امنیت پایگاه داده
DataBase Security

جلسه اول- مرور بر مباحث

مسعود نیازی ترشیز

www.mniazi.ir

تعریف ایمنی

- ایمنی عبارتست از حفاظت داده ها در قبال دستیابی غیرمجاز، تغییر غیر مجاز یا تخریب آنها و نیز در قبال دستیابی به داده ها با سوء نیت

تفاوت ایمنی با جامعیت

- در ایمنی: مسئله حفاظت داده ها در مقابل کاربر غیر مجاز مطرح است و حصول اطمینان از اینکه کاربران به انچه که بدان اقدام می ورزند مجازند.
- در جامعیت: نوعی حفاظت داده ها در مقابل عملیات کاربر مجاز اعمال می شود و حصول اطمینان از اینکه اقدام کاربر مجاز، صحیح است و صحت و دقت داده ها را خدشه دار نمی کند.

شباهت ایمنی با جامعیت

- سیستم مدیریت پایگاه داده ها از وجود پاره ای قواعد محدودیتها که کاربران نباید نقض کنند، باید آگاه باشد.
- محدودیتها و قواعد باید به نحوی توصیف شوند و در کاتالوگ نگهداری گردند.
- باید روی عملیات کاربر نظارت داشته باشد.

امنیت پایگاه داده ها مشتمل بر سه جنبه مهم زیر است:

1. محرمانگی: به مفهوم جلوگیری یا کشف افشای غیر مجاز اطلاعات
2. صحت: به مفهوم جلوگیری یا کشف تغییرات یا اصلاحات غیرمجاز اطلاعات
3. دسترس پذیری: به مفهوم جلوگیری یا کشف ممانعت غیر مجاز از سرویسهای فراهم شده سیستم

Threats خطرات

- خطر هر وضعیت و رویدادی است که عمدا یا سهوا روی سیستم و در نتیجه روی سازمان تاثیر نامساعد داشته باشد.

رده بندی خطرات

- خطرات فیزیکی
- خطرات منطقی

انواع خطرات

- خطرات غیرعمدی(اتفاقی)
  - درخواست سهوی داده از سوی کاربر غیر مجاز
  - بروز خرابی سخت افزاری
  - قطع برق و از بین رفتن داده ها و ....
- خطرات عمدی
  - استراق سمع
  - سوء استفاده از گذرواژه یک کاربر مجاز
  - تهدید و ارعاب کاربران مجاز و ....

شیئ ایمنی

- داده ها (از سطح صفت تا کل پایگاه داده ها)
- برنامه ها و تراکنشها
- کاتالوگ سیستم
- نسخه های پشتیبان
- فایلهای ثبت
- خود سیستم مدیریت پایگاه داده ها
- سیستم عامل
- سخت افزار
- شبکه
- محیط فیزیکی
- اعضا تیمهای مدیریتی
- کاربران سیستمها

تدابیر ایمنی

- تدابیر غیر کامپیوتری
  - وضع سیاستهای ایمنی و تعیین طرح مقابله
  - کنترل افراد
  - جایدهی تجهیزات در مکانهای امن
  - تنظیم توافق نامه ها از سوی طرف ثالث
  - تنظیم توافق نامه های نگهداری
  - کنترل دستیابی فیزیکی افراد

تدابیر ایمنی (ادامه)

- تدابیر کامپیوتری
  - شناسایی کاربر
  - تشخیص اصلیت کاربر
  - مجاز شماری و مدیریت آن
  - کنترل دستیابی
  - کنترل دستیابی از طریق قفل گذاری
  - نهان نگاری
  - استفاده از مفهوم دید خارجی
  - فرایند رد گیری
  - کنترل گردش اطلاعات
  - کنترل استنتاج

User Identification شناسایی کاربر

- به هر کاربر یک شناسه داده می شود و از طریق آن سیستم، کاربر را می شناسد.
- کاربر ممکن است: منفرد، گروه کاربران یا سلسله مراتب کاربران باشد.

User Authentication تشخیص اصلیت کاربر

- آیا کاربر همان است که ادعا می کند یا احیانا مجعول است.
- مبتنی بر یک یا چند مورد زیر است:
  - چیزی که کاربر بداند
  - چیزی که کاربر مالک آن است
  - چیزی که کاربر از نظر بیولوژیک دارد

تشخیص اصلیت کاربر (ادامه)

- این امکانات وجود دارند:
  - گذر واژه
  - اثر انگشت
  - الگوی شبکه چشم
  - کارت الکترونیکی
  - پرسشنامه
  - نشان
  - بعضی ویژگیهای فیزیولوژیک

Authorization مجاز شماری

- عبارتست از اعطای یک حق یا امتیاز یا مجوز به کاربر به نحوی که کاربر با استفاده از آن در دستیابی به داده های مورد نظرش مجاز می شود

برای اقدامات زیر می توان به کاربر امتیاز داد:

- ایجاد و حذف میدان
- ایجاد و حذف رابطه (جدول) مبنا
- اضافه کردن یا حذف کردن ستونی از جدول مبنا
- ایجاد و حذف دید
- ایجاد و حذف یک محدودیت جامعیتی
- ایجاد و حذف یک استراتژی دستیابی
- اعطا یا سلب یک حق دستیابی با منظور مشخص
- درخواست یک جدول لحظه ای
- بازیابی از جدول مبنا یا جدول مشتق
- درج در جدول
- حذف از جدول
- بهنگام سازی جدول
- تولید آرشیو از روی جدول

نمونه ای از قواعد یا محدودیتهای ایمنی

کاربر	داده	عمل مجاز	محدودیت ایمنی
U100	رابطه ORDER	درج	مبلغ سفارش کمتر از ۱۰۰۰۰۰۰ریال
U200	رابطه ORDER	بازیابی	–
U250	رابطه EMPLOYEE	بازیابی	کارمندان ساعتی
U300	اجازه بازیابی از رابطه EMPLOYEE	اعطاء حق	به u250

کنترل دستیابی

- روش DAC

(Discretionary Access Control)

- روش MAC

(Mandatory Access Control)

- روش مبتنی بر نقش RBAC

(Role Based Access Control)

DAC روش اختیاری

- این روش برای کنترل دستیابی امتیازاتی به کاربران اعطا می کند و هرگاه لازم باشد از آنها سلب می نماید.
- کاربران مختلف می توانند حقوق متفاوت روی شیئ واحد داده داشته باشند.
- مدیریت مجاز شماری لزوما حالت متمرکز ندارد و حالات زیر می تواند وجود داشته باشد:

1. مدیریت متمرکز: یک نفر اجازه دهنده مجوزها را می دهد و سلب می کند.
2. مدیریت سلسله مراتبی: یک نفر مسئول واگذاری مسئولیتهای مدیریتی به سایر مدیران است. این مدیران خود می توانند مجوزها را به کاربران بدهند یا سلب کنند.
3. مدیریت جمعی (تعاونی): با همیاری و همکاری چند نفر اعطا مجوز انجام می شود.
4. مدیریت تملکی: کاربر ایجاد کننده هر شیئ مالک آن است و مجوزها را او میدهد.
5. مدیریت نامتمرکز: مالک شیئ می تواند اختیار مدیریت مجاز شماری آن را به دیگران تفویض کند
6. ترکیب حالات قبلی

قواعد کنترل ایمنی

- هر قاعده دارای اجزای زیر است:
  - نام قاعده
  - یک یا بیش از یک امتیاز
  - حیطه اعمال قاعده
  - یک یا بیش از یک کاربر
  - اقدام در صورت عدم رعایت قاعده

```
CREATE SECURITY RULE <rule name>
GRANT    <privileges list>
ON       <expression>
TO       <users>
ON VIOLATION <action>
```

یک مثال

```
CREATE SECURITY RULE SR1
GRANT  RETRIEVE (COID,COTITLE,CREDIT)
ON     COT WHERE COT.DEID=D101 OR
       COT.CEID=D202
TO     U1,U2
ON VIOLATION REJECT
```

قواعد کنترل ایمنی (ادامه)

برای حذف قاعده از دستور زیر استفاده می شود:

DESTROY SECURITY RULE <rule name>

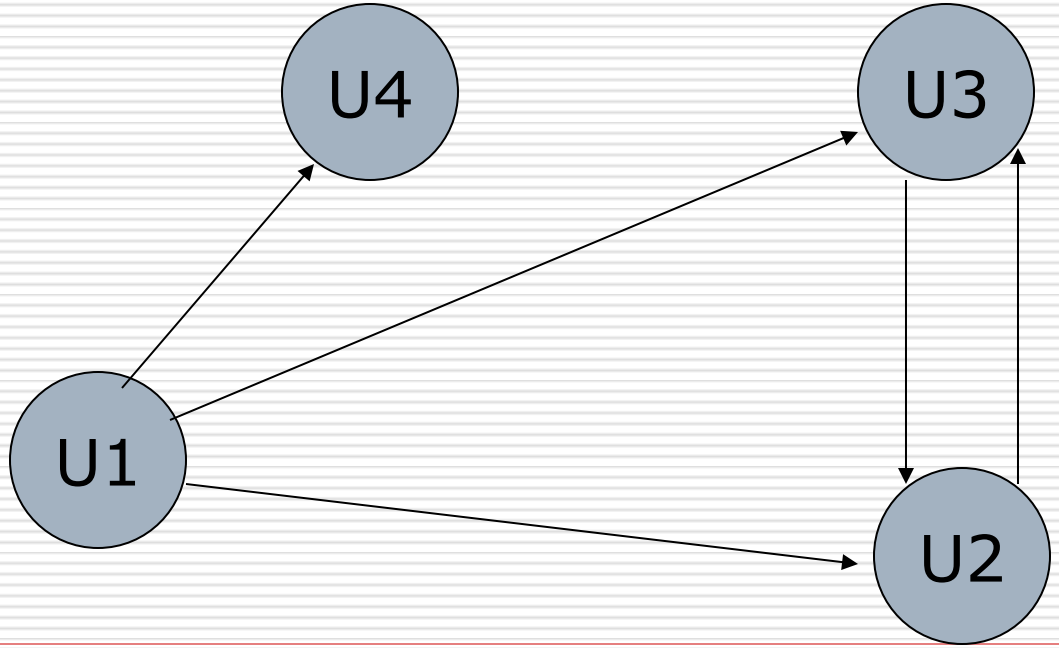
مزایا و معایب

- مزیت روش اختیاری این است که بسیار انعطاف پذیر است
- عیب آن این است که کاربر غیرمجاز ازطریق کاربر مجاز می تواند امتیازاتی را کسب کند. از این نظر روش قابل اطمینانی نیست. بعلاوه کاربر می تواند امتیاز خود را به کاربر دیگر اعطا کند (**انتشار امتیاز**) در این صورت عملیات سلب امتیاز با مشکلاتی مواجه می شود.

اعطا و سلب امتیاز

U1 امتیاز p1 را به U2و U3 می دهد.

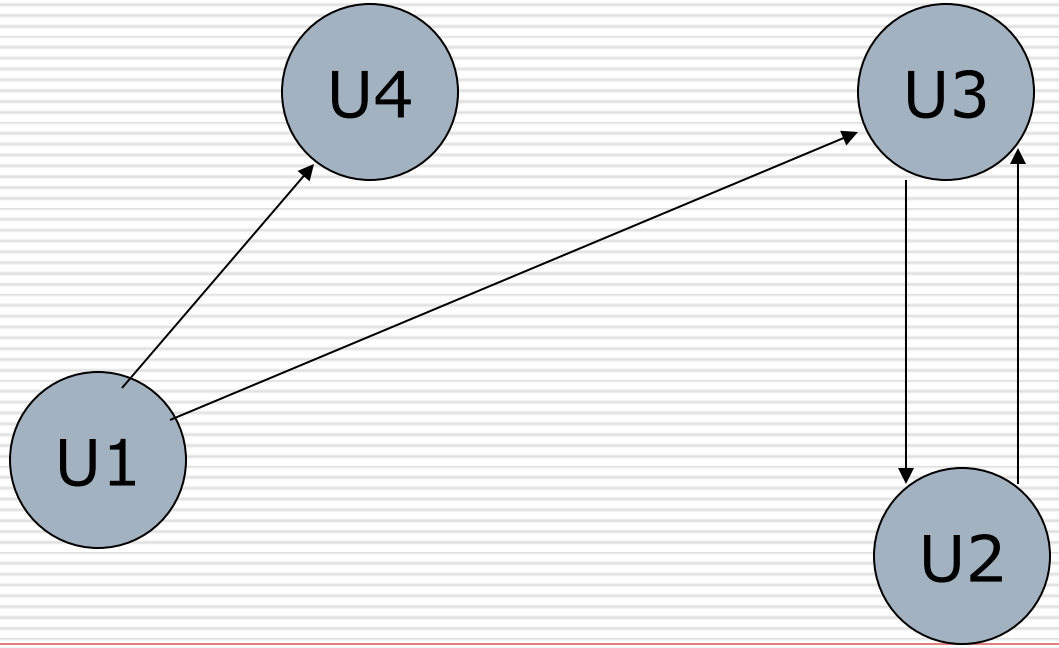
U2و U3 نیز متقابلا این امتیاز را به هم می دهند.



اعطا و سلب امتیاز (ادامه)

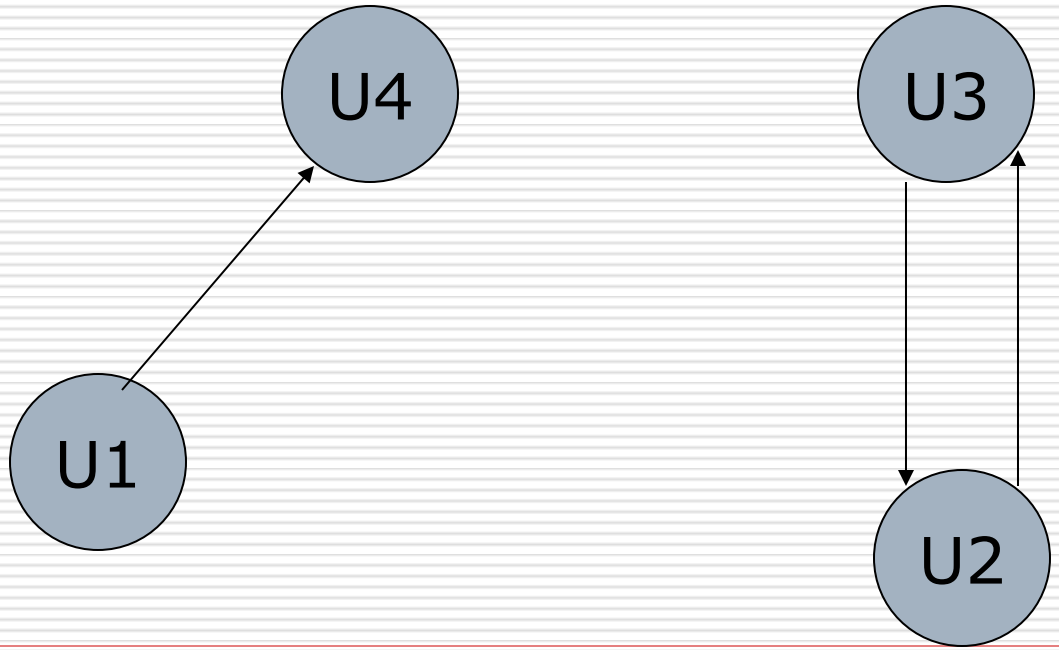
حال U1 امتیاز p1 را از u2 سلب می کند.

U2 هنوز از طریق U3 این امتیاز را در اختیار دارد.



اعطا و سلب امتیاز (ادامه)

حتی اگر U1 از U3 نیز سلب امتیاز نماید، باز هم امتیاز از U2 و U3 سلب نمی شود.



تکنیکهای محدود کردن انتشار امتیاز

- انتشار افقی
  - با مشخص کردن یک عدد صحیح i برای کاربر دارای یک امتیاز، به این کاربر اجازه اعطای امتیاز به حداکثر i کاربر دیگر داده می شود.
- انتشار عمودی
  - در واقع عمق مسیر گراف مجاز شماری کنترل می شود. به این ترتیب که اگر کاربر U1 دارای یک امتیاز باشد، با تعیین مقدار j>0 برای این کاربر به U1 اجازه اعطای امتیاز به U2 داده می شود. در این صورت U1 یک واحد از j کم می کند و در نتیجه U2 فقط به j-1 کاربر دیگر می تواند آن امتیاز را بطور عمودی اعطا کند. همینطور این روال تکرار می شود تا زمانیکه مقدار j صفر شود.

MAC روش اجباری

- این روش "یا همه یا هیچ" است.
- یک کاربر یا امتیاز انجام یک عمل را دارد یا ندارد.
- این روش در محیط های بسیار نظم مند مثل محیط نظامی ایجاد شده است.

سطح محرمانگی داده ها و کاربران

- به هر شیئ داده ای یک عدد که نشان دهنده سطح محرمانگی آن است منتسب می شود.
- بعلاوه هر کاربر نیز یک مجوز برای دستیابی به سطح مشخصی از شیئ داده ای دارد. بنابراین تنها کاربر دارای مجوز دستیابی به یک شیئ داده ای می تواند به آن دستیابی داشته باشد.

سطح محرمانگی داده ها و کاربران (ادامه)

- داده ها به چهار رده زیر تقسیم می شوند:
  - خیلی سری TS (Top Secret)
  - سری S (Secret)
  - محرمانه C (Confidential)
  - رده بندی نشده U (Unclassified)

رابطه بین آنها به این شکل است:

TS>S>C>U

سطح محرمانگی داده ها و کاربران (ادامه)

- کاربران نیز به چهار رده تقسیم می شوند.
- رده نشان دهنده سطح محرمانگی داده را با $cl(D)$ و رده مجوز کاربر را با $cl(U)$ نمایش می دهیم.
- **خصوصیت ایمنی ساده:**

کاربر U نمی تواند داده D را بخواند مگر اینکه: $cl(U) >= cl(D)$

- **خصوصیت ستاره دار:**

کاربر U نمی تواند داده D را بنویسد مگر اینکه: $cl(U) <= cl(D)$

یک مثال

- رابطه های STT و STCOT را در نظر می گیریم.
- Cl(STT)=C & cl(STCOT)=TS
- دانشجو:C کارمند آموزش:S استاد:TS

به این ترتیب دستیابی کاربران کنترل می شود.

روش مبتنی بر نقش

- در این روش اجازه دستیابی کاربر به داده ها، وابسته به نقش کاربر در سازمان است.
- کاربران به عنوان اعضا نقشها تعریف می شوند و هر کاربر می تواند مجوز مربوط به نقش خود را برای دستیابی به داده ها دریافت کند.
- برای وظایف کاری هر فرد یا گروه دارای وظایف مشابه در سازمان، نقش تعریف می شود.

کنترل ایمنی چند سطحی در پایگاه داده رابطه ای

می توان علاوه بر اعمال محدودیت ایمنی روی رابطه، محدودیت را در سطح تاپل و حتی صفت هم اعمال کرد.

برای اعمال ضابطه ایمنی در سطح صفت به هر صفت A_i یک صفت رده بندی C منضم می شود.

برای اعمال ضابطه ایمنی در سطح تاپل، صفت رده بندی تاپل TC به صفات رابطه اضافه می شود.

$R(A_1,C_1,A_2,C_2,\ldots,A_n,C_n,TC)$

یک مثال

EMPL(EMP#,	ENAME,	ESALARY,	EJOBPER,	TC)
E101,U	EN1,U	SAL1,C	FAIR,S	S
E102,C	EN2,U	SAL2,S	GOOD,C	S

اگر این رابطه را برای کاربران با مجوز رده C فیلتر کنیم:

EMPL(EMP#,	ENAME,	ESALARY,	EJOBPER,	TC)
E101,U	EN1,U	SAL1,C	null,C	C
E102,C	EN2,U	null,C	GOOD,C	C

و اگر برای کاربر با مجوز U فیلتر کنیم:

EMPL(EMP#,	ENAME,	ESALARY,	EJOBPER,	TC)
E101,U	EN1,U	null,U	null,U	U

کنترل دستیابی از طریق قفل گذاری

می توان با قفل گذاری روی واحدهای داده ای در چندین سطح، دستیابی به آنها توسط کاربران را کنترل کرد

Encryption رمز نگاری

- عبارتست از کدگذاری داده ها بوسیله یک الگوریتم خاص به نحوی که کاربر نتواند بدون داشتن کلید رمز گشایی داده ها را بخواند.

اجزای سیستم رمز نگاری

- کلید رمز نگاری
- الگوریتم رمز نگاری
- کلید رمز گشایی
- الگوریتم رمز گشایی

اگر از یک کلید برای رمزنگاری و رمز گشایی استفاده شود، سیستم رمز نگاری متقارن است و در غیر اینصورت نامتقارن خواهد بود.

الگوریتم RSA نمونه رمزنگاری نامتقارن است.

Audit Process فرایند ردگیری

- عبارتست از جمع آوری داده هایی در مورد فعالیتها در سیستم و تحلیل آنها به منظور یافتن موارد عدم رعایت ضوابط ایمنی و یا تشخیص علت بروز این موارد.
- این داده ها در فایلی به نام فایل ردگیری ذخیره می شوند.
- تحلیل داده ها ممکن است بصورت برون خط و با تاخیر یا برخط و بیدرنگ باشد.
- در حالت بیدرنگ فرایند ردگیری را کشف مزاحمت(Intrusion detection) می گوییم.

کنترل گردش اطلاعات

با کنترل گردش اطلاعات از گردش غیر مجاز اطلاعات بطور صریح (مثل نسخه ای از اطلاعات) و یا ضمنی بین سطوح مختلف هرم مدیریتی- عملیاتی سازمان جلوگیری می شود.

کنترلهای امنیتی از طریق اقداماتی برای:

۱- کنترل جریان: در این روش، جریان اطلاعات مابین کاربران سیستم کنترل می‌شود. مثلا، خواندن از X و نوشتن روی Y .

اهمیت: عدم جریان صریح یا ضمنی اطلاعات به سطوح و اشیاء کمتر حفاظت شده.

- در مواقعی عین اطلاعات منتقل نمی شود بلکه جزئی از اطلاعات و یا برگرفته از اطلاعات: جریان اطلاعاتی جزئی (Partial Flow Control)

- جریانات مجاز باید مشخص و قاعده مند شوند. یعنی درجه حساسیت اشیاء مشخص شود و اینکه تمایز اشیاء چیست.

کنترلهای امنیتی از طریق اقداماتی برای:

۲- کنترل استنتاج: حفاظت از داده ها از تشخیص غیر مستقیم.

$Y = f(X)$، یعنی بدست آوردن Y از طریق X.

کانال استنتاجی :

۲-۱ دسترسی غیرمستقیم: کاربر تنها به X حق دسترسی دارد ولی مقدار Y را هم می فهمد.

- SELECT X FROM r WHERE Y = value.

یا درج رکوردی با کلیدی مشابه آنچه قبلا وجود دارد ولی کاربر حق دانستن آنرا ندارد!

کنترلهای امنیتی از طریق اقداماتی برای:

۲-۲ داده های مرتبط با هم: $Z = T * K$

که کاربر تنها حق دسترسی به T و K را دارد.

۲-۳ داده های ارائه نشده در پاسخ یک پرس و جو (Missing)
که مهاجم می فهمد داده های حساس چیستند!

۲-۴ استنتاج آماری: از طریق توابع آماری SQL

مقابله: اختلال در داده ها (Perturbation)

کنترل پرس و جو (مثلا کران بالا و پایین اندازه)

کنترل استنتاج Inference Control

- در این کنترل از کسب اطلاعات از طریق استنتاج جلوگیری می شود.
- با استفاده از برخی پرسشهای خاص و جهت یافته می توان اطلاعات مورد نظر را استنتاج کرد. در بعضی از پایگاه داده ها کاربران فقط اجازه بازیابی داده های آماری (مثل میانگین، حاصلجمع، تعداد، ماکزیمم و ...) را دارند و حق دسترسی مستقیم به داده های منفرد پایگاه داده ها را ندارند. در چنین پایگاهی ممکن است مشکلاتی بوجود بیاید.

یک مثال

- رابطه PERSON را در نظر بگیرید:

PERSON(NAME,SSN,INCOME,ADDRESS,
CITY,STATE,ZIP,SEX,LAST_DEGREE)

پرسشهای زیر را نیز در نظر می گیریم:

Q1:SELECT COUNT(*) FROM PERSON
WHERE condition;

Q2:SELECT AVG(INCOME) FROM
PERSON WHERE condition;

یک مثال (ادامه)

حال اگر بخواهیم دستمزد کارمند e را پیدا کنیم و بدانیم او زنی ا ست با مدرک دکترا و در شهر a در ایالت s1 زندگی می کند، در Q1 بجای condition شرایط زیر را قرار می دهیم:

LAST_DEGREE=phd AND SEX=f AND CITY=a
AND STATE= s1

اگر نتیجه این پرس و جو ۱ باشد و همین شرایط را در Q2 استفاده کنیم، دستمزد این کارمند بدست می آید.

حتی اگر نتیجه پرس و جو ۱ نباشد و عدد کوچکی مثل ۲ یا ۳ باشد، با استفاده از min یا max می توان محدوده دستمزد وی را بدست آورد

راه حل

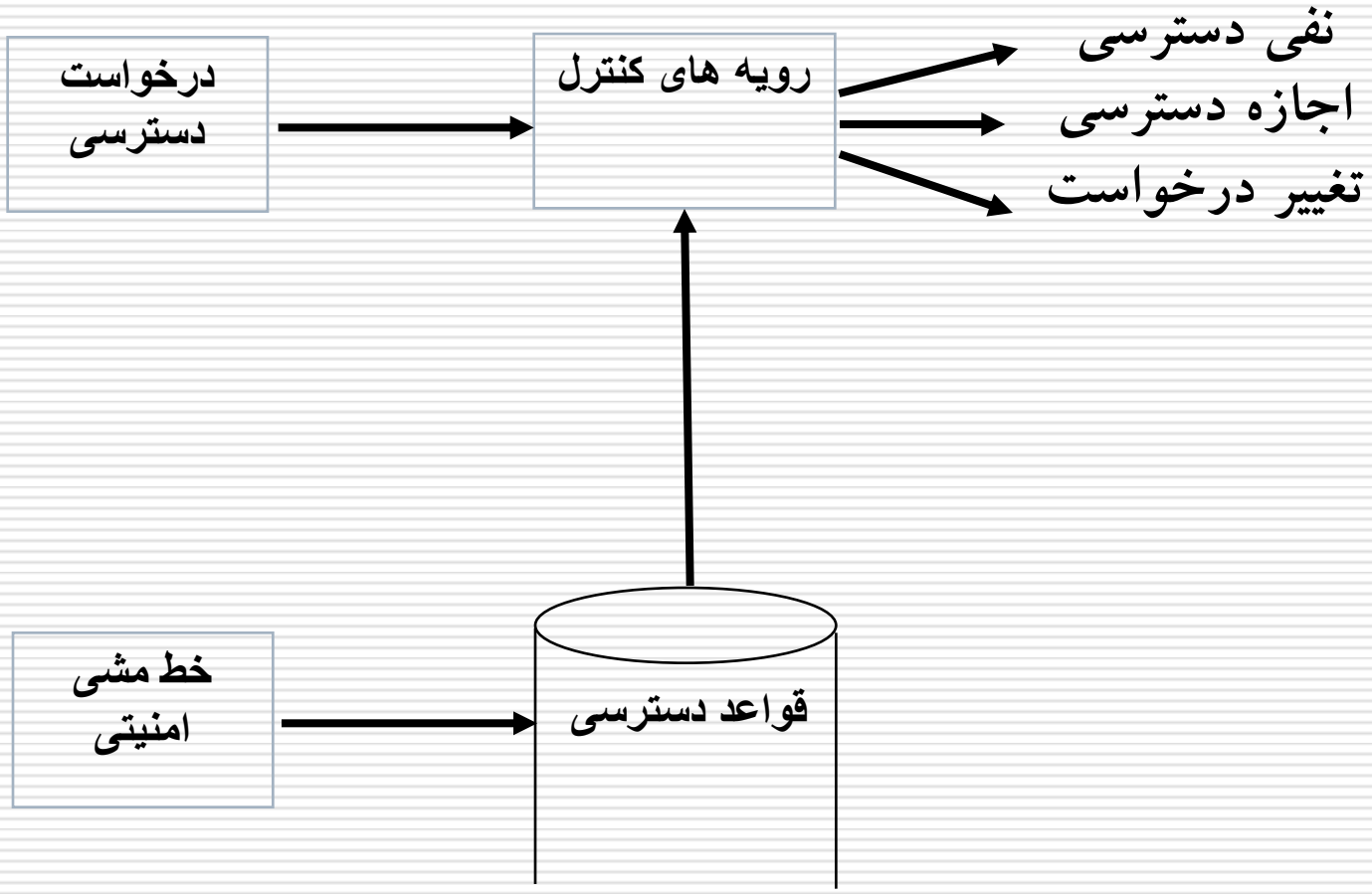
- یک راه برای رفع این مشکل آن است که یک حد آستانه برای تاپلها در نظر بگیریم و اگر نتیجه از این حد کمتر است جلوی انجام پرسش را بگیریم.
- راه دیگر ممانعت از اجرای دنباله ای از پرسشها است که مکررا به جمعیت ثابتی از یک رابطه دستیابی پیدا می کند.

کنترلهای امنیتی از طریق اقداماتی برای:

۳- کنترل دسترسی: اطمینان از اینکه همه دسترسی های مستقیم به داده ها دقیقاً متناظر با خط مشی امنیتی است.

- سیستم کنترل دسترسی شامل
  - مجموعه ای از قواعد و خط مشی های دسترسی
  - مجموعه ای از رویه های کنترلی

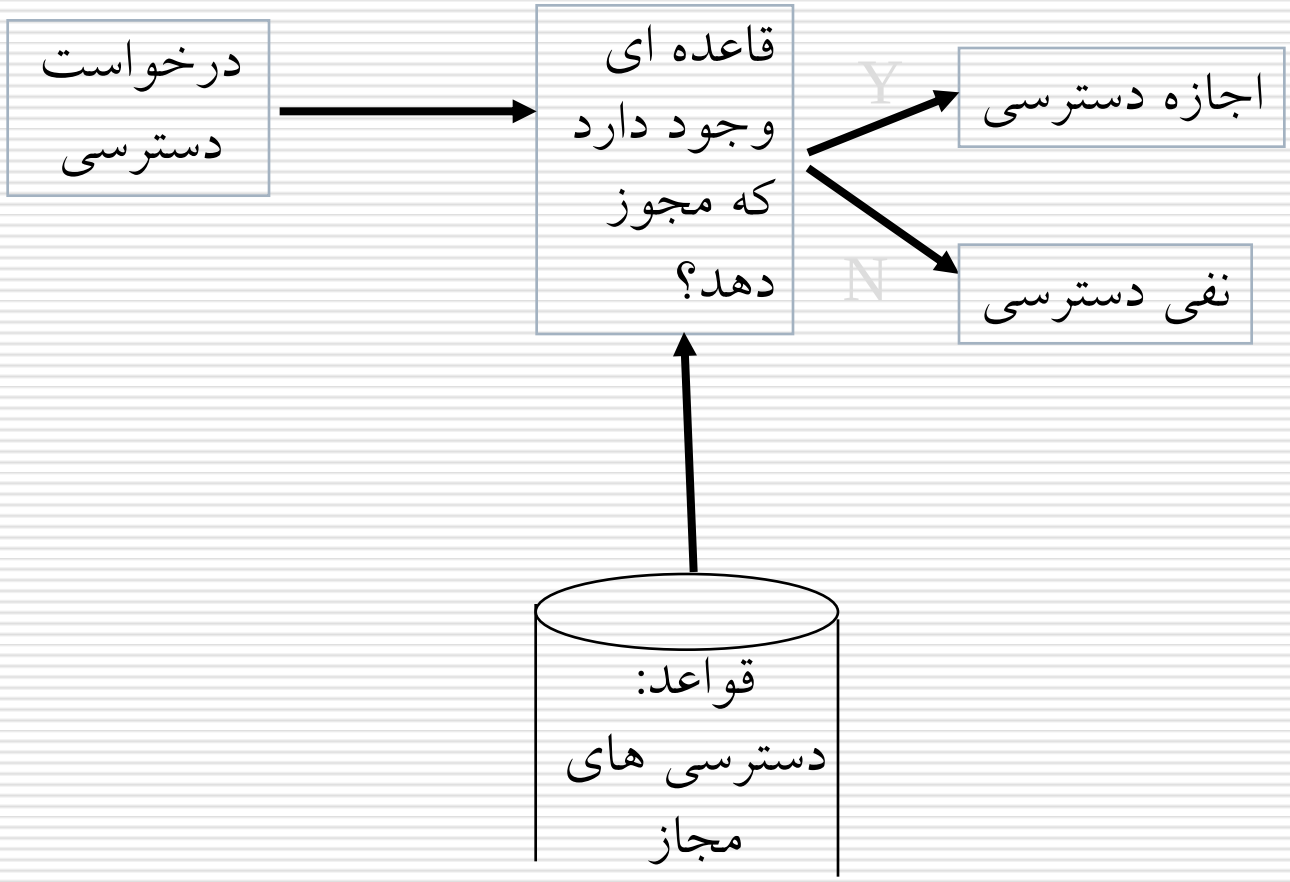
کنترل دسترسی



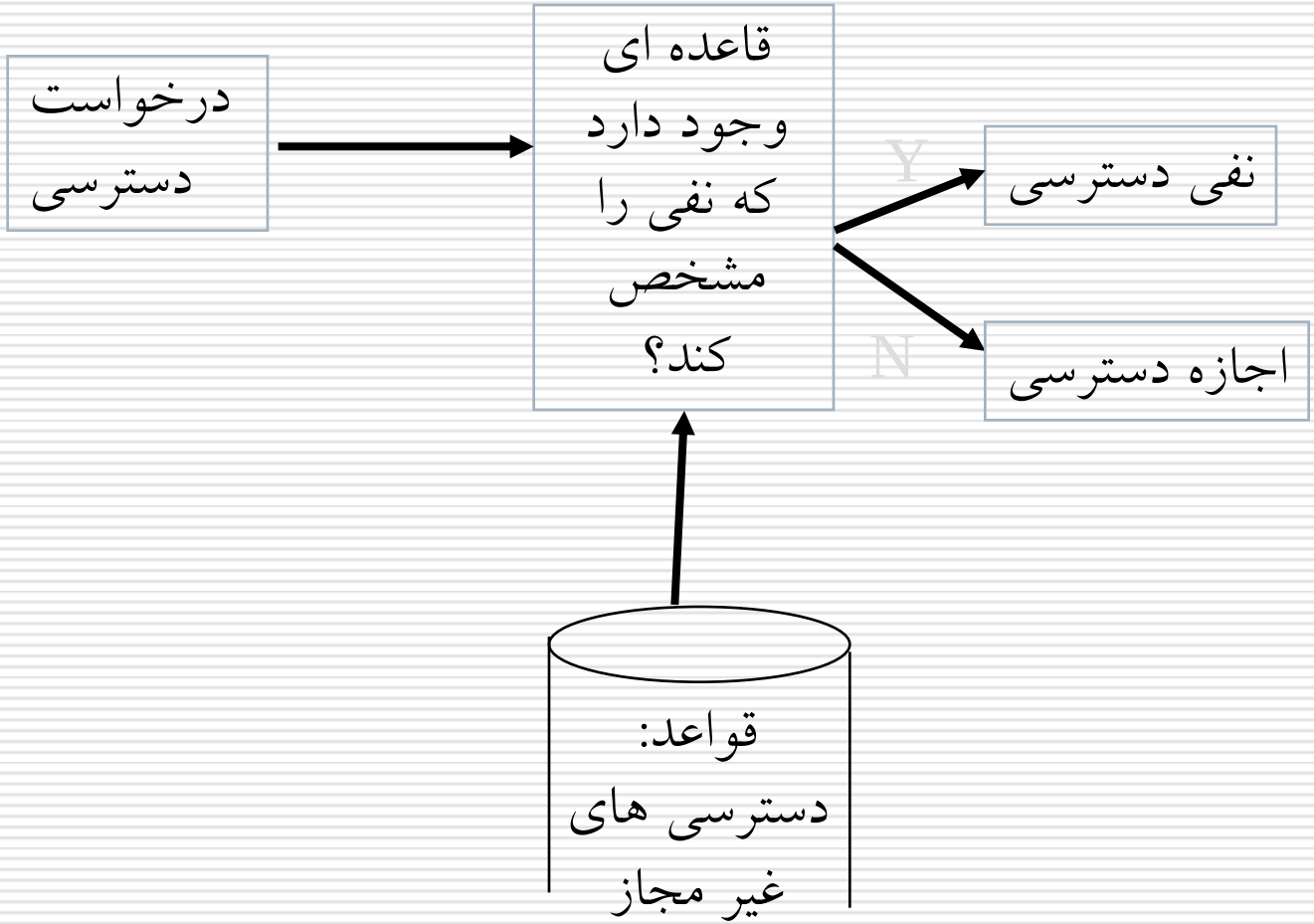
خط مشی های دسترسی

- ضرورت تعریف مفاهیم و راهبردها
- خط مشی های اصلی در محدود سازی دسترسی:
  - حداقل مجوز
  - حداکثر مجوز
- سیستم های بسته (شکل ص بعد)
- سیستم های باز (شکل دو ص بعد)
- خط مشی های مدیریت مجوزدهی !! کی حقِ دادن و پس گرفتنِ حق دارد؟

کنترل دسترسی: سیستم بسته



کنترل دسترسی: سیستم باز



امکانات امنیتی که DBMS باید فراهم کند

- درجات مختلف دانه‌بندی دسترسی
- انواع مختلف کنترلهای دسترسی
- مجازشناسی (Authorization) پویا
- حفاظت چندسطحی
- نداشتن کانال مخفی (Covert Channel): روش ارتباط غیرمستقیم برای دسترسی غیرمجاز به اطلاعات.
- کنترل استنتاج (Inference)

امکانات امنیتی که DBMS باید فراهم کند (ادامه)

- چند نمونگی (polyinstantiation) برای جلوگیری از استنتاج: مشاهدهٔ متفاوت دادهٔ یکسان از نظر کاربران مختلف.
- یکپارچه بودن روشهای کنترل محرمانگی و کنترل جامعیت
- نظارت (auditing)
- کارآیی معقول در برابر سربار حاصل از هزینه‌های امنیتی
- کنترل جریان (flow) برای بررسی مقصد اطلاعات

امنیت پایگاه داده‌ها و DBA

مدیر پایگاه داده‌ها (DBA) باید مجوز دستوراتی را برای انجام وظایف زیر داشته باشد (برای تمامی مدلهای داده‌ای و انواع DBMSها):

- ایجاد کاربر: ایجاد کاربر و تعیین کلمهٔ عبور برای وی.
- اعطای مجوز: دادن مجوزهای لازم به یک کاربر.
- لغو مجوز: باطل کردن مجوزهای داده شده.
- تخصیص سطح امنیتی: اختصاص سطح امنیتی مناسب به کاربر.

معیارهای ارزیابی سیاستهای امنیتی در یک DBMS

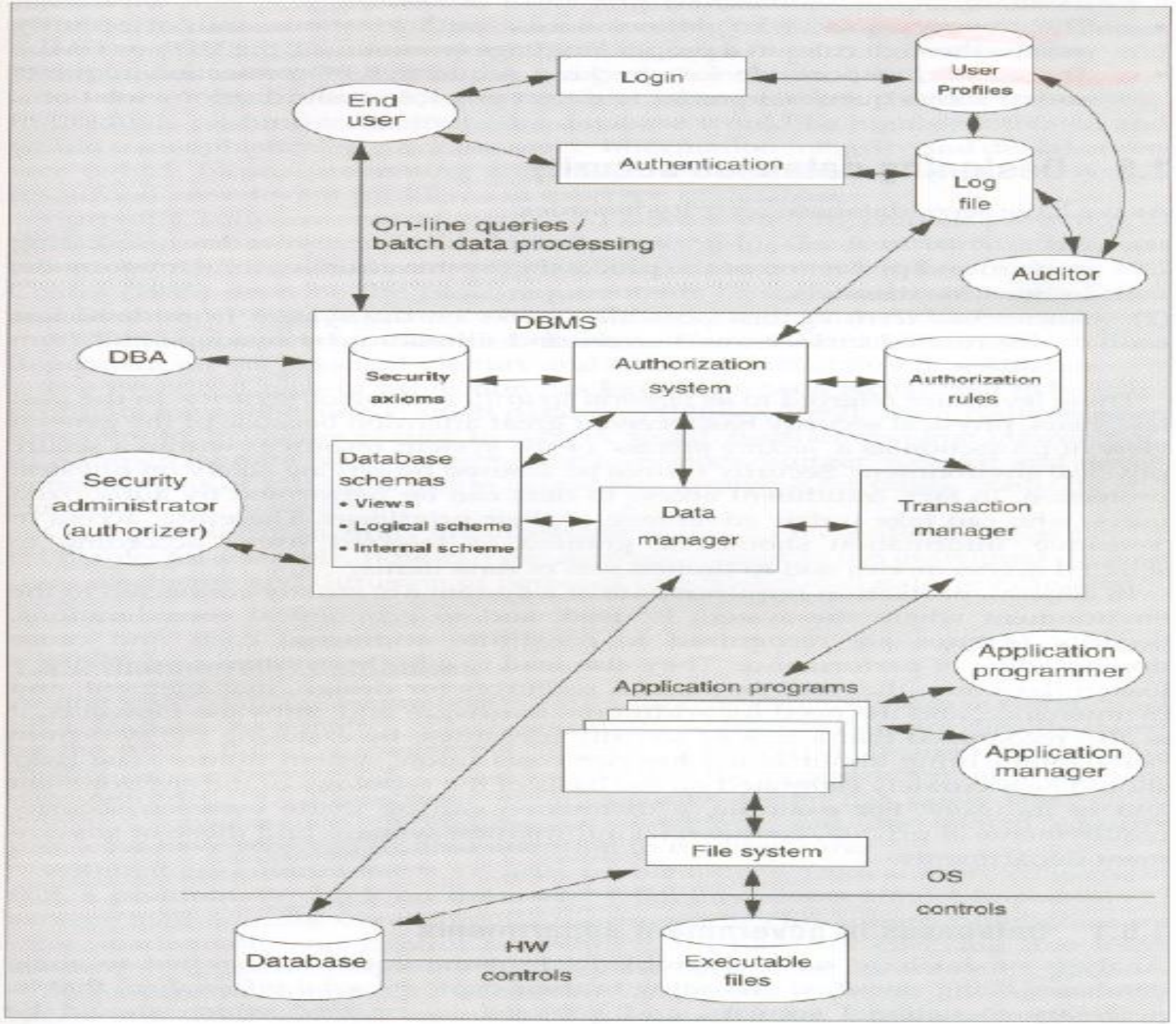
- تراکنشهای خوش - ساخت
- حداقل مجوز (Least Privilege): کاربران با حداقل مجوزهای لازم، به داده‌های مورد نظر دسترسی یابند.
- کاربران هویت‌شناسی شده
- تفکیک وظایف (Separation of Duties): هیچ کاربری نتواند از مجوزهای خود سوء استفاده کند (یا داده‌ها را تخریب کند).

Well-formed transaction

- The principle of well-formed transaction is defined as a transaction where the user is unable to manipulate data arbitrarily, but only in constrained (limitations or boundaries) ways that preserve or ensure the integrity of the data. A security system in which transactions are well-formed ensures that only legitimate actions can be executed. Ensures the internal data is accurate and consistent to what it represents in the real world

معیارهای ارزیابی سیاستهای امنیتی در یک DBMS (ادامه)

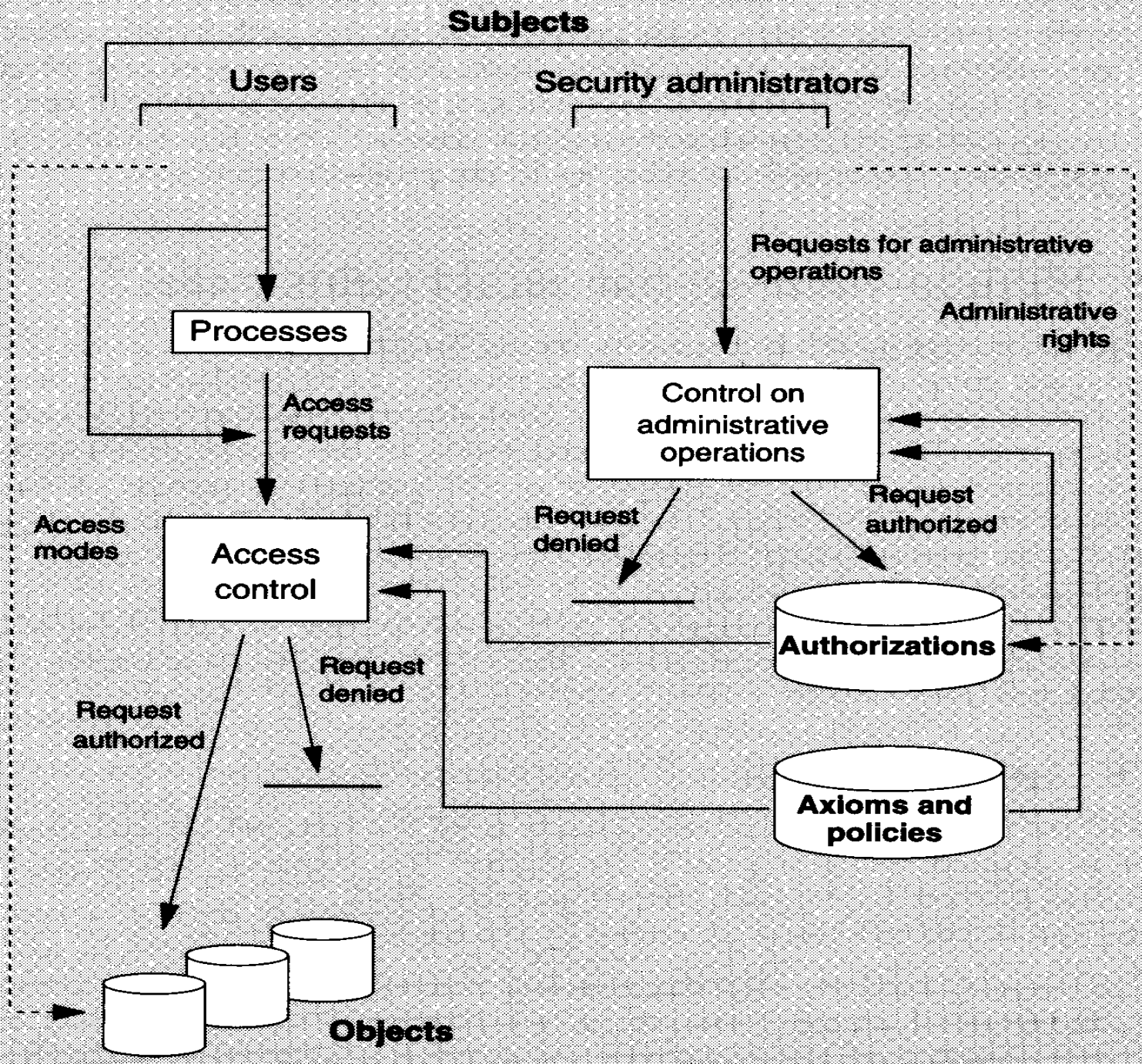
- تداوم عملیات DBMS به هنگام نقض امنیت.
- بررسی متناوب موجودیتهای دنیای واقعی.
- بازسازی وقایع برای بررسی سوء استفاده از مجوزها.
- کاربر پسندی و وجود روالهای امنیتی عاری ازخطا.
- واگذاری اجازه: اختصاص مجوزها بر اساس سیاستها.



معماری یک سمپاد شامل ویژگی های امنیتی

اجزای یک مدل امنیتی

- عاملها (subjects)
- اشیاء (objects)
- حالتهای دسترسی (access modes)
- سیاست ها (policies)
- مجازشناسی‌ها (authorizations)
- مجوزهای مدیریتی (administrative rights)
- اصول (axioms)



اجزاي يك مدل امنيتي (ادامه)

تعاریف پایه

- خط‌مشی امنیتی
  - بیانگر نیازمندی‌های امنیتی یک سازمان
  - تفکیک حالات مجاز از حالات غیرمجاز در سیستم
- مدل امنیتی
  - یک انتزاع از خط‌مشی امنیتی
  - به اعتقاد برخی از محققین: بیان صوری خط‌مشی امنیتی
- کنترل دسترسی: مکانیزم امنیتی پایه

شناسایی و تصدیق اصالت (Identification & Authentication)

+

مکانیزم مجازشناسی (Authorization)