A secure authentication model for Cloud federation

Belbergui Chaimaa, Elkamoun Najib, Hilal Rachid

STIC Laboratory Chouaib Doukkali University El jadida, Morocco

Summary

The cloud computing is a revolutionary change in the IT field. One of Cloud Computing evolution is Cloud Federation. Thanks to this paradigm, cloud providers can federate themselves, in order to reduce costs and enlarge their capabilities, through cooperating together. However, some limitations have to be overcome firstly. One of the major requirement is a strong identity management solution.

Using Cloud Federation, the customers can get services from several Cloud Service Providers belonging to the federation. In this context, Single Sign-On property can be adopted to verify identities of users without requiring them to be authenticated with each service provider separately. The advantage is that only one authentication is required to access all resources. However, if a password is hacked by a malicious person, he will have access to all services. Thus, authentication in Cloud federation is still a major research challenge that remains unsolved.

This paper suggests a new authentication model to address authentication concerns in the Cloud federation context and support multi-domain clients in a multi-provider environment. It is based on Single Sign-on property combined with One Time Password mechanism to enhance security. The paper also shows how the proposed solution can be successfully applied to manage the authentication needed among clouds for the federation establishment and present some implementation details. The proposed architecture offers significant advantages like the easy to use and strong security.

Key words:

Cloud computing; Cloud Federation; Security; Identity Management; Authentication; Single Sign-On.

1. Introduction

The cloud computing is an explosive revolution in the IT field that allows to provision resources as a service over the network [1]. Services range from Software as a Service (SaaS) to Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). Furthermore, four different deployment models are offered: private, community, public, and hybrid clouds. Thanks to this paradigm, the user can benefit from on-demand access to resources that can be rapidly provisioned, reduced IT management and maintenance costs, high availability, and pay per use [2].

In Cloud computing, it is desirable that users are able to access or use applications hosted in another cloud. In this context, "Cloud Federation" came to light. Providers federate themselves to cooperate with other federated ones with the purpose to enlarge their computing and storage capabilities, and allow users to access various resources or services after verification of their identity [3].

Despite Cloud Federation benefits, there is the downside associated with the use of the Cloud federation model such as security concerns [4]. Federated identity management represents the first issue to be solved. It deals with the establishment of trust relationships between various security domains to share authentication data, and reduce management complexity and security risks.

Current federated identity solutions help to simplify authentication procedures for end users using, generally, Single Sign-On (SSO) mechanism based-password. However, authentication based-password do not provide strong security and its use is not recommended. Also, when the password is violated, all services related to this one will be impacted.

In this paper, we try to face the identity management and authentication issues in cloud federation. We propose a complex and strong solution using the Single Sign-On authentication based on the One Time Password (OTP). The proposal brings multiple advantages, it allows user to access and use several services without having to be authenticated by providing credentials several times. Also, even if the password is violated, a hacker cannot access or use services since an OTP code is required to complete the authentication process.

The paper is organized as follows. Section II presents preliminaries. Section III highlights the main related works. After that, we provide the proposal in section IV and its implementation in section V. Finally, conclusions are summarized in section VI.

2. Preliminaries

2.1 Federation

Cloud federation (Fig. 1) is an association between several Cloud providers which will be aggregated in a single pool [2]. The main goal is to overcome limitations like the lack of available resources, and to meet the dynamic and unpredictable user requirements like quality of service or easy authentication [4].

Identity federation is one of the basic elements of any interoperable infrastructure. If it does not exist, users cannot use the infrastructure easily. They will deal with managing multiple identities and credentials and will need to be

Manuscript received September 5, 2017
Manuscript revised September 20, 2017

concerned with the specific details of each service provider authentication process separately.

Moreover, any federated infrastructure should leverage the establishment of relationships between the users and the resource providers. If a federated identity system does not exist, the resource providers need to define access policies individually for each of the users and groups willing to access the infrastructure, whereas the users need to negotiate their access policy and shares of the resources with each of the resource providers. When the number of users increase this becomes an overwhelming task for the resource providers [5].

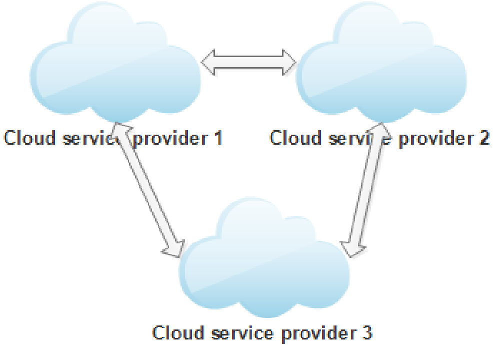


Fig 1. Cloud Federation

2.2 Single Sign On

Single Sign-On (SSO) is an authentication mechanism in which a Cloud Service Consumer needs to be authenticated only once while accessing various services from multiple service providers, or when accessing multiple services from the same service provider.

This service relies on several identity federation standards, such as the WS-Federation Security Assertion Markup Language (SAML), OAuth and other ones, to simplify the federation across multiple applications.

In the context of Cloud Federation, we distinguished two types of cloud: home cloud and foreign cloud [6]. Software as a Service allows users to register or log in using their home Cloud credentials. Once users have successfully authenticated themselves, proof of authentication and associated attributes are shared securely so that foreign Clouds can authenticate them without intervention on their part.

The using of the SSO mechanism offers several advantages such us enhanced user experience with single-sign-on across multiple IT domains, increased external access security for identity information control and multiplication of business partnership opportunities to provide more services to the customers [7]. However, security concerns have persisted since, if a password is hacked by a malicious person, he will have access to all network services related to this password.

3. Related works

With the increasing interest in the cloud computing paradigm, security is becoming an important concern for researchers since it constitutes the main barrier to its adoption.

Between the main security open issues is an appropriate identity management system in the context of Cloud Federation.

In [1], the authors analyze the Federated Identity Management process and propose a taxonomy that helps in the classification of the involved risks in order to mitigate vulnerabilities and threats when decisions about collaboration are made.

The authors propose in paper [3] a solution based on the Cross-Cloud Federation Manager, a new component placed inside the cloud architectures, allowing a cloud to establish the federation with other clouds according to a three-phase model: discovery, matchmaking and authentication. As for [6], it presents a reference architecture to address the Identity Management (IdM) problem in the InterCloud context. In the same context, the work [8] proposes a technical solution based on the Security Assertion Markup Language (SAML) technology. More specifically, it designed a new SAML profile named Cross-Cloud Authentication Agent, which defines the steps needed for a secure cloud SSO authentication to be performed by the authentication agents of the involved clouds. The work [9] concerns the use of the Virtual Organization Membership Service (VOMS), a well proven technology in the Grid area, to provide identity federation across different providers.

The papers [4], [10] give the workflow model for the proposed approach of SSO in the Cloud Federation. Also, authors of papers [11], [12] are working on improving the way to use SSO to achieve Authentication. In the same context, [13] proposes an authentication infrastructure that achieves single sign-on (SSO), which allows users to log in once and access the various cloud systems without being asked to log in again at each system. Furthermore [14], [15] also work on authentication based SSO. The paper [14] offers a scalable user authentication scheme for cloud computing environment. In the suggested model, various tools and techniques have been introduced and used by using the concept of agent. Therefore, a client-based user authentication agent has been introduced to confirm identity of the user in client-side. For the work [15], it leads to implementation of Cloud for Storage and Virtual Machines Images to run the SSO on the top layer of the Cloud.

The authentication in the context of IaaS was proposed in the paper [16]. It presents a proposal to tackle a much more complex scenario, allowing sharing of information through all cloud abstraction layers, as well as on environments spanning multiple IaaS providers.

Other works like [17], [18] are based on trust. In [17], the authors extend the optimization to include identity federation in the Marketplace. This optimization is achieved by introducing provisioning steps to pre-establish trust amongst enterprise applications' Resource Servers, its associated Authorization Server and the clients interested in access to protected resources. They then introduce the notion of referral tokens to enable Marketplace applications federation across organizations. In this architecture, the trust is provisioned and synchronized as a prerequisite step to authentication amongst all communicating entities in OAuth protocol, and referral tokens are used to establish a trust federation for Marketplace applications across organizations. For the paper [18], it is designed and proposed a privacy enhanced and trust-aware IdM architecture compliance with SAMLv2/ID-FF standards. The aim is to provide an efficient identity management and access control, as well as dynamic, autonomic, and user-centric system for better scalability in cloud computing services. With the inclusion of reputation information and the introduction of the Trust. Mobile users may participate in the cloud federation in a more active way.

Existing authentication solutions are diverse but generally based on SSO technique. Sometimes, the used authentication mechanism is not specified and often times it relies on passwords which are inconvenient to the user and sometimes insecure. When a password is stolen all services used by the consumer will be violated. For this reason, existing solutions still have to be improved.

4. Proposed model

In this work, we suppose that several Cloud service providers are part of a given federation and that trust relationship is already established between those providers. The access to Cloud resources can be done online through a Web browser.

Unlike the majority of solutions that rely on SSO based password and that are so unsecured, we will propose an easy to use and a secure model that supports authentication in Cloud Federation. Thanks to this proposal, the user has not to choose one password per service which is hard to remember. Using SSO mechanism, he can use just one password to access to all services supplied by Cloud providers belonging to the federation. Also, in order to enhance security in this context, two factor authentication is used. After password verification, an OTP code will be sent to the user number phone. Next, the user is asked to enter the received code. Finally, if the entered code is correct, access will be allowed to him.

Authentication is managed by a trusted third party (Fig. 2) that verifies if the requested service belongs to the federation to enable automatic authentication or not. It acts as an intermediary between the Cloud providers.

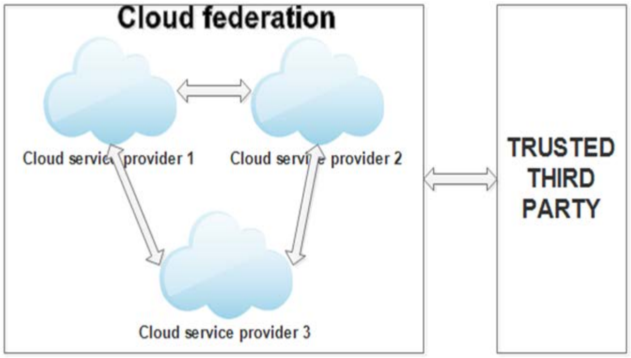


Fig 2. Cloud Federation and trusted party

In order to illustrate the applicability of our proposal, we present an example scenario

We start from the use case in where the user is registered to the cloud 1. But he is not registered to the cloud 2, and has not wished to register with another set of information for registering to another service.

Cloud 1 and Cloud 2 are part of the same federation. For this, the user can choose to register with Cloud 1 information. Third party verifies if the user is effectively registered to Cloud 1, if yes, he will be automatically registered to Cloud 2 without providing his information another time.

In the Cloud 2 login in case, after the user verification, the user will not be asked to provide his credentials since he is already authenticated in Cloud 1. The user will be automatically redirected to the OTP page to type the received code. If it is correct, he will be redirected to the Cloud 2 homepage. So, he does not need to enter the identity credentials each time he wants to use resources from the cloud partners in the federation, only the OTP code will be required.

4.1 Registration process

The figure 3 shows the registration process. When the user does registration in one of Clouds belonging to the federation, for each registration request to another Cloud belonging to the same federation, he will not be required to provide his information another time, the registration will be done automatically. The registration steps are as follows.

1. User requests to register to use the resources of Cloud 1.
2. The subscription page appears.
3. The user should size the required information to register.
4. Register is successfully done.
5. When the user requests to register to use Cloud 2 or Cloud 3 resources with Cloud 1.
6. TTP verifies if the user belongs to the database.
7. If yes, the subscription is done automatically since the both clouds belong to the federation.

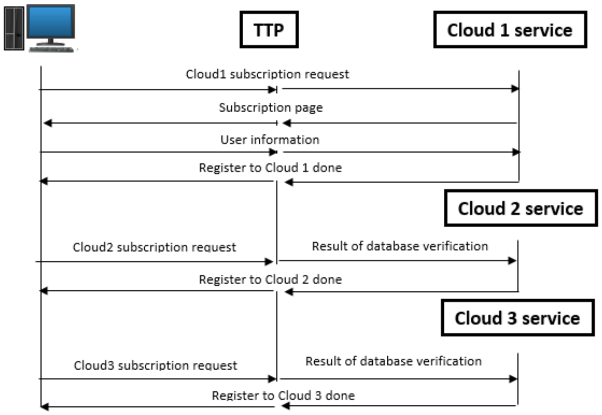


Fig 3. Registration process

4.2 Authentication process

Figure 4 shows the subscription process. When the user is registered and authenticated in the Cloud 1, and registered in the Cloud 2 belonging to the same federation, he will not be required to provide his credentials another time, just the received one time password is required to secure authentication since it is valid only for once.

1. The user requests to log in to use the resources of Cloud 1.
2. The authentication page appears.
3. The user should type his credentials and the received OTP code to log in.
4. Log in is successfully done.
5. When the user requests to login in to use Cloud 2 or Cloud 3 resources with Cloud 1.
6. TTP verifies if the user belongs to the database.
7. The login in is done automatically, after typing OTP code only, since the both clouds belong to the federation.

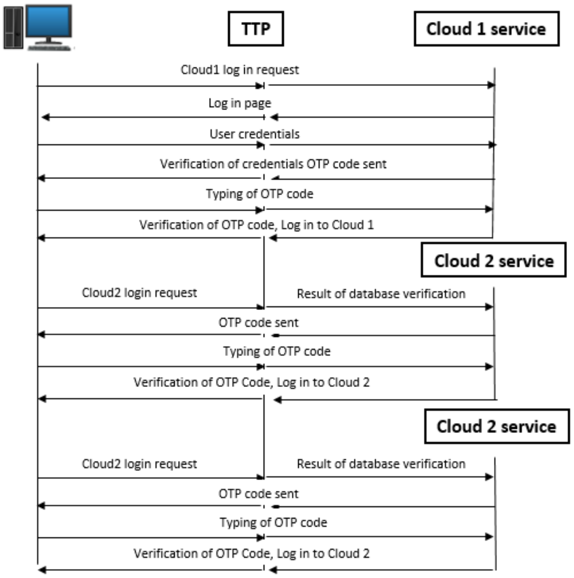

TTP
Cloud 1 service
Cloud1 log in request
Log in page
User credentials
Verification of credentials OTP code sent
Typing of OTP code
Verification of OTP code, Log in to Cloud 1
Cloud 2 service
Cloud2 login request
Result of database verification
OTP code sent
Typing of OTP code
Verification of OTP Code, Log in to Cloud 2
Cloud 2 service
Cloud2 login request
Result of database verification
OTP code sent
Typing of OTP code
Verification of OTP Code, Log in to Cloud 2

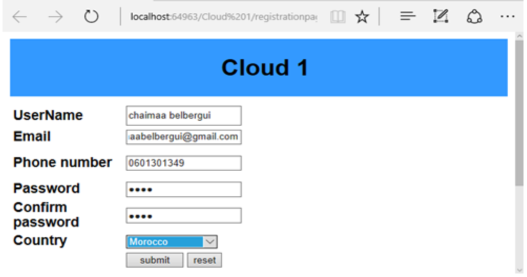
Fig 4. Authentication process

5. Implementation and discussion

The implementation of the proposed solution uses SSO based-OTP. It was developed by using C# language, .NET framework and Visual Studio environment. The integrated database is used to store user information.

5.1 Registration steps

The user should firstly register to one of the Clouds belonging to the federation. For this reason user will register to Cloud 1 by providing information such as username, email, number phone, password and country (Fig. 5). After that, for other Clouds, user can choose to register normally by providing his information another time or register automatically with Cloud 1 by clicking on "register with Cloud 1" (Fig. 6). In the last case, the user will be directly redirected to the Cloud 2 login page (Fig 7).



UserName chaimaa belbergui
Email aabelbergui@gmail.com
Phone number 0601301349
Password ••••
Confirm password ••••
Country Morocco

Fig 5. Cloud 1 registration

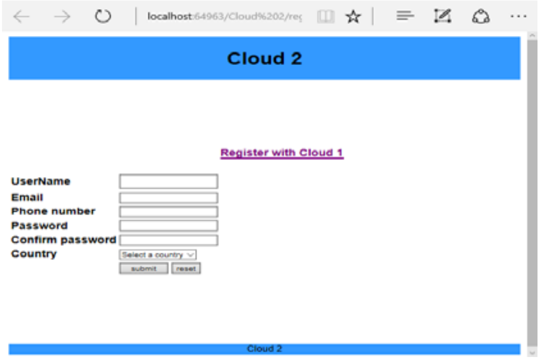


Fig 6. Cloud 2 registration page

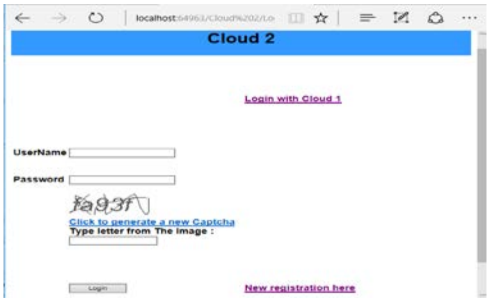

localhost:64963/Cloud%202/Lo
Cloud 2
Login with Cloud 1
UserName
Password
fa93f
Click to generate a new Captcha
Type letter from The image :
Login
New registration here

Fig 7. Cloud 2 login page

5.2 Authentication steps

When the user is registered and authenticated in Cloud 1 by providing his username, password and CAPTCHA code, to discriminate himself with machine (Fig. 8), and after the registration in Cloud 2 (Fig. 6), the user can authenticate himself to access or use resources of Cloud 2 normally by providing his credentials (username and password) another time or log in automatically with Cloud 1 by clicking on "log in with Cloud 1" (Fig. 7). In the last case, he does not have to redo all authentication process, he will be directly redirected to the OTP page and the OTP code will be generated and sent to him on his phone. When the entered OTP code is correct, he will be redirected to the Cloud 2 home page (Fig. 9).

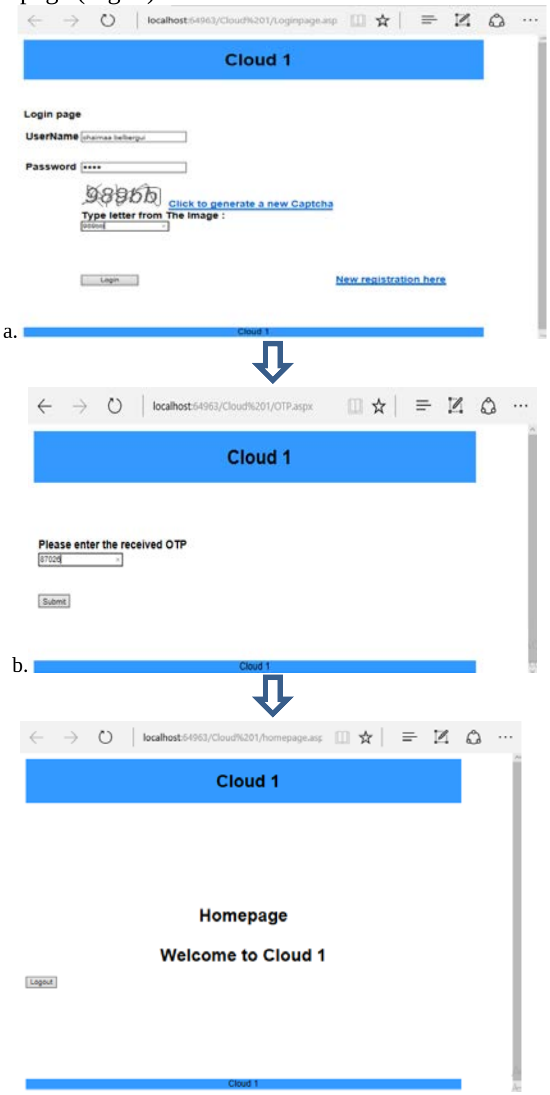

localhost:64963/Cloud%201/Loginpage.asp
Cloud 1
Login page
UserName
Password
Click to generate a new Captcha
Type letter from The Image :
Login
New registration here
Cloud 1
a.
localhost:64963/Cloud%201/OTP.aspx
Cloud 1
Please enter the received OTP
Submit
Cloud 1
b.
localhost:64963/Cloud%201/homepage.asp
Cloud 1
Homepage
Welcome to Cloud 1
Logout
Cloud 1

Fig 8. Cloud 1 authentication

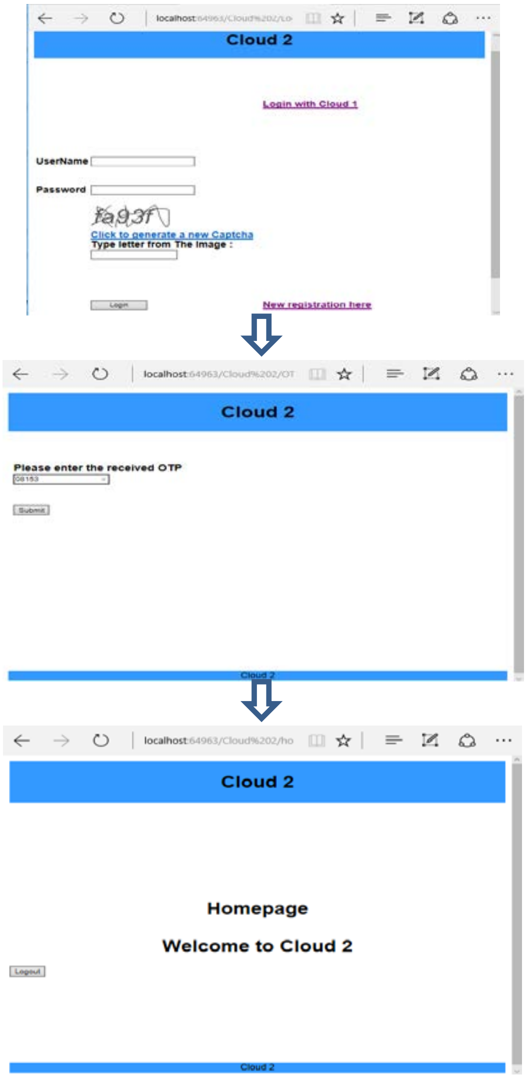

localhost:64963/Cloud%202/Lo
Cloud 2
Login with Cloud 1
UserName
Password
Click to generate a new Captcha
Type letter from The Image :
Login
New registration here
localhost:64963/Cloud%202/OT
Cloud 2
Please enter the received OTP
Submit
Cloud 2
localhost:64963/Cloud%202/ho
Cloud 2
Homepage
Welcome to Cloud 2
Logout
Cloud 2

Fig 9. Cloud 2 authentication

Acknowledgments

This research was supported by the National Center for Scientific and Technical Research of Morocco.

6. Conclusion

In the context of Cloud Federation, one of the main security issues is the identity management. Many cloud solutions deals with this concern, however, it does not meet security requirements.

In order to overcome the limitations of the current authentication solutions in the context of the Cloud federation, we have provided an authentication solution focusing our attention on the need of users to access resources easily and securely. The proposed Identity

Federation approach has been described, designed using SSO based OTP to enforce security and implemented using Asp.Net.

Thanks to our proposal, consumer can use services easily, without having to authenticate himself several times, and securely since an OTP cannot be reused.

References

[1] P. Arias-Cabarcos, F. Almenárez-Mendoza, A. Marín-López, D. Díaz-Sánchez, and R. Sánchez-Guerrero, “A Metric-Based Approach to Assess Risk for ‘On Cloud’ Federated Identity Management,” J. Netw. Syst. Manag., vol. 20, no. 4, pp. 513–533, Dec. 2012.

[2] T. Kurze, M. Klems, D. Bermbach, A. Lenk, S. Tai, and M. Kunze, “Cloud federation,” CLOUD Comput., vol. 2011, pp. 32–38, 2011.

[3] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “How to Enhance Cloud Architectures to Enable Cross-Federation,” 2010, pp. 337–345.

[4] Department of Computer Science and Engineering, National Institute of Technology Karnataka Surathkal, Karnataka, India-575025, M. V. Thomas, A. Dhole, and K. Chandrasekaran, “Single Sign-On in Cloud Federation using CloudSim,” Int. J. Comput. Netw. Inf. Secur., vol. 7, no. 6, pp. 50–58, May 2015.

[5] H. Medhioub, “Architectures et mécanismes de fédération dans les environnements cloud computing et cloud networking,” Evry, Institut national des télécommunications, 2015.

[6] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Security and Cloud Computing: InterCloud Identity Management Infrastructure,” 2010, pp. 263–265.

[7] N. Dewaele, "Single Sign On," Conservatoire national des arts et métiers, 2010.

[8] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Three-Phase Cross-Cloud Federation Model: The Cloud SSO Authentication,” 2010, pp. 94–101.

[9] A. L. Garcia, E. Fernandez-del-Castillo, and M. Puel, “Identity Federation with VOMS in Cloud Infrastructures,” 2013, pp. 42–48.

[10] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Federation establishment between clever clouds through a saml sso authentication profile,” Int. J. Adv. Internet Technol., vol. 4, no. 1, pp. 14–27, 2011.

[11] C. Ramos, T. Kim, R. S. Sudhakar, and K. K. Hari, “SSO Use Case in Cloud Computing for Securacy to Worldwide Users.”

[12] A. Pérez Méndez, R. Marín López, and G. López Millán, “Providing efficient SSO to cloud service access in AAA-based identity federations,” Future Gener. Comput. Syst., vol. 58, pp. 13–28, May 2016.

[13] C. Powell, T. Aizawa, and M. Munetomo, “Design of an SSO authentication infrastructure for heterogeneous inter-cloud environments,” in Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on, 2014, pp. 102–107.

[14] F. F. Moghaddam, S. G. Moghaddam, S. Rouzbeh, S. K. Araghi, N. M. Alibeigi, and S. D. Varnosfaderani, “A scalable and efficient user authentication scheme for cloud computing environments,” in Region 10 Symposium, 2014 IEEE, 2014, pp. 508–513.

[15] A. G. Revar and M. D. Bhavsar, “Securing user authentication using single sign-on in Cloud Computing,” in Engineering (NUiCONE), 2011 Nirma University International Conference on, 2011, pp. 1–4.

[16] M. Stihler, A. O. Santin, A. L. Marcon Jr, and J. da Silva Fraga, “Integral federated identity management for cloud computing,” in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, 2012, pp. 1–5.

[17] M. Noureddine and R. Bashroush, “An authentication model towards cloud federation in the enterprise,” J. Syst. Softw., vol. 86, no. 9, pp. 2269–2275, Sep. 2013.

[18] R. Sánchez, F. Almenares, P. Arias, D. Díaz-Sánchez, and A. Marín, “Enhancing privacy and dynamic federation in IdM for consumer cloud computing,” IEEE Trans. Consum. Electron., vol. 58, no. 1, 2012.

Belbergui Chaimaa was born in Morocco in 1991. She obtained her Masters in networks and systems from “Sciences and technologies Faculty of Settat ” in 2013. She is currently studying for a doctorate at Chouaib Doukkali University in Morocco. Her field of interest is Modeling and assessment of the security of a companies’ information systems.

Najib Elkamoun received his Ph.D. degree in Optical and Microwave Communication from the National Polytechnic Institute of Grenoble, France, in 1990. He is currently Professor Researcher at Faculty of Science, University Chouaib Doukkali, El Jadida, Morocco. With over 20 years of expertise in information technology and communication, he has conducted several thesis and overseas missions in e-learning and telecommunication networks. His research interests include High Speed Network Architectures (MPLS), Mobility Management, security and QoS in Emerging Networks (MANET, VANET and WSN), Wireless Communications and Traffic Engineering for Computer and Telecommunication Networks.

Rachid Hilal was born in Rabat, Morocco, in 1965. He received the Ph.D degree in telecommunications from the University of Limoges, France, in 1996. Since 2003, he was the General Secretary of the Cadi Ayyad University Marrakech. Since 2012, he is a vice president of the Chouaïb Doukkali University El Jadida. He is member of the STIC Laboratory and hability professor. His research interests include distributed power amplifiers, microwave nonlinear circuit design, and inset-fed patch antenna