An Efficient Framework for Enhancing User Authentication in Cloud Storage Using Digital Watermark

Article · February 2015

DOI: 10.15866/irecos.v10i2.5236

3 authors, including:

Abderrahim Abdellaoui
Université Ibn Tofail
9 PUBLICATIONS **51** CITATIONS
SEE PROFILE

Youness Idrissi Khamlichi
Sidi Mohamed Ben Abdellah University, National School of Applied Sciences, Fez, …
35 PUBLICATIONS **127** CITATIONS
SEE PROFILE

International Review on Computers and Software (I.RE.CO.S.), Vol. 10, N. 2
ISSN 1828-6003 February 2015

An Efficient Framework for Enhancing User Authentication in Cloud Storage Using Digital Watermark

Abderrahim Abdellaoui[1], Younes Idrissi Khamlichi[2], Habiba Chaoui[3]

Abstract – *Security issues in cloud computing is one of the major reasons in slowing down its adoption by businesses and among these issues: weak user authentication. In fact, the use of text password is still relatively widespread, especially, for authentication in a cloud environment. Therefore, numerous approaches have been proposed to overcome this problem such as graphical passwords, biometric scans and 3D password objects. In this paper, we propose a cloud-based two-factor authentication framework called Two Levels Authentication Cloud (2LAC). The framework uses an image and a secret watermark as factors of authentication. Experimental results illustrate that 2LAC offers an efficient mechanism for enhancing user authentication in the cloud environment and can eliminate common types of attacks.*

Keywords: *Cloud Computing, Security, Watermark, Multi-Factor Authentication, Steganography*

Nomenclature

U	Identity user
Un_i	Username
Ps_i	User's Password
S	Cloud Server
$U \triangleright S[M]$	Message M is sent from U to S
$U \triangleleft S[M]$	Message M is sent from S to U
$\psi(\cdot)$	Hash function
Γ	Image
ω	Secret watermark / random number
Γ_ω	Watermarked image
$\xi^k(\cdot)$	Symmetric key encryption (AES encryption) and k is the secret key
C_r	Credentials
φ	First factor
ϕ	Second factor
Te	Time of embedding
Tex	Time of extraction and compare (s)
$Tauth$	Time of authentication (full process) (s)

I. Introduction

Cloud computing is one of the most popular technologies of the last decade. It's the latest technology of computing models after distributed and Grid computing.

It considered as a highly scalable platform in which computing resources are offered as a service leveraging virtualization and internet technologies [1].

It makes the work more flexible and therefore more effective.

Certainly, it has been recently more spotlighted than any other computing services, due to its capacity in providing an unlimited amount of resources and great flexibility to users [2], where they can process, store and access to their data in the cloud server anytime, anywhere using internet. Also, it provides easy maintenance, reduced costs, better performance and reliability.

However, this new paradigm of computing introduces new security challenges, especially, for businesses, industries and governments, since the data is outsourced therefore it is out of controls and can be easily threatened by attackers. While a variety of definitions of cloud computing have been suggested, this paper uses the NIST Cloud Computing definition (NIST SP 800-145) embraced by many researchers reads as follows: A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [3]."

Cloud computing offers services that can be grouped into three layers: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IAAS):

Infrastructure as a Service (IAAS) refers to an on-demand infrastructure that can host and run applications, services or store data. It provides computing resources such as CPUs, networks, storage, bandwidth, hardware load, and others as a service instead of buying and managing hardware [4], [5]. Specifically, IAAS is characterized by a physical infrastructure often made available by a service provider. Amazon EC2, GoGrid, Flexiscale and Openstack are examples of IAAS service providers.

Platform as a service (PAAS) is an outsourced platform implementation, deployment and development application. It provides a set of solution which aims to support the setting up and the delivery of applications in the cloud without the need of buying and managing the underlying hardware and software layers [6], [7]. Google App Engine and Force.com are examples of PAAS.

Software as a service (SAAS) refers to on-demand software that run on the Cloud and that is offered in a pay-per-use manner, such as Salesforce.com, Rackspace and SAP Business ByDesign [8], [9].

Since its introduction, the market of cloud computing has seen a phenomenal growth all over the world. More and more businesses are adopting it. Gartner's PaaS Road Map report illustrates this point clearly and has shown that 50% of independent software vendor will be SaaS providers by 2015. Thus cloud-based solutions will increase faster compared to on-premises solutions which would incite most companies to switch to cloud computing infrastructure [10]. Along with this growth, however, there are increasing concerns over security in this environment, since its security from a business viewpoint is still unclear.

Furthermore, existing security mechanisms still have some flaws. Hackers and attackers can exploit these flaws in order to gain unauthorized access to servers and therefore get some secret and sensitive information from the cloud. Weak user authentication is a good illustration of these flaws. It was recently shown that the combination "username / password" is no longer sufficient to ensure a fully secure access to the cloud servers, due to different kinds of attacks [11]-[15]. For instance, network eavesdropping, brute force and dictionary attacks, and what makes things worse is that the use of text password is still relatively widespread, mostly for authentication in the cloud. In this context, it is necessary to well strengthen the process of authentication.

Additionally, data confidentiality is another important example of cloud security issues. Indeed, users may not fully trust the cloud provider and worry that the data stored in the cloud could be modified, corrupted or even removed. In order to overcome these security issues, significant researches have been carried out in order to ensure a satisfactory level of security and to establish trust in the services offered by cloud.

In this regard, the aim of this paper is to enhance authentication in a cloud environment and develop secure solutions to ensure security of cloud user access and of course data storage. In order to better describe our work, we organize this paper as follows: section I gives an overview of the fundamental concepts and issues of cloud computing.

Section II deals with related work. In section III we explain in detail a conceptual and theoretical authentication framework called 2LAC. Then, section IV is dedicated to the implementation of the proposed two-level authentication framework. Finally, we conclude this paper and present some future works.

II. Related Work

In order to overcome the problem of the username / password scheme, a considerable amount of literature has been published in terms of enhancing authentication such as third-party authentication, graphical passwords, biometric scans, and 3D password objects [16], [17].

This section describes previous works in this field. The scheme suggested by [18] in which the server stores the hashed value of user's passwords and a password table was used to verify the user authentication.

However, the most serious disadvantage of this method is that the system could be completely compromised if the password table is compromised. The authors of [19] proposed authentication scheme based on digital objects. They use hash values of digital objects to generate stronger strings and use them as passwords which particularly named as object based passwords. [20] had presented the challenges concerning security of cloud computing and most notably efficient handling of the IAM (Identity and Access Management) using protocols.

However, they had been mostly restricted to identity and access management and they have not treated access control in much detail. In [12] a strong user authentication framework for cloud computing is used, the idea is to verify the user legitimacy by using a smart card and an extra OOB (out of band) factor [11] proposes two-factor authentication scheme based on Schnorr digital signature and feature extraction from a fingerprint. On the other hand, [21] develop another solution based on two levels of authentication called the Cloud Cognitive Authenticator (CCA).

It is an API, integrating biosignals, one round Zero Knowledge Protocol (ZKP) for authentication. It uses Electro Dermal Responses (EDR) for the first level authentication. The major limitation of this scheme is the requirement of extra device and software. CCA uses data captured from an EDR biometric scanner when the users request to establish connection with the hypervisor to access the cloud services ([29]). [22] seeks to solve a weak authentication problem by an implementation of a multi-factor authentication method in the cloud environment which authenticates the customer in multiple levels. However, this system has a number of drawbacks. For examples, the administrator has full control over the data that is stored in the cloud and this raises some security issues like insider attacks. So far we have focused on research related to user authentication in the cloud environment and their limitations. The following section will discuss our proposal in terms of enhancing username/password scheme.

III. Proposed Work

We propose a new framework allowing strong authentication in a cloud environment based on an image and a secret watermark [30]. The main contributions of this paper are:

- ✓ An authentication framework which uses images and technique of steganography instead of text password.
- ✓ A framework allowing to secure user access.

III.1. Watermarking

Digital watermarking is a pattern of bits inserted into a digital image, audio or video file that specifies the file's copyright information such as author, rights and so on [23]. Watermarking is designed to be completely invisible.

There are several watermarking methods and techniques and among these methods LSB (Least significant bit). It's a simple and widely used method in the field of information security thanks to its high hiding capacity and quality [24]. It embeds a secret bit stream into the LSB plane of an image. We use the technique of LSB for the construction of our authentication framework.

III.2. Description of the Proposed Scheme

Our proposed scheme uses two factor authentication: the first factor φ : $\{Un_i, Ps_i\}$ is composed of username: Un_i and a password: Ps_i.

The second factor ϕ is composed of $\left\{\Gamma_{\zeta^k(\omega)}, \omega\right\}$, $\Gamma_{\zeta^k(\omega)}$: a watermarked image and a secret watermark ω.

Step 0 (Registration phase)

The user provides his/her username Un_i and password Ps_i, $U \triangleright S[Un_i, Ps_i]$ then the cloud provider S generates alphanumerical code ω, retrieve image Γ from database, embed the code in the image Γ_ω and send the code and the watermarked image to the client $U \triangleleft S\left[\Gamma^k{}_{(\omega)}, \omega\right]$.

The client and the server save (login, password, watermarked image, code) as credentials $C_r : \left\{Un_i, Ps_i, \Gamma_{\xi^k(\omega)}, \omega\right\}$ such as $\varphi : \{Un_i, Ps_i\}$ and $\phi : \left\{\Gamma_{\zeta^k(\omega)}, \omega\right\}$.

In this phase the clients and service provider are supposed to be honest. Fig. 1 Illustrate the registration phase.

Step 1

A user $Un_{i\in[1,\ldots,n]}$ must be authenticated for access to the cloud services. So he/she must provide $\varphi_1 : \left\{Un_{i_1}, Ps_{i_1}\right\}$ for access. The user sends, the username Un_i and password Ps_i to the cloud provider $U \triangleright S[Un_i, Ps_i]$, and then the cloud service provider checks the authenticity of the user ($\varphi \stackrel{?}{=} \varphi_1$). If the user is authorized, cloud server will provide a restricted access to the client information.

Step 2

If the first phase is successfully done, then the user can view its stored data. He/she has no right to upload or to download their data until the 3rd step.

Step 3

When the client wants to apply changes (upload or download or edit), he/she must provide the watermarked image $\Gamma_{\zeta^k(\omega_1)}$, and code ω_1 that were provided by the cloud server during the phase of registration (2 levels authentication). Then The client sends the combination ($\phi_1 : \left\{\Gamma_{\xi(\omega_1)}, \omega_1\right\}$) to the cloud server $U \triangleright S[\phi_1]$.

Step 4

The combination ϕ_1 will be verified by the CTL module. If $\phi \stackrel{?}{=} \phi_1$ is correct, CTL module will allow data access and grant privileges of editing, uploading and downloading, otherwise return to Step 2.

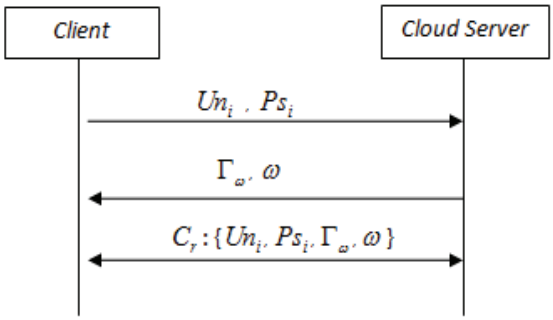

Fig. 1. Registration phase

Password change phase

In the proposed scheme, if a user $Un_{i\in[1,\ldots,n]}$ wants to change his/her code ω_i he/she performs the following steps:

Step 1: The user U inserts his/her username Un_i and password Ps_i.

Step 2: The cloud server checks whether the user is registered by verifying the first factor $\varphi : \{Un_i, Ps_i\}$, then the user Un_i request to change the code ω_i, so the cloud server requests the combination $\phi : \left\{\Gamma_{\zeta^k(\omega_i)}, \omega_i\right\}$ and a new code ϖ.

Step 3: The user sends his/her second factor ϕ to the cloud server and checks whether the information provided by the user is correct. If this is the case, then the cloud server register:

$\phi:\left\{\Gamma_{\zeta^k(\varpi)},\varpi\right\}$ instead of $\phi:\left\{\Gamma_{\zeta^k(\omega)},\omega\right\}$ in its database, and sends the new combination $\phi:\left\{\Gamma_{\zeta^k(\varpi)},\varpi\right\}$ to the user. Henceforth, this combination will be used for the second level authentication. This phase is illustrated schematically in Fig. 2.

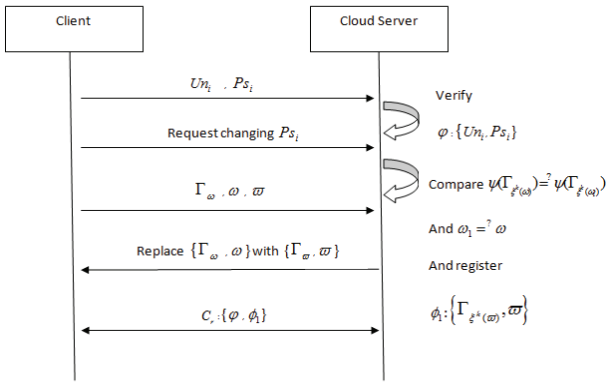

Fig. 2. Password change phase

III.2.1. Description of Controller(CTL) Module

The main functions of CTL module are twofold: verify user access (step 1,2) and construct the watermarked image $\Gamma_{\xi^k(\omega_i)}$ (step 0) for this reason this module includes the following tasks:

- ✓ It extracts ω_i from $\Gamma_{\xi^k(\omega_i)}$ using extraction algorithm mentioned below and advanced encryption standard (AES) to decrypt $\xi^k(\omega_i)$.
- ✓ It checks if the code ω_i embedded in the image $\Gamma_{\xi^k(\omega_i)}$ provided by the user Un_{i_1}, and the code ω_i' embedded in the image $\Gamma_{\xi^k(\omega_i')}$ stored in the database are equal ($\omega_i =^? \omega'_i$).
- ✓ It checks if the hash of the image $\psi\left(\Gamma_{\xi(\omega_i)}\right)$ provided by the user Un_{i_1}, and the hash of the image stored in the database $\psi\left(\Gamma_{\xi^k(\omega_i')}\right)$ are equal $\psi\left(\Gamma_{\xi^k(\omega_i')}\right)=^? \psi\left(\Gamma_{\xi^k(\omega_i)}\right)$.

III.2.2. Construction of the Watermarked Image

The server retrieves the image Γ from the database and CTL module generates a random alphanumeric code ω (8 characters), encrypt the code ω_i using advanced encryption standard (AES) $\xi^k(\omega_i)$, convert it to binary values and after that it will be embedded in the image $\Gamma_{\xi^k(\omega)}$.

Then, watermarked image will be produced and it will be sent to the client side $U \lhd S\left[\Gamma_{\xi^k(\omega_i)},\omega_i\right]$.

Embedding algorithm

Input:
Image: Γ *, Watermark text :* ω *;*
Output:
Watermarked Image: $\Gamma_{\xi^k(\omega)}$*;*

Begin:
Step1- *Retrieve Image* Γ *from the database* and *generate a code* ω *(8 characters);*
Step2- *Encrypt the watermark text* ω *using AES encryption* $\xi^k(\omega_i)$;
Step3- *Convert the encrypted watermark text from characters to bit;.*
Step4- *Inverse the watermark bit;*
Step5- *Embed the encrypted watermark in the LSB plane of the image* $\Gamma_{\xi^k(\omega)}$*;*
Step6- *Send the Image* $\Gamma_{\xi^k(\omega)}$ *as png to the client side* $U \lhd S\left[\Gamma_{\xi^k(\omega)},\omega\right]$
End

After receiving the watermarked image $\Gamma_{\xi^k(\omega)}$, the server will extract the watermark bits from the image, inverse the bits, convert the encrypted watermark from bits to text $\xi^k(\omega)$, decrypt the code using AES decryption $\xi^k\left(\xi^k(\omega)\right)=\omega$.

Extracting Algorithm

Input:
Watermarked Image: $\Gamma_{\xi^k(\omega)}$.
Output:
Watermark text: ω_1 .
Begin:
Step1 - *Receive the Image from* Un_{i_1} *:* $U \rhd S\left[\Gamma_{\zeta^k(\omega)}\right]$ *and retrieve the encrypted watermark*;
Step2 *- Inverse the watermark bit;*
Step3 *- Convert the encrypted watermark code from bits to characters* $\xi^k(\omega_1)$.
Step4 *- Decrypted watermark code using AES decryption* $\xi^k\left(\xi^k(\omega_1)\right)$;
Step5 *- Save the decrypted code in array* ω_1;
End

III.2.3. Description of Crypto Module

The Advance Encryption Standard (AES) algorithm is the primary tool of this module.

It is a symmetric key algorithm which is responsible for the confidentiality of data in our framework. Crypto module encrypt/decrypt file, image using AES encryption before sending/receiving to/from the cloud provider. We have opted for the AES algorithm for several reasons, including: Simplicity, low memory and resource requirements, ease of computing and implementation flexibility [25]. In other words, this algorithm combines security, efficiency and ease of implementation.

IV. Implementation

We have used more than 1000 clients to prove the efficiency of the proposed scheme. We have tried to find out different execution results which helped us to demonstrate our model with better result.

IV.1. Lab Setup

- Platform : Vsphere v5 (2Gb RAM)
- Client 1 : Ubuntu 12.04 (2Gb RAM),
- Client 2 : Windows 7 (2Gb RAM),
- Processor : Core i7
- ORACLE database
- Java(TM) SE Runtime Environment

In this environment, the embedding and transfer of the watermark to the client took an average of 3 seconds for executing all the steps. This model is fast enough and can be applied to the cloud computing environments. The authentication time varies from image to image.

As shown in Table I, we present the numeric simulation results of 2LAC applied for 1000 images

TABLE I
EMBEDDING AND RETRIEVING TIME OF VARIOUS IMAGE

Image size AND Dimension	TE	TEX	TAUTH
62 KO/ 271X186	0.0082 S	3.28 S	4S
2.24KO/ 225X225	0.0067 S	2.56 S	3S
11KO/ 271X186	0.0063 S	2.79 S	3S
1.87 KO/ 102X102	0.0046 S	1.74 S	2S
1.01KO/ 48X48	0.0043 S	1.63 S	2S
4.33KO / 255X255	0.0053 S	2.83 S	3S
5.41KO/ 276X183	0.0059 S	2.82 S	3S

Key Logging: One of the most common ways to steal passwords is by using a malicious key logging tool during the phase of authentication. Our proposed method is not only based on text password only, but we use authentication image $\Gamma_{\zeta^k(\omega_i)}$. Thus, even if a hacker gain information of Un_i and Ps_i, he can't get the authentication image $\Gamma_{\zeta^k(\omega_i)}$. In other words, it's obviously clear that the logging attack is eliminated.

Man-In-The-Middle (MITM): 2LAC can overcome (MITM) attacks using a VPN tunnel to secure communication between the client side and the server side. Additionally, the factor ω_i is securely encrypted in the authentication image $\Gamma_{\zeta^k(\omega_i)}$.

Dictionary and brute force attacks: 2LAC is not only based on alphanumeric strings, the user must own the authentication image $\Gamma_{\zeta^k(\omega_i)}$ in order to be authenticated.

In other words, these attacks are fully eliminated.

Online and off-line guessing attacks: an online attack is where a hacker tries to log on in a system pretending to be the legitimate user by guessing the user's password.

On the other hand, the off-line attack is where an attacker steals the encrypted password from the server, then decrypts this password. In our case, we use in addition to the text password, we use an authentication image. 2lac overcame this attack using a combination of the authentication image $\Gamma_{\zeta^k(\omega_i)}$ and the code instead of text password. 2LAC is an alternative form of user authentication that is intended to be difficult for an attacker if he doesn't own the authentication image.

Password change: Our framework provides the password change ability for users. Thus, whenever they forget the code or they get hacked, this ability is used to get a new password and a new authentication image $\phi:\left\{\Gamma_{\zeta^k(\varpi)},\varpi\right\}$ instead of $\phi:\left\{\Gamma_{\zeta^k(\omega_i)},\omega_i\right\}$.

Security of the password: the cloud server does not contain a file password. ω_i is encrypted and embedded in $\Gamma_{\zeta^k(\omega_i)}$. Our proposed scheme can supply security of the password.

TABLE II
COMPARISON BETWEEN EXISTING CLOUD AUTHENTICATION AND 2LAC

	A1	A2	A3	A4	A5	B1	B2	B3
2LAC	*o*	*o*	*o*	*o*	*o*	*N*	*Easy*	*Y*
Yassin[11]	-	-	*o*	*o*	*o*	*Y*	*Medium*	*Y*
Jivanadham[21]	-	-	*o*	*o*	*x*	*N*	*Hard*	*N*
Sumathi[22]	-	-	*x*	*o*	*o*	*N*	*Medium*	*Y*
Lamport[18]	*x*	*x*	*x*	*x*	*x*	*N*	*Easy*	*N*
Gurav [26]	-	-	-	*o*	*x*	*N*	*Easy*	*N*
Mannan[19]	*o*	*o*	-	*o*	*x*	*N*	*Easy*	*N*
Cheng[27]	-	-	*o*	*o*	*x*	*Y*	*Medium*	*N*
Soyjaudah[28]	-	-	-	*o*	*x*	*Y*	*Medium*	*N*
Gunawardena[13]	*o*	*o*	*o*	*o*	*x*	-	*Easy*	*N*
Banyal[15]	*o*	*o*	*o*	*x*	*x*	-	*Medium*	*Y*
Choudhury[12]	*o*	*o*	*o*	*o*	*x*	*Y*	*Medium*	*N*

o:Attack is eliminated; **x** :Partially or weak elimination of the attack; **A1**:Dictionary attacks; **A2**:Brute force attacks; **A3**:MITM; **A4**:key logging; **A5**: insider attack; **B1**:Extra device; **B2**:Ease of use; **B3**:Multifactor authentication, **Y**:Yes **N**:No

Stolen authentication image: In our proposed scheme, all authentication factors are not available simultaneously. Thus, even if $\Gamma_{\zeta^k(\omega_i)}$ is stolen or lost, authentication needs the φ_i, and ω_i. Additionally the framework provides the password change ability, and in

case of a theft, the user can change φ_i and ϕ. It is helpful at this point to provide a comparison between 2LAC and some existing cloud authentication. The Table II below summarizes briefly this comparison.

Security of the stored data: 2LAC uses the CryptoModule to encrypt data using (AES encryption) before sending it to the provider side.

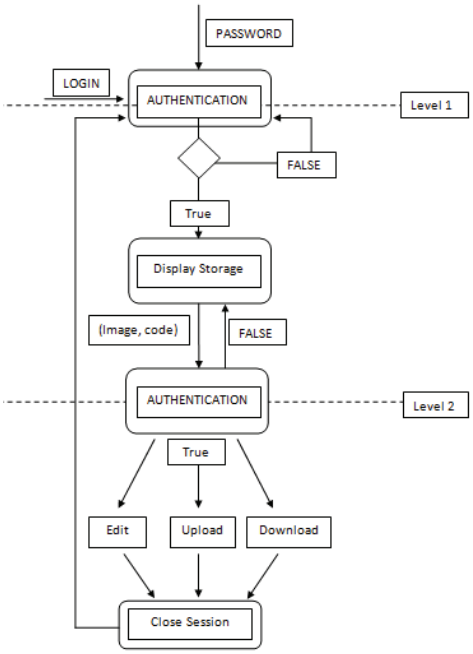

Fig. 3. Two Levels Authentication in the cloud (2LAC)

V. Conclusion

The main goal is to secure the cloud server access. To meet this need, we exploit the framework of 2LAC to protect data access in cloud.

This method increases security since it requires an additional authentication level. It also complicates the task of potential attackers who successfully obtain the information of a user and seek to impersonate authorized users. We assume that this way of accessing and storing data is more secure and has a high performance.

VI. Future Work

Additionally, we expect applying the results obtained in this work in other areas and extended it to strengthen confidentiality and integrity.

In our future research, we focus on conducting more experiments in cloud computing security and test the performance of our approach which may provide a reference solution for cloud security.

References

[1] Govinda K. , Sathiyamoorthy E.: Agent Based Security for Cloud Computing using Obfuscation, *Procedia Engineering*, Volume 38, pp. 125-129, (2012). doi: 10.1016/j.proeng.2012.06.018

[2] Zhidong Shen , Li Li , Fei Yan , Xiaoping Wu: Cloud Computing System Based on Trusted Computing Platform , (ICICTA), *International Conference on Intelligent Computation Technology and Automation*, pp.942-945. IEEE(2010). doi: 10.1109/ICICTA.2010.724

[3] National Institute of Standards and Technology : The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800145.pdf, September (2011)

[4] Patidar, S., Rane, D., Jain, P.: A survey paper on cloud computing. In: *2nd International Conference on Advanced Computing Communication Technologies*, pp. 394–398. IEEE (2012). doi:10.1109/ACCT.2012.15

[5] Kulkarni, G. ; Gambhir, J. ; Patil, T. ; Dongare, A.: A SecurityAspects in Cloud Computing, *3rd International Conference on Software Engineering and Service Science*(ICSESS),vol. 1, pp.547-550.IEEE(2012). doi:10.1109/ICSESS.2012.6269525

[6] Subashini, S., Kavitha, V.: A survey on security issues in service Delivery models of cloud computing. *J. Netw.Comput.Appli.* 34(1),1–11 (2011). doi:10.1016/j.jnca.2010.07.006

[7] Patidar, S., Rane, D., Jain, P.: A survey paper on cloud computing, *2nd International Conference on Advanced Computing Communication Technologies*, pp. 394–398. IEEE(2012).doi:10.1109/ACCT.2012.15

[8] Geong Sen Poh, Mohd Amril Nurman Mohd Nazir, Bok-Min: An Authentication Framework for Peer-to-Peer Cloud *„SIN '13 Proceedings of the 6th International Conference on Security of Information and Networks* , ACM New York 2013, pp.94 -101, doi:10.1145/2523514.2523531

[9] Lenk, A., Klems, M., Nimis, J., Tai, S., Sandholm, T: What's inside the cloud? An architectural map of the cloud landscape. In*: Proceedings of the ICSE Workshop on Software Engineering Challenges of Cloud Computing*, pp. 23–31. IEEE Computer Society, Washington, DC, USA (2009). doi:10.1109/CLOUD.2009.5071529

[10] Natis Y. V., Lheureux B. J. , Pezzini M., Cearley D. W., Knipp E., Plummer D. C.: PaaS Road Map: A Continent Emerging, Gartner, Tech. Rep., January 2011, http://www.gartner.com/id=1521622.

[11] Yassin, A.A. ; Hai Jin ; Ibrahim, A. ; Deqing Zou : Anonymous Password Authentication Scheme by Using Digital Signature and fingerprint in Cloud Computing, Second *International Conference on cloud and Green Computing*, pp. 282-289, IEEE(2012) doi:10.1109/CGC.2012.91

[12] Choudhury, A.J., Kumar P., Sain M., Hyotaek Lim , Hoon Jae-Lee: A Strong User Authentication Framework for Cloud Computing, Services Computing Conference (APSCC), *2011 IEEE Asia-Pacific*, pp.110-115. doi:10.1109/APSCC.2011.14.

[13] Gunawardena, S. , Kulkarni, D. , Gnanasekaraiyer, B.: Steganography based Framework to Prevent active attacks during user authentication , *The 8th International Conference on Computer Science and Education* (ICCSE 2013) April 26-28, IEEE (2013), doi:10.1109/ICCSE.2013.6553942

[14] Gonzalez, N., Miers, C., Redigolo, F., Carvalho, T., Simplicio, M.,Naslund, M., Pourzan di,M.:A quantitative analysis of current Security concerns and solutions for cloud computing, *IEEE 3rd International Conference on Cloud Computing Technology and Science*, pp.231-238,IEEE(2011).doi:10.1109/CloudCom.2011.39

[15] Banyal R.K., Jain P. ; Jain V.K.n. : Multi-factor Authentication Framework for Cloud Computing , 2013 *Fifth International Conference on Computational Intelligence, Modelling and Simulation* (CIMSim),IEEE 2013, pp.105-110,(2013). doi:10.1109/CIMSim.2013.25

[16] Diogo A. B., Fernandes Liliana F. B., Soares João V., Gomes Mário M., Freire Pedro R., InácioSecurity M. : Issues in cloud environments: a survey, *International Journal of Information Security*,Vol.13, Springer, pp.113-170,(2014) doi: 10.1007/s10207-013-0208-7

[17] Nirmalrani, V., Sakthivel, P., Protection of resources using role based access control with multilevel authentication, (2014) *International Review on Computers and Software (IRECOS),* 9 (11), pp. 1867-1874.

doi: http://dx.doi.org/10.15866/irecos.v9i11.4050
[18] Lamport L., Password Authentication with Insecure Communication, *Communications of the ACM*, Vol. 24(11),pp. 770-772(1981), doi:10.1145/358790.358797
[19] Mannan M., van Oorschot P.:Digital objects as passwords. *3rd USENIX Workshop on Hot Topics in Security* (HotSec '08), San Jose, CA, US
[20] Almulla, S.A. , Chan Yeob Yeun: Cloud Computing security Management,*Second International Conference on Engineering Systems Management and Its Applications* (ICESMA), pp.1-7.IEEE(2010)
[21] Jivanadham, L.B. , Islam, A.K.M.M. , Katayama, Y. , Komaki, S., Baharun, S., Cloud Cognitive Authenticator (CCA) A Public Cloud Computing Authentication Mechanism, *2013 International Conference On Informatics, Electronics and Vision* (ICIEV), pp.1-6.IEEE(2013)doi:10.1109/ICIEV.2013.6572626
[22] M. Sumathi, Implementation of Multifactor Authentication System accessing cloud service, *International Journal of Scientific And Research Publications*, Volume 3, Issue 6, June 2013
[23] Bamatraf A., Rosziati Ibrahim, Mohd Salleh, Mohd Najib: A new Digital watermarking algorithm using combination of least significant bit and Inverse Bit, *Journal of Computing*, Vol 3, Issue 4, April,2011,pp.1-8
[24] Lou D.C., Hu C.H.:LSB steganographic method based on Reversible histogram transformation function for resisting statistical Steganalysis, Elsevier Science Inc. New York, NY, USA, Vol. 188, pp.346-358. doi:10.1016/j.ins.2011.06.003
[25] Jivanadham L.B. , Construction and Maintenance of a Secured Dynamic Cluster- Based Wireless Sensor", MJIIT-JUCJoint Symposium (MJJS 2012), November 2012, Kuala Lumpur, Malaysia.
[26] Gurav, S.M. , Gawade, L.S. , Rane, P.K., Khochare, N.R., Graphical Password Authentication Cloud securing scheme, *IEEE International Conference on Electronic Systems, Signal Processing and Computing Technologies*(ICESC),IEEE 2014,pp. 479-483,(2014). doi: 10.1109/ICESC.2014.90.
[27] Cheng Guo, Chin-Chen Chang, Chaotic maps-based password authenticated key agreement using smart cards , *Commun NonlinearSci Numer Simulat,ELSEVIER*,Vol. 18, Issue 6 ,2013,pp.1433-1440,(2013). doi: 10.1016/j.cnsns.2012.09.032.
[28] Soyjaudah, K.M.S. , Ramsawock, G. , Khodabacchus, M.Y.:Cloud Computing Authentication using Cancellable Biometrics, *AFRICON 2013,* IEEE 2013, pp.1-4.(2013). doi: 10.1109/AFRCON.2013.6757821.
[29] Ram Mohan, N.R., Baburaj, E., Genetic clustering with workload multi-task scheduler in cloud environment, (2014) *International Journal on Communications Antenna and Propagation (IRECAP),* 4 (3), pp. 77-86.
[30] Sabri, A., Karoud, M., Tairi, H., Aarab, A., A robust image watermarking based on the empirical mode decomposition, (2009) *International Review on Computers and Software (IRECOS),* 4 (3), pp. 360-365.

Authors' information

[1,3]Systems Engineering Laboratory, Data Analysis and Security Team, National School of Applied Sciences, Campus Universitaire, B.P 241, 14000, Ibn Tofail University, Kénitra, Morocco.
E-mails: abderrahim90@gmail.com
mejhed90@gmail.com

[2]IR2M laboratory, UH1 University, National School of Applied Sciences, khouribga, Morocco.
E-mail: ykhamlichi@gmail.com

A. Abdellaoui is a Phd student at the National School of Applied Sciences - Kénitra, Ibn tofail University (UIT), Morocco. He holds a Master's degree in Networks and Systems from faculty of Sciences (UIT) University. His current research interest includes Networks and Systems, security of Cloud and mobile cloud computing.

Y. Idrissi Khamlichi is professor of higher education at National School of Applied Sciences - Khouribga, Hassan 1st University, Morocco. Member of Laboratory of Computer, Networks, Mobility and Modeling. His current research interests include Security of Cloud Computing, Big Data, Mobile Agent and Internet of things.

H. Chaoui is Professor of Computer Engineering at Ibn Tofail University – National High School of Applied Science (ENSA), Kenita - Morocco. Coordinator of "Information Systems Security" Master – ENSA, Kenitra-Morocco. Researcher at the Systems Engineering Laboratory. Her current research interest includes Cloud Computing Security, Evaluation of IDS using Mobile Agents and Data mining algorithms, Big Data and Data mining technology: Analysis, Security and Privacy.