Authentication and authorization in service oriented cloud computing architecture

Arbër Beshiri [0000-0003-0258-7274]

Faculty of Computer Science and Engineering, "Ss. Cyril and Methodius" University, Rugjer Boshkovikj 16, 1000 Skopje, North Macedonia
arber.beshiri@gmail.com

Abstract. The cloud computing architecture is composed of various types of configurable distributed systems with a broad range of connectivity, accessibility and usage. Authorization and authentication are two important security mechanisms in the cloud computing, especially in securing authorized accesses to services and resources. With proper security management, authentication and authorization also provide managing and preventing the various unauthorized accesses in the cloud system. Securing services in the cloud, controlling access to resources through the proper authentication and authorization mechanisms, protecting and providing their security are considered critical tasks for the cloud service provider. In this paper are surveyed issues that are related to authentication and authorization management of services in the cloud environment. Here are studied and compared details about cloud computing services and providers, with particular emphasis the service oriented cloud computing architecture in terms of authentication and authorization. The existing mechanisms of authentication and authorization in the cloud computing are discussed comprehensively and their necessary requirements, evaluating them against the respective requirements.

Keywords: Cloud Computing · Service Oriented Cloud Architecture · Authorization · Authentication · Security.

1 Introduction

Cloud computing is a collection of various configurable computational resources such as networks, servers, storages, services and applications which can provide users flexible as well as on-demand access [1, 2]. It also offers very cost-effective demand service and stability [1, 3, 4], highly efficient processing and accessibility of resources. Cloud providers take responsibility for the optimization of resources [5].

The deployment models associate the aim and existence of the cloud computing. There are three categories of the deployment model, respectively public cloud, private cloud and hybrid cloud [6 - 10]. Cloud computing essentially offers three separate service distribution models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) [6, 7, 8, 11, 12] as depicted in Fig. 1.

In terms of cloud services, authorization and authentication as the key issues should be ensured [2]. In cloud computing are needed robust mechanisms of authentication and authorization in order to protect and maintain its resources [1].

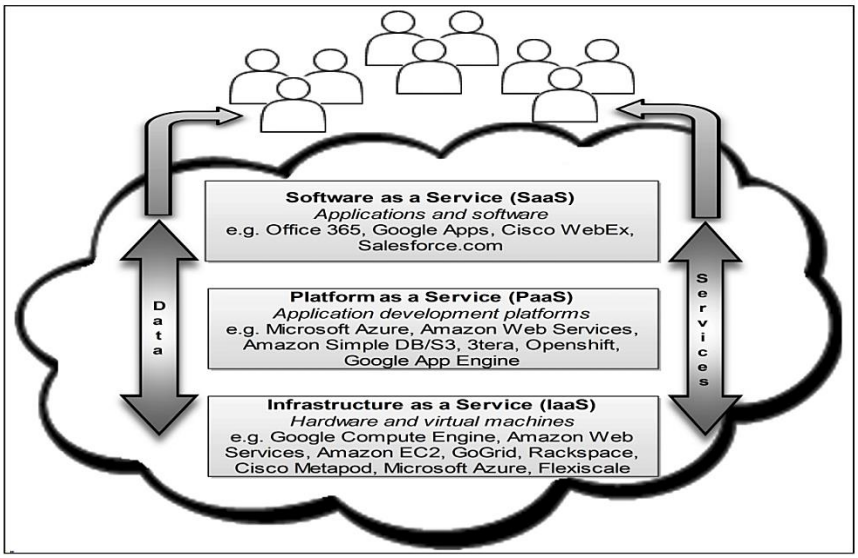

Fig. 1. Cloud service distribution architecture

In the cloud, security is considered as the serious concern because the cloud service provider (CSP) enables the distribution of resources across members/organizations and it needs to define who has authorization and how it can have accessing in resources. Based on this issue we have two basic concepts of security, i.e., authentication that is a process that enables confirmation of the claimed identity for systems that enables identifying their entities securely, while authorization is considered as a systematized mechanism from the system that determines the access level of authenticated entities in secured resources. These two steps must be executed sequentially to provide the appropriate level of cloud security [13-16]. The convenient authentication and identification of cloud entities is essential in order to prevent unauthorized access. This is hard to maintain because many services as well as CSP and their employees can access to common resources [17].

The concern of the CSP is that its services and resources to be accessible for the authorized entities. If the cloud does not support and contain adequate access control policies, it will be often vulnerable to different threats and attacks [17]. Cloud computing can be attacked from conventional security attacks of systems: malicious code (viruses and Trojans), back door, Man-in-the Middle and Distributed Denial-of-Service (DoS) attacks, the API that is insecure, abuse and misuse of cloud computing and malicious interference within the cloud. Because of these attacks, cloud services can be inaccessible and have bad impacts. For CSPs, ensuring that their services are completely accessible and usable at all times is an essential and main requirement. In

such circumstances, resources can be faced with issues such as privacy and unauthorized access [18].

Even the confidentiality and integrity of resources should not be compromised in any way, in cases where services manipulate resources in the cloud, but also in cases when they are stored on servers of third party public cloud. Therefore, an adequate mechanism for access management and control is essential and plays an important role in the above cases. Cloud providers must provide essential features for controlling unauthorized accesses, such as ensuring secure access to the services, defending access of service's resources from other services, controlling access to services according to their previously determined privileges, i.e. to maintain and manage the rules of access control constructively [17].

In cloud environments, CSPs are accountable for identity and other types of management. Nevertheless, because of the weaknesses in identity management systems, a significant number of resource leakage problems are caused. The absence of an effective mechanism affects in many issues in the cloud computing environment, including identity management, service security, privacy and resource leakage [1].

This work presents a comprehensive analysis and literature review with the purpose of better understanding different authentication and authorization techniques of cloud computing architecture services, which can point the way for future study and research.

2 Methodology

This paper provides a survey and literature review from various credible resources which they describe aspects of authentication and authorization about the cloud computing architecture. The relevant study provides the most important and useful techniques related to the authentication and authorization of cloud computing services, which can provide several directions on how services can be developed and designed in the cloud architecture based on genuine authentication and authorization techniques and mechanisms. The analyzed subject is extraordinarily wide, so it is impossible to describe all the topics covered in the relevant subject. As a result, we have briefly discussed several related subjects.

Based on searching in the databases of Google Scholar, IEEE Xplore, ACM, Springer and Elsevier, we have picked the relevant and most cited papers that relate and describe the aforementioned technologies. According to the title of the paper, keywords and the content of the analyzed papers, we have separated the paper into the following sessions: Cloud Computing Security Issues, Cloud Computing Authentication Mechanisms and Cloud Computing Authorization Mechanisms. Each technology discussed in the paper has its advantages and disadvantages, therefore referring to these two features are given several recommendations for future research.

3 Cloud computing security issues

Cloud computing includes security issues related to Internet-based distributed services such as security technology of visualization, service availability, traffic handling,

service security, access management and control, authentication and authorization [2, 13, 17]. The security of cloud computing is based on a variety of infrastructures, applications and security policies that are used for service security in the cloud environment. There are used different technologies, including intrusion detection systems, firewalls and segregation of obligations on various cloud service models and layers provide security in the cloud computing [15]. In the security of the cloud services are contributing the mutual authentication and security standards of web services [1].

The architectural design, attack areas, preventives from different attack ways and access controls are involved in cloud security [2, 17]. The services based on the cloud are accessible from the cloud users, but their security can be influenced by the APIs and protocols utilized that they can also generate cloud computing insecurity [2]. The service provider must care that cloud services, resources and infrastructure to be secured in the cloud environment [1].

There are numerous security problems that jeopardize resources and services in the process of service access and resource storage in the cloud environment. One such issue is the case of resource storage with the support of third party organizations which can sometimes have a compromising role as a malicious attacker. The best practices enable the cloud service providers to overcome these security issues and to secure their network by updating it with the package of security requirements such as managing users, roles and identities; ensuring the appropriate protection of services and resources, enforcing policies for ensure of services and resources; review the security facilities for cloud services; assess security mechanisms on cloud environment and provisions; etc. One of the best practices for estimation of cloud services is the identity and access management (IAM) [1]. Currently it enables efficient security and identity management and access control to cloud resources and services for registered subjects in cloud systems [1, 2, 17].

In addition to providing security which is essential for the cloud environment, IAM systems enable various security operations in cloud computing including authentication and authorization. The identity of each entity must be verified first, i.e. passing the authentication process that is followed by the authorization process, for having the appropriate access level to resources [1, 2, 17].
In the following, in each subsection of this section a security property is included.

3.1 Security polices

Preventive measures through appropriate security policy rules like identification and authentication, logical service access control, protection services, secure service management, handling cloud security incidents, service access control and resource use and protection of cloud systems against attacks are included in security policies [6]. The relevant security policy rules should enable a secure operating environment, without affecting the performance and reliability of the cloud [6, 16]. Security policies operate and derive according to regulatory authorities. They include different "service-level agreements, client/service management issues, and antecedent trust" [6].

3.2 Identity and access management

Identity and access management (IAM) stands for security related mechanisms that enable resource security and maintains the cloud service identity. It has the possibility to perform many functions such as identity management, maintenance, policy enforcement, authentication and authorization. IAM verifies whether the correct identities are used for certain services. It manages them and provides security for the respective identities. Through the IAM is enabled the authentication of users, services or other system resources. It allows or denies the access right to resources. In the case of access to any application, the service does not request that its identity to be stored or to be authenticated by the authentication mechanism. The identity verification as a process can be passed to a trusted identity provider in order to be reduced the service/application load [1, 15].

IAM can be used in organizations, enterprises, private enterprises and cloud providers. It can be used in cloud computing to identify cloud objects, entities, control the access of services to resources based on predefined policies. There are numerous operational areas and multiple of them relate to IAM. These operational areas related to IAM include authentication and authorization management, federated IAM and compliance management. The authentication management through IAM enables that usernames, passwords and digital certificates in the cloud to be managed properly and securely. It also provides the possibility of authentication of cloud services by utilizing the identity provider. Once the authentication is successful, the authorization mechanism is considered, which determines whether the authenticated entity can carry out any operation within the certain service [1].

The IAM system is provided by many organizations to protect resources/information by controlling and managing service access permissions. SailPoint, IBM, Oracle, RSA and Core Security are the most widely recognized the IAM system providers. Four main solutions for cloud security are offered by Oracle IAM. The first solution offered by Oracle IAM is identity management by including "self-service account request, identity lifecycle management, password management and enterprise role management" [1]. The management of authentication and trust of services is offered as the second solution by Oracle IAM by including specifications such as privacy, single sign on and identity federation. As a third solution offered by Oracle IAM is the access control by including features such as fine-grained rights/privileges, authorization based on risk and security of web services. The identity and access administration is offered as a four solution by Oracle IAM by including features like role mining and applying, certification, resource analysis for identity and embezzlement-prevention and directory services (database security for services, consistent storage, etc.) [1, 6].

4 Cloud computing authentication mechanisms

The mechanism that is used to verify the identity of the user/service is called authentication. In the cloud system, authentication means that the right user is getting access to the resources provided by the cloud provider [15]. Authentication is considered the mechanism which enables through one entity to approve another entity [11]. Its pur-

pose is to ensure that the proper person or application is accessing certain resource [2]. The authentication as a process is performed through the software or as a part of it [1].

Cloud computing authentication is ensured if the resources stored in the cloud are accessed; in this situation the identity of the user is offered to the cloud service provider [15]. Cloud provider is able to choose and provide different authentication mechanisms that have various strength of security. Reliability and integrity determine the strength of these mechanisms [16].

In Fig. 2 is presented the general authentication scheme in the cloud systems. Users for using the services in the cloud server must be verified by the authentication server and then access to the cloud server. Its strength has an impact on the cloud environment in terms of reliability and security [15]. Access permissions are granted to users when they introduce themselves with something that is convenient for the system, such as a card number or password, which is dedicated to users and defined by them [6].

In the following are presented and discussed several digital security authentication mechanisms [1, 6] that are very important and enable the service oriented cloud computing authentication.

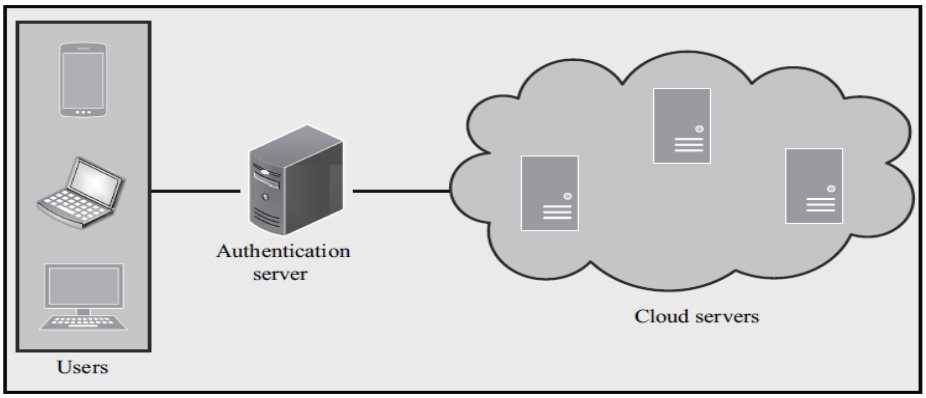

Fig. 2. The general authentication scheme in the cloud systems [15]

4.1 Password authentication

Password authentication is considered simple and not complex to use. It must have a complex composition and be regularly renovated to keep the possible degree of security. This authentication technology is known for its weaknesses, so even if the username and password are provided correctly, it is still hard to verify whether the owner of the given credentials is the rightfulness and the resource request is sent by the right owner. It often happens that users reuse passwords when they are authenticated in different cloud services. Usually, the high security risks in user account information come mainly from fragile password practices. In the latest cloud deploy-

ment, password authentication is the simple model of the challenge-response authentication protocol [16, 19].

The challenge-response authentication protocol is a set of protocols where one pair presents a “challenge” (to be responded) and another pair must provide a valid “response” (the answer needs to be validated (checked)) for the question (challenge) in order to be authenticated. These protocols request the claimant to prove its identity to the verifier by presenting its information as secret value which only the claimant knows and they are not disclosed during the authentication process, as part of the authentication protocol [19, 20].

4.2 Public key infrastructure authentication

Public key infrastructure (PKI) authentication as an authentication method based on public key cryptography. This authentication mechanism allows users to authenticate other parties through a certificate without distributing their secret information [15]. The right level of trust in the cloud is achieved when the Trusted Third Party (TTP) is used, which it provides the solution for maintaining confidentiality, integrity, resource authenticity and communication. Joining two authentication methods, respectively PKI and TTP and their application in the cloud result with strong and effective authentication and authorization in that system [16]. In order to provide proper authentication, PKI is used to develop and design Secure Socket Layer (SSL), Transport Layer Security (TLS) and Secure Electronic Transaction (SET). SSL, TLS and SET are security protocols [15, 19]. PKI's effectiveness lies in managing private key access, identical to other forms of encryption systems [15].

4.3 SSO and cloud federation authentication

Since the applications of SaaS need a centralized management system which restricts the software polices, the traditional mechanisms of authentication are not always considered appropriate for remote authentication. Clients can use many services in the cloud, therefore they cause many requests for logging and these bring different problems. This happens as a result that a single consumer should maintain a large amount of credentials. Based on the above mentioned reasons, the Single Sign-On (SSO) mechanism is considered as the potential solution for such issue [7].

Federated identity is really a valuable functionality for managing identity. The fundamental principles and protocols for federated authentication of the cloud service are considered OpenID, Open Authorization (OAuth), and Security Assertion Markup Language (SAML) [15]. SAML, OAuth and OpenID offer SSO facilities by enabling the Identity Provider (IdP) to exchange information of authorization and authentication with the Service Providers (SPs) [1].

4.3.1 Single sign-on

SSO is a system (mechanism) for identity management in which a user can be authenticated through a single authentication. Then, the user can access to the specific resources by not repeating authentication (without logging in to an application/service

again). SSO [13] is considered something as a passport that is used for authentication only the first time. The user does not need to login again, for other sites or a process in which is applied this authentication mechanism. Multiple clients are defined by this protocol. Such clients can access resources and application/service. When a consumer (user) uses the SSO [14], it usually has the proof through which verifies its identity and access. Afterwards it uses that to access certain services [15].

Fig. 3 shows the SSO architecture workflow in the cloud system (environment) context. Different expressions are used in systems where SSO protocols are included. All expressions are discussed in following. Identity provider (IdP) has responsibility about the process of authentication. In addition, the user information stored as attributes in a token of identity is handled by the IdP. Once a user is authenticated, an object that holds the user information is created by IdP. When the service provider requires user attributes, it uses the user information. Service provider (SP) mainly provides the specific service and it is secured from a security protection in general. If the user decides to use the service, the security protection requires the identification of its information. Authorization server is also considered with the term of the trusted authority. After the user is authenticated, the authorization server provides access tokens for it. There are various structures of the SSO, but the enterprise single sign-on (ESSO) and web single sign-on (WSSO) are two the most used structures of the SSO [15].

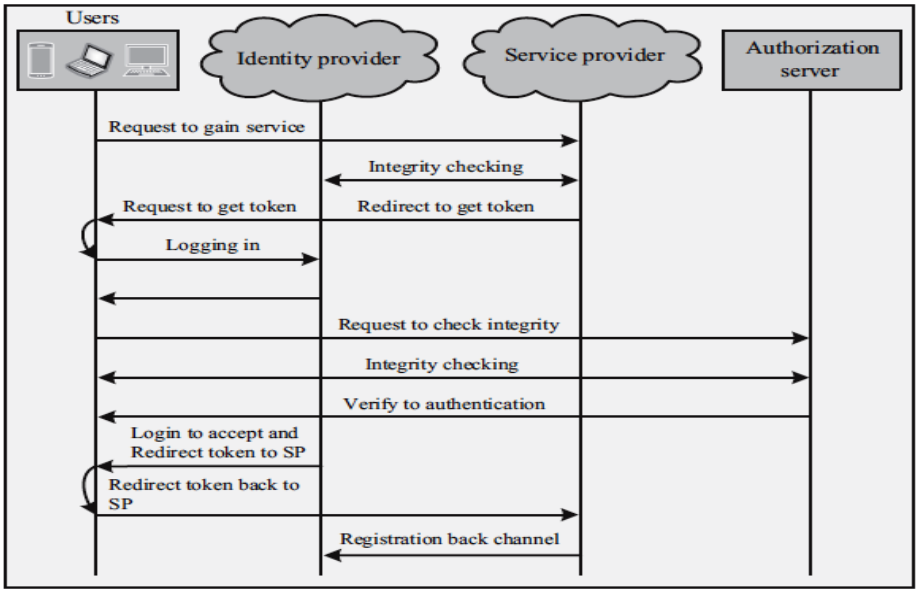

Fig. 3. The SSO architecture workflow in the cloud environment context [15]

4.3.2 OpenID

An authentication protocol that it is also an open standard is called OpenID. It enables the authentication of users to the relying parties (RP) through the support of third

party organizations. ”A relying party (RP) is a resource provider which could be a website or application that requires the end-user verification” [1]. OpenID [14] is based on SSO services’ features, therefore this enables the authentication to be performed using the credentials only once to authenticate and access multiple websites and web services [1].

It is a decentralized authentication system. OpenID does not need the administration by webmasters. The users’ list is stored in the OpenID provider. Then users create their accounts with the support of the provider’s list. The cloud users through their accounts can sign in (access) any website that enables OpenID authentication. OpenID Connect (OIDC) is the latest version of the OpenID mechanism. It is built as the identity layer based on the OAuth protocol. The authentication mechanisms for cloud and mobile applications are supported by the OpenID Connect protocol. In the case of communications between the cloud interaction parties, OpenID Connect enables their encryption and sign in [1].

4.3.3 OAuth

OAuth is an authentication mechanism used in cloud computing and it enables one-way or mutual authentication in the cloud environment. This is also an open standard that allows delegating and granting access to the user on another application/service without distributing the password by the authenticated service/application. OAuth 2.0 is the latest version of OAuth [1].

Using of OAuth authentication standard undoubtedly provides favorable authentication options, as in the case where users can exchange private resources which are usually stored on a secured resource server. In this case, the user’s credentials are not exchanged. The OAuth's goal is to complement OpenID and delegate access for users/services to the protected resources. This part is enabled through the authorization server, which usually generates tokens do not contain information about user credentials [15].

OAuth as an authorization framework enables third parties to access user/service resource without revealing the username and password to the third party service. For example, the user uses HP's SnapFish service to print photos online, and he/she may authorize this service to access his/her Facebook account images without granting his/her SnapFish his/her Facebook account password. OAuth can execute the restrictive policies in access domain and token expiration for restricting clients/services access to specific resources and functions for a certain time period. The need to integrate APIs and cloud services and their prevalence in cloud environment has made it necessary to use a common protocol for delegating authorization [21].

OAuth is being used as a security layer and standard protocol in the cloud computing. For example, we have a cloud image-storage service and an image printing service and we want to print the images (photos) that we have stored in the cloud storage service. An API is used for communication between cloud printing service and cloud storage service. The two services mentioned above operate in various companies, so our storage service account has not connection with our printing service account. In this case, OAuth is considered as a solution to this problem by enabling us to delegate access to our photos to various services, without providing our password to the photo printer. The OAuth system consists of four major actors such as: the client, the au-

thorization server and the protected resource. In this example, the OAuth client is considered the printing service, while the photo storage site represents the protected resource. The end-user is identified as the resource owner, who wants to print its photos. For its protected resources, the photo storage site runs using its in-house authorization server [22].

4.3.4 SAML

Security Assertion Markup Language (SAML) [13] is an open standard mechanism that enables communication and exchange of authentication and authorization resources between two interacting parties. Its mechanism operates according to the request and response techniques based on the token. Service provider and identity provider are two interaction parties. SAML assures that user authentication with service provider to be performed securely. No user credentials are included in tokens of the SAML. It also enables data communication to be encrypted and encoded between two interaction parties (the identity provider and the service provider) [1].

SAML takes care and enables secure authentication of the user in the service provider. SAML supports the SSO specifications and it enables interoperability based on this mechanism. It includes several roles such as user, identity provider and service provider. The user requests a web service from the service provider, which requests and receives assertions of authentication from the identity provider. The service provider decides about the access privileges/permissions based on the received assertion [1].

5 Cloud computing authorization mechanisms

Authorization is considered as a systematized mechanism from the cloud system that determines the access level of authenticated entities in secured resources [2, 15]. Authorization presents a method that permits or prevents the access to a specific resource based on the rights (permissions and privileges) of the authorized entity. There is a system administrator who monitors the access permissions in systems where entities (users/services) have permission to access. Since the cloud network is made up of various service providers, there are situations where the user can access different types of services at a specific time; each service that is provided by the specific service provider may have different levels of security [1].

There are cases when the authorization rights are managed (granted) by third-party organizations, which are authorized to have access to specific private information about services or applications as shown in Fig. 4 [1]. For example, if the application (service) is authorized by the user, then the application (service) hosted in the cloud can be accessed outside of it. In this case, the authorization is performed through the delegation of access privileges or access control policies. The cloud service provider provides and applies access control policies for services and resources where their access is only available to the authorized users/services [1, 6].

The protection of confidential information, minimization of management and security tasks are several benefits of the centralized authorization mechanisms. Nevertheless, there are authorization mechanisms like MAC, DAC, RBAC and ABAC and

they are shown in Fig. 4 [1, 6]. These mechanisms are discussed in the subsections of this section.

5.1 Mandatory access control

Mandatory Access Control (MAC) [16, 23] is the conventional mechanism for determining users' access privileges (rights) as is shown in the Fig. 4. The permission for accessing is granted by the MAC via the operating system or security kernel. The MAC controls the capability of data owners for permitting or rejecting the access rights to the customer for a file system [9]. In this mechanism are decided the access control rights by the system manager, while the operating system or security kernel enforce them. In MAC, the objects of the file system are classified according to sensitivity labels as secret, top secret or confidential. Each device or client is also classified according to the above mentioned levels [11].

The operating system or security kernel is responsible for controlling the username and password for persons or systems when they access specific resources. They are also responsible for specifying the access rights for parties (person or device) who access or attempt to access. Although the MAC provides a lot of security in resource access, the right planning and frequent monitoring are key factors that must be considered to hold classification labels updating [1, 6, 17].

The MAC must have a central authority to define what resources will be accessible and who can access resources [18]. For example, a company manager wants to access the resources of a company staff member. Full access to all staff member resources should not be allowed to the manager, because if s/he has full access, s/he can access and disclose sensitive resources such as the details of the bank accounts of the company staff members. While cloud computing uses web applications to provide its services, MAC needs to sophisticate semantic models for cloud security because there is a lack of them, especially in representing and communicating the privileges and restrictions that are enabled through access control policies.

5.2 Discretionary access control

Discretionary Access Control (DAC) [23] also known as Identity-Based Access Control (IBAC) [11], is a mechanism for security access control that controls the access permissions via the data owner, as is shown in the Fig. 4. In DAC, any user's access rights are completed through authentication by validating the credentials (username and password). DAC is considered discretionary since owner specifies access rights. File/information or resources possess the owner in DAC, while the resource owner controls the policies of the resource access. Nevertheless, the DAC mechanism offers more flexibility than the MAC mechanism, while it has less security compared with MAC [1, 6, 23, 24].

The DAC can also be used in cloud computing, but it presents side effects, despite the DAC is influenced on authorizing of objects' owners to check permissions of access to objects. For example, if there were any mechanism or technique to enable the administration of inappropriate rights (risk awareness) that object owners could

provide to users, it would be an extraordinary element for the DAC. Unfortunately, such a feature does not exist in the DAC [18].

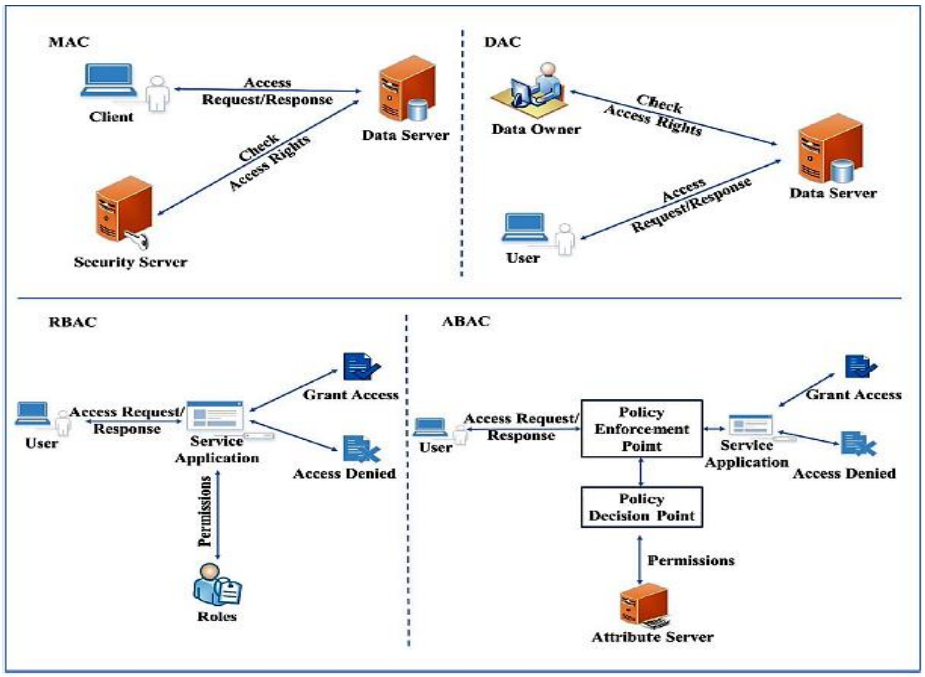

Fig. 4. Comparison of the authorization mechanisms in cloud computing [2]

Sometimes, users/services are requested to utilize privileges that disclose resources for entities to third parties. For example, when the employee has to read the contents of a file in the company where it works and then it copies the contents of the file to another file and transfers it to another employee. The DAC have not the authority to control the flow of information or deal with malicious content that may be carried as a result of access permissions. Besides the above case, the possibility of transferring rights of the user/service to another is presented as a problem in the DAC and as a consequence the integrity and confidentiality of the objects can be violated [18]. It means that the DAC is not scalable enough for using in cloud computing.

5.3 Role based access control

This is an access control mechanism briefly referred as RBAC [23] allows access rights for users according to roles and permissions (Fig. 4). The policies of access control present rules that tell how the setup process authorization allow or deny users [11]. The user is defined as a human, process, machine or network. A role presents the approval for performing an object operation, which can be an action, function or duty that user should be done. The object is another term that is included in RBAC, which it refers information containers such as files, directories, databases' table or resources

(printers, PC, etc.). The permission is defined as a 'tool' that enables the user to assign roles is actually active along to user sessions. Permission as a part of RBAC model has functions to analyze a set of users, which they want to assign a role or a set of roles [9].

In RBAC, user permissions are provided by different parameters and they can be as user-roles, permissions of roles, and role-role relationships. Roles in RBAC are divided into two categories, namely as application/technical role and organizational/business role. The application/technical role involves the combination of various application/service specific rights or tasks that have elements of permissions, specifically based on permissions. Its domain is restricted to the specific applications. The organizational/business role consists of various job functions and the rights of access allocated for employees. It consists of combining various application/technical roles. In organizations that have many users and required multiple permissions, RBAC is used to administrate their security [1, 6, 17].

The RBAC mechanism has advantages and disadvantages in comparison with the DAC and MAC mechanisms. Selecting the proper roles that represent the cloud system is not a simple duty and categorizing of entities based on roles can make things problematic. In the RBAC mechanism, roles categorize (rank) the subjects into a variety of categories. Therefore, each entity (subject) must have a role to enable access the cloud system. Nevertheless, roles sometimes give the subject more rights than are necessary to it, so this can lead to the abuse and infringement of the access security policies [18].

It must ensure that access decisions are made within a reasonable period of time and based on system requests before using the RBAC in cloud computing. For instance, the response time is essential for a lot of applications by including even the health care system. The system must be accessed in a timely way by a remote consultant from a hospital by ignoring an amount of RBAC and distance access requests. There may be critical infrastructure of service provider who wants to migrate to cloud computing. It can have many users, dozens of roles, thousands of permissions. Such infrastructure can be faced with enormous tasks which cannot be centralized by small groups of security administrators [18].

The cloud system consists of a sequence of operations that must be controlled. Each operation requires various sets of permissions. Therefore, the RBAC may not be able to provide access to a series of operations in cloud computing.

5.4 Attribute based access control

Attribute-Based Access Control (ABAC) [23] is considered as a mechanism that is needed to control the access permissions as shown in Fig. 4. This access control mechanism uses its policies to define various sets of attributes that needed to control the user access rights separately [11] as depicted in the Fig. 4. The policies are mainly created through various types of attributes. The system is based on these policies and decides the access permissions. Here includes a series of attributes which are subject attributes, object attributes, resource attributes and environmental attributes. Under the ABAC mechanism, each user's roles and permissions/privileges are predetermined. This model enables the solution of many issues of authorization, ensures suc-

cessful regulatory enforcement and enables flexibility in implementation [1, 6, 25, 26].

The starting date of the user's work, his location, the user role, etc. can be attributes. Attributes are first determined to be used in the system, and then each attribute is accounted as a discrete value. These values are then compared to the set of values from the policy decision level to allow or deny access. In addition, a subject does not need to be identified preliminary to the system. It must once be authenticated in the system and then ensure its attributes. Nevertheless, an agreement must be reached to know what type of attributes should be utilized and how many of them are taken into consideration to create access decisions. Such an issue is considered quite complicated in cloud computing [18].

It is necessary to propose a security policy which can work exactly with the ABAC model in cloud computing, due the security policy is accountable for picking the substantial attributes that are used to create access decisions.

6 Discussion

The paper provides a comprehensive overview of the service authentication and authorization as an essential part of the cloud computing architecture. It is primarily concerned with the surveying of recent technological and techniques' developments in these fields. This analysis is concentered on each mechanism of authentication and authorization in cloud computing architecture by outlining their advantages and disadvantages.

7 Conclusion

The cloud service is considered as an important digital solution because it reduces the capital and operational services of the organization. Security risks and threats are major concerns of the cloud computing because its nature is multi-tenant and third party delegation to maintain the environment of this technology. This study has analyzed and surveyed current security issues, access control mechanisms and potential mitigations involved in cloud services, with particular emphasis the technologies and mechanisms of authentication and authorization needed to manage access, security and services in the cloud environment. It discusses different topics about authentication and authorization mechanisms and main aspects related to each mechanism in the cloud computing.

The survey of the various authentication and authorization mechanisms, their cloud-related architecture, and the different services offered by this technology highlights the need to improve existing authorization and access management models and authentication services. According to the researched literature, we have found that the RBAC model is considered as the most used authorization and access control mechanism. MAC and DAC are the most reliable mechanisms among the systems that are examined. They are not so preferred to be used as a single due to the flexibility of MAC and the low security that DAC has compared to MAC. The described authentication technologies and mechanisms can be appropriately combined to provide better

security or a secure authentication method can be developed for effective authentication in cloud computing. The appropriate and secure authentication and authorization mechanisms and protocols for cloud systems are suggested to be designed and developed in the future to improve the effectiveness of these domains in terms of cloud service security.

References

1. Indu, I., Anand, P. R., Bhaskar, V. Identity and access management in cloud environment: mechanisms and challenges. Engineering Science and Technology, an International Journal, Elsevier 21 (4), 574-588, 2018.
2. Ayo, I.O., Ajayi, O., Misra, S. Cloud computing security: issues and developments. In: World Congress on Engineering, pp. 175-181. International Association of Engineers (IAENG), London (2018).
3. Mahmoud, M. S., Xia, Y. Cloud computing. In: Networked Control Systems - Cloud Control and Secure Control, pp. 91-125. Butterworth-Heinemann & Elsevier (2019).
4. Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., Basu, K., Chaudhury, S., Sarkar, P. Cloud computing security challenges and solutions - a survey. In: 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 347-356, IEEE, Las Vegas, NV, USA (2018).
5. Aldossary, S., Allen, W. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications 7 (4), 1-14 (2016).
6. Tabrizch, H., Rafsanjani, M.K. A survey on security challenges in cloud computing: issues, threats, and solutions. The Journal of Supercomputing, Springer 12 (2020), 1-40 (2020).
7. Chaimaa, B., Elkamoun, N., Hilal, R. Cloud computing: overview and risk identification based on classification by type. In: Cloud Computing and Big Data: Technologies, Applications and Security. 1st edn, vol. 49, pp. 19-34. Springer International Publishing, Rabat (2019).
8. Ayo, I. O., Ananya, M., Agono, F., Worlu, R. G. Cloud computing architecture: a critical analysis. In: 18th International Conference on Computational Science and Applications (ICCSA), pp. 1-7, IEEE, Melbourne, VIC, Australia (2018).
9. Sifou, F., Kartit, A., Hammouch, A. Different access control mechanisms for data security in cloud computing. In: International Conference on Cloud and Big Data Computing (ICCBDC 2017), pp. 40-44, ACM, London, United Kingdom (2017).
10. Tsai, W. T., Sun, X., Balasooriya, J. Service-oriented cloud computing architecture. In: Seventh International Conference on Information Technology: New Generations, pp. 684-689, IEEE, ACM, Las Vegas, NV, USA (2010).
11. Sibai, R. E., Gemayel, N., Abdo, J.B., Demerjian, J. A survey on cccess control mechanisms for cloud computing. Transactions on Emerging Telecommunications Technologies (ETT) Journal, Wiley 31 (2), 1-21 (2019).
12. Khan, M. A. A survey of security issues for cloud computing. Journal of Network and Computer Applications, Elsevier 71, 11-29 (2016).
13. Chaimaa, B., Najib, E., Rachid, H. A secure authentication model for cloud federation. International Journal of Computer Science and Network Security 17 (10), 89-94 (2017).

14. Hasan, M., Riaz, H., Rahman, A. Authentication techniques in cloud and mobile cloud computing. International Journal of Computer Science and Network Security 17 (11), 28-39 (2017).
15. Rashidi, B. Authetication issues for cloud applications. In: Authentication Technologies for Cloud Computing, IoT and Big Data, vol. 9, pp. 209-240. The Institution of Engineering and Technology, Herts (2019).
16. Lim, S. Y., Kiah, M. L. M., Ang, T. F. Security issues and future challenges of cloud service authentication. Acta Polytechnica Hungarica - Journal of Applied Sciences, IEEE Hungary Section 14 (2), 69-89 (2017).
17. Harnal, S., Chauhan, R. K. Efficient and flexible role-based access control (EF-RBAC) mechanism for cloud. Endorsed Transactions on Scalable Information Systems Jurnal 7 (26), 1-10 (2019).
18. Younis, Y. A. , Kifayat, K., Merabti, M. An access control model for cloud computing. Journal of Information Security and Applications, Elsevier 19 (1), 45-60, (2014).
19. Babaeizadeh, M., Bakhtiari, M., Mohammed, A.M. Authentication methods in cloud computing: a survey. Research Journal of Applied Sciences, Engineering and Technology 9 (8), 655-664 (2015).
20. Zuccherato, R. Challenge-response protocol; identity verification protocol. In: Encyclopedia of Cryptography and Security. 2nd edn. Springer Science and Business Media, Boston, MA (2011).
21. Ferry, E., Raw, J.O., Curran, K. Security evaluation of the OAuth 2.0 framework. Information and Computer Security Journal 23 (1), 73-101 (2015).
22. Richer, J., Sanso, A. OAuth in action. Manning Publications Co., Shelter Island, New York (2017).
23. Kayes, A. S. M., Kalaria, R., Sarker, I. H., Islam, S., Watters, P. A., Ng, A., Hammoudeh, M., Badsha, S., Kumara, I. A survey of context-aware access control mechanisms for cloud and fog networks: taxonomy and open research issues. Sensors 20 (9), 1-34 (2020).
24. Karataş, G., Akbulut, A. Survey on access control mechanisms in cloud computing," Journal of Cyber Security and Mobility 7 (3), 1-36 (2018).
25. Joshi, M., Joshi, K. P., Finin, T. Attribute based encryption for secure access to cloud based EHR systems. In: 11th International Conference on Cloud Computing, pp. 932-935, IEEE, San Francisco, CA, USA (2018).
26. Shen, J., Zhou, T., Chen, X., Li, J., Susilo, W. Anonymous and traceable group data sharing in cloud computing. Transactions on Information Forensics and Security, IEEE 13 (4), 912-925 (2018).