Identity Management Based Security Architecture of Cloud Computing on Multi-Agent Systems

Alguliev Rasim, and Abdullayeva Fargana

***Abstract*—In traditional identity management systems user authentication is usually carried out on the basis of management list, previously defined in a system. But with the increasing number of users in such environment as a cloud the management of this list becomes more difficult. For this purpose, in this paper the model supplying the dynamic management of the users' identity federation was introduced. With the implementation of multi-agent systems and the decision making solutions the identity federation dynamization was ensured.**

***Index Terms*—Cloud computing, federated identity management, provider, single sign-on.**

I. Introduction

THE emergence of cloud computing has recently caused a revolutionary coup in the Internet. However, main abstacle to wide range application of this technology is information security.

In the majority of cloud computing security investigations and standardization documents the identity management, risk assessment and trust management are considered as the key issues.

In the guideline published by the ENISA (European Network and Information Security Agency) [1] the establishment of trust relationship in the cloud infrastructure is defined as an important research area.

Also in the recommendations prepared by the NIST (National Institute of Standards and Technology) [2] and the CSA (Cloud Security Alliance) [3] the identity management and trust management are highlighted as an important issue.

In addition, in a number of other documents published by the standardization organizations and research institutions the identity federation is considered as an invaluable mechanism [4,5].

There is a wide rang of research works lead in the area of federated identity management problems in the cloud computing environments.

Among these studies, the approaches devoted to the federation of the clouds [6], as well as the identity management integration approaches [7] draw more attention.

Rasim Alguliev is with the Institute of Information Technology, Azerbaijan National Academy of Sciences, Azerbaijan, Baku (e-mail: director@iit.ab.az).

Fargana Abdullaeva is with the Institute of Information Technology, Azerbaijan National Academy of Sciences, Azerbaijan, Baku (e-mail: farqana@iit.ab.az).

Lack of these approaches is that the identity management architectures are constructed on the basis of pre-existing trust relationships between providers and are based only on the static technologies such as digital certificates, PKI (Public Key Infrastructure).

At present, by series of the world leading organizations there has been developed a number of identity management systems. An example of these systems can be shown as McAfee Cloud Identity Manager, Microsoft Identity & Access, Novell Identity Manager, EmpowerID SSO Manager, Symplified Trust Cloud, OneLogin, IdM4Cloud etc. The functioning of these systems within certain limitations is one of the biggest drawbacks. The integration means of these systems are not constructed sufficiently, therefore they do not allow us to expand the scope of the systems rapidly. In other words, the increasing number of the providers makes the integration functions of the systems unable to integrate.

In this paper we offered a dynamic federated identity management model that allows us to rapidly decrease and increase the scope of the cloud. For this reason, we applied the multi-agent systems. One of the functions of the multi-agent systems is to perform the collection of necessary information about the user, which allows us to make dynamic decisions in the real-time system.

In such uncertain environment as a cloud the assessement of the subject's trust degree is considered to be an important means of realization of the decision-making process.

On the basis of the trust degree calculated by the number of metrics we can construct a dynamic trust relationship between cloud providers. And this trust value may be the best tool in the federation prosess among clouds.

II. IDENTITY MANAGEMENT

Digital identity is the representation of an entity (or group of entities) in the form of one or more elements of information (attributes) that enable the entity to be recognized only within a context [8,9,10].

Identity Management (IdM) is a set of functions and capabilities, such as administration, management and maintenance, discovery, information exchange, policy enforcement and authentication, used to ensure identity information, thus assuring security. An identity management system (IMS) provides tools for managing individual identities in a digital environment [10].

The main functions of an IMS are follows [10]:

- *Provisioning:* the practice of provisioning of identities within an organization addresses the provisioning and deprovisioning of several types of user accounts (e.g. end user, the application administrator, IT administrator, supervisor, developer, etc.).
- *Authentication:* the process of ensuring that the individual is who he claims to be, and is identified through various mechanisms, such as login, password, biometrics, token, etc.
- *Authorization:* a common need in security to provide different access levels (e.g. deny/allow) for different parts or operations within a computing system. This need is called authorization.
- *Federation:* a group of organizations or SPs that establish a circle of trust that allows the sharing of information of user identities to each other.

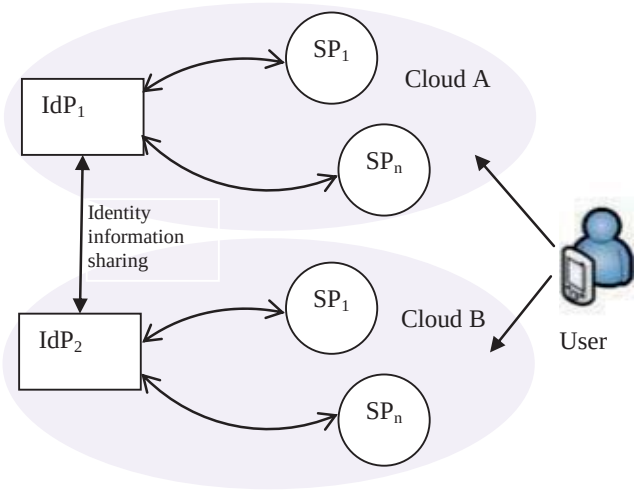

Figure 1. Identity federation prosess

III. SINGLE SIGN ON AND FEDERATED IDENTITY MANAGEMENT

In the Internet users obtain access to the resources belonging to the different service providers by using different accounts. Passwords and user names generated in these accounts are different from each other. For this reason, the vast majority of the network users tries to use the same password in each possible place. This leads to serious security risks. The repeated authentication of the users causes the troubles among them, and beside that it also strongly increases the series of the administrative expenses. Nowdays, the majority of the world global organizations, in order to struggle with passwords, try to use SSO (Single Sign On) technologies as these technologies allow to replace a number of network passwords with a single password.

Single Sign On − is the technology that allows the users to authenticate at a single IdP and gain access to all SPs in a federation with IdPs without providing any additional information.

Identity Federation − is the one of the identity management concepts [11], that share and distribute attributes and identity information across different administrative domains according to certain established policies.

Following three actors are forms the identity federation model (Figure 1):

- *Service Providers (SPs).* Actors which consume user's identity data. They rely on the user authentication made by a third party. SP are also called Relying Parties (RP).
- *Identity Providers (IdPs).* Actors that assert information about a subject. IdP are also called Asserting Parties (AP). IdPs focus on the authentication of the users as well as on the management of identity information, which can be shared with various SP.
- *Users.* Actors which interact (usually via the user agent, e.g. web browser) with SPs. They are the subject of the assertions.

As shown in the figure 1, the share of the identity information between the two providers (IdP1 and IdP2) allows a user to log in only once and gain a seamless access to services and applications offered in different domains.

Identity federation can be accomplished by means of formal Internet standards, such as the OASIS SAML specification, or by using open source technologies and other openly published specifications, like the Liberty Alliance Identity Federation Framework (ID-FF), Shibboleth, OpenID or WS-Federation.

SAML (Security Assertion Markup Language). It is an XML-based protocol which provides the exchange of security returns between the subjects. In this model trust relations between IDPs and SPs are defined in advance. Trust establishment is based on PKI technology [12]. It is founded in 2005 by the organization OASIS.

Shibboleth. It is a system based on SAML technology and is a project of "Internet2 Middleware Initiative" consortium. The world's most widely used federated identity management mechanism, allows users to gain access to the resources whitin and out of organization. In this model the federation process between the providers is conducted on the base of the list containing the names of the providers. This list allows to use common rules between the providers. One of the shortcomings of this model is the complexity of the management of the providers' list.

OpenID. This is a user-centric protocol. This means that the user chooses the IdP for authentication by himself. The trust model is not used there.

Identity Federation Framework (ID-FF). It is the Liberty Alliance organization's project. In this model the federation between the subjects is provided on the basis of the "Circle of Trust" (COT) concept.

WS-Federation. In this model the federation between the subjects is provided on the basis of the WS-Trust (Web service) concept.

The conducted researches show that the organization of the federation prosess is accomplished between the providers on the basis of current technologies known in advance as static trust relationships. This approachs is not

suitable in such dynamic environment as a cloud. For this reason, there arises the necessity to develop a new kind of dynamic federated management model, which takes into account the main characteristics of the cloud.

IV. FEDERATED IDENTITY MANAGEMENT MODEL FOR CLOUD COMPUTING

The model presented in Figure 2 provides the dynamical management of the user identity federation process and is based on authentication and authorization tasks.

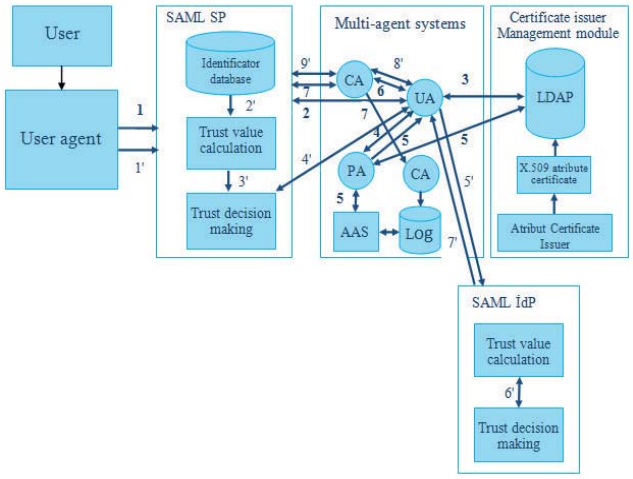

Figure 2. Identity federation dynamic management architecture

Here for providing a user's single access to cloud infrastructure the protocol SAML is used. The users' dynamic federated identity management process is based on PKI technology and the calculation of trust value. The user's access to the cloud infrastructure is provided on the basis of their attribute certificates, also the privileges to each user are given by the role based on the access control mechanisms. Cloud environments are dynamic. Because of that statically the determination of the users' roles only by certificates has lost its actuality. In this case, the dinamic management of roles becomes necessary. The application of multi-agent systems in architecture allows the dinamic determination of users' roles. The content of these roles also contains behavioral characteristics of the users.

For the maintenance of the architecture as a single sisytem the following components are used:

Multi-agent system (MAS). Provides the authentication, authorization and audit operations within the cloud environment. The trust degree of the MAS module is defined by the Public Key İnfrastructure (PKI). MAS contains the following agents:

- *User agent (UA).* Provides the validation of user certificates, the verification of user requests, acquires the authorization of the information from the policy agent (PA), presenting a list of privileges for the user.
- *Collecting agent (TA).* The agent which generates the interface with a log server. Each component of the architecture sends the users' log records to this agent. This agent plays an interface role between the log server and another components of an architecture. All records to the log server are added via this interface.
- *Policy agent (PA).* Combines the roles obtained from the user's attribute certificate with DPL created in AAS and on the basis of this generates a single privilege list (SPL) for the user.
- *Contact agent (CA).* Agent which provides the communication with SP.

Activity Analyzer Server (AAS). Performs two functions: analyses the log files and generates a Dynamic Privileges List (DPL) for the user. This list is called DPL, because it comprises the data associated with the users' behavior.

Log server. Collects log records associated with the activity of each entity in the system.

Certificate Issuer Management Module. It is a component which produces X.509 type attribute certificate. This certificate is physically stored in the catalog LDAP (Lightweight Directory Access Protocol).

Attribute Certificate (AC). The management of the users' privileges is carried out in accordance with the roles included in AC. Attribute Certificate contains version, holder, issuer, signature, serial number, validity period, and attributes. In the attributes field the user's roles can be assigned.

V. INFORMATION FLOW IN FEDERATED IDENTITY MANAGEMENT MODEL

In the given architecture the information flow is implemented in two phases (Figure 2). These phases are based on the circle of trust which may be known or unknown for the providers.

Federated identity management with a known circle of trust

1. User sends a request to SP to authenticate himself by using smart card or tokens (which contains certificates).
2. If the user signed up in the SP identifiers database, the SP sends a request to the MAS module. This module on the basis of this request creates a UA for the user. The purpose of the UA is to manage all user requests. MAS creates UA only for the users which are verified by the SP and this new UA is automatically accepted as a trusted subject.
3. The UA looking for the LDAP directory, confirms the authenticity of the user certificate and verifies it in conformity with systems' predefined security policy.
4. Here the creation of the user privilege list is carried out on the basis of these privileges the users gain the ability to implement any transactions in cloud infrastructure. For this purpose the UA creates a privilege list for a certified user by sending a request to the PA.
5. The PA obtains user static roles contained in certificates by addressing LDAP directory and combines them with a dynamic privilege list greated in AAS and sends them to the UA. The privilege list created in AAS contains information

associated with the user activity, therefore its structure is dynamically changeable.

6. The users' query shipped to the UA is compared with his privilege list. If the user is an authorized user, the UA sends a request to the CA for starting a new session.
7. The CA signs the request and sends it to the SP. The SP accepts the request, checks the signature signed by the CA in the previous stage, determines the trust degree of the request and on the basis of this allows to start the session.

In the above described process on the basis of pre-determined contracts there is a certain trust relationship between the SP and the IdP. Previously registration of the user in IdPs allows him to gain access to the SP infrastructure, without any additional registration process.

Assume that the user does not have the registration in the SP infrastructure, and he wants to use SP recources by authenticating himself in his own IdP. And these providers (SP and IdP) are unknown to each other, in other words the pre-determined static trust relationship is not established between these providers and their circles of trust are different. In this case, it is becoming necessary to ensure the identity management prosess in a federation. This prosess can be described as follows.

The federated identity management with the unknown circle of trust

1. For the using of SP resources the user sends a request to the SP.
2. The *identifier database* discovers that the user is not registered, and then it automaticaly sends the query to the trust value calculation block. On the basis of some metrics (for example, the IdP reputation, data on the service level agreements etc.) it calculates the trust value of the IdP belonging to the user.
3. The trust value is sent to the decision making block, and if the calculated trust value is not greater than that of the threshold adopted by the SP, then the SP evaluates the IdP as a trusted subject.
4. In order to create the federation, decision making block sends a request to the MAS module and on the basis of this request the MAS sets the UA for the user.
5. The UA sends this request to the IdP.
6. For the establishment of the federation process between the providers, their trust value should be known to each other. Therefore, to build a trust relationship and to start the federation prosess with the SP the IdP also calculates the trust value of the SP and sends it to the decision making block.
7. If the calculated trust value is not greater than that of the threshold adopted by the IdP, then the IdP evaluates the SP as a trusted subject and in order to create the federation, it sends a request to the UA block.
8. On the basis of this information the UA sends a request to the CA.
9. The CA signes the request and sends it to the SP. The SP checks the signature of the CA, ensures that the request is trusted and then provides the starting of the new session.

REFERENCES

[1] D. Catteddu, G. Hogben, "Cloud computing: benefits, risks and recommendations for Information security," European Network and Information Security Agency Technical Report, 2009, 125 p.

[2] SP 800-144. "Guidelines on Security and Privacy in Public Cloud Computing," National Institute of Standards and Technology Special Publication, 2011, 70 p.

[3] "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, 2011, 176 p.

[4] "Identity in the Cloud−Use Cases," Organization for the Advancement of Structured Information Standards, 2012, 111 p.

[5] "Moving to the Cloud," Cloud Computing Use Case Discussion Group, 2011, 11 p.

[6] V. Casola, M. Rak, U. Villano, "Identity federation in cloud computing," In Proc. of the IEEE 6th International Conference on Information Assurance and Security, 2010, pp. 253–259.

[7] A. Celesti, F. Tusa, F.M. Villari, A. Puliafito, "Security and cloud computing: Intercloud identity management infrastructure," In proc. of the 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 2010, pp. 263–265.

[8] ITU-T X.1250, "Baseline capabilities for enhanced global identity management trust and interoperability," Draft New Recommendation ITU-T (X.idmreq), February 2009.

[9] D.W. Chadwick, "Federated identity management," Springer Verlag: Berlin, Heidelberg, 2009, pp. 96–120.

[10] M.A. Leandro, T.J. Nascimento, D.R. Santos, C.M. Westphall, C.B. Westphall, "Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth," The Eleventh International Conference on Networks (ICN), 2012, pp. 88-93.

[11] R.M. Əliquliyev, F.C. Abdullayeva, "Bulud texnologiyalarının təhlükəsizlik problemlərinin tədqiqi və analizi," İnformasiya Texnologiyaları Problemləri, 2013, to be published.

[12] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL)," RFC 5280, 2008, 151 pp.