AUTHENTICATION MECHANISMS IN CLOUD COMPUTING ENVIRONMENTS

Belbergui Chaimaa, Elkamoun Najib, Rachid Hilal

STIC Laboratory, Chouaib Doukkali University, El jadida
e-mails: Belbergui.c@ucd.ac.ma, Elkamoun.n@ucd.ac.ma, Hilal.r@ucd.ac.ma
Morocco

Abstract: Cloud Computing is an emerging and ubiquitous trend. It allows users to enjoy the on-demand services, without the burden of data storage and maintenance costs. However, the outsourcing of resources, raises the security issues. The most critical concerns are access control and authentication. This work presents a survey of the previous researches proposing solutions to authentication issues in Cloud. The main aim is to perform a classification of the authentication mechanisms, related to the cloud services, and deployment models, given that, to our knowledge, there is no synthesis work at this level. This classification will be useful to consumers.

Key words: Cloud Computing, Authentication mechanisms, Cloud services, deployment models.

1. INTRODUCTION

Cloud computing is a paradigm that has been developed very rapidly during the last years. It is defined by providing a shared pool of configurable computing resources (storage, software, etc.) on demand via the Internet [1]. By adopting this technology, the user almost needs only a display terminal to use software or access data which are outsourced in the data centers.

The three famous Cloud services are: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2]. Each Cloud service can belong to one of the following Cloud deployment models: public, private, community or hybrid [3].

The use of Cloud Computing allows to benefit from a variety of advantages [2] such as flexibility, since the user can use services any time and from anywhere, costs economy, performance and others.

However, pooling, sharing, as well as outsourcing of resources to a remote server, causes security concerns that are of fundamental concern [4]. It is related to the security of virtualization technology, massive distributed processing technology and traffic management, availability of services, application security, access control, and authentication in the Cloud Computing environment.

This work will focus on the authentication issue in Cloud Computing. To protect the user's privacy, it is essential to use a robust authentication system. This, ensures that only approved and authentic consumers can access and use resources [5]. Authentication within Cloud Computing receives a lot of attention in the academic and industrial world. Some works propose general authentication solutions independently of the service or deployment model, and others develop models specific to a precise type of cloud. However, to our knowledge, there is no synthesis work.

This article aims to state the art of current trends in authentication with a classification appropriate to the cloud services and deployment models. This study leads to the development of a framework to concentrate the information related to this mechanism and will therefore help Cloud customers to choose the most appropriate authentication solution according to the type of the used Cloud.

The remainder of the paper is organized as follows. In section II, we define the basic concepts of cloud computing and authentication. As for section III, it develops a framework which concerns the authentication models and their use in Cloud Computing with an appropriate and justified classification. After that, section IV summarizes the results of the classification and finally, section V concludes the work. The Conclusion should summarize the main results, advantages, possible application and future work.

2. PRELIMINARIES

In this section, we will introduce the basics of cloud computing and authentication.

2.1. Cloud Computing

Cloud Computing is a new technology that is currently experiencing rapid growth in the IT industry. According to the National Institute of Standards and Technology of the United States (NIST) [6], Cloud Computing is a model that enables convenient and on-demand network access to a shared pool of configurable computing resources (Networks, Servers, Storage, Applications, and Services). These resources can be rapidly delivered and disseminated with minimal management effort or interaction with the service provider. Cloud Computing promotes availability and consists of five core features, three service models and four deployment models.

Cloud Computing is distinguished by five key features: on-demand self-service, extended access to the network, resource pooling, fast elasticity and measurement service. It offers several benefits [6]: the increase of outflow, the Cost reduction and improving accessibility. However, the paradigm of outsourcing IT resources has raised serious concerns about security [8].

Several security concerns have been reported [2], among them: Governance, disaster recovery, incident response, application security, identity and access management, and others.

In this work, we will focus on the authentication problem. In cloud computing, hardware, software and services are used by many consumers. The role of identity and authorization management is to ensure that only authorized people can use the IT resources. Access to all services must be secured by identifying and authenticating users or computer systems requesting the access of these ones.

2.2. Authentication

Authentication is the process that allows the user to provide proof of his identity [9]. It is often done through the login method, based on the using of a username and a password. This static mechanism leaves the system vulnerable to attacks, since hackers can use many techniques, such as sniffing and guessing, to steal user passwords [10]. So, to alleviate the problems associated with identity theft, it is essential to adopt a strong form of authentication techniques.

The user authentication is generally based on three factors, something he knows, who is he and what he possess. Something he know may be a password, a pass phrase, a pin number or a secret question. Face recognition, iris scan or the other authentication methods based on body parts allow to identify who is the user. Finally, something that the user possesses may be a smart card, a software token or even a mobile phone. When authentication is performed by combining two or more of the factors presented above, it is named a two or a multiple factor authentication.

3. AUTHENTICATION MODELS AND THEIR PROPOSED CLASSIFICATION IN THE CONTEXT OF CLOUD COMPUTING

In this section, we start by presenting the Cloud types. Then, we organize authentication models by categories. Finally, we classify authentication models by Cloud types with arguments.

3.1. Cloud types

Cloud Computing is able to cross software, platform and infrastructure layers, and treat them indifferently by considering the specific behavior of each one.

Thus, several Cloud typologies can be implemented (public, private, community and hybrid). Cloud services and deployment models are presented in Fig.1.

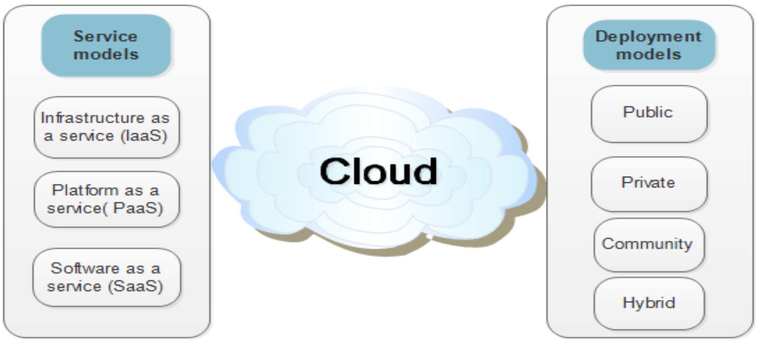
Service models
Infrastructure as a service (IaaS)
Platform as a service(PaaS)
Software as a service (SaaS)
Cloud
Deployment models
Public
Private
Community
Hybrid

Fig. 1. Cloud services and deployment models.

3.1.1. Cloud services

Cloud Computing offers a versatile access to several services. These ones can be categorized according to the functionalities they provide, infrastructure, platform and software as a service (respectively IaaS, PaaS and SaaS) [11]. Advantages and disadvantages of each Cloud service are listed in Table 1.

Table 1. Advantages and disadvantages of Cloud services.

Service	Definition	Advantages	Disadvantages
IaaS	Commissioning of a computer infrastructure; Servers, network, etc.	-Mastering of IT -The customer manages his infrastructure himself.	-Management of IT teams.
PaaS	Commissioning of a platform to deploy applications.	- Homogeneous and mastered infrastructure. -Development aligned with infrastructure.	- Changes in development trades.
SaaS	Commissioning of software.	- Increased flexibility.	-Everything is outsourced.

3.1.2. Deployment models

Deployment models define the complexity of a cloud, by determining how it is used and managed. Four cloud deployment models exist; Public, private, community and hybrid [11]. Advantages and disadvantages of each Cloud deployment model are presented in Table 2.

Table 2. Advantages and disadvantages of Cloud deployment models.

Deployment model	Definition	Advantages	Disadvantages
Public	Managed by the supplier and provided to everyone.	-Open to the general public. -No great investment.	-Located at the provider and managed by him. - Multilocation security issues. -Used by several consumers at once.
Private	Managed and used by the consumer only.	-Dedicated to one organization and can be managed by itself. -Supports the internal security policy.	-No reduction in operational costs. -High operating and maintenance costs.
Community	Managed and used by a group of consumers with common objectives.	- Meets the needs of collaboration.	-Risk of unauthorized access to resources of the other organizations of the community.
Hybrid	Combination of the two deployment models; Public and private.	-Combines the benefits of both types of cloud. - Constant network availability.	-Possibility of access to sensitive resources from less sensitive ones. -Vulnerable to all risks of the public network.

3.2. Authentication models

In this section, we will first make a classification of authentication models and mechanisms by specifying those that are general and those that are specific to the Cloud, then we will make a classification by category. Advantages and disadvantages of each authentication model are listed in Table 3.

3.2.1. General mechanisms

3.2.1.1. Authentication by password

The login and the password are confidential information that the user employs in order to access a specific service (mailbox, shopping sites, etc.) [9]. This is the weakest authentication and identification mechanism, because it is possible to intercept the password in transit or when it is typed on the keyboard.

➢ Typology of passwords

• Simple and easy to remember password: The choice of the password is often left free to the user. Most users simply use an easy-to-remember password. However, it is easy to be guessed.

• Complex passwords: A complex password is hard to be guessed. It combines numbers and letters, with uppercase and special characters.

• Identifiers and passwords with a lifetime: Although complex passwords are more secure than simple ones, several mechanisms can be used to break them. To reinforce the security policy, a password expiration period must be imposed [12]. Thanks to the lifetime technique, a hacked password cannot be used indefinitely.

• One time password (OTP): By adopting the OTP mechanism, the password will be unique, automatically generated, random and can only be used once [12]. For each access request, a new password will be sent to the user, via SMS or email.

• Encrypted password: During communication between user and server, the password is encrypted so as not to be revealed to a third party during transit or recording.

➢ Uses of passwords

• Unique password: Single sign-on allows to use the same password to access all services and applications [13], For example, one password can be used to access both mailbox and social network.

• Multiple passwords: Adopting the technique of multiple passwords allows to specify, one password per service depending on the confidentiality of the secret to protect [12].

3.2.1.2. Authentication by Captcha or image scan

• Captcha: This is a sequence of characters that the user must type to prove that he is not a robot.

• Image scan: When a user is connected to a service from the laptop and want to be connected from the smartphone, the system provides to him an image that must be scanned by this smartphone to access the service without having to remake the whole authentication procedure.

3.2.1.3. Authentication by address, MAC or IP

• Authentication by MAC address: The authentication by MAC address allows to authenticate the machine, not the person. It is a particularly effective method of authenticating users who usually have access to their accounts from a regular set of machines.

• Authentication by IP address: The authentication is successful or not depending on the network from which the access requestor is connected.

3.2.1.4. Biometrics

Biometrics illustrated in Fig. 2 can be used to identify a user through his physiological characteristics such as face, iris and fingerprint, or behavioral characteristics such as gestures and signature [14]. Everyone has his own unique biometric feature. However, it can change over time (age, accident, injury, etc.).

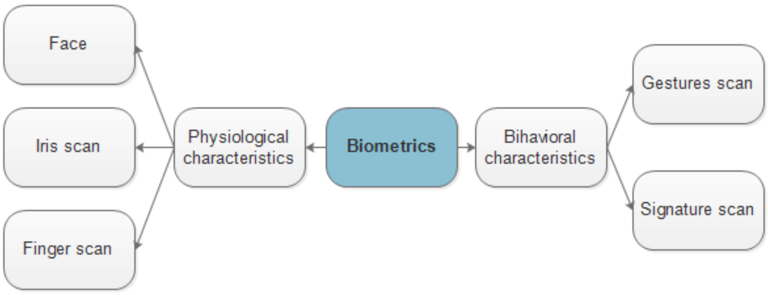

Fig. 2. Biometrics

- ➢ Methods based on physical characteristics

• Face recognition: Authentication by face recognition is a widespread technique. The significant features for face recognition are: eyes, mouth and face shape. During the identification, the low frequency components contribute to the overall description and allow to determine the sex of the user. On the other hand, the high frequency components are more important for the authentication task.

• Iris scan: The detailed texture of the iris is specific to each individual. Moreover, this texture is stable and cannot be modified without significant loss of visual capacities.

• Finger scan: This is one of the first biometrics used in context of authentication, and the most mature technology. The fingerprints are unique to each person, and even to each finger. The fingerprint image is taken using a specific image acquisition device.

- ➢ Methods based on behavioral characteristics

• Gestures scan: The authentication is done by hand gestures. Specifically, the position of the fingers may be in the form of V, W, etc.

• Digital signature: A signature consists of a fixed and variable parts. Authentication using signature allows to identify a user from the fixed part of his signature, from the pressure exerted with the pen and also from the writing speed. This solution requires the use of a touch screen equipment and a stylus.

3.2.1.5. Data encryption

This is a good authentication, avoiding the identity theft and the replay of an authentication. It implements a proof of possession of a secret element (cryptographic key), by means of an authentication protocol guaranteeing the confidentiality of the secret element [15]. Encryption is also an indispensable tool for protecting information in computer systems.

3.2.1.6. Two factor and multi-factor authentication

Two-factor or multi-factor authentication provides strong authentication by the combination of two or more of the solutions presented above.

3.2.1.7. Multilevel authentication

The multi-level authentication reinforces security by authenticating user at several levels. The authentication process is made, for example, at the organization level, then at the team level, and finally at the user level.

3.2.1.8. Authentication duration

Regardless of the used authentication method, when the user fails to authenticate himself in the defined authentication duration, the action is recorded as fraudulent and therefore access will be refused for him thereafter.

3.2.2. Models specific to Cloud

3.2.2.1. Trust

Trust is currently used in Cloud Computing as a means of authentication [16]. Depending on the adopted security policy and the trust level of the user, which judges his behavior, the authentication is accepted or refused.

3.2.2.2. Trusted third party (TTP)

A trusted third party (TTP) is an entity used in the context of the Cloud to facilitate and secure interactions between two parties (consumer and provider) that both trust this third party [17]. It can manage authentication, control access to resources, and more.

Table 3. Advantages and disadvantages of authentication models and mechanisms.

Authentication models and mechanisms			Advantages	Disadvantages
General models and mechanisms	**Password**	**Simple password**	- Cost-effective. -Easy to use and retain.	- Easy to be found by a pirate.
		Complex password	-Guessed with difficulty.	- Forgetfulness. -Not very robust, reusable by an attacker.
		Password with lifetime	-The password discovered by a malicious user, will not be usable indefinitely in time.	-Possibility to find it after each renewal.
		OTP	-No forgetting and reuse, dynamism, and randomization.	- Little comfort of use. -The use of the password by a hacker before the concerned person.
		Encrypted password	-Difficult to be intercepted.	-Possibility to be seen when typing and authentication reply.
		Unique password	-Easy authentication and password memorization.	- The hacking of one account involves hacking of all other accounts at once.
		Multiple passwords	- The hacking of an account does not impact other accounts.	- Difficult to remember.

	Captcha/scan	**Captcha**	- Countermeasure against DOS attacks.	- Unsecured method.
		Image scan	- Flexibility and simplicity.	- Possibility to scan the image from the computer by a nearby pirate.
	@ MAC/IP	**MAC address**	- Simple filtering. - Authentication is authorized to a limited number of machines.	- Access to the authenticated machine by a hacker. -Tedious in a large network.
		IP address	-Simple to use.	-Problem in the case of need to be connected from another network.
	Biometrics	**Face recognition**	-No forgetfulness.	- Variations caused by makeup, aging and expression of emotions. - Easily counterfeited. -The need for a camera.
		Iris scan	-Solution less binding.	-Possibility to photograph the iris pattern for later usurpation. - Necessity to purchase the device.
		Finger scan	-Mature technology, less intrusive, processing relatively fast.	-The need for a specific image acquisition device. -Problem in case of injured or dirty fingers.
		Gestures scan	-Easy to use.	-The need for a camera.
		Digital signature	-Easy to remember.	- Necessity of a touch screen. -The writing changes during the life of the individual.
	Encrypted data		- High-level authentication.	- Calculation time. -Unable to manage and inspect the client process.
	Multi-factor authentication		-A strong authentication.	- Complex.
	Multilevel authentication		-Authentication verified on several levels.	- Authentication problem at the high-level (organization), impacts the authentication of all users.
	Authentication duration		-Securing user accounts.	- Even if the user is authentic, when he has difficulties to be connected, he will be impacted.
Models specific to Cloud	**Trust**		-Dynamic management of authentication corresponding to the user behavior.	- Not enough, the behavior of the user may change over time.
	TTP		-Management of authentication by a neutral third party.	-Difficulty of trusted third-party choice.

3.3. Proposed classification of the authentication models in the context of Cloud Computing

Authentication is the process of verifying the identity of a user, it allows to check whether he is effectively the person he claims to be. The authentication technologies used in the Cloud Computing environment are multiple as presented in the previous section, that are login / password, encryption, trust, and so on.

Based on related works, advantages and disadvantages of Cloud types and authentication mechanisms, we conclude that some authentication mechanisms can be employed regardless of the used Cloud type, while others are more used or only used in specific Cloud types. This is related to the fact that each of Cloud types has its own specificities, which must be taken into account when choosing the appropriate mechanism. The proposed classification is presented below.

3.3.1. Common authentication models

Common authentication mechanisms include the use of password, captcha, image scan, encryption, and authentication duration.

3.3.1.1. Authentication by password

The password is generally the basis of any other authentication model or mechanism. For this reason, it can be used, in its various forms, regardless of the Cloud service or deployment model.

Most systems adopt a simple identifier / password authentication mechanism, recommending that password should be complex and difficult to guess. The paper [18] proposes an authentication platform that uses the password only as a mean of authentication. It allows a user to authenticate using information such as ID / Password, time, position, place, and so on. Then, authenticate him by comparing the entered password with that one registered in the user profile database.

Thus, almost all other authentication mechanisms are based on password combined with other solutions. The authors propose in [19] a password-based authentication solution incorporating the concept of lifetime. The aim is to limit the using of a hacked password indefinitely over time.

Other works limit this lifetime to a one time use. By adopting the one time password technique (OTP), it becomes impossible for any malicious person to re-use the password. The paper [20] provides an additional security mechanism to authenticate and authorize users by adding an e-mail identification. After confirming the authenticity of the user by password. The Cloud system sends a link to the email address, allowing the user to access the required service. The user must authenticate with the link before the expiration time. The research [21] also proposes a unique and dynamic password technique with an authentication system in which mobile phone is used as an authentication device. After authenticating the user by password. An OTP is generated and transmitted to him by SMS.

Another technique is the use of encrypted passwords. It is very widespread for the advantage of the difficulty of interception during the transit. The paper [22] proposes an authentication system in which the user authenticates among data owner using his private key. The data owner is also authenticated by the Cloud provider using his private key. After that, communication between users and the cloud service provider is done after an authentication process using the two-step verification approach based on security keys and mobile phones. The password is encrypted during transmission to the mobile.

In the [23], the authentication phase is supported by the cloud access management server (CAM) which decides whether a user can access the Cloud services and resources. The user is dynamically authenticated after calculating the value of the password using the secret key. The [24] also ensures protection against authentication and identity theft by encrypting all authentication information stored in the system and concerning consumers. A session key is generated after being encrypted with a pre-shared key. It is then added to the customer information. In the solution [25], the credentials submitted by the users consist of the biometric feature vector and the verification code. To successfully authenticate users, the biometric feature vector and the verification code are combined, transformed and mixed correctly. The article [26] proposes an innovative authentication scheme for mobile cloud computing, Message Digest Authentication (MDA). Technically, MDA uses the encrypted and hashed message to obtain secure authentication. For the work [27], the user authenticates using his email address and password. Subsequently, the secret key will be calculated by the user's system. The authentication server verifies the validity of the provided information. When the verification is successful, the server generates a dynamic token and sends it by email to the user for a second authentication.

When a user subscribes to several services that all require the use of a password, a security issue arises. It concerns the management of passwords. Some researchers recommend the use of a single password for all services.

The proposition [28] results in the implementation and execution of this technique, called single sign on (SSO), on the top layer of the Cloud, having as motivation the ease to use. However, it is technically recommended to use one password per service. This allows the isolation of user accounts, that so if one of them is hacked, the others remain intact.

3.3.1.2. Authentication by Captcha or image scan

Authentication by captcha or image scan is widely used. It is always associated with another mechanism. In fact, it is not specific to a specific type of cloud.

The work [29] proposes a solution for Cloud in general. The user must enter the ID and the password received by mail or SMS in the authentication phase followed by the captcha that is dynamically generated to prove that he is not a robot. The goal is to prevent identity theft and DOS attacks.

Another authentication solution for Cloud is presented in the [30]. It consists in using the fast response code (QR). The code is composed of black modules arranged in a square pattern on a white background.

The mechanism allows the user to be connected from his mobile phone quickly, by scanning the QR code from the computer in which the authentication is already done.

3.3.1.3. Data encryption

It is a high-level authentication mechanism, guaranteeing the confidentiality of the secret element. It can be used in all types of clouds since they all contain data that must be protected. For services; in the IaaS, all resources are saved in the Cloud, and should be preserved, using the PaaS, the source code of developed application must not be revealed to other parties, and adopting SaaS, personal information and hosted data need to be secured. As for deployment models, encryption is more used in the public and hybrid cloud because the data is outsourced. It is also used in the private cloud to enhance security.

The paper [31] describes how to store a client's data in the cloud. The process includes key agreement, data encryption, and profile creation and update. The article [32] also proposes a secure data access system using identity-based encryption and biometric authentication for cloud computing. Thus, the paper [33] suggests an access control system based on hierarchical attributes by extending the text-based attribute-based encryption with a hierarchical multiple authorization structure and exploiting the attributes-based signature (ABS). As for the system [34], it introduces the added functionality of access control in which only valid users can decrypt the stored information. Another paper [17], also proposes an authentication protocol based on encryption. The methodology is based on providing a private key of an instance, and then data sharing and encryption using image-based session keys. To enforce confidentiality and authenticity, the encryption based on, key-policy attributes (KP-ABE) is used.

Some encryption solutions specific to the public Cloud have been developed. The authors propose in [35], an authentication solution based on the encrypted image. In the [36], the confidential data are randomly incorporated into images, using steganography as a basic technique, in which a new method of encryption and decryption is proposed. The encryption or decryption methodology uses odd Fibonacci series values and a hash function to prepare a series of hash values. This set of hash values is multiplied by the ASCII codes of the original data that must be embedded in a decryption process. For the solution [37], a Cloud-based Secure Authentication (CSA) protocol suite is implemented to provide a secure authentication mechanism in the public cloud. To ensure data confidentiality, AES with several encryptions is implemented.

Other researchers are interested in encryption for private cloud. Such as paper [38] that uses the MD5 for data encryption.

Encryption is also a means of authentication in the hybrid cloud. It is used in the article [39]. It offers a new e-mail security model that combines image-based authentication, encryption, and compression.

3.3.1.4. Authentication duration

Regardless of the used authentication mechanism and Cloud type, the definition of an authentication duration is required in order to limit the attempts of unauthorized accesses in the Cloud.

The authentication method proposed in [40] is an attempt to make an existing authentication technique safer and stronger by recording the authentication duration. This duration is considered as a partial user authentication procedure. Then, in each subsequent authentication, the user must have to complete the authentication at the same time taken during the last authentication or may take a few seconds more or less.

3.3.2. Authentication solutions by service

All common authentication solutions can be used in all three service types, as presented above. There is almost no solution specific to one of them.

The IaaS uses authentication by password, captcha, image scanning, encryption and authentication time.

The PaaS also uses the common mechanisms, as in the paper [41]. The proposed system is based on encryption and Diffie-Hellman Key Exchange algorithm, and uses two-server authentication based password and key exchange protocol.

Thus, SaaS employs the common mechanisms such as in the article [42]. It proposes an improvement of the AES algorithm for 1024 bits key length. The aim is to increase security in banking systems. Encryption makes the system viable and secures communication and authentication.

3.3.3. Authentication solutions by deployment model

3.3.3.1. Authentication in public Cloud

In the public cloud, resources are completely outsourced. This means that the consumer loses control over his resources and data, and so the service provider takes care of it. When the Cloud consumer and Cloud provider do not trust each other, it is advisable to add a trusted third party (TTP or TPA) to whom the authentication management and the control of the compliance with the security requirements are delegated.

The article [43] proposes an authentication solution based on a trusted third party (TPA) in which the third party auditor verifies publicly the integrity of the user's knowledge in the cloud before being shared among several users. In the same logic, the articles [44], [45] provide security in the cloud with the help of the third-party auditor to reassure cloud users and cloud service providers that their data are secured. Thus, the paper [46] suggests establishing a Global Authentication Recording System (GARS) on trusted third parties (TTP). The work [47] also proposes a solution in which data integrity checking is done by introducing a third party auditor (TPA) who has privileges to verify the integrity of the dynamic data in the cloud on behalf of Cloud Client.

3.3.3.2. Authentication in private Cloud

➢ Authentication by MAC and IP addresses

MAC and IP addresses are means of authentication in the Cloud. This mechanism works best when the number of users is not huge, if not it will be complex. For this, it is more recommended to use it in a private cloud.

The article [30], for example, presents the authentication method based on MAC address that can be performed locally or with a RADIUS server.

The MAC address of the client machine is checked against a global list of MAC addresses that are allowed or denied to access the system. This function is performed by configuring a MAC filter.

➢ Biometrics

Authentication by physiological or behavioral characteristics is adopted by several authors, as an effective means of authentication. It is generally used in the context of the private cloud, since it requires devices such as camera, fingerprint device, the touchscreen and others that are not available to the general public. On the other hand, an organization opting for the private cloud and choosing this authentication method, can provide to employees the necessary tools.

➢ Methods based on physical characteristics

Methods based on physical characteristics include authentication by face recognition, iris scan and finger scan.

The article [48] proposes a new face recognition system (FRS), in which the face serves as a password. The paper [49] suggests an authentication solution in the same logic, but takes into account the distortions, for example the loss and gain of weight, etc.

However, the work [50] uses iris scan authentication, combined with other types of biometrics.

As for [51], it proposes an authentication scheme based on the finger scan.

For the article [52], a Cloud Cognitive Authenticator (CCA) is proposed to improve cloud security through offering two levels of authentication as well as encryption / decryption of the user ID.

The novelty of CCA is that it uses the Electro Dermal Responses (EDR) for first-level authentication. EDR is the conductance of the user's skin, consisting of the behavioral or the mental information of the user. The captured EDR reading of the skin conductance meter is converted, and then this electrical conductance of the skin is checked to determine physiological emotion of the user and thus to know whether it is a malicious person or not.

➢ Methods based on behavioral characteristics

The methods based on behavioral characteristics include authentication by gestures scan security used in the paper [50] associated with other authentication techniques, and by digital signature proposed in the article [53].

➢ Multi-level authentication

The multi-level authentication provides user authentication at several levels. It is used in the context of private cloud that is generally adopted by organizations. This is due to the fact that in organizations, the hierarchical aspect on which the mechanism can be applied exists.

The articles [30], [54] present a strict authentication system by introducing the multi-level authentication technique that generates the password and authenticates Cloud user at multiple levels (organization, team and user).

➢ Tunnel

The tunnel is typically used by organizations opting for private cloud to provide secure access to resources for the subsidiaries. It is impossible to use it as a means of authentication in a public cloud because, in this type of cloud, consumers do not have the right to control the security themselves.

The article [55] exploits the IPSec extension, to have a secure tunnel, with a private cloud for users, who can move dynamically without using the same machine. Strong authentication with a key tuning scheme is proposed to establish the secure tunnel. In addition, several related security properties of the proposed mechanism are presented.

3.3.3.3. Hybrid

The hybrid cloud is the use of two types of cloud (private and public) by the same organization. For this reason, authentication in the private or public cloud level requires the use of authentication mechanisms that are presented above, specific to each one. However, a user authenticated in the public cloud and want to access a service in the private cloud must be controlled. The transition from public to private Cloud, with more sensitive resources, requires additional authentication layers.

The authentication system proposed in [56] uses the RADIUS method and two-factor authentication schemes. The paper [57] also provides an authentication system in the same logic. Thus, the article [58] proposes a technique of authentication with two factors using the mobile devices. The method makes it possible to use the biometric characteristics inseparable from the device owner, characterized by the specifications of his handwriting.

4. SYNTHESIS

Authentication is one of the major issues in Cloud computing [59]. After finely studying the Cloud types and the authentication models, which are used in the Cloud, we have developed a classification of these models by Cloud type. Indeed, there are authentication solutions that can be used regardless of the cloud to protect [60]. In the other hand, there are authentication mechanisms that are specific to certain Cloud types. The whole is clearly explained and argued in the previous section. Our proposal is presented in the table below (Table 4). It summarizes the results.

Table 4.The use of authentication mechanisms in Cloud

Cloud types		Appropriate authentication mechanisms	Explications
All Cloud types		Common mechanisms:	
		-Authentication by password	-The password is the initial of any other authentication model or mechanism. It is not specific to a precise type of cloud
		-Authentication by Captcha or image scan	-It can be used independently of Cloud type.
		-Encryption of data	-It can be used in all cloud types since they all contain data that should be protected.
		- Authentication duration	-The adoption of any type of authentication requires the definition of an authentication duration in order to limit the attempts of the unauthorized accesses in the Cloud.
Cloud services		Common mechanisms	-All common authentication solutions can be used in the three Cloud services. There is hardly any solution specific to one of them.
Cloud deployment models	**Public**	-Trust (TTP, TPA)	-When the consumer does not trust the supplier or in the opposite case, it is advisable to have recourse to a trusted third party (TTP or TPA) to whom the management of authentication or the control of compliance with the security requirements are delegated.
	Private	-Authentication by address, MAC or IP	- This mechanism works well when the number of users is not huge (private cloud), if not the management of authentication with it will be complex.
		-Biometrics	-It requires the existence of devices such as the camera, the fingerprint acquisition device, the touch screen and others, which are not available to the grand public.
		-Multilevel authentication	-In organizations opting for the private cloud, the hierarchical aspect on which the mechanism can be applied is present.
		-Tunnel	-The tunnel is generally used by organizations opting for private cloud to provide secure access to the cloud by the subsidiaries.

	Hybrid	-The mechanisms used in the public and private cloud. -Multi-factor authentication.	-The hybrid cloud combines the use of two types of clouds (private and public). -The transition from public to private cloud requires the addition of other authentication layers because the latter one contains more sensitive resources.

5. CONCLUSION

Cloud Computing provides to customers, via the Internet, IT resources such as software, hardware, infrastructure and data storage. It is a ubiquitous technology for all the advantages it offers; flexibility, cost reduction and others. However, security is an important consideration in the Cloud. One of the security issues that was discussed in this work is user authentication. Using a good authentication allows to protect user identities and information.

This paper has closely studied the authentication mechanisms used in the Cloud Computing environment. It shows that each type of Cloud has its specificities in terms of authentication. Some authentication mechanisms are valid for all Cloud typologies, while others are only valid or used extensively in specific cloud types. The classification made will allows anyone interested in the Cloud to have a clear and accurate view of authentication solutions and which one best matches each type of Cloud.

Acknowledgment

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

REFERENCES

[1] Y. Jadeja and K. Modi. Cloud computing-concepts, architecture and challenges, in *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, 2012, pp. 877–880.

[2] S. Bulusu and K. Sudia. *A Study on Cloud Computing Security Challenges*, 2013, pp. 1-137.

[3] Z. Javaid and I. Ijaz. Secure user authentication in cloud computing,” in *5th International Conference on Information & Communication Technologies (ICICT)*, 2013, pp. 1–5.

[4] C. Rong, S. T. Nguyen, and M. G. Jaatun. Beyond lightning: A survey on security challenges in cloud computing. *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, Jan. 2013.

[5] A. A. Elmrabti, A. A. El Kalam, and A. A. Ouahman. Security Challenges in the Cloud Computing: Cloud Computing Security Issues and Solutions. in *National Days of Network Security and Systems (JNS2)*, 2012, pp. 80–85, 2012. (In French)

[6] P. Mell, T. Grance, et al. *The NIST definition of cloud computing*, 2011, pp. 1-7.

[7] B. S. Kaliski Jr and W. Pauley. Toward Risk Assessment as a Service in Cloud Environments, *HotCloud*, 2010, pp 1-7.

[8] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.*, vol. 34, no. 1, Jan. 2011, pp. 1–11.

[9] H. Chang and E. Choi. User authentication in cloud computing. in *International Conference on Ubiquitous Computing and Multimedia Applications*, 2011, pp. 338–342.

[10] B. Sumitra, C. Pethuru, and M. Misbahuddin. A Survey of Cloud Authentication Attacks and Solution Approaches. *International Journal of Innovative Research in Computer and Communication Engineering*, 2014, pp. 1-9.

[11] Q. Zhang, L. Cheng, and R. Boutaba. Cloud computing: state-of-the-art and research challenges. *J. Internet Serv. Appl.*, vol. 1, no. 1, May 2010, pp. 7–18.

[12] P. Ministre. *Technical Note Security Recommendations for Passwords*. 2010, pp. 1-11 (In French)

[13] O. Salaün. *Introduction to Web architectures of Single-Sign On*. Resume, 2003, pp. 1-8, 2003 (In French).

[14] V. N. Opris, S. Eftimie, & C. Racuciu. Biometric multi-factor authentication scheme in Cloud Computing. *Scientific Bulletin of Naval Academy*, vol. 19, no 1, 2016, p. 530.

[15] R. Arora, A. Parashar, and C. C. I. Transforming. Secure user data in cloud computing using encryption algorithms. *Int. J. Eng. Res. Appl.*, vol. 3, no. 4, 2013, pp. 1922–1926.

[16] K. Hwang and D. Li. Trusted cloud computing with secure resources and data coloring. *IEEE Internet Comput.*, vol. 14, no. 5, 2010, pp. 14–22.

[17] S. Poongodi, P. Murugan, and P. Kuppusamy. Shared authority based privacy-preserving authentication protocol in Cloud Computing. *Cloud Computing*, vol. 19, 2015, pp 1-3.

[18] H. Ahn, H. Chang, C. Jang, and E. Choi. User authentication platform using provisioning in cloud computing environment. in *Advanced Communication and Networking*, Springer, 2011, pp. 132–138.

[19] N. M. Gonzalez et al. *A Framework for Authentication and Authorization Credentials in Cloud Computing*. 2013, pp. 509–516.

[20] A. H. M. Emam. Additional authentication and authorization using registered email-ID for cloud computing. *Int. J. Soft Comput. Eng.*, vol. 3, no. 2, 2013, pp. 110–113.

[21] R. K. Chhabra and A. Verma. Strong authentication system along with virtual private network: A secure cloud solution for cloud computing. *Int. J. Electron. Comput. Sci. Eng.*, vol. 1, no. 3, 2012, pp. 1566–1573.

[22] D. Saraswat and P. Tripathi. Secure Data Access with Enhanced Two Factor Authentication in Cloud Computing. *Int. J.*, vol. 4, no. 11, 2014, pp. 1-5.

[23] R. K. Banyal, P. Jain, and V. K. Jain. Multi-factor Authentication Framework for Cloud Computing. 2013, pp. 105–110.

[24] M. Darwish, A. Ouda, and L. F. Capretz. A cloud-based secure authentication (CSA) protocol suite for defense against Denial of Service (DoS) attacks. *J. Inf. Secur. Appl.*, vol. 20, Feb. 2015, pp. 90–98.

[25] K. S. Wong., & M. H. Kim. Towards Biometric-based Authentication for Cloud Computing. In *CLOSER*, 2012, pp. 501-510.

[26] S. Dey, S. Sampalli, and Q. Ye. Message digest as authentication entity for mobile cloud computing. in *IEEE 32nd International Performance Computing and Communications Conference (IPCCC)*, 2013, pp. 1–6.

[27] G. V. Gujar, S. Sapkal, and M. V. Korade. STEP-2 User Authentication for Cloud Computing. *Int. J. Eng. Innov. Technol*. 2013, pp. 2277–3754.

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

[29] Y. Patel and N. Sethi. Enhancing Security in Cloud Computing Using Multilevel Authentication. *Int. J. Electr. Electron. Comput. Sci. Eng.*, vol. 1, no. 1, 2014, pp 1-5.

[30] S. R. Telrandhe and D. Kapgate. *Authentication Model on Cloud Computing*. 2014, pp. 33-37.

[31] J. Yeh. A PASS Scheme in Cloud Computing-Protecting Data Privacy by Authentication and Secret Sharing. in *Proc. of International Conference on Security Management*, 2011, pp. 1-8.

[32] H. Cheng, C. Rong, Z. Tan, and Q. Zeng. Identity based encryption and biometric authentication scheme for secure data access in cloud computing. *Chin. J. Electron.*, vol. 21, no. 2, 2012, pp. 254–259.

[33] X. Liu, Y. Xia, S. Jiang, F. Xia, and Y. Wang. Hierarchical Attribute-Based Access Control with Authentication for Outsourced Data in Cloud Computing, 2013, pp. 477–484.

[34] S. Ruj, M. Stojmenovic, and A. Nayak. Privacy Preserving Access Control with Authentication for Securing Data in Clouds. 2012, pp. 556–563.

[35] R. Sharma, A. Saxena, and M. Manoria. An Efficient Data Sharing in Public Cloud using two way Authentication & Encryption. *IJCSIT*, vol. 6, 2015, pp.4807-4811.

[36] B. Goswami and G. Ravichandra. Public cloud user authentication and data confidentiality using image steganography with hash function. *Am. J. Appl. Math.*, vol. 3, no. 1–2, 2015, pp. 1–8.

[37] R. Tamilarasi and S. Prabu. Data Security Mechanism for Public Cloud through Cloud-Based Secure Authentication. *Journal of Supercomputing*, 2013, pp. 1-32, 2013.

[38] S. Nivedha, N. Saranya, and P. G. Scholar. Accessing the File in a Private Cloud with an Authentication-Openstack. *Int. J. Eng. Sci.*, vol. 5851, 2016, pp. 1-4.

[39] M. N. Rathi, M. P. Nahar, and M. V. K. Verma. A New Hybrid Cloud Based Email Security Model Using Image Sequence Authentication, Compression and Cryptography. *IJCSIT*, vol. 6, 2015, pp. 3051-3056.

[40] P. C. Talhan, R. M. Thakare, and A. D. Patil. A survey on secure authentication with 4-D password in Cloud Computing," *IJSER*, vol. 4, 2013, pp. 27-31.

[41] A. Kumari and L. Rohini. A Symmetric Two-Server Password based Authentication and Key Exchange Protocol Deployed in PaaS. *ICICT*, 2015, pp. 1-7.

[42] D. K. Shah, V. Bharadi, V. Kaul, S. Amrutia, and A. Ambardekar. Implementing Enhanced AES for Cloud based Biometric SaaS on Raspberry Pi as a Remote Authentication Node, 2015, pp. 17-22.

[43] P. Rahul, T. Malathi, and S. Archana. Ring signatures based homomorphic authentication for public auditing in Cloud. *Advanced Engineering Technologies*, vol. 5, 2015, pp. 264-268.

[44] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for secure cloud storage. *IEEE Trans. Comput.*, vol. 62, no. 2, 2013, pp. 362–375.

[45] A. Patidar and M. Sheikh. Cloud storage Security Mechanism with Authentication in Public Cloud. *International Journal of Technology Research and Management*, vol. 2, 2015, pp. 1-5.

[46] C.-Y. Chen and J.-F. Tu. A Novel Cloud Computing Algorithm of Security and Privacy. *Math. Probl. Eng.*, vol. 2013, 2013, pp. 1–6.

[47] V. Patel, R. Kumar, and A. Raj. Improving Security and Integrity of Data Storage in Cloud Computing by Using Homomorphic Authentication technique. *Int. J. Innov. Eng. Technol.*, vol. 3, no. 2, 2013, pp. 197-202.

[48] N. Gajra, S. S. Khan, & P. Rane. Private cloud security: Secured user authentication by using enhanced hybrid algorithm. In *International Conference on Advances in Communication and Computing Technologies (ICACACT)*, 2012, pp. 1-6.

[49] K. M. S. Soyjaudah, G. Ramsawock, and M. Y. Khodabacchus. Cloud computing authentication using cancellable biometrics. in *AFRICON*, 2013, pp. 1–4.

[50] V. N. Opris, S. Eftimie, & C. Racuciu. Biometric multi-factor authentication scheme in Cloud Computing. *Scientific Bulletin of Naval Academy*, vol. 19, no 1, 2016, p. 530.

[51] A. A. Yassin, H. Jin, A. Ibrahim, and D. Zou. Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing, 2012, pp. 282–289.

[52] L. B. Jivanadham, A. M. Islam, Y. Katayama, S. Komaki, and S. Baharun. Cloud Cognitive Authenticator: A public cloud computing authentication mechanism. In *International Conference on Informatics, Electronics & Vision*, 2013, pp. 1–6.

[53] P. Rewagad and Y. Pawar. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing, 2013, pp. 437–439.

[54] H. A. Dinesha and V. K. Agrawal. Multi-level authentication technique for accessing cloud services. in *International Conference on Computing, Communication and Applications (ICCCA*), 2012, pp. 1–4.

[55] Y.-F. Lu and C.-F. Kuo. Portable tunnel establishment with a strong authentication design for secure private cloud. in *Proceedings of the 2012 ACM Research in Applied Computation Symposium*, 2012, pp. 304–309.

[56] J.-M. Kim and J.-K. Moon. Secure Authentication System for Hybrid Cloud Service in Mobile Communication Environments. *Int. J. Distrib. Sens. Netw.*, vol. 10, no. 2, Feb. 2014, p. 828092.

[57] J. K. Wang and X. Jia. Data Security and Authentication in hybrid cloud computing model. in *IEEE Global High Tech Congress on Electronics*, 2012, pp. 117–120.

[58] V. A. Pasenchuk and D. A. Volkov. SignToLogin cloud service of biometric two-factor authentication using mobile devices. in *17th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices*, 2016, pp. 164–167.

[59] D. Hyseni, B. Çiço & B. Selimi. Conception, design and implementation of an interface for security in Cloud controlled by the end user. *International Journal on Information Technologies & Security*, Vol. 8, No. 2, 2016, pp. 35-44.

[60] D. Y. Chang, M. Benantar, J. Y. C. Chang, & V. Venkataramappa. Authentication and authorization methods for cloud computing platform security. *U.S. Patent No. 9,288,214*. Washington, DC: U.S. Patent and Trademark Office, 2016.

Information about the authors:

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 PhD 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 Chouaib Doukkali University El Jadida. He is member of the STIC Laboratory and ability professor. His research interests include distributed power amplifiers, microwave nonlinear circuit design, and inset-fed patch antenna.

Manuscript received on 04 July 2017