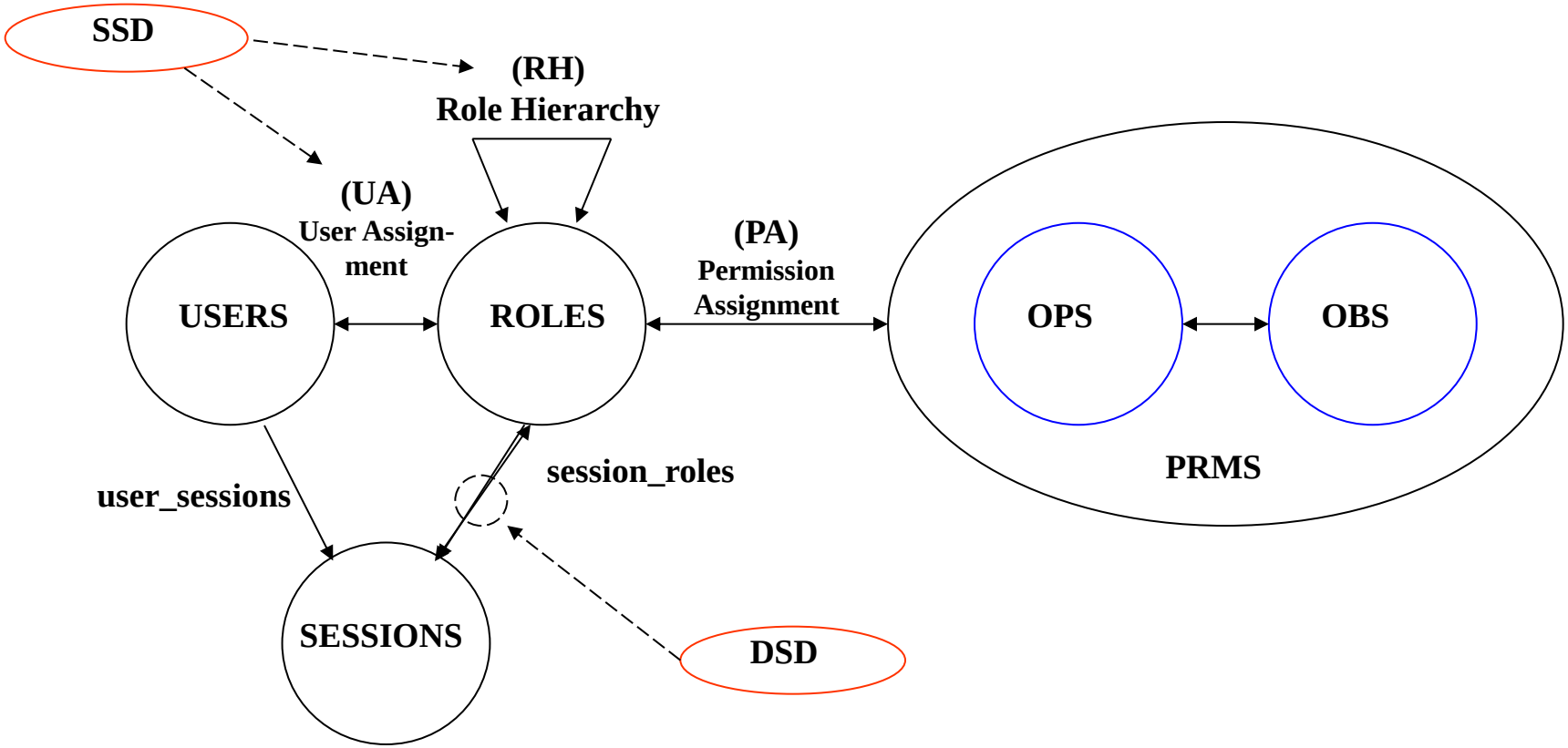
مدل کنترل دسترسی نقش-مبنا (RBAC)

Masood Niazi Torshiz
www.mniazi.ir

مدل RBAC

- نمای کلی مدل



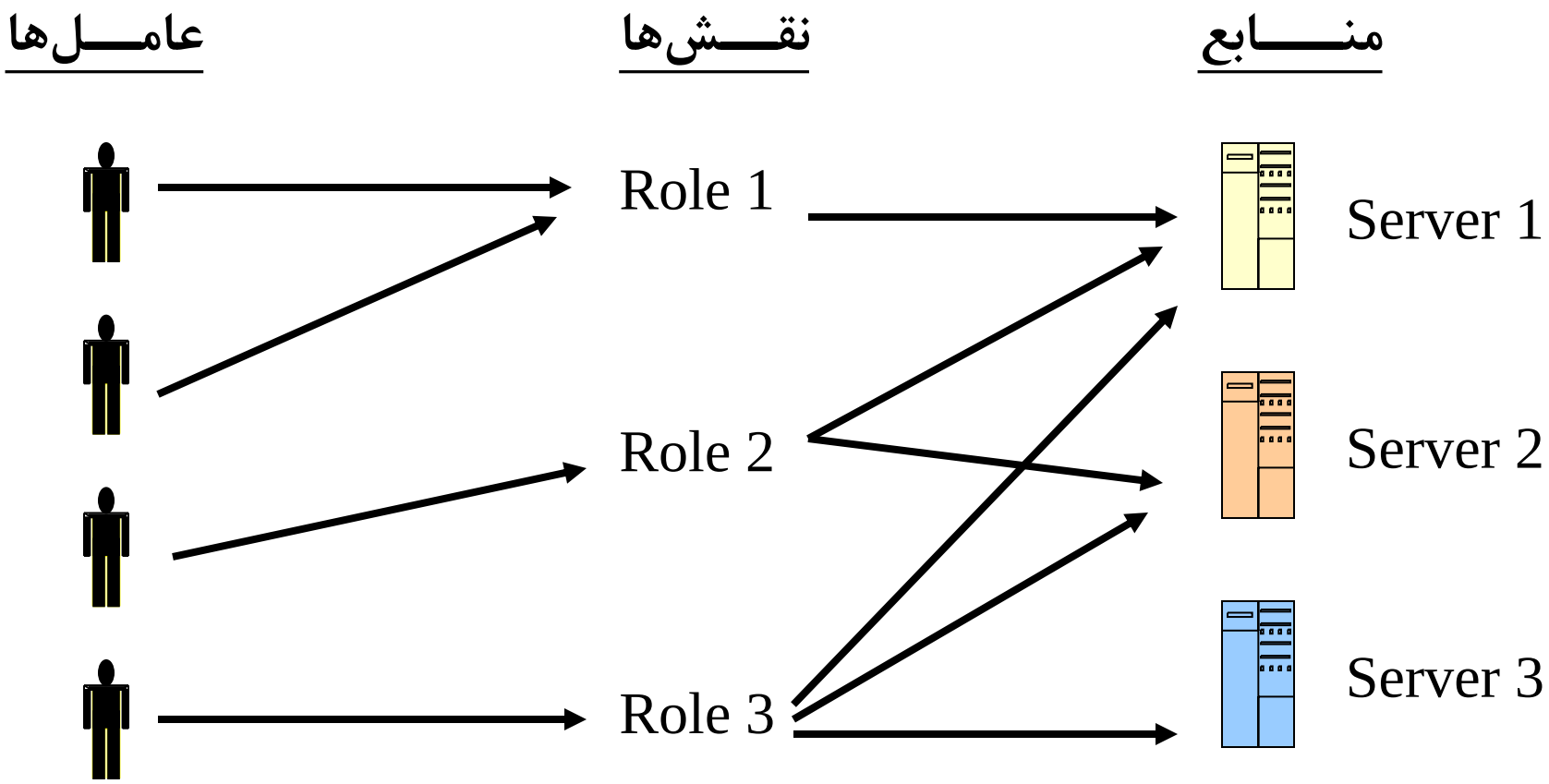
مدل RBAC – اهداف

- سازگاری با ساختار سازمانی
- سادگی مدیریت کنترل دسترسی
- قدرت بیان: امکان بیان خط‌مشی‌های اختیاری (DAC) و اجباری (MAC)
- اصل حداقل مجوزها (least privilege)
- تفکیک وظایف (SoD)

مدل RBAC - کنترل دسترسی

- اعطای مجوزها به نقش‌ها و نقش‌ها به کاربران (به جای اختصاص مستقیم مجوزها به کاربران)
- تعیین نقش‌ها بر اساس اصل حداقل مجوزها
- اعطای مجموعه مجوزهای موردنیاز برای اجرای وظایف مربوطه به هر نقش به آن
- امکان توصیف تفکیک وظایف (Separation of Duties)

مدل RBAC



کاربران دائماً تغییر می‌کنند اما نقش‌ها خیر

مدل RBAC - چارچوب مدل

- مدل نقش-مبناي پايه ($RBAC_0$)
  - مولفه‌هاي مدل پايه
- مدل نقش-مبناي سلسله مراتبي ($RBAC_1$)
  - سلسله مراتب عمومي
  - سلسله مراتب محدودشده
- مدل نقش-مبنا با محدوديت ($RBAC_2$)
  - تفكيك وظايف ايستا (SSoD)
  - تفكيك وظايف پويا (DSoD)

مدل RBAC – انواع

Models	Hierarchies	Constraints
$RBAC_0$	–	–
$RBAC_1$	✓	–
$RBAC_2$	–	✓
$RBAC_3$	✓	✓

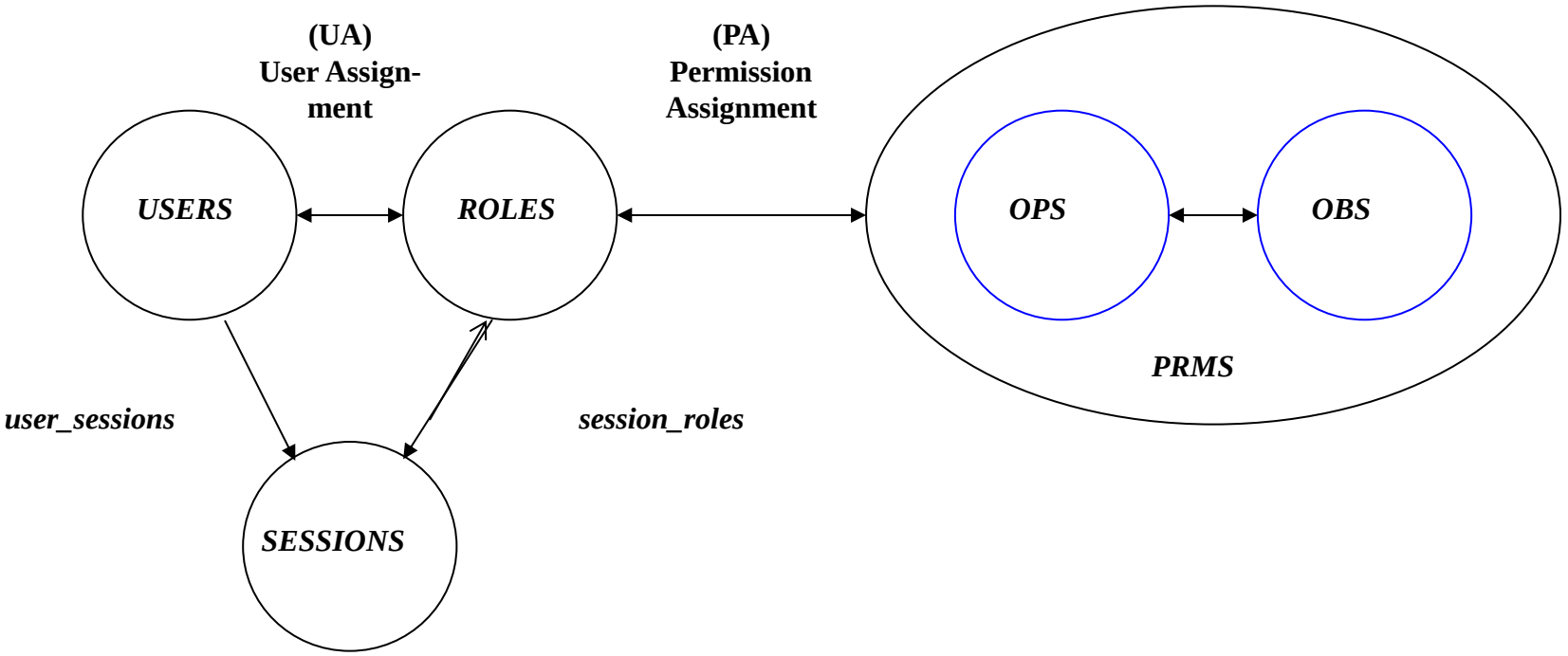
مدل نقش مبنای پایه $RBAC_0$

مدل نقش مبنای پایه $RBAC_0$

- مولفه‌های مدل پایه $RBAC_0$:
  - عامل‌ها یا کاربران(USERS)
  - نقش‌ها (ROLES)
  - مجوزها (PRMS)
    - اعمال (OPS)
    - اشیاء (OBS)
  - رابطه اختصاص نقش به کاربر (UA)
  - رابطه اختصاص مجوز به نقش (PA)
  - نشست‌ها (SESSIONS)

۲- مدل $RBAC_0$

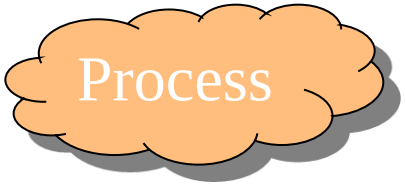
- نمای کلی مدل $RBAC_0$



۳- مدل $RBAC_0$

- کاربران (USERS)

Person



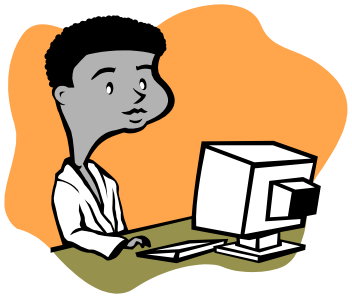
Intelligent Agent

۴- مدل $RBAC_0$

- نقش‌ها (ROLES): هر نقش شامل تعدادی وظیفه‌مندی

مدیر کل

مدیر مالی



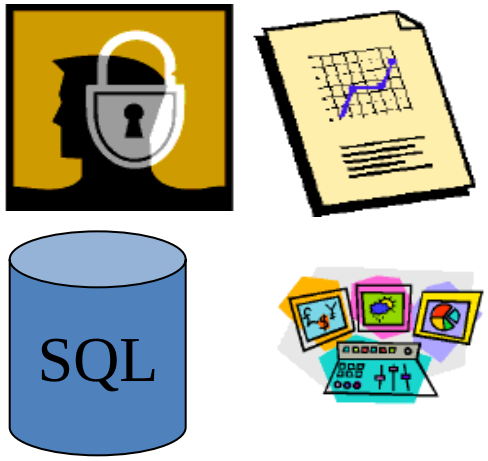
برنامه‌نویس

اپراتور راهنما

۵- مدل $RBAC_0$

- اعمال (OPS): اجرای عملی خاص (تابعی از یک برنامه) بر روی یک شیئ یا منبع

  - Database – Update Insert Append Delete
  - Locks – Open Close
  - Reports – Create View Print
  - Applications - Read Write Execute



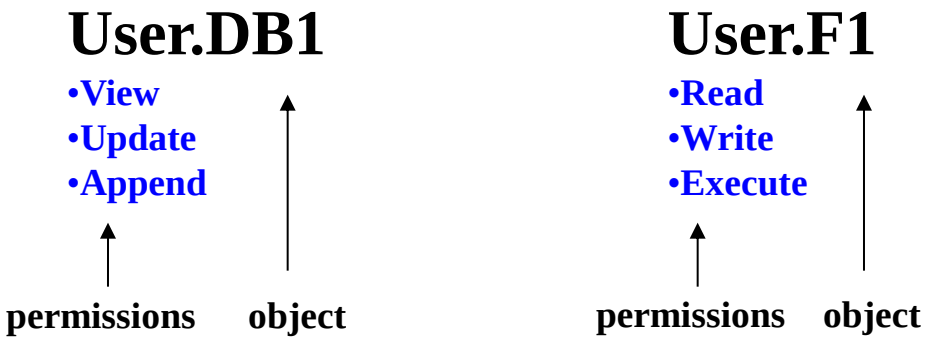
۶- مدل $RBAC_0$

- اشیاء یا منابع (OBS): حاوی داده‌ها

•OS Files or Directories
•DB Columns, Rows, Tables, or Views
•Printer
•Disk Space
•Lock Mechanisms

۷- مدل $RBAC_0$

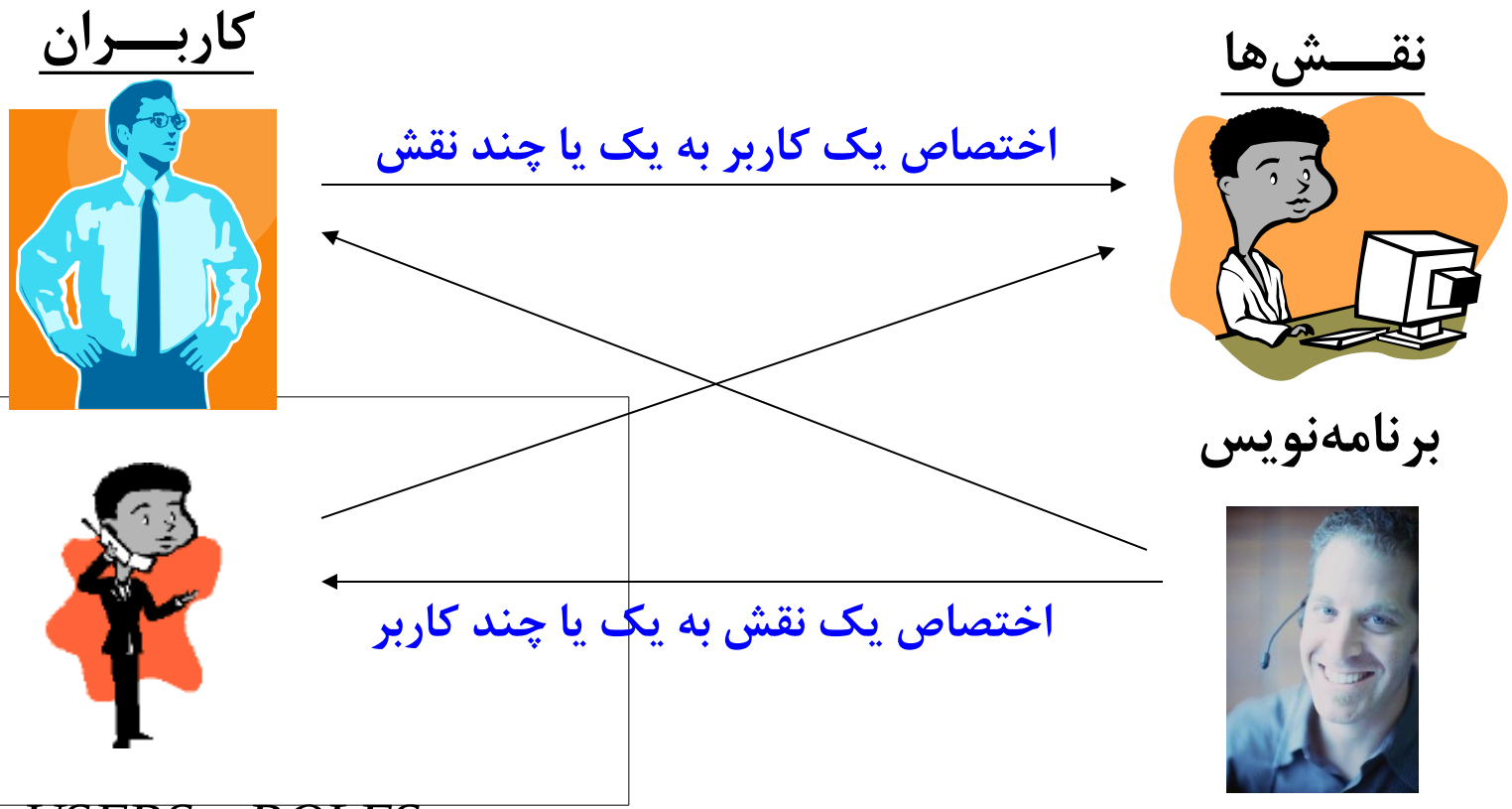
- مجوزها (PRMS): مجموعه‌ای از مجوزها که هریک اجرای یک عمل را بر روی یک شیئ یا منبع حفاظت شده ممکن می‌سازد.



$$PRMS = 2^{(OPS \times OBS)}$$

۸- مدل $RBAC_0$

- رابطه اختصاص نقش به کاربر (UA)



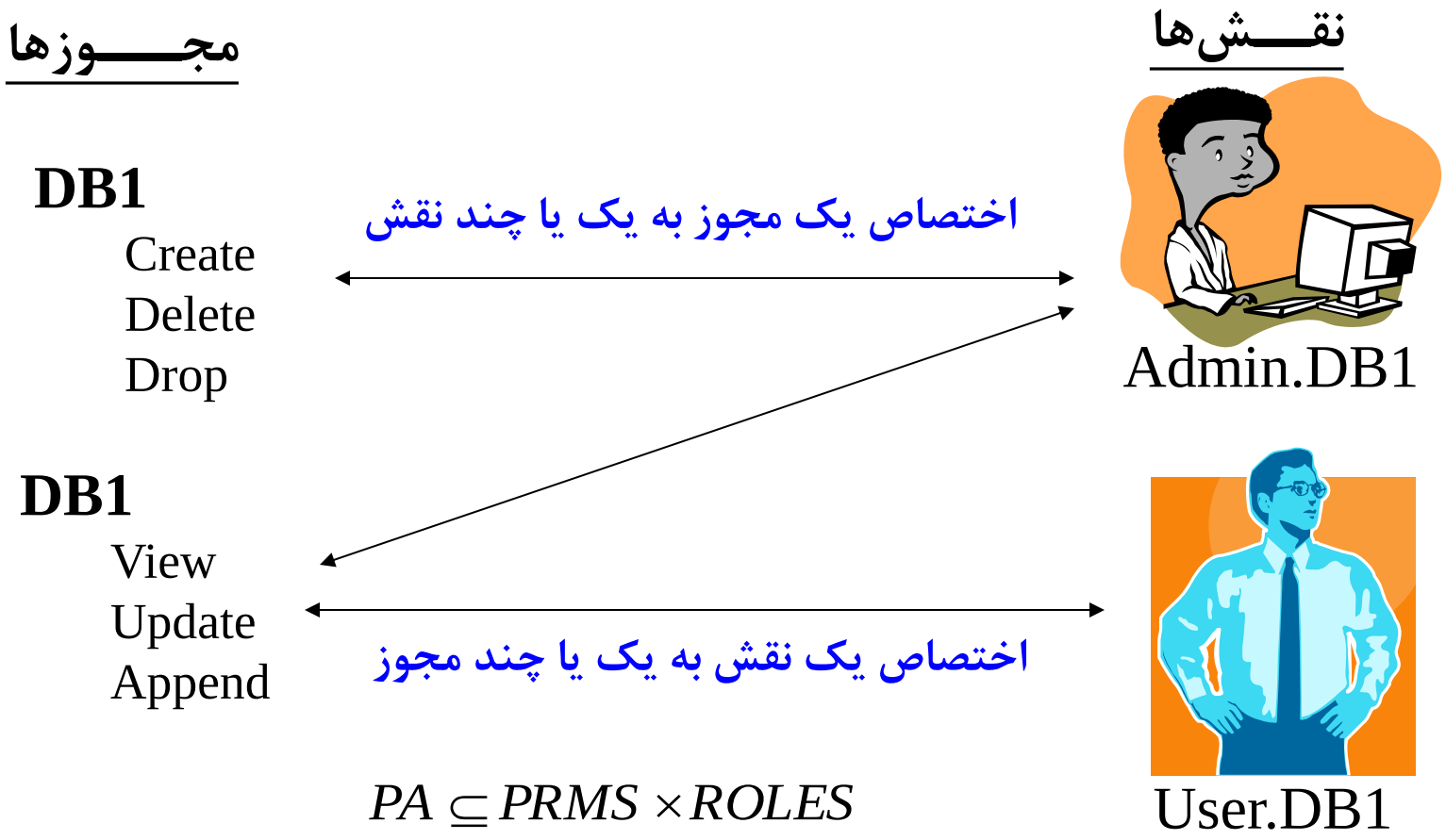
$$UA \subseteq USERS \times ROLES$$

$$assigned\_user : (r : ROLES) \rightarrow 2^{users}$$

$$assigned\_user(r) = \{u \in USERS \mid (u, r) \in UA\}$$

۹- مدل $RBAC_0$

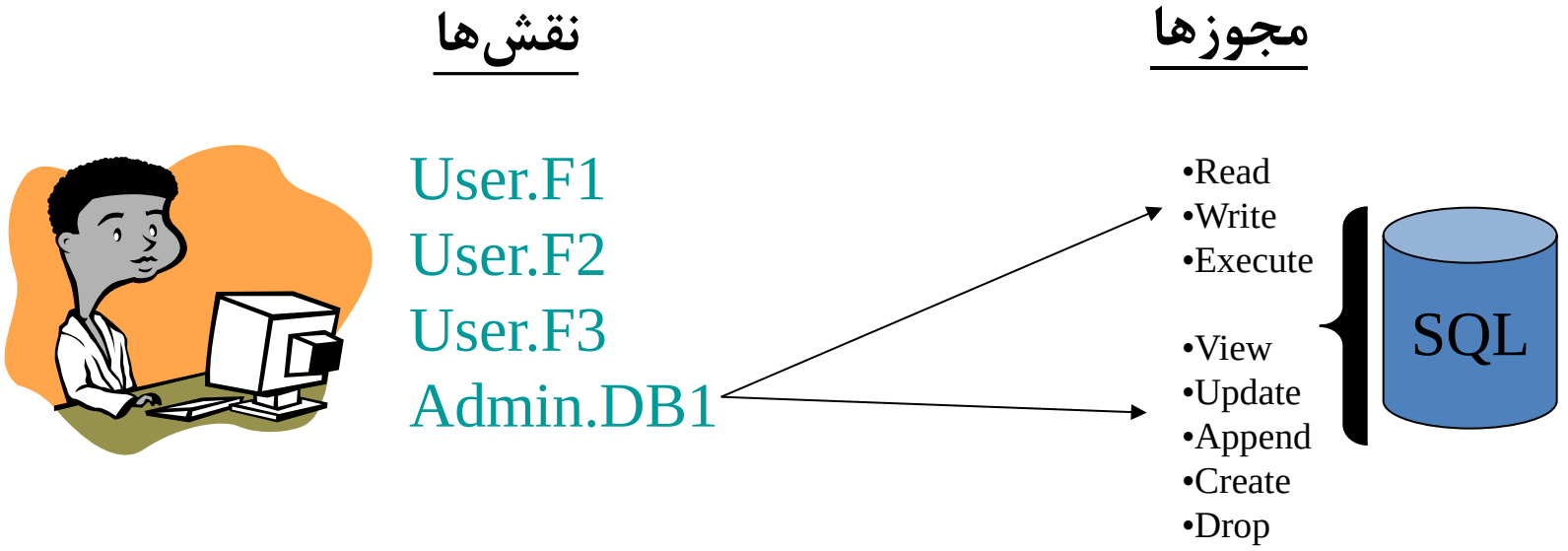
- رابطه اختصاص مجوز به نقش (PA)



$$PA \subseteq PRMS \times ROLES$$

۱۰- مدل $RBAC_0$

- رابطه اختصاص مجوز به نقش (PA)

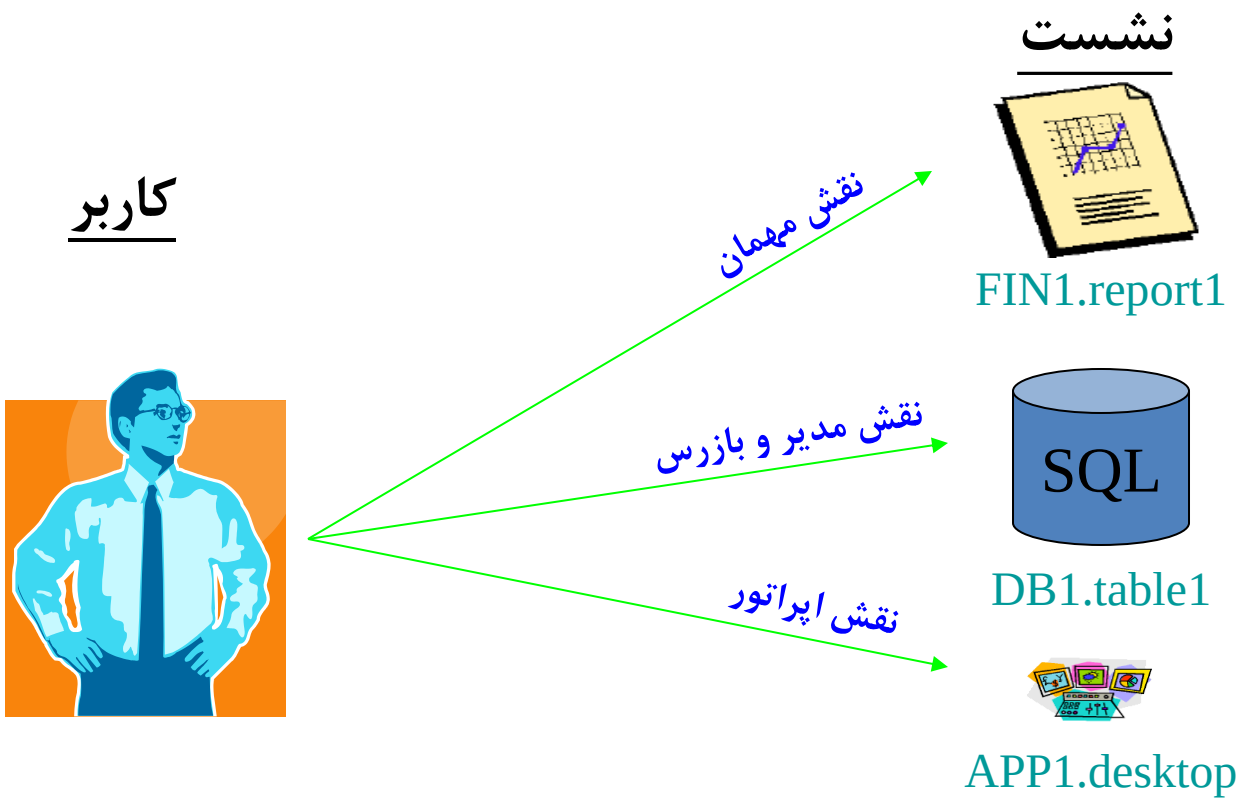


$$assigned\_permissions(r : ROLES) \rightarrow 2^{PRMS}$$

$$assigned\_permissions(r) = \{p \in PRMS \mid (p, r) \in PA\}$$

۱۱- مدل $RBAC_0$

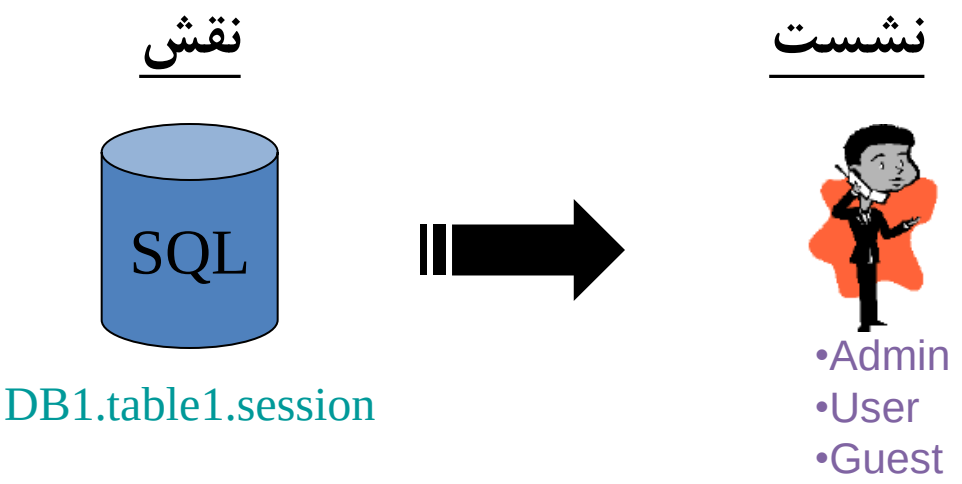
- نشست‌ها: هر کاربر می‌تواند چند نشست داشته باشد.



$$user\_sessions(u:USERS) \rightarrow 2^{SESSIONS}$$

۱۲- مدل $RBAC_0$

- نقش‌های فعال در یک نشست = مجموعه نقش‌های فعال شده توسط کاربر نشست (از مجموعه نقش‌های اختصاص یافته با UA).

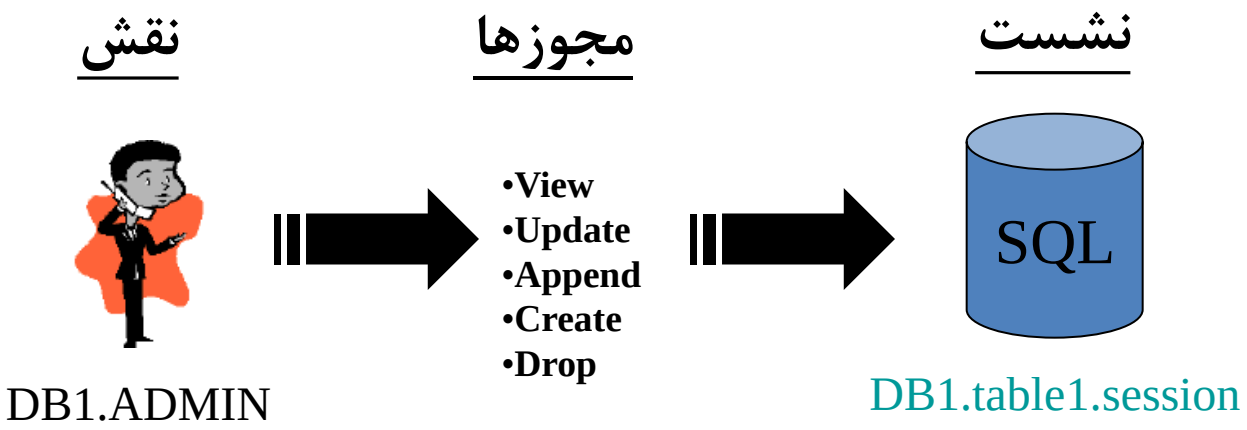


$$session\_roles(s:SESSIONS) \rightarrow 2^{ROLES}$$

$$session\_roles(s_i) \subseteq \{r \in ROLES \mid (session\_user(s_i), r) \in UA\}$$

۱۲- مدل $RBAC_0$

- مجوزهای یک نشست = مجموعه مجوزهای نقش‌های فعال شده در نشست

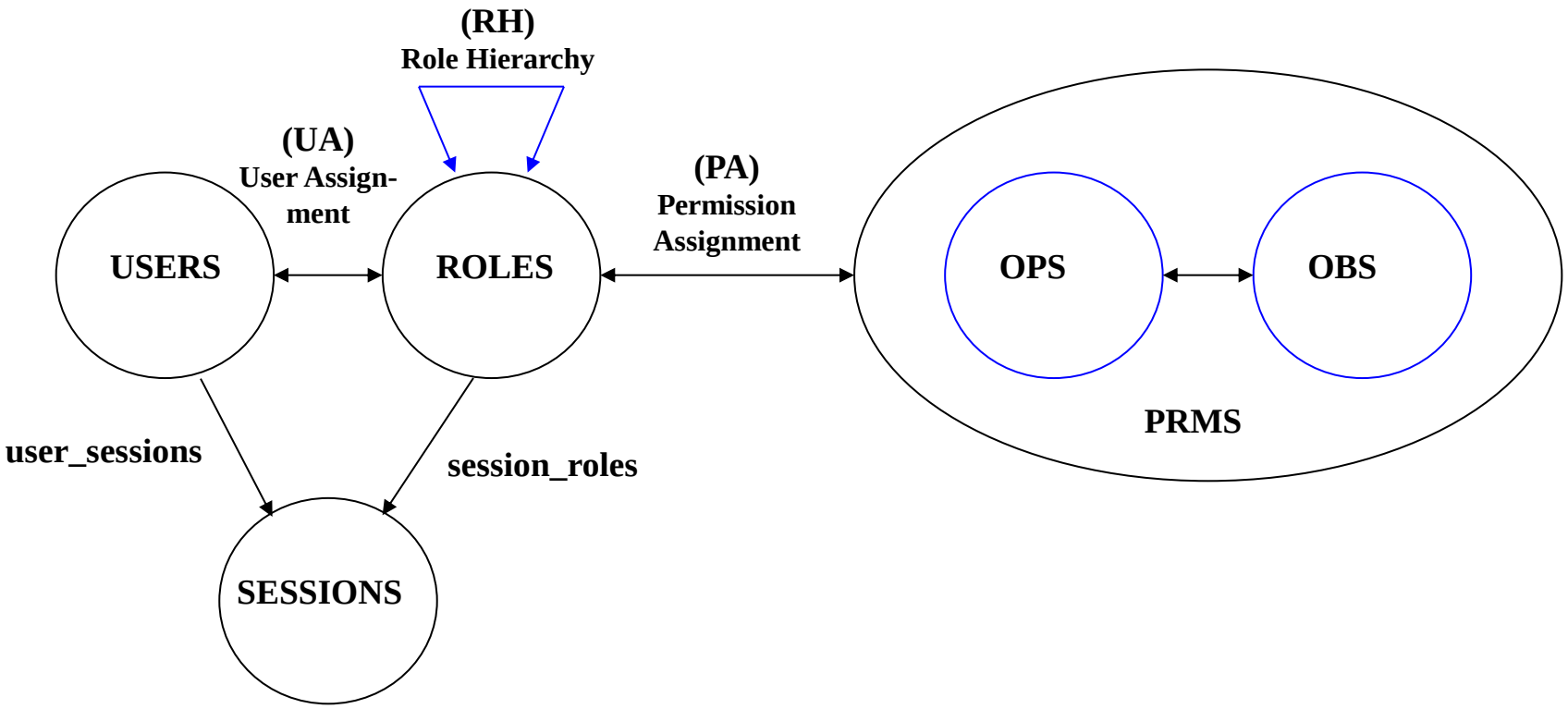


$$avail\_session\_perms(s:SESSIONS) \rightarrow 2^{PRMS} = \bigcup_{r \in session\_roles(s)} assigned\_permissions(r)$$

مدل نقش-مبنای سلسله‌مراتبی $RBAC_1$

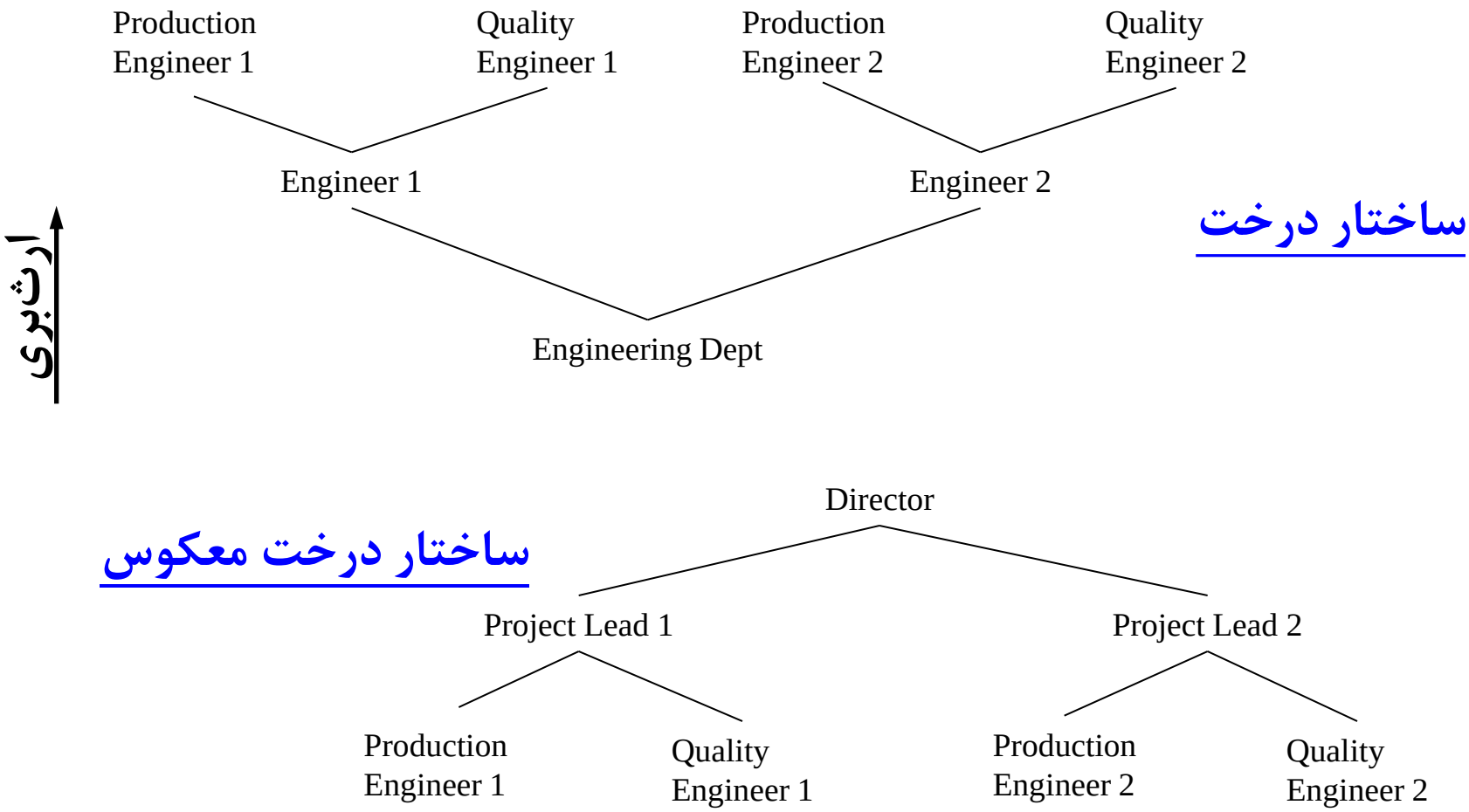
مدل نقش-مبنای سلسله‌مراتبی $RBAC_1$

- نمای کلی مدل $RBAC_1$



۲- $RBAC_1$ مدل

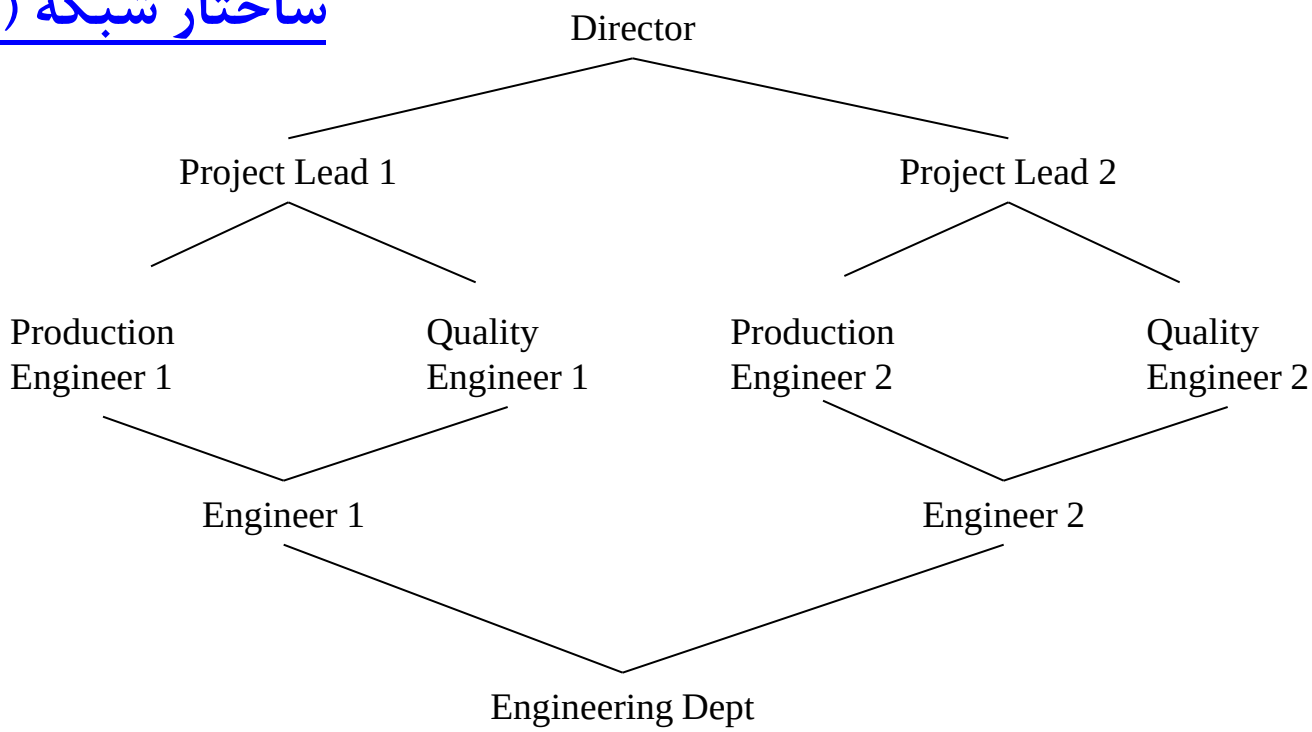
- انواع سلسله مراتب نقش‌ها



۳- $RBAC_1$ مدل

- انواع سلسله مراتب نقش‌ها

ساختار شبکه (Lattice)



۴- مدل $RBAC_1$

- رابطه نقش و زیرنقش (RH)
- ساختار سلسله مراتبی نقش‌ها می‌تواندبرگرفته از ساختار سازمانی باشد.
- دو نوع سلسله‌مراتب:
  - سلسله مراتب عمومی: پشتیبانی از ارث‌بری چندگانه
  - سلسله مراتب محدودشده: عدم ارث‌بری چندگانه

- در صورتیکه نقش r_1 فرزند نقش r_2 در سلسله مراتب باشد، همه مجوزهای آن را به ارث می‌برد.

r_1 *به ارث می‌برد از* r_2

$$RH \subseteq ROLES \times ROLES$$

۵- $RBAC_1$ مدل

- کاربران یک نقش در سلسله مراتب نقش ها

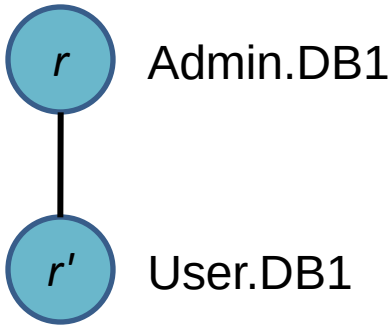
$$authorized\_users(r:ROLES) \rightarrow 2^{USERS}$$

$$authorized\_users(r) = \{u \in USERS \mid r' \succeq r \wedge (u, r') \in UA\}$$

- مجموعه مجوزهای یک نقش در سلسله مراتب نقش ها

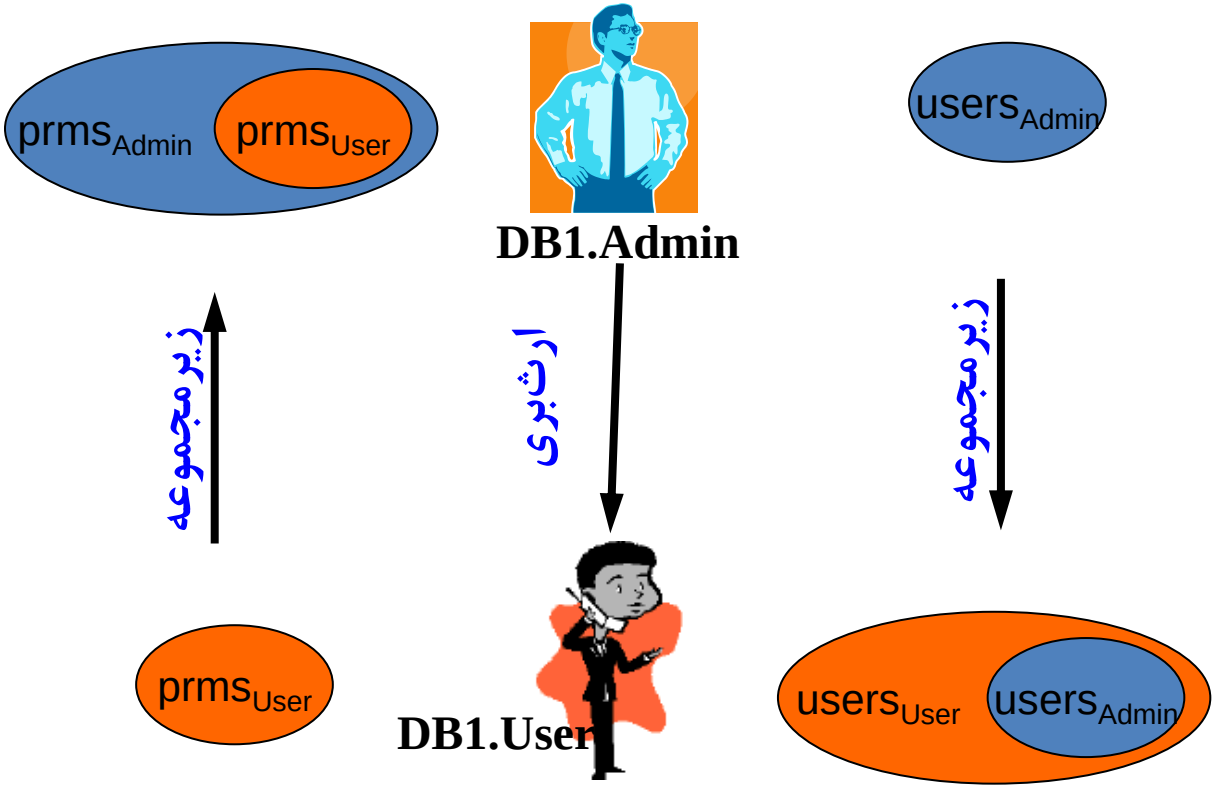
$$authorized\_permissions(r:ROLES) \rightarrow 2^{PRMS}$$

$$authorized\_permissions(r) = \{p \in PRMS \mid r \succeq r', (p, r') \in PA$$



۶- مدل $RBAC_1$

- رابطه کاربران و مجوزها در ارث‌بری نقش‌ها



$$r2 \succeq r1 \Rightarrow authorized\_permissions(r_2) \subseteq authorized\_permissions(r_1)$$
$$\wedge\, authorized\_users(r_1) \subseteq authorized\_users(r_2)$$

$r2 :: user,$

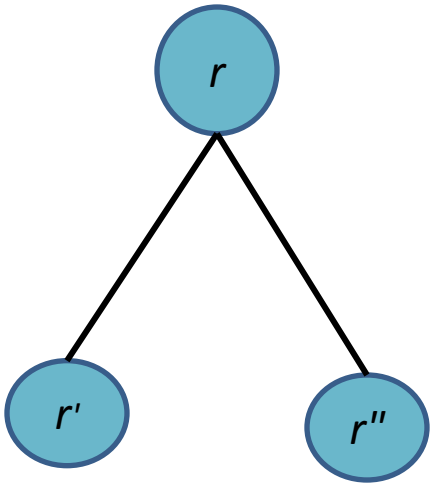
$r1 :: Admin$

7- مدل $RBAC_1$

سلسله مراتب عمومی: پشتیبانی از ارث بری چندگانه

$$r \succeq_i r'$$

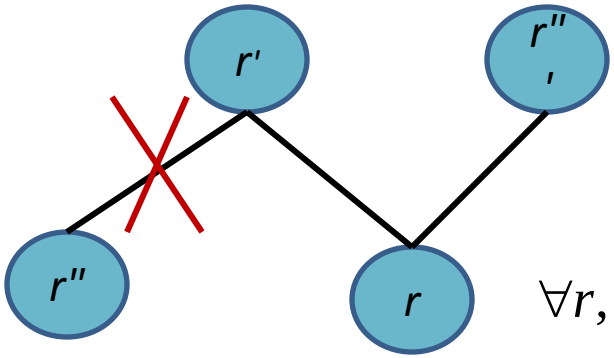
$$r \succeq_i r''$$



8- مدل $RBAC_1$

سلسله مراتب محدود: فقط ارث بری یگانه

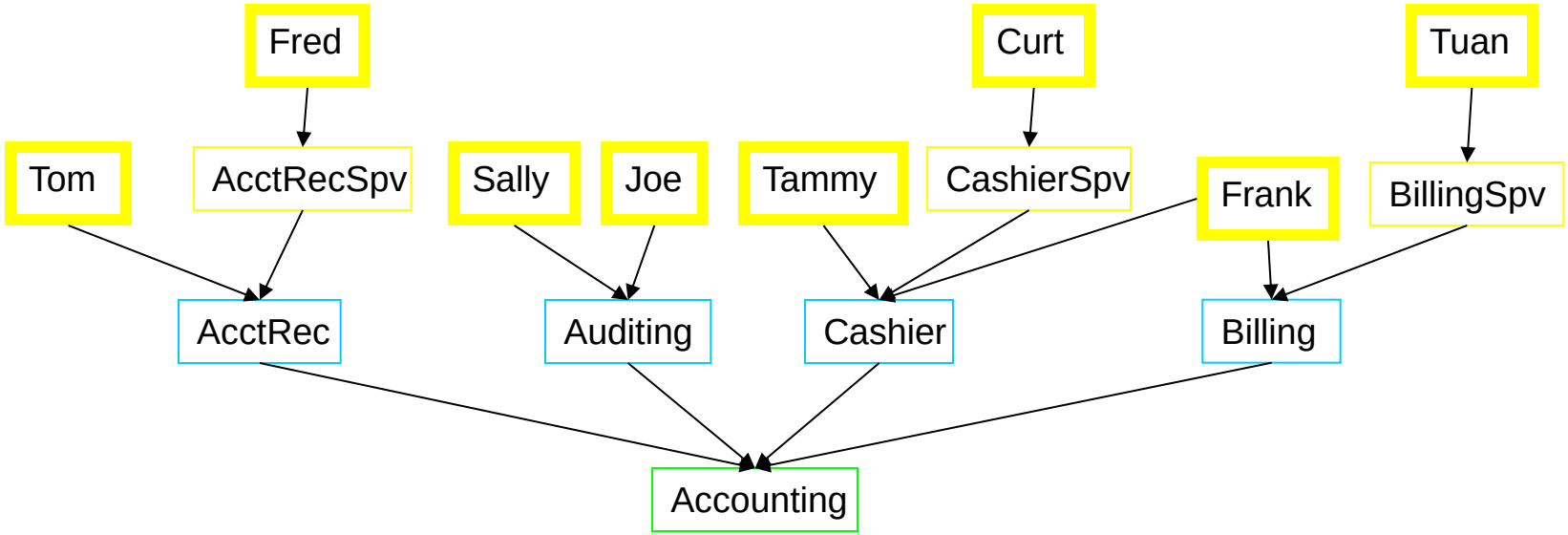
هر نقش تنها یک پدر بی واسطه در سلسله مراتب نقش ها دارد.



$$\forall r, r', r'' \in ROLES, \quad r \succeq_i r' \wedge r \succeq_i r'' \Rightarrow r' = r''$$

۹- مدل $RBAC_1$

مثالی از سلسله مراتب محدود نقش ها

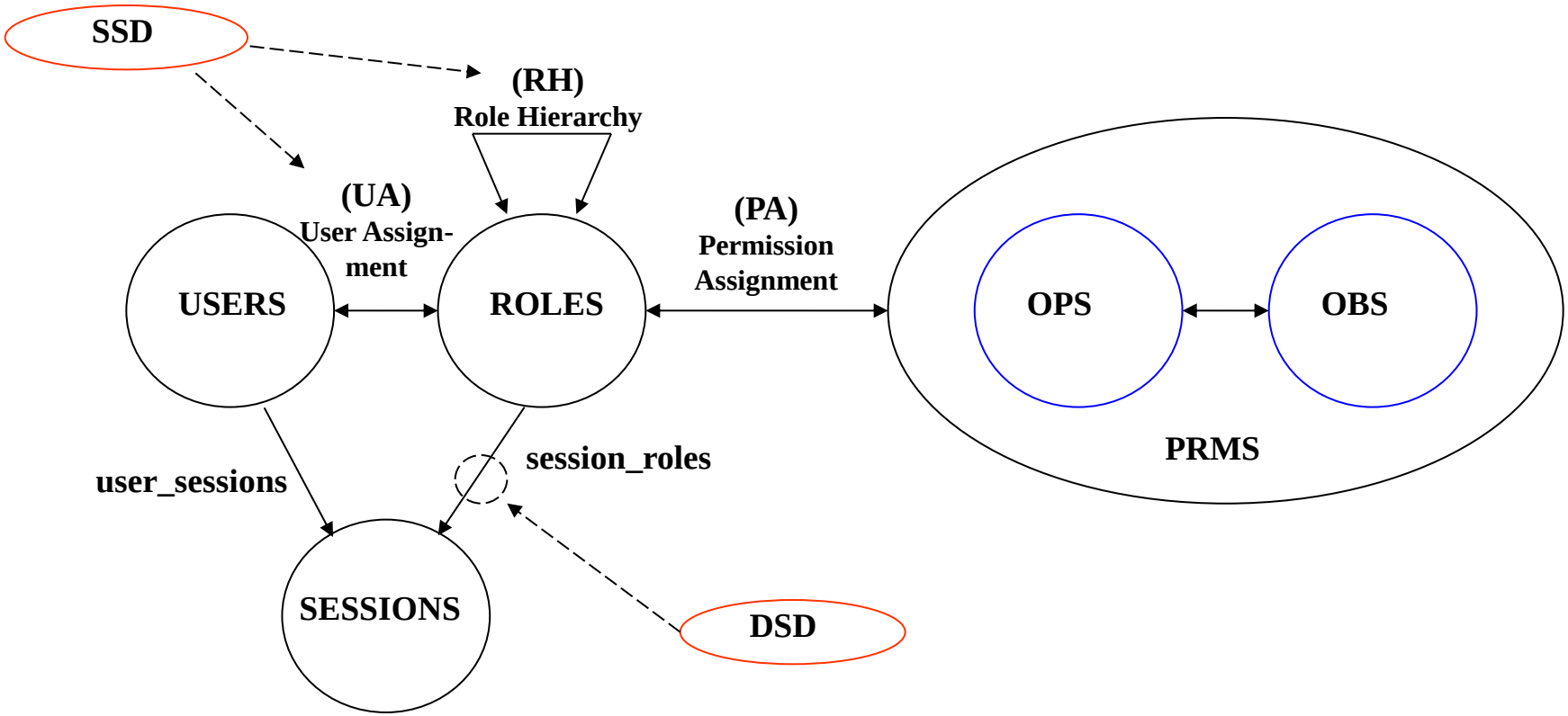


Accounting Role

مدل نقش-مبنا با محدویت $RBAC_2$

مدل نقش-مبنا با محدویت $RBAC_2$

- نمای کلی مدل $RBAC_2$



۳- مدل $RBAC_2$

SSoD: اِعمال محدودیت در اختصاص نقش به کاربر در رابطه UA

- از یک مجموعه از نقش‌های متداخل، نمی‌توان n نقش و یا بیشتر را به یک کاربر اِعطا کرد.
- ممکن است یک کاربر امکان داشتن دو نقش در یک زمان را نداشته باشد – دو نقش دو بدو ناسازگار

$SSoD = \{ssod_1, \ldots, ssod_n\}$

$ssod_i = (rs, n)$

rs = یک مجموعه نقش ناسازگار

$$SSoD \subseteq \left(2^{ROLES} \times N\right)$$
$$ssod_i = \left(\{r_1, r_2, \ldots, r_k\}, n\right)$$
$$\forall (rs, n) \in SSoD, \forall t \subseteq rs, |t| \geq n \Rightarrow \bigcap_{r \in t} assigned\_users(r) = \varnothing$$

۴- مدل $RBAC_2$

DSoD: اِعمال محدودیت در فعال‌سازی نقش توسط کاربر در یک نشست

- از یک مجموعه از نقش‌های متداخل، نمی‌توان n نقش و یا بیشتر را در طی یک نشست فعال کرد.
- اِعمال این محدودیت نیاز به نگهداری سابقه نقش‌های فعال شده در طی یک نشست دارد.

$DSoD = \{dsod_1, \ldots, dsod_n\}$

$dsod_i = (rs, n)$

rs = یک مجموعه نقش ناسازگار

$$DSoD \subseteq \left(2^{ROLES} \times N\right)$$

$$dsod_i = \left(\{r_1, r_2, \ldots, r_k\}, n\right), \quad k \geq 2$$

$$\forall (rs, n) \in DSoD, \forall s \subseteq SESSIONS, \ \forall t, t \subseteq rs, t \subseteq session\_roles(s) \Rightarrow |\, t \,| < n$$

۵- مدل $RBAC_2$

مثالی از تفکیک وظایف ایستا

- فرآیند خرید

1) سفارش کالا و درج جزئیات سفارش
2) دریافت فاکتور و کنترل آن با سفارش انجام شده
3) دریافت کالا و کنترل آن با فاکتور
4) صدور مجوز پرداخت فاکتور

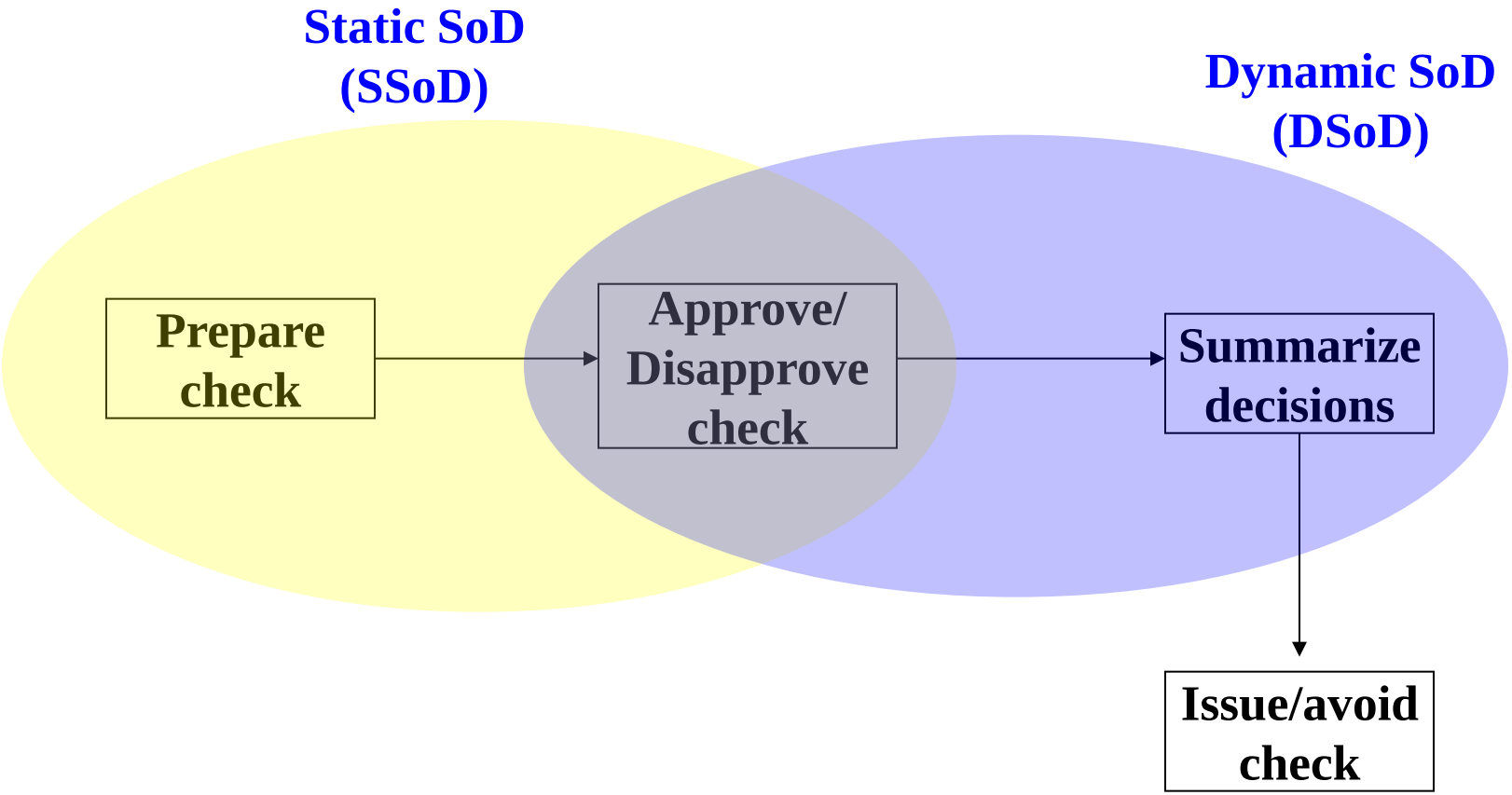
- محدودیت تفکیک وظایف ایستا:
  - هیچ فردی نمی‌تواند مسئولیت وظایف (۱) و (۳) را باهم داشته باشد.

ssod1=<{1,3}, 2>

  - حداقل ۳ نفر برای انجام ۴ مرحله فوق موردنیاز است.

۶- مدل $RBAC_2$

- مثالی از تفکیک وظایف ایستا و پویا



مدل نقش-مبنای سلسله‌مراتبی با محدودیت $RBAC_3$

گونه‌های توسعه‌یافته RBAC برای محیط‌های جدید محاسباتی

توسعه‌های RBAC (ادامه)

- GRBAC (Generalized RBAC) [Covington et al 2000]
  - یک مدل آگاه از زمینه
  - نقش‌های (گروههای)
    - عاملی: مشابه RBAC
    - شیئی: دسته‌بندی بر اساس خصوصیات مشترک، مثال: Laptop
    - محیطی: تعیین شرایط محیطی، مثال: Lab، Working-Days
  - قواعد دسترسی به‌صورت ترکیبی از نقش‌های محیطی، شیئی و عاملی (Students, Lab, Laptop)

توسعه‌های RBAC

- [Bertino et al 2001] TRBAC (Temporal RBAC)
  - یک مدل با قابلیت توصیف محدودیت‌های زمانی
  - تعریف محدودیت‌های زمانی در فعال سازی نقش‌ها
    - امکان فعال‌سازی نقش در بازه‌های زمانی مشخص

([1/1/2007, ∞], Night-time, enable doctor-on-night-duty)

enable nurse-on-day-duty → enable nurse-on-training after 16

توسعه‌های RBAC

- Drive RBAC [Wilikens et al 2002]

– یک مدل مبتنی بر خصوصیت (Attribute Based) و آگاه از زمینه

– نقش‌های از پیش تعریف‌شده

- هنگام ثبت کاربر بنا بر اعتبارنامه‌های وی

– نقش‌های فعال‌شده

- بر اساس زمینه کاری کاربر

– انتساب مجوزها به نقش‌ها

- به صورت پویا بر اساس محدودیت‌های زمینه‌ای هر کاربر