Received 14 April 2022
Revised 1 June 2022
Accepted 6 July 2022

A systematic literature review for authorization and access control: definitions, strategies and models

Aya Khaled Youssef Sayed Mohamed, Dagmar Auer, Daniel Hofer and Josef Küng

Institute for Application-oriented Knowledge Processing, Johannes Kepler University Linz, Linz, Austria and LIT Secure and Correct Systems Lab, Johannes Kepler University Linz, Linz, Austria

Abstract

Purpose – Authorization and access control have been a topic of research for several decades. However, existing definitions are inconsistent and even contradicting each other. Furthermore, there are numerous access control models and even more have recently evolved to conform with the challenging requirements of resource protection. That makes it hard to classify the models and decide for an appropriate one satisfying security needs. Therefore, this study aims to guide through the plenty of access control models in the current state of the art besides this opaque accumulation of terms meaning and how they are related.

Design/methodology/approach – This study follows the systematic literature review approach to investigate current research regarding access control models and illustrate the findings of the conducted review. To provide a detailed understanding of the topic, this study identified the need for an additional study on the terms related to the domain of authorization and access control.

Findings – The authors' research results in this paper are the distinction between authorization and access control with respect to definition, strategies, and models in addition to the classification schema. This study provides a comprehensive overview of existing models and an analysis according to the proposed five classes of access control models.

Originality/value – Based on the authors' definitions of authorization and access control along with their related terms, i.e. authorization strategy, model and policy as well as access control model and mechanism, this study gives an overview of authorization strategies and propose a classification of access control models providing examples for each category. In contrast to other comparative studies, this study discusses more access control models, including the conventional state-of-the-art models and novel ones. This study also summarizes each of the literature works after selecting the relevant ones focusing on the database system domain or providing a survey, a classification or evaluation criteria of access control models. Additionally, the introduced categories of models are analyzed with respect to various criteria that are partly selected from the standard access control system evaluation metrics by the National Institute of Standards and Technology.

Keywords Authorization, Access control, Authorization strategy, Access control model, Classification, Criteria

Paper type Literature review

The research reported in this paper has been partly supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria. The work was also funded within the FFG BRIDGE project KnoP-2D (grant no. 871299).

International Journal of Web Information Systems
Vol. 18 No. 2/3, 2022
pp. 156-180
Emerald Publishing Limited
1744-0084
DOI 10.1108/IJWIS-04-2022-0077

1. Introduction

Access control ensures data security by protecting assets and private information against unauthorized access by defined subjects. It helps to avoid information leaks or improper modification by potentially malicious parties. Besides traditional well-known access control models, there are many others that recently evolved to match advanced security requirements. Because of the increase of access control models, it seems promising to classify the models to enhance the selection of an appropriate model to fulfill the requirements of the overall system. Thus, it is necessary to clarify the core concepts of authorization and access control (e.g. definitions, strategies and models) along with the commonly used, partly ambiguous, synonyms.

In this paper, we overcome this opaque accumulation of terms and their meaning by guiding researchers and practitioners through the vast amount of available access control models. We further provide support in selecting an appropriate access control model with respect to security requirements. The contributions of our work are the following:

- definition of authorization and access control along with their related terms;
- distinction between authorization strategies and access control models;
- rough classification schema for access control models;
- illustration of classification schema by providing state of the art as well as not commonly discussed models for each class of access control models;
- review of a selected list of comparative studies on access control that are in the context of databases, include a survey of models, provide evaluation criteria and/or introduce a taxonomy of models; and
- analysis of the classification schema based on selected criteria of access control models.

Concerning the methodology, we conduct a *systematic literature review (SLR)* which is a formal repeatable method to identify, analyze and interpret the existing research related to a particular topic of interest. According to the SLR definition in Kuhrmann *et al.* (2017), we started our research with an extensive literature study on access control models. We selected a specific range of publications according to our filter criteria and studied them in detail. Because of the differences in the definition of authorization and access control along with their related terms, we discuss the various views for each concept and state which of them we follow. Then, we identified authorization strategies and derived categories for classifying all these models. Finally, we analyzed the resulting selections in addition to the main features of each category.

The remainder of this paper is organized as follows. Section 2 defines the related terms we use throughout this work. Section 3 explains authorization strategy and illustrates existing discretionary, mandatory and hybrid strategies. We introduce a classification of access control models along with examples in Section 4. We provide a summary of survey works comparing the included access control models in Section 5. In Section 6, we analyze the proposed categories with respect to selected criteria before concluding our paper in Section 7.

2. Related terms

Although authorization and access control have already been important in theory and practice for several decades, there are still differences concerning the understanding of basic terms in this domain. Therefore, we discuss the most important ones for our research.

Starting with authorization and access control, we see the following common differences. While Kane and Browne (2006), some publications by the National Institute of Standards and Technology (NIST) such as Hu *et al.* (2014) and sources from IBM (IBM-Corporation, 2015) use them as synonyms, Bertino *et al.* (2011), Ferrari (2009), Josang (2017), Kizza (2020) and other NIST publications (Ross *et al.*, 2021) clearly differentiate between them.

We follow (Bertino *et al.*, 2011; Ferrari, 2009; Josang, 2017; Ross *et al.*, 2021; Kizza, 2020) to clearly distinguish between these two terms and discuss our view including associated concepts in the following. A brief overview is given in Figure 1, which also shows how we assign the terms according to the two dimensions:

(1) authorization and access control; and

(2) strategy, model and instance level.

2.1 Authorization

While authorization not only refers to the result (authorizations, authorization policy), but also to the *process of specifying access policies* (Josang, 2017; Kizza, 2020), most sources including (Bertino *et al.*, 2011; Ferrari, 2009; Kane and Browne, 2006; Ross *et al.*, 2021; Hu *et al.*, 2014; Ahmad and Whitworth, 2011) focus on the result only.

We are aware that authorizations are usually developed in an iterative process of requirements analysis, definition and authorization specification at different levels of granularity and with respect to the access control model.

Definition 1 (Authorization). Is about the specification of access rights and combines authorization strategy as well as authorization model and authorization policy including their components (i.e. subject, object and action). It also considers the process of defining the authorization policy with respect to the selected model framed by its strategy.

In the following discussion and definitions, we focus on the artifacts in their final level of details. We start from the strategic level down to the instance level.

2.1.1 Authorization strategy. Bertino (2016) uses the term access control technique to summarize discretionary (DAC) and mandatory access control (MAC) as the” fundamental building blocks”. Kizza (2020) uses the term authorization mechanism accordingly. In contrast, Eckert (2014) considers them as access control strategies, among which she includes role-based access control (RBAC). From our perspective, these fundamental viewpoints are strategic and not a matter of technique or mechanism. Therefore, we follow Eckert (2014) concerning the term strategy. However, as it is about specifying access rights,

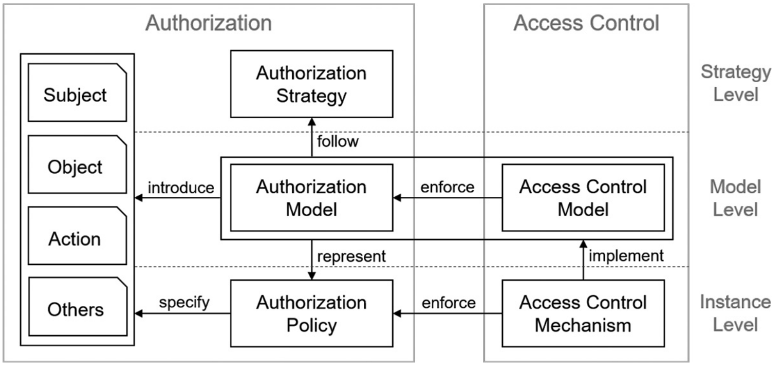

Figure 1.
Authorization and access control

we follow Kizza (2020) and use the term authorization rather than access control like Eckert (2014) and Bertino (2016). Furthermore, we do not consider RBAC a strategy, but an access control model (Section 4). Authorization strategies are discussed in Section 3 in more detail and further used in the analysis of the access control models along with their underlying authorization models in Section 6.

Definition 2 (Authorization Strategy). Defines the overall perspective of how to specify authorizations, i.e. owner-centric, administration-centric or hybrid and thus sets the frame for the authorization models.

2.1.2 Authorization model. Defines the model for the definition of the access rights, i.e. the components and their interactions. An authorization model is usually defined by its three main components (Ferrari, 2009; Bertino *et al.*, 2011; Josang, 2017): subject, object and action. However, with respect to the access control model which enforces the authorization model, additional components can be relevant such as role and session with RBAC or environmental variables with attribute-based access control (ABAC):

- Subject is the active entity (e.g. user, group, organizational role, process, application program) to which access rights are granted. With a focus rather on the implementation, the term principal is also used as a synonym.
- Object is the passive entity of the system, which needs to be protected, e.g. a file, a database table or record, an object in an object-oriented system, a node in a graph database. Different levels of granularity as well as sensitivity can be considered. Alternative terms for object are resource or asset.
- Action states what the subject can perform on the object. There are several alternative terms for action such as privilege, (access) right, type of operations or activity, access mode and property. Privilege is the preferred term not only in the context of databases where privileges are granted to users (Bertino *et al.*, 2011), but also in the context of basic discussions such as Ferrari (2009) and Josang (2017). However, privileges are often used with slightly differing semantics (Center, Computer Security Resource, 2022), which may lead to misconceptions. Atlam *et al.* (2020) even explicitly distinguish between action and privilege. While actions represent the types of activities subjects can perform on objects, the privileges are the permissions granted to a subject to be able to perform particular activities on certain objects. Thus, privileges are considered as synonyms to authorizations (Josang, 2017).
- Additional components are often demanded by specific access control models such as roles and sessions for RBAC, environmental attributes for ABAC or conflict of interest classes for the Chinese Wall model.

Definition 3 (Authorization Model). Defines the model for the specification of the access rights, i.e. the components needed and their interactions with respect to the core authorization strategy.

2.1.3 Authorization policy. We have also seen differences with the term policy in terms of authorization and access control. Often authorization policy, access policy and access control policy are used synonymously. Authorization policies are considered on different levels of detail. For example, Hu (2016) describes access control policies as the “high-level requirements that specify how access is managed and who may access information under what circumstances”. Also Ferrari (2009) and Bertino *et al.* (2011) consider access control policies as the (high-level) rules to which access control must occur or authorizations are granted. The OASIS eXtensible Access Control Markup Language (XACML) technical committee provides an example with the OASIS standard (OASIS, 2013), which shows an access control policy in plain text and the respective XACML policy in the XACML policy language. Thus, in this case it only differs in the level of granularity and language.

We follow the OASIS view in our definition of authorization policy considering the focus and the openness with regard to nearly any granularity of the specification. The authorization model defines all components and their required dependencies to specify the authorization policy. Thus, Figure 1 contains not only an edge from the authorization model to the set of components, but also from the authorization policy.

Definition 4 (Authorization Policy). Is an instance-level artifact, which specifies the access rights for a system according to the selected authorization model, on nearly any level of granularity, i.e. from simple text up to a policy definition language.

2.2 Access control

While authorization is about specifying the access rights, access control is about their enforcement (Josang, 2017). Kizza (2020) describes this as "... a process to determine who does what to what based on a policy". We follow these sources and consider access control as the process of enforcing access rights defined in an authorization policy.

2.2.1 Access control model. The enforcement of access rights, which are defined according to some specific authorization model, is defined in the access control model. It states what needs to be done to determine the decision whether allow or deny access. Ferrari (2009) proposes the term authorization verification as a synonym to access control model. This view contrasts other sources such as Hu *et al.* (2017a), who rely on a different definition of policy and further do not distinguish between authorization and access control model. They, for example, consider the access control model to "bridge the gap in abstraction between policy and mechanism" as their policies rather define the organizational frame for the access rights and not the access rights themselves.

Definition 5 (Access Control Model). Defines the enforcement of the authorization model, i.e. what needs to be checked to determine whether to allow or deny access for a subject to a protected resource.

2.2.2 Access control mechanism. Is an instance-level artifact, i.e. a piece of software implementing a certain access control model (Bertino *et al.*, 2011; Ferrari, 2009). When receiving a request (i.e. a subject requesting a specific kind of access on an object), the mechanism determines whether it can be allowed or must be denied (Bertino *et al.*, 2011; Ferrari, 2009; Hu *et al.*, 2014). As it typically works as a reference monitor intercepting all requests to the system, thus, this term is also used as a synonym (Bertino *et al.*, 2011; Ferrari, 2009; Samarati and De Capitani di Vimercati, 2001).

Definition 6 (Access Control Mechanism). Is an implementation of an access control model and thus, an instance-level artifact. It enforces an authorization policy which fits to the access control model of the mechanism. The mechanism determines if an access request evaluation is allowing or restricting the access.

Although there are numerous other technical terms with divergent definitions, the selection presented in this paper forms the basis for our further work.

3. Authorization strategies

An authorization strategy (Definition 2) defines the view point of describing authorization policies, i.e. owner-centric, administration-centric or hybrid. Different terms are used as alternatives to authorization strategy. Eckert (2014) refers to it as access control strategy, Samarati and De Capitani di Vimercati (2001) as well as Benantar (2005) called it access control policies class while others regard it as an access control model (Bertino and Sandhu, 2005).

Even though we use the term authorization strategy, we keep the well-established DAC (i.e. Discretionary Access Control) and MAC (i.e. Mandatory Access Control) abbreviations.

3.1 Discretionary strategy

The discretionary strategy (DAC) is owner-centric, i.e. ownership of each resource is assigned to one or more entities. The subject, who is allowed to access a resource, is either the object creator (i.e. the default owner) or a principal with delegated ownership rights. The resource can be only destroyed by the owner and its ownership may optionally be shared with other subjects as well (Benantar, 2005).

DAC systems provide more flexibility to the user, but less administration control. Moreover, they do not scale well and are hard to manage in large environments. Because the propagation and usage of information cannot be controlled after giving access to the legitimate subjects, they are insecure and vulnerable to Trojan Horse attacks. A trojan horse program executes more actions, unknown to users, than it seems and should do (Bertino *et al.*, 2011; Harris, 2012).

3.2 Mandatory strategy

The mandatory strategy (MAC) is non-discretionary because access decisions are not made at the discretion of the user. A MAC policy is obligatory as the access rights are regulated by a central authority. The owner and subject users can neither control the defined access nor override the policy. This strategy often is based on the security label concept where the subjects are associated to security clearance and objects to sensitivity classifications (Hu *et al.*, 2017b; Benantar, 2005).

Although MAC systems provide stronger security than the DAC ones and overcome the trojan horse problem, they are vulnerable to covert channels (i.e. tunnels created for transferring information in an unauthorized manner). Furthermore, the required administrative overhead makes it more costly.

3.3 Hybrid strategy

The advanced access control models are typically based on a middle ground strategy mixing DAC and MAC because the pure mandatory and discretionary strategies are often no longer sufficient. For instance, the originator-controlled strategy (ORCON or ORGCON) (Abrams, 1995; Park and Sandhu, 2002) combines DAC and MAC such that only the originator (i.e. original owner) can alter the privileges on a subject/object basis (Matt, 2018) (cp. DAC). On the other hand, access restrictions on original resources are automatically copied to derived objects without owner control (cp. MAC).

4. Access control models

An access control model defines the enforcement of the authorization model to decide whether to allow or deny access for a subject to a protected resource. We grouped the access control models into five main classes based on their characteristics. In the following subsections, we explain these categories and provide an overview of a selected subset of the access control models including some recent models that are not previously discussed in other surveys (Section 5).

4.1 Access control by explicit Object-Subject assignment

The oldest and simplest access control model is the access matrix (ACM) proposed by Lampson in 1971. It is built upon the strategy of DAC (i.e. identity-based) where the subjects' privileges are described over the objects in a matrix data structure. A single entry in the matrix *A[s,o]* represents the access rights (i.e. actions) a subject *s* can take upon an object *o* (Benantar, 2005). The access rights representation is straightforward and was commonly used in practice, but typically the matrix becomes sparse and oversized because of lots of empty cells. In the following, we give an overview of available access matrix model variants.

4.1.1 Authorization table. Typically used in database management systems. The non-empty matrix authorization entries are stored as tuples in a table with three columns for the subject, object and action (Petkovic and Jonker, 2007).

4.1.2 Access control list (ACL). The most common and basic form of access control for limiting access to data on shared systems. It represents the access matrix in a column perspective (i.e. resource view) where the objects to be accessed are associated with a list of subjects along with the operations allowed to be executed on these objects (Petkovic and Jonker, 2007).

4.1.3 Capability list. The conceptual approach is similar to ACL, but with the access matrix stored by row (i.e. subject view). Each subject holds a list of capability certificates containing the access rights to be performed by this principal over a set of resources (Petkovic and Jonker, 2007).

4.2 Access control by model-specific rules

Traditionally, this class of models has been used in MAC systems enforcing the concept of rules. A set of predefined rules must be met to grant/deny the subject access to a particular resource. The models in this category have fixed rules that apply all the time for all users regardless of their identity. The rules are an implicit part of the access control model specifying detailed situations, i.e. whether a given subject can or cannot access an object and what that subject can do once access is granted. For example, the subject's security level determines the classes of objects to be accessed in the Bell-LaPadula (BLP) and Biba models. Administrators can only manage the basic parameters (e.g. security level) whereas users have no control at all on the rules. In the following, we give an overview of some model-specific rule examples.

4.2.1 Bell-LaPadula (BLP). This model was formulated by Bell and La Padula in 1976 for government and military purposes (Bell and La Padula, 1976). The access rights are specified according to subjects and objects associated to different security levels, i.e. top secret (TS) as the highest sensitivity label, secret (S), Confidential (C) and unclassified (U) as a public category with the least security clearance (Benantar, 2005). The subject's security level determines the classes of objects to be accessed. The BLP model has the following properties (Bertino *et al.*, 2011):

- *Simple security*: also known as the no-read-up (i.e. read-down) property such that a subject is not allowed to read objects with higher sensitivity. The subject security clearance must dominate the object security classification.
- *Star property*: also known as the no-write-down (i.e. write-up) policy where it is not possible for a subject with some security level to write any object with lower sensitivity. To avoid the leakage of confidential information, the object security classification has to dominate the subject security clearance.
- *Strong star property (optional)*: read and write operations are performed at a single security level such that the subject and object sensitivity are equal.

4.2.2 Biba. The Biba integrity model ensures data security through preventing information flow in an unauthorized direction using a set of access control rules. The integrity labels given to the system's subjects and objects indicate the degree of confidence. A subject is not able to corrupt higher sensitive data and will also not be corrupted by lower security levels. It is quite similar to the BLP in the state transition system architecture and level classification, but opposite in the characteristics as follows (Benantar, 2005):

- *Simple integrity*: *read-up* rule controls a subject's access from reading lower integrity level data, so that bad information will not flow upwards from lower clearance levels.
- *Star integrity*: also known as write-down such that subjects are not allowed to write data or pass information to higher classified levels than theirs.
- *Invocation property*: a service can only be invoked by subjects at a lower integrity level.

4.2.3 Lipner. The purpose of the Lipner model is to preserve confidentiality in addition to addressing commercial integrity concerns. It is a matrix-based model with security levels and functional compartments (i.e. categories) associated with subjects and objects. Each subject/object is assigned to only one of the confidentiality and/or integrity levels, but could be classified to zero or more compartments. Objects are split into data and programs for the first time using Lipner's method. There are two ways of implementing integrity: (Matt, 2018)

- Based on the BLP: subjects and objects are assigned to one of the two confidentiality levels. In this case, five defined compartments are responsible for integrity and access control.
- Full Model: is a hybrid combination of the BLP and Biba integrity models. Three integrity levels and two categories are added to Lipner's first mechanism, after collapsing some confidentiality compartments, to be assigned to subjects and objects. This is to prevent low-integrity data or programs from impacting those with higher integrity. The purpose of integrity levels is to avoid unauthorized modification of system programs whereas the categories are used to separate domains according to functional areas.

4.2.4 Clark–Wilson. Clark and Wilson (1987) introduced a model for commercial purpose to prevent fraud by requiring subjects to access objects via programs. The model consists of five certification rules (CR) and four enforcement rules (ER) to ensure the external and internal integrity of the data items. The basic components along with the corresponding rules are (Matt, 2018):

- *Subject*: (ER3): is an authenticated user who attempts to initiate a transformation procedure (TP). (ER4): Only the certifier of a TP can change the list of entities associated with that TP to prevent violating the integrity constraints by changing the qualifications of a TP.
- *Object*: is either classified as a *constrained data item (CDI)* with high protection level or *unconstrained data item (UDI)* representing untrusted information entered to the system. (ER2): The system must associate a user with each TP and set of CDIs. (CR1): The validity of CDIs is ensured by *integrity* verification procedures (IVPs).
- *Transformation procedure (TP)*: a set of operations performed on data items. (CR2): It transforms CDIs in the system from one valid state to another. (CR5): The TP can also take an UDI as input and either produce a CDI or reject the UDI. (ER1): Only TPs certified to run on a CDI can manipulate it so that the certified relations are maintained. (CR3): The relations allowed by the system must enforce the separation

of duty principle. (CR4): Transactions are logged using a CDI and the TP only appends to it.

4.2.5 Chinese-Wall (CW). The Chinese-Wall model (Brewer and Nash, 1989), also known as the Brewer and Nash model according to the inventors names, is designed to avoid conflict of interest (COI) problems. The name is inspired by the Great Wall of China so that no subject can access any object from the wrong side of that wall using a set of rules. The data objects in this model are hierarchically structured to the individual objects, company datasets grouping objects that belong to the same corporation and conflict of interest classes containing the company datasets of competing corporations. There are two properties for the access definition based on the object organization: (Sandhu and Samarati, 1994)

- *Simple security*: the object can be accessed by a specific subject if it belongs to either the same company dataset of the previously accessed objects or a different conflict of interest class.
- *Star property*: for the write access, the simple security rule must be satisfied besides the permission to read the objects which are sanitized (i.e. filtered from sensitive data) and belong to the same company dataset as the one for which write access is requested.

4.2.6 Multi-level security (MLS) database. The MLS database model (Keefe *et al.*, 1993) follows the MAC authorization strategy and extends the concept of the BLP model to apply fine-grained access control to database systems at the level of relations (i.e. tables), attributes (i.e. columns), tuples (i.e. rows) and elements (i.e. cells). This is done by regulating access to data resources by subjects according to their predefined classification in the system. The classification is based on a partially ordered set of access classes (i.e. labels) such that an access class c_i dominates an access class c_j if and only if the security level of c_i is greater than or equal to that of c_j (Bertino and Sandhu, 2005). Having a classification associated to a value represents the sensitivity of that attribute value for a particular entity not the value itself. For example, a classification (e.g. *Secret*) associated to a salary value is not for this absolute value, but rather the salary of the given employee. There are three MLS architectures: *kernalized architecture*, *distributed architecture* and *trusted subject architecture*. They are classified according to whether access control is enforced by the database management system (DBMS) or delegated to a trusted operating system (Rjaibi, 2004).

However, the MLS database introduces complications in real-world cases because of *polyinstantiation*. This problem arises when there are multiple instances of the same entity with different access classes in the system. Possible options are either notify the subject or accept the change replacing the existing value. The first solution compromises secrecy because of revealing protected information causing a covert channel while the overwriting approach compromises integrity because high classified data would be lost. Because both solutions are not viable, the only applicable option is to have the original and the new tuples coexist and manage their presence. Thus, polyinstantiated tuples result and the database loses its semantics after executing few operations. Accordingly, current DBMSs do not support element-level classification, but rather on the tuple level (e.g. Trusted Oracle, DB2 for z/OS and SYBASE Secure SQL Server) (Samarati and De Capitani di Vimercati, 2001).

4.3 Access control by roles

In this category, system activities and resource permissions are associated to some defined role(s) rather than assigned directly to users. The role-based access control (RBAC) model (Ferraiolo and Kuhn, 1992; Ferraiolo *et al.*, 1995; Sandhu *et al.*, 1996) has emerged to adapt with the dynamic organizational needs because individuals change unlike the business functions. The core RBAC components are users, objects, roles, permissions and sessions. In this model, the roles act as an intermediate layer between the subjects and the access rights. The user-role assignment changes over time whereas the role-permission assignment is relatively stable. The access decision depends on the user being a member to the applicable role(s). The session represents the active roles for a user. The RBAC model has several forms: (Kriti, 2013; Benantar, 2005):

- *Flat RBAC*: applies basic RBAC, but considers many-to-many relations between users and roles such that a user can have many roles and vice versa. The same applies to the permission-role assignment.
- *Hierarchical RBAC*: organizational and administrative roles are defined in a general or limited hierarchy (i.e. tree) for structuring authorities and responsibilities within the organization. The hierarchies are reflexive and transitive, but anti-symmetric.
- *Constrained RBAC*: adds constraints associated with the user-role assignment relations and/or role activation within user sessions to the hierarchical RBAC. The separation of duty (SoD) concept is applied to prevent the users from being over-authorized and enforce conflict of interest policies. The SoD can be static (SSoD) or dynamic (DSoD). In SSoD, the user cannot be a member of roles having shared principles. However, this is allowed in the DSoD without activating these exclusive roles at the same time even across multiple simultaneous sessions initiated by the same subject.

Besides the standard RBAC, advanced models are proposed to structure the RBAC model and manage its policies. Moreover, several works extended the capabilities of RBAC to deal with contextual information.

4.3.1 Administration role-based access control. This model uses roles as a central concept, but dedicated to the management of policies in RBAC. Sandhu *et al.* (1999) proposed the first RBAC administration model called *ARBAC97*. Administrative roles and permissions are independent of the regular ones. ARBAC97 is decentralized, but without compromising the broad policy objectives. It has three components to deal with different RBAC administration aspects: *URA97* for user-role assignment, *PRA97* for permission-role assignment and *RRA97* for role-role assignment. URA97 and PRA97 are based on a ternary relation (i.e. *can_assign*) with prerequisite conditions. For instance, an administration role member can assign a user to a regular role in URA97 only if this user satisfies the prerequisite role(s) condition. URA97 and PRA97 control user-role and permission-role weak and strong revocation by means of a relation called *can_revoke* without involving prerequisite conditions. Weak revocation applies only to explicit membership in a single role whereas strong revocation cascades upwards in the role hierarchy, however, both apply downward cascading. Last but not least, the role hierarchy is constructed in the RRA97 sub-model.

Additionally, two extensions (i.e. *ARBAC99* and *ARBAC02*) have been proposed by the same research group to address the shortcomings in ARBAC97. The objective of ARBAC99 is to manage mobile and immobile users (e.g. visitor or consultant) and permissions. ARBAC02 focuses on resolving the multi-step user assignment, duplicated permission-role assignment (PA) information and restricted composition of permission pools. This is done by creating an organization structure as a user and permission pools independent of the role hierarchy in addition to introducing a bottom-up permission–role administration unlike the top-down approach in the ARBAC97 model. On the other hand, scoped administration of role-based access control *(SARBAC)* is proposed by Crampton and Loizon (2002) as an extension of RRA97 and an alternative to ARBAC97 (Cuppens and Miège, 2003). It relies on administrative scope which dynamically changes upon changing the role hierarchy. This improves rule consistency when deleting roles. Finally, administrative roles are not separated from the regular ones anymore.

4.3.2 Organization-based access control (OrBAC). The OrBAC model has evolved because of the need to structure a given organization into sub-organizations and specify their different authorization policies within one framework. It is based on the concept of organization as an organized group of subjects such that each of them plays some role in the organization. In OrBAC, policies associated with different organizations can be handled simultaneously (Kalam *et al.*, 2003).

Permissions are typically applied directly to subjects, actions and objects while in OrBAC, subject, action and object are respectively abstracted into role, activity and view. The subject in this context is either an active entity (i.e. user) or an organization. A role acts as the link between subjects and organizations in a ternary relationship called *Employ*. A view corresponds to a set of objects satisfying a common property whereas an activity joins actions that partake of the same principles (Kalam *et al.*, 2003). As organizations can define views differently, the object, view and organization entities are related to each other via the *Use* ternary relationship. The same applies to the action, activity and organization using another ternary relationship, i.e. *Consider*.

An authorization policy is specified as a set of facts, i.e. in an organization, a given role is permitted to perform a given *activity* on a given *view* in a given *context* (e.g. working hours, night and urgency) (Cuppens and Miège, 2003). In addition to permissions, obligations and prohibitions can be specified using OrBAC. It is assumed that any organization is a subject ($Org \subseteq S$), any subject is an object ($S \subseteq O$) and entity attributes are represented as functions, e.g. the name of a subject s is represented as *name(s)*. Furthermore, an administration model for OrBAC (AdOr-BAC) is proposed by Cuppens and Miège (2003). The AdOr-BAC model includes the URA and PRA components as in the ARBAC model, but has an additional component called UPA (i.e. user-permission administration). The two variations of the UPA component are *UPA1* and *UPA2* for enabling a user to delegate a permission to perform an action on an object and an activity on a view respectively.

4.3.3 Role-based access control extensions. Several RBAC models are proposed to consider context information for access control decisions. For instance, temporal RBAC (T-RBAC) model extends RBAC such that users are limited to only use the role permissions in specific temporal periods. Depending on the specified time interval(s), the roles are either in an active or inactive state. Furthermore, role triggers are supported for controlling the time of action execution. The priority resolves the conflicts between triggers and periodic activation/deactivation (Bertino *et al.*, 2011). The language is formally defined and checked for inconsistencies or ambiguities in (Bertino *et al.*, 2000).

Another extension is *GEO-RBAC* (Damiani *et al.*, 2007) that evolved because of the increasing need for securing mobile applications and location-based services. Spatial capabilities are added to the conventional RBAC model to support location-specific constraints in which a given role can be accessed by a user. The location can be physically or logically expressed in terms of absolute coordinates or relative to spatial objects respectively. In this model, the role is only enabled if the user is located within the spatial boundary of that role (Bertino *et al.*, 2011).

Tie-RBAC (Tapiador *et al.*, 2012) extends RBAC to be applied in social networks. It gives full control to the resource owner by allowing users to define their social circle (i.e. contacts) and establish in-between relations to grant access. Thus, the users control which requestor has access to their resources. The access control policies for all users are stored and enforced by a central server.

Last but not least, Historical RBAC (HRBAC) (Hosseini and Azgomi, 2010) is proposed to deal with historical information (e.g. deleted users and user-role de-assignment) unlike most of the extensions which rely on the existing information. The term historical is not only describing the past, but also the current information. This model extends RBAC by introducing:

- new elements to model historical as well as deleted information;
- analyzing functions; and
- historical constraints such as historical separation of duty (HSD) to deny undesired requests according to the previous and current information.

To sum up, the models in the role-based access control category have many forms and extensions, but all of them are based on the concept of roles which are associated to access permissions and assigned to users.

4.4 Access control by content

This category applies the concept of comprehensive data protection where access control decisions are based on data content (e.g. attribute values) (Zeng *et al.*, 2014). Besides the flexible policy definition, authorizations are dynamically granted and revoked (Bertino *et al.*, 2011). In content-based models, the policies are only applicable to the users satisfying specific criteria according to the rules defined by users or administrators. On the other hand, the model-specific rules category has static rules that can neither be modified nor controlled by administrators. Selected content-based models are explained in the rest of this section.

4.4.1 Attribute-based access control. The ABAC model overcomes the limitations of other models concerning long-term maintenance as well as representing complex access control requirements. In ABAC, a given subject can have access to a wide range of objects without specifying individual relationships to each resource. Authorization policies are specified in terms of the subject, resource and environment condition (e.g. time and location) attributes. The access decision is determined by evaluating the attribute values of the applicable policy (or policies). The ACL and RBAC models are even considered as a special case of ABAC using an attribute for the identity and role respectively (Hu *et al.*, 2014).

Although there are several proposed ABAC policy models, the eXtensible access control markup language (XACML) (OASIS, 2013) has become the defacto standard not only in specifying ABAC policies, but also enforcing them in a multi-step authorization process using XACML's reference architecture (Hu *et al.*, 2017b; Ferraiolo *et al.*, 2016). The second commonly used approach is based on next generation access control (NGAC) (Council, Information Technology Industry, 2018, 2016) and its functional architecture.

4.4.2 View-based access control (VBAC). This model is specific to databases. Theoretically, a view is a static typed language construct while from the technical perspective, it is a virtual table having rows and columns defined by a query based on the database tables, but without physical storage. The access control policy is based on a set of predefined interfaces (i.e. views).

Firstly, views are created to handle fine-grained access control requirements. Then, particular principals are allocated to one or more views so that users interact with the resources only via these interfaces. The access decision is denied if:

- the user is not permitted to access the view; or

- the operation to be performed on the object is explicitly denied within one of the views to which the principal or the relevant role is associated (Bertino *et al.*, 2011; Sahafizadeh and Parsa, 2010).

New data that satisfy a given policy will be automatically included in the view result. However, new views are created upon modifications to access control policies and their number further increase because users have different permissions. The Oracle VPD mechanism (Browder and Davidson, 2002) addresses some of these problems where the queries are initially written against the base tables and then, automatically rewritten by the system against the view available to the subject user.

4.4.3 Relation-based access control. The ReBAC model (Fong, 2011; Gates, 2007) addresses the limitations of ABAC to deal with the interpersonal relationships between users in expressing authorization policies. The access control decision is based on the type, depth and trust level of the relationship between the owner and access requester of the resource. This model has been typically applied in social networks focusing on the privacy of end users (Hu *et al.*, 2012). A policy language based on modal logic and an access control model formulated as a state transition system are introduced in (Fong, 2011) for specifying and enforcing complex relations (e.g. friends-of-friends). However, ReBAC supports neither fine-grained access control at attribute level nor entities other than subjects and objects.

4.4.4 Entity-based access control (EBAC). This model takes into account both attributes and relationships in policy evaluation using the concept of entities. The EBAC model addresses the expressiveness limitations of ABAC and ReBAC such that the relationships between entities can be navigated reasoning about these entities along paths of arbitrary length by comparing their corresponding properties. In EBAC, an entity-relationship (ER) model and logical expressions, including logical operators (e.g. *or* and, *not*) and quantifiers (i.e. ∀ and ∃), are introduced into the policy expressions as a generalization to ABAC. The ER-model describes the entities along with their properties and relationships for a particular application which is then represented in an entity graph. This is a directed multi-labelled graph mapping the entities and relationship types to vertices and edges respectively. Authorization policies are specified in terms of the entity model which is then instantiated for evaluating attribute values of the relevant entities (i.e. subject, object, action and environment). An authorization system called Auctoritas provides a policy language and an evaluation engine for EBAC (Bogaerts *et al.*, 2015). However, this model is neither popular nor commonly used like the other conventional access control models.

4.5 Access control by context

The access decision is not only relying on the policy in terms of subject and resource, but also contextual parameters, such as the sequence of events preceding the access attempt (i.e. history), location, time and sequence of responses, are taken into account. The permission to access resources is dependent on these contextual information, unlike the content-based access control, which makes access decisions according to the data values. The final decision is based on the result of reviewing the situation (Harris, 2012). The models in this class, as in the following, are often used as a complement to conventional access control models.

4.5.1 Emotion-based access control. A system could be in danger when an angry user is granted access despite being an authorized subject. The opposite scenario is also valid as there could be unauthorized individuals who need access urgently to save the system from risky incidents. Hence, this model introduces the concept of sensibility to access control systems instead of relying on the authorization component only.

The emotion factor (i.e. feelings of the person trying to access the protected resources) can be used as a complement to the existing access control mechanisms. Firstly, the spontaneous brain signals are recorded from the scalp of the requesting user in the sensing layer. This is primarily a hardware component called Emotiv EPOC headset which collects the EEG signals and transmits them to a listener module. The received data is then analyzed in a signal processing module where the emotions are classified into positive or negative. According to the emotion level, the decision maker determines whether to allow access to the requested resource or not (Almehmadi and El-Khatib, 2013). Although the emotion detection technology is a novel method in access control, it is still an ongoing research and not commonly used in practice.

4.5.2 Risk-based access control. This model, also referred to as risk-adaptive access control (RAdAC*)*, originated from the need of the enterprise to real-time assessment of the current situation and possible risks even when the subjects lack proper permissions. A possible strategy is to deny the access in this case, however, emergency data access is crucial in some domains (e.g. healthcare and military). Hence, this model introduces risk levels into the process of access decision such that the access is determined by computing the security risk and operational need (e.g. subject trustworthiness, information sensitivity and history events) instead of only using the rigid policies which provide the same decision in different circumstances. After the risky access event, the system will take some mitigating actions for minimizing possible information disclosure in the future. Several methods for estimating access risks are proposed by various works including machine learning (Molloy *et al.*, 2012), probability theory (Rajbhandari and Snekkenes, 2010) and fuzzy logic (Cheng *et al.*, 2007 and Ni *et al.*, 2010). The work of Atlam *et al.* (2020) provides a survey of the state-of-the-art risk-based access control model along with the existing risk estimation techniques (Section 5).

4.5.3 Sequence-based access control (SeqBAC). The SeqBAC model is used as a complement to existing access control models to restrict the order of actions performed on databases by legitimate users, e.g. read or write data. It is based on the fact that actions are not totally independent. In some cases, they are used to collect values for the subsequent ones. Thus, it is crucial to audit the sequences in which actions are executed to avoid bypassing the dependency logic between actions. Although this can be handled in the application or even using stored procedures, they are hard to manage and prone to implementation mistakes that can compromise the system correctness. Furthermore, the model allows more flexibility in terms of reusing and branching the sequences of actions which can be validated automatically in real-time. SeqBAC is based on a CRUD expression driven access control model where the policy defines a set of authorized users and a set of actions along with their input parameters and directed transition relations between them (i.e. action flowchart). The model concept and formal definition are proposed in Regateiro *et al.* (2018), however, it is still in the research phase, i.e. no actual implementation is provided.

4.5.4 History-based access control (HBAC). This model aims to maintain a selective history of the access requests initiated by individual subjects and use this history to identify potentially malicious requests. It protects software execution environments (e.g. operating systems and mobile code platforms) against potential damages caused by codes with inappropriate behavior. For example, a previously killed malicious program can be denied from execution on a specific machine by specifying a HBAC policy that keeps track of aborted programs identity along with their past termination events (Edjlali *et al.*, 1998).

History information is a sequence of events which are an abstraction of security-relevant activities (e.g. opening a socket connection and reading/writing a file) (Bartoletti *et al.*, 2005). Based on the sequence of requests, each program is dynamically classified to one of the defined equivalence classes and only access the allowed resources associated to the programs of that class. Authorization decisions depend on the real-time evaluation of access history of the inquiring party, e.g. behavior, time between requests, and content of requests. Execution monitors are the typical run-time mechanisms for enforcing history-based policies. They are responsible for observing computations and terminating them upon violating the defined authorization policy. HBAC has been the focus of many researches on the conceptual (Banerjee and Naumann, 2004; Fong, 2004) and implementation (Abadi and Fournet, 2003; Edjlali *et al.*, 1998) levels.

5. Comparative Studies

In this section, we review a selected list of access control model literature studies. The related works are sorted ascendingly by their publishing year. The older surveys focus on data security whereas the newer ones deal with access control in specific domains, e.g. cloud computing, social networks and internet of things (IoT). In the following, we summarize each of the survey works and map the presented access control models into our classification categories.

Access control: principle and practice (Sandhu and Samarati, 1994). This work is one of the earliest works in the area of access control. It provided a concrete explanation for authentication, administration (i.e. centralized, hierarchical, cooperative, ownership and decentralized), access control and auditing in addition to how they are related to each other. The difference between policy and mechanism is also illustrated. The DAC and MAC strategies are explained along with the access matrix including its implementation approaches (i.e. ACL, capabilities and authorization relations). They had a different perspective regarding RBAC because of being relatively recent at the time of publishing this work. They considered the role-based approach as an alternative to traditional DAC and MAC policies with several advantages, e.g. authorization management, hierarchical roles, least privilege, separation of duties and object classes.

Data security (Bertino, 1998). In this paper, Bertino surveyed the state of the art in access control for database systems and outlined the main research issues. The System R (Astrahan *et al.*, 1976) access control is discussed as the basic DAC model for protecting tables and views with specific access modes (i.e. select, insert, update and delete) in addition to the existing extensions for supporting negative authorizations (Bertino *et al.*, 1997), non-cascading revoke and temporal duration of authorizations (Bertino *et al.*, 1996a, 1996b). Moreover, RBAC as an extension to access control models is described as well as how MAC strategy is applied in databases enforcing the BLP principles and multilevel relational model using views. Finally, the research directions of access control for database systems are addressed with respect to data protection against intrusions (e.g. trojan horses and covert channels) besides developing authorization and access control models for advanced data management systems.

Access control: policies, models and mechanisms (Samarati and De Capitani di Vimercati, 2001). One of the earliest literature reviews providing definitions for security policy, model and mechanism. They clarified the basic concepts and explained the access control models along with the current implementations in the context of MAC, DAC and RBAC categories. Some models belong to only one category while others are hybrid. For instance, the Access Matrix is a DAC model whereas the Chinese Wall combines DAC with MAC policies. We partly relied on this classification, especially for the DAC and MAC strategies and the basic state-of-the-art access control models.

Database security – concepts, approaches and challenges (Bertino and Sandhu, 2005). In 2005, Bertino and Sandhu discussed database security with focus on confidentiality and integrity. They gave an overview of the System R model along with its extensions in the context of DAC, BLP principles as well as the MLS database model for applying MAC policies, RBAC models and content-based access control using views to enforce fine-grained authorization policies. Further, requirements and features for XML and object-based database systems are presented.

Survey on access control models (Sahafizadeh and Parsa, 2010). This work provided a short survey and comparison of access control models. They briefly explained only five access control models, i.e. MAC, BLP, MLS database, RBAC and VBAC, with a basic description of the main concepts. However, their definition of MAC is not consistent. They considered MAC as a model relying on the comparison of the subjects and objects sensitivity labels. Then, they referred to the MLS model as an implementation of the MAC idea. Thus, they did not clarify whether MAC is a model or a type. Finally, they evaluated all the models with respect to access control criteria:

- support for fine/coarse grained specification;
- evaluation using conditions;
- least privilege;
- support for single/multiple policy types;
- information used for making authorization decisions;
- use of application-specific information only while processing the client request;
- enterprise-wide consistent access control policy enforcement; and
- support for changes.

Access control for databases: concepts and systems (Bertino et al., 2011). This monograph presented a comprehensive state of the art about the access control approaches and models in the DBMS domain. They illustrated the current access control models in relational databases, i.e. the System R and multilevel relational model, which enforces the MAC strategy by classifying tuples and even cells at different access classes. Moreover, they explained how fine-grained access control is applied in databases through query rewriting, SQL extension and authorization views as techniques for content-based access control. Three case studies implemented in popular commercial DBMSs are presented:

(1) Microsoft's SQL Server 2008 DBMS with its base authorization model and access control administration features;

(2) the Oracle Virtual Private Database (VPD) technology (Browder and Davidson, 2002) for controlling database access at the level of columns and rows; and

(3) Oracle Label security mechanism implementing the strategy of MAC.

Last but not least, they gave an overview of access control models for object databases, XML data, Geographical data and digital libraries.

Database security and access control models: a brief overview (Kriti, 2013). The work of Kriti discussed the access control models in the context of databases presenting security threats and policy requirements as a motivation. An overview of the security models basic terms (i.e. subjects, objects, access modes, policies, authorizations, administrative rights and axioms) as well as the access control principles of administration (i.e. centralized vs decentralized), system (i.e. open vs closed) and privilege (i.e. minimum vs maximum) are provided. The DAC, MAC and RBAC are explained in addition to how they are applied in databases along with their vulnerabilities. For instance, the DAC authorization is applied in databases using *System R* model and its extensions, but vulnerable to trojan horse attacks.

Taxonomy and classification of access control models for cloud environments (Majumder et al., 2014). The authors classified various existing access control models according to a proposed taxonomy of access control schemes for cloud environments. They discussed the access control challenges in cloud computing regarding cost, granularity, data loss, taking the data sensitivity into account, data theft by malicious users and accessing data from an outside server. Furthermore, they explained 11 models (Table 1) and analyzed them based on:

- identity vs nonidentity in terms of whether the model is tree-structured or not; and
- centralized (i.e. per user, group users and all users) vs collaborative.

Different access control mechanisms (Sifou et al., 2017). This work analyzed and compared different access control models in the context of cloud computing. Based on the National Institute of Standards and Technology's (NIST) view in (Mell *et al.*, 2011), the authors illustrated the main features of cloud computing service and deployment models. They demonstrated DAC, MAC, RBAC, ABAC and OrBAC along with the advantages and disadvantages of each access control model. According to the current cloud computing requirements, they defined nine criteria to evaluate the current access control models: dynamicity, flexibility, reliability, ease of administration, security policy implementation, global management, support scalability, computational costs and fine-grained access.

Survey on access control mechanisms in cloud computing (Karatas and Akbulut, 2018). The work of Karatas and Abkulut provided a survey of access control approaches and works related to cloud computing. They reviewed 109 research papers in that domain throughout the past decade. They provided not only a comparative explanation for the existing access control models, but also a unique evaluation using NIST access control metrics (Hu and Scarfone, 2012). For each access control model, an overview followed by an analysis with respect to the applicable criteria is given. The models are reviewed according to the satisfaction degree for each metric (i.e. low, medium, high, optional, not applicable and not mentioned). Additionally, their study is compared versus seven other survey works in terms of the presented approaches, graphical definitions, advantages/disadvantages, the use of NIST metrics, number of reviewed articles and queried databases (e.g. IEEE, ACM, Springer, etc).

A Survey on access control in the age of internet of things (Qiu et al., 2020). The article presented a survey on the access control characteristics, technologies, a taxonomy of access control models requirements and future development direction in the IoT research field. In the IoT environment, the data are dynamic, massive, need strong privacy and continuously exchanged between different cooperation organizations. This work is compared with other literature reviews with similar focus in terms of access control policy description method, combination, conflict resolution and authoring (i.e. attribute discovery mechanism, policy mining and authorization model) explaining each requirement in detail. They described the authorization by categories based on the following: ABAC, RBAC, capability-based access control (CapBAC), usage control-based access model (UCON), OrBAC, blockchain and open authorization (OAuth).

Risk-based access control model: a systematic literature review (Atlam et al., 2020). A systematic review of the risk-based access control model is provided. According to their search strategy, they chose 44 recent studies to summarize their contributions, analyzed the various risk factors and investigated the used risk estimation techniques. First, they briefly illustrated:

- the aim of access control;
- the difference between authentication, authorization and access control;
- the five core elements of access control models (i.e. subjects, objects, actions, privileges and access policies); and
- the access control process flow.

Furthermore, they compared the static and dynamic access control models with respect to features, decision, pros/cons, examples and applications. For the traditional access control approaches, they just mentioned ACL, DAC, MAC and RBAC with a basic description. Then, an overview of the risk-based access control model and its elements is provided. Finally, they addressed the research methodology phases and analyzed the results providing answers to the research questions through comparing all the selected works.

In summary, Table 1 presents the models addressed in the previously discussed surveys with respect to our classification. We indicate whether all the models (✓) listed for each category in Section 4, some of them (O) or none (✕) are addressed in a given citation. For the roles category, all the works discuss the standard RBAC in different levels of details, however, only three of them addressed the OrBAC model while the ARBAC model is not mentioned at all.

We also include the models that are not stated in our work under the column *Other*. Only one access control model related to databases, i.e. System R (Griffiths and Wade, 1976), is not mentioned. The rest belong to cloud computing and IoT domains, e.g. gateway-based access control (GBAC) (Wu *et al.*, 2012), novel data access control (NDAC) (Gao *et al.*, 2013), usage control-based access model (UCON) (Danwei *et al.*, 2009), purpose-based usage access control

Table 1. Models included for each category in the survey works list

Citation	OSA	MsR	Roles	Content	Context	Other
Sandhu and Samarati (1994)	✓	O[b,c]	O	✕	✕	
Bertino (1998)	✕	O[b]	O	O[h]	✕	System R
Samarati and De Capitani di Vimercati (2001)	✓	✓[d]	O	✕	✕	
Bertino and Sandhu (2005)	✕	O[b]	O	O[h]	✕	
Sahafizadeh and Parsa (2010)	✕	O[b,e]	O	O[h]	✕	
Bertino *et al.* (2011)	✓	O[b]	O	O[h,i]	✕	System R
Kriti (2013)	✕	O[b,c]	O	✕	✕	System R
Majumder *et al.* (2014)	O[a]	✕	✓[g]	O[i]	✕	CapBAC, PBAC, TTAC, GBAC, NDAC, UCON
Sifou *et al.* (2017)	✕	✕	✓[g]	O[i]	✕	
Karatas and Akbulut (2018)	✕	✕	O	O[i]	✕	FGAC, HABE, ABE-FGAC
Qiu *et al.* (2020)	✕	O[b,c,f]	✓[g]	O[i,j]	✕	CapBAC, UCON, P-ABAC
Atlam *et al.* (2020)	O[a]	✕	O	✕	O[k]	

Notes: [a] ACL; [b] BLP; [c] Biba; [d] Except Lipner; [e] MLS; [f] Clark–Wilson; [g] Except ARBAC; [h] VBAC; [i] ABAC; [j] ReBAC; [k] RAdAC

(PBAC) (Sun and Wang, 2010), toward temporal-based access control (TTAC) (Zhu *et al.*, 2012), fine-grained access control (FGAC) (Li *et al.*, 2010), capability-based access control (CapBAC) (Hota *et al.*, 2011), hierarchical attribute-based access control (HABE) (Xie *et al.*, 2015), attribute-based encryption fine-grained access control (ABE-FGAC) (Tamizharasi *et al.*, 2016) and privacy-preserving ABAC (P-ABAC) (Xu *et al.*, 2018).

6. Analysis

Based on the results of our literature study in Sections 4 and 5, we define ten criteria to study the differences between the five classes of access control models presented in Section 4. We partly relied on the standard metrics for evaluating access control systems from NIST (Hu and Scarfone, 2012) and added other criteria to make it feasible in selecting the appropriate class and access control model according to the application security requirements. The criteria along with their description are listed below:

- *Authorization strategy*: whether MAC, DAC or hybrid (recall Section 3);
- *Dynamic authorization*: represents the dynamic definition of access rights in terms of rules and policies evaluating their attributes in real-time;
- *Granularity of control*: indicates the objects' levels of granularity, i.e. fine and/or coarse grained;
- *Least privilege principle support*: the minimum access rights required for performing a task;
- *Separation of duty*: ensures that access is only granted to subjects that are duty-related to the objects to limit power and avoid conflict of interests;
- *Vulnerable to attacks*: is for ensuring the safety of the model to avoid the leakage of permissions to an unauthorized principal, e.g. trojan horse and covert channel attacks;
- *Bypass*: is about whether policy rules are allowed to be bypassed for critical access decisions in emergency situations or not and how tolerant the risk is;
- *Conflict resolution or prevention*: deals with preventing or resolving deadlocks and conflicting rules from the same or different policies;
- *Operational/situational awareness*: considers operational/situational factors (e.g. some environment variables) in access rules specification and enforcement (i.e. decision-making);
- *Privileges/capabilities discovery*: is the discovery of capabilities/objects (or object groups) of a given subject (or subject group) and vice versa.

After defining the selected criteria, we summarize them against our access control models categories in Table 2. For each criterion, we indicate whether it is satisfied by all the models within a given classification group (✓), partially supported either with further considerations (i.e. based on access control requirements and model implementation) or by specific access control models within that category (O) or not at all (✕). If applicable, the level of satisfaction is indicated, i.e. low (L), medium (M) or high (H).

7. Conclusion

Access control mitigates the risks of unauthorized access attempts to data, resources and systems. The definition of authorization and access control in addition to their related

Table 2. Access control model categories analysis with respect to the defined criteria

Criteria	OSA	MsR	Roles	Content	Context
Authorization strategy	DAC	MAC	Hybrid	Hybrid	Hybrid
Granularity of control	L	L[a]	M	H	H
Least privilege principal support	L	M	M	H	O[b]
Dynamic authorization	×	×	✓	✓	✓
Separation of duty	×	O[c]	✓	✓	✓
Vulnerable to attacks	✓	✓	×	×	×
Bypass	×	×	×	×	✓
Conflict resolution or prevention	×	×	×	O[d]	O[b]
Operational/situational awareness	×	×	✓	✓	✓
Privileges/capabilities discovery	✓	×	✓	O[e]	×

Notes: [a]Except the MLS database model; [b]Depends on the underlying access control model; [c]Supported by the *Chinese-Wall* model; [d]Supported by *ABAC* and *EBAC* models; and [e]Supported by the VBAC model

concepts (i.e. strategy, model, policy and mechanism) are inconsistent in the literature. Besides, there are a lot of existing access control models; some of them are commonly known and used in practice while others have evolved recently and are not yet popular like the conventional models. The already available access control survey works are either including the state-of-the-art models at the publishing time or focusing on the taxonomy and classification of models for a particular domain.

In this paper, we first discussed authorization and access control along with the terms related to our research on the level of strategy, model and instance. We then explained authorization strategies and proposed a general classification for access control models without being restricted to a specific field (e.g. cloud computing and IoT). Moreover, we provided some examples of access control models along with the current implementations and extensions for the five categories, i.e. explicit object-subject assignment, model-specific rules, roles, content and context. We selected a list of comparative studies about survey, taxonomy and evaluation of access control models. Then, we summarized each work and compared the included models according to our classification. Finally, we analyzed the proposed classes of models with respect to several criteria; some of them are selected from the NIST standard access control system evaluation metrics, according to the level of support and considerations (if any).

The comparison result (Table 1) shows that we discussed more models than other works for all the categories. We did not include advanced domain-specific models as we focus on general access control models with a view to databases.

References

Abadi, M. and Fournet, C. (2003), “Access control based on execution history”, *NDSS*, Vol. 3, pp. 107-121.

Abrams, M.D. (1995), “Renewed understanding of access control policies”, in *Proceedings of the 16th National Computer Security Conference-Information System Security: User Choices*, pp. 87-96.

Ahmad, A. and Whitworth, B. (2011), “Access control taxonomy for social networks”, in *2011 7th International Conference on Information Assurance and Security*. (Ed.) by Ieee Corporate Author. IEEE, pp. 256-261, ISBN: 978-1-4577-2155-7, doi: 10.1109/ISIAS.2011.6122829.

Almehmadi, A. and El-Khatib, K. (2013), “Authorized! access denied, unauthorized! access granted”, in *Proceedings of the 6th International Conference on Security of Information and Networks*, pp. 363-367.

Astrahan, M.M., Blasgen, M.W., Chamberlin, D.D., Eswaran, K.P., Gray, J.N., Griffiths, P.P., King, W.F., Lorie, R.A., McJones, P.R., Mehl, J.W., Putzolu, G.R., Traiger, I.L., Wade, B.W. and Watson, V. (1976), "System R: relational approach to database management", *ACM Transactions on Database Systems (TODS)*, Vol. 1 No. 2, pp. 97-137.

Atlam, H.F., Azad, M.A., Alassafi, M.O., Alshdadi, A.A. and Alenezi, A. (2020), "Risk-based access control model: a systematic literature review", *Future Internet*, Vol. 12 No. 6, p. 103, doi: 10.3390/fi12060103.

Banerjee, A. and Naumann, D.A. (2004), "History-based access control and secure information flow", In *International Workshop on Construction and Analysis of Safe, Secure, and Interoperable Smart Devices*. Springer, pp. 27-48.

Bartoletti, M., Degano, P. and Ferrari, G.L. (2005), "Historybased access control with local policies", in Sassone, V. (Ed.), *Foundations of Software Science and Computational Structures*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 316-332. ISBN: 978-3-540-31982-5.

Bell, D.E. and La Padula, L.J. (1976), Secure computer system: unified exposition and multics interpretation, *Tech. rep. Mitre Corp Bedford MA*.

Benantar, M. (2005), *Access Control Systems: security, Identity Management and Trust Models*, Springer Science and Business Media.

Bertino, E., Bettini, C., Ferrari, E. and Samarati, P. (1996a), "A temporal access control mechanism for database systems", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 8 No. 1, pp. 67-80.

Bertino, E., Bettini, C., Ferrari, E. and Samarati, P. (1996b), "Supporting periodic authorizations and temporal reasoning in database access control", *VLDB*, Citeseer, pp. 472-483.

Bertino, E., Samarati, P. and Jajodia, S. (1997), "An extended authorization model for relational databases", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 9 No. 1, pp. 85-101.

Bertino, E., Bonatti, P.A. and Ferrari, E. (2000), "TRBAC: a temporal role-based access control model", in *Proceedings of the 5th ACM Workshop on Role-Based Access Control*, pp. 21-30.

Bertino, E. and Sandhu, R. (2005), "Database security – concepts, approaches, and challenges", *IEEE Transactions on Dependable and Secure Computing*, Vol. 2 No. 1, pp. 2-19.

Bertino, E., Ghinita, G. and Kamra, A. (2011), "Access control for databases: concepts and systems", *Foundations and Trends in Databases*, Vol. 3 Nos 1/2, pp. 1-148, doi: 10.1561/1900000014, ISSN: 1931-7883.

Bertino, E. (2016), "Data security and privacy: concepts, approaches, and research directions", in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, pp. 400-407, ISBN: 978-1-4673-8845-0, doi: 10.1109/COMPSAC.2016.89.

Bertino, E. (1998), "Data security", *Data and Knowledge Engineering*, Vol. 25 Nos 1/2, pp. 199-216.

Bogaerts, J., Decat, M., Lagaisse, B. and Joosen, W. (2015), "Entity-based access control: supporting more expressive access control policies", In *Proceedings of the 31st Annual Computer Security Applications Conference*, pp. 291-300.

Brewer, D.F. and Nash, M.J. (1989), "The Chinese wall security policy", in IEEE symposium on security and privacy, Oakland ,Vol. 1989, p. 206.

Browder, K. and Davidson, M.A. (2002), "The virtual private database in oracle9ir2", In: Oracle Technical White Paper, Oracle Corporation 500.280.

Center, Computer Security Resource (2022), "Glossary", available at: https://csrc.nist.gov/glossary (accessed 14 April 2022).

Cheng, P.-C., Rohatgi, P., Keser, C., Karger, P.A., Wagner, G.M. and Reninger, A.S. (2007), "Fuzzy multi-level security: an experiment on quantified risk-adaptive access control", in *2007 IEEE Symposium on Security and Privacy (SP'07)*, IEEE, pp. 222-230.

Clark, D.D. and Wilson, D.R. (1987), "A comparison of commercial and military computer security policies", in *1987 IEEE Symposium on Security and Privacy*, IEEE, pp. 184-184.

Council, Information Technology Industry (2016), "Information technology: next generation access control - generic operations and data structures (NGAC GOADS)", *in American National Standard for Information Technology INCITS, 526-2016*.

Council, Information Technology Industry (2018), "Information technology: next generation access control - functional architecture (NGAC-FA)", in *American National Standard for Information Technology INCITS, 499-2018*.

Crampton, J. and Loizon, G. (2002), SARBAC: a new model for role-based administration. Tech. rep. Technical Report BBKCS-02-09, *Birkbeck College, University of London*.

Cuppens, F. and Miège, A. (2003), "Administration model for or-BAC", in Meersman, R. and Tari, Z. (Eds), *On The Move to Meaningful Internet Systems 2003: OTM 2003 Workshops*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 754-768, ISBN: 978-3-540-39962-9.

Damiani, M.L., Bertino, E., Catania, B. and Perlasca, P. (2007), "GEO-RBAC: a spatially aware RBAC", *ACM Transactions on Information and System Security (TISSEC)*, Vol. 10 No. 1, p. 2–es.

Danwei, C., Xiuli, H. and Xunyi, R. (2009), "Access control of cloud service based on ucon", in *IEEE International Conference on Cloud Computing*, Springer, pp. 559-564.

Eckert, C. (2014), *IT-Sicherheit*, 9th ed., De Gruyter Oldenbourg, ISBN: 978-3-486-85916-4.

Edjlali, G., Acharya, A. and Chaudhary, V. (1998), "History-based access control for mobile code", in *Proceedings of the 5th ACM Conference on Computer and Communications Security*, pp. 38-48.

Ferraiolo, D.F. and Kuhn, D.R. (1992), "Role-based access controls", in *Proceedings of the 15th NIST-NSA National Computer Security Conference*, pp. 554-563.

Ferraiolo, D., Cugini, J. and Kuhn, D.R. (1995), "Role-based access control (RBAC): features and motivations", in *Proceedings of the 11th annual computer security application conference*, pp. 241-248.

Ferraiolo, D., Chandramouli, R., Kuhn, R. and Hu, V. (2016), "Extensible access control markup language (XACML) and next generation access control (NGAC)", in *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control*, pp. 13-24.

Ferrari, E. (2009), "Access control", in Tamer Ozsu, M. and Ling, L. (Eds), *Encyclopedia of Database Systems*, Springer, New York, NY, pp. 7-11, doi: 10.1007/978-0-387-39940-9_6, isbn: 978-0-387-35544-3.

Fong, P.W. (2004), "Access control by tracking shallow execution history", *IEEE Symposium on Security and Privacy*, IEEE, pp. 43-55.

Fong, P.W. (2011), "Relationship-based access control: protection model and policy language", in *Proceedings of the first ACM conference on Data and application security and privacy*, pp. 191-202.

Gao, X., Jiang, Z.M. and Jiang, R. (2013), "A novel data access scheme in cloud computing", *Advanced Materials Research*, Vols 756/759, pp. 2649-2654.

Gates, C. (2007), "Access control requirements for web 2.0 security and privacy", in *IEEE Web 2.0*, pp. 12-15.

Griffiths, P.P. and Wade, B.W. (1976), "An authorization mechanism for a relational database system", *ACM Transactions on Database Systems (TODS)*, Vol. 1 No. 3, pp. 242-255.

Harris, S. (2012), *CISSP All-in-One Exam Guide*, 6th ed., McGraw-Hill, New York, NY, Chicago, San Francisco, Lisbon, London, Madrid, Mexico City, Milan, New Delhi, San Juan, Seoul, Singapore, Sydney, Toronto, ISBN: 978-0-07-178173-2.

Hosseini, A. and Azgomi, M.A. (2010), "HRBAC: historical role-based access control".

Hota, C., Sanka, S., Rajarajan, M. and Nair, S.K. (2011), "Capability-based cryptographic data access control in cloud computing", *International Journal of Advanced Networking and Applications*, Vol. 3 No. 3, pp. 1152-1161.

Hu, H., Ahn, G.-J. and Jorgensen, J. (2012), "Multiparty access control for online social networks: model and mechanisms", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 25 No. 7, pp. 1614-1627.

Hu, V.C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R. and Scarfone, K. (2014), "Guide to attribute based access control (ABAC) definition and considerations", *NIST Special Publication*, Vol. 800, p. 162, doi: 10.6028/NIST.SP.800-162, available at: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-162.pdf

Hu, V.C., Ferraiolo, D.F., Chandramouli, R. and Kuhn, D.R. (2017b), *Attribute-Based Access Control*, Artech House.

Hu, V.C. and Scarfone, K. (2012), *Guidelines for Access Control System Evaluation Metrics*, *National Institute of Standards and Technology*, Gaithersburg, MD, doi: 10.6028/NIST.IR.7874.

Hu, V.C., Kuhn, R. and Yaga, D. (2017a), "Verification and test methods for access control policies/models", *NIST Special Publication*, Vol. 800, p. 192.

Hu, V. (2016), "Access control policy and implementation guides", available at: https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides (accessed 14 April 2022).

IBM-Corporation (2015), "Authentication versus access control", available at: www.ibm.com/docs/en/wca/3.5.0?topic=security-authentication-versus-access-control (accessed 14 April 2022).

Josang, A. (2017), "A consistent definition of authorization", in Livraga, G. and Mitchell, C. (Eds), *Security and Trust Management*, Lecture Notes in Computer Science, Springer International Publishing, Cham, Vol. 10547, pp. 134-144, isbn: 978-3-319-68062-0, doi: 10.1007/978-3-319-68063-7_9.

Kalam, A.A.E., Baida, R.E., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miége, A., Saurel, C. and Trouessin, G. (2003), "Organization based access control", in *Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks*, IEEE, pp. 120-131.

Kane, K. and Browne, J.C. (2006), "On classifying access control implementations for distributed systems", in Ferraiolo D. and Ray I. (Eds), *Proceedings of the eleventh ACM symposium on Access control models and technologies*, *ACM Digital Library, ACM*, New York, NY, p. 29, isbn: 1595933530, doi: 10.1145/1133058.1133064.

Karatas, G. and Akbulut, A. (2018), "Survey on access control mechanisms in cloud computing", *Journal of Cyber Security and Mobility*, doi: 10.13052/2245-1439.731, ISSN: 2245-1439.

Keefe, T.F., Tsai, W.-T. and Srivastava, J. (1993), "Database concurrency control in multilevel secure database management systems", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 5 No. 6, pp. 1039-1055.

Kizza, J.M. (2020), "Access control and authorization", Kizza, J.M. (Ed), *Guide to Computer Network Security Texts in Computer Science*, Springer International Publishing, Cham, pp. 187-206, isbn: 978-3-030-38140-0, doi: 10.1007/978-3-030-38141-7_9.

Kriti, I.K. (2013), "Database security and access control models: a brief overview", *International Journal of Engineering Research and Technology (IJERT)*, Vol. 2 No. 5.

Kuhrmann, M., Fernández, D.M. and Daneva, M. (2017), "On the pragmatic design of literature studies in software engineering: an experiencebased guideline", *Empirical Software Engineering*, Vol. 22 No. 6, pp. 2852-2891.

Li, J., Zhao, G., Chen, X., Xie, D., Rong, C., Li, W., Tang, L. and Tang, Y. (2010), "Fine-grained data access control systems with user accountability in cloud computing", In *2010 IEEE Second International Conference on Cloud Computing Technology and Science*,IEEE, pp. 89-96.

Majumder, A., Namasudra, S. and Nath, S. (2014), "Taxonomy and classification of access control models for cloud environments", in Zaigham, M. (Ed), *Continued Rise of the Cloud, Computer Communications and Networks*, Springer London, London, pp. 23-53, isbn: 978-1-4471-6451-7, doi: 10.1007/978-1-4471-6452-4_2.

Matt, B. (2018), *Computer Security: art and Science*, Addison-Wesley Professional, isbn: 978-0-13-409714-5.

Mell, P. and Grance, T, (2011), "The NIST definition of cloud computing", National Institute of Science and Technology, Special Publication.

Molloy, I., Dickens, L., Morisset, C., Cheng, P.-C., Lobo, J. and Russo, A. (2012), "Risk-based security decisions under uncertainty", in *Proceedings of the 2nd ACM conference on Data and Application Security and Privacy*, pp. 157-168.

Ni, Q., Bertino, E. and Lobo, J. (2010), "Risk-based access control systems built on fuzzy inferences", in *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 250-260.

OASIS (2013), "Extensible access control markup language (XACML) version 3.0", OASIS Open, available at: http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html (accessed 14 April 2022).

Park, J. and Sandhu, R. (2002), "Originator control in usage control", in *Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks*, IEEE, pp. 60-66.

Petkovic, M. and Jonker, W. (2007), *Security, Privacy, and Trust in Modern Data Management*, Springer.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B. (2020), "A survey on access control in the age of internet of things", *IEEE Internet of Things Journal*, Vol. 7 No. 6, pp. 4682-4696, issn: 2327-4662, doi: 10.1109/JIOT.2020.2969326.

Rajbhandari, L. and Snekkenes, E.A. (2010), "Using game theory to analyze risk to privacy: an initial insight", in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*, Springer, pp. 41-51.

Regateiro, D., Pereira, Ó. and Aguiar, R. (2018), "SeqBAC: a sequence based access control model", In *Proceedings of the 30th International Conference on Software Engineering and Knowledge Engineering (SEKE 2018)*, pp. 276-319, doi: 10.18293/SEKE2018-099.

Rjaibi, W. (2004), "An introduction to multilevel secure relational database management systems", in *Proceedings of the 2004 Conference of the Centre for Advanced Studies on Collaborative Research*, pp. 232-241.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and Mcquaid, R. (2021), "Developing cyber-resilient systems", Gaithersburg, MD, doi: 10.6028/NIST.SP.800-160v2r1, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf (accessed 14 April 2022).

Sahafizadeh, E. and Parsa, S. (2010), "Survey on access control models", in *2010 2nd International Conference on Future Computer and Communication* ,IEEE, Vol. 1.

Samarati, P. and De Capitani di Vimercati, S., *et al.* (2001), "Access control: policies, models, and mechanisms", in Goos, G. (Ed), *Foundations of Security Analysis and Design*, Lecture Notes in Computer Science, Springer Berlin Heidelberg, Berlin, Heidelberg, Vol. 2171, pp. 137-196, isbn: 978-3-540-42896-1, doi: 10.1007/3-540-45608-2_3.

Sandhu, R., Coyne, E.J., Youman, C.E. and Feinstein, H.L. (1996), "Role-based access control models", *Computer*, Vol. 29 No. 2, pp. 38-47, doi: 10.1109/2.485845.

Sandhu, R.S. and Samarati, P. (1994), "Access control: principle and practice", *IEEE Communications Magazine*, Vol. 32 No. 9, pp. 40-48, ISSN: 0163-6804, available at: https://ieeexplore.ieee.org/document/312842 (accessed 14 April 2022).

Sandhu, R., Bhamidipati, V. and Munawer, Q. (1999), "The ARBAC97 model for role-based administration of roles", *ACM Transactions on Information and System Security*, Vol. 2 No. 1, pp. 105-135, doi: 10.1145/300830.300839, issn: 1094-9224.

Sifou, F., Kartit, A. and Hammouch, A. (2017), "Different access control mechanisms for data security in cloud computing", in *Proceedings of the 2017 International Conference on Cloud and Big Data Computing*, ACM, *New York, NY*, pp. 40-44, isbn: 9781450353434, doi: 10.1145/3141128.3141133, available at: https://dl.acm.org/doi/pdf/10.1145/3141128.3141133 (accessed 14 April 2022).

Sun, L. and Wang, H. (2010), "A purpose based usage access control model", *International Journal of Computer and Information Engineering*, Vol. 4 No. 1, pp. 44-51.

Tamizharasi, G.S., Balamurugan, B. and Manjula, R. (2016), "Attribute based encryption with fine-grained access provision in cloud computing", in *Proceedings of the International Conference on Informatics and Analytics*, pp. 1-4.

Tapiador, A, Carrera, D. and Salvachúa, J. (2012), "Tie-RBAC: an application of RBAC to social networks", CoRR abs/1205.5720, arXiv: 1205.5720, available at: http://arxiv.org/abs/1205.5720

Wu, Y., Suhendra, V. and Guo, H. (2012), "A gateway-based access control scheme for collaborative clouds", in *Proceedings of the 7th International Conference on Internet Monitoring and Protection*, pp. 54-60.

Xie, U., Wen, H., Wu, B., Jiang, Y. and Meng, J. (2015), "A modified hierarchical attribute-based encryption access control method for mobile cloud computing", *IEEE Transactions on Cloud Computing*, Vol. 7.2, pp. 383-391.

Xu, Y., Zeng, Q., Wang, G., Zhang, C., Ren, J. and Zhang, Y. (2018), "A privacy-preserving attribute-based access control scheme", in *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*, Springer, pp. 361-370.

Zeng, W., Yang, Y. and Luo, B. (2014), "Content-based access control: use data content to assist access control for large-scale content-centric databases", in *2014 IEEE International Conference on Big Data*, IEEE, pp. 701-710.

Zhu, Y., Hu, H., Ahn, G.-J., Huang, D. and Wang, S. (2012), "Towards temporal access control in cloud computing", in *2012 Proceedings IEEE Infocom*, IEEE, pp. 2576-2580.

Corresponding author
Aya Khaled Youssef Sayed Mohamed can be contacted at: aya.mohamed@jku.at