(۱۵) احراز هویت براساس آن چیزی هست: در این نوع احراز هویت از مشخصه های بیولوژیکی فرد، نظیر: اثر انگشت، عنبیه چشم، چهره، صوت و موارد مشابه برای احراز اصالت استفاده می شود. به این نوع احراز اصالت در مقایسه با دو نوع قبل آن است که فرد ممکن است ~~اطلاعات مربوطه~~ رمز یا داشته خود را به ترتیب فراموش یا گم کند اما خواص بیولوژیکی او همواره همراه اوست.

با این حال مسأله اصلی استفاده از چنین احراز هویتی، هزینه بالا و پیچیدگی مسئله مربوط به آن است.

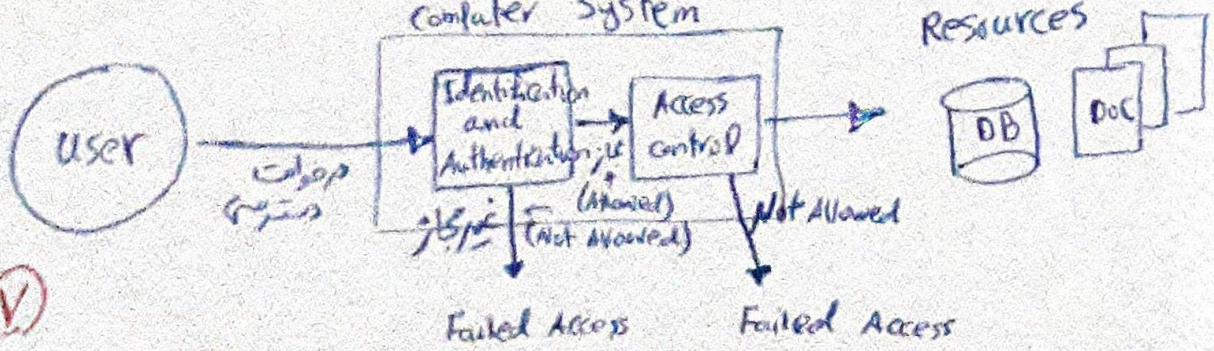
(۱۶) لازم به ذکر است که همواره می بایست از اطلاعات مربوط به احراز هویت (گذرواژه، توکن، مشخصه های بیولوژیکی که در قالب داده در شبکه جریان دارد و یا بر روی سیستم ذخیره شده) مستقر است اطمینان حاصل کرد.

(احراز هویت کننده)

(۱۷) کنترل دسترسی (Access control)

کنترل دسترسی به عنوان یک مکانیزم مرکزی برای حفظ امنیت در هر سیستم (اساسی) کامپیوتری به شمار می آید. این مکانیزم مسئولیت کنترل دسترسی کاربران و دیگر سیستم های کامپیوتری به منابع و اطلاعات یک سیستم یا شبکه (سازمانی) را بر عهده دارد.

سناریو مدل کلی یک سیستم کامپیوتری مجهز به مکانیزم کنترل دسترسی به صورت زیر است:



همانطور که در شکل فوق مشخص است پس نیاز کنترل دسترسی، شناسایی کاربر و احراز اصالت هویت فرد مورد ادعاست. پس از شناخت کاربر و تصدیق ادعای او، دسترسی های کاربر به منابع بر اساس تدابیر اعمیز و منع شده توسط مدیر سامانه امکان پذیری میشود.

(۱۸) مکانیزم های کنترل دسترسی را برحسب نحوه انتشار حقوق (مجوزها) می توان به سه رده کلی زیر تقسیم بندی کرد:

۱ـ کنترل دسترسی اختیاری (DAC = Discretionary Access Control)،

۲ـ کنترل دسترسی اجباری (MAC = Mandatory Access Control)،

۳ـ کنترل دسترسی نقش-مبنا (RBAC = Role-Based Access Control).

پیش از شرح مختصر هریک از روش های بالا نیاز است تا برخی از مفاهیم را معرفی کنیم.

عامل (subject): هر آنکه متقاضی دسترسی به منبع یا اطلاعات است.
به عنوان مثال یک عامل در سامانه می تواند یک عامل انسانی، عامل ماشینی، برآنند، یک وب سرویس و یا موارد مشابه باشد.

شی یا منبع (object or Resource): هر آنچه مورد دسترسی قرار می گیرد. به عنوان مثال یک شی می تواند یک فایل، یک جدول پایگاه داده، یک برآنند و موارد مشابه باشد.

عمل (Action): به عملی اطلاق می شود که توسط یک عامل بر روی شی یا منبع اعمال می شود. به عنوان مثال یک عمل می تواند خواندن، نوشتن، تغییر، حذف، چاپ و موارد مشابه باشد.

نکته: یک موجودیت (عنصر) در سامانه می تواند هم نقش عامل و هم نقش شی را در یک زمان داشته باشد. به عنوان مثال یک برآنند در تعامل با یک وب سرویس در محیط وب

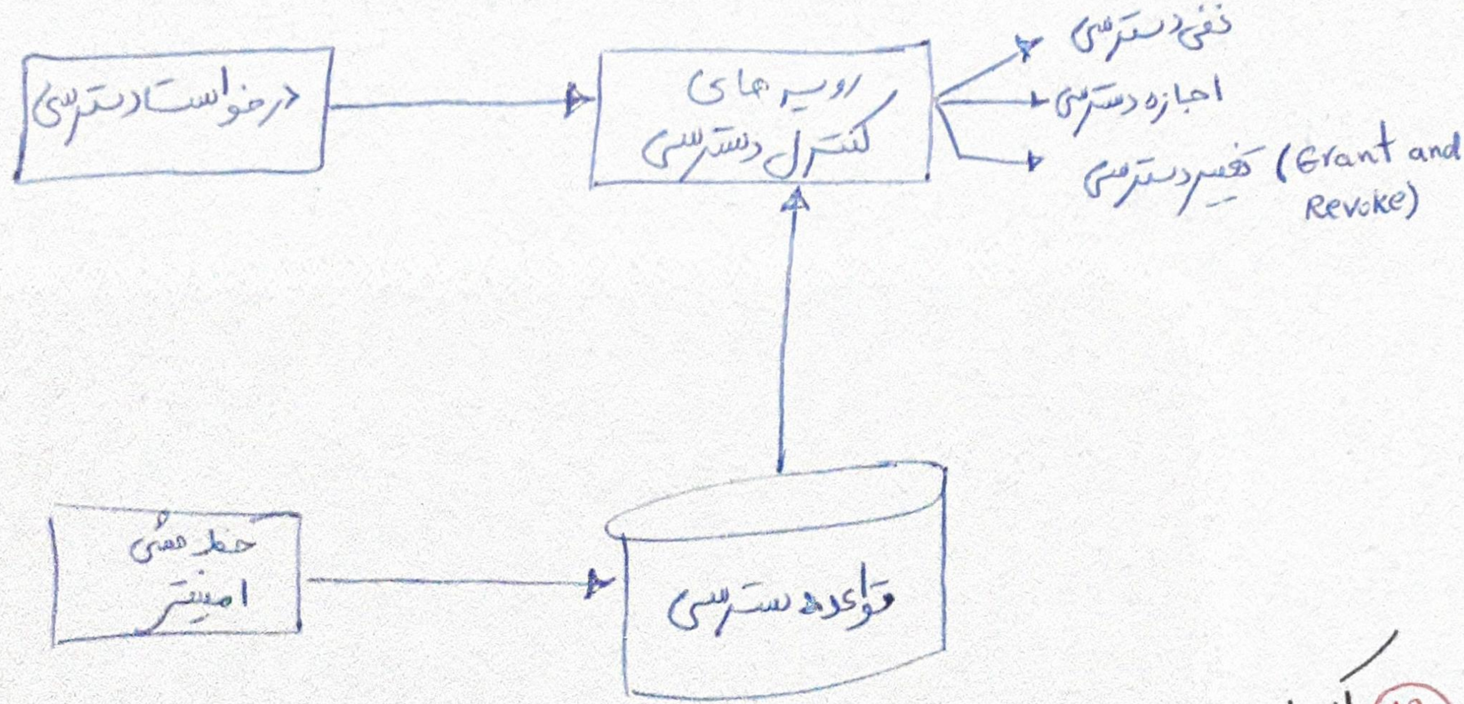
عنوان اصلی

می‌توانند نمونه‌هایی از چنین موجودیتی در سامانه شناخته شوند.

قواعد دسترسی: خط مشی‌های کنترل دسترسی (Access control Policy) در قالب مجموعه‌ای از قواعد دسترسی (Access Rules) بیان می‌گردد و تعیین کننده آن است که هر عامل هایی اجازه انجام چه اعمالی را بر روی چه اشیائی دارند یا ندارند.

از حیث ساز و کار کلی

نکته: با توجه به مفاهیم معرفی شده در بالا، یک مکانیزم کنترل دسترسی در سامانه سناریو عملی مشابه شکل زیر دارد.



(۱۹) کنترل دسترسی اختیاری:

در این مدل، عامل ها مالک اشیا هستند و اختیار دارند دسترسی به اشیا را به هر عامل مورد نظری اعطا (Grant) یا از آن سلب (Revoke) کنند.

یکی از مدل های پیاده سازی چنین کنترل دسترسی، استفاده از ماتریس دسترسی به شکل زیر است.

ACL

	فرآیند ۱	فایل ۱	فرآیند ۲	فایل ۲
فرآیند ۱ (C-List)	O, R, W	—	R	R, W
فرآیند ۲	W	O, R	O, R, W	—

حاشیه: R=Read، W=write و O=Owner است.

در شکل فوق، دو اصطلاح ACL برای ستون اول و C-List برای سطر اول نشان داده شده است که در ادامه هر یک از آنها را تعریف می کنیم.

- لیست کنترل دسترسی (ACL = Access Control List): لیستی است که در آن لیست عامل ها و مجوزهای آنها در کنار هر شی یا منبع مربوطه قرار می گیرد.

لیست توانایی (C-List = Capability List): لیستی است که در آن مجوزهای دسترسی عامل ها به اشیا در کنار هر عامل نگهداری می شود.

برخی معایب کنترل دسترسی اختیاری عبارتند از:

۱. در این مدل با حجم زیادی از مجوزها و افراد سروکار داریم.

۲. در این مدل سیاستی برای انتشار کنترل دسترسی (اعطا و ابطال مجوز به صورت آشکار) لحاظ نشده است.

(۲) کنترل دسترسی اجباری:

در این مدل، کنترل دسترسی عامل ها به اشیا براساس سطوح امنیتی و یکسری قواعد به طور معمول ثابت تعریف می شود.

به عنوان مثال در یک سازمان نظامی می توان عامل ها و اشیا را به صورت زیر (از اهمیت زیاد به کم) در نظر گرفت:

عامل ها	اشیاء
سرتیپ	اطلاعات به کلی سری
سرهنگ	اطلاعات سری
سرگرد	اطلاعات خیلی محرمانه
سروان	اطلاعات محرمانه
ستوان	⋮
استوار	
⋮	

قواعد برای چنین مدلی می‌تواند به صورت‌های زیر تعریف شود:

۱. سرهنگ به اطلاعات سری و پایین‌تر از آن دسترسی خواندن و نوشتن دارد و به اطلاعات بسیار سری (اطلاعات بالاتر) فقط مجوز خواندن دارد.

۲. سرگرد به اطلاعات محرمانه دسترسی خواندن دارد، به اطلاعات بالاتر از آن دسترسی خواندن و نوشتن ندارد و به اطلاعات پایین‌تر از اطلاعات محرمانه تنها مجوز خواندن دارد.

(۲۱) کنترل دسترسی نقش معنا

در این مدل، کنترل دسترسی براساس نقش ما در سیستم اعطا می‌شود و هدف از این کار آن است که عامل ما (کاربران) دائماً در سازمانه در حال تغییر هستند اما نقش ما تقریباً ثابت می‌باشد.

شکل زیر ساختار دسترسی در چنین مدلی را نشان می‌دهد.