International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3404-3414
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3404-3414

A Novel Hybrid Approach for Access Control in Cloud Computing

Sara Alayda, Najad.A. Almowaysher
[1,2] *College of Computer and Information Sciences, Jouf University, Saudi Arabia.*

Mamoona Humayun
[3] *Department of Information systems, College of Computer and Information Sciences, Jouf University, Saudi Arabia. ORCID: 0000-0001-6339-2257*

NZ Jhanjhi
[4]*School of Computer Science and Engineering (SCE), Taylor's University, Malaysia. ORCID: 0000-0001-8116-4733*

Abstract

Access control is essential to protect data and system resources by preventing unauthorized access. Cloud computing ensures that users get benefit from such resources by following their requests. Hence, users can access applications, programs, and storage. Data security is a significant concern to be dealt with in the cloud computing area. The dispersion of data across multiple storage devices in cloud computing and abundant access from heterogeneous devices pose serious security threats. Therefore, the protection of data and resources using proper access control mechanisms is a critical task for cloud service providers. Various access control approaches and models for cloud computing have been suggested in existing research , however; security breaches in these approaches cause great threats for cloud service providers. Based on the analysis of existing works, we proposed that the combination of multiple approaches is the best solution to ensure access control according to users' requirements and to the network conditions. Hence, concerning the analysis conducted on related works, we propose a hybrid approach based on the Attribute-based-Access-control and Role-Based-Access-Control models. Our approach combines the best features of these models and ensures both security and flexibility. Compared to the conventional models, the proposed approach defines different security levels via the assignment of a different number of attributes for each role by guaranteeing the least privilege concept.

Keywords - Access control, Cloud Computing Security, Attribute-based access control (ABAB), data security, Role-based access control

I. INTRODUCTION

Cloud computing (CC) is the accessibility of computing resources on demand, especially data storage (cloud storage) and computing power, without the user's direct active management. In general, the term is used to describe data centers accessible over the Internet to many users [1, 2]. Large clouds, prevalent today, also have functions spread from central servers over several locations. However; despite the abundant benefits of CC and quick paradigm shift from traditional computing to CC brought lot of challenges and one of the important challenge is Access control (AC). AC or authorization permits the control of access to information, resources, and systems. AC mechanisms aim to indicate about what particular resources users are allowed or authorized to access [3-5]. To achieve that control, each entity attempting to gain access must be authenticated before providing access to it so that only authorized user could access the data. Consequently, it will save the computing resources from unauthorized users' attacks and will prevent security problems [6-8].

The cloud is a virtual space in which it is possible to place, in a virtual manner, a server, network infrastructures, execution platforms, and services. CC is an effective way to produce and consume computing with a set of resources that are provided in the form of on-demand services: SaaS, PaaS, and IaaS. There are many advantages of migrating to CC, such as automation, easy maintenance, efficiency, cost control, energy-saving, and great agility in software deployment [9, 10]. However, Cloud computing can only keep all of its promises if it assure a high level of security, accessibility, and availability. Authentication and authorization are the key terms used in the context of well-protected cloud access. Cloud security concerns are very crucial as huge number of individuals as well as companies use to store sensitive personal data and large quantities of projects on Cloud. Among the different cloud topologies, the public cloud is the most demanding in terms of security and should be managed with reasonable care [11, 12].

The idea of the Cloud is to share physical resources between untrusted tenants. This feature presents a real challenge for access control mechanism of CC. In addition, the cloud services are in general heterogenic, which requires variable degrees of granularity in access control mechanisms. Therefore, if the access control mechanism is not efficient or untrustworthy, it will increase the risk of using cloud resources and services illegally by unauthorized users. Consequently, managing identities and access to cloud services is one of the primary security concerns. Hence, it is primordial to conceive flexible access control mechanisms to avoid unauthorized access [13, 14]. Figure 1 shows how access control is managed in CC, it shows that the data owner sends it encrypted data to the cloud server. Once a user tries to access this data, the identity of this user is checked to verify whether it is an authorized peer or not. The data owner checks the AC policy according the used AC model. If the user has an authorization, the data owner sends him keys and certificates. The user on his turn will send certificates to the cloud server which sends back the data in an encrypted form. Finally, the user uses the received key to

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3404-3414
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3404-3414

decrypt data.

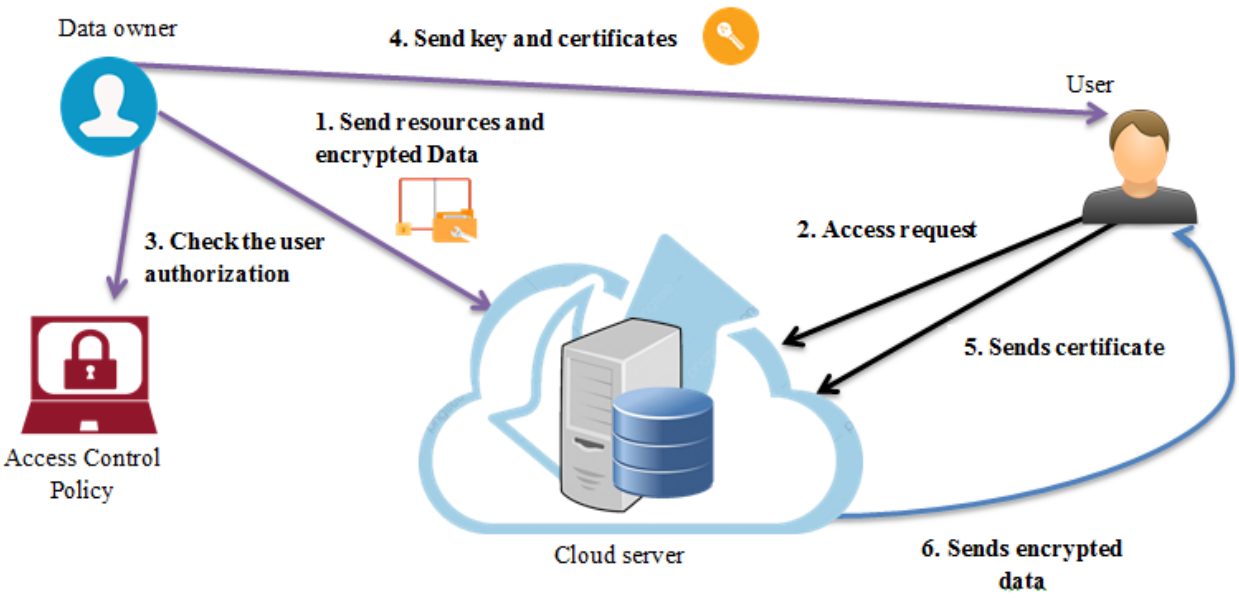

Figure 1: Access control in cloud computing

This paper mainly focus on access control, as it is essential to preserve the security in CC. In literature, different AC models were proposed for proper AC in CC. A good AC mechanism should address some key requirements which include availability, dynamicity, scalability, flexibility, quality of services, and computational costs [15, 16]. In this work, an access control mechanisms for cloud computing is proposed with the aim to address key security features. The proposed hybrid mechanism combines the best features of commonly used existing models namely ABAC and RBAC. Our hybrid approach is based on the assignment of attributes to roles, thus several security levels are engaged in our model. Further details will be given in next sections. For the sake of understanding, Table 1 presents abbreviations used in this work along with their explanations.

Table 1. Abbreviations and their explanations

Abbreviation	Explanation
DAC	*Discretionary access control*
MAC	*Mandatory access control*
ARBAC	*Attribute role based access control*
ABAC	*Attribute-Based Access Control*
CBAC	*Coalition based access control*
RBAC	*Role based access control*
CSP	*Cloud service provider*
ABE	*Attribute-Based Encryption*
AC	*Access Control*
ACP	*Access Control Policy*
CA	*Cloud Application*
CACE	*Context-Aware Access Control Engine*
CC	*Cloud Computing*
CC-CPS	*Cloud Connected Cyber Physical Systems*
CMM	*Cloud-Assisted Mobile Multimedia*
CPABE	*Cipher Text Policy Attribute Based Encryption*
CSP	*Cloud Service Provider*
E/D	*Encryption/Decryption*
FAP	*Fine-Grained Access Policy*
HCI	*Heterogeneous Cloud Infrastructure*
IC	*Intermediate Cipher Text*
MC	*Mobile Cloud*
PEKS	*Public Key Encryption Keyword Search*
RAAB-AC	*Role-Attribute Assignment based Access Control*

The remaining of this paper is structured as follows. Section 2 presents overview of existing AC approaches, and also provide a comparison that highlights the main differences between these approaches. Section 3 discuss our methodology along with proposed model. Section 4 discuss the proposed solution and compare it with existing ones. Section 5 concludes the paper by providing directions for future research.

II. LITERATURE REVIEW

AC is crucial for the success of CC, various solutions have been provided in existing literature that address the issues of CC security. Below we discuss some latest studies that propose access control approaches for CC.

In the domain of CC-CPS, authors in [17] introduce a novel industrial architecture based on the combination of several AC models for cloud technologies. Authors claim that CC improves CSPs' efficiency and reliability by enhancing the connectivity and integration between computational and physical industry elements. The main focus of the paper is security CC-CPS and authors proposed a solutions for this issue by extracting a set of requirements for AC. Moreover, they conducted a comparison between AC models. The comparison aims to classify models suitable for varied scenarios across various indicators. A compromise between effectiveness and security is reached by this method. Requirements of access control for CC-CPS were also discussed such as: dynamicity, scalability, transparency, quality of service, and flexibility. Further, this paper emphasizes that AC's solutions must identify all the possible variation of requirements related to the type of business network and organization. Thus, they deduced that conventional models are unsuitable because they lack heterogeneity. According to authors, one single model does not fulfill all the requirements needed in cloud-industry environment. Therefore, they propose to combine multiple access solutions. However, the main shortcoming of this method is its complexity, especially for distributed networks. Furthermore, this work proposes an architecture for industry while smart manufacturing's modular characteristics must be considered.

In the MC computing area, authors in [3] propose to use mobile devices dynamic attributes to secure AC's protocols and systematically provide confidentiality. For this purpose, the exchange of secret keys was performed using the anonymous key-issuing protocol to keep the identity of the user private. Authors are motivated by the fact that security vulnerabilities are higher when the stored data is accessed via smart devices. Meanwhile, data confidentiality is not ensured in CC because a third-party storage entity handles it. In order to guarantee AC and confidentiality, authors focus on ABE cryptographic method. This method is used in MC where data is stored using FAPs. Hence, access privileges must be accomplished before getting authorized access. Authors propose an AC method based on multiple authorities ABE. They put forward an ACP associated with multiple dynamic attributes that were gathered from mobile devices. To evaluate their method, the solution was implemented in a real MC environment. According to experiments' results, the approach improves performance and sustains secure communication without disruption. However, since this method is based on mobile devices, the constraints related to these entities must be considered, such as computational and memory capabilities. Hence, the collection of dynamic attributes used for accessing the cloud and encryption algorithms must be adapted to preserve devices' life time.

Another solution for MC is proposed in [18] to preserve CMM data sharing systems' privacy. Authors propose a schema to secure the exchange of ACP and multimedia data with minimum computation cost, using two modes of encryption: off-line and online. The encryption based on attributes is an optimal solution to reinforce AC over encrypted data in CMMs. Thus, the proposed schema is based on CPABE. However, because the access control policy is sent without encryption, the user's privacy can be violated by non-authorized peers. Further, mobile devices cannot handle the frequent E/D operations required for CPABE. For these reasons, authors separated the encryption process; an IC is prepared for the off-line mode. When receiving specific ACP requirements, the final version is extracted from IC into the online mode. Noting that, authors used a novel format of CPABE attribute, each attribute is presented with two parts: a name and a value. The value is encrypted and sent as the cipher-text while the name is used to identify the ACP. Nevertheless, the generation of IC is a complicated task because of both the size and the structure of the text's descriptors. Unlike the cloud with very rich computing resources, a large number of attributes can cause tedious decryption overhead for mobile devices with limited computing resources.

Cloud computing based on AC attributes was discussed in [19]. The authors introduce their solution as a combination of RBAC model and PEKS. The proposed schema called R-PEKS resolve the problem of high computational cost caused by pairing-based cryptography used with PEKS. Unlike classic threat models, authors assume that CSP and users are all honest yet curious. They exclude the bilinear mapping from their model and implement AC according to three cases: a single user, peer to peer multi users, and a group of multi users. Further, authors assume that RBAC model is the best way to ensure security for multi-user applications where users' permissions can be updated regularly. Regarding evaluation, the R-PEKS model is 97% more efficient than the classic model, with the same security level. However, as the authors mentioned, requirements and the users' permission are frequently updated, but RBAC model is not able to achieve the granularity of data access unless the initial architecture is modified. Additionally, assignments of dynamic users' permissions are not handled.

Regarding security provision for cloud data, an AC mechanism for cloud storage based on hybrid security was proposed in [20]. This work presents a cost effective and credible data hosting system. This system provides a distributed data hosting architecture in HCI. Authors discussed different security mechanisms for securing cloud storage. Their mechanism ensures applicability and efficiency and focuses on access pattern costs during the data migrating within the cloud environment. Study results prove to be effective in terms of key management and cryptographic mechanisms.

In [6], authors considered alleviating CC's security concerns regarding protecting their critical sensitive data and operations. They proposed a security-by-design framework that facilitates the design and implementation of ACPs for developers by safeguarding their data against unauthorized accesses. The framework is a generalization of a previous work proposed in [21]. In [21], the authors proposed an ontology model for ACP that captures the concepts related to contextual attributes for ABAC scheme. This model permits to extend and instantiate the knowledge related to policy for making it suitable to any particular CA prerequisites, independently from the code employed by the application. The authors identified several

shortcomings in the ontology model; therefore, they extended this model to support the ability to relate a relevant entity with a context and to allow stakeholders to define rules and the structure by which their ACP must abide. The authors also implemented a CACE and enhanced it with the capability of reasoning. However, the authors failed to evaluate and demonstrate their framework efficiency. It is, therefore, difficult to draw any conclusion on the performance of this work.

In [22], the authors considered the problem of ensuring confidentiality in CC databases. The CC databases can be accessed anywhere at any time. It is, therefore, imperative to protect the data from been altered or accessed by unauthorized users. The authors proposed in this work a model based on an enhanced encryption algorithm (RSA), they combine this algorithm with RBAC model to guarantee the confidentiality, integrity, and proper AC. They showed that their model can achieve E/D lower costs and execution time than simple RSA. The simulation experiments showed that the proposed AC model is more advantageous than the traditional RBAC with increased throughput. The authors concluded that their model has more secure permission granting mechanism that can improve CC data security. It is worth noting that the authors have compared their work with simple algorithms and methods without investigating similar recent works in the literature. Therefore, it is not possible to ensure the true effectiveness of their approaches compared to the literature. Table 2 presents a comparison of studies discussed so far

Table 2 Comparison between related works

Paper	Type	Access control mechanism	Pros	Cons	Limitations
[17]	Journal paper: Computer Networks (2018)	Combination of multiple access control such as RBAC and UCON.	Identification of the important access control requirements for industry in the context of cloud-connected CPS. Assessment of the adaptability of each of these models.	Further characteristics must be added to this analysis such as the specific smart manufacturing characteristics.	The complexity enforced by the combination of multiple access models.
[3]	Journal paper: Pervasive and Mobile Computing (2019)	Multiple Authorities Attribute-Based Encryption	The cloud server and the client can securely communicate without interruption via the pairs of mobile agents. The approach is employed in a real-world scenario in the context of MC environment.	Mobile devices constraints were not considered in this method such as the battery life time and the complexity of encryption algorithms	The impact of the constrained nature of mobile devices must be evaluated.
[18]	Journal paper: IEEE Access (2019)	A sharing scheme of cloud-assisted mobile multimedia data based on CPABE	The proposed model preserves the ACP privacy. Preserves the security of multimedia data shared in MC.	The number of attributes can pose complexity problems when producing IC	The decryption in the user side and limited computation resources of mobile devices must be taken into consideration.
[19]	Journal paper: IEEE Access (2019)	Role Based Access Control (RBAC)	Provides hosted data confidentiality. Ensure secure AC	The assignment of dynamic user-permissions are not taken into consideration	The granular data access is not completely ensured by RBAC model.
[20]	Conference paper (2019)	Unspecified	Provide security for AC of cloud storage. Efficient in terms of key management and cryptographic mechanism.	The proposed mechanism does not deal with the dynamism caused by the cloud clients and the changing privileges	This work does not provide all the needed AC requirements for CC such as flexibility and scalability.

Paper	Type	Access control mechanism	Pros	Cons	Limitations
[6]	Journal paper: Future Generation Computer Systems (2019)	Attribute-Based Access Control (ABAC)	Securing CA's ACP by safeguarding their data against unauthorized accesses. Implementation of a CACE enhanced by capability of reasoning.	The authors failed to evaluate and demonstrate the efficiency of the proposed framework	It is hard to draw conclusions on the performance of this work.
[22]	Journal paper: Journal of Information Processing Systems (2019)	Role-Based Access Control (RBAC)	Achieve better E/D in terms of execution costs and time. The updated AC model has more secure permission and guaranteed mechanism which improves data security in CC.	Authors have compared their work to simple algorithms and without investing in similar recent works.	The efficiency of the proposed model is not proved

III. RESEARCH METHODOLOGY

This section presents a comparison between the most relevant models used so far to ensure access control in cloud computing. In what follows, we introduce the following AC models: DAC, MAC, RBAC, CBAC and ABE.

Discretionary-Access-Control Model (DAC)

In DAC models, the ACP is based on the concept of subject, action, and object. Subjects represent the system active entities that are generally the users; objects represent the passive entities or the data. The actions that define the direct access that the subjects can perform on the objects. DAC models are qualified as discretionary because the permissions refer directly to a particular user; they support the notion of user group, which simplifies the management of authorizations (the permission granted to a group is automatically applied to its members.). They also include the notion of proprietary rights which gives users the privilege of administering the access control regulations that apply to their data. Hence, the object owner defines the users' privileges and allocates the amortization of access to them. When using group of users, an object owner can control the group and gives permissions to its members [23, 24].

Nevertheless, such an approach may cause security issues when the object owner is not trustworthy. Thus, he can change the SP using malicious software, such as Trojan horse. The management of security in DAC models is not evident; its main shortcoming resides in the fact that it does not control the flow of information. The lack of copy privileges and constraints lacks in DAC models prevents information verification. Hence, an object can copy information to another one that has not an access authorization. The security problems related to DAC models motivated the researchers to replace it with MAC [25, 26].

Mandatory-Access-Control Model (MAC)

Unlike DAC models, MAC models fall into the category of flow-control models since the only way to fully guarantee multi-level security is to control all possible information flows. In MAC models, a security level is assigned to each subject (authorization level) and to each object (classification level). The security policy is mandatory. That is, it is binding on all users and cannot be changed. In this type, two AC properties must be applied. The first is "No read up", which means that a subject cannot read an object classified at a level of confidentiality that is higher than the subject's authorization. The second is "no write down", meaning that a subject cannot write in an object classified at a level of confidentiality lower than the subject's authorization. By the mandatory nature of security regulations, MAC models are inflexible but provide a higher security level than DAC models [27, 28].

The MAC model is characterized by its simplicity and high security. The prohibition of unauthorized users from modifying information ensures transparency because it prohibits the flow of information between users. Nevertheless, MAC model does not guarantee the duty separation and the fine-grained AC. Additionally, MAC systems are difficult to use because they need an application for MAC properties and labels and their dependence on trusted components [29, 30].

Role-Based-Access-Control Model (RBAC)

The DAC and MAC models are not well suited to business organizations' needs that depend on users' role within the organization. As a result, RBAC models appeared and established themselves as an alternative to traditional DAC and MAC models. In RBAC models permissions related to tasks of an organizational nature such as purchase and transfer. Therefore, in this type, roles correspond to a professional function, and permissions are granted to the users' roles according to their responsibilities. The ARBAC model is a sub-model of RBAC. It is based on roles corresponding to the administrative functions for the safety regulations [31, 32].

Before introducing the proposed hybrid approach, we give a brief explanation of RBAC and ABAC's functioning. Regarding RBAC, users are assigned to one or more roles. When a new user joins a company, a particular role is assigned to him, noting that there is no need to withdraw the role from the policy if he leaves. However, each user must have an assigned role to be able to execute any action in the system. The main components of this model are: users, roles, objects,

permissions and operations [33]. A basic implementation of RBAC is shown in figure 2.

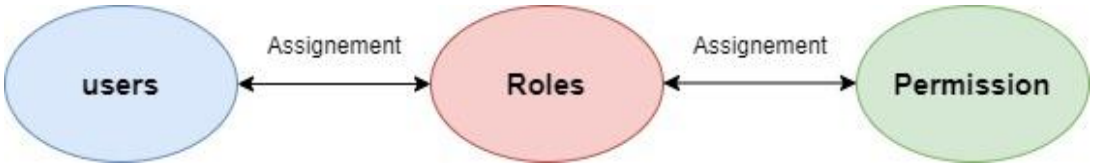

Figure 2. Basic implementation of RBAC model

The RBAC model is characterized by its ease of implementation, hierarchal framework support, duties separation, scalability and security. However, RBAC models' main shortcomings refer to its static nature; it cannot use contextual information such as location, time, and device type. In addition, similar to DAC model, it is an error prone model. This limit exacerbates when the number of entities is dynamic and large [32, 33].

Coalition-based-Access-Control Model (CBAC)

When the number of applications is large, the security policy can no longer be defined using static authorization rules. AC models, which allow the expression of dynamic rules (where the distribution of permissions depends on contextual conditions) belongs to the CBAC model family. An important feature of CBAC models is that they allow expressing authorization rules that do not require users to be authenticated. A user can obtain access to information simply because certain contextual conditions are met in such situation CBAC model is a suitable choice. In this model, permissions depend on Boolean conditions that apply to the subject, object, and environmental attributes. Each user is related with attributes associated to its group, role, or department. The Organization-Based AC (ORBAC) model is also considered as CBAC model. It is based on first-order logic to express contextual rules, and it integrates the administration model (ADORBAC) as well [34, 35].

Attributes-based-Access-Control Model (ABAC)

As mentioned above, ABAC is based on users and resources' associated attributes. It uses more developed attributes such as time, location, qualification… etc. In addition to users, subjects and objects, it contains users, subjects and objects attributes, policies of authorization, and constraint checking policies, and permissions. ABAC's advantages are multiple such as its ability to identify the accessibility of user according to the policies assigned to the application. The administrator of the system does not need to verify the account of users to assign roles or modify their AC list. Further, AC is made dynamically based on restructured policies [34, 35].

ABAC model establishes a set of attributes for each element (object/subject) in the system. The combination of user/object attributes is defined according to policy. The main components of this model are: attributes, subjects, objects, operations and policy. On the contrary of RBAC, ABAC incorporates attributes that are not yet recorded in the system but it needs more time and effort for the attribute definition [36]. An example of ABAC implementation is shown in figure3.

Despite its advantages, ABAC model suffer from some problems. In ABAC, requirements of authorization are coded as policies of authorization that are managed centrally. Thus, authorization requirements gathering and use case definition should be implemented in a new manner. Another issue is related to the complex ownership of authorization and the lack of auditability. Auditability defines which users can access resources; this feature is basically covered in the RBAC model. Though, in ABAC, it is complicated to provide this feature. Furthermore, the separation of duties is considered as a limit for ABAC. Unlike the RBAC model in which people cannot get conflicting roles provided by static duty separation, applying this feature for ABAC is more complicated. Finally, the problem of scalability is yet to be considered [37].

Attributes-based-Encryption Model (ABE)

To secure the sensitive data stored in third parties and safeguard it from any unauthorized use, data may be stored in an encrypted form. However, the sharing of encrypted data cannot be done at a fine-grained level. Therefore, the ABE model is

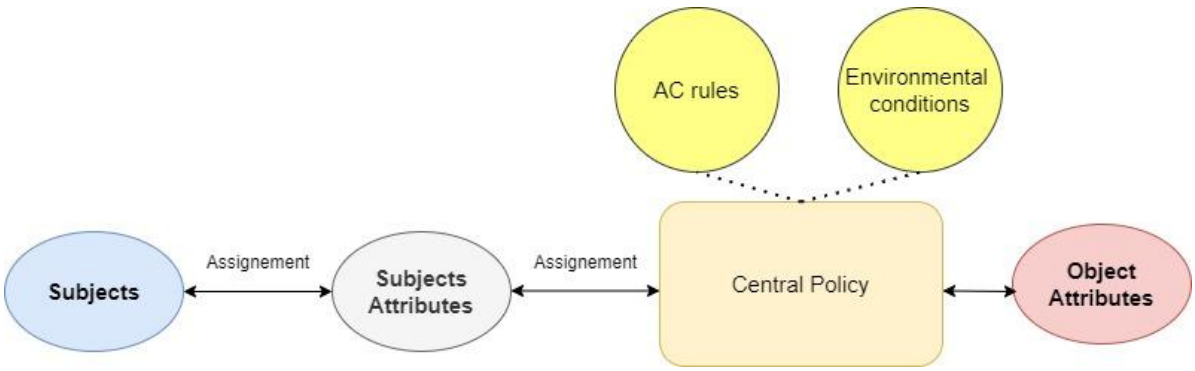

Figure 3. Implementation of ABAC model

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3404-3414
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3404-3414

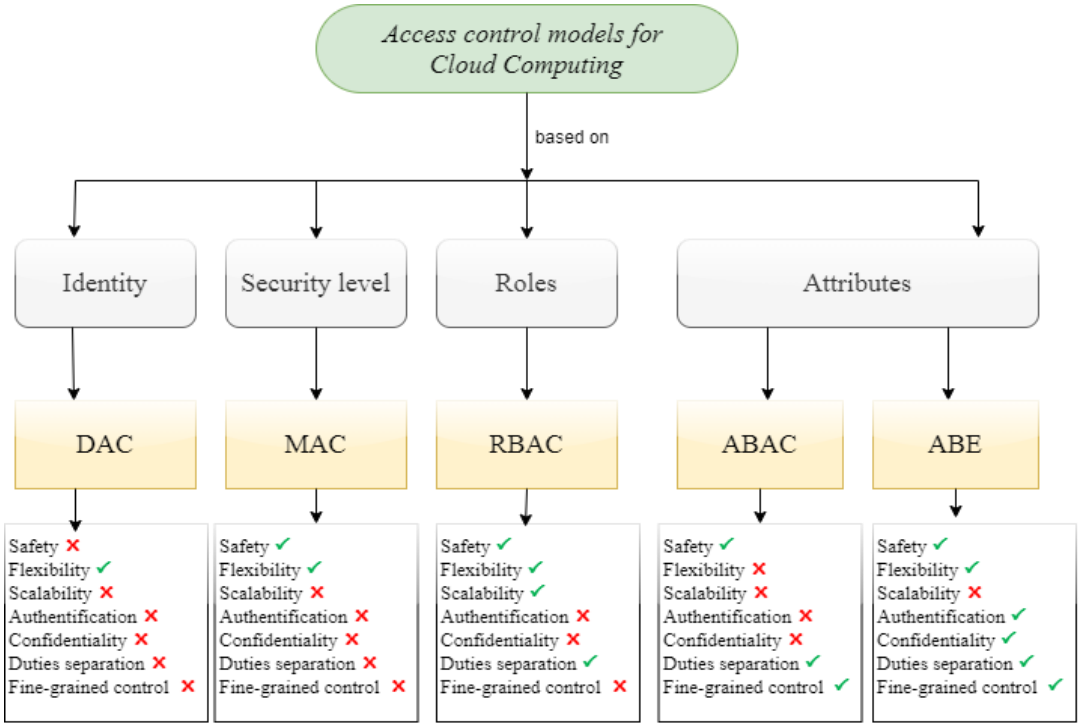

Figure 4. Comparison between AC models for cloud computing

created to perform the encryption and decryption of data using user attributes. The user identity is represented with its keys and the cipher texts nominated by the encryption party. Cipher text is decrypted with a key only if the cipher-text attributes and the user's private key attributes are matched. There are other variant of ABE model such as the cipher text-policy ABE (CP-ABE), the key policy ABE (KP-ABE) and the hierarchical ABE (HABE).

Based on the detailed analysis and study of above models, we propose an AC model based on ABAC and RBAC role model. Thus the concept of role is added to ABAC model. More details on the proposition are given in the next section. A comparison between the models mentioned above is presented in figure 4.

Proposed Model

Among all models presented in the previous section, we assume that RBAC and ABAC are the best methods to ensure efficient AC. Despite their several advantages, they suffer from certain limitations. Comparing these two models, RBAC is unable to provide flexibility and dynamicity such as ABAC. On the other hand, ABAC is unable to provide permission management simplicity and security such as RBAC [38]. Therefore, we assume that the best way is to combine these two models in order to benefit from the strengths of both of them. In this work, we propose a hybrid AC approach called RAAB-AC based on both RBAC and ABAC models. RAAB-AC refers to Role-Attribute Assignment based Access Control. As presented above, RBAC and ABAC may have some limits but, we assume that the merge of these two models is the best solution to ensure a simple, flexible, and robust AC model for cloud. The combination of AC models is considered efficient in several researches [39-41]. There are three different methods to combine these models:

Role centric: this approach constrains roles by relating attributes to them to minimize the available users' permissions. This method reinforces data security.

Attribute centric: a user attribute is added as role to identify attributes required for a certain role.

Dynamic roles: the subject role is identified using attributes like "time". Hence, dynamic attributes determine the user's role.

Our hybrid approach aims to combine the features of RBAC and ABAC, this is done in two ways. In the first phase, we propose to assign user attributes to roles in a way when a role is assigned to a user, this means that he can access the object based on these assigned attributes. Noting that, the number of attributes can be different from one role to another. If we suppose that we have two roles R1 and R2. R1 have two attributes A1 and A2 while R2 have four attributes, A3, A4, A5, and A6. To obtain R2, the user U1 must fulfil all the attributes from A3 to A6. However, it can obtain R2 by just matching A1 and A2, thus the least privileges are met. The administrator affects one time attributes to roles to able the affectation is these roles to users. Note that each role may have serval attributes, strengthening the security of the system. The second way to merge the two models is the assignment of attributes to objects. As the user's assignment, each role may have one or more object-attribute. Objects with the minimum number of attributes are considered less secure than those with multi-attributes. The attribute assignment process is explained in figure 5.

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3404-3414
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3404-3414

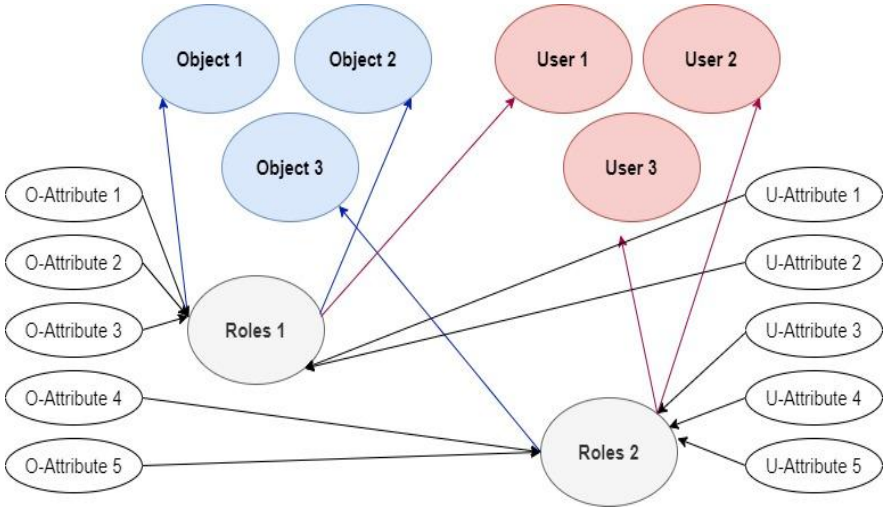

Figure 5. Hybrid approach attributes assignment

The RAAB-AC approach is advantageous in terms of cost, because it reduces the administrator charges by assigning attributes only once. Hence, it doesn't need to affect the attributes to individual users or objects each time. Thus, once roles' attributes assignments are done, the administrator affects each specific role to users and objects. Furthermore, the roles addition in the RAAB-AC model ensures the concept of least privileges. The model flowchart of proposed scheme is presented in figure 6.

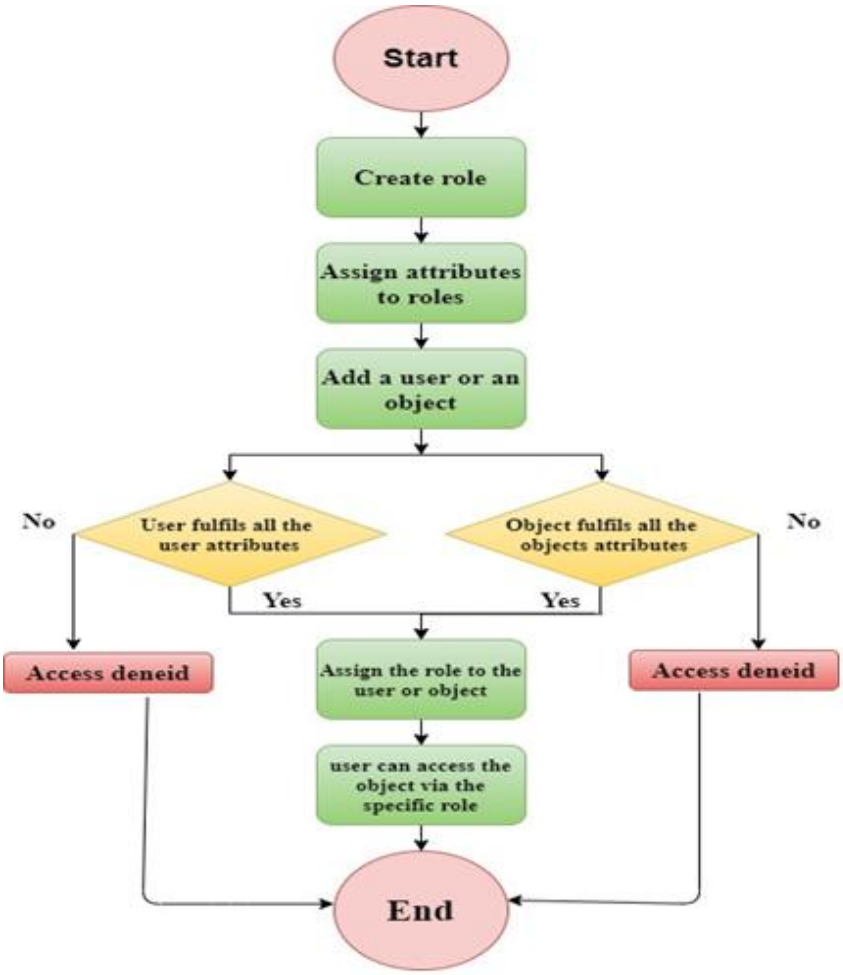

Figure 6. RAAB-AC model flow chart

International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 11 (2020), pp. 3404-3414
 https://dx.doi.org/10.37624/IJERT/13.11.2020.3404-3414

The algorithm of proposed scheme RAAB-AC is as follows:

RAAB-AC Algorithm

Entries: P: Policy

Variables : R : role, U : user, A : Attribute, UA : user Attribute, OA : Object Attribute and NbR : number of rules

Functions: AddRole(R): function that creates a role

AddObject (R): function that creates an object

AddAtt(R): function that creates an attribute

AssignAtt (A, R): function that assign an attribute or more to a given role R.

AssignRole2User(R, U): function that assign a role to a given user.

AssignRole2Object(R, U): function that assign a role to a given object.

Authorized (U, O): function return a true or false to indicate if the user U is authorized to access the object O

Proposed Algorithm

Begin

for *i= 0 to Nbr* ***do***

For each role in P AddRole (R);

For each object in P AddObject (O);

For each Attribute in P AddRole (A);

i++;

end for

//Assignment of attributes

for *each new user or object*

AssignAtt(A, R);

AssignRole2User(R,U);

AssignRole2Object(R,U);

//verification of authorization

if *U wants to Access O*

if *authorized (U, O)* ***then***

for *each attribute UA and OA*

If *userfulfil(U,R) and fuflfil(O,R) //verify if the user and the object fulfil attributes assigned to the role R that give access*

then *Permission (U,O); // accord the permission for U to access the object O*

else *deniedaccess (U,O); // denied the access of U to R*

else *deniedaccess (U,O);*

end

The benefit of the merge is clear in this situation; the user can only access an object under a specific role and on the basis of specific attributes. Additionally, this hybrid approach defines the different security levels via the assignment of a different number of attributes for each role. The schema of the proposed model RAAB-AC is presented in figure 7.

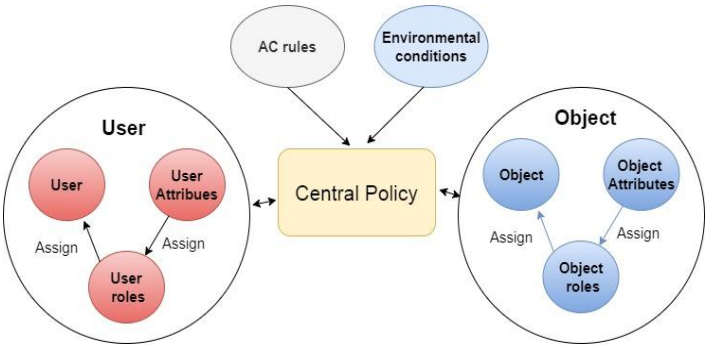

Figure 7. The proposed RAAB-AC model

IV. DISCUSSION

The key solution proposed in this work is the merge between the two models ABAC and RBAC. Our Hybrid approach is more efficient than the two conventional models. Our model integrates the concept of roles in ABAC and introduces the notions of attributes in RBAC. Our proposed model RAAB-AC is based on the assignment of attributes for each role defined in the system policy. On the contrary to the existing models, RAAB-AC reduces both time and efforts for administrators because they assign attributes only once. In addition, it imposes a fitted security in ABAC model. The main advantage of our hybrid approach is that the access to the system's resources is limited to users with assigned roles. Thus, the assignment of roles to users and objects is implemented with the least privileges. Therefore, the proposed scheme incorporates different level of security which was not ensured in the conventional models.

V. CONCLUSION

Access control is considered an indispensable technology for information and resource security. Nowadays, research on AC models has accomplished perceptible advancement. The paradigm of cloud computing needs this technology to provide resources' effective protection. Thus, AC is crucial for CC and presents one of the most significant issues in this domain. We compared existing models and analyze the differences between each solution and the essential characteristics of existing AC models. Based on the detailed analysis of existing AC approaches, we have proposed a hybrid approach to control users' data flow and resource exploitation. We discussed existing AC approaches and highlighted their pros and cons as well. Based on the gap identified in existing approaches, we have provided a hybrid approach that combines the best features of two well-known AC models namely RBAC and ABAC. The proposed approach is based on attributes

assignment, which increases the system's security and ensures the concept of least privileges.

REFERENCES

[1] Dang, L.M., et al., A survey on internet of things and cloud computing for healthcare. Electronics, 2019. 8(7): p. 768.

[2] Humayun, M., Role of Emerging IoT Big Data and Cloud Computing for Real Time Application. International Journal of Advanced Computer Science and Applications (IJACSA), 2020. 11(4).

[3] Agrawal, N. and S. Tapaswi, A trustworthy agent-based encrypted access control method for mobile cloud computing environment. Pervasive and Mobile Computing, 2019. 52: p. 13-28.

[4] Cai, F., et al., Survey of access control models and technologies for cloud computing. Cluster Computing, 2019. 22(3): p. 6111-6122.

[5] Mishra, S.K., et al., Energy-Aware Task Allocation for Multi-Cloud Networks. IEEE Access, 2020.

[6] Veloudis, S., et al., Achieving security-by-design through ontology-driven attribute-based access control in cloud environments. Future Generation Computer Systems, 2019. 93: p. 373-391.

[7] Li, J., N. Chen, and Y. Zhang, Extended file hierarchy access control scheme with attribute based encryption in cloud computing. IEEE Transactions on Emerging Topics in Computing, 2019.

[8] Ali, S., et al., Towards Pattern-Based Change Verification Framework for Cloud-Enabled Healthcare Component-Based. IEEE Access, 2020. 8: p. 148007-148020.

[9] Shafiq, D.A., N. Jhanjhi, and A. Abdullah. Proposing A Load Balancing Algorithm For The Optimization Of Cloud Computing Applications. In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS). 2019. IEEE.

[10] Almusaylim, Z.A. and N. Jhanjhi, Comprehensive Review: Privacy Protection of User in Location-Aware Services of Mobile Cloud Computing. Wireless Personal Communications, 2020. 111(1): p. 541-564.

[11] Shakya, S., An efficient security framework for data migration in a cloud computing environment. Journal of Artificial Intelligence, 2019. 1(01): p. 45-53.

[12] Amamou, S., Z. Trifa, and M. Khmakhem. Towards a Better Security in Public Cloud Computing. In International Conference on Hybrid Intelligent Systems. 2019. Springer.

[13] Sun, P.J., Privacy protection and data security in cloud computing: a survey, challenges, and solutions. IEEE Access, 2019. 7: p. 147420-147452.

[14] Alhenaki, L., et al. A survey on the security of cloud computing. In 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). 2019. IEEE.

[15] Chenthara, S., et al., Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE access, 2019. 7: p. 74361-74382.

[16] Abbasi, A.A., et al., Software-defined cloud computing: A systematic review on latest trends and developments. IEEE Access, 2019. 7: p. 93294-93314.

[17] Lopez, J. and J.E. Rubio, Access control for cyber-physical systems interconnected to the cloud. Computer Networks, 2018. 134: p. 46-54.

[18] Li, Q., et al., Efficient Privacy-Preserving Access Control of Mobile Multimedia Data in Cloud Computing. IEEE Access, 2019. 7: p. 131534-131542.

[19] Rao, K.R., et al., R-PEKS: RBAC Enabled PEKS for Secure Access of Cloud Data. IEEE Access, 2019. 7: p. 133274-133289.

[20] Sankaran, K.S., et al. Access Control based Efficient Hybrid Security Mechanisms for Cloud Storage. In 2019 International Conference on Communication and Signal Processing (ICCSP). 2019. IEEE.

[21] Veloudis, S., et al. Context-aware Security Models for PaaS-enabled Access Control. In CLOSER (2). 2016.

[22] Mahmood, G.S., D.J. Huang, and B.A. Jaleel, A Secure Cloud Computing System by Using Encryption and Access Control Model. Journal of Information Processing Systems, 2019. 15(3).

[23] Tirosh, O. and E. Werner, Method and system for implementing mandatory file access control in native discretionary access control environments. 2018, Google Patents.

[24] Win, K.Z. and K.M.L. Tun. Implementation of Discretionary Access Control and Role-Based Access Control Policy in Online Shopping System. 2017. Eighth Local Conference on Parallel and Soft Computing.

[25] Wadhwa, A. and V.K. Gupta, Proposed Framework with Comparative Analysis of Access Control & Authentication based Security Models Employed over Cloud. International Journal of Applied Engineering Research, 2017. 12(24): p. 15715-15722.

[26] Kashmar, N., M. Adda, and M. Atieh. From Access Control Models to Access Control Metamodels: A Survey. In Future of Information and Communication Conference. 2019. Springer.

[27] Kerr, L. and J. Alves-Foss. Combining Mandatory and Attribute-Based Access Control. In 2016 49th Hawaii International Conference on System Sciences (HICSS). 2016. IEEE.

[28] Choi, E.-B. and S.-J. Lee, Access control mechanism based on MAC for cloud convergence. Journal of the Korea Convergence Society, 2016. 7(1): p. 1-8.

[29] Devyanin, P.N., About modeling of MIC and MAC in PostgreSQL within framework of the MROSL DP-model. Prikladnaya Diskretnaya Matematika. Supplement, 2019(12): p. 161-165.

[30] Servos, D. and S.L. Osborn, Current research and open problems in attribute-based access control. ACM Computing Surveys (CSUR), 2017. 49(4): p. 1-45.

[31] Nakamura, S., et al., A read-write abortion protocol to prevent illegal information flow in role-based access control systems. International Journal of Space-Based and Situated Computing, 2016. 6(1): p. 43-53.

[32] Liu, Q., et al., An access control model for resource sharing based on the role-based access control intended for multi-domain manufacturing internet of things. IEEE Access, 2017. 5: p. 7001-7011.

[33] Trnka, M. and T. Cerny. On security level usage in context-aware role-based access control. In Proceedings of the 31st Annual ACM Symposium on Applied Computing. 2016.

[34] Chakraborty, S. and I. Ray. TrustBAC: integrating trust relationships into the RBAC model for access control in open systems. In Proceedings of the eleventh ACM symposium on Access control models and technologies. 2006.

[35] Cohen, E., et al. Models for coalition-based access control (CBAC). In Proceedings of the seventh ACM symposium on Access control models and technologies. 2002.

[36] Liscano, R. and K. Wang. A context-based delegation access control model for pervasive computing. In 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07). 2007. IEEE.

[37] Ghazal, R., et al. Intelligent Agent-Based RBAC Model to Support Cyber Security Alliance Among Multiple Organizations in Global IT Systems. In 17th International Conference on Information Technology–New Generations (ITNG 2020). 2020. Springer.

[38] Li, J., Q. Yu, and Y. Zhang, Hierarchical attribute based encryption with continuous leakage-resilience. Information Sciences, 2019. 484: p. 113-134.

[39] Soni, K. and S. Kumar. Comparison of RBAC and ABAC Security Models for Private Cloud. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon). 2019. IEEE.

[40] Premarathne, U., et al., Hybrid cryptographic access control for cloud-based EHR systems. IEEE Cloud Computing, 2016. 3(4): p. 58-64.

[41] Ahmad, M., et al., A Software Engineering Approach for Access Control to Multi-Level-Security Documents, in Software Development Techniques for Constructive Information Systems Design. 2013, IGI Global. p. 345-353.