Access Control Techniques

Access control techniques: Access control techniques are used to manage and regulate the access to resources and data in a computer system or network.

Types of Access Control Techniques:

Constrained User, Access control Matrix, Content-dependent, Context – dependent

Content Dependent Access Control: Content dependent access control is a method of performing access control based on the type of content contained in an object. Imagine that an organization keeps track of the types of content held in each object. Certain subjects are allowed to access certain types of content. A subject is allowed to access an object if the object contains only types of content that the subject is allowed to access.

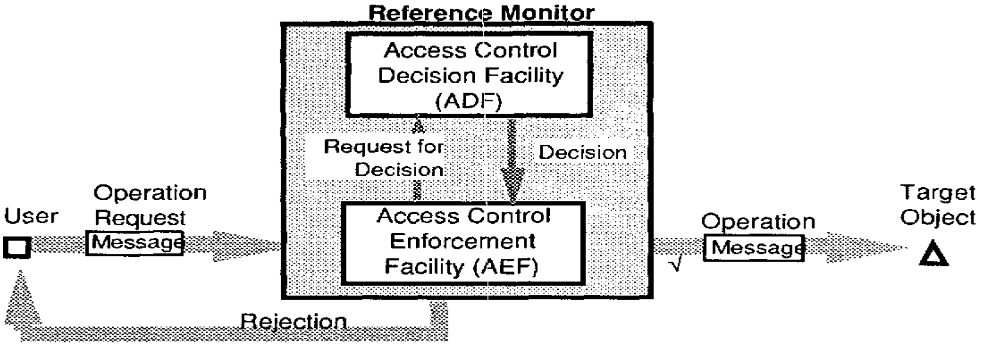
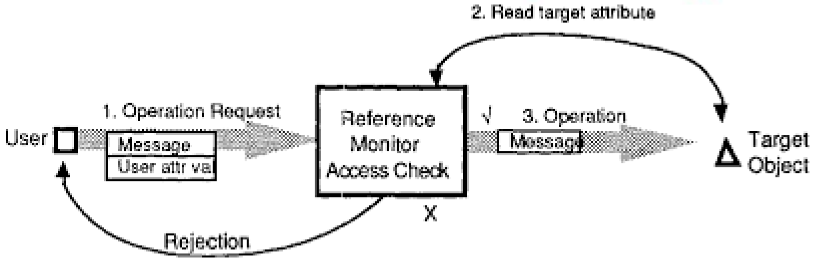

Reference Monitor
Access Control Decision Facility (ADF)
Request for Decision
Decision
Access Control Enforcement Facility (AEF)
User
Operation Request Message
Operation Message
√
Target Object
Rejection

Figure 2 Reference Monitor

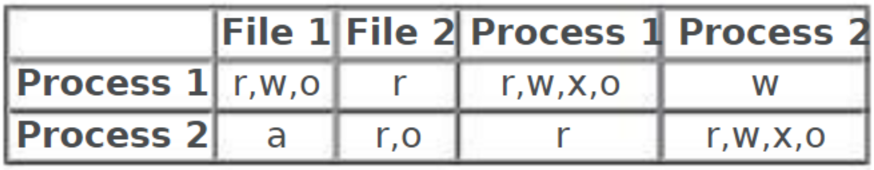
Context Based Access Control : Context based access control is an access control method based on the context of a subject's request to an object, in addition to just the identities of the subject and object themselves. This is a little different from other methods, and requires more information to make a decision.

For example, consider an organization with an employee, Bob. Usually, Bob reads information about the organization's transactions at the end of each week to ensure that nothing suspicious is happening.



Constrained User Interfaces: One way that we can enforce access control is by constraining the user interface used to get access. This can be done by not allowing certain types of access on the interface, or not including the ability to request certain types of access, or access to certain objects. There are three major types of constrained user interfaces. They include menus and shells, database views, and physically constrained interfaces.

Access Control Matrix (ACM) In addition to constraining user interfaces, we can control access to objects through other methods such as access control matrices. Imagine that we have a table, where each row corresponds to a subject in a system and each. column corresponds to an object in the system. Then, each cell in the table corresponds to a subject-object pair, and can contain what access rights the subject has to the object. An example of an access control matrix is demonstrated below.



	File 1	File 2	Process 1	Process 2
Process 1	r,w,o	r	r,w,x,o	w
Process 2	a	r,o	r	r,w,x,o

In this example we have two subjects, Process 1 and Process 2, and each of them could have the following rights over an object: read (r), write (w), execute (x), append (a), and own (o). This is quite straightforward, but things get interesting when we begin to pay attention to the objects of the system.

Access Control Lists (ACLs) One problem with access control matrices is that they can grow very large very quickly. Imagine a system with thousands of subjects, and millions of objects. Storing the matrix itself becomes a very costly thing to do. In order to address this problem, we have the concept of an access control list. An access control list (ACL) is a set of permissions that correspond to an object. Each permission usually specifies a subject and an access right to the object. For example, consider a system with three subjects: Alice, Bob, and Carla. The following represents an ACL for a file on this system, File A. acl(File A): {(Alice: write), (Bob: read, execute)} As we can see in the example above, Alice can write to File A, and Bob can read and execute File A. Since Carla is not mentioned on the ACL, she has no rights to access File A in any way

Constrained User Access Control:

Constrained User Access Control, also known as Discretionary Access Control (DAC), is a technique where access permissions are associated with users or processes. In this model, users have control over the access permissions for their own resources, and they can grant or revoke access to others. It's called "constrained" because users can only control access within the constraints defined by the system administrator. Each resource (e.g., files, folders) has an associated Access Control List (ACL) that specifies which users or groups can access it and what type of access they have (read, write, execute, etc.). This technique is commonly used in desktop operating systems like Windows and Unix-based systems.

Access Control Matrix:

The Access Control Matrix (ACM) is a model that represents the access control policies of a system in a matrix format. It lists all the subjects (users or processes) in rows and all the objects (resources) in columns. The cells of the matrix indicate the permissions or access rights each subject has on each object. This technique allows for a clear and concise representation of access control rules but can become unwieldy in systems with many subjects and objects. It's mainly used for formal analysis of access control systems and is not as common in practical implementations.

Content-dependent Access Control:

Content-dependent access control focuses on controlling access to resources based on the content or attributes of those resources. For example, a content-dependent access control system can restrict access to certain documents or data based on keywords, classification, or sensitivity levels contained within the content. This technique is often used in information classification and data leakage prevention systems, where access is determined by the content's characteristics rather than just the user's identity or role.

Context-dependent Access Control:

Context-dependent access control considers various contextual factors when determining access rights. These factors may include the user's location, time, device, network conditions, and more. Access is dynamically adjusted based on the context to enhance security and flexibility. For example, a context-dependent access control system might grant different levels of access to a user based on whether they are accessing a system from within the company's office network or from an external location. Context-dependent access control is particularly useful for mobile and remote access scenarios where the context of access can change frequently.