- **اعطای مجوز(Authorization)** : اعطای یک امتیاز یا مجوزبه کاربر، به نحوی که کاربر با استفاده از آن دردستیابی به داده‌های مورد نظرش مجاز می‌شود را اعطای مجوز گویند.
- **تأیید اصالت یا احراز هویت(Authentication)** : بر اساس تصمیمات محدودیتی برای درخواست‌های دستیابی به داده ، سیستم باید توانایی تشخیص کاربرانی که درخواست را دارند، داشته باشد. برای نمونه علاوه برکنترل شناسه، سیستم رمز عبور افراد را هم کنترل می‌کند و به این وسیله کاربران احراز هویت یا تایید اصالت می‌شوند.

- **روش اختیاری (DAC):** در اینجا توضیحاتی بیشتر در زمینه DAC خواهیم داد. در این روش کاربران، معمولاً قوانین دستیابی مختلفی روی داده‌های مختلف دارند که به آن امتیازات(Privileges) گویند. این امتیازات به کاربران اعطاء و هرگاه لازم باشد سلب می‌شود. در این روش محدودیت‌هایی برای کاربران به منظور دسترسی به داده‌ها ایجاد می‌شود. مانند این‌که کاربر ۱ می‌تواند A را ببیند ولی B را نمی‌تواند، درصورتی‌که کاربر ۲ می‌تواند B را ببینید ولی A را نمی‌تواند، بنابراین، این روش بسیار انعطاف‌پذیر است.

نمونه:

```
AUTHORITY SA3
        GRANT RETRIEVE {S# , SNAME, CITY}, DELETE
          ON S
          TO Jim, Fred, Mary;
```

دراین جا به Mary , Fred , Jim اجازه دسترسی به صفات یا فیلدهای S#، CITY, SNAME و حذف رکوردها یا تاپل‌ها روی S داده شده است .

نمونه دیگر :

```
VAR SSPO VIEW
      { S  JOIN SP  JOIN {P  WHERE  CITY = 'Oslo' } {P#} }
                                  {ALL BUT P#,QTY};
   AUTHORITY EX3
      GRANT RETRIEVE
        ON      SSPO
        TO      Lars;
```

در این‌جا به Lars اجازه دسترسی به تاپل‌های دید(View) تعریف شده به نام SSPO داده شده است.

همانطور که دیده می‌شود، تعریف دید، نوعی محدودیت در دسترسی به داده‌ها ایجاد می‌کند. لذا خود مقوله تولید دید در پایگاه داده می‌تواند به امنیت بیشتر ختم شود.

- **بررسی ردپا (Audit trail):** بررسی ردپا یا حسابرسی، روشی برای برآورده شدن امنیت و جامعیت است. یعنی علاوه بر امنیت، در مقوله‌ای مانند ترمیم هم به کار می‌رود. در این روش، یک فایل یا پایگاه داده خاص وجود دارد که درآن سیستم به طور اتوماتیک مراحل همه عملیات‌ها را که توسط کاربران برروی داده‌های مجاز انجام شده است، نگهداری می‌کند. دربعضی ازسیستم‌ها، این بررسی مسیر به طور فیزیکی در بخش ثبت ترمیم ذخیره می‌شود که شامل اطلاعات زیر می‌باشد :
  - ✓ درخواست‌ها
  - ✓ پایانه‌ای ازعملیات درخواست شده
  - ✓ تاریخ وزمان عملیات
  - ✓ متغیرهای رابطه ای ، صفات و تاپل‌های ساخته شده
  - ✓ مقادیر قبلی
  - ✓ مقادیر جدید

این فایل مشابه همان فایل ثبت(Log File) است که در بحث ترمیم در مورد آن صحبت شد. این اطلاعات می‌تواند به نحوی ذخیره شود که برای بررسی ردپای اعمال غیرمجاز و ضد امنیتی در سیستم نیز به کار رود.

- **روش الزامی (MAC):** دراین روش به هرشیء یا واحد داده یک عدد که نشان دهنده سطح محرمانگی(Classification level) آن است، منتسب می‌شود . به‌علاوه، هرکاربر نیز یک مجوز برای دستیابی به داده با سطح محرمانگی مشخصی را دارد. بنابراین تنها کاربر دارای مجوزدستیابی به یک شی داده‌ای، می‌تواند به آن دستیابی داشته باشد. این روش درمحیط‌های نظامی یا با امنیت بالا کاربرد دارد. MAC شامل دو قانون می‌باشد :
  - ✓ ویژگی امنیتی ساده(Simple security property): کاربر i می‌تواند داده j را بخواند، اگر سطح مجوز i ، بالاتر یا مساوی سطح محرمانگی j باشد.
  - ✓ ویژگی امنیتی ستاره‌دار(Starred security property): کاربر i می تواند داده j را بنویسید، اگرسطح مجوز i برابر با سطح محرمانگی j باشد. دلیل آن اعمال کنترل بیش‌تر روی کاربران است.

- **امنیت چند سطحی:** فرض کنید ما می‌خواهیم روش الزامی را برای متغیر رابطه‌ای S پیاده سازی کنیم. برای این منظور می‌خواهیم این روش را روی تاپل مستقل اعمال کنیم که هر تاپل احتیاج به برچسب گذاری بر اساس سطح محرمانگی دارد. برای نمونه می توان چنین طبقه بندی برای تاپل‌های S داشت: ۴ = فوق سری ،۳ = سری ،۲ = خیلی محرمانه ،۱ = محرمانه. به دلیل این‌چنین طبقه‌بندی‌هایی است، که به اسناد ذخیره شده در این ساختار، اسناد طبقه‌بندی شده می‌گویند.
  جدول زیر می‌تواند در این مورد توضیح دهد:

S

S#	SNAME	STATUS	CITY	LEVEL
S1	Smith	20	London	2
S2	Jones	10	Paris	3
S3	Black	30	Paris	2
S4	Clark	20	London	4
S5	Adams	30	Athens	3

فرض کنید که کاربران U3 و U2 به ترتیب دارای سطح مجوز ۳ و ۲ هستند. بنابراین U3و U2 به صورت جداگانه می‌توانند متغیررابطه‌ای S را ببینند و اگر درخواست دیدن تمام تاپل‌ها را داشته باشند، U3 می‌تواند چهار تاپل (S1 , S2 , S3 , S5) را ببیند. ولی U2 فقط دوتاپل (S1 , S3) را می‌تواند ببیند و هیچ کدام از این دو کاربر نمی‌توانند S4 را ببینند.

- **پایگاه داده آماری(Statistical database)**: پایگاه داده‌ای است که به پرس و جوها(Queries) اجازه می‌دهد از اطلاعات اطلاعات تجمعی به‌دست آورند. برای نمونه مجموع یا میانگین و حقوق کارمندان. اما اطلاعات فردی مانند حقوق یک کارمند را نتوانند بپرسند. یکی از مشکلاتی که در این پایگاه داده وجود دارد این است که از نتایج پرسش‌های مجاز، پاسخ های غیرمجاز استنباط شود.

نمونه : فرض کنید که پایگاه داده فقط شامل یک متغیر رابطه‌ای STATS می‌باشد.

NAME	SEX	CHILDREN	OCCUPATION	SALARY	TAX	AUDITS
Alf	M	3	Programmer	50K	10K	3
Bea	F	2	Physician	130K	10K	0
Cyn	F	0	Programmer	56K	18K	1
Dee	F	2	Builder	60K	12K	1

فرض کنید که کاربر U فقط مجاز به اجرای پرسش‌های آماری می‌باشد. او می‌داند که Alf برنامه نویس و مرد و با این اطلاعات می‌خواهد حقوق Alf را بیابد. سعی می‌کند با پرسش‌های آماری این داده را بیابد:

```
1. WITH (STATS WHERE SEX = 'M' AND
        OCCUPATION = 'Programmer') AS  X :
         COUNT (x)
             Result :1.
2. WITH (STATS WHERE SEX ='M' AND
        OCCUPATION= 'Programmer') AS  X:
        SUM(X,SALARY)
     ReSult : 50k .
```

در این جا امنیت پایگاه داده به خطر افتاده، حتی اگرکاربر U فقط اجازه طرح پرسش آماری داشته باشد. با توجه به مثال، اگر کاربر بتواند یک عبارت بولی پیدا کند که خصوصیت انفرادی توسط آن قابل تعریف باشد دیگر آن خصوصیت انفرادی دارای امنیت پایینی خواهد بود. در این حالت پیشنهاد می‌شود که برای حالت‌هایی که کاردینالیتی مجموعه خلاصه شده کم‌تر از حدی باشد سیستم باید از پاسخ دادن به این پرسش جلوگیری کند. مثلا وقتی جواب پرس و جوی نخست، ۱ می‌شود این پاسخ نباید به کاربر ارائه شود. در واقع کاربر نباید اطلاعاتی که کاردینالیتی آن از حدی (مثلا ۲ یا ۳) کمتر می‌شود را ببیند.

فرض کنید که این محدودیت در پایگاه داده آماری اضافه شده. حال ممکن است کاربر U از راه دیگری وارد شود:

3. COUNT (STATS)
Resualt : 4.

4. WITH (STATS WHERE NOT (SEX = ‘M’ AND OCCUPATION = ‘Programmer’)) AS X :
COUNT (X)
Resualt : 3
4 – 3 = 1

5. SUM(STATS, SALARY)
Resualt : 296

6. WITH (STATS WHERE NOT(SEX = ‘M’ AND OCCUPATION = ‘Programmer’)) AS X :
SUM (X, SALARK)
Resualt : 246
296 – 246 = 50 K

به نظر می‌آید که این محدودیت نه تنها در حد پایین، بلکه در حد بالای کاردینالیتی هم باید رعایت شود. اما باز هم راه‌هایی برای کاربرانی که می‌خواهند از داده های تجمعی ردگیری فردی(Individual tracking) کنند وجود دارد.

- **رمزگذاری داده(Data Encryption)**: تا زمانی‌که درون یک سامانه محلی هستیم و این سامانه با دنیای خارج ارتباط ندارد، ممکن است با تکنیک‌های ارائه شده بتوان امنیت داده‌ها را تا حد زیادی رعایت کرد. اما در دنیای حاضر که داده‌ها در سیستم‌های توزیع‌شده‌ای در سطح اینترنت در جریان هستند، به چیزی بیشتر نیاز داریم و آن اینکه اگر داده به هر نحوی به دست فرد غیرمجاز افتاد، امکان فهمیدن یا ایجاد تغییر غیر مجاز در آن را نداشته باشد. یکی از مهمترین راهکارها، رمزگذاری است. در الگوریتم‌های رمز گذاری به داده‌ای که رمز نشده اصطلاحا متن ساده(Plain Text) و به داده رمز شده اصطلاحا متن رمزشده(Ciphered Text) گفته می‌شود.معمولا الگوریتم‌های رمزنگاری از یک یا چند کلید برای رمزنگاری و رمزگشایی

استفاده می‌کنند. خود الگوریتم‌های رمزنگاری معمولا شناخته شده هستند. اما طوری طراحی شده‌اند که بدون داشتن کلید، رمزگشایی بسیار بسیار سخت خواهد بود.

در الگوریتم‌های رمزنگاری معمولا از دو روش جانشینی و جایگشت یا تلفیق این دو استفاده می‌شود. در روش جانشینی به جای داده ها، داده های دیگری جانشین می‌شود. مثلا هر جا حرف A باشد، به جایش حرف E قرار گیرد و به همین ترتیب برای حروف دیگر. این‌که جانشینی با چه فرمولی انجام شود را کلید مشخص می‌نماید. در جایگشت ترتیب چینش داده‌ها تغییر می‌کند و در نتیجه این دو روش باعث می‌شوند که داده رمز شده برای کسی که کلید رمزنگاری مورد نظر را ندارد به یک داده بی معنی تبدیل شود.

از معروف‌ترین الگوریتم‌های رمز نگاری که از سال ۱۹۷۷ به عنوان یک استاندارد در سیستم‌های کامپیوتری استفاده شد، الگوریتم DES (Data Encryption Standard) است. در این الگوریتم کلیدها ۶۴ بیتی (در واقع ۵۶ بیت کلید و ۸ بیت توازن) هستند و متن ساده برای رمز گذاری به بلوک‌های ۶۴ بیتی تقسیم می‌شوند و در ۱۶ مرحله تحت جانشینی و جایگشت قرار می‌گیرند.

با وجود پیچیدگی DES، با افزایش کارایی کامپیوترها این رمزنگاری در حدود سال ۲۰۰۰ در معرض خطر قرار گرفت، این بود که از سال ۲۰۰۰ برای امنیت بیشتر امکان استفاده از استاندارد جدیدی به نام AES (Advance Encryption Standard) فراهم شد. در این الگوریتم امکان داشتن کلیدها با طول بیشتر، مثلا ۱۲۸ یا ۲۵۶ بیتی به وجود آمد.

- **کلید عمومی(Public Key) و کلید خصوصی(Private Key)**: یکی از مشکلات الگوریتم‌های رمزنگاری تک کلیده این است که یک کلید هم برای رمزنگاری و هم رمزگشایی وجود دارد. لذا رساندن این کلید به مقصد، خود یک چالش است. بنابراین الگوریتم‌های رمزنگاری با دو کلید تولید شد. اگر متن ساده با یکی از این کلیدها رمز شود. تنها با کلید دوم باز خواهد شد. حال در تماس بین رو گره در یک سیستم، هر گره یکی از این زوج کلیدها تولید می‌کند. یکی را که به آن کلید خصوصی گفته می‌شود، نزد خود نگاه می‌دارد و دیگری که به کلید عمومی موسوم است، برای گره دیگر ارسال می‌کند. این روش هم برای محرمانه ماندن داده های ارسالی و هم اطمینان طرف مقابل از هویت درست فرستنده استفاده می‌شود. به این مورد آخری، اصطلاحا امضای دیجیتال گفته می‌شود.