents the a trust relationship between IdP a and IdP b where delegated authentications take place. Given an event with two equiprobable random vertices a,b, $a \neq b$, if it exists one and at least one walk from the vertex a to the vertex b, nothing is done, else an edge ab is created. The meaning of each element $ab \in V$ of $G_{DIdP-TN}$ is the following: if we read ab, it will be read the IdP b is trusts IdP a. It is important to notice that as we are considering a digraph, if IdP a trusts IdP b it does not mean that IdP b trusts IdP a. This implies that the digraph representing the DIdP-TN has to be only complete (and not connected as in the previous scenario). In this case, a walk $a \to b$ of length $1 \leq l \leq N-1$ from IdP a to the IdP b represents a trust relationship between the two IdPs. Note that in this case considering $G_{DIdP-TN}$, $\epsilon \leq \omega \leq N(N-1)$, that is, the number of needed trust relationships between IdPs is less or equal to

 ISBN: 978-1-61208-153-3

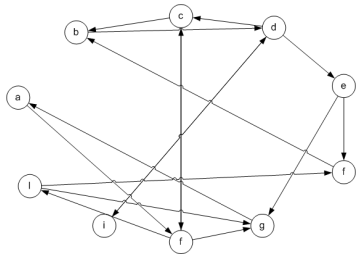

Figure 4. Example of digraph representing a distributed system of IdPs with delegated authentication in federated cloud environment.

t_r. Figure 4 depicts an example of a digraph representing the trusted relationships between IdPs, by means of each cloud is able to perform a SSO authentication on each other.

B. Comparison Between the two Authentication Approaches

For each authentication scenario we built a digraph creating edges according to the simulation of K events. For both graphs, we assumed an order $v = 25$. In simple terms, we considered a scenario including 25 Idps. For each event $i, i = 1, 2, \ldots, K$, we stored the number ϵ_i of edges created and the percentage X_i of total overlay on the whole digraph up to event i as:

$$X_i = \frac{\epsilon_i \cdot 100}{N(N-1)} \quad (3)$$

The total overlay is a parameter indicating how clouds cover the network of federated clouds from the point of view of authentications. The 100% of total overlay is obtained when each cloud of the federation is able to perform the authentication with all the other ones.

For simplicity, all the simulations have been performed with equiprobable events, and without the possibility of cancellation of a created edge, i.e., without the possibility to break trusted relationships. For each of the two authentication scenarios, we assumed 25 IdPs and 8000 events, repeating the simulations 50 times, picking up the mean values of both the created edges and the total overlay percentage for each $i - th$ event. For each simulation, we also calculated variances and confidence intervals at 95%. The goodness of our experiment is motivated by the fact that we have obtained confidence intervals rather small.

Figures 5 and 6 depict a comparison between the two authentication scenarios respectively considering the percentages of overlay on the whole cloud federation and the number of established trust relationships. In Figure 5, on the x-axis is reported the number of simulated events instead on the y-axis is reported the percentage of overlay on the whole cloud federation. Regarding the traditional IdP/SP authentication scenario, we obtained the 100% of overlay on the whole cloud federation after 6765 events (i.e, the need of establish authentications between clouds), instead in the case of the DIdP-TN we obtained the 100% of

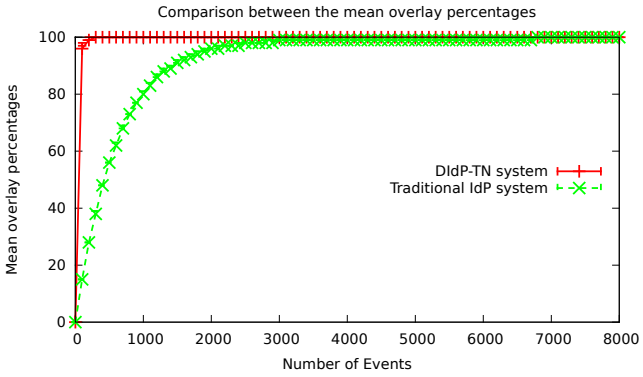

Figure 5. Comparison between the two authentication systems, considering the overlay percentages.

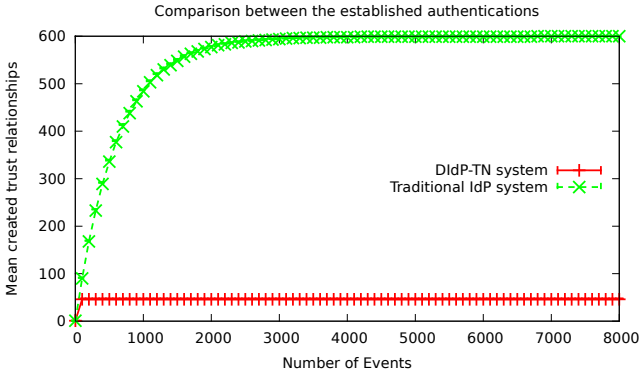

Figure 6. Comparison between the two authentication systems, considering the mean value of created authentications.

total overlay after 285 events (i.e., the need of establish agreements between IdPs). In Figure 6, on the x-axis is reported the number of simulated events, instead on the y-axis is the number established trusted relationships. We remark that for the traditional IdP/SP authentication scenario a trust relationship is an enrollment of a cloud in one IdP, and that in the case of DIDP-TN authentication scenario a trust relationship is an agreement between two IdPs. Regarding the traditional IdP system scenario, we can observe that we obtained a connected digraph after 6765 events. In fact, after 6765 events, we obtain $N(N-1) = 25 \cdot 24 = 600$ enrollments of clouds on IdPs. Instead, regarding the DIdP-TN system, we obtained a system in which each cloud is able to perform authentication on each other after 285 events, and 47,860 mean established agreements between IdPs. In both cases the variance had a Gaussian trend. This meant that the confidence intervals had their maximum amplitude around the midpoint of all the curves, before their saturation. Saturation is reached when each cloud is able to perform the authentication with each other, i.e., when the overlay percentage is 100%.

 ISBN: 978-1-61208-153-3

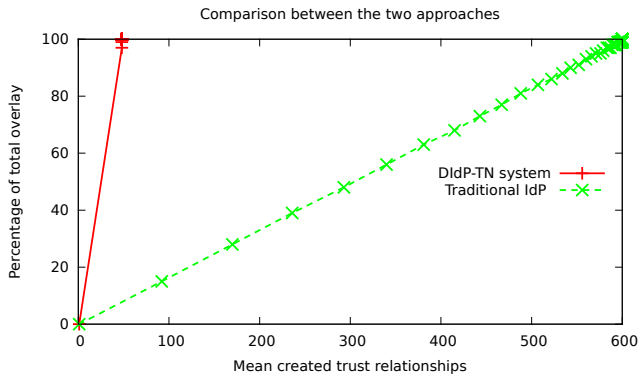

Figure 7. Comparison between the two approaches considering both the number of created authentications and the respective overlay percentages.

Figure 7 depicts a comparison between the two approaches considering both the number of created trust relationships on the x-axis and the respective overlay percentages on the y-axis. It is possible to notice how for the DIdP-TN system the 100% of overlay is obtained faster than the traditional IdP system.

C. Overcoming issues with Transitive Trust

The paper we are presenting is a preliminary work that needs to be refined. In the context of Transitive Trust, systems authentication performed along through the delegation mechanism might raise problems. In particular in our case a subset of IdPs that are nor recognized in the chain of trustiness of whatever cloud provider. To address such a problem we introduced the Access Control List (ACL) for preventing the involvement of untrusted IdPs no directly accesses but present in the list of delegation. Indeed there could be the possibility that even though a trust relationship exists from an IdP a to an IdP b through a cloud c, the cloud a decide to create a direct trust relationship with cloud b because it considers too much risky a delegated authentication through a cloud c. For example cloud a could consider cloud c not so reliable from the point of view of security. We are looking at a much more complex trustiness scenarios in which the links weight of trusting walks along with the IdP reputation must be taken into account (i.e., [20]).

V. Conclusions

In this paper, we focused on two authentication scenarios for federated cloud environments: the first based on the adoption of a traditional IdP system, and the second based on a DIdP-TN. From the simulations, it is evident how the DIdP-TN system allows to drastically reduce the needed operations for clouds, simplifying the management of accounts and enrollments. However, even if on one hand it is possible to reduce the number of needed authentications, on the other hand a few problems might rise. In this work, we assumed equiprobable events, but if we consider also the possibility of breaking the trust relationships, the scenario on one hand might be fault tolerant as alternative trust relationships (i.e., walks considering the digraph) might exist, whereas on the other hand the scenario might become more complicated.

References

[1] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "How to enhance cloud architectures to enable cross-federation," in *Proceedings of IEEE CLOUD '10*, pp. 337–345, IEEE, July 2010.

[2] April 2011. IEEE works towards cloud interoperability standards: http://www.cloudcomputingzone.com/2011/04/ieee-works-towards-cloud-interoperability-standards/.

[3] Forum of Federations: http://www.forumfed.org/en/index.php.

[4] B. Rochwerger, D. Breitgand, A. Epstein, D. Hadas, I. Loy, K. Nagin, J. Tordsson, C. Ragusa, M. Villari, S. Clayman, E. Levy, A. Maraschini, P. Massonet, H. Munoz, and G. Toffetti, "Reservoir - when one cloud is not enough," *Computer*, vol. 44, pp. 44–51, 2011.

[5] "C. Adams and S. Farrell, Internet X.509 Public Key Infrastructure: Certificate Management Protocols, RFC 2510: http://tools.ietf.org/html/rfc2510."

[6] "Security assertion markup language, oasis, http://www.oasis-open.org/committees/security."

[7] K. Traw, S. Yang, and P. Comitz, "Federated identify management in service oriented architectures," in *Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pp. 1–6, May 2008.

[8] R. McKenzie, M. C. M, and C. Wallis, "Use cases for identity management in e-government," in *Security & Privacy, IEEE*, vol. 6, pp. 51–57, March-April 2008.

[9] Goiri, J. Guitart, and J. Torres, "Characterizing cloud federation for enhancing providers' profit," *Proceedings of IEEE Cloud '10*, pp. 123–130, 2010.

[10] D. Artz and Y. Gil, "A survey of trust in computer science and the semantic web," *Web Semantics: Science, Services and Agents on the World Wide Web*, vol. 5, no. 2, pp. 58 – 71, 2007.

[11] S. Florian, S. Daniel, and D. Schahram, "The cycle of trust in mixed service-oriented systems," in *Proceedings of SEAA '09*, pp. 72–79, 2009.

[12] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Three-phase cross-cloud federation model: The cloud sso authentication," *Second International Conference on Advances in Future Internet (AFIN)*, pp. 94–101, 2010.

[13] P. Arias Cabarcos, F. Almenárez Mendoza, A. Marín-López, and D. Díaz-Sánchez, "Enabling saml for dynamic identity federation management," in *Wireless and Mobile Networking*, vol. 308, pp. 173–184, Springer Boston, 2009.

[14] T. Komura, Y. Nagai, S. Hashimoto, M. Aoyagi, and K. Takahashi, "Proposal of delegation using electronic certificates on single sign-on system with saml-protocol," in *SAINT*, pp. 235–238, 2009.

[15] S. Shen and S. Tang, "Cross-domain grid authentication and authorization scheme based on trust management and delegation," in *CIS*, pp. 399–404, 2008.

[16] W. Jun, D. V. David, and H. Marty, "Extending the security assertion markup language to support delegation for web services and grid services," in *Proceedings of IEEE ICWS '05*, pp. 67–74, 2005.

[17] M. S. F. Jingwei Huang, "An ontology of trust: formal semantics and transitivity," in *ICEC*, pp. 259–270, 2006.

[18] J. Huang and M. S. Fox, "An ontology of trust: formal semantics and transitivity," in *Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet*, ICEC '06, (New York, NY, USA), pp. 259–270, ACM, 2006.

[19] Y. Chen, T.-M. Bu, M. Zhang, and H. Zhu, "Max-minimum algorithm for trust transitivity in trustworthy networks," *Web Intelligence and Intelligent Agent Technology, IEEE/WIC/ACM International Conference on*, vol. 3, pp. 62–64, 2009.

[20] Y. Chen, T.-M. Bu, M. Zhang, and H. Zhu, "Measurement of trust transitivity in trustworthy networks," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 4, 2010.

 ISBN: 978-1-61208-153-3