بسم الله الرحمن الرحیم

دانشگاه صنعتی شریف

آزمایشگاه امنیت داده و شبکه

کنترل دسترسی بر مبنای اعتماد و آگاه از مخاطره در گرید

Trust-driven Risk-aware Access Control in Grid

صادق دری نوگورانی

سخنرانی انجمن رمز ایران – ۲ مرداد ۱۳۹۵

اعتماد در دنیای مجازی

- مفهومی مشابه اعتماد در دنیای واقعی مورد نیاز است...

Fig. by Peter Steiner (The New Yorker, 5 July 1993)

چشم‌انداز ارائه

- مقدمات
  - اعتماد محاسباتی
  - تصمیم‌گیری
  - کنترل دسترسی
  - توری
- چارچوب پیشنهادی
  - معرفی چارچوب
  - مثالی از خط‌مشی‌ها
  - کاربرد در توری واقعی (EGI)

تعاریف اعتماد (محاسباتی)

- گَمبتّا (Gambetta): تعریف احتمالاتی اعتماد
  - «اعتماد احتمالی شخصی است که با استفاده از آن، یک فرد «آ» از فرد دیگری «ب» انتظار دارد که عمل مفروضی را انجام دهد که خیر او (آ) در آن است.»

- مِیِر (Mayer) و همکاران:
  - اعتماد تمایل یک طرف به قرارگرفتن در معرض آسیب اَعمال طرفی دیگر است. این تمایل در سایه انتظار اعتمادگر از طرف دیگر است به طوری که صرف نظر از توانایی نظارت یا کنترل، اعتمادپذیر عمل خاصی را انجام دهد که برای اعتمادگر مهم است.

تعاریف اعتماد (محاسباتی)

- مارش (Marsh):
  - «آ» به «ب» اعتماد می‌کند اگر و تنها اگر «آ» انتظار داشته باشد که «ب» به نفع وی رفتار می‌کند، و سعی نمی‌کند به وی آسیبی برساند.
- هاردین (Hardin):
  - «من به تو اعتماد می‌کنم چون فکر می‌کنم به نفع توست که منافع من را در خصوص موضوع مربوطه جدی بگیری.»
- روسو (Rousseau) و همکاران:
  - «[اعتماد] حالتی روحی-روانی در اعتمادگر مشتمل بر قصد پذیرش آسیب در شرایطی است که امکان مخاطره وجود دارد؛ بر اساس انتظارات مثبت از مقاصد یا رفتارهای \معتمد.»

تعریف ما از اعتماد

- تعریف ما از اعتماد
  - اعتماد، **باوری** شخصی است که با آن اعتمادگر ارزیابی می‌کند که وارد **رابطه‌ای** با اعتمادپذیر بشود که **مفید** (یا حداقل بی‌ضرر) برای اوست؛ در شرایطی که تلقی مداوم از **مخاطره** وجود دارد.
- نکات برجسته:
  - اعتمادگر یک عامل (Agent) است که می‌خواهد در مورد رابطه‌ای با اعتمادپذیر تصمیم‌گیری کند. مثال‌ها: انسان، ربات، نرم‌افزار، ترکیبی از اینها
  - اعتماد در شرایط عدم قطعیت معنادار است.
  - اعتماد ناظر به نوعی رابطه و نه لزوماً تعامل بین اعتمادگر و اعتمادپذیر است.
  - ارزیابی و انتظار حصول نتیجه نقش کلیدی در اعتماد دارد.

سناریوی اعتماد

اعتماد مستقیم

(عملکردی)

اعتمادگر

اعتماد غیر مستقیم (استنتاج)

اعتمادپذیر

ارجاعی

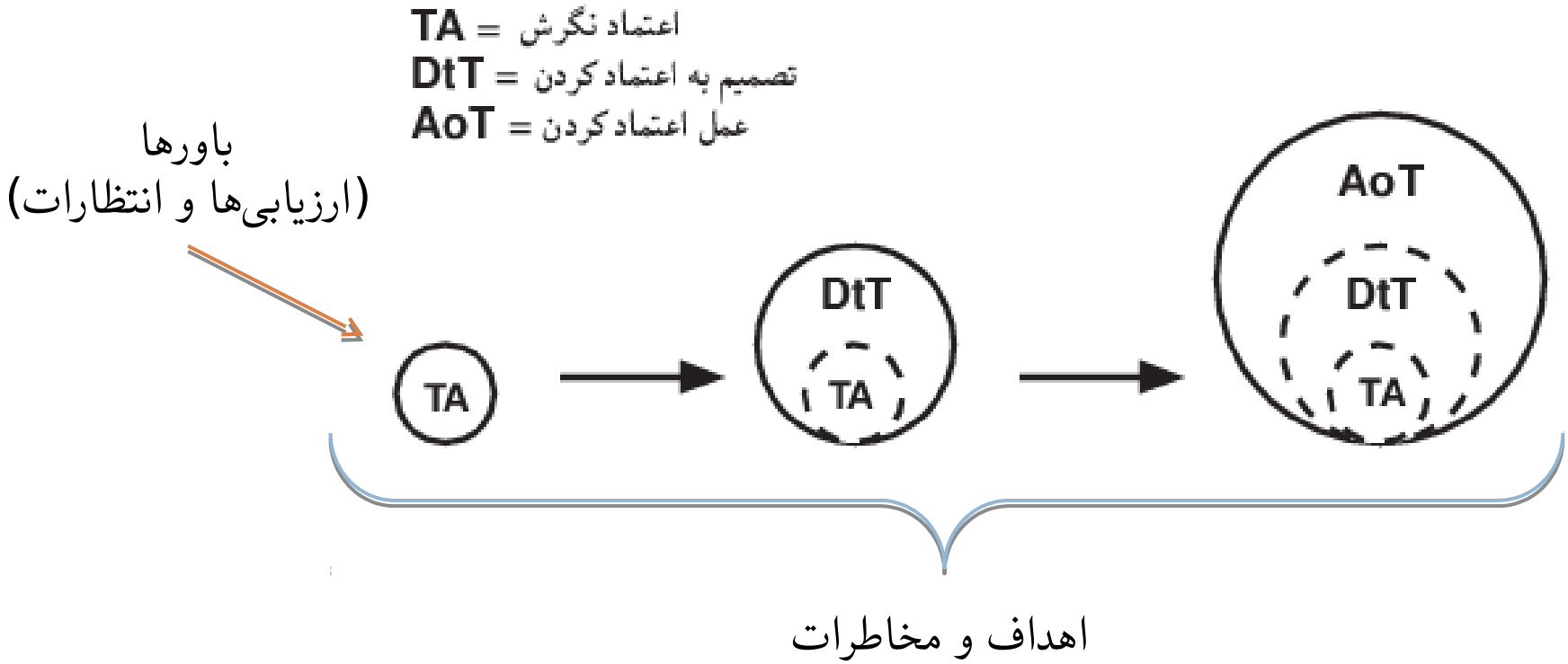
عملکردی

عملکردی

توصیه‌گران

لایه‌های اعتماد

- جایگاه اعتماد: پوشش عدم قطعیت اعتمادپذیر



منابع اعتماد

- ابعاد ضروری برای قابل اعتماد بودن
  - شایستگی: مثلاً توانایی‌ها و دانش چگونگی انجام کار
  - قابل پیش‌بینی بودن و تمایل
  - ایمنی (اعتمادگر نسبت به اعتمادپذیر)
- برخی منابع کسب اعتماد
  - سرشت اعتمادگر: تمایل کلی به اعتماد کردن (اعتماد پیش‌فرض)
  - شناخت (از صفات مرتبط با اعتماد)
  - رسته (category): عضویت در یک شبکه یا سازمان یا اجتماع
  - توصیه
  - حسابگری: ارزیابی معقول هزینه/فایده تقلب/رفتار صادقانه در ارتباط
  - **سابقه ارتباطات گذشته**

فعالیت‌های اعتمادگر

مدل‌سازی و پردازش اعتماد

- مدل‌های قطعی
  - رتبه‌بندی، امتیازدهی، روش‌های مبتنی بر جریان، ...
- احتمالاتی
  - انتخاب توابع احتمال، تخمین پارامترها، پیش‌بینی
- فازی
  - فازی‌سازی ورودی‌های صریح، استنتاج فازی، صریح‌سازی خروجی‌های فازی
- شواهدی (نظریه ریاضی شواهد یا نظریه دِمپستر و شِیفر)
  - اغلب متمرکز بر مدل‌سازی

کنترل دسترسی

- پرسش اصلی:
  - آیا فاعل s اجازه عمل a را بر روی شیء o در زمینه c دارد؟
- اطلاعات
  - **فاعل:** کاربر یا برنامه به وکالت از کاربر
  - **شیء:** فایل، سیستم کامپیوتری، شبکه، یا هر منبع دیگر
  - **عمل:** انواع آن وابسته به شیء و فاعل است. مثلاً خواندن فایل، اجرای برنامه بر روی سیستم، ارسال بسته در شبکه، و...
  - **زمینه:** سایر اطلاعات عموماً محیطی یا پویا و وابسته به متغیرهایی غیر از سه‌گانه ذکر شده؛ از قبیل زمان، مکان، اطلاعات تکمیلی در خصوص فاعل، عمل یا شیء.
- اعتماد خط‌مشی‌بنیاد و کنترل دسترسی

تصمیم‌گیری در کنترل دسترسی مبتنی بر اعتماد

- صورت مسئله
  - گزینه‌ها: ندادن مجوز، دادن مجوز (با شرایط مختلف)
  - حالات: برآورده شدن انتظارات، نقض انتظارات
  - ترجیحات: تابع مطلوبیت
- تابع مطلوبیت (utility): تابع اثر $e : R \to \mathbb{R}$
  - یک انتساب دلخواه از اعداد به حالات نتیجه تصمیم‌گیری که e(x) اثر x نامیده می‌شود.
  - رابطه ترجیح در اینجا

- $x \succ y$ اگر و تنها اگر اثر x بر اهداف بهتر از اثر y باشد.

- $x \sim y$ است اگر و تنها اگر اثر x با y یکسان باشد.

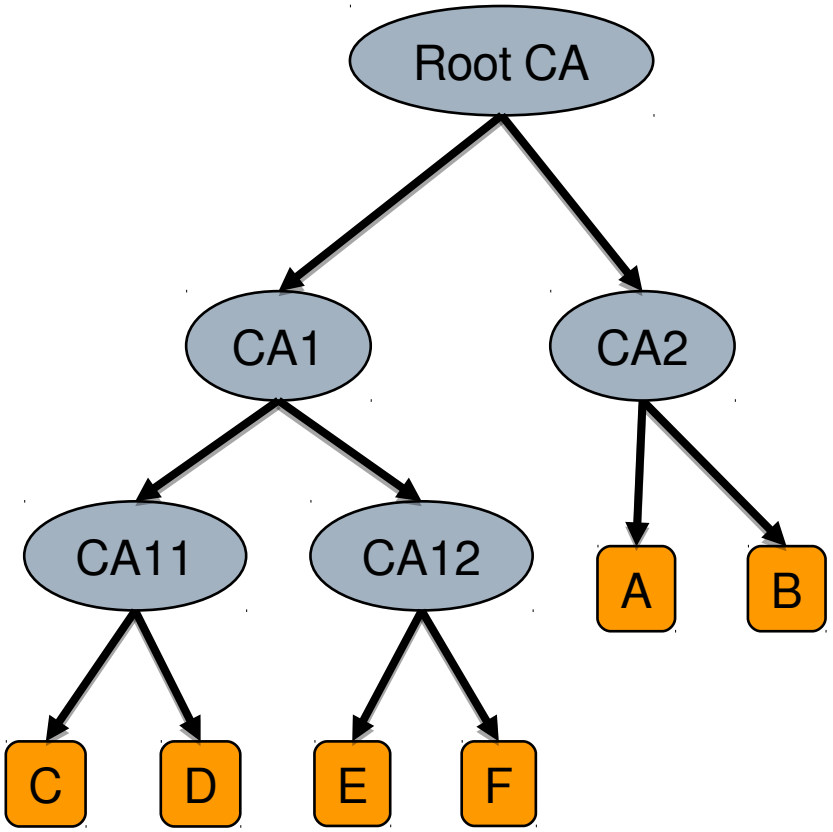
انواع مدل‌های تصمیم

- تصمیم در حضور عدم قطعیت احتمالاتی
  - مطلوبیت یک گزینه = امید ریاضی تابع مطلوبیت

$$Utility = p*u(s) + (1-p)*u(f)$$

- تصمیم در حضور جهل: وابسته به نگرش تصمیم‌گیرنده
  - بدبینانه: مطلوبیت گزینه = بدترین مطلوبیت ممکن
  - خوش‌بینانه: مطلوبیت گزینه = بهترین مطلوبیت ممکن
  - هورویچ: مطلوبیت گزینه = میانگین وزن‌دار مطلوبیت‌های ممکن
  - میانگین ساده: مطلوبیت گزینه = میانگین حسابی مطلوبیت‌های ممکن
- تصمیم در حضور سایر انواع عدم قطعیت
  - انتگرال شوکه (Choquet)، انتگرال سوگنو (Sugeno)، سایر انتگرال‌های فازی

مثال: اعتماد در PKI



مثال

Certificate Viewer:"*.wikipedia.org"

General | Details

This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	*.wikipedia.org
Organization (O)	Wikimedia Foundation, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	11:21:A2:25:BA:04:02:D7:91:85:48:54:C8:BA:60:68:6A:9B

Issued By

Common Name (CN)	GlobalSign Organization Validation CA - SHA256 - G2
Organization (O)	GlobalSign nv-sa
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	جمعه, 20 آذر 1394
Expires On	یکشنبه, 21 آذر 1395

Fingerprints

SHA-256 Fingerprint	30:15:34:18:F0:9D:DF:DF:32:B4:45:B1:25:4B:33:1E:B7:D9:25:7B:C3:79:7F:C2:AF:95:BF:A1:86:69:99:FE
SHA1 Fingerprint	87:F5:BA:BB:D8:97:C5:79:B6:6A:F5:2F:D8:63:8B:99:BD:1C:E8:26

توری چیست؟

توری سامانه‌ای است که ساماندهی می‌کند: (تعریف آقای فاستر)

- منابعی را که تحت کنترل مرکزی نیستند
  - منابع و کاربران در دامنه‌های مدیریتی مختلف
- برای ارائه کیفیت خدمات مناسب
  - همچون زمان پاسخ، گذردهی، امنیت و...
  - ارزش مجموع، بیش از تک تک منابع
- با پروتکل‌ها و رابط‌های عام-منظوره، باز و استاندارد
  - همچون خدمات وب، پروتکل‌های شبکه، اجزای امنیتی و...
- کاربرد واقعی در عمل:
  - تشریک مساعی علمی و اشتراک منابع برای محاسبات علمی با کارایی بالا (HPC)

ساختار فیزیکی و مجازی توری

- سایت
  - مجموعه‌ای از منابع و کاربران
  - یک دامنه مدیریتی که اجزای آن معمولاً از لحاظ فیزیکی هم نزدیک به هم هستند.
  - مثال: یک کلاستر، یک سازمان (فیزیکی)
  - ساختار فیزیکی یک گرید را مجموعه سایت‌های آن تعیین می‌کنند.
- سازمان مجازی (VO)
  - مجموعه‌ای از منابع و کاربران که برای حل مسئله‌ای خاص بسیج شده‌اند.
  - ممکن است چندین سایت را در دامنه‌های مدیریتی مختلف دربرگیرد.
  - هر کاربر ممکن است عضو چند سازمان مجازی باشد و به واسطه عضویت، کارهایی را به منابع غیر محلی بسپارد.

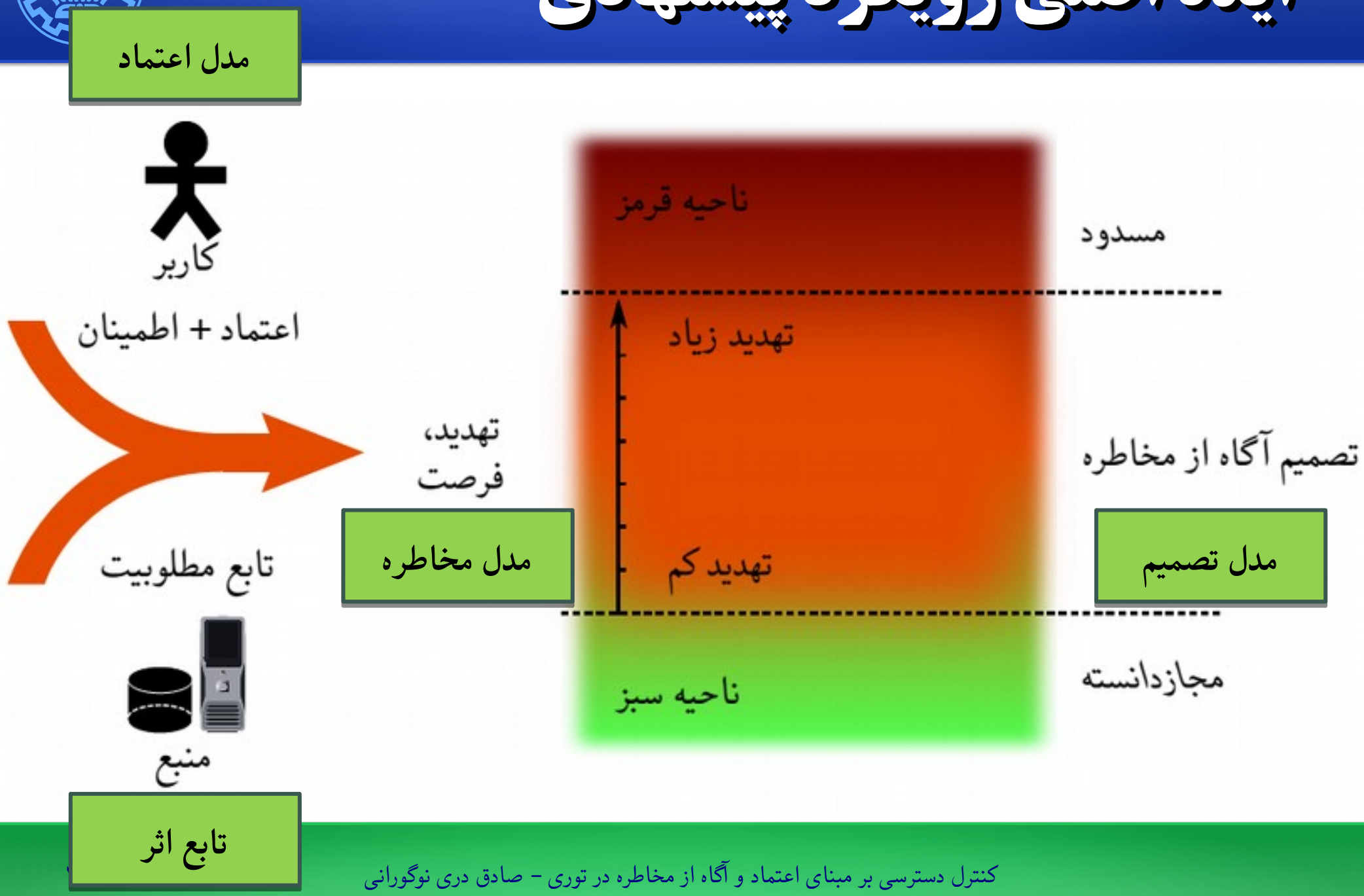
اعتماد و مخاطره در کنترل دسترسی توری

- چالش کنترل دسترسی در توری
  - کاربران و وظایف غریبه و ناشناخته (پویا)
  - خطر سوءاستفاده از مجوزها، حملات از درون، و بی‌مسئولیتی
- کنترل دسترسی مبتنی بر اعتماد (سابقه-بنیاد):
  - تعیین مجوزهای کاربر بر اساس سابقه رفتار وی
- کنترل دسترسی آگاه از مخاطره:
  - مجوزها بر اساس ارزیابی صریح منفعت و ضرر صادر می‌شوند.

چارچوب پیشنهادی: آرام

چارچوب کنترل دسترسی اعتماد-رانۀ آگاه از مخاطره

ایده اصلی رویکرد پیشنهادی



التزام‌ها (Obligations)

- قیدهایی برای مجوزهای دسترسی
  - پیش‌نیاز (pre-obligation/provision): باید قبل از دسترسی برآورده شود.
  - هم‌نیاز: باید همزمان با دسترسی برآورده شود.
  - پس‌نیاز (post-obligation): باید پس از دسترسی برآورده شود.
- انواع
  - کاربری: یک کاربر باید آن را برآورده کند.
  - سیستمی: یک سیستم یا منبع باید آن را برآورده کند.
- خصوصیات
  - نوع عمل و آرگومان‌های آن، فاعل، زمان انجام، وضعیت برآورده شدن

التزام‌های ویژه آرام

- کاربرد التزام‌ها در آرام
  - تعیین صریح انتظارات ارائه دهنده خدمت از خدمت‌گیرنده
  - معیاری برای تعیین بازخورد/نتیجهٔ دادن مجوز
  - راهکاری برای مقابله با مخاطره
- التزام‌های اعتماد (برای درخواست دهنده)
  - توقعات مالک منبع که نگران برآورده نشدنشان هستیم.
  - ملاک تعیین اعتماد هستند.
  - هر التزام اعتماد، یک التزام بازرسی مرتبط دارد.
- التزام‌های بازرسی (برای بازرس)
  - فاعل آن یکی از کاربران محلی با صلاحیت است.
- التزام‌های تخفیف مخاطره (mitigation؛ برای مالک منبع)
  - فاعل آن مالک منبع مرتبط است.
  - به واسطه خط‌مشی‌های تخفیف مخاطره به درخواست‌های دسترسی ملحق می‌شوند.

خط‌مشی‌ها در آرام

- خط‌مشی‌های کنترل دسترسی
  - وابسته به قواعد بیان و پردازش خط‌مشی‌ها در ناظر مرجع (پایه)
  - هر مجوز، می‌تواند مجموعه‌ای از التزام‌ها (عادی/اعتماد) را نیز مشخص کند.
- خط‌مشی‌های تخفیف مخاطره
  - تعیین کننده تابع مطلوبیت (اثر) و خط‌مشی تخفیف مخاطره هر اتلزام اعتماد

$$\{(\text{بسیار-کم}, B_1), (l_2, B_2), \ldots, (\text{بسیار-زیاد}, B_l)\}$$

  - التزام ویژه $\perp$: مخاطره غیر قابل پذیرش
- خط‌مشی‌های ظرفیت مخاطره
  - تعیین کننده خط قرمز مالک منبع در خصوص میزان مخاطره قابل پذیرش

$$eval(ri_a) = \begin{cases} \text{قابل‌قبول} & ri_a > th \\ \text{غیرقابل‌قبول} & \text{غیر آن} \end{cases}$$

- ملاک‌های تعیین مطلوبیت (اثر) یک دسترسی

- **هزینهٔ اجرای وظیفه** (EC): متناسب با هزینه‌ای است که مالک منبع برای نگهداری و اجرای وظایف بر روی آن خرج می‌کند.
- **منفعت کامل شدن وظیفه** (CB): متناسب با منفعتی است که مالک منبع از مشارکت در یک سازمان مجازی و اجرای موفق یک وظیفه می‌برد.
- **منفعت مشارکت** (PB): متناسب با منفعتی است که مالک منبع از مشارکت در یک سازمان مجازی و اجرای یک وظیفه می‌برد هرچند وظیفه به طور موفق خاتمه نیافته باشد.

التزام ۱

مثال ۱. التزام۱: وظیفهٔ مربوطه باید بدون خطا پایان یابد.

کاربران بی‌مسئولیت ممکن است کد غیرقابل اتکا و خرابی را اجرا کنند که منابع توری را هدر می‌دهد. با این التزام می‌توان نسبت به استفاده مؤثر از منابع تخصیص یافته و جلوگیری از دسترسی‌های مخاطره‌انگیز اطمینان نسبی حاصل کرد. تابع اثر و راهبرد تخفیف مخاطره مربوطه عبارتند از:

$$u_s = CB - EC, \quad u_f = PB - EC. \tag{۳.۹}$$

$$\{(\text{بسیار-کم}, \emptyset), (\text{کم}, \emptyset), (\text{متوسط}, \emptyset), (\text{زیاد}, \{\bot\}), (\text{بسیار-زیاد}, \{\bot\})\} \tag{۴.۹}$$

التزام ۲

مثال ۲. التزام۲: یک دستمزد اجرای وظیفه (EF) باید پرداخته شود؛ در صورتی که وظیفه با موفقیت خاتمه یافته باشد.

مالک وظیفه باید پس از اینکه وظیفه‌اش با موفقیت و در مهلت مقرر به پایان رسید، دستمزدی را به مالک منبع بپردازد. اما اگر منبع موفق به اجرای وظیفه نشود، هیچ مبلغی نمی‌پردازد. تابع اثر و راهبرد تخفیف مخاطره به شکل زیر است:

$$u_{\mathsf{s}} = CB - EC + EF, \quad u_{\mathsf{f}} = PB - EC. \tag{۵.۹}$$

$$\{(\text{بسیار-کم}, \emptyset), (\text{کم}, \emptyset), (\text{متوسط}, \{\text{deposit}(\circ/۳EF)\}), \\ (\text{زیاد}, \{\text{deposit}(\circ/۶EF)\}), (\text{بسیار-زیاد}, \{\bot\})\} \tag{۶.۹}$$

التزام ۳

مثال ۳. التزام۳: نباید از داده‌های ورودی سوء استفاده شود.

داده‌های ورودی وظیفه نباید در اختیار موجودیت‌هایی که عضو سازمان مجازی نیستند قرار گیرد. همچنین نباید به صورتی غیر از آنچه قرار بوده است استفاده شود. تابع اثر و راهبرد تخفیف مخاطره مربوطه عبارتند از:

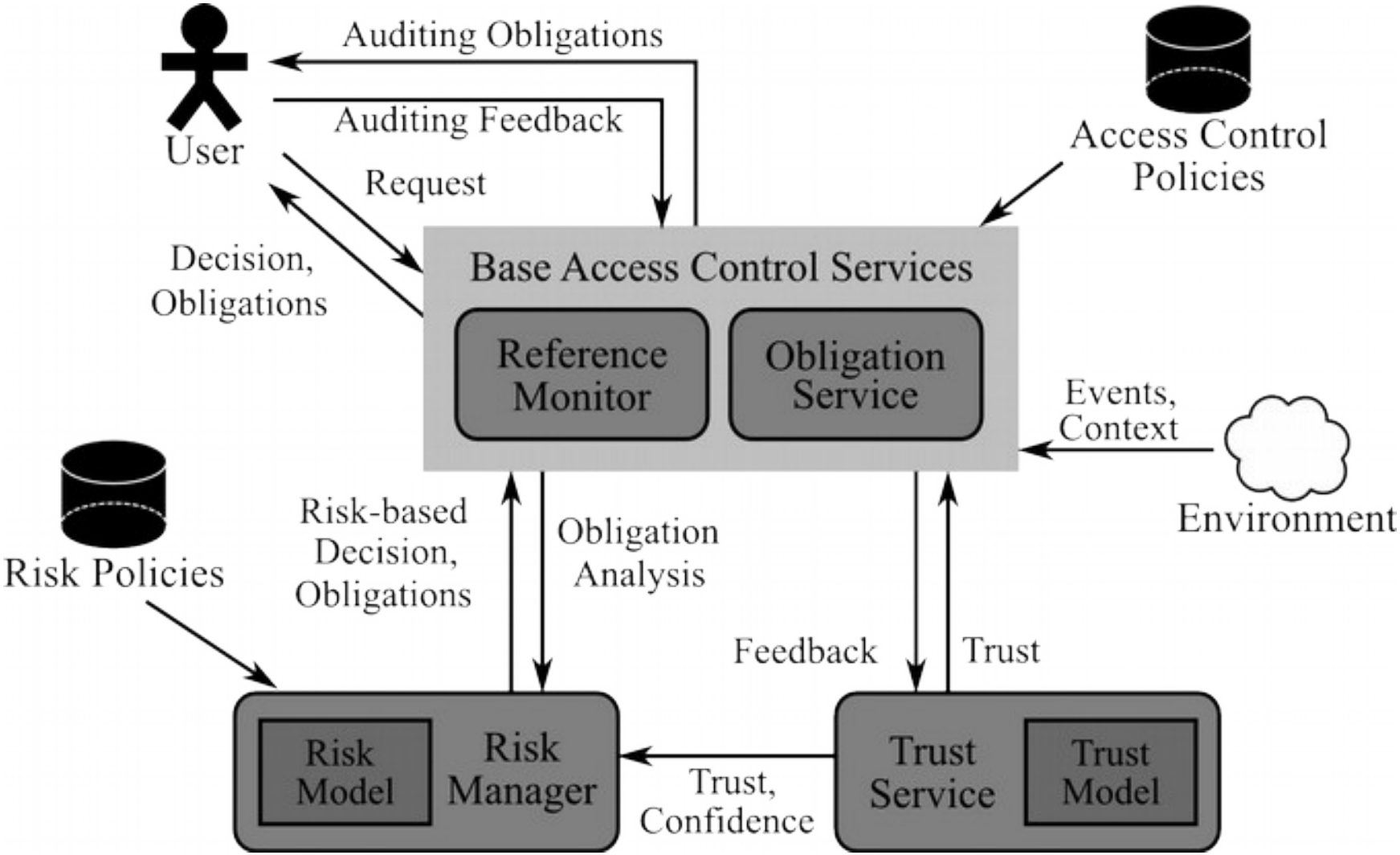
$$u_s = CB - EC, \quad u_f = PB - EC - DL. \tag{۷.۹}$$

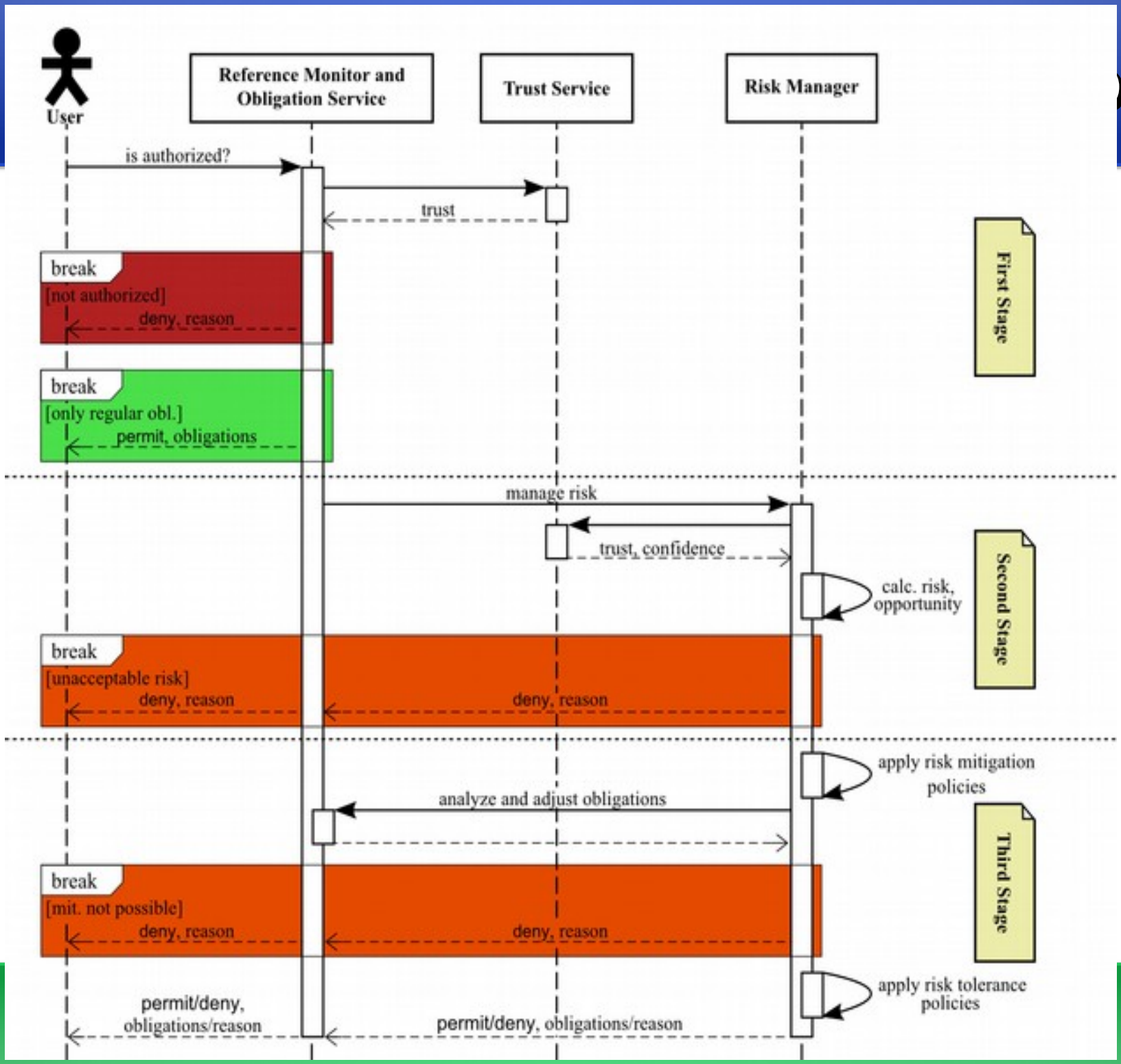
$$\{(\text{بسیار-کم}, \{\text{sign-nda}\}), (\text{کم}, \{\text{sign-nda}\}),$$

$$(\text{متوسط}, \{\text{sign-nda, vo-confirm}\}), \tag{۸.۹}$$

$$(\text{زیاد}, \{\text{sign-nda, vo-confirm, insure}\}), (\text{بسیار-زیاد}, \{\bot\})\}$$

معماری آرام


Auditing Obligations
Auditing Feedback
User
Request
Decision,
Obligations
Access Control
Policies
Base Access Control Services
Reference
Monitor
Obligation
Service
Events,
Context
Environment
Risk Policies
Risk-based
Decision,
Obligations
Obligation
Analysis
Feedback
Trust
Risk
Model
Risk
Manager
Trust,
Confidence
Trust
Service
Trust
Model


User
Reference Monitor and Obligation Service
Trust Service
Risk Manager
is authorized?
trust
break
[not authorized]
deny, reason
break
[only regular obl.]
permit, obligations
First Stage
manage risk
trust, confidence
calc. risk, opportunity
Second Stage
break
[unacceptable risk]
deny, reason
deny, reason
apply risk mitigation policies
analyze and adjust obligations
Third Stage
break
[mit. not possible]
deny, reason
deny, reason
apply risk tolerance policies
permit/deny, obligations/reason
permit/deny, obligations/reason

ارزیابی مخاطره مثال‌ها

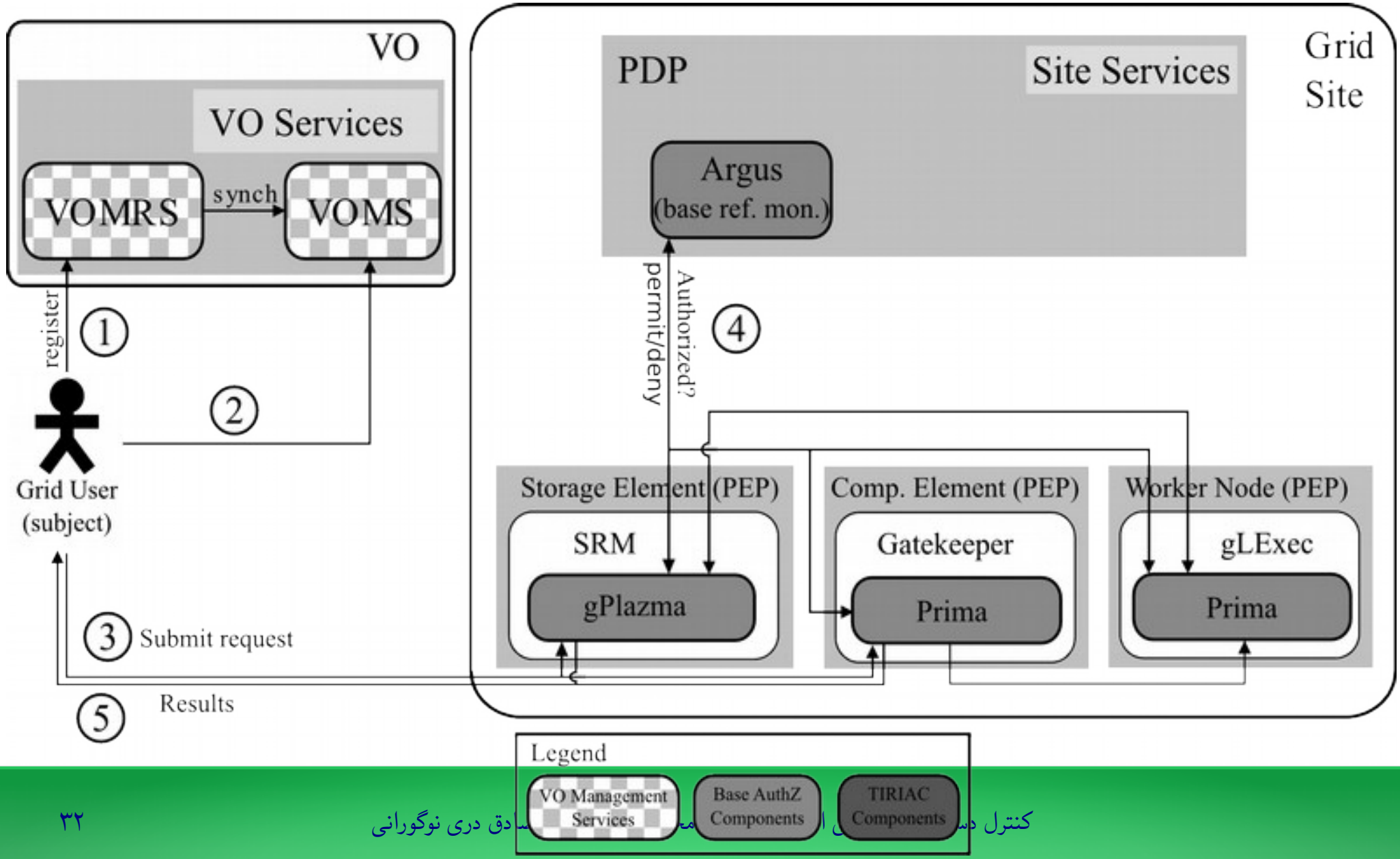
- مقادیر نمونه برای پارامترهای مثال‌ها

شرح	پارامتر	مقدار (وظیفه/U)
هزینهٔ اجرای وظیفه	EC	۴۸٪
منفعت کامل شدن وظیفه	CB	۱۱۰٪
منفعت مشارکت	PB	۱۰٪
دستمزد اجرای وظیفه	EF	۵۰٪
ضرر سوء استفاده از داده	DL	۵۰٪

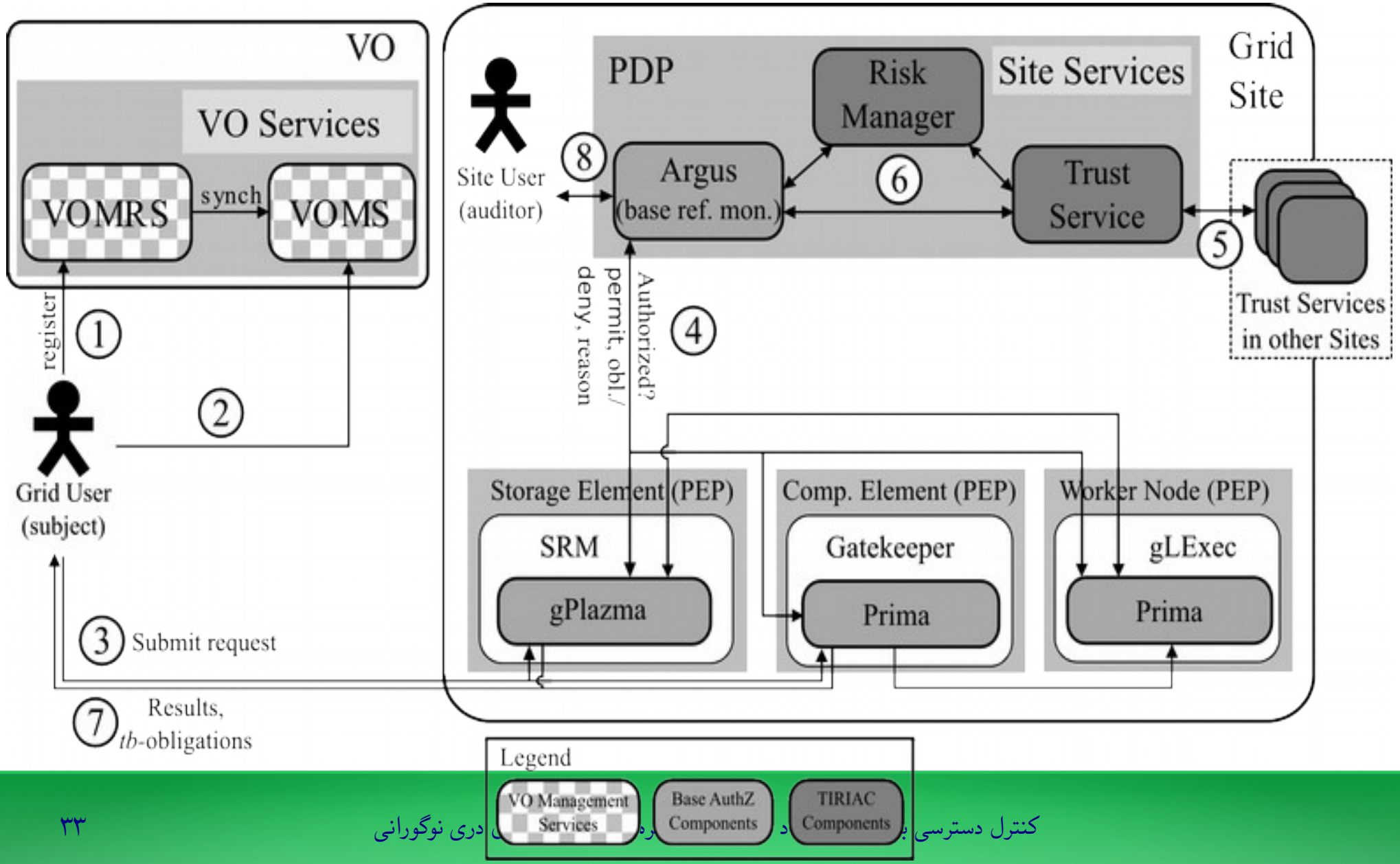
- مخاطره و سطح تهدید برای مقادیر مختلف اعتماد

	u_s	u_f	$\tau = ۰/۱$	$\tau = ۰/۴$	$\tau = ۰/۶$	$\tau = ۰/۹$
التزام۱	۶۲٪	−۳۸٪	بسیار-زیاد (−۲۸٪)	بسیار-زیاد (۲٪)	کم (۳۲٪)	بسیار-کم (۵۲٪)
التزام۲	۱۱۲٪	−۳۸٪	بسیار-زیاد (−۲۳٪)	کم (۲۲٪)	بسیار-کم (۶۷٪)	بسیار-کم (۹۷٪)
التزام۳	۶۲٪	−۸۸٪	بسیار-زیاد (−۷۳٪)	بسیار-زیاد (−۲۸٪)	متوسط (۱۷٪)	بسیار-کم (۴۷٪)

کنترل دسترسی در EGI



کنترل دسترسی با استفاده از آرام



جمع‌بندی

- اعتماد سابقه‌بنیاد می‌تواند به خوبی با خط‌مشی‌ها ترکیب شود.
- استفاده از التزام‌ها انعطاف‌پذیری بی‌مانندی را به سیاستگزاران می‌دهد.
- امکان به‌کارگیری چارچوب آرام در یک توری واقعی وجود دارد.

با تشکر

منابع

- ص. دری نوگورانی، اعتماد محاسباتی در حضور عدم قطعیت، رساله دکتری با راهنمایی ر. جلیلی، دانشگاه صنعتی شریف، بهمن ۱۳۹۴

- S. Dorri Nogoorani and R. Jalili, "**TIRIAC: A Trust-driven Risk-aware Access Control Framework for Grid Environments**," *Future Generation Computer Systems, Special Issue on Trust, Security and Privacy in Emerging Distributed Systems*, Elsevier, ۲۰۱۶, pp. ۲۳۸–۲۵۴.