INT J COMPUT COMMUN, ISSN 1841-9836
8(2):263-274, April, 2013.

An Hybrid Text-Image Based Authentication for Cloud Services

D.E. Popescu, A.M. Lonea

Daniela Elena Popescu, Alina Madalina Lonea
Faculty of Electrical Engineering and Information Technology, University of Oradea
Romania, 410087 Oradea, 1, Armatei Romane Str.
E-mail: depopescu@uoradea.ro, madalina_lonea@yahoo.com

Abstract:
The problem of securing access to the online information is acute today when access to bank accounts, health records, intellectual property and business or politically sensitive information are made by only a few clicks, regardless of geographic location. At the same time, more and more of these accesses are made from handsets. Cloud Computing is eminently suitable for addressing problems related to limited client resources, as it offloads computation from clients and offers dynamic provisioning of compute resources. Authentication of the companys users to the cloud service is mandatory because in this way it is eliminated the attacks risks to enter into the Cloud services. A suitable authentication is required for organizations that want to access the Cloud services. Our solution regards increasing security at the Security Access Point level of Cloud Computing and it is in fact a strong hybrid user authentication solution based on using image combined with text in order to avoid the weakness of simple user and password solution for authentication. A two factor password image based authentication method is proposed in this paper for cloud services. This authentication approach is used without additional hardware involved and presents the advantages of utilization in terms of security and usability. Every time when the user will be asked to provide his/her identity, a form for each image included in the photo will be listed. The user will have to remember the secret code for each image and to carefully introduce them in the forms. The global cloud access solution will be based on our hybrid proposed text-image based solution, and will be completed by the X.509 certificates.

Keywords: authentication, multi factor password authentification, strong authentification, image based, cloud services, IaaS, PaaS, SaaS.

1 Introduction

As Cloud Computing (CC) model seems to be the best solution for solving the online access to services that became ubiquitous, authentication is becoming a focal point for security professionals [1]. The problem of securing access to the online information is acute today when access to bank accounts, health records, intellectual property and business or politically sensitive information are made by only a few clicks, regardless of geographic location. At the same time, more and more of these accesses are made from handsets. This introduces security vulnerabilities and complications, because handsets have computational, and power limitations compared with traditional computers and they are constrained in terms of text input being more prone to theft than traditional computers. It is also important to point out that mobile devices input constraints make difficult for users to input complex passwords. Cloud Computing is eminently suitable for addressing problems related to limited client resources, as it offloads computation from clients and offers dynamic provisioning of compute resources. So, CC emerges as a new computing paradigm which aims to provide on-demand scalable services over the Internet via Cloud vendors to multi-tenant organizations. Enterprises are interested to move their on-premises infrastructure into cloud computing. However they are still concerned about the security risks implied by the act of embedding their resources within the cloud computing environment.

Authentication of the companys users to the cloud service is mandatory because in this way it is eliminated the attacks risks to enter into the Cloud services. A suitable authentication is required for organizations that want to access the Cloud services. Therefore, credential management, strong authentication, delegated authentication are leveraged across the cloud delivery models. Implementing authentication is very important, but organizations should be carefully at the attack implications. Attacks (like: impersonation, phishing, brute force dictionary based password) could occur on the credential details. Thus, authentication must be secured using the best techniques. Decreasing the risks in the cloud environment should be the priority for the Cloud providers and the organizations that adopt the cloud services. They also should select the appropriate solution in terms of cost [2].

CSA (2010) provides different recommendations for each type of the cloud services used. Thus:

- Software as a Service (SaaS) and Platform as a Service (PaaS) cloud environment provide several authentication options for their customers. In the case of enterprises, the Identity provider (IdP) authenticates users and a trust relationship should be realized between the organizations and the cloud services by federation. Besides the enterprises could exist individual users that will want to authenticate at the cloud services. They could do it using the user-centric authentication (like: Google, Yahoo ID, OpenID, Live ID etc.). Hence, those individual users will access multiple sites using a single set of credentials [2].

- Infrastructure as a Service (IaaS) cloud environment disposes by two categories of users: the enterprise IT personnel and the application users. The enterprise IT personnel are the ones that develop and manage applications in the IaaS cloud model. For this type of users the solution that is recommended is to use a dedicated VPN with the IaaS environment, in order to apply the existing enterprise authentication systems (e.g. Single Sign-On solution or LDAP-based authentication) into the Cloud environment. If the VPN tunnel is not realized for feasibility reason, then authentication assertions (SAML, WS-Federation) are applied together with standard web encryption (SSL), which will determine the expanding of the enterprises SSO capabilities to the Cloud service. Another solution that could be implemented in order to obtain the credentials authentication of users is to use the OpenID outside of the enterprise and to control the access of the users by specifying the appropriate privileges. Furthermore, also the OATH-compliant solution (Open Authentication) could be implemented in the Cloud systems for authenticating the users. These compliant solutions uses strong authentication [2].

Our solution regards increasing security at the Security Access Point level of CC and it is in fact a strong hybrid user authentication solution based on using image combined with text in order to avoid the weakness of simple user and password solution for authentication.

Beyond this introductory section, our paper contains other 5 sections. Section 2 points some background related with identity and access management in CC, section 3 emphasizes some background and related work concerning authentication based on image and text, section 4 presents our proposed solution and section 5 contains our concluding remarks.

2 Identity and Access Management in Cloud Computing

The General Cloud Computing Architecture is composed by a massive network of "cloud servers" [3] that uses virtualization to maximize the utilization of the computing power available/per server (Figure 1). According to Tianfield (2011) [4] the cloud architecture consists of

Cloud Platform Architecture (CPA) and Cloud Application Architecture (CAA). Clouds users interact with CPA and CAA using the Cloud Portal, which allows the user to select a service from a service catalogue. Further, the system management will find the correct resources that will be allocated in the cloud by the provisioning service. The optional monitoring and metering component tracks the usage of the cloud, so the resources used can be attributed to a certain user.

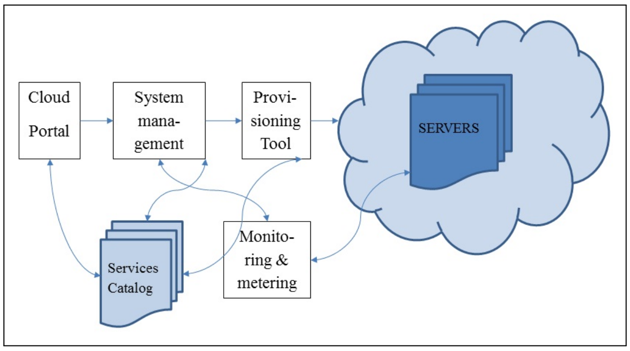


Figure 1: Cloud Computing Architecture [3]

CC offers a lot of advantages such as: it is an efficient way to store and maintain databases, being an helpful tool for business, the services offered by CC are in cloud as SaaS, cloud computing solutions are in general less expensive than their software counterparts (pricing being offered on a per-user basis), an efficient use of CC reduce energy consumption significantly, the costumers are freed of problems related to the technological issues of installing and maintaining the IT. In [3] are identified as threats in CC:

- Abusive and Flagrant Use of CC Solution: use of stringent registration and validation process, improving the monitoring and coordination throughput the CC, analysing the customer traffic, monitoring network blocks
- Serious breach in interface and API Solution: the use of security model analysis of cloud APIs, the implementation of a strong authentication and access controls and the evaluation of the API chain dependency
- Insider threats and attacks Solution: securing overall information, efficient compliance reporting, efficient breach notification processing

It is important to note that all the mitigation techniques proposed by [3] are related with the authentication process.

In conclusion, Cloud providers should have established a secure access and technical solutions for doing it, in order to ensure that the right people access the right services. The data that will be stored in the cloud could be accessed only by authorized users, which are specified by the provider. The solution is to integrate the data and services accesses in the Identity and Access Management (IAM) infrastructure, whose requirements are [2] [5]:

1. Identity provisioning/de-provisioning
2. Authentication
3. Identity Federation
4. Access Control

Authentication and authorization aspects of cloud computing are related with various forms of identity federation and claims-based authentication that facilitate transactions between cloud entities.

In CC the servers are not accessed direct through network connections, they are accessed by the services they provide, ensuring a high degree of transparency to the cloud. Users in fact access certain cloud components (request brokers) and those cloud components distribute requests to individual servers, as appropriate. This important functioning aspect of CC was use as a basis for the security components and architecture solution for CC Environments given in [6]. In order to preserve the transparency character for CC, security components and services must be transparent and also generic - adjustable to individual users, requirements, applications, and required services. Further, Figure 2 was introduced and discussed, with the purpose to emphasize the security components for CC environment. Because our paper is based on the authentication solution, our contribution will be on the Security Access Point (SAP) component. Hence, the security components of Figure 2 are:

- The Application Access Point (AAP) Server is the service that distributes - based on types of requests, or other parameters - cloud service requests to individual application servers. It is related and use the Services Publishing and Dispatching (SPD) Server. The SPD server is based on the UDDI standard for discovering application services available in the cloud and it is used for publishing and discovering of cloud applications services [6].

- The Communication Access Point (CAP) is in fact the communication services provider, which is able to accept requests coming through different communications protocols [6].

- The Security Access Point (SAP) is the cloud server that provides front-end security services and is responsible with the authentication of users. It must be based on open standards and applicable in an open environment [6].

- Certification Authority (CA) server provides certification services in the cloud by issuing certificate to the client and to the SAP [6].

- The Identity Management System (IDMS) X.500 compliant directory, is another server that provides registration and identification services in the cloud [6].

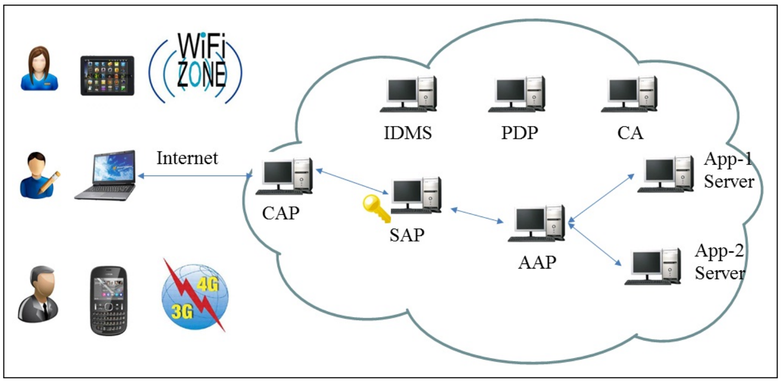


Figure 2: Security Components and Architecture for Cloud Computing Environments [6]

We have to point out that, in order to ensure the CC security, we can implement our proposed solution at the Client level, at the SAP level and at the AAP level, but this paper consider only the authentication at SAP level.

3 Background and Related Work

There are three main techniques for user authentication: *knowledge based techniques*, *token-based techniques* and *techniques based on biometrics.* The problem with the biometrics systems is the difficult trade-off between impostor pass rate and false alarm rate and the fact that they often require specialized devices unpleasant to use. They eliminate the limitations of the human brain [7] Recall problems are eliminated, and so are security problems concerning users writing down or choosing simple passwords. This eliminates nearly all of the problems with security.

Knowledge-based systems are the most frequently used for user authentication in our days. Most *token-based authentication systems* are also using knowledge based authentication to prevent impersonation through theft or loss of the token. But, the fundamental weakness of knowledge-based authentication schemes based on recall-based authentication, is the human limitation to remember secure text passwords.

Text-based authentication is vulnerable to more complex attacks, such as Brute force attacks and packet sniffing. With Brute force attacks, an intruder tries to guess the users password, or uses a password hash file. Alternatively, an intruder can use easily downloaded packet sniffing technologies such as Ethereal (Akula). Although a random, nonsensical password offers good security, the human brain finds them almost impossible to remember.

An alternative for these knowledge-based authentication systems is to orient to the *recognition-based systems* [8].

The passwords have evolved from a simple dictionary or personal piece of text, to a nonsense mixture of different types of characters. This new approach of text based passwords is in conflict with the human brains ability to remember strings. All studies made on human memory patterns show that the brain is more adept at remembering images.

In [9] is examined the requirements of a recognition-based authentication system and proposed Deja Vu, which authenticates a user through his ability to recognize previously seen images. The proposed authentication system is more reliable and easier to use than traditional recall-based schemes based on user passwords or PINs and it has the advantage that it prevents users from choosing weak passwords and makes difficult to write down and share passwords with others. This is demonstrated by Dhamija et al (2000) in their user study where 90% of all participants succeeded in the authentication tests using Deja Vu, and only 70% succeeded using passwords and PINs.

Another important study in this field was made by Jackson (2006) [10], where the author considered from the beginning that brute force attacks can still be a problem for an image-based system, and it is important to identify the right number of combinations available that does not compromise the system to this type of attack, and does not overload the user with images. Furthermore, Jackson (2006)also proposed a solution against shoulder surfing, which is a grid based image authentication system that randomize the position of different images each session (in situations where the intruder was not able to get a clear view of the image clicked, only an area view).

The prototype designed by Jackson (2006) was used to evaluate the possibility of image-based authentication (IBA) method to be the main security method. He made some experimental studies and found that images, faces and text mixed with images seemed to offer good results concerning human memory. Five experiments were made for testing security, usability, recall, methodology undertaken and whether user were able to remember passwords based on multiple image-based interfaces. The results of these experiments indicates that the recall levels over the three interfaces was about 90% and the best performers were obtained by the text mixed with images (story-based interface) and images (picture based-interface). The results experiments have been encouraging for IBA method; they showed that users were quite able to remember

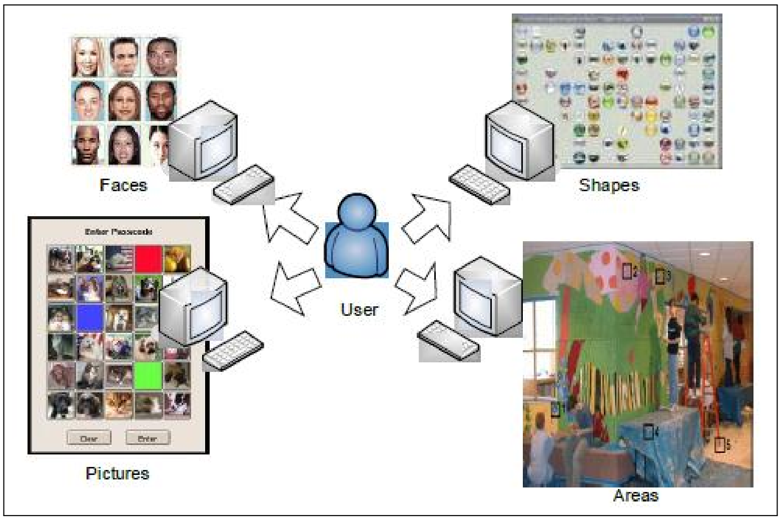
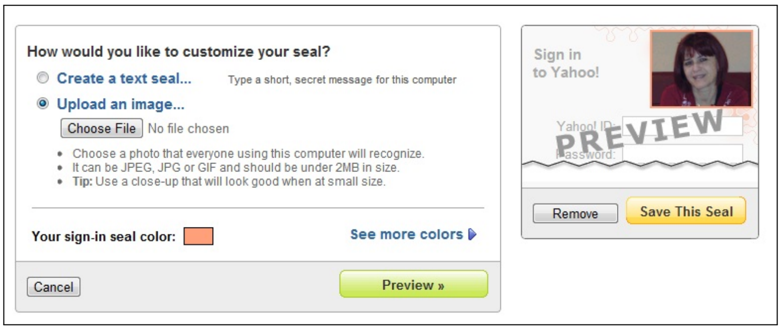


Figure 3: Different image-based interfaces on security systems [10]

passwords contained on different image-based interfaces, and the human brain is able to hold successfully passwords on three completely different interfaces. Furthermore, they demonstrated that the method of combining text with images is the most effective which is the basis for our approach, together with the idea of randomizing the images as solution against shoulder surfing.

Nitin et al.(2008), in [11] described the new facility for authentication added to JUIT-IBA system which is running within the Jaypee University and Information Technology (JUIT) and is globally accessible through the website: www.juit-iba.org. Being an IBA system, it is user-friendly and it uses Kerberos protocol in order to strengthen the security during authentication process. The Sign in seal advanced security feature was introduced to this system in order to make it more secure. A sign-in seal is a secret between the computer that is setting up and IBA. Your sign-in seal is saved to your computer and it is associated with your computer. if you log in from multiple computers, you will need to create a separate sign-in seal for each one. It is convenient to instantly recognize a genuine IBA sign-in page that ensure you that you are not on a page created by hackers attempting to steal your IBA ID and password The seal can be customized by creating a text seal or by uploading an image. From the security point of view it is important that even if the hacker knows or guesses the ID on your personal information, he cannot use it to discover your sign in seal.

Even Yahoo has implemented the sign in seal method, with a seal that can be a text or an uploaded image (Figure 4) and it must be used in combination with our proposed method in order to increase the security. This will be subject for our future work.


How would you like to customize your seal?

○ Create a text seal... Type a short, secret message for this computer

● Upload an image...

Choose File No file chosen

- Choose a photo that everyone using this computer will recognize.
- It can be JPEG, JPG or GIF and should be under 2MB in size.
- **Tip:** Use a close-up that will look good when at small size.

Your sign-in seal color: 🟧 See more colors ▶

Cancel Preview »

Sign in to Yahoo!

PREVIEW

Yahoo! ID:

Password:

Remove Save This Seal

Figure 4: Sign in seal at yahoo

Newman et al. (2005) presents and analyses in [12] a user authentication techniques using images that can be used in local or in remote authentication. The system consists of an authentication server (AS), and an authentication user agent (AUA) and it requires that the user have assigned a subset of images (as passwords) from a larger set. The set of all images used by IBA system, named image set, contains images that are distinctive to the human eye, they are not easily describable and they differ in structure. The AS has the authentication database of images and associations of users with their individual image sets. It is part of the trusted computing base, being never compromised. When the authentication is made remote, the channel is encrypted using Diffie-Hellman. For the attack scenarios, they considered four locations of vulnerabilities: information stored on the AS, information sent between AS and the AUA, the output of the AUA and the input of the AUA. For security analysis purposes, they considered the situations: keystroke logging: AUA Input, shoulder surfing: AUA output logging, TEMPEST Attack: AUA Output, Brute force attack, Frequency correlation attack: presentation sets, leaking image set size. For storing the individual image set for each individual user, only the indices into the image space will be stored. If the encryption is required, a good proposed solution is to send the images in clear over the channel with the permutation encrypted. The hidden permutation is applied by AUA to the images in order to display them, record the users selections and sent these back to the AS. Their study was important for our proposed solution and we apply our solution within the AS and AUA components, which are called in this paper as SAP (Security Access Point) authentication solution.

In the past few years, an important research was made regarding the usability and security of challenge questions, that are commonly used as a backup when users forgot their main" authentication secret. Most challenge questions rely on a user's knowledge of their early life, something static over time. This kind of information can be discovered by a determined attacker.

So, the standard mechanism based on textual questions can be replaced by the challenge protocol developed by Renaud et al (2010) in [14]; it uses a set of pictorial elements to prompt answers. The prompts solicit associative memories and serve as a stronger cue to aid the recall. All the pictures serve as an additional recall aid, while the use of an indirect question (the direct answer is not in a database or a public source) helps to reduce the exposure of the user to targeted observation attacks [15]. By using this more usable picture-based system it is maintained the same level of security as traditional questions as long as multiple questions are used in serial order.

Another approach for authentication was proposed by Micallef, et al. (2009) and uses an Authentication Avatar which represents the identity, including personality, of a fictional person that is generated almost randomly from a minimal user input [16]. An Avatar Profile (AP) contains information about the avatar, and a subset of the AP information is used by the user to respond to challenge questions regarding the avatar. In this way the security is improved since, unlike the users own information, the avatar information is not as easily determined by an attacker. Since such fiction information is likely to be more challenging for a user to recall (than their own, personal information), the proposed approach uses techniques such as repeated exposure to graphical imagery (related to the avatar) of users at every login in order to improve the memory association. Such images can be associated with the avatar itself, and also with elements of the AP (a picture of the Avatars pet). This recovering password solution was used as basis in our authentication solution, for increasing the security level in authentication.

The proposed solutions from [14] and [16] can be integrated into the global authentication process. Our proposed approach share with them the idea of combining text with images and the idea of using a randomize process in the authentication procedure.

Another work in context of IBA was realized by Confident Technologies. They provides image-based, multifactor authentication solutions for enterprise companies, websites, web and mobile applications, and mobile devices [13]. It encrypts one-time authentication codes within an image-based challenge, being easy to use and highly secure. Users simply identify which pictures match their previously-chosen, secret categories to authenticate. Image-based authentication solves the traditional trade-off between security and usability by providing strong authentication that is easy for people to use. As users simply tap a few pictures to authenticate, it is ideally suited for use on mobile devices.

Confident technology can be used as a standalone multifactor authentication solution, or as an additional layer of authentication.

4 The proposed authentication solution

The system consists of an authentication service server (AS), and an authentication user agent (AUA) and it requires that the user have assigned a subset of images (as passwords) from a larger set. The set of all images used by the Image Based Authentication (IBA) system, named image set, contains images that are distinctive to the human eye, they are not easily describable and they differ in structure. The AS has access to the authentication database of images and associations of users with their individual image sets. The current solution for authenticating in CC is given in Figure 5 and concerns the access of the user to the Security Access Point (SAP).

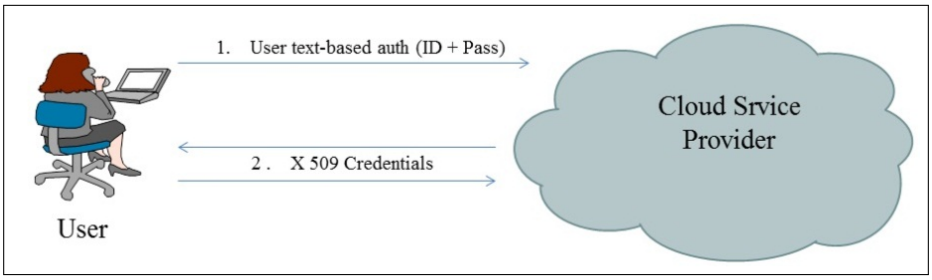


Figure 5: The current CC SAP authentification Solution

In order to perform stronger authentication for accessing the cloud services, we propose to use an authentication scheme (Figure 6) that perform the following steps:

1. Make a text-based authentication based on the user ID and a text password to have access to the cloud services

2. Make an hybrid text-image based authentication that uses our own proposed solution for authentication; it combines the images with text and is a good solution for avoiding the brute force attacks and to ensure a strong authentication scheme

3. Use the X.509 standards for obtaining the user credentials

Step 2 from the authentication scheme of Figure 6 suppose that when the user will register into the cloud service, he/she will receive a randomly grid of images. Each grid of images will contain 3 images and each image will have a corresponding number (e.g. 1, 2, 3) (Figure 7).

The user will have to provide a secret code for each image. In this sense, the user will receive a registration form, where it is asking to introduce secret characters for each corresponding number like in Figure 8.

Lets suppose that there were introduced the following codes like it is emplasized in Figure 8.

After the user introduced their specific secret code for each corresponding image, the registration will be realized. The user should remember which code he/she had provided for each

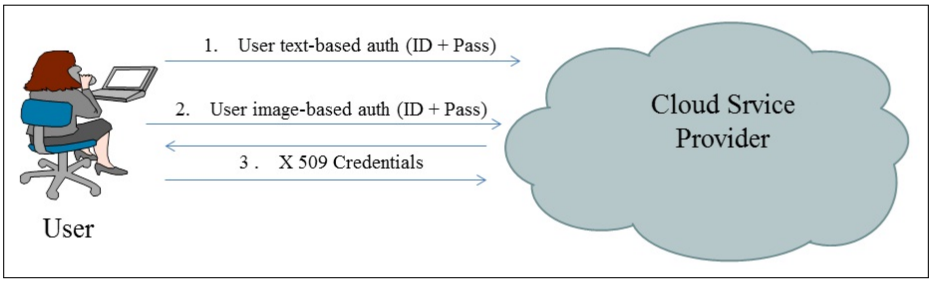

1. User text-based auth (ID + Pass)
2. User image-based auth (ID + Pass)
3 . X 509 Credentials
User
Cloud Srvice Provider

Figure 6: Our CC SAP authentification Solution

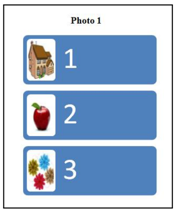
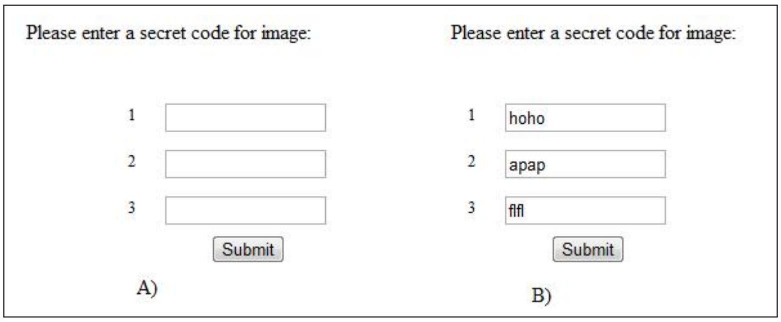


Figure 7: Grid of images


Please enter a secret code for image:

1
2
3

Submit

A)

Please enter a secret code for image:

1 hoho
2 apap
3 flfl

Submit

B)

Figure 8: The Registration Form

type of image (e.g. in the above example the user choose for the house image the hoho code, for the apple image the apap code and for the flower image the flfl code), because the proposed authentication method requires entering these codes, but each time the images will be associated with different numbers (from 1 to 3), because the numbers are generated using a permutation algorithm. Therefore, for authentication procedure there will be the same images each time, but with another corresponding numbers (Figure 9).

Our hybrid text-image solution can be applied not only for accessing the cloud, but also as a authentication method at cloud client level (especially for mobile clients) and also at the application level.

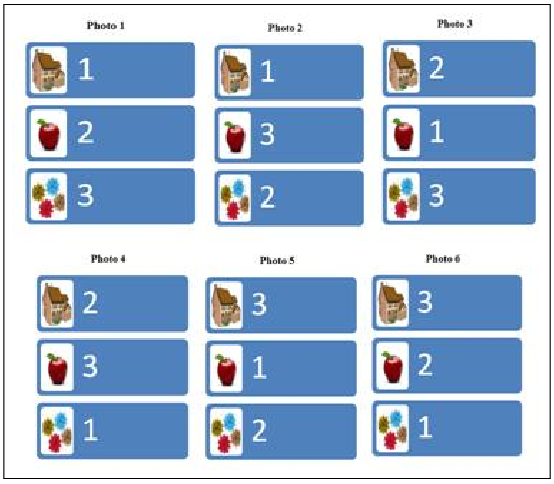


Figure 9: Relationship between the randomly grid of images and the secret code provided by user.

5 Conclusions and further work

A suitable authentication is required for organizations that want to access the Cloud services. Our solution regards increasing security at the Security Access Point level of Cloud Computing and it is in fact a strong hybrid user authentication solution based on using image combined with text in order to avoid the weakness of simple user and password solution for authentication.

All authentication methods have drawbacks and currently there is not a system that cannot be attacked. It is reasonable to assume that there is never likely to be a 100% secure system of authentication.

The biometric concept is extremely secure, but the biometric systems have the disadvantage that require additional authentication periphery. This adds an additional cost that the standard user is not willing to pay. Token-based authentication has seen a massive expansion in recent years, especially in the banking sector. Adoption of smart card technology in the banking world and access based on smartcards for access to companies and organizations have increased the degree of usability of chip and PIN-based authentication.

Image-based authentication appears to offer the best solution. It provides increased security; is very versatile and does not require significant organizational changes in the enterprise. In terms of cost, image-based authentication is convenient as an alternative to text-based, because it require no significant extra costs. The main advantage of text-based authentication means that all approaches of this kind of authentication are similar. Users are familiar with these authentication systems. In contrast, image-based approaches are likely to have different interfaces, which is likely to be different from a security system of an organization to another one.

A two factor password image based authentication method is proposed in this paper for cloud services. This authentication approach is used without additional hardware involved and presents the advantages of utilization in terms of security and usability. Every time when the user will be asked to provide his/her identity, a form for each image included in the photo will be listed. The user will have to remember the secret code for each image and to carefully introduce them in the forms.

As a future work, we want to develop our approach for these randomizing appearing of images that will increase the security level of the authetication system in cloud environment, being an effective solution against shoulder surfing attacks.

Acknowledgement

This work was partially supported by the strategic grant POSDRU/88/1.5/S/50783, Project ID50783 (2009), co-financed by the European Social Fund Investing in People, within the Sectoral Operational Programme Human Resources Development 2007-2013.

Bibliography

[1] PARC,R.C., et al.,Authentication in the Clouds: A Framework and its Application to Mobile Users, *ACM Cloud Computing Security Workshop (CCSW)*; 2010 October 8; Chicago, IL, 2011.

[2] CSA, 2010. Domain 12: Guidance for Identity & Access Management V2.1., *Cloud Security Alliance*. Available at: http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf, 2010.

[3] Metri P. and Sarote G., Privacy Issues and Challenges in Cloud computing, *International Journal of Advanced Engineering Sciences and Technologies*, 5(1): 5-6, 2011.

[4] Tianfield H., Cloud Computing Architectures, *Proc. of 2011 IEEE Int. Conf. on Systems, Man and Cybernetics (SMC11)*, Anchorage, Alaska, USA, 2011.

[5] Lonea A.M., Tianfield H., Popescu D.E., Identity management for cloud computing, In *New Concepts and Applications in Soft Computing, Studies in Computational Intelligence Series*, Volume 417, May 2012.

[6] SETECS Inc, *Security Architecture, for Cloud Computing Environments,* White Paper, February 1, Available at: http://security.setecs.com/Documents/5 _SETECS _Cloud _Security _Architecture.pdf, 2011.

[7] Kay, R., Biometric authentication, Available at: http://www.computerworld.com/securitytopics/security/st
2006.

[8] Tari, F., Ant Ozok, A., Holdon, H.S, A Comparison of Percieved and Real Shoulder-surfing Risks Between Alphanumeric and Graphical Passwords, retrieved June 10 2006 Available at: http://cups.cs.cmu.edu/soups/2006/proceedings/p56 _tari.pdf, 2006.

[9] Dhamija R., et al, DĂŠjĂ Vu: a user study using images for authentication, *Proc. of the 9th conference on USENIX Security Symposium* - Vol. 9, USENIX Association Berkeley, CA, USA 2000, Available at: http://sparrow.ece.cmu.edu/ adrian/projects/usenix2000/usenix.pdf, 2000.

[10] Jackson L., Analysis of Image-Based Authentication and its Role in Security Systems of the Future, Available at: http://www.soc.napier.ac.uk/ bill/lee2006.pdf, 2006.

[11] Nitin, Vivek Kumar Sehgal, et al., Image Based Authentication System with Sign-In Seal, *Proc. of the World Congress on Engineering and Computer Science, WCECS 2008*, San Francisco, USA, 2008.

[12] Newman R.E. HarshP., and Jayaraman P, Security Analysis of and Proposal for Image Based Authentication, *IEEE Carnahan*, 2005.

[13] Confident Technologies Inc., Confident ImageShieldTM, Available at: http://www.confidenttechnologies.com/products/confident-imageshield, 2011.

[14] Renaud K., Just M., Pictures or Questions? Examining User Responses to Association-Based Authentication, *ACM Proceedings of the British HCI Conference 2010*, Dundee, Scotland, 6-10 September 2010.

[15] Just M. and Aspinall D., Personal choice and challenge questions: A security and usability assessment. In L. Cranor, editor, SOUPS, ACM International Conference Proceeding Series. ACM, 2009.

[16] Micallef N., Just M., Using Avatars for Improved Authentication with Challenge Questions, *Proc. of the The Fifth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2011)*, August 2011.