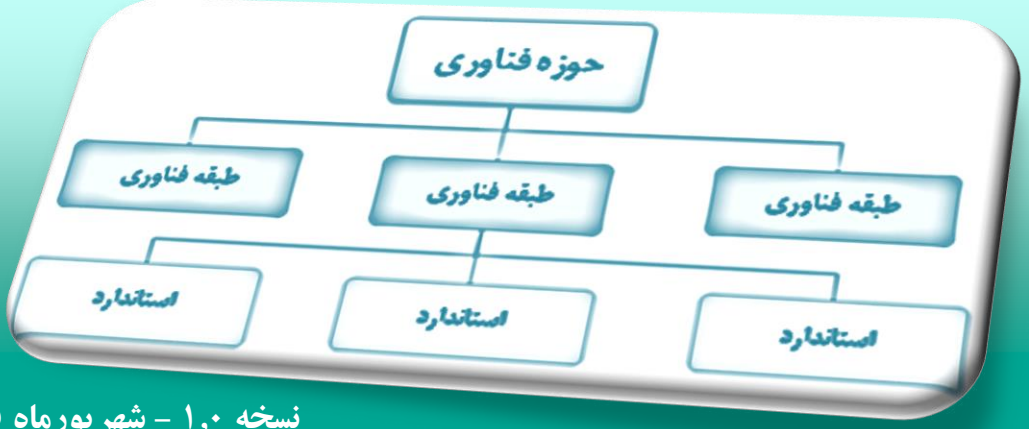
شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

مدل مرجع فناوری



نسخه ۱,۰ - شهریورماه ۱۳۹۵

پیشگفتار

این سند در راستای تشریح مدل مرجع فناوری(دولت)، به عنوان یکی از شش مدل مرجع چارچوب معماری سازمانی ایران تهیه و منتشر می‌گردد. این مدل، دربردارنده ساختار طبقه‌بندی فناوری‌ها، استانداردها و ابزارهای فناوری اطلاعات در راستای ارایه سرویس‌های فاوا به ذینفعان است.

استفاده از این مدل مرجع در سطح ملی(دستگاه‌های اجرایی) باعث ایجاد یک زبان و ساختار مشترک برای شناسایی، طبقه‌بندی و مقایسه فناوری‌ها می‌شود و بدین ترتیب دایره‌المعارفی مشترک از فناوری‌ها و استانداردها فراهم می‌کند که جستجو، همکاری و تعامل‌پذیری بین دستگاه‌های مختلف را تسهیل می‌کند. با استفاده از مدل مرجع فناوری، کلیه دستگاه‌های اجرایی نیازی به بررسی چندین باره فناوری‌ها و استانداردها جهت انتخاب نداشته و در وقت و هزینه تحلیل‌های فنی صرفه‌جویی قابل توجهی خواهد شد.

این سند، تنها به تشریح یکی از شش مدل مرجع چارچوب معماری سازمانی ایران می‌پردازد و مخاطبان باید سایر اسناد مربوط به چارچوب را نیز مطالعه کرده و در کنار این سند مورد استفاده قرار دهند.

از آنجا که محتوای این سند حاصل اولین تجربه تدوین مدل مرجع عملکرد در دولت جمهوری اسلامی ایران است، احتمال می‌رود اشکالات و نواقصی در این سند دیده شود که امید است با همکاری و مشارکت صاحب‌نظران امر، تکمیل شود، لذا از مخاطبان درخواست می‌شود نظرات و پیشنهادات اصلاحی خود را از طریق پست الکترونیکی info@ieaf.ir به اطلاع متولیان طرح برسانند.

جهت اطلاع و دریافت اسناد فنی، رهنمون‌ها و مثال‌ها، ضوابط قانونی، مدل‌های مرجع و اطلاع از آخرین تغییرات مربوط به چارچوب معماری سازمانی ایران، به پورتال www.IEAF.ir مراجعه شود.

ارکان اجرای طرح تدوین چارچوب معماری سازمانی ایران	
کارفرمای طرح	شورای اجرایی(عالی) فناوری اطلاعات کشور – کمیسیون توسعه دولت الکترونیکی
مدیریت طرح	معاونت دولت الکترونیکی سازمان فناوری اطلاعات ایران
ناظر طرح	مدیریت امور اصلاح ساختار و توسعه دولت الکترونیک سازمان امور اداری و استخدامی کشور
مشاور(مجری)	آزمایشگاه مرجع معماری سازمانی سرویس‌گرا دانشگاه شهید بهشتی

اعضای تیم مدیریت و نظارت طرح	
مدیر ارشد طرح	جناب آقای نصرالله جهانگرد جناب آقای رضا باقری اصل
مدیریت فنی و اجرایی	جناب آقای مازیار مباشری سرکار خانم فائزه حسینی سرکار خانم پریسا صیادی
نظارت بر طرح	جناب آقای علی‌رضا شاه‌پری جناب آقای محمدرضا زین‌الدینی

اعضای تیم تدوین چارچوب (مجری)	
راهبر و مدیر ارشد پروژه	جناب آقای فریدون شمس علیئی
مدیر فنی و اجرایی پروژه	جناب آقای امیر مهجوریان
کمیته مشورتی و خبرگانی	سرکار خانم نسترن حاجی‌حیدری
	جناب آقای ابراهیم ابطحی
	جناب آقای محمود خراط
	جناب آقای رضا کرمی
	جناب آقای سعید مومنی
	سرکار خانم بتول ذاکری
	جناب آقای پیمان سنایی
	جناب آقای علی فیروزی
تیم فنی و کارشناسی	جناب آقای سعید شکراللهی
	جناب آقای رضا رضایی
	سرکار خانم مهسا رجب‌پور
	سرکار خانم آزاده احمدی
	سرکار خانم فروزان مخصوص
	سرکار خانم مرضیه سمغانی‌نژاد
	جناب آقای حمید لیوانی
	جناب آقای حسام الدین وزیری
	جناب آقای حسین آذرپناه
	سرکار خانم فاطمه ربیع‌نیا
	جناب آقای مهدی فعال
	جناب آقای پیمان ناصرآبادی
	سرکار خانم شبنم نوابی

فهرست مطالب

۱ معرفی مدل مرجع فناوری ۹

۱-۱ تعریف مدل مرجع فناوری ۹

۱-۲ کاربردهای مدل ۱۰

۱-۳ سیاست‌های بالادستی مرتبط با مدل مرجع فناوری ۱۰

۱-۴ جایگاه مدل در چارچوب معماری سازمانی ایران ۱۱

۲ تشریح مدل مرجع فناوری ۱۳

۲-۱ حوزه دسترسی و تحویل سرویس ۱۵

۲-۲ حوزه یکپارچه‌سازی و واسط سرویس ۳۲

۲-۳ حوزه چارچوب مؤلفه سرویس ۴۸

۲-۴ حوزه زیرساخت و سکوی سرویس ۷۴

۳ اصول پیاده‌سازی مدل مرجع فناوری ۱۰۰

۳-۱ پشتیبانی از استانداردها و معماری‌های باز ۱۰۰

۳-۲ تعامل‌پذیری ۱۰۰

۳-۳ استفاده از فناوری‌های جدید و اثبات‌شده صنعتی ۱۰۱

۳-۴ مقیاس‌پذیری، قابلیت دسترسی، پشتیبان‌گیری و بایگانی ۱۰۱

۳-۵ تغییرات بر اساس نیازهای کسب‌وکار ۱۰۲

پیوست الف: واژه‌نامه ۱۰۴

فهرست جدول‌ها

جدول ۲-۱ مثال‌هایی از کانال‌های دسترسی..... ۱۵
جدول ۲-۲ مثال‌هایی از کانال‌های تحویل..... ۲۰
جدول ۲-۳ مثال‌هایی از نیازمندی‌های سرویس..... ۲۲
جدول ۲-۴ مثال‌هایی از پروتکل‌های ارتباطی جهت برقراری اتصالات متقابل..... ۲۵
جدول ۲-۵ مثال‌هایی از ابزارها و استانداردهای یکپارچه‌سازی فرایند..... ۳۲
جدول ۲-۶ مثال‌هایی از ابزارها و استانداردهای یکپارچه‌سازی کاربرد/ سرویس..... ۳۵
جدول ۲-۷ مثال‌هایی از پروتکل‌ها و استانداردهای یکپارچه‌سازی داده..... ۴۰
جدول ۲-۸ مثال‌هایی از واسط‌های یکپارچه‌سازی بیرونی..... ۴۶
جدول ۲-۹ مثال‌هایی از نرم‌افزارها و پروتکل‌های تعریف قوانین کسب‌وکار..... ۴۸
جدول ۲-۱۰ مثال‌هایی ازپروتکل‌ها و روش‌های کنترل داده..... ۴۹
جدول ۲-۱۱ مثال‌هایی از ابزارهای نمایش..... ۵۹
جدول ۲-۱۲ مثال‌هایی از ابزارها و روش‌های مدیریت اطلاعات..... ۶۲
جدول ۲-۱۳ مثال‌هایی از پایگاه‌داده‌ها و دستگاه‌های ذخیره‌سازی..... ۷۴
جدول ۲-۱۴ مثال‌هایی از خدمتگزارهای تحویل..... ۷۷
جدول ۲-۱۵ مثال‌هایی از سکوهای پشتیبان..... ۷۹
جدول ۲-۱۶ مثال‌هایی از زیرساخت‌ها و سخت‌افزارهای قابل استفاده..... ۸۰
جدول ۲-۱۷ مثال‌هایی از فناوری‌های قابل به‌کارگیری در مهندسی نرم‌افزار..... ۸۸

فهرست شکل‌ها

شکل ۱-۱ جایگاه مدل مرجع فناوری در چارچوب معماری سازمانی ایران..... ۱۱
شکل ۲-۱ حوزه‌های مدل مرجع فناوری..... ۱۳
شکل ۲-۲ ساختار مدل مرجع فناوری..... ۱۴

فصل اول

معرفی مدل مرجع فناوری

۱ معرفی مدل مرجع فناوری

محتوای این فصل به معرفی تعاریف، مفاهیم، محدوده و کاربردهای مدل مرجع فناوری اختصاص دارد.

۱-۱ تعریف مدل مرجع فناوری

"مدل مرجع فناوری"[۱] به عنوان یکی از شش مدل مرجع "چارچوب معماری سازمانی ایران"[۲] دربردارنده ساختار طبقه‌بندی فناوری‌ها، استانداردها و ابزارهای فناوری اطلاعات در راستای ارایه سرویس‌های فاوا به ذینفعان است. این مدل، طبقه‌بندی همه فناوری‌ها و استانداردهای فناوری اطلاعات را با نگاه سرویس‌محور ارایه نموده و اصول و رهنمون‌هایی برای استفاده از آن در سطح دستگاه‌های اجرایی ارایه می‌نماید.

استفاده از این مدل مرجع در سطح ملی(دستگاه‌های اجرایی) باعث ایجاد یک زبان و ساختار مشترک برای شناسایی، طبقه‌بندی و مقایسه فناوری‌ها می‌شود و بدین ترتیب دایره‌المعارفی مشترک از فناوری‌ها و استانداردها فراهم می‌کند که جستجو، همکاری و تعامل‌پذیری بین دستگاه‌های مختلف را تسهیل می‌کند. با استفاده از مدل مرجع فناوری، کلیه دستگاه‌های اجرایی نیازی به بررسی چندین باره فناوری‌ها و استانداردها جهت انتخاب نداشته و در وقت و هزینه تحلیل‌های فنی صرفه‌جویی قابل توجهی خواهد شد.

مدل مرجع فناوری تصویر کلان معماری فناوری دولت را ترسیم می‌نماید تا در مرحله بعد هر دستگاه اجرایی جزئیات و نحوه پیاده‌سازی این نقشه کلان را در قالب جزئیات معماری سازمانی خود تدوین و پیاده‌سازی نماید. همچنین این مدل به توصیف همه گزینه‌ها و مصادیق قابل استفاده می‌پردازد و تصمیم‌گیری برای انتخاب نهایی فناوری یا استاندارد را به دستگاه‌های اجرایی و متولیان حوزه فناوری واگذار نموده است.

این مدل براساس چندین سال بررسی‌های تحلیلی نمونه مدل‌های مرجع معماری در دیگر کشورها و انطباق آن با نیازهای کشور طراحی و سفارشی‌سازی شده است.

مدل مرجع فناوری، همانگونه که از نام آن مشخص است یک مدل و الگوی طبقه‌بندی است و تا زمانیکه به‌صورت موثر و کاربردی توسط دستگاه‌ها و متولیان مربوطه مورد استفاده و پیاده‌سازی قرار نگیرد، منجر به تغییر و تحول در لایه فناوری دولت و دستگاه‌های زیرمجموعه نخواهد شد.

---

[۱] Technology Reference Model(TRM)

[۲] Iran Enterprise Architecture Framework (IEAF)

۱-۲ کاربردهای مدل

مدل مرجع فناوری به عنوان یکی از اجزاء چارچوب معماری سازمانی ایران، در طی اجرای معماری سازمانی یا مستقلا برای کاربردهای زیر قابل استفاده است:

- فراهم‌سازی یک چارچوب و زبان مشترک برای شناسایی و طبقه‌بندی فناوری‌ها، استانداردها و ابزارهای مرتبط با فناوری اطلاعات
- ترسیم نقشه جامع فناوری‌ها و استانداردهای فاوا دولت و ابلاغ آن به دستگاه‌های اجرایی
- کمک به دستگاه‌های اجرایی برای اینکه وضعیت موجود فناوری‌های مورد استفاده را طبق یک الگوی آماده تهیه نموده و شکاف‌ها و کمبودهای وضعیت موجود را استخراج نمایند.
- صرفه‌جویی در مطالعات و بررسی‌های تحلیلی که در دستگاه‌های اجرایی مختلف برای شناسایی و طبقه‌بندی فناوری‌ها و استانداردهای فاوا انجام می‌شود
- شناسایی فناوری‌های مشترک در دستگاه‌های اجرایی و در نتیجه برنامه‌ریزی برای کاهش تفاوت‌ها و تضادهای فناوری که عامل اصلی عدم تعامل‌پذیری بین دستگاه‌ها است.

۱-۳ سیاست‌های بالادستی مرتبط با مدل مرجع فناوری

در استفاده از مدل مرجع فناوری و تعیین و انتخاب مصادیق برای هر استاندارد سرویس، علاوه بر اصول ارائه شده در فصل سوم این سند، نیاز است که سیاست‌های دولت در زمینه‌های ذیل نیز توسط مخاطبین سند لحاظ گردد.

- سیاست‌های دولت در توسعه سفارشی و بومی نرم‌افزارها[۳]
- سیاست‌های دولت در تعامل‌پذیری[۴]
- سیاست‌های دولت در استفاده از IPv6[۵]
- سیاست‌های دولت در ارتباط با امنیت و محرمانگی[۶]
- سیاست‌های دولت در استفاده از رایانش سبز[۷]
- سیاست‌های دولت در استفاده از نرم‌افزارهای متن‌باز[۸]

---

[۳] Customization Development

[۴] Interoperability

[۵] Internet Protocol version 6

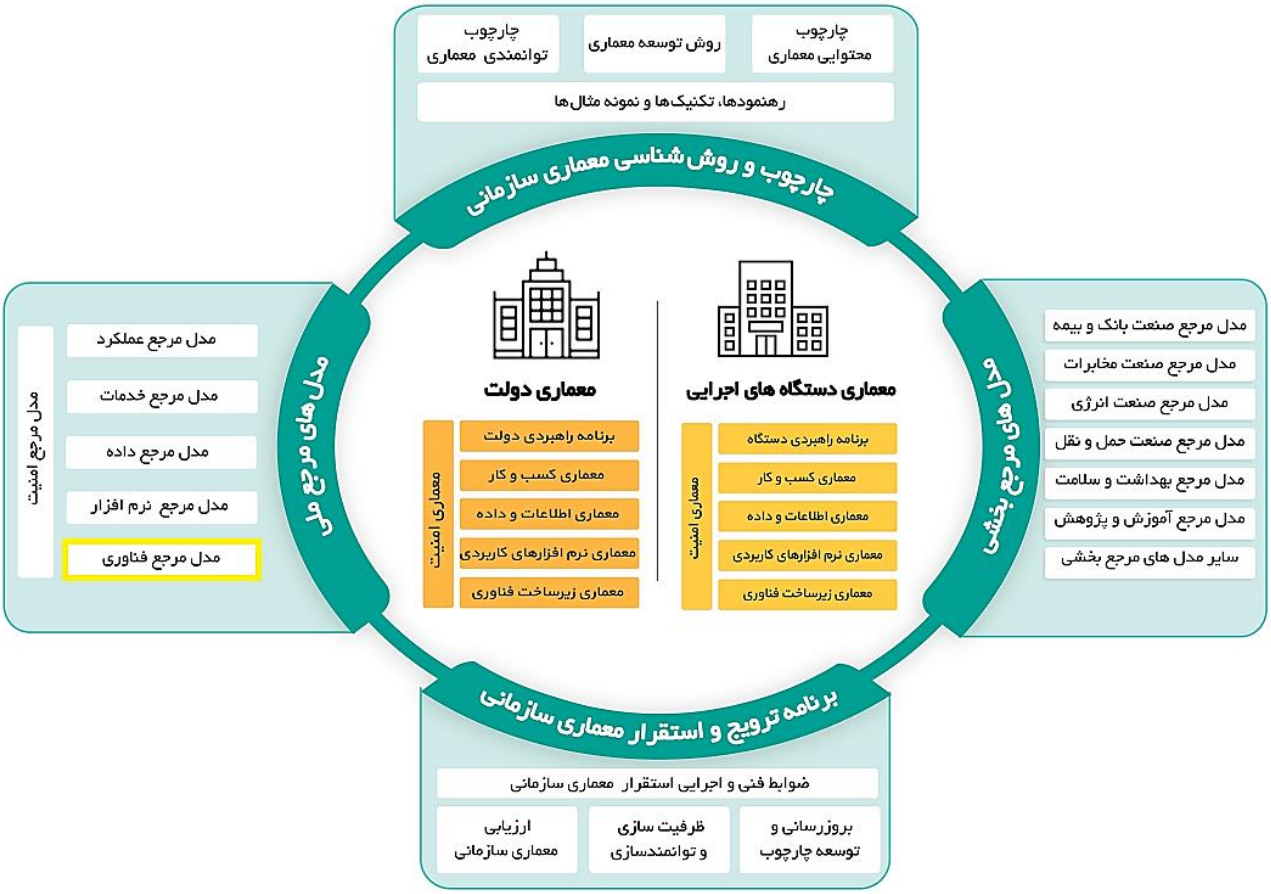
[۶] Security and Privacy

[۷] Green Computing

دستورالعمل‌ها، شاخص‌ها و روش‌هایی که برای تحقق هر یک از این سیاست‌های فوق توسط دستگاه‌های متولی در سطح دولت تهیه شده است باید در فرایند استفاده از مدل مرجع فناوری در نظر گرفته شود.

۱-۴ جایگاه مدل در چارچوب معماری سازمانی ایران

چارچوب معماری سازمانی ایران شامل چهار مولفه(جزء) اصلی "چارچوب و متدولوژی"، "مدل‌های مرجع ملی"، "مدل‌های مرجع بخشی" و "برنامه ترویج و استقرار" می‌شود که در شکل ۱-۱ نشان داده شده است. همانطور که در مشخص است مدل مرجع فناوری که در این گزارش به صورت تفصیلی تشریح می‌شود، یکی از شش مدل مرجع از چارچوب معماری سازمانی ایران است.



شکل ۱-۱ جایگاه مدل مرجع فناوری در چارچوب معماری سازمانی ایران

[۸] Open Source

فصل دوم

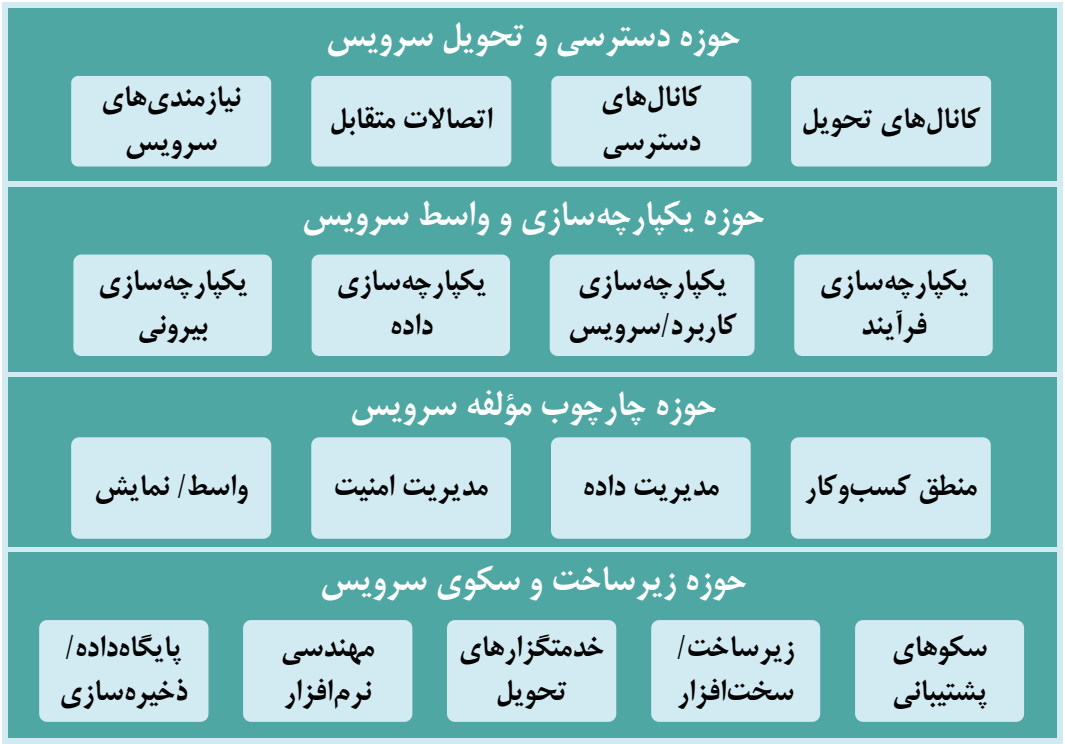
تشریح مدل مرجع فناوری

۲ تشریح مدل مرجع فناوری

مدل مرجع فناوری از یک ساختار سلسله‌مراتبی از حوزه فناوری، طبقه فناوری و استاندارد(فناوری) تشکیل شده است. این طبقه‌بندی شامل چهار حوزه و هفده طبقه است که سطح اول و دوم آن در شکل ۲-۱ مشخص شده است.

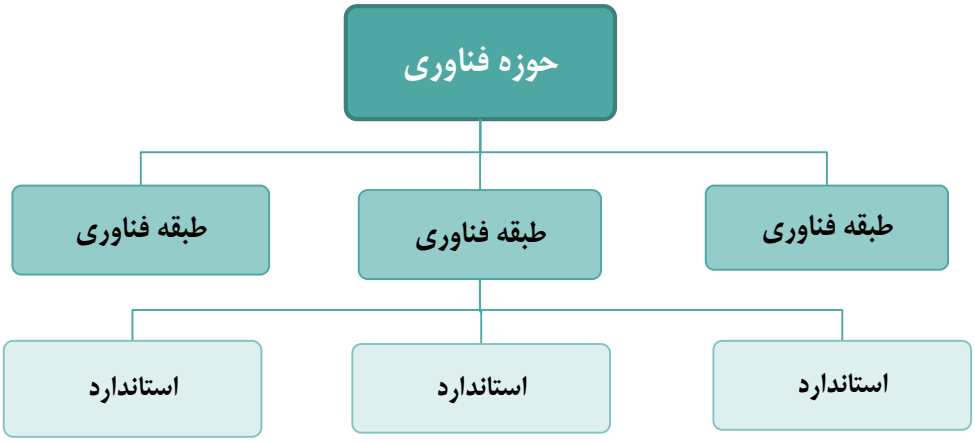
مدل مرجع فناوری، تصویر کلان معماری فناوری دولت را ترسیم می‌نماید تا در مرحله بعد هر دستگاه اجرایی جزئیات و نحوه پیاده‌سازی این نقشه کلان را در قالب جزئیات معماری سازمانی خود تدوین و پیاده‌سازی نماید. همچنین این مدل به توصیف همه گزینه‌ها و مصادیق قابل استفاده می‌پردازد و تصمیم‌گیری برای انتخاب نهایی فناوری یا استاندارد را به دستگاه‌های اجرایی و متولیان حوزه فناوری واگذار نموده است.

این مدل براساس چندین سال بررسی‌های تحلیلی نمونه مدل‌های مرجع معماری در دیگر کشورها و انطباق آن با نیازهای کشور طراحی و سفارشی‌سازی شده است.



شکل ۲-۱ حوزه‌های مدل مرجع فناوری

ساختار مدل مرجع فناوری در سه سطح حوزه فناوری، طبقه فناوری و استاندارد(فناوری) مطابق با شکل ۲-۲ تنظیم شده است.



شکل ۲-۲ ساختار مدل مرجع فناوری

حوزه فناوری: هر لایه از فناوری که از تحویل، تبادل و ساختِ امن سرویس‌ها پشتیبانی می‌کند توسط یک حوزه فناوری نمایش داده می‌شود. هر حوزه، فناوری‌ها و استانداردها را در طبقه‌های وظیفه‌مندی سطح پایین‌تر تجمیع می‌کند و شامل تعدادی طبقه فناوری و استاندارد است.

طبقه فناوری: فناوری‌ها و استانداردهای سطح پایین‌تر با توجه به نوع فناوری که ارائه می‌کنند در طبقه‌های فناوری دسته‌بندی می‌شوند. در حقیقت هر طبقه فناوری شامل یک یا چند استاندارد سرویس است.

استاندارد(فناوری): فناوری‌ها و استانداردهایی که از یک طبقه پشتیبانی می‌کنند را تعریف می‌کند. جهت پشتیبانی از نگاشت بهتر دستگاه‌ها به مدل مرجع فناوری برای هر استاندارد، مثال‌هایی نیز ارائه شده است.

۲-۱ حوزه دسترسی و تحویل سرویس

حوزه دسترسی و تحویل سرویس(Service Access and Delivery Area) شامل مجموعه‌ای از استانداردها، خصوصیات و نیازمندی‌های قانونی است که برای پشتیبانی از دسترسی بیرونی، تبادل و تحویل قابلیت‌ها و مؤلفه‌های سرویس مورد استفاده قرار می‌گیرند. طبقه‌ها و استانداردهای مربوط به این حوزه در ادامه معرفی شده است.

کانال‌های دسترسی(Access Channels)

کانال‌های دسترسی واسطهای بین برنامه‌های کاربردی و کاربران آنها را تعریف می‌کنند. یک مرورگر وب، تلفن هوشمند، تبلت یا هر رسانه دیگری می‌تواند نمونه‌ای از یک کانال دسترسی باشد.

جدول ۲-۱ مثال‌هایی از کانال‌های دسترسی

استانداردهای سرویس	مثال
مرورگر وب **(Web Browser)** مرورگر وب به نوعی نرم‌افزار کاربردی گفته می‌شود که برای دریافت، نمایش و مرور اطلاعات از وب جهان‌گستر مورد استفاده قرار می‌گیرد. هر منبع اطلاعاتی با یک شناسانه یکنواخت منبع شناخته می‌شود. منبع می‌تواند یک صفحه وب، تصویر، ویدئو یا هر نوع اطلاعاتی دیگری باشد. برای نمایش یک سایت در مرورگر وب کافی است که آدرس URL آن سایت در نوار آدرس مرورگر تایپ شود.	**مرورگر Microsoft Internet Explorer (IE)** تولید کننده: شرکت Microsoft هزینه: به همراه سیستم عامل ویندوز محاسبه می‌شود مجوز: پروانه اختصاصی و نیاز به مجوز سیستم عامل ویندوز دارد سیستم عامل: Windows, OS X
	مرورگر Mozilla Firefox تولید کننده: شرکت Mozilla هزینه: رایگان مجوز: MPL 2.0 سیستم عامل: Windows, OS X, Linux, BSD, Android, IOS
	مرورگر Google Chrome تولید کننده: شرکت Google هزینه: رایگان مجوز: Freeware سیستم عامل: Windows, OS X, Linux, Android, IOS
	مرورگر Apple Safari تولید کننده: شرکت Apple هزینه: رایگان مجوز: پروانه اختصاصی و تجاری، برخی از مؤلفه‌های آن مجوز GNU LGPL سیستم عامل: Windows, OS X, Linux, BSD, Android, IOS

استانداردهای سرویس	مثال
	مرورگر Opera تولید کننده: شرکت Opera Software هزینه: رایگان مجوز: Freeware سیستم عامل: Windows, OS X, Linux, BSD, Android, IOS
استانداردهای دسترسی وب **(Web Access Standards)** استانداردهای دسترسی وب جهت فراهم کردن دسترسی بیشتر به محتوای وب برای افرادی با انواع محدودیت‌ها (محدودیت در ابزارهای مورد استفاده مانند موبایل یا معلولیت‌هایی همچون نابینایی) مورد استفاده قرار می‌گیرند. وب‌گاه‌هایی که بر مبنای این استانداردها برپا شده باشند، برای همه کاربران با هرگونه توانمندی جسمی، به‌گونه‌ای یکسان در دسترس خواهند بود.	**استاندارد WCAG (Web Content Accessibility Guidelines)** استاندارد خطوط راهنمای دسترس‌پذیری وب (WCAG) توسط کنسرسیوم وب جهان‌گستر (W3C) ارئه شده است. آخرین نسخه این استاندارد WCAG 2.0 است. این نسخه بر پایه چهار اصل قرار گرفته است که به‌منظور فراهم کردن امکان دسترسی به محتوای وب ضروری است. همچنین این نسخه بر پایه دوازده خط راهنمای کلی قرار گرفته است که اصطلاحاً به آنها اهداف پایه گفته می‌شود که تهیه کننده محتوای وب باید آنها را رعایت نماید.
دستگاه‌های موبایل **(Mobile Devices)** دستگاه‌های محاسباتی هستند که برای انتقال اطلاعات از امواج رادیویی استفاده می‌کنند. این دستگاه‌ها اصطلاحاً توجیبی بوده و معمولاً دارای یک صفحه نمایش هستند. ورودی در این دستگاه‌ها به‌صورت لمسی بوده یا یک صفحه کلید کوچک برای این منظور در آنها تعبیه شده است.	**تلفن هوشمند (Smart Phone)** ویژگی‌ها و اتصالات بیشتری نسبت به موبایل‌های معمولی در اختیار کاربران قرار می‌دهد. این ویژگی‌ها می‌تواند استفاده از اینترنت و پخش موزیک باشد.
	تبلت (Tablet) کامپیوترهای شخصی قابل حملی بوده که ورودی اصلی آنها به‌صورت لمسی است.
	دستگاه ناوبری سامانه موقعیت‌یابی جهانی (GPS) دستگاهی که با گرفتن اطلاعات از ماهواره‌های GPS، موقعیت جغرافیایی را محاسبه می‌کند.
	پیجر (Pager) یک دستگاه گیرنده رادیویی کوچک است که امکان دریافت پیام، توام با دسترسی مداوم یک طرفه را برای کابر فراهم می‌کند.
	کامپیوتر پوشیدنی(Wearable Computer) کامپیوتری است که مانند یک ساعت هوشمند پوشیده می‌شود و در حوضه‌هایی مانند مدل کردن رفتار، سامانه‌های نظارت بر سلامت، فناوری اطلاعات و توسعه رسانه کاربرد دارد. سازمان‌های دولتی و نظامی و بخش بهداشت هم‌اکنون به طور روزمره از این کامپیوترهای پوشیدنی استفاده می‌کنند.
	دستیار دیجیتالی شخصی (Personal Digital Assistant)

استانداردهای سرویس	مثال
	دستگاه کوچک قابل حمل شخصی است که دارای سیستم‌عامل است. تقویم، دفتر آدرس الکترونیکی شخصی، ماشین حساب، ارتباط با اینترنت، دوربین عکاسی و سامانه موقعیت‌یابی جهانی (GPS) از جمله امکانات این دستگاه است.
	دستگاه‌های BlackBerry نوعی از تلفن‌های هوشمند است که توسط کمپانی بِلَک‌بِری عرضه می‌شود.
همکاری/ ارتباطات **(Collaboration/Communications)** شامل انواع مختلفی از ارتباطات الکترونیکی است که برای تبادل پیام‌ها، مستندات و اطلاعات به‌کار گرفته می‌شوند. استفاده از این ارتباطات الکترونیکی سرعت تحویل اطلاعات را افزایش داده و در نتیجه سبب بهبود کارایی می‌شود.	**سرویس‌های شبکه‌های اجتماعی (Social Networking Services)** سرویس‌هایی همچون Facebook, Twitter و YouTube که برای ساخت گروه‌های اجتماعی برخط استفاده می‌شوند. در این گروه‌ها، محتویات بر اساس علاقه‌ها و روابط به اشتراک‌گذاشته شده تبادل می‌شود.
	نرم‌افزارهای Groupware نرم افزارهایی هستند که به گروهی از کاربران کمک می کنند تا در امور و فعالیتهای مشترک و مورد علاقه خود فعالیت کنند. این نرم افزارها بیشتر در وب‌گاه‌ها و پایگاه‌های مبتنی بر شبکه های اجتماعی استفاده می شوند.
	سرویس پیام کوتاه (Short Message Services (SMS)) شامل سرویس ارتباط متنی مربوط به تلفن، وب یا سیستم‌های ارتباطی سیار هستند که از پروتکل‌های استاندارد برای تبادل پیام‌های کوتاه بین خطوط ثابت یا سیار استفاده می‌کنند.
	سیستم تلفن گویا (Interactive Voice Response((IVR)) به سیستم هایی اطلاق می‌شود که با گرفتن یک شماره، یک قطعه ضبط‌شده صوتی فعال شده و از شنونده می‌خواهد با استفاده از صفحه کلید تلفن خود، عدد یا کاراکتری (مثل # یا *) را وارد کرده تا داده‌ای در پایگاه‌داده درج شده یا داده‌ای از پایگاه داده برای شنوده خوانده شود.
	صدا روی پرتکل اینترنت (Voice over IP(VoIP)) به گروهی از فناوری‌ها گفته می‌شود که برای انتقال صدا و چندرسانه‌ای از شبکه‌های مبتنی بر پروتکل اینترنت استفاده می‌کنند. تلفنIP، تلفن اینترنتی، تلفن پهن‌باند، صدای پهن‌باند و صدا بر روی پهن‌باند از جمله مفاهیمی هستند که به VoIP مربوط می‌شوند.

استانداردهای سرویس	مثال
	تلویزیون اینترنتی (Internet Protocol Television (IPTV)) به فناوری گفته می‌شود که در آن با استفاده از پروتکل اینترنت (IP) بر روی یک زیرساخت شبکه با پهنای باند وسیع، برنامه‌های تلویزیونی به صورت دیجیتال ارائه می‌شود. خدمات تلویزیون اینترنتی فقط به خدمات ویدیویی محدود نمی‌شود و کاربران می‌توانند از موارد دیگری مانند دسترسی به وب و تلفن اینترنتی نیز استفاده کنند.
	پست الکترونیکی (Electronic Mail) روشی است که برای تبادل راه دور پیام‌های تولید شده یا ذخیره شده بر روی کامپیوتر مورد استفاده قرار می‌گیرد. پست الکترونیکی می‌تواند به‌صورت دستی توسط برنامه‌های کاربردی مختلف یا به‌صورت خودکار توسط سیستم‌های پاسخگوی خودکار تولید و ارسال شود.
	کیوسک (Kiosk) ساختار فیزیکی کوچکی است که شامل یک کامپیوتر و صفحه نمایش بوده و اطلاعات را به افراد نمایش می‌دهد. کیوسک‌ها معمولاً در مکان‌های عمومی به‌کار گرفته می‌شوند. همچنین از کیوسک‌ها در کنفرانس‌ها و نمایشگاه‌های تجاری نیز استفاده می‌شود.
فناوری مربوط به تلفن **(Telephony)** این فناوری مربوط به انتقال الکترونیکی صدا، فکس و سایر اطلاعات از طریق اتصال تلفن‌ها به یکدیگر است. این فناوری در حال حاضر به نرم‌افزارها، سخت‌افزارها و شبکه‌های کامپیوتری که کار تجهیزات قدیمی تلفن را انجام می‌دهند نیز اطلاق می‌شود. در این صورت فناوری‌هایی همچون VoIP را می‌توان در این طبقه در نظر گرفت.	**تلفن آنالوگ (Analogue Telephony)** سیستم آنالوگ، امواج و سیگنال‌ها را به شکل اولیه و کاملا ابتدایی ارسال و دریافت می‌کند. تلفن‌های آنالوگ نیز به دلیل پیروی از شرایط و ویژگی‌های این فناوری ارتباطی دارای قابلیت‌هایی محدود هستند.
	تلفن دیجیتال(Digital Telephony) سیستم دیجیتال سیگنال صوت را به اعداد صفر و یک تبدیل می‌کند. این سیستم قادر است هر خطایی که در هنگام ارسال و دریافت رخ می‌دهد را متوجه شده و اصلاح کند و این امر سبب بهبود وضوح صدا در تلفن‌های دیجیتال می‌شود.
سایر کانال‌های الکترونیکی **(Other Electronic Channels)** شامل سایر استانداردها و پروتکل‌هایی است که برای رسانه‌های تبادل اطلاعات و واسطهای بین برنامه‌های کاربردی و کاربران مورد استفاده قرار می‌گیرند.	**سیستم به سیستم (System to System)** شامل حداقل دو کامپیوتر که بدون دخالت انسان با یکدیگر تعامل داشته و داده‌ها را تبادل می‌کنند.
	سرویس‌های وب (Web Services) سرویس‌های وب (در برخی موارد سرویس‌های کاربردی هم نامیده می‌شوند) سرویس‌هایی هستند که از طریق خدمتگزاران وب در دسترس کاربران وب یا سایر برنامه‌های متصل به وب قرار می‌گیرند.
	آدرس یکسان منبع (Uniform Resource Identifier(URL)) URL آدرس سراسری اسناد و منابع در شبکه وب جهان‌گستر است.

استانداردهای سرویس	مثال
	قسمت اول این آدرس (http://) مشخص می‌کند از چه نوع پروتکلی استفاده شده است و قسمت دوم آدرس IP و دامنه‌ای که منبع در آن قرار دارد را توصیف می‌کند.

کانال‌های تحویل(Delivery Channels)

کانال‌های تحویل، نوع شبکه‌ای که برای تحویل سرویس‌ها مورد استفاده قرار می‌گیرد را تعریف می‌کند. بر این اساس سطح دسترسی به برنامه‌های کاربردی و سیستم‌ها مشخص می‌شود.

جدول ۲-۲ مثال‌هایی از کانال‌های تحویل

استانداردهای سرویس	مثال
اینترنت **(Internet)** اینترنت سامانه‌ای جهانی از شبکه‌های کامپیوتری به هم پیوسته است که کاربر هر کامپیوتر در آن اگر مجوز داشته باشد می‌تواند از اطلاعات سایر کامپیوترهای متصل به آن استفاده کند.	
اینترانت **(Intranet)** شبکه‌ای خصوصی است که از پروتکل‌های مرتبط با اینترنت برای سازماندهی شبکه استفاده می‌کند. در حقیقت اینترانت مقیاس بسیار کوچکی از کل اینترنت است که بر خلاف اینترنت که هیچکس مالک آن نیست، یک شبکه خصوصی است. این شبکه از اتصال تعداد زیادی از شبکه‌های محلی شکل گرفته و منابع و اطلاعات یک سازمان را بین کارمندان آنها به اشتراک می‌گذارد.	
اکسترانت **(Extranet)** اکسترانت یک اینترانت است که به طور کاملاً خصوصی اداره می شود. اکسترانت‌ها برای اینکه بتوانند اینترانت را گسترش دهند به کاربران خود اجازه می دهند که به اینترنت نیز از راه‌های مطمئن دسترسی داشته باشند.	
نقطه به نقطه **(Peer-to-Peer(P2P))** در شبکه‌های نقطه به نقطه کلاسی از برنامه‌های کاربردی وجود دارند که بدون استفاده از سرویس نام دامنه (DNS) عمل می‌کنند و خودمختاری کامل یا مهمی نسبت به خدمتگزارهای مرکزی دارند. این برنامه‌های کاربردی از منابع موجود در اینترنت سود می‌برند. در شبکه های نقطه به نقطه کامپیوترها هیچ برتری نسبت به هم در ارائه خدمات ندارند، یا به‌عبارتی	

استانداردهای سرویس	مثال
امکانات و منابع خود را با یکدیگر به اشتراک می‌گذارند. در این شبکه‌ها، گره‌های پیوندی، منابع را در میان یکدیگر و بدون استفاده از یک سیستم مدیریت متمرکز تقسیم می‌کنند.	
شبکه خصوصی مجازی **(Virtual Private Network(VPN))** شبکه خصوصی مجازی به طور عمده برای ایجاد ارتباط بین شعبه‌های مختلف شرکت‌ها و یا فعالیت راه دور مورد استفاده قرار می‌گیرد. اطلاعات در این شبکه از طریق یک شبکه عمومی مانند اینترنت جابه‌جا می‌شود اما در عین حال با استفاده از الگوریتم‌های امنیتی این ارتباط اختصاصی باقی می‌ماند.	
شبکه ملی اطلاعات **(National Internet Network (NIN))** شبکه ملی اطلاعات، که با نام‌های دیگری مانند اینترنت ملی، اینترانت ملی ایران و شبکه ملی اینترنت نیز شناخته می‌شود، پروژه‌ای برای توسعه شبکه زیرساخت امن و پایدار ملی در ایران است. طبق تعریف مصوب در تبصره ۲ ماده ۴۶ قانون برنامه پنجم توسعه و مصوبه شورای عالی فضای مجازی "شبکه ملی اطلاعات کشور، شبکه‌ای مبتنی بر پروتکل اینترنت (IP) به همراه سوئیچ‌ها، مسیریاب‌ها و مراکز داده‌ای است به صورتی‌که درخواست‌های دسترسی داخلی و أخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به هیچ‌وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود."	
شبکه علمی کشور (شبکه ملی تحقیقات و آموزش) **(National Research and Education Network (NREN))** شبکه علمی کشور، شبکه‌ای مستقل است که کلیه دانشگاه‌ها و مراکز علمی و پژوهشی را به یکدیگر متصل کرده و امکان اتصال به سایر شبکه‌های علمی معتبر جهانی از جمله شبکه علمی اروپا را دارا می‌باشد. دانشگاه‌ها، حوزه‌های علمیه و مراکز علمی و پژوهشی دولتی و غیر دولتی مورد تأیید وزارت علوم تحقیقات و فناوری و وزارت بهداشت درمان و آموزش پزشکی، مشترکین این شبکه هستند. از تسهیلات این شبکه جستجوی منابع دانشگاهی و علمی پژوهشی است و کاربران می‌توانند از این طریق منابع مورد نیاز خود را جستجو کنند.	

استانداردهای سرویس	مثال
این شبکه اطلاعات مربوط به کتابخانه‌ها، دانشگاه‌ها، پروژه‌های تحقیقاتی در حال انجام، بانک‌های اطلاعاتی، پژوهشی و آماری کشور را در اختیار کاربران قرار می‌دهد.	

نیازمندی‌های سرویس (Service Requirements)

نیازمندی‌های سرویس، جنبه‌های ضروری یک برنامه کاربردی، سیستم یا سرویس را تعریف می‌کند. این نیازمندی‌ها می‌تواند شامل جنبه‌های قانونگذاری، کارایی و میزبانی باشد.

جدول ۲-۳ مثال‌هایی از نیازمندی‌های سرویس

استانداردهای سرویس	مثال
قانونگذاری/ پذیریش (Legislation/Compliance) پیش‌نیازهایی که از طرف دولت برای یک برنامه کاربردی، سیستم یا سرویس تعریف شده است.	**سیاست‌های متن‌باز (Open Source)** سیاست‌های مربوط به نرم‌افزارهای متن‌باز که از سوی دولت برای کلیه دستگاه‌های دولتی در نظر گرفته شده است.
	توسعه سفارشی و بومی نرم‌افزار (Customization development) سیاست‌های مربوط به توسعه سفارشی و بومی نرم‌افزارها که دستگاه‌های اجرایی برای توسعه نرم‌افزارها باید از آنها تبعیت کنند.
	سیاست‌های IPv6 مربوط به استراتژی در نظر گرفته شده برای انتقال به IPv6 می‌شود که در آن کلیه دستگاه‌های دولتی نیاز است که سیستم‌ها و تجهیزاتشان را به سمت استفاده از IPv6 انتقال دهند.
	سیاست‌های تعامل‌پذیری (Interoperability) مربوط به چارچوب تعامل‌پذیری به کارگرفته شده توسط دولت می‌شود. این چارچوب مربوط به تعامل‌پذیری در ابعاد اطلاعات، فرایندهای کسب‌وکار و فناوری است. این چارچوب اصول، استانداردها و متدولوژی‌های لازم جهت ارائه سرویس‌های یکپارچه را فراهم می‌کند. چارچوب تعامل‌پذیری خود شامل سه چارچوب تعامل‌پذیری اطلاعات، چارچوب تعامل‌پذیری فرایندهای کسب‌وکار و چارچوب تعامل‌پذیری فناوری می‌شود.
	سیاست‌های دسترسی به محتوی وب (Web Content Accessibility) مربوط به استفاده دولت از راهنمای دسترسی به محتوی وب (WCAG) جهت فراهم کردن دسترسی بیشتر به محتوای وب برای مردم با انواع محدودیت‌ها (محدودیت در ابزارهای مورد استفاده مانند موبایل یا انواع معلولیت) می‌شود که رعایت آنها در آماده سازی محتوای وب بسیار

استانداردهای سرویس	مثال
	مهم است.
	سیاست‌های امنیت (Security) مربوط به سیاست‌ها و رویه‌هایی می‌شود که داده‌ها را در مقابل دسترسی، استفاده، تغییر، کشف و تخریب غیرمجاز محافظت می‌کند.
	سیاست‌های محرمانگی (Privacy) مربوط به سیاست از استفاده از پروتکل‌هایی همچون P3P (Platform for Privacy Preferences Project) است که به کاربران اجازه می‌دهد در زمان استفاده از مرورگرها کنترل بیشتری بر روی اطلاعات شخصی خود داشته باشند.
شناسایی یگانه **(Single Sign-on (SSO))** روشی برای احراز هویت کاربران جهت دسترسی به برنامه‌های کامپیوتری یا وب‌گاه‌های امن است. در این روش از خدمتگزارهای مرکزی شناسایی یگانه استفاده می‌شود که در دسترس برنامه‌های کامپیوتری و وب‌گاه‌های مربوطه قرار می‌گیرند. با این روش کاربر فقط یک بار بر روی یک وب‌گاه رمزعبور خود را وارد کرده و بعد از آن به بقیه وب‌گاه‌هایی که از شناسایی یگانه استفاده می‌کنند دسترسی خواهد داشت و لازم نیست رمزعبور خود را بیش از یک بار وارد کند.	**شناسایی یگانه وب (Web SSO)** شناسایی یگانه وب برای امن کردن دسترسی در معماری‌های مبتنی بر وب طراحی شده است. با احراز هویت کاربر در شناسایی یگانه وب، کاربر به کلیه منابع وب که برای آن مجاز است دسترسی پیدا خواهد کرد.
	شناسایی یگانه سازمانی (Enterprise SSO) شناسایی یگانه سازمانی همانند شناسایی یگانه وب بوده با این تفاوت که برنامه‌های کاربردی غیر وبی سازمان را نیز پوشش می‌دهد. بر خلاف شناسایی یگانه وب این روش نیاز به توسعه بر روی ایستگاه‌های کاری دارد. اگر چه این روش برای همه برنامه‌های کاربردی به‌کار گرفته می‌شود ولی شناسایی یگانه وب به لطف قوانینی که دارد سطح امنیت بالاتری را نسبت به این روش فراهم می‌کند.
	شناسایی یگانه متحد (Federated SSO) شناسایی یگانه متحد مشابه شناسایی یگانه وب بوده ولی مفهوم گسترده‌تری دارد. معمولاً در این نوع شناسایی از پروتکل SOAP و زبان SAML استفاده شده و این امکان فراهم می‌شود که یک کاربر با توجه به نقشی که در یک سازمان دارد یک بار شناسایی شده و بدون شناسایی مجدد به تمام وب‌گاه‌های متحد شده و مطمئن دسترسی پیدا کند.
	شناسایی یگانه موبایل (Mobile SSO) شناسایی یگانه موبایل، کلیه وظایف شناسایی یگانه سازمانی، متحد و وب را برای دستگاه‌های موبایل فراهم کرده و دسترسی به برنامه‌های

استانداردهای سرویس	مثال
	کاربردی سیستم‌های اطلاعاتی سازمان از طریق دستگاه‌های موبایل را امن می‌کند.
میزبانی (Hosting) سرویسی است که قابلیت‌دسترسی به یک وب‌گاه یا برنامه‌کاربردی را فراهم و مدیریت می‌کند. این سرویس معمولاً بر اساس یک توافق سطح سرویس (SLA) ارائه می‌شود. میزبان معمولاً شامل یک خدمتگزار است که دارای پشتیبانی شبکه، برق پشتیبان، حافظه پشتیبان، تحمل‌پذیری خطا و متعادل نمودن بار ترافیکی است.	**میزبانی داخلی (Internal Hosting)** در این حالت میزبانی وب‌گاه‌ها یا برنامه‌های کاربردی در درون یک سازمان صورت می‌گیرد. سازمان مسئول نگهداری، پشتیبانی و قابلیت‌دسترسی وب‌گاه و برنامه‌کاربردی خواهد بود.
	میزبانی خارجی (External Hosting) در این حالت یک وب‌گاه یا برنامه‌کاربردی به یک فراهم کننده سرویس مدیریت‌شده برون‌سپاری می‌شود. ISPها و ASPها نمونه‌هایی از میزبان خارجی هستند. Internet Service Provider (ISP) یا فراهم‌کننده سرویس اینترنت، امکان میزبانی وب‌گاه‌ها و برنامه‌های کاربردی را فراهم می‌کند. Application Service Provider (ASP) یا فراهم‌کننده سرویس کاربردی، سرویس‌های نرم‌افزاری را بر روی شبکه ارائه می‌کند.

اتصالات متقابل(Interconnections)

اتصالات متقابل شامل مجموعه‌ای از پروتکل‌های ارتباطی است که بر روی شبکه‌های کامپیوتری و اینترنت مورد استفاده قرار می‌گیرند. این پروتکل‌ها در سه لایه کاربرد، انتقال و اینترنت دسته‌بندی شده و قالب و ساختار داده‌ها و اطلاعاتی که از طریق دایرکتوری‌ها در دسترس قرار می‌گیرند یا از طریق ارتباطات مبادله می‌شوند را تعریف می‌کند.

جدول ۲-٤ مثال‌هایی از پروتکل‌های ارتباطی جهت برقراری اتصالات متقابل

استانداردهای سرویس	مثال
پروتکل‌های لایه کاربرد **(Application Layer Protocol)** پروتکل‌های لایه کاربرد در مدلTCP/IP، شامل تمام پروتکل‌هایی است که در حوزه ارتباطات پردازش–به–پرداش در سرتاسر شبکه پروتکل اینترنت (IP) قرار می‌گیرند. پروتکل‌های لایه کاربرد تنها ارتباطات را استانداردسازی کرده و برای برقراری ارتباطات میزبان به میزبان از پروتکل‌های لایه انتقال بهره می‌برند. این پروتکل‌ها چگونگی کاربردها را تعریف نمی‌کنند بلکه سرویس‌هایی را که کاربردها به آنها نیاز دارند معرفی می‌کنند. در مدلOSI، دو لایه نشست و لایه نمایش بین لایه کاربرد و لایه انتقال قرار دارد و پروتکل‌های لایه کاربرد در این مدل عملیات بیشتری نسبت به پروتکل‌های لایه کاربرد در مدل TCP/IP را باید در نظر بگیرند.	**پروتکل DNS (Domain Names System)** سیستم DNS یک سیستم سلسله‌مراتبی نام‌گذاری است که برای کامپیوترها، سرویس‌ها یا هر منبع دیگری که به شبکه اینترنت یا یک شبکه محلی متصل است استفاده می‌شود. برای وارد شدن به یک وبگاه باید آدرس IP را بدانیم. به خاطر سپردن آدرس IP دشوار است. می‌توان به جای آدرس IP، از نام‌های دامنه استفاده کرد. برای هر آدرس IP یک نام دامنه در نظر گرفته می‌شود. مثلاً آدرس IP وبگاه گوگل 173.194.33.104 است. با استفاده از سیستم DNS برای دسترسی به گوگل، می‌توان از نام دامنه آن یعنی www.google.com استفاده کرد. **پروتکل DHCP (Dynamic Host Configuration Protocol)** پروتکلی است که برای اختصاص پویای آدرس‌های IP به دستگاه‌ها بر روی شبکه مورد استفاده قرار می‌گیرد. هر دستگاه می‌تواند برای اتصالات مختلف به شبکه، آدرس‌های مختلفی دریافت کند. با استفاده از این پروتکل، حجم کار مدیریت سیستم به شدت کاهش یافته و دستگاه‌ها می‌توانند با حداقل تنظیمات و یا بدون تنظیمات دستی به شبکه متصل شوند. **پروتکل FTP (File Transfer Protocol)** پروتکلی است که برای انتقال فایل‌ها بر روی شبکه‌های TCP/IP مورد استفاده قرار می‌گیرد. به‌عنوان مثال صفحات HTML را با استفاده از پروتکل FTP بر روی خدمتگزارهای مورد نظر بارگذاری می‌کنیم. پروتکل FTPS نیز در اصل همان پروتکل FTP با گواهینامه SSL است که در آن برای کنترل کانال و باز کردن یک ارتباط امن برای انتقال اطلاعات نیاز به یک گواهینامه SSL خواهد بود. **پروتکل SFTP (Secure File Transfer Protocol)** برخلاف پروتکل FTP در پروتکل SFTP دستورات و اطلاعات رمزنگاری می‌شوند. با این پروتکل از آشکار شدن رمزهای عبور و اطلاعات حساس بر روی شبکه جلوگیری می‌شود. **پروتکل HTTP (Hyper Text Transfer Protocol)** پروتکل HTTP به پروتکلی گفته می‌شود که برای ایجاد ارتباط، دریافت، و ارسال داده ها بین خدمتگزار و مشتری استفاده می‌شود. این پروتکل از پروتکل TCP/IP برای ایجاد پلی بین خدمتگزار و مشتری

استانداردهای سرویس	مثال
	استفاده می‌کند. طریقه کار ارتباط مشتری با خدمتگزار، با استفاده از پروتکل HTTP به این ترتیب است که داده‌ها، از طریق بسته‌های اطلاعاتی، بین خدمتگزار و مشتری رد و بدل می‌شود. به این ترتیب که برای ارسال داده‌ای به سمت مقصد، در ابتدا، داده، به بخش‌های کوچکتری شکسته می‌شود و سپس از هر کدام به سمت مقصد و با ترتیب مشخص ارسال می شوند. لازم به ذکر است که پروتکل TCP/IPکه در پروتکل HTTP مورد استفاده قرار می‌گیرد، امنیت داده‌ها و تضمین ارسال آنها را به عهده گرفته است.
	پروتکلHTTPS (Hyper Text Transfer Protocol Secure) برای دسترسی امن به خدمتگزار وب مورد استفاده قرار می‌گیرد. قرار دادن HTTPS به‌جای HTTP در آدرس URL سبب می‌شود که پیام‌ها به یک شماره پورت امن به‌جای شماره پورت پیش‌فرض وب که ۸۰ است هدایت شوند. پس از آن نشست با استفاده از یک پروتکل امنیتی مدیریت می‌شود.
	پروتکل‌های سرویس پست الکترونیکی IMAP و POP3 در پروتکل POP3 (Post Office Protocol) پست‌های الکترونیکی از خدمتگزار پست الکترونیکی به روی کامپیوتر کاربر به‌طور کامل دانلود شده و پس از آن کاربر به مطالعه آنها می پردازد. به‌عبارتی یک فناوری غیربرخط به حساب می‌آید. پروتکل IMAP (Internet Message Access Protocol) یکی از پروتکل‌های لایه کاربرد در مدل TCP/IP است که امکان دریافت پست الکترونیکی از خدمتگزار را فراهم می‌کند. این پروتکل به کاربران پست الکترونیکی اجازه می دهد به پست‌های موجود در یک خدمتگزار پست الکترونیکی راه دور دسترسی داشته باشند. IMAP نسخه‌های پست الکترونیکی را در برنامه پست الکترونیکی مشتری نگهداری نمی‌کند، و برخلاف شیوه عملکرد پروتکلPOP، نسخه‌های موجود در خدمتگزار هستند که به‌عنوان نسخه‌های اصلی شناخته می‌شوند. پروتکل IMAP تنها اقدام به نمایش پست‌ها به کاربران در سطح شبکه می‌کند. زمانی که درخواست مشاهده پست الکترونیکی می‌شود، فایل‌ها مستقیماً از روی بانک اطلاعاتی خدمتگزار پست الکترونیکی نشان داده می‌شود. IMAP همچنین امکاناتی را جهت همگامی با خدمتگزار برای کاربران غیربرخط فراهم می‌کند.
	پروتکلIRC (Internet Relay Chat) پروتکلی برای چت و برگزاری کنفراس‌های اینترنتی است. پروتکل IRCبرای گفتگوهای گروهی طراحی شده و گفتگوها به‌صورت عمومی در محل‌هایی به نام کانال انجام می‌گیرد، علاوه بر بحث‌های گروهی

استانداردهای سرویس	مثال
	و برگزاری کنفراس، از این پروتکل برای ارتباط خصوصی (دو نفره) و انتقال اطلاعات نیز می‌توان بهره گرفت.
	پروتکل LDAP (Lightweight Directory Access Protocol) پروتکلی است که برای دسترسی و به‌روزرسانی فهرست‌های (دایرکتوری‌های) توزیع‌شده مورد استفاده قرار می‌گیرد. این پروتکل مجموعه‌ای از پروتکل‌ها و روش‌ها، برای دسترسی به اطلاعات شاخه‌های توزیع‌شده است. پروتکل LDAP از استانداردهای موجود در X.500 پیروی می‌کند و بر خلاف X.500 از TCP/IP پشتیبانی می‌کند که برای استفاده از اینترنت مفید است. پروتکل LDAP سبک‌تر از X.500است و به همین دلیل گاهی به آن X.500 Lite نیز گفته می‌شود. این پروتکل در سال ۱۹۹۰ توسط کارگروه مهندسی اینترنت (IETF) عرضه شد، تا پیاده سازی X.500 در پست الکترونیکی را آسان نماید.
	پروتکل MIME (Multipurpose Internet Mail Extensions) پروتکل MIME برای ارسال داده‌های چندرسانه‌ای از قبیل تصویر و صدا یا دیگر قالب‌های غیرآسکی به کار می‌رود. به‌منظور ارسال این گونه داده‌ها، عامل کاربر باید شامل سرآیندهای اضافی باشد.
	پروتکل SMTP (Simple Mail Transfer Protocol) پروتکلی ساده و در عین حال مهم و اساسی برای انتقال پست الکترونیکی است. این اصطلاح از آن رو به کار می‌رود که نسبت به سایر پروتکل‌های پست االکترونیکی قبلی بسیار ساده عمل می‌کند. پروتکل SMTP فقط به نام کاربری و دامنه نیاز دارد تا مستقیم پیغام را به سمت گیرنده مسیریابی کند. پروتکل SMTP یک پروتکل ارسال است و برای دریافت مناسب نیست، به همین دلیل برای دریافت پست‌های الکترونیکی به‌جای SMTP از پروتکل‌های دریافت مثل IMAP و POP3 استفاده می‌شود. پروتکل ESMTP این اجازه را می‌دهد که سرویس‌های توسعه‌ای بر روی پروتکل SMTP تعریف و ثبت شود.
	پروتکل SNMP (Simple Network Management Protocol) این پروتکل امکان نقل و انتقال اطلاعات مدیریتی را بین عناصر شبکه ایجاد می‌کند. این پروتکل توانایی مدیریت و پیدا کردن مشکلات و حل آنها را در شبکه برای مدیران مهیا می‌کند. مشکل بزرگی که در نسخه های ۱ و۲ این پروتکل وجود دارد این است که اطلاعات بر روی بستر غیر رمز شده ارسال می شود که این نکته برای شبکه‌ای که حساسیت اطلاعات آن بالاست، بسیار خطرناک است. در نسخه ۳

استانداردهای سرویس	مثال
	تمرکز بر روی حل آسیب‌پذیری‌های نسخه‌های قبلی بوده است. لذا قابلیت‌های امنیتی به آن افزوده شده است.
	پروتکل RIP (Routing Information Protocol) یکی از قدیمی‌ترین پروتکل‌های مسیریابی در شبکه است که در شبکه‌های کوچک به خوبی کار می‌کند. این پروتکل برای شبکه‌های بزرگ با تعداد بسیار زیادی مسیریاب مناسب نمی‌باشد.
	پروتکل BGP (Border Gateway Protocol) پروتکل مسیریابی که برای تبادل اطلاعات مسیریابی مربوط به مسیریاب‌های مختلف بر روی یک شبکه به کار می‌رود و سبب بهبود کارایی مسیریابی داده‌ها بر روی شبکه می‌شود. این پروتکل بخشی از پروتکل RFC 1771 است. این پروتکل برای ردوبدل کردن پیام‌های خود بین مسیریاب‌ها از یک اتصال قابل اعتماد بهره می‌برد و برای این کار از پروتکل TCP و پورت ۱۷۹ استفاده می‌کند.
	پروتکل OSPF (Open Shortest Path First) یک پروتکل مسیریابی دروازه داخلی (IGP) است واطلاعات مسیریابی را تنها بین مسیریاب‌های متعلق به یک سیستم خودمختار (AS) توزیع می‌کند. این پروتکل استاندارد باز بوده و توسط مجموعه‌ای از تولیدکنندگان شبکه از جمله شرکت سیسکو ایجاد شده است. در این پروتکل از الگوریتم دایجسترا برای پیداکردن کوتاه‌ترین مسیر استفاده شده است.
	پروتکل SSH (Secure Shell) یک پروتکل اینترنتی است که امکان تبادل اطلاعات با استفاده از یک کانال امن را بین دو دستگاه متصل در شبکه ایجاد می‌کند.
	پروتکل Telnet یکی از پروتکل‌های شبکه است که در اتصالات اینترنت و شبکه‌های محلی مورد استفاده قرار می‌گیرد. از Telnet برای مکالمه دو سیستم با هم استفاده می‌شود. این پروتکل یکی از قدیمی‌ترین استانداردهای شبکه است و پیدایش آن به سال ۱۹۶۹ باز می‌گردد.
	پروتکل Directory Services (X.500) یک سرویس شبکه است که وظیفه ذخیره‌سازی و سازمان‌دهی اطلاعات مربوط به کاربران و منابع یک شبکه را به عهده داشته و به مدیر شبکه این امکان را می‌دهد که دسترسی کاربران به منابع شبکه را مدیریت نماید. در عین حال به‌عنوان یک لایه محافظ بین کاربران و منابع مشترک شبکه عمل می‌کند. با استفاده از این سرویس کاربر نیاز ندارد تا آدرس فیزیکی منابع شبکه را به خاطر بسپارد، چرا که تنها نام

استانداردهای سرویس	مثال
	منبع کافی است تا محل آن مشخص شود.
	پروتکل X.400 استاندارد ISO و IUT برای آدرس‌دهی و انتقال پست‌های الکترونیکی است. این استاندارد از روش‌های انتقال در TCP/IP، dial-up، Ethernet و X.25 پشتیبانی می‌کند.
	پروتکل WAP (Wireless Application Protocol) پروتکلی است که به کاربران دستگاه‌های بی‌سیم این امکان را می‌دهد که به‌صورت امن به محتوا، برنامه‌های کاربردی و سرویس‌های موجود در اینترنت، اینترانت یا اکسترانت دسترسی پیدا کرده و با آن تعامل داشته باشد. مرجع استاندارد WAP اتحادیه استانداردهای باز موبایل (OMA) است.
	پروتکل SIP (Session Initiation Protocol) SIP یک پروتکل نشانه‌گذاری است که توسط کارگروه مهندسی اینترنت (IETF) استاندارد شده است. از این پروتکل می‌توان برای کنترل جلسات ارتباطی مانند تماس‌های صوتی و تصویری بر روی بستر IP استفاده کرد. این پروتکل می‌تواند جلسات دونفره و چندنفره را ایجاد و اصلاح کرده و آنها را به اتمام برساند.
	پروتکل SOAP (Wireless Application Protocol) پروتکل SOAP (دسترسی آسان به اشیاء) پروتکلی است که برای تبادل پیغام‌های مبتنی بر XML در میان شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرد. این پروتکل برای انتقال پیام‌ها اغلب از پروتکل HTTP و SMTP استفاده می‌کند. به‌عبارت دیگر، SOAP فراخوانی رویه راه دور (RPC) مبتنی بر HTTP/XML را برای وب‌سرویس‌ها فراهم می‌کند.
	پروتکل H.323 این پروتکل مجموعه‌ای از پروتکلها است و به‌عنوان استاندارد رسانه‌ای سازمان بین المللی ارتباطات (ITU) برای انتقال صدا و تصویر از طریق پروتکل اینترنت استفاده می‌شود. این استاندارد چندین پروتکل از جمله Q.931 برای سیگنالینگ، H.245 برای تبادل پیام و RAS12 برای کنترل نشست‌ها را ترکیب می‌کند. H.323 اولین استاندارد در آدرس‌دهی کنترل تماس‌ها در VoIP است که تمامی دروازه‌های صدای شرکت سیسکو از آن پشتیبانی می‌کنند.

استانداردهای سرویس	مثال
پروتکل‌های لایه انتقال **(Transport Layer Protocol)** پروتکل‌های انتقال، سرویس‌های ارتباطی میزبان به میزبان را برای برنامه‌های کاربردی فراهم می‌کند. این سرویس‌ها شامل پشتیبانی از جریان داده اتصال‌گرا، قابلیت اطمینان، کنترل جریان و تسهیم‌سازی است.	**پروتکل TCP (Transmission Control Protocol)** مهمترین وظیفه پروتکل TCP اطمینان از صحت ارسال اطلاعات است این پروتکل اصطلاحاً اتصال‌گرا نامیده می شود. علت این امر ایجاد یک ارتباط مجازی بین کامپیوترهای فرستنده و گیرنده بعد از ارسال اطلاعات است. پروتکل‌هایی از این نوع، امکانات بیشتری را به‌منظور کنترل خطاهای احتمالی در ارسال اطلاعات فراهم نموده ولی بدلیل افزایش بار عملیاتی سیستم کارایی آنان کاهش خواهد یافت. از پروتکلTCP به‌عنوان یک پروتکل قابل اطمینان نیز یاد می‌شود. در صورتی‌که بسته‌های اطلاعاتی به‌درستی دراختیار گیرنده قرار نگیرند، فرستنده مجدداً اقدام به ارسال اطلاعات می‌نماید.
	پروتکل UDP (User Datagram Protocol) پروتکل UDP بر خلاف پروتکل TCP به‌صورت بدون اتصال است. بدیهی است که سرعت پروتکل فوق نسبت به TCP سریعتر بوده ولی از نظر کنترل خطا امکانات لازم را ارائه نخواهد داد. بهترین جایگاه استفاده از پروتکل فوق در مواردی است که برای ارسال و دریافت اطلاعات به سطح بالایی از اطمینان نیاز نداشته باشیم.
	پروتکل DCCP (Datagram Congestion Control Protocol) کار پروتکل DCCP کنترل ازدحام دیتاگرام است.
	پروتکلSCTP (Stream Control Transmission Protocol) پروتکل SCTP ترکیبی از ویژگی‌های پروتکل‌های TCPوUDP را ارائه می‌دهد. همانند UDP پیام‌گرا است و مانند TCP انتقال به ترتیب پیام‌ها وکنترل ازدحام را تضمین می‌کند.
	پروتکلRSVP (Resource Reservation Protocol) پروتکل RSVP به‌عنوان یک پروتکل سیگنالینگ برای رزرو منابع در اینترنت استفاده می شود.
پروتکل‌های لایه اینترنت **(Internet Layer Protocol)** لایه اینترنت مجموعه‌ای از متدها، پروتکل‌ها و مشخصاتی است که برای انتقال بسته ها از میزبان مبدأ تا میزبان مقصد به کار می‌رود. این عمل با استفاده از آدرس آی‌پی که توسط پروتکل اینترنت برای همین منظور تعریف شده است، انجام می‌شود. پروتکل‌های لایه اینترنت از بسته‌های مبتنی بر آی‌پی استفاده می‌کنند. لایه اینترنت شامل پروتکل‌هایی نیست که ارتباط بین نودهای شبکه محلی را تعریف می‌کنند. اینگونه پروتکل‌ها در لایه پیوند گنجانده شده‌اند.	**پروتکل اینترنت (Internet Protocol (IP))** پروتکل اینترنت مهمترین قراردادی است که برای مبادله اطلاعات در شبکه‌های اینترنتی وجود دارد. این قرارداد بنیادی‌ترین قرارداد شکل‌دهنده اینترنت است و وظیفه مسیردهی بسته‌های اطلاعاتی را در گذر از مرزهای شبکه‌ها به عهده دارد. پروتکل اینترنت. بسته‌ها را از TCP گرفته و سرآیندهای خود را به آن اضافه کرده و یک دیتاگرام به لایه پیوند تحویل می‌دهد. این پروتکل ممکن است بسته‌ها را برای پشتیبانی از حداکثر واحد انتقال (Maximum Transmission Unit (MTU)) تکه تکه کند. IPv4 چهارمین بازبینی پروتکل اینترنت و اولین نسخه‌ای است که به گستردگی به کارگرفته شد. نسخه ششم پروتکل

استانداردهای سرویس	مثال
	اینترنت (IPv6) که دارای فضای آدرس‌دهی بسیار بالایی است قرار است که جای نسخه چهارم پروتکل اینترنت را بگیرد.
	پروتکل IPSEC مجموعه‌ای از پروتکل‌ها که برای تبادل امن بسته‌های IP مورد استفاده قرار می‌گیرد. پروتکل IPSEC (IP SECURITY) از دو حالت تونل و انتقال پشتیبانی می‌کند و از گواهی‌نامه‌ها و کلیدهای عمومی برای احراز هویت و اعتبارسنجی فرستنده‌ها و گیرنده‌ها استفاده می‌کند.
	پروتکل (ICMP) پروتکل ICMP(Internet Control Message Protocol) یکی از پروتکل‌های اصلی بسته پروتکل‌های اینترنت است. مهمترین کاربرد این پروتکل در سیستم‌عامل‌های کامپیوترهای متصل به شبکه، ارسال پیام‌های خطا است. در دسترس نبودن سرویس مورد درخواست و غیرفعال بودن میزبان یا مسیریاب نمونه‌ای از این پیام‌ها است . ICMP برای پروتکل اینترنت نسخه ۴ (IPv4) با نام ICMPv4 و برای پروتکل اینترنت نسخه ۶ با نام ICMPv6 شناخته می‌شود.
	پروتکل IGMP پروتکل IGMP (Internet Group Management Protocol)نام پروتکلی است که در لایه دوم مدل TCP/IP استفاده می‌شود. این پروتکل مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IPرا بر عهده دارد. فرآیند Multicasting یک پیام را برای گروهی انتخاب شده از گیرندگان که گروه multicast نامیده می‌شود ارسال می‌کند پروتکل IGMP لیست گیرندگان را نگهداری می‌کند.

۲-۲ حوزه یکپارچه‌سازی و واسط سرویس

حوزه یکپارچه‌سازی و واسط سرویس(Service Interface and Integration Area) شامل مجموعه‌ای از فناوری‌ها، متدولوژی‌ها، استانداردها و خصوصیاتی است که چگونگی اتصال داخلی و بیرونی به مؤلفه‌های سرویس را تعیین می‌کنند. این حوزه همچنین شامل روش‌هایی است که مؤلفه‌ها از طریق آنها به سایر سیستم‌های پشتیبان و کاربردی متصل می‌شوند.

یکپارچه‌سازی فرایند(Process Integration)

یکپارچه‌سازی فرایند شامل ابزارها، استانداردها، پروتکل‌ها و روش‌هایی است که در یکپارچه‌سازی فرایندهای کسب‌وکار مورد استفاده قرار می‌گیرند.

جدول ۲-۵ مثال‌هایی از ابزارها و استانداردهای یکپارچه‌سازی فرایند

استانداردهای سرویس	مثال
مدیریت فرایند کسب‌وکار (Business Process Management (BPM)) مدیریت فرایند کسب‌وکار شامل سطح گسترده‌ای از پیاده‌سازی وظایف مدیریت فرایندها است و می‌تواند همه جنبه‌های طراحی، پیاده‌سازی، نظارت و مدیریت فرایندهای کسب و کار (خودکار یا دستی) را در بر بگیرد. ابزارهای مدیریت فرایند کسب‌وکار می‌توانند شامل مدلسازی فرایندها، یکپارچه‌سازی گردش‌های کاری، یکپارچه‌سازی و اتوماسیون فرایندها، نظارت بلادرنگ فرایندها، داشبوردهای کسب‌وکار، تحلیل، اجرا و بهبود فرایندها باشند. بنابراین سازمان‌هایی که به دنبال داشبورد کسب‌وکار، مدیریت بهینه فرایندهای کسب‌وکار و بهبود مستمر فرایندهای کسب‌وکار هستند از این ابزارها استفاده می‌کنند.	**XPDL (XML Process Definition Language)** XPDL (زبان تعریف فرایند به‌صورت XML) یک فرمت استاندارد است که توسط کنسرسیوم WfMC در سال ۲۰۰۸ مطرح گردید و هدف آن فراهم نمودن امکان تبادل تعاریف فرایندهای کسب‌وکار بین محصولات ارائه‌دهنده گردش‌کار و همچنین دستگاه‌های مدیریت فرایندهای کسب‌وکار است. هدف XPDL ذخیره و انتقال فرآیند است. XPDL به یک ابزار طراح فرآیند اجازه می‌دهد تا فرآیند را در فایلی ذخیره نموده و طراح فرآیند دیگر آن را فراخوانی نماید و نمادهای مخصوص به خود را نمایش دهد.
	Wf – XML یکی از استانداردهای مربوط به مدیریت فرایند کسب‌وکار است که در یکپارچه‌سازی و اتصال گردش‌های کاری با هم به‌کار می‌رود. این استاندارد توسط کنسرسیوم WfMC توسعه یافته است.
	BPMN (Business Process Model & Notation) مجموعه‌ای از علائم، نشانه‌ها و شیوه‌ای استاندارد برای مدل‌سازی فرایندهای کسب‌وکار است و یکی از ابزارهای اصلی در مدیریت فرایندهای کسب‌وکار محسوب می‌شود. نسخه BPMN 2.0 در سال ۲۰۱۱ توسط گروه OMG ارائه شده است.
	BPEL (Business Process Execution Language) زبان WS-BPEL (Web Services BPEL) که عموماً به‌عنوان BPEL شناخته می‌شود، زبان اجرای فرایندهای کسب‌وکار است که جهت توصیف کنش‌ها در فرایندهای کسب‌وکار با استفاده از وب‌سرویس‌ها

استانداردهای سرویس	مثال
	مورد استفاده قرار می‌گیرد. به‌عبارت دیگر اطلاعات فرایندها در BPEL با استفاده از واسط وب‌سرویس‌ها صادر و وارد می‌گردد. زبان BPEL استاندارد سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) بوده و مبتنی بر XML است که سیستم مدیریت فرایندهای کسب‌وکار می‌تواند با آن فرایندها را اجرا کند. این استاندارد در همنواسازی سرویس‌های وب (Web Service Orchestration(WSO)) به کار می‌رود.
	(Business Activity Monitoring) BAM BAM (نظارت فعالیت کسب‌وکار) این امکان را به مدیریت فرایند کسب‌وکار می‌دهد که فرایندهای کسب‌وکار را نظارت کند، خطاها و موارد خاص پیش‌آمده در کسب‌وکار را شناسایی نموده و به‌صورت بلادرنگ از آنها گزارش‌گیری نماید.
نظارت فعالیت کسب و کار **(Business Activity Monitoring (BAM))** با استفاده از BAM (نظارت فعالیت کسب‌وکار) این امکان فراهم می‌شود که سازمان‌ها فرایندهای کسب‌وکارشان را نظارت کنند، خطاها و موارد خاص پیش‌آمده در کسب‌وکار را شناسایی نموده و به‌صورت بلادرنگ از آنها گزارش‌گیری نمایند. BAM نحوه اجرای فرایندها را پیگیری کرده و با تولید گزارشات مبنی بر موفق بودن یا نبودن فرایندها باعث مدیریت بهتر فعالیت‌های موجود می‌گردد، سوددهی تراکنش کسب‌وکار را ضمانت می‌کند و بروز خطر را تا حد امکان کاهش می‌دهد. در برخی از ابزارهای BAM از تحلیل‌های هوشمند بلادرنگ برای هشداردهی استفاده می‌شود و واکنش مناسب بدون دخالت انسانی صورت می‌گیرد. BAM می‌تواند به‌عنوان یکی از مؤلفه‌های مدیریت فرایند کسب‌وکار نیز مورد استفاده قرار گیرد.	
یکپارچه‌سازی فرایند کسب و کار **(Business Process Integration (BPI))** ابزارهای یکپارچه‌سازی فرایند کسب‌وکار توانایی طراحی، مدلسازی، یکپارچه‌سازی و نظارت فرایندها را دارند. در حقیقت این ابزارها یکپارچه‌سازی فرایندها بدون مدیریت بر روی آنها را فراهم می‌کنند. در این ابزارها امکانات تحلیل و شبیه‌سازی وجود ندارد. بنابراین این ابزارها در سازمان‌هایی که علاقه‌ای به مدیریت و بهبود فرایندها نیست و یکپارچه‌سازی سریع فرایندها مورد نیاز است مناسب هستند.	

استانداردهای سرویس	مثال
اتوماسیون فرایند کسب و کار **(Business Process Automation (BPA))** ابزارهای اتوماسیون فرایند کسب‌وکار تراکنش‌گرا بوده و نیازی به پشتیبانی از فرایندهای دستی ندارند. این ابزارهای معمولاً شامل مدلسازی فرایند، یکپارچه‌سازی فرایند و قوانین پردازشی هستند. ممکن است امکانات نظارت و مدیریت سطح عملیات نیز در این ابزارها در نظر گرفته شود. سازمان‌هایی که علاقه به فرایندهای تراکنش‌گرا بدون دخالت انسانی دارند می‌توانند از این ابزارها استفاده کنند.	
موتور گردش‌کاری **(Workflow Engine)** موتور گردش‌کاری یک سرویس نرم‌افزاری است که با ایجاد یک محیط زمان‌اجرا از مدیریت گردش‌کاری سازمان‌ها پشتیبانی می‌کند. یک سیستم گردش‌کاری یا ابزار اتوماسیون گردش‌کاری می‌تواند شامل چندین موتور گردش‌کاری باشد. موتور گردش‌کاری گردش اطلاعات، وظایف و رویدادها در سازمان را تسهیل کرده و با تعریف فرایندهای کسب‌وکاری که برنامه‌های کاربردی ارائه شده توسط تولیدکننده‌های مختلف را پوشش می‌دهد به یکپارچه‌سازی فرایندهای داخلی و بیرونی سازمان کمک می‌کند. برای این منظور معمولاً نیاز به داشتن محیط‌های توسعه گردش‌کاری استاندارد است. مدیریت گردش‌کاری را می‌توان بخشی از مدیریت فرایند کسب‌وکار محسوب کرد. به‌عبارت دیگر مدیریت فرایند کسب‌وکار یک ابرمجموعه برای مدیریت گردش‌کاری به‌شمار می‌آید و برای یکپارچه‌سازی فرایندها دارای قابلیت بیشتری است.	
موتور قوانین کسب‌وکار **(Business Rules Engine)** موتور قوانین کسب‌وکار از ابزارهای مناسب جهت مدیریت قوانین کسب‌وکار است. قوانین کسب‌وکار، پشتیبانی‌کننده سیاست‌ها و روش‌های خاص یک سازمان بوده و ساختار کسب‌وکار را مشخص می‌نمایند. این قوانین رفتار کسب‌وکار را تحت تاثیر و کنترل خود قرار می‌دهند. در صورتی‌که این قوانین به‌صورت صحیح مدیریت شوند، دستیابی به اهداف برای سازمان تسهیل شده، هزینه‌ها کاهش و نیازمندی‌های منطقی برآورده می‌شود. از مزایای استفاده از موتور قوانین کسب‌وکار می‌توان به‌مواردی نظیر افزایش چابکی، اثربخشی و	

استانداردهای سرویس	مثال
بهره‌وری، کیفیت تصمیمات اتخاذ شده، ثبات و شفافیت اشاره نمود. برای استفاده بهینه از موتور قوانین کسب‌وکار در یکپارچه‌سازی فرایندها نیاز است که موتور قوانین کسب‌وکار با سیستم‌هایی همچون سیستم مدیریت فرایندهای کسب‌وکار یا سیستم نظارت بر فعالیت‌های کسب‌وکار یکپارچه شود.	

یکپارچه‌سازی کاربرد/سرویس(Application/Service Integration)

یکپارچه‌سازی کاربرد/سرویس شامل میان‌افزارها، استانداردها و پروتکل‌هایی است که در یکپارچه‌سازی برنامه‌های کاربردی و سرویس‌ها مورد استفاده قرار می‌گیرند و بر روی انواع میان‌افزارهای یکپارچه‌سازی کاربردها/سرویس‌ها و روش‌های کشف و توصیف سرویس‌ها تمرکز دارند.

جدول ۲-٦ مثال‌هایی از ابزارها و استانداردهای یکپارچه‌سازی کاربرد/ سرویس

استانداردهای سرویس	مثال
میان‌افزار پیام‌گرا (Message Oriented Middleware (MOM)) در این میان‌افزار از پیام‌ها به‌عنوان انتزاع مرکزی استفاده می‌شود و فرستنده‌ها و گیرنده‌ها می‌توانند با تبادل پیام به‌صورت غیرمستقیم و ناهمگام با یکدیگر ارتباط برقرار کنند. پیامِ یک فرستنده می‌تواند توسط یک یا چند گیرنده دریافت شود. در سیستم تبادل پیام الگوی‌های صف‌بندی (Queuing) و ناشر–متقاضی (Publish-subscribe) به‌کار گرفته می‌شود. برای میان‌افزار پیام‌گرا پیاده‌سازی‌های مختلفی توسط شرکت‌های مختلف ارائه شده است.	**(Advanced Message Queuing Protocol) AMQP** پروتکل AMQP یک پروتکل استاندارد باز برای لایه کاربرد است که در میان‌افزارهای پیام‌گرا مورد استفاده قرار می‌گیرد. از ویژگی‌های بارز این پروتکل می‌توان به پیام‌گرا بودن، صف‌بندی، مسیریابی (نقطه به نقطه یا ناشر–متقاضی)، قابلیت اطمینان و امنیت نام برد. برای ایجاد ارتباط بین دو فناوری (دو سیستم عامل مختلف یا دو نرم افزار مختلف)، ایجاد ارتباط بین دو سیستم که به‌صورت همزمان در دسترس نیستند، صف‌بندی و مدیریت پیام‌های ارتباطی بین سیستم‌ها و کاهش بار ترافیک پایگاه‌داده‌ها می‌توان از این پروتکل استفاده نمود. این پروتکل توسط نرم‌افزارهای متن‌بازی همچون Rabbit MQ پیاده‌سازی شده است.
	(MQ Telemetry Transport) MQTT پروتکل MQTT به معنای انتقال پیام از طریق دورسنجی (Telemetry) و صف‌بندی است. این پروتکل استاندارد ISO بوده و به‌صورت یک انتقال پیام ناشر–متقاضی بسیار سبک‌وزن، طراحی‌شده است. MQTT برای اتصال به موقعیت‌های مکانی دوردستی که به حافظه کمی نیاز دارد یا پهنای باند شبکه در آنها بسیار ارزشمند است، مؤثر و سودمند است. در حقیقت این پروتکل یک پروتکل اتصال اینترنت اشیا/ماشین به ماشین (M2M) است.
	(eXtensible Messaging and Presence Protocol) XMPP پروتکل XMPP (پروتکل پیام‌رسانی و حضور گسترش‌پذیر) یک پروتکل ارتباطی مبتنی بر XML برای میان‌افزارهای پیام‌گرا است. این

استانداردهای سرویس	مثال
	پروتکل توسط انجمن متن‌باز Jabber برای پیام‌دهی نزدیک به بلادرنگ (Near-real-time) ، اطلاعات حضور (Presence information) و فهرست تماس‌ها (Contact list) توسعه داده شده است. از این پروتکل در سیستم‌های چت گروهی، تماس‌های صوتی و تصویری استفاده می‌شود.
	JMS (Java Message Service) JMS یک API برای میان‌افزارهای پیام‌گرا است که محیط برنامه‌سازی Java EE آن را فراهم کرده است. این API این امکان را فراهم می‌کند که مؤلفه‌های برنامه‌های کاربردی توزیع‌شده به‌صورت ناهمگام، قابل اعتماد و امن ارتباط برقرار کنند. JMS قالب پیام‌هایی که باید مبادله شوند را مشخص نمی‌کند. بنابراین سطح تعامل‌پذیری بالایی ندارد.
	IBM MQ MQ یک میان‌افزارهای پیام‌گرا است که توسط شرکت IBM برای یکپارچه‌سازی برنامه‌های کاربردی توزیع‌شده بر روی سکوهای مختلف ارائه شده است. MQ از صف‌بندی پیام استفاده می‌کند. و اجازه می‌دهد که برنامه‌های کاربردی توزیع‌شده به‌صورت امن با یکدیگر ارتباط برقرار کنند.
	MSMQ (Microsoft Message Queue) MSMQ یک پیاده‌سازی از صف‌بندی پیام است که توسط شرکت Microsoft توسعه داده شده است و بر روی سیستم‌عامل‌های ویندوز مستقر شده است.
میان‌افزار داده–محور **(Data-Centric Middleware)** در میان‌افزارهای داده–محور از محفظه داده (Data Container) مشترک به‌عنوان انتزاع مرکزی استفاده می‌شود. فرستنده و گیرنده با نوشتن داده‌ها در محفظه‌ها و خواندن از آنها با یکدیگر ارتباط برقرار می‌کنند. از اولین سیستم‌های داده– محور می‌توان به سیستم‌های با حافظه مشترک توزیع-شده اشاره کرد. نمونه دیگری از این سیستم‌ها مفهوم فضای تاپل است که توسط زبان لیندا مطرح شده است.	**سرویس توزیع داده (Data Distribution Service(DDS))** میان‌افزار سرویس توزیع داده که توسط گروه OMG توصیف شده است، امکان ارتباطات ناشر– متقاضی، داده– محور و بلادرنگ را برای سطح گسترده‌ای از محیط‌های محاسباتی فراهم می‌کند. این میان‌افزار از مدل ارتباطی یک به یک استفاده کرده و مستقل از موقعیت و سکو است. در سال‌های اخیر مقیاس‌پذیری و کارایی سرویس توزیع داده در سطح شبکه جهانی و سیستم‌های مقیاس وسیع افزایش پیدا کرده است. OpenDDS، Connext DDS و Vortex OpenSplice نمونه‌هایی از سرویس توزیع داده هستند.
گذرگاه سرویس سازمانی **(Enterprise Service Bus(ESB))** گذرگاه سرویس سازمانی میان‌افزاری است که از نیازمندی‌هایی مانند یکپارچه‌سازی سرویس‌ها، امنیت،	**Mule ESB** تولید کننده: شرکت MuleSoft مجوز: پروانه اختصاصی برای نسخه‌های اختصاصی زبان برنامه‌سازی:Java سیستم عامل: مستقل از سیستم‌عامل

استانداردهای سرویس	مثال
مدیریت، کنترل سرویس و مدیریت ارتباطات پشتیبانی می‌کند. برای این منظور گذرگاه سرویس سازمانی استانداردهای مربوط به میان‌افزارهای پیام‌گرا، وب‌سرویس‌ها، تبدیل داده‌ها، مسیریابی هوشمند و هماهنگی تعاملات بین برنامه‌ها با پشتیبانی از یکپارچگی تراکنش‌ها را باهم ترکیب کرده و به کار می‌گیرد.	**JBoss ESB** تولید کننده: شرکت Red Hat مجوز: GNU Lesser General Public License زبان برنامه‌سازی:Java سیستم عامل: مستقل از سیستم‌عامل
	OpenESB تولید کننده: انجمن OpenESB مجوز: CDDL زبان برنامه‌سازی:Java سیستم عامل: مستقل از سیستم‌عامل
	Petals ESB تولید کننده: کنسرسیوم OW2 مجوز: LGPL 2.0 زبان برنامه‌سازی:Java سیستم عامل: مستقل از سیستم‌عامل
	ServiceMix تولید کننده: شرکت Apache Software Foundation مجوز: Apache License 2.0 زبان برنامه‌سازی:Java سیستم عامل: مستقل از سیستم‌عامل
	IBM Integration Bus تولید کننده: شرکت IBM مجوز: پروانه اختصاصی زبان برنامه‌سازی:Java ، ESQL ، C++،.NET Visual Basic سیستم عامل: مستقل از سیستم‌عامل
	Microsoft BizTalk Server تولید کننده: شرکت Microsoft مجوز: پروانه اختصاصی سیستم عامل: Windows
دلال درخواست شیء **(Object Request Broker(ORB))** فناوری است که با استفاده از آن اشیاء توزیع‌شده با اشیاء راه دور ارتباط برقرار کرده و تبادل داده می‌کنند. ORB پیاده‌سازی اشیاء را محصورسازی کرده و به کاربران اجازه می‌دهد که با دسترسی به واسطها به توسعه کاربردها بپردازند. وقتی یکی از مؤلفه‌های کاربردها بخواهد از سرویس‌های فراهم شده توسط شیء دیگری استفاده کند ابتدا باید یک ارجاع از شیء مذکور	**(Common Object Request Broker Architecture) CORBA** معماری CORBA استانداردی است که توسط گروه OMG معرفی شده و اجازه می‌دهد مؤلفه‌های نرم‌افزاری که با زبان‌های برنامه‌سازی مختلف نوشته شده و بر روی سکوهای مختلف اجرا می‌شوند با یکدیگر تعامل کنند.
	(Component Object Model) COM استاندارد واسط باینری است که توسط شرکت Microsoft برای طراحی و ساخت کاربردهای مبتنی بر مؤلفه معرفی شده است. این

استانداردهای سرویس	مثال
بدست آورده و بر اساس آن متدهای فراهم شده توسط آن شیء را فراخوانی کند. وظیفه اصلی ORB تصمیم‌گیری در مورد ارجاع به اشیاء مورد نظر و برقراری ارتباط کاربردها از طریق ارتباط این اشیاء است. در ORB از پروتکل فراخوانی رویه از راه دور (RPC) استفاده می‌شود که شفافیت مکانی را برای ORB فراهم می‌کند.	استاندارد به‌منظور توانمندسازی ارتباطات بین فرایندی و ایجاد اشیاء پویا در تعداد زیادی از زبان‌های برنامه‌سازی مورد استفاده قرار گرفته است. مؤلفه‌های COM تنها برای برقراری ارتباطات بین فرایندی در محدوده فرایندهای یک کامپیوتر مورد استفاده قرار می‌گیرند. COM به‌عنوان پایه بسیاری از فناوری‌های شرکت Microsoft مانند COM+، DCOM، OLE، OLE Automation و ActiveX محسوب می‌شود.
	(Distributed Component Object Model) DCOM توسعه‌ای از COM است که اجازه می‌دهد مؤلفه‌های COM در محدوده شبکه با یکدیگر ارتباط برقرار کنند. این در حالی است که مؤلفه‌های COM تنها برای برقراری ارتباطات بین فرایندی در محدوده فرایندهای یک کامپیوتر مورد استفاده قرار می‌گیرند.
فراخوانی رویه راه دور **(Remote Procedure Call(RPC))** پروتکلی است که در آن یک میان‌افزار اجازه می‌دهد که یک رویه همانطور که بر روی کامپیوتر محلی اجرا می‌شود بر روی فضای آدرس‌دهی دیگری (که معمولاً بر روی کامپیوتر دیگری در شبکه مشترک قرار دارد) اجرا شود، بدون آنکه برنامه‌ساز صریحاً جزئیات تعاملات راه دور در آن را پیاده‌سازی نماید. این پروتکل شکلی از تعاملات مشتری–خدمتگزار است که نوعاً از طریق سیستم‌های ارسال پیام و به‌صورت درخواست–پاسخ پیاده‌سازی شده و می‌تواند همگام یا غیرهمگام باشد	**XML-RPC** پروتکلی است که برای پیاده‌سازی فراخوانی‌ها از XML و برای انتقال آنها از HTTP استفاده می‌کند.
	(Wireless Application Protocol) SOAP نسخه بهبودیافته XML-RPC است که برای پیاده‌سازی فراخوانی‌ها از XML و برای انتقال آنها از HTTP استفاده می‌کند. به‌عبارت دیگر، SOAP فراخوانی رویه راه دور مبتنی بر HTTP/XML را برای وب‌سرویس‌ها فراهم می‌کند.
	JSON-RPC پروتکلی است که برای جایگزینی XML-RPC و SOAP ارائه شده و در آن از JSON استفاده شده است. JSON (JavaScript Object Notation) یک استاندارد باز با ساختاری خوانا برای انسان و ماشین است. می‌توان اطلاعات و داده‌های مختلف از جمله داده‌های یک پایگاه‌داده را با استفاده JSON بین عوامل مختلف منتقل کرد.
	JSON-WSP پروتکلی است مبتنی بر وب که مشابه پروتکل JSON-RPC از JSON استفاده می‌کند. به دلیل عدم وجود توصیفات سرویس در JSON-RPC این پروتکل طراحی شده و در آن توصیفات سرویس نیز افزوده شده است.
سایر انواع میان‌افزار **(Other Middleware Types)**	**دسترسی داده SQLگرا (SQL Oriented Data Access)** میان‌افزارهایی هستند که بین کاربردها و خدمتگزارهای پایگاه‌داده قرار می‌گیرند. ODBC و ADO.Net نمونه‌هایی از این میان‌افزارها هستند.

استانداردهای سرویس	مثال
شامل میان‌افزارهایی است که با توجه به خصوصیاتی که دارند در گروهی غیر از میان‌افزارهای پیام‌گرا، داده–محور، گذرگاه سرویس سازمانی، دلال درخواست شیء و فراخوانی رویه راه دور قرار گرفته‌اند.	**کنترل پردازش تراکنش (Transaction Processing Monitor)** میان‌افزارهایی هستند که انتقال داده‌ها بین چند پایانه محلی یا راه دور را کنترل کرده تا از کامل شدن تراکنش‌ها مطمئن شده یا در صورت به‌وجود آمدن خطا اقدام مناسب جهت رفع آن را انجام دهند.
	میان‌افزارهای هوشمند (Intelligent Middleware(IMW)) میان‌افزارهایی هستند که از طریق عامل‌های هوشمند امکان هوشمندی بلادرنگ و مدیریت رویدادها را فراهم می‌کنند. این میان‌افزارها پردازش‌های بلادرنگ بر روی حجم زیادی از داده‌های حسگرها را مدیریت کرده و اطلاعات کسب‌وکار هوشمندی را فراهم می‌کنند.
	میان‌افزار تعبیه‌شده (Embedded Middleware) میان‌افزارهایی هستند که سرویس‌های ارتباطی و واسط‌های یکپارچه‌سازی را بین کاربردهای تعبیه‌شده، سیستم‌عامل‌های تعبیه شده و کاربردهای بیرونی فراهم می‌کنند.
کشف، توصیف و تعامل‌پذیری سرویس (Service Discovery, Description & Interoperability) روش‌ها و استانداردهایی که چگونگی ثبت، کشف و استفاده از سرویس‌ها همچنین تعامل بین سرویس‌ها را مشخص می‌کنند.	**UDDI (Universal Description Discovery Integration)** UDDI (توصیف، کشف و یکپارچه‌سازی فراگیر) یک استاندارد مبتنی بر XML است که توسط شرکت‌های Microsoft، IBM و شرکت‌های بزرگ دیگر ارائه شده است و کاربردهای گوناگون را قادر می‌سازد به جستجوی آسان، سریع و پویای سرویس‌های وب بر روی اینترنت بپردازند. UDDI شامل یک مخزن است که ارائه دهندگان سرویس به انتشار و تبلیغ سرویس خود در آن می‌پردازند تا کاربردها به‌صورت پویا و مطابق با نیاز خود بتوانند آن سرویس‌ها را شناسایی و استفاده کنند. استاندارد UDDI می‌تواند از زبان WSDL برای توصیف سرویس‌ها استفاده کرده و از طریق پروتکل SOAP ارتباط برقرار کند.
	WSDL (Web Services Description Language) WSDL (زبان توصیف وب سرویس) زبانی است که سرویس‌های وب را توصیف کرده و چگونگی دسترسی به آنها را مشخص می‌کند. WSDL محل قرار گرفتن وب‌سرویس‌ها و متدهایی که ارائه می‌دهند را در قالب فایل XML در دسترس قرار می‌دهد.
	WS-I Basic Profile استانداردی صنعتی است که برای ارتقای تعامل‌پذیری وب‌سرویس‌ها بین زیرساخت‌ها، برنامه‌های کاربردی و زبان‌های برنامه‌سازی متفاوت مورد استفاده قرار می‌گیرد. WS-I Basic Profile توسط سازمان تعامل‌پذیری وب‌سرویس‌ها (WS-I Organisation) استاندارد شده است.

یکپارچه‌سازی داده (Data Integration)

یکپارچه‌سازی داده شامل استانداردها، پروتکل‌ها و روش‌هایی است که برای تسهیل یکپارچه‌سازی داده‌ها و افزایش تعامل‌پذیری سیستم‌ها مورد استفاده قرار می‌گیرند و بر روی مواردی همچون ساختار و قالب داده، تبادل داده، تبدیل داده، استخراج و بارگذاری داده تمرکز دارند.

جدول ۲-۷ مثال‌هایی از پروتکل‌ها و استانداردهای یکپارچه‌سازی داده

استانداردهای سرویس	مثال
تبدیل و تبادل داده **(Data Exchange & Transformation)** شامل پروتکل‌ها و زبان‌هایی است که چگونگی نمایش داده‌ها در واسط کاربران و برنامه‌های کاربردی را تغییر می‌دهند.	**(Extensible Stylesheet Language Transformations) XSLT** XSLT زبانی است که برای تبدیل یک سند XML به سایر سندهای XML یا سایر فرمت‌ها مانند HTML مورد استفاده قرار می‌گیرد. این فناوری توسط کنسرسیوم وب (W3C) توسعه داده شده است.
	(XML Metadata Interchange) XMI XMI استاندارد گروه OMG برای تبادل اطلاعات فراداده از طریق فایل‌های XML است. هر چند که بیشترین استفاده XMI برای مدل‌های زبان UML است، ولی می‌تواند برای مدل‌های سایر زبان‌ها هم مورد استفاده قرار بگیرد. به‌عبارت دیگر، XMI امکان تبادل فراداده‌ها بین ابزارهای مدل‌سازی (مبتنی بر مدل‌های UML) و مخازن فراداده‌ها (مبتنی بر MOF ارائه شده توسط گروه OMG) در محیط‌های توزیع‌شده ناهمکن را فراهم می‌کند.
	ISO 8601 Data elements and interchange formats استاندارد ISO است که برای تبادل داده‌های مربوط به زمان و تاریخ مورد استفاده قرار می‌گیرد.
طبقه‌بندی و قالب تبادل داده **(Data Exchange Format/Classification)** شامل قالب فایل‌ها و دسته‌بندی آنها است. قالب فایل روشی استاندارد برای کدگذاری اطلاعات جهت ذخیره‌سازی، بازنمایی و انتقال آنها است. برای هر نوع کاربرد قالب‌های فایل مختلفی وجود دارد. به‌عنوان مثال قالب‌های فایلی که برای کاربردهای متنی، صوتی، تصویری واجرایی وجود دارد. هر قالب طرح داده خود را دارد. قالب‌های فایل مربوط به متن ساده‌ترین قالب‌های فایل هستند. هر فایل داری یک پسوند است که با یک نقطه از اسم فایل جدا می‌شود و نمایانگر قالب فایل است.	**پسوندهای فایل‌های متن(Text Files)** .DOC, .DOCX, .LOG, .MSG, .ODT, .PAGES, .RTF.TEX, .TXT, .WPD, .WPS
	پسوندهای فایل‌های داده(Data Files) .CSV, .DAT, .GED, .KEY, .KEYCHAIN, .PPS, .PPT, .PPTX, .SDF, .TAR, .TAX2014
	پسوندهای فایل‌های صوتی(Audio Files) .AIF, .IFF, .M3U, .M4A, .MID, .MP3, .MPA, .WAV, .WMA
	پسوندهای فایل‌های تصویری(Video Files) .3G2, .3GP, .ASF, .AVI, .FLV, .M4V, .MOV, .MP4, .MPG
	پسوندهای فایل‌های عکس سه‌بعدی(3D Image Files) .3DM, .3DS, .MAX, .OBJ
	پسوندهای فایل‌های عکس رَستر(Raster Image Files) .BMP, .DDS, .GIF, .JPG, .PNG, .PSD, .PSPIMAGE, .TGA, .THM, .TIF, .TIFF, .YUV

استانداردهای سرویس	مثال
	پسوندهای فایل‌های عکس برداری(Vector Image Files) .AI, .EPS, .PS, .SVG
	پسوندهای فایل‌های طرح صفحه(Page Layout Files) .INDD, .PDF, .PCT
	پسوندهای فایل‌های صفحه گسترده(Spreadsheet Files) .XLS, .XLXS, .XLR
	پسوندهای فایل‌های پایگاه داده(Databased Files) .ACCDB, .DB, .DBF, .MDB, .PDB, .SQL
	پسوندهای فایل‌های اجرایی(Executable Files) .APK, .APP, .BAT, .CGI,.COM,.EXE,.GADGET, .JAR,.WSF
	پسوندهای فایل‌های بازی(Game Files) .DEM, .GAM, .NES,.ROM,.SAV
	پسوندهای فایل‌های GIS (GIS Files) .GPX, .KML, .KMZ
	پسوندهای فایل‌های وب (Web Files) .ASP, .ASPX, .CER, .CFM, .CSR, .CSS, .HTM, .HTML, .JS, .JSP, .PHP, .RSS, .XHTML
	پسوندهای فایل‌های فونت (Font Files) .FNT, .FON, .OTF, .TTF
	پسوندهای فایل‌های فشرده (Compressed Files) .7Z, .CBR, .DEB, .GZ, .PKG, .RAR , .RPM, .SITX, .TAR.GZ, .ZIP, .ZIPX
	پسوندهای فایل‌های تصویر دیسک (Disk Image Files) .BIN, .CUE, .DMG, .ISO, .MDF, .TOAST, .VCD
	پسوندهای فایل‌های توسعه‌کننده (Developer Files) .C, .CLASS, .CPP, .CS, .DTD, .FLA, .H, .JAVA, .LUA, .M, .PL, .PY, .SH, .SLN, .SWIFT, .VB, .VCXPROJ, .XCODEPROJ
	پسوندهای فایل‌های پشتیبان (Backup Files) .BAK, .TMP
	پسوندهای فایل‌های سیستمی (System Files) .CAB, .CPL, .CUR, .DESKTHEMEPACK, .DLL, .DMP, .DRV
فرازبان یکپارچه‌سازی داده (Data Integration Meta Language) شامل فرازبان‌هایی است که برای یکپارچه‌سازی و تبادل داده‌ها و تعامل‌پذیریِ بیشتر بین بخش‌های مختلف مورد استفاده قرار می‌گیرند.	**SAML (Security Assertion Markup Language)** زبان SAML (زبان نشانه‌گذاری توافق امنیتی) زبانی استاندارد مبتنی بر XML است که برای تبادل داده‌های احراز هویت (Authentication) و مجازشماری (Authorization) بین بخش‌های مختلف مورد استفاده قرار می‌گیرد. SAML توسط کمیته فنی سرویس‌های OASIS تولید شده است.
	XACML (eXtensible Access Control Markup Language)

استانداردهای سرویس	مثال
	زبان XACML (زبان نشانه‌گذاری کنترل دسترسی قابل گسترش) زبانی استاندارد است که برای تعریف سیاست‌های کنترل دسترسی خصوصیت‌مبنا (Attribute-based) مورد استفاده قرار می‌گیرد. از اهداف XACML افزایش تعامل‌پذیری بین پیاده‌سازی‌های کنترل دسترسی است که توسط تولیدکننده‌های مختلف ارائه می‌شود. این زبان توسط سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) ارئه شده است.
	(Digital Signature Services) DSS DSS (سرویس‌های امضای دیجیتال) دو پروتکل مبتنی بر XML درخواست–پاسخ را برای امضاء و تأیید تعریف می‌کند. با این پروتکل‌ها مشتری می‌تواند اسناد خود را به یک خدمتگزار ارسال کرده و امضای آنها را دریافت کند. همچنین مشتری می‌تواند اسناد و امضای آنها را به خدمتگزار ارسال کرده و تأیید صحت امضای آنها را دریافت نماید. استاندارد DSS توسط کمیته فنی OASIS ارائه شده است.
	(XML-Sig and XML-Enc) XML Signature and Encryption استانداردهای مبتنی بر XML است که توسط کنسرسیوم وب جهان‌گستر (W3C) برای امضاهای دیجیتال و رمزنگاری مورد استفاده قرار می‌گیرند.
	XML-Key Management Specification استانداردهای مبتنی بر XML است که توسط کنسرسیوم وب جهان‌گستر (W3C) برای توزیع و ثبت کلیدهای عمومی (Public Key) مورد استفاده قرار می‌گیرند.
مجموعه کاراکترهای تعامل‌پذیر (Interoperable Character Set) شامل روش‌ها و استانداردهای کدگذاری (Encoding) کاراکترها است که برای انتقال اطلاعات به‌کار گرفته می‌شوند.	**Unicode** استاندارد Unicode یک استاندارد صنعتی برای کدگذاری کاراکترهای کامپیوتری و نمایش و پردازش متون به اکثر زبان‌های دنیا است. ترتیب کدگذاری Unicode بر اساس اعداد منحصر به فرد است. سه کدگذاری مختلف با نام‌های UTF-32 ، UTF-16 ، UTF-8 برای Unicodeساخته شده است.. همانطور که از نامشان پیدا است، در فرمت UTF-8 ، کاراکترهای Unicode به‌صورت ۸ بیتی کدگذاری می‌شوند و برای شناسایی هر کاراکتر ، یک بایت یا بیشتر اختصاص پیدا می‌کند. بهترین نکته درباره این فرمت این است که از استاندارد ASCII استفاده می‌کند. بنابراین عبارات انگلیسی و کاراکترهای موجود در استاندارد ASCII بدون کدگشایی، در متنی که فرمت UTF-8 دارد قابل مشاهده هستند. به همین خاطر یکی از فرمت های پر طرفدار Unicode است.

استانداردهای سرویس	مثال
	ASCII استاندارد ASCII استاندارد کدگذاری آمریکایی برای تبادل اطلاعات است. کدگذاری ASCII بر اساس ترتیب حروف الفبای انگلیسی طراحی شده است. تمامی ماشین‌های کدگذاری داده‌های امروزی از استاندارد ASCIIهمانند استانداردهای دیگر موجود در این زمینه پشتیبانی می‌کنند. ASCII اجازه استفاده از ۱۲۸ کاراکتر را می‌دهد اما Unicode تعداد کاراکتر بسیار زیادی را پشتیبانی می‌کند. بیشترین تفاوت ASCII و Unicodeدر نمایش صفحات وب است.
انواع/اعتبارسنجی داده (DataTypes/Validation) شامل استانداردهای است که برای تشخیص و اعتبارسنجی ساختارها و قوانین پردازشی مشترک در اسناد و منابع داده مورد استفاده قرار می‌گیرند.	**DTD (Document Type Definition)** DTD (تعریف نوع سند) روشی برای تشریح، مستندسازی و اعتبارسنجی ساختار استفاده شده در یک سند SGML، HTML یاXML است. با استفاده از DTD ، المان‌های مورد نیاز یک سند تعریف شده و المان‌های اختیاری، تعداد دفعات تکرار یک المان و ترتیب المان‌ها از لحاظ استقرار در آن سند مشخص می‌گردد. استفاده از DTD در اسناد XML نسبت به XML Schema محدودتر است.
	XML Schema XML Schema در سال ۲۰۰۱ به‌عنوان یکی از زبان‌های شِمای XML (XML Schema Language) توسط کنسرسیوم وب جهان‌گستر (W3C) ارائه گردید. برنامه‌سازان از این زبان می‌توانند برای توصیف رسمی المان‌های سند XML و اعتبارسنجی هر بخش از سند XML استفاده کنند. این زبان مانند هر زبان شِمای XML دیگر می‌تواند مجموعه‌ای از قوانین را تعریف کند که با رعایت آن قوانین اعتبار سند XML مشخص می‌شود. XML Schema تحت عنوان (XML Schema Definition) XSD نیز شناخته می‌شود. فرمت XSD همانند یک سند XML است.
	RELAX NG یک زبان شِما (Schema Language) برای XML است. شِماهای تعریف شده توسط RELAX NG الگوهایی را برای ساختار و محتوای اسناد XML توصیف می‌کند. RELAX NG خود یک سند XML بوده و نسبت به سایر زبان‌های شِمای XML ساده است. این زبان در سال‌های ۲۰۰۱ و ۲۰۰۲ توسط کمیته فنی OASIS RELAX NG ارائه شد.
	NVDL NVDL استاندارد ISO/IEC بوده و یک زبان شِمای XML است که برای اعتباسنجی اسناد XMLای که با چندین namespaceیکپارچه شده‌اند مورد استفاده قرار می‌گیرد.

استانداردهای سرویس	مثال
استخراج و تبدیل و بارگذاری داده (Extract, Transformation and Load(ETL)) فرآیندی است که بر اساس آن داده‌ها از منابع اطلاعاتی مورد نیاز موجود در سازمان یا خارج از آن مانند پایگاه‌های داده، فایل‌های متنی، سیستم‌های قدیمی و صفحات گسترده استخراج شده و تبدیل به اطلاعاتی سازگار با فرمت مشخص می‌شوند و سپس در یک مخزن اطلاعاتی که در اغلب اوقات یک انبار داده(Data Warehouse) است، بارگذاری می‌شوند. در این فرایند فراداده‌هایی تولید و نگهداری می‌شود. فراداده‌ها شامل طلاعاتی در رابطه با انتقال و تبدیل داده‌ها، عملکرد انبار داده ، تناظر منابع اطلاعاتی و جداول پایگاه‌داده (که در آنها مشخص شده است منابع اطلاعاتی اولیه به چه قسمت‌هایی از انبار داده نگاشت شده اند) می‌باشد. برای ETL ابزارهای تجاری و متن باز زیادی وجود دارد.	**PowerCenter** تولید کننده: شرکت Informatica نوع ابزار: تجاری
	Infosphere Information Server تولید کننده: شرکت IBM نوع ابزار: تجاری
	Data Integrator تولید کننده: شرکت Oracle نوع ابزار: تجاری
	SQL Server Integrated Services تولید کننده: شرکت Microsoft نوع ابزار: تجاری
	Data Integration studio تولید کننده: شرکت SAS نوع ابزار: تجاری
	Talend Open Studio for Data Integration تولید کننده: شرکت Talend نوع ابزار: رایگان
	CloverETL تولید کننده: شرکت Javlin نوع ابزار: رایگان
	Pentaho Data Integration تولید کننده: شرکت Pentaho نوع ابزار: رایگان

استانداردهای سرویس	مثال
تبادل اطلاعات مبتنی بر هستی‌شناسی **(Ontology-Based Information Exchange)** شامل استانداردها و زبان‌هایی است که برای نشر و تبادل اطلاعات از هستی‌شناسی استفاده می‌کنند.	**(Web Ontology Language) OWL** زبان OWL (زبان هستی‌شناسی وب) زبانی مبتنی بر XML است که جهت نشر و تبادل دانش در فضای اینترنت از هستی‌شناسی (ontology) استفاده می‌کند. این زبان براساس بازبینی زبان DAML+OIL ساخته شده است. کنسرسیوم وب جهان‌گستر (W3C) این زبان را در سه سطح باقابلیت‌های مختلف (OWL Lite , OWL DL و OWL Full) پیشنهاد کرده است. OWL نسبت به XML, RDF (Resource Description Framework) و شمای RDF خوانایی بیشتر محتوای وب را برای ماشین‌ها فراهم می‌آورد. RDF و OWL چارچوبی را برای اشتراک‌گذاری و استفاده مجدد از داده‌های موجود بر روی وب فراهم می‌کنند. توسعه دهندگان محتوی وب, با استفاده از RDF و OWL می توانند فرادادهایی را به اسناد خود متصل کنند تا قابلیت‌های جستجوی بهتری را ممکن سازند. RDF شیوه‌ای را برای تامین اطلاعات توصیفی فراهم کرده و OWL برای مدل کردن دانش مربوط به یک حوزه خاص به کار می‌رود. تمام دانش موجود در آن حوزه، به‌صورت خانواده‌ای از مفاهیم وابسته مدل‌سازی می‌شود.
توصیف داده **(Data Description)** شامل استانداردها و زبان‌هایی است که برای توصیف داده استفاده می‌کنند.	**زبان XML (eXtensible Markup Language)** زبان XML یک زبان فرامتنی قابل توسعه است که با هدف نگهداری و انتقال اطلاعات طراحی شده است. زبان فرامتنی در اصطلاح به زبانی گفته می‌شود که با استفاده از یکسری علائم یا نشانه‌ها، به کاربر یا هر برنامه دیگری که اطلاعات به آن وارد می‌شود، می‌فهماند که اطلاعات را چگونه ویرایش یا استفاده نماید. تگ‌ها و نشانه‌های XML از قبل تعریف نشده‌اند، بلکه کاربر بر حسب نیاز و کاری که می‌خواهد انجام دهد، تگ‌های دلخواه خود را ایجاد می‌کند. به همین دلیل به XML یک زبان قابل توسعه می‌گویند.
	(Resource Description Framework) RDF RDF (چارچوب توصیف منابع) نوعی مدل داده‌ای است که برای ذخیره و بازیابی معنای قابل پردازش توسط ماشین به کار می‌رود. به‌عبارت دیگر RDF مدلی است مبتنی بر گراف که از آن به‌منظور توصیف منابع اینترنتی (نظیر صفحات وب و پست‌های الکترونیکی) و نیز چگونگی ارتباط این منابع با یکدیگر استفاده می‌شود. در حقیقت RDF یک سیستم هستی‌شناسی سبک‌وزن را برای تبادل دانش در اینترنت فراهم می‌کند. RDF/XML نمایش مدل داده‌ای RDF به زبان XML است.
	(extensible Name and Address Language) xNAL زبان xNAL زبانی مبتنی بر XML است که برای توصیف و مدیریت نام و آدرس مشتری ارائه شده است. این زبان زیر مجموعه (Customer

استانداردهای سرویس	مثال
	Information Quality) CIQ است که توسط سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) ارائه شده است. CIQ توصیفات XML است که جهت تعریف، بازنمایی و مدیریت بخش‌های مختلف اطلاعات مورد استفاده قرار می‌گیرد.
	(extensible Customer Information Language) xCIL زبان xCIL زبانی مبتنی بر XML است که برای توصیف و مدیریت اطلاعات مشتری ارائه شده است. این زبان زیر مجموعه (Customer Information Quality) CIQ است که توسط سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) ارائه شده است. CIQ توصیفات XML است که جهت تعریف، بازنمایی و مدیریت بخش‌های مختلف اطلاعات مورد استفاده قرار می‌گیرد.
	(extensible Customer Relationship Language) xCRL زبان xCRL زبانی مبتنی بر XML است که برای توصیف و مدیریت روابط مشتری ارائه شده است. این زبان زیر مجموعه (Customer Information Quality) CIQ است که توسط سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) ارائه شده است. CIQ توصیفات XML است که جهت تعریف، بازنمایی و مدیریت بخش‌های مختلف اطلاعات مورد استفاده قرار می‌گیرد.

یکپارچه‌سازی بیرونی (External Integration)

یکپارچه‌سازی بیرونی شامل واسطهایی است که در یکپارچه‌سازی برنامه‌های کاربردی و سرویس‌ها با دروازه‌های بیرونی مورد استفاده قرار می‌گیرند.

جدول ۲-۸ مثال‌هایی از واسطهای یکپارچه‌سازی بیرونی

استانداردهای سرویس	مثال
واسط سرویس با دروازه‌های بیرونی **(Service interface with external gateways)** شامل واسطها و شبکه‌هایی است که سرویس‌ها و برنامه‌های کاربردی را با دروازه‌های بیرونی همچون دروازه‌های پرداخت، دروازه‌های دولت و دستگاه‌های بیرونی متصل و یکپارچه می‌کند.	**یکپارچه‌سازی بانکی با استفاده از SWIFT** SWIFT (انجمن ارتباط مالی بین بانکی بین‌المللی) شبکه‌ای را فراهم کرده است که موسسات بانکی می‌توانند به‌صورت امن اطلاعات مربوط به تراکنش‌های مالی را ارسال و دریافت کنند. تمامی اعضای SWIFT در یکی از بانک‌های مورد نظر SWIFT دارای حساب می‌باشند و حق برداشت از این حساب ها توسط اعضاء به مؤسسه SWIFT داده شده است. بانک‌ها می‌توانند از انواع پیام‌های SWIFT از جمله پیام‌های مربوط به حواله شخصی، ارسال منابع بین بانکی، پیام‌های مربوط به وام، اعتبارات اسنادی، وصول‌ها و پیام‌های غیرمالی استفاده نمایند.

استانداردهای سرویس	مثال
	شبکه تبادل اطلاعات بانکی (شتاب) وظیفه تبادل اطلاعات بانکی در سطح بین‌المللی و خارج از کشور به عهده شبکه‌های بین‌المللی مانند SWIFT است. اما در داخل کشور و با توجه به ارتباط بین بانک‌های داخلی، SWIFT کارایی و ویژگی‌های لازم را برای این کار ندارد. شبکه شتاب (شبکه تبادل اطلاعات بانکی) این خلاء را پر می‌نماید.

۲-۳ حوزه چارچوب مؤلفه سرویس

حوزه چارچوب مؤلفه سرویس(Service Component Framework Area) شامل فناوری‌ها، استانداردها و توصیفاتی است که استفاده از آنها در یک معماری توزیع‌شده یا سرویس‌گرا امکان ساخت، تبادل و توسعه مؤلفه‌های سرویس را فراهم می‌آورد. این حوزه شامل چهار طبقه منطق کسب‌وکار، مدیریت داده، واسط/نمایش و مدیریت امنیت است.

منطق کسب‌وکار(Business Logic)

منطق کسب‌وکار شامل نرم‌افزارها، پروتکل‌ها و روش‌هایی است که با استفاده از آنها قوانین کسب‌وکار در برنامه‌های کاربردی اِعمال می‌شود. منطق کسب‌وکار بخشی از یک برنامه نرم‌افزاری است که قوانین کسب‌وکار را پیاده‌سازی کرده و تعیین می‌کند که داده‌ها چگونه باید ایجاد، نمایش، ذخیره و تغییر داده شوند. منطق کسب‌وکار متفاوت از سایر مواردی است که در نرم‌افزار مطرح شده و بر روی جزئیات سطح پایین مدیریت پایگاه‌داده‌ها، نمایش واسط کاربر، زیرساخت سیستم و اتصال چند بخش از یک برنامه به یگدیگر تمرکز دارند.

جدول ۲-۹ مثال‌هایی از نرم‌افزارها و پروتکل‌های تعریف قوانین کسب‌وکار

استانداردهای سرویس	مثال
زبان‌های مستقل از سکو **(Platform Independent Languages)** توصیفی است برای زبان‌های برنامه‌سازی و روش‌هایی که قابلیت اجرا بر روی انواع مختلفی از سیستم‌عامل‌ها و سکوها را دارند.	**(Enterprise Java Beans) EJB** یک مؤلفه نرم‌افزاری در محیط J2EE (محیط ارئه شده توسط شرکت SUN) است که برای توسعه و اجرای کاربردهای توزیع‌شده مورد استفاده قرار می‌گیرد.
	C/C++ زبان C یک زبان رویه‌ای است. زبان C++ نسخه شئ‌گرای زبان C است که به‌صورت گسترده در توسعه کاربردهای سازمانی و تجاری مورد استفاده قرار می‌گیرد.
	JavaScript زبانی اسکریپتی است که بر روی مرورگرهای وب اجرا می‌شود.
زبان‌های وابسته به سکو **(Platform Dependent Languages)** توصیفی است برای زبان‌های برنامه‌سازی و روش‌هایی که قابلیت اجرا بر روی انواع مختلفی از سیستم‌عامل‌ها و سکوها را دارند.	**Visual Basic** نسخه‌ای از زبان برنامه‌سازی Basic است که شرکت Microsoft آن را برای توسعه برنامه‌های کاربردی Windows ارائه کرده است.
	(Visual Basic.Net) VB.Net نسخه‌ای از زبان برنامه‌سازی Basic است که شرکت Microsoft آن را برای توسعه برنامه‌های کاربردی Windows که در محیط .Net استفاده می‌شوند ارائه کرده است.

استانداردهای سرویس	مثال
	C# (C-Sharp) زبانی شئ‌گرا بر پایه زبان C است که شرکت Microsoft آن را با استفاده از المان‌هایی از زبان‌های Basic و Java ارئه کرده است.
	VB Script زبانی اسکریپتی است که شرکت Microsoft آن را ارائه کرده است. این زبان زیرمجموعه‌ای از زبان Visual Basic است. این زبان هم در پردازش‌های سمت مشتری در صفحات وب و هم در پردازش‌های سمت خدمتگزار مورد استفاده قرار می‌گیرد.

مدیریت داده (Data Management)

مدیریت داده شامل مدیریت تمام داده‌ها/اطلاعات در یک سازمان است که در برگیرنده استانداردهای تعریف داده‌ها و روش‌هایی است که برای تبادل داده‌ها، کیفیت داده‌ها، پشتیبانی و بازیابی داده‌ها مورد استفاده قرار می‌گیرند.

جدول ۲-۱۰ مثال‌هایی ازپروتکل‌ها و روش‌های کنترل داده

استانداردهای سرویس	مثال
اتصال پایگاه‌داده‌ها (Database Connectivity) شامل پروتکل‌ها و روش‌هایی است که از طریق آنها برنامه‌های کاربردی به پایگاه‌داده‌ها و محل‌های ذخیره‌سازی داده‌ها متصل می‌شوند	**JDBC (Java Database Connectivity)** JDBC یک واسط برنامه‌سازی کاربردی (API) برای زبان برنامه‌سازی Java است که چگونگی دسترسی به پایگاه‌داده‌ها را تعریف می‌کند. ODBC اتصال بین سیستم‌های مدیریت پایگاه‌داده (DBMS) را برای تعداد زیادی از پایگاه‌داده‌های SQL و داده‌های جدولی همانند صفحات گسترده فراهم می‌کند.
	ODBC (Open Database Connectivity) یک واسط برنامه‌سازی پایگاه‌داده است که توسط شرکت Microsoft ارائه شده و توسط برنامه‌های کاربردی Windows برای اتصال به پایگاه‌داده‌ها بر روی شبکه مورد استفاده قرار می‌گیرد.
	OLE/DB (Object Linking and Embedding/Database) واسط برنامه‌سازی کاربردی (API) سطح پایین است که شرکت Microsoft آن را برای اتصال به منابع مختلف داده فراهم کرده است. OLE/DB امکان اتصال به منابع SQL مبتنی بر ODBC و همچنین منابع متنی را فراهم می‌کند. در OLE/DB از فناوری (Component Object Model) COM استفاده شده است که امکان ایجاد واسطهای مستقل از زبان و بر اساس یک استاندارد باینری را فراهم کرده است.
	ADO (ActiveX Data Objects) یک واسط برنامه‌سازی است که به‌عنوان استاندارد شرکت Microsoft برای دسترسی به داده‌ها طراحی شده است. ADO این امکان را فراهم

استانداردهای سرویس	مثال
	می‌کند که توسعه‌دهندگان بدون اطلاع از چگونگی پیاده‌سازی پایگاه‌داده‌ها به داده‌ها دسترسی داشته باشند. ADO براساس OLE/DB طراحی شده و به برنامه‌سازان امکان دستیابی به منابع داده متنوعی را می‌دهد.
	ADO.Net (Active Data Objects .Net) مؤلفه دسترسی داده در چارچوب .Net است که توسط شرکت Microsoft ارائه شده است. ADO.Net مجموعه وسیعی از کلاس‌ها را فراهم می‌کند که دسترسی بهینه به داده‌ها از منابع مختلف را تسهیل می‌کنند.
	DAO (Data Access Objects) کتابخانه‌ای است که شرکت Microsoft آن را برای دسترسی به منابع موتور پایگاه‌داده Jet (Jet Database Engine) ارائه کرده است. DAO به‌عنوان یک خانواده از کلاس‌های مبتنی بر COM (Component Object Model) که از واسط دوگانه پشتیبانی می‌کنند، ارائه شده است.
	DB2 Connector واسط برنامه‌سازی کاربردی (API) شرکت IBM برای اتصال به منابع DB2 است.
تبادل داده **(Data Interchange)** تبادل داده روش‌هایی را تعریف می‌کند که در آنها داده‌ها انتقال پیدا کرده یا داده‌ها در کاربردهای نرم‌افزاری و بین آنها بازنمایی (Represent) می‌شوند.	**XMI (XML Metadata Interchange)** XMI استاندارد گروه OMG برای تبادل اطلاعات فراداده از طریق فایل‌های XML است. هر چند که بیشترین استفاده XMI برای مدل‌های زبان UML است، ولی می‌تواند برای مدل‌های سایر زبان‌ها هم مورد استفاده قرار بگیرد. به‌عبارت دیگر، XMI امکان تبادل فراداده‌ها بین ابزارهای مدل‌سازی (مبتنی بر مدل‌های UML) و مخازن فراداده‌ها (مبتنی بر MOF ارائه شده توسط گروه OMG) در محیط‌های توزیع‌شده ناهمکن را فراهم می‌کند.
	XQuery زبان XQuery زبانی استاندارد است که توسط کنسرسیوم وب جهان‌گستر (W3C) برای پردازش و ارزیابی داده‌های XML طراحی شد. اولین نسخه این زبان (نسخه ۱,۰) در سال ۲۰۰۷ نهایی گردید.
	SOAP (Wireless Application Protocol) پروتکل SOAP (دسترسی آسان به اشیاء) پروتکلی است که برای تبادل پیغام‌های مبتنی بر XML در میان شبکه‌های کامپیوتری مورد استفاده قرار می‌گیرد. این پروتکل برای انتقال پیام‌ها اغلب از پروتکل HTTP و SMTP استفاده می‌کند. در حقیقت SOAP فراخوانی رویه راه دور (RPC) مبتنی بر HTTP/XML را برای وب‌سرویس‌ها فراهم می‌کند.
	ebXML (Electronic Business Using XML)

استانداردهای سرویس	مثال
	استاندارد ebXML یک استاندارد مبتنی بر XML است که توسط سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) و UN/CEFACT حمایت می‌شود. هدف ebXML فراهم کردن زیرساخت مبتنی بر XML و باز است که استفاده سراسری از اطلاعات کسب‌وکار الکترونیکی به روشی امن، تعامل‌پذیر و سازگار بین تمام شرکای تجاری فراهم می‌کند. استانداردهای ebMS، ebXML RS و ebXML RIM زیرمجموعه‌ای از استانداردهای ebXML هستند.
	(eXtensible Business Reporting Language) XBRL زبانی استاندارد و مبتنی بر XML است که توسط شرکت بین‌المللی XBRL برای تسهیل تعامل‌پذیری معنایی در تبادل گزارش‌های کسب‌وکار بین سازمان‌های مختلف ارائه شده است.
	(Resource Description Framework) RDF RDF (چارچوب توصیف منابع) نوعی مدل داده‌ای است که برای ذخیره و بازیابی معنای قابل پردازش توسط ماشین به‌کار می‌رود. به‌عبارت دیگر RDF مدلی است مبتنی بر گراف که از آن به‌منظور توصیف منابع اینترنتی (نظیر صفحات وب و پست‌های الکترونیکی) و نیز چگونگی ارتباط این منابع با یکدیگر استفاده می‌شود. در حقیقت RDF یک سیستم هستی‌شناسی سبک‌وزن را برای تبادل دانش در اینترنت فراهم می‌کند. RDF/XML نمایش مدل داده‌ای RDF به زبان XML است.
	(Web Services User Interface) WSUI WSUI یک استاندارد باز برای مؤلفه‌های واسط کاربری چند سکویی (Cross-platform) است که در وب‌سرویس‌ها به‌کار می‌رود. WSUI از سَبک‌دهی صفحه XSLT برای ایجاد دید کاربر و تعامل کاربر با وب‌سرویس‌ها استفاده می‌کند.
نگاشت اشیاء و رابطه **(Object Relational Mapping (ORM))** نگاشت اشیاء و رابطه یک تکنیک دسترسی به پایگاه‌داده‌های رابطه‌ای از طریق زبان‌های برنامه‌سازی شئ‌گرا است. به‌عبارت دیگر، برای تطبیق پایگاه‌داده‌های رابطه‌ای (مثل SQL Server ، MySQL و غیره) با زبان‌های برنامه‌سازی شئ‌گرا (مثل C#، Java و غیره) و استفاده از امکاناتی همچون وراثت می‌توان از ابزارهای ORM استفاده کرد. در واقع با استفاده از ابزارهای ORM می‌توان ساختار رابطه‌ای پایگاه‌داده‌ها را به ساختار شئ‌گرای یک برنامه متصل کرد و به این ترتیب پیچیدگی‌های مربوط به ذخیره و بازیابی در پایگاه‌داده را به	**Doctrin** تولید کننده: Konsta Vesterinen دسترس‌پذیری: متن باز مجوز: MIT زبان: PHP سکو: Cross-platform
	DataNucleus تولید کننده: DataNucleus Team دسترس‌پذیری: متن باز مجوز: Apache License 2 زبان: Java سکو: JVM ، Cross-platform

استانداردهای سرویس	مثال
عهده ORM قرار داد. برای کاهش بیشتر پیچیدگی و داشتن واسطهای شئ‌گرای سبک‌وزن در برخی مواقع از الگوی طراحی DAO (Data Access Object) استفاده می‌شود. DAO یک شئ برنامه‌سازی است که یک واسط مجرد برای کار با برخی پایگاه‌داده‌ها فراهم می‌آورد.	**RedBeanPHP** دسترس‌پذیری: متن باز مجوز: BSD License زبان: PHP سکو: Cross-platform
	Dapper دسترس‌پذیری: متن یاز مجوز: Apache License 2.0 زبان: C# سکو: Cross-Platform ،.Net 4.0
	ECO تولید کننده: Capable Objects AB دسترس‌پذیری: تجاری سکو: Windows ،.Net 4.0
	EntitySpaces تولید کننده: EntitySpaces, LLC دسترس‌پذیری: متن باز مجوز: Modified BSD License زبان: C# سکو: Cross-Platform ،.Net 4.0
	EclipseLink تولید کننده: Eclipse Foundation دسترس‌پذیری: متن باز مجوز:Eclipse Public and Eclipse Distribution Licenses زبان: Java سکو: Cross-platform ، JVM
	Hibernate تولید کننده: Red Hat دسترس‌پذیری: متن باز مجوز: GNU Lesser General Public License زبان: Java سکو: Cross-platform ، JVM
	MyBatis تولید کننده: The MyBatis team دسترس‌پذیری: متن باز مجوز: Apache License 2.0 زبان: Java

استانداردهای سرویس	مثال
	سکو: Cross-platform
	JOOQ تولید کننده: Data Geekery GmbH دسترس‌پذیری: تجاری و متن باز مجوز: تجاری و Apache License 2.0 زبان: Java سکو: Cross-platform
	Apache Cayenne تولید کننده: Apache Software Foundation دسترس‌پذیری: متن باز مجوز: تجاری و Apache License 2.0 زبان: Java سکو: Cross-platform
	EntitySpaces دسترس‌پذیری: متن باز مجوز: GNU Lesser General Public License زبان: C# سکو: Cross-Platform ،.Net 4.5
	ODB تولید کننده: Code Synthesis دسترس‌پذیری: تجاری و متن باز مجوز: تجاری و GNU General Public License زبان: C++ سکو: Cross-Platform
	Storm تولید کننده: .Canonical Ltd دسترس‌پذیری: متن باز مجوز: LGPL 2.1 زبان: Python سکو: Cross-Platform
	TopLink تولید کننده: Oracle Corporation دسترس‌پذیری: تجاری مجوز: Oracle License زبان: Java سکو: Cross-platform ، JVM

استانداردهای سرویس	مثال
	SQLObject تولید کننده: Ian Bicking دسترس‌پذیری: متن باز مجوز: LGPL زبان: Python سکو: Cross-platform
بازیابی، پشتیبانی و بایگانی داده **(Data Recovery. Backup & Archival)** شامل ابزارهایی است که در ارتباط با بازیابی کردن داده‌های از دست رفته یا حذف شده، گرفتن پشتیبان از داده‌های موجود و بایگانی کردن داده‌های غیرفعال مورد استفاده قرار می‌گیرند.	**ابزارهای گرفتن پشتیبان (Backup Tools)** شامل ابزارهایی است که برای گرفتن داده‌های پشتیبان مورد استفاده قرار می‌گیرند. در واقع داده‌های پشتیبان یک نسخه واقعی یا یک کپی از داده‌های موجود و مورد استفاده در محیط عملیاتی هستند و می‌توانند در فرایند بازیابی داده‌ها مورد استفاده قرار گیرند. برخی از ابزارها، سرویسِ گرفتن پشتیبان به‌صورت برخط (Online Backup Service) را هم فراهم می‌کنند. **ابزارهای رایگان:** AMANDA, Areca Backup, Attic, BackupPC, Bacula, Back In Time, Box Backup, DirSyncPro, duplicity, Duplicati, FlyBack, obnam, luckyBackup, star/gtar, rdiff-backup, Syncthing, Unison, git-annex, DAR **ابزارهای تجاری:** @MAX SyncUp, Acronis True Image, Aomei Backupper, Argentum Backup, Backup4all, BackupAssist, Backup Exec, Catalogic DPX, Bitser, Bvckup 2, ChronoSync, Argentum Backup, Comodo Backup, Crashplan, Dmailer Backup, Double Image Backup, Druva InSync, EMC NetWorker, Genie Backup Manager, Handy Backup, HP Data Protector, IASO Backup, IBM Tivoli Storage Manager, InMage DR-Scout, Image for Windows, Iperius Backup, KeepVault, Langmeier Backup, LazySave, .Mac Backup aka MobileMe, Memopal, Mozy, NetVault Backup, Novabackup, NTBackup, NetBackup, Norton 360, Norton Ghost, EMC RecoverPoint, Retrospect, ShadowProtect, System Center Data Protection Manager, SpiderOak, SyncBack, SyncToy, Time Machine, Tonido Backup, TotalRecovery Pro, UltraBac, Ventis BackupSuite 2008, Windows Home Server Computer Backup, Windows Backup and Restore, Yintersync.NET, Yosemite Server Backup **ابزارهای دارای سرویس گرفتن پشتیبان برخط:** Acronis, ASUS WebStorage, Backblaze, Barracuda, Backup Service, Bitcasa, Box, BullGuard Backup, Carbonite, CloudMe, Comodo Backup, CrashPlan, Cubby, Diino, Dropbox, Dropmysite, Druva Insync,

استانداردهای سرویس	مثال
	Egnyte, Provider, ElephantDrive, EVault, FilesAnywhere, Google Drive, Handy Backup, Trend Micro SafeSync, IASO Backup, iCloud, Infinit, Infrascale, Iperius Online Storage, Intronis, Jumpshare, Jungle Disk, KeepVault, KineticD, Livedrive, MediaFire, MEGA, Memopal, MiMedia, Mozy, MyVault, OneDrive, OwnDrive (ownCloud), SpiderOak, Provider, SugarSync, Syncplicity
	ابزارهای بایگانی کردن (Archive Tools) شامل ابزارهایی است که برای بایگانی کردن داده‌ها مورد استفاده قرار می‌گیرند. بایگانی کردن داده‌های موجود در واقع یک نوع انتقال داده‌های غیرفعال است. این داده‌ها دیگر به‌صورت فعال مورد استفاده قرار نمی‌گیرند و به همین دلیل بایگانی می‌شوند. این داده‌ها در فرایند بازیابی داده‌ها مورد استفاده قرار نمی‌گیرند ولی یک سیستم کنترل نسخه خوب ارائه می‌دهد. **ابزارهای رایگان:** 7-Zip, Archive Manager, Ark, B1 Free Archiver, Bitser, Disk ARchiver, Expander, Filzip, FreeArc, Info-ZIP (Wzip), IZArc, KGB Archiver, PeaZip, TAR, The Unarchiver, TUGZip, Xarchiver, ZipGenius **ابزارهای تجاری:** ALZip, ALZip for Mac, Archive Utility, BetterZip, BulkZip, Commander One, Compressed Folders, CRAX Commander, iArchiver, PKZIP, PowerArchiver, StuffIt, WinAce, WinRAR, WinZip, XAD a.k.a. XADMaster.library
	ابزارهای بازیابی (Recovery Tools) شامل ابزارهایی است که برای بازیابی داده‌های از دست رفته یا حذف شده مورد استفاده قرار می‌گیرند. برخی از این نوع ابزارها عبارتند از: **ابزارهای کنترل سازگاری (Consistency Checker):** CHKDSK, Disk First Aid, Disk Utility, fsck, gparted **ابزارهای بازیابی فایل (File Recovery):** CDRoller, Data Recovery Wizard, Data Rescue PC3, NTFS , Disk Drill Basic, dvdisaster, FileSalvage, GetDataBack, Hetman Partition, Recovery, IsoBuster, Mac Data Recovery Guru, Norton Utilities, PhotoRec, Recover My Files, Recuva, TestDisk, TotalRecovery, TuneUp Utilities, iRecover **ابزارهای Forensic :** EnCase, Foremost , Forensic Toolkit, Open Computer Forensics Architecture, The Coroner's Toolkit, The Sleuth Kit **ابزارهای Imaging :** Clonezilla, CopyCatX, ddrescue, dd

استانداردهای سرویس	مثال
	ابزارهای کنترل نسخه (Version Control Tools) شامل ابزارهایی است که کنترل نسخه و مدیریت پیکربندی نرم‌افزارها را انجام می‌دهند که تعدادی از آنها عبارتند از: AccuRev SCM, GNU Bazaar, BitKeeper, ClearCase, Code Co-op, Codeville, CVS, CVSNT, darcs, Dimensions CM, Endevor, Fossil, Git, GNU arch, IC Manage, MKS Integrity, Mercurial, Monotone, stic SCM, PVCS, Rational Team Concert, Revision Control System, SCM Anywhere, Source Code Control System, StarTeam, Subversion (SVN), Surround SCM, SVK, Team Foundation Server (TFS), Synergy, Vault, Veracity, Vesta, Visual SourceSafe (VSS)
	ابزارهای همگام‌سازی فایل (File Synchronization Tools) شامل ابزارهایی است که اطمینان حاصل می‌کنند که فایل‌های موجود در چند نقطه با قوانین مشابهی به‌روزرسانی می‌شوند. **ابزارهای متن باز:** Conduit, DirSync Pro, FreeFileSync, iFolder, luckyBackup, OneSync, ownCloud, rsync, Seafile community edition, SparkleShare, SymmetricDS, Synchronizer (krusader), Syncthing, Synkron, Unison **ابزارهای تجاری:** @MAX SyncUp, Allway Sync, AIMstor, Argentum Backup, BackupAssist, Backup4all, BatchSync, BitTorrent Sync, Box Sync, ChronoSync, Cloudike, CloudMe, Cubby – Pro, Distributed Storage, Dropbox, Easy2Sync for Files, Egnyte, Gladinet, GoDrive, GoodSync, Handy Backup, IBM Connections, MediaFire, Mega, RepliWeb, Robocopy, SecureSafe, SpiderOak, ShareFile, SugarSync, SyncBack, Syncdocs, Synchronize It!, Syncplicity, TeamDrive, Tonido,XXL Box, Zetta.net
هوشِ کسب‌وکار **(Business Intelligence(BI))** شامل مجموعه‌ای از روش‌ها و فناوری‌هایی است که برای تبدیل داده خام به اطلاعات مفید و معنادار استفاده می‌شود. هوش کسب‌وکار مقادیر بزرگی از اطلاعات را برای شناسایی و توسعه فرصت‌های جدید به کار می‌گیرد. در بسیاری مواقع هوش کسب‌وکار داده‌هایی را که در انباره‌های داده (Data	**ابزارهای هوش کسب‌وکار متن باز و رایگان** ▪ BIRT ▪ D3.js ▪ JasperReports ▪ KNIME ▪ Pentaho ▪ R ▪ Seal Report ▪ SpagoBI ▪ TACTIC

استانداردهای سرویس	مثال
(Warehouses جمع‌آوری شده‌اند را مورد استفاده قرار می‌دهد. از اینرو برخی مواقع از BI/DW به‌جای BI استفاده می‌شود. ابزارهای بسیار زیادی برای هوش کسب‌وکار ارائه شده است. این ابزارها می‌توانند برای اهداف کسب‌وکاری ذیل به کار روند: ▪ اندازه‌گیری (Measurement): برنامه‌ای که سلسله مراتبی از شاخص‌های عملکرد و محک زنی ایجاد می‌کند. ▪ تحلیلی (Analytic) برنامه‌ای که فرایندهای کمی برای کسب‌وکار ایجاد می‌کند که بتواند به شناخت تصمیمات بهینه دست بیابد و به اکتشاف دانش کسب‌وکار بپردازد. داده‌کاوی، فرایندکاوی، تحلیل آماری، تحلیل پیشنگرانه، مدل‌سازی پیشنگرانه، مدل‌سازی فرایندهای کسب‌وکار، پردازش رویدادهای پیچیده نمونه‌های از برنامه‌های تحلیلی محسوب می‌شوند. ▪ گزارش‌دهی (Reporting): برنامه‌هایی که زیرساخت‌های لازم برای گزارش‌دهی استراتژیک را در خدمت به مدیریت استراتژیک کسب‌وکار انجام می‌دهند. این نوع گزارش‌ها شامل مصورسازی داده، سیستم اطلاعات مدیریتی و پردازش تحلیلی برخط (Online analytical processing(OLAP)) می‌شوند. ▪ همکاری (Colaboration): برنامه‌هایی که از طریق به اشتراک گذاری داده و تبادل اطلاعات الکترونیکی، مناطق مختلف (داخل یا بیرون از کسب‌وکار) را برای انجام کار کنار یکدیگر می‌آورد. ▪ مدیریت دانش: برنامه‌هایی که از طریق استراتژی‌ها و اقداماتشان برای شناخت، ایجاد، بازنمایی، توزیع و قادر ساختن سازمان به درک بینش‌ها و تجربه‌هایی که دانش واقعی کسب‌وکار هستند سازمان‌ها را تبدیل به شرکت‌هایی داده محور می‌سازند. با توجه به اهداف مطرح شده برای ابزارهای هوش کسب‌وکار، ابزارهایی که هر یک از این اهداف را دنبال می‌کنند را می‌توان در طبقه ابزارهای هوش کسب‌وکار قرار داد.	**ابزارهای هوش کسب‌وکار متن باز و تجاری** ▪ Palo ▪ Pentaho ▪ TACTIC **ابزارهای هوش کسب‌وکار مالکانه و رایگان** ▪ Biml ▪ Datacopia ▪ icCube ▪ InetSoft ▪ Splunk **ابزارهای هوش کسب‌وکار مالکانه** ▪ ActiveReports ▪ Actuate Corporation ▪ AnyChart ▪ AnswerRocket ▪ ApeSoft ▪ BOARD ▪ Comarch ▪ Data Applied ▪ datapine ▪ Decision Support Panel ▪ Domo ▪ Dundas Data Visualization ▪ Dimensional Insight ▪ Grapheur ▪ GoodData - Cloud Based ▪ IBM Cognos ▪ icCube ▪ InetSoft ▪ Information Builders ▪ InfoZoom ▪ JackBe ▪ Jedox ▪ Klipfolio Dashboard ▪ Lavastorm Analytics ▪ LIONsolver ▪ List & Label ▪ Logi Analytics ▪ Looker ▪ Microsoft SQL Server Reporting Services ▪ Microsoft SQL Server Analysis Services ▪ Microsoft PerformancePoint Server 2007 ▪ Microsoft Proclarity ▪ Microsoft Power Pivot ▪ MicroStrategy ▪ Oracle Hyperion Solutions Corporation

استانداردهای سرویس	مثال
موارد ذیل گروه‌های اصلی ابزارهای هوش کسب‌وکار محسوب می‌شوند: ▪ صفحات گسترده (Spreedsheets) ▪ گزارش‌دهی (Reporting) ▪ داشبورد دیجیتال (Digital Dashboard) ▪ پردازش تحلیلی برخط (OLAP) ▪ داده‌کاوی (Data Mining) ▪ انباره‌های داده (Data Warehouse) ▪ سیستم اطلاعات محلی (LIS).	▪ Oracle Business Intelligence Suite Enterprise Edition ▪ Panorama Software ▪ Pervasive DataRush ▪ Phocas Software ▪ Plotly ▪ Qlik ▪ Quantrix ▪ RapidMiner ▪ Roambi ▪ RW3 Technologies ▪ SAP NetWeaver Business Intelligence ▪ Saiku Analytics ▪ Sisense ▪ SAS ▪ Siebel Systems ▪ Spotfire (now Tibco) ▪ Sybase IQ ▪ Tableau Software ▪ TARGIT Business Intelligence ▪ Teradata ▪ XLCubed ▪ Yellowfin Business Intelligence ▪ Zoho Reports ▪ Zoomdata

موتورهای جستجو

(Search Engines)

موتورهای جستجو برای جستجوی داده مورد نظر در بین گروهی از داده‌ها مورد استفاده قرار می‌گیرند. برای این منظور واسطی در اختیار کاربران گذاشته می‌شود که معیارهای خود را برای داده مورد نظر بیان کرده و موتوری وجود دارد که داده مورد نظر را پیدا می‌کند. از موتورهای جستجوی گوگل و بینگ می‌توان به‌عنوان قدرتمندترین موتورهای جستجو در دنیا نام برد.

با این حال نیاز به طراحی و استفاده از موتورهای جستجوگر بومی جهت فراهم کردن بستری مطمئن و امن برای جستجوهای اینترنتی، رفع نیازمندی‌ها به زبان فارسی و تمرکز

جستجو به وسیله منبع (Search By Source)

فناوری‌های زیر مبتنی بر جستجو به وسیله منبع هستند:

- جستجوی دسکتاپ (Desktop Search)
- جستجوی متحد (Federated Search)
- موتور جستجوی انسانی (Human Search Engine)
- موتور فراجستجو (Metasearch Engine)
- چندجستجویی (Multisearch)
- موتور جستجوی وب (Web Search Engine)

جستجو به وسیله نوع محتوا (Search By Content Type)

فناوری‌های زیر مبتنی بر جستجو به وسیله محتوا هستند:

- جستجوی متن کامل (Full Text Search)
- جستجوی عکس (Image Search)
- موتور جستجوی ویدئو (Video Search Engine)

استانداردهای سرویس	مثال
بر سرویس‌های محلی امری ضروری به نظر می‌رسد. موتورهای جستجوگر بومی پارسی‌جو و یوز برای پاسخ به این نیاز در داخل کشور تولید شده‌اند.	**جستجو به وسیله واسط (Search By Interface)** فناوری‌های زیر مبتنی بر جستجو به وسیله واسط هستند: ▪ جستجوی تدریجی (Incremental Search) ▪ پاسخ لحظه‌ای (Instant Answer) ▪ جستجوی معنایی (Semantic Search) ▪ جستجوی مبتنی بر انتخاب (Selection-based Search)
	جستجو به وسیله عنوان (Search By Topic) فناوری‌های زیر مبتنی بر جستجو به وسیله عنوان هستند: ▪ پایگاه‌داده فهرست کتب (Bibliographic Database) ▪ جستجوی سازمانی (Enterprise Search) ▪ جستجوی عمودی (Vertical Search)

واسط/نمایش (Interface/Presentation)

واسط/نمایش اتصال بین کاربر و نرم‌افزار را برقرار می‌کند و شامل نمایشی است که به‌صورت فیزیکی بر روی صفحه نمایش ظاهر می‌شود.

جدول ۲-۱۱ مثال‌هایی از ابزارهای نمایش

استانداردهای سرویس	مثال
نمایش ایستا **(Static Display)** نرم‌افزارها و پروتکل‌هایی که برای ایجاد واسطهای گرافیکی از پیش تعریف شده و غیرقابل تغییر بین کاربر و نرم‌افزار استفاده می‌شوند.	**(Hypertext Markup Language) HTML** زبان HTML یک زبان توصیف ساختار صفحه‌های وب است که توسط کنسرسیوم وب جهان‌گستر (W3C) پیشنهاد شده است. این زبان شکلی از زبان SGML است که از تگ‌ها برای نشانه‌گذاری عناصری چون متن و گرافیک استفاده می‌کند تا برای مرورگرهای وب مشخص شود که این عناصر را چگونه برای کاربر نمایش دهند و به عملیاتی چون فعال کردن یک پیوند از طریق فشردن یک کلید یا کلیک ماوس چگونه پاسخ دهند.
	(Portable Document Framework) PDF یک استاندارد باز برای قالب فایل است که برای نمایش دوبعدی مستندات مستقل از نرم‌افزار، سخت‌افزار و سیستم‌عامل به‌کار گرفته می‌شود.
نمایش پویا (نمایش سمت خدمتگزار) **(Dynamic / Server-Side Display)** نرم‌افزارها و پروتکل‌هایی که برای ایجاد واسطهای گرافیکی با قابلیت تغییر در هنگام اجرای برنامه استفاده می‌شوند	**(Java Server Page) JSP** JSP نوعی فناوری مبتنی بر زبان JAVA است که امکان تولید وب‌گاه‌های پویا را فراهم می سازد. JSP توسط شرکت Sun برای برنامه‌سازی سمت سرور تولید شده است. فایل‌های JSP همان فایلهای html است که قطعات ویژه شامل کدهای Java که قابلیت پویای

استانداردهای سرویس	مثال
	صفحات را ایجاد می‌کند به آن اضافه شده است.
	(Active Server Pages) ASP فناوری خدمتگزار وب مربوط به شرکت مایکروسافت است که امکان ایجاد نشست‌های پویا و تعاملی با کاربران را ایجاد می‌کند.
	(Active Server Pages .Net) ASP.Net مجموعه‌ای از فناوری‌های چارچوب Net. است که برای ساخت برنامه‌های کاربردی وب و سرویس‌های وب XML استفاده می‌شود. صفحات ASP.Net بر روی خدمتگزارها اجرا شده و خروجی‌های نشانه‌گذاری مانند خروجی‌های HTML، WML و XML تولید می‌کند که به مرورگرهای دسکتاپ و موبایل ارسال می‌شوند.
رِندِر کردن محتوا **(Content Rendering)** نرم‌افزارها و پروتکل‌هایی که برای تبدیل داده‌ها جهت نمایش آنها در واسط گرافیکی کاربران مورد استفاده قرار می‌گیرند.	**(Dynamic HTML) DHTML** در DHTML قابلیت‌های جدیدتری نسبت به HTML تعریف شده است که بر اساس آن می‌توان کنترل بیشتری بر روی مؤلفه‌های موجود در یک صفحه وب اعمال کرد و بتوان به صفحه وب جلوه‌های ویژه (مبتنی بر شرایط مرورگر) بخشید. با DHTML می‌توان امکاناتی به صفحات وب اضافه کرد که باعث شود کاربر با آن صفحه تعامل داشته باشد. معمولاً DHTML از چهار بخش DOM، CSS، رویدادهای HTML و اسکریپت‌ها تشکیل شده است. با استفاده از یک زبان اسکریپتی اشیای مشخص در DOM را می‌توان کنترل کرد. JavaScript رایج‌ترین زبان اسکریپتی روی اینترنت است که با همه مرورگرها کار می‌کند. JavaScript اولین بار در مرورگر Netscape 2.0B3در دسامبر ۱۹۹۵ معرفی و ظاهر شد. استاندارد رسمی جاوا اسکریپت ECMA-262 است.
	(Extensible HTML) XHTML همان HTML است به همراه رعایت دقیق تمامی قواعد و دستورات نحو نزدیک‌تر به زبان XML که موجبات افزایش اطمینان از عملکرد صحیح سندها در شرایط پیچیده‌تر موجود در اینترنت را فراهم می‌سازد. XHTML در واقع زیر مجموعه و گسترش یافته HTML4 است. این نوع اسناد بر پایه XML هستند و برای کار در ترکیب با عامل کاربر مبتنی بر XML طراحی شده‌اند. XHTML نیز توسط کنسرسیوم وب جهان‌گستر (W3C) پیشنهاد شده است.
	(Cascading Style Sheet) CSS روشی ساده برای نمایش چیدمان و جلوه‌های تصویری (مانند نوع قلم، رنگ و اندازه‌ها) در صفحات وب است. CSS اولین بار توسط کنسرسیوم وب جهان‌گستر (W3C) به تمامی جهانیان به‌عنوان یک استاندارد طراحی وب معرفی شد.

استانداردهای سرویس	مثال
	(Extensible 3D Graphics) X3D نوعی فرمت فایل‌های سه بعدی است که فرمت XML دارد و نسل بعدی فرمت‌های VRML است. این فرمت استاندارد ISO برای گرافیک‌های کامپیوتری سه بعدی بلادرنگ است.
بی‌سیم/موبایل/صوت **(Wireless/Mobile/Voice)** نرم‌افزارها و پروتکل‌هایی که برای دستگاه‌های نمایش بی‌سیم، موبایل و صوتی به کار می‌روند.	**(Wireless Markup Language) WML** پروتکل مبتنی بر XML که برای دستگاه‌های بی‌سیم طراحی شده است.
	(Wireless Markup Language Script) WML Script زبان WML Script یک گویش یا مشتق از زبان جاوا اسکریپت است که برای صفحات WML استفاده می‌شود و قسمتی از پروتکل برنامه‌های بی‌سیم و رادیویی است.
	(XHTML Mobile Profile) XHTMLMP برای مشتریان وب با منابع محدود همانند موبایل‌ها و پیجرها که نمی‌توانند از تمام ویژگی‌های XHTML استفاده کنند طراحی شده است.
	(Voice XML) VXML زبان VXML یک زبان بر پای XML است که برای نرم افزارهای صوتی تحت شبکه به‌وجود آمده است. VXML به‌عنوان یک استاندارد باز که الگوی توسعه وب را به بازار تلفن گویا و تشخیص صدا آورده است پدیدار شده است.
شخصی‌سازی **(Personalization)** شخصی‌سازی به تطبیق دادن یک محصول یا سرویس با خصوصیات یک کاربر یا گروهی از کاربران گفته می‌شود و از عناصر اصلی سیستم‌های توصیه‌گر و رسانه‌های اجتماعی است. شخصی‌سازی وب‌گاه‌ها این امکان را می‌دهد که محتوا و سرویس‌های وب بر اساس علاقه، نیاز و نقش کاربر یا گروه کاربران در دسترس آنها قرار بگیرد. در این شخصی‌سازی انتظار می‌رود که رفتار وب‌گاه متناسب با خواست کاربران و در محدوده‌ای که اجازه داده می‌شود تغییر کند.	**شخصی‌سازی صریح (Explicit Personalization)** در شخصی‌سازی صریح، کاربران بر اساس ویژگی‌هایی که یک سیستم اطلاعاتی یا یک وب‌گاه در اختیارشان می‌گذارد نحوه دریافت محتوا و سرویس از آن سیستم یا وب‌گاه را تغییر می‌دهند.
	شخصی‌سازی ضمنی (Implicit Personalization) در شخصی‌سازی ضمنی، رفتار کاربران در استفاده از یک سیستم اطلاعاتی یا یک وب‌گاه بررسی شده و بر اساس الگوی رفتاری به دست آمده نحوه دریافت محتوا و سرویس از آن سیستم یا وب‌گاه تغییر می‌کند.
	شخصی‌سازی ترکیبی (Hybrid Personalization) در شخصی‌سازی ترکیبی، از قابلیت‌های شخصی‌سازی ضمنی و شخصی‌سازی صریح استفاده می‌شود.

مدیریت امنیت(Security Management)

مدیریت امنیت شامل پروتکل‌ها، روش‌ها، استانداردها و ابزارهایی است که برای محافظت اطلاعات و زیرساخت‌های اطلاعاتی از دسترسی غیرمجاز، استفاده غیرمجاز، تغییر غیرمجاز، خرابی، تهدید و افشای اطلاعات استفاده می‌شوند و سه هدف اصلی محرمانگی (Confidentiality)، صحت (Integrity) و قابلیت‌دسترسی(Availability) را دنبال می‌کنند.

جدول ۲-۱۲ مثال‌هایی از ابزارها و روش‌های مدیریت اطلاعات

استانداردهای سرویس	مثال
ضد ویروس (Anti-Virus) نرم‌افزار ضد ویروس (ویروس‌یاب، ویروس‌کش یا ضد بدافزار) نرم‌افزاری است که با مشاهده و بررسی محتوای فایل‌ها و پرونده‌ها به دنبال الگوهای آشنای بدافزار شامل ویروس‌ها یا کرم‌های اینترنتی می‌گردد. نرم‌افزار ضد ویروس در صورت مشاهده این الگوها که به آن امضای ویروس (Virus Signature) گفته می‌شود، از ورود آن به کامپیوتر و اجرا شدنش جلوگیری کرده یا هشدار لازم را می‌دهد و دستور می‌گیرد که آیا فایل را حذف کند یا سعی نمایند آن را اصلاح و پاکسازی کند. شرکت‌های سازنده نرم‌افزارهای ضدویروس، با ساخته شدن ویروس‌های جدید، الگوهای نرم‌افزاری آنها را کشف و جمع‌آوری می‌کنند و به همین علت اغلب لازم است تا این نرم‌افزارها هر از چندگاهی به‌روزرسانی شوند تا الگوهای جدید ویروس‌ها را دریافت کنند. نرم‌افزارهای ضد ویروس زیادی برای خدمتگزارها، دسکتاپ‌ها، موبایل‌ها و تبلت‌ها ارائه شده است.	**نرم‌افزارهای ضد ویروس برای دسکتاپ و خدمتگزار** AhnLab V3 Internet Security, Avast!, AVG, Avira Internet Security, BitDefender, BullGuard, ClamWin, Clam AntiVirus, Comodo Antivirus, Comodo Internet Security, Dr. Web, ESET NOD32, F-Secure, F-PROT, Fortinet, G Data, VIPRE, Advanced SystemCare, iolo System Shield, K7 Total Security, Kaspersky Anti-Virus, Kaspersky Internet Security, KingSoft, Mac Internet Security Malwarebytes' Anti-Malware, McAfee VirusScan, Microsoft Security Essentials, Windows Defender, NANO Antivirus (ru), Panda, PSafe TOTAL, 360 Safeguard, Outpost Security Suite, Sophos, Symantec Endpoint Protection, Immunet, Element Anti-Virus, Norton AntiVirus, Norton Internet Security, Spyware Doctor, VirIT eXplorer, VirusBarrier, Trend Micro Internet Security, TrustPort, Vba32 AntiVirus, ZoneAlarm **نرم‌افزارهای ضد ویروس برای موبایل و تبلت** AhnLab Mobile Security, Avast Antivirus, AVG AntiVirus, Avira Free Android Security, Bitdefender Mobile Security, BullGuard Mobile Security, CM Security, Comodo Mobile Security, Dr. Web Mobile Security Suite, ESET Mobile Security, F-Secure Mobile Security, G Data MobileSecurity, Lookout Mobile Security, McAfee Mobile Security, PSafe TOTAL Android, FireAMP Mobile, Trend Micro Mobile Security, TrustPort Mobile Security, VirusBarrier
فایروال (Firewall) به سیستم‌هایی اطلاق می‌شود که شبکه خصوصی یا کامپیوترهای شخصی را در مقابل نفوذ مهاجمین، دسترسی‌های غیرمجاز، ترافیک‌های مخرب و حملات هکری خارج از آنها محافظت می‌کند. فایروال‌ها می‌توانند ترافیک ورودی و خروجی شبکه را کنترل و مدیریت کرده و با توجه به	**فایروال‌های نرم‌افزاری** در حقیقت نرم‌افزارهایی هستند که می‌توانند روی سیستم‌عامل‌های مختلف نصب شوند و ترافیک ورودی و خروجی شبکه یا سیستم‌عامل را کنترل کنند. اینگونه فایروال‌ها بیشتر مورد استفاده سازمان‌ها و شرکت‌های کوچک و متوسط قرار می‌گیرند. فایروال‌های نرم‌افزاری سیستم‌ها را از خطرات معمولی که در اینترنت وجود دارند اعم از دسترسی‌های غیرمجاز، تروجان‌ها و کدهای مخرب و کرم‌های

استانداردهای سرویس	مثال
قوانینی که در آنها تعریف می‌شود به کاربر یا برنامه‌های کاربردی خاصی اجازه ورود، خروج و دسترسی به یک سیستم خاص را بدهند. قوانینی که در یک فایروال وجود دارد بر اساس نیازمندی‌های امنیتی یک سازمان تعیین می‌شود. فایروال‌ها می‌توانند به‌صورت نرم‌افزاری یا سخت‌افزاری مورد استفاده قرار گیرند. چهار فناوری مهم به‌کار گرفته شده در فایروال‌ها عبارتند از: ▪ **Packet Filtering Firewall** این نوع فایروال یکی از ساده‌ترین انواع فایروال‌ها است که در سال ۱۹۸۵ عرضه شده است. در این فایروال، بسته‌ها براساس پروتکل، پورت، آدرس مبدأ یا آدرس مقصد عبور کرده یا مسدود می‌شوند. این نسل از فایروال‌ها تنها با لایه‌های اول OSI برای به دست آوردن IPها سروکار دارند. ▪ **Circuit Level Gateway** این دسته از فایروال‌ها از دسته قبلی دارای امنیت بیشتری هستند و در سال ۱۹۸۹–۱۹۹۰ به میان آمدند. این دسته در لایه نشست مدل OSI کار می‌کنند و به‌عنوان واسط بین لایه کاربردی و لایه انتقال TCP/IP عمل می‌کنند و ترافیک شبکه را براساس آدرس و پورت‌ها در لایه نشست فیلتر می‌کنند. ▪ **Aplication Level Gateway** دو دسته قبلی فایروال‌ها تنها سرآیندهای لایه‌های شبکه و نشست را مورد بررسی قرار می‌دادند. برخلاف دو دسته قبل، در این دسته از فایروال‌ها امکان دیدن محتوای بسته‌ها وجود دارد. به این دسته از فایروال‌ها، فایروال‌های پروکسی نیز گفته می‌شود که در در حالت proxy server و proxy client مورد استفاده قرار می‌گیرند. ▪ **Staeful Multi Level Inspection** این فایروال‌ها نسل چهارم از فایروال‌ها هستند که در سال ۱۹۹۴ ارائه شدند. در این فایروال‌ها از فناوری بکار برده شده در سه نسل قبلی استفاده شده است. درواقع این فایروال‌ها می‌توانند عمل فیلترکردن بسته‌ها را در لایه شبکه، نشست و همچنین لایه کاربردی انجام دهند. تنظیم قوانین در این فایروال‌ها کمی پیچیده است و اگر این کار خوب صورت نپذیرد، فایروال قادر به برقراری امنیت نخواهد بود. یکی از مزایای این فایروال‌ها این	کامپیوتری حفاظت می‌کنند. اینگونه فایروال‌ها به کاربران این قابلیت را می‌دهند که بتوانند برای به اشتراک گذاشتن منابع خود از جمله پرینتر و پوشه‌ها در قوانین فایروال تغییرات دلخواه خود را اعمال کنند. در برخی اوقات فایروال‌های نرم‌افزاری امکان تنظیمات محرمانگی و فیلترینگ خاصی را می‌دهند. اینگونه فایروال‌ها در دو نوع شبکه‌ای و تک‌محصولی ارائه می‌شوند. فایروال‌های نرم‌افزاری تحت شبکه می‌توانند یک شبکه را تحت کنترل خود گرفته و از آن محافظت کنند، اما فایروال‌های تک‌محصولی صرفاً بر روی یک سیستم‌عامل نصب می‌شوند و می‌توانند از آن محافظت کنند. هزینه پیاده‌سازی و استفاده از فایروال‌های نرم‌افزاری بسیار کمتر از فایروال‌های سخت‌افزاری است. **نمونه‌هایی از فایروال‌های نرم‌افزاری عبارتند از:** Comodo Internet Security, Glasswire, Intego VirusBarrier, Jetico Personal Firewall, Kaspersky, Internet Security, Lavasoft Personal Firewall, Microsoft Forefront Threat Management Gateway, Norton 360, Online Armor Personal Firewall, Outpost Firewall Pro, PC Tools Firewall Plus, Privacyware Privatefirewall, Sunbelt Personal Firewall, Sygate Personal Firewall, Windows Firewall, ZoneAlarm, Netfilter/iptables Shorewall, PeerBlock, FirewallD, NPF, PF, ipfirewall, IPFilter
فایروال‌های سخت‌افزاری فایروال‌های سخت‌افزاری معمولا به‌صورت زیرساخت‌هایی هستند که توسط شرکت‌های تولیدکننده بر روی بوردهای سخت‌افزاری با سیستم عامل خاص نصب و راه‌اندازی شده‌اند و معمولاً در قالب یک مسیریاب در شبکه فعالیت می‌کنند. یک مسیریاب نیز می‌تواند در یک شبکه به‌عنوان یک فایروال سخت‌افزاری فعالیت کند. در واقع فایروال سخت‌افزاری نیز نوعی فایروال نرم‌افزاری است که بر روی سخت‌افزارها و سیستم‌عامل‌های خاص نصب شده است. فایروال‌های سخت افزاری سرعت و کارایی بیشتری نسبت به فایروال‌های نرم‌افزاری دارند. نمونه‌هایی از فایروال‌های سخت‌افزاری عبارتند از: Check Point, FortiGate, Palo Alto Networks, WatchGuard, Sophos, Cisco Asa Firepower, Cisco PIX, Mcafee Firewall, Juniper SSG, Juniper SRX, Sonicwall, Barracuda Firewall, Cyberoam, D-Link, Endian Firewall, Opendium Iceni, IPCop, pfSense, IPFire, Untangle, Zeroshell, SmoothWall, WinGate, Calyptix Security, Halon Security, Vantronix	

استانداردهای سرویس	مثال
است که زمانی که یک نشست کامل شد، هر پورتی که در آن نشست استفاده شده بسته می‌شود. این فایروال‌ها اجازه میدهند تا نشست‌ها مورد پیگیری قرار گرفته و نشست‌های مجازی برای پروتکل‌هایی نظیر UDP فراهم شود.	
امنیت پست الکترونیکی (Email Security) شامل روش‌ها، استانداردها و پروتکل‌هایی است که جهت افزایش امنیت پست‌های الکترونیکی به‌کار گرفته می‌شوند.	**(Secure/Multipurpose Internet Mail Extensions) S/MIME** استانداردی است که برای رمزنگاری کلید عمومی پست الکترونیکی و حفظ حریم خصوصی پیام‌ها استفاده می‌شود. این سرویس نیازمند مجوز شخص ثالث است. وقتی با این سرویس پیام ارسال می‌شود، در واقع پیام دارای یک امضای دیجیتالی می‌شود و زمانی که پیام به دست گیرنده می‌رسد این امضا با اطلاعات فرستنده پیام تطبیق داده می‌شود تا از هویت شخصی که این پیام را فرستاده، اطمینان حاصل شود.
	(Pretty Good Privacy) PGP یک برنامه رمزنگاری و رمزگشایی است که جهت احراز هویت و رمزنگاری داده‌ها استفاده می‌شود. از PGP معمولاً برای رمزنگاری، رمزگشایی و امضای پست‌های الکترونیکی و افزایش امنیت ارتباطات از طریق پست الکترونیکی استفاده می‌شود. OpenPGP استانداردی است که کارگروه مهندسی اینترنت (IETF) برای همین منظور ارائه کرده است.
	(DomainKeys Identified Mail) DKIM روشی است که برای احراز هویت در پست‌های الکترونیکی و تشخیص پیام‌های با فرستنده غیرمجاز استفاده می‌شود.

استانداردهای سرویس	مثال
امنیت آی‌پی **(IP Security)** شامل پروتکل‌ها و استانداردهایی است که برای تبادل امن بسته‌ها (Packets) در لایه IP استفاده می‌شوند.	**(Internet Protocol Security) IPsec** پروتکل IPSec شامل مجموعه‌ای از پروتکل‌ها است که تبادل امن بسته‌ها در لایه IP را پشتیبانی می‌کنند. IPSec به‌طور گسترده در فناوری شبکه‌های مجازی خصوصی جهت احراز هویت، محرمانگی، یکپارچگی و مدیریت کلید در شبکه های مبتنی برIP مورد استفاده قرار می‌گیرد. IPSec امنیت ارتباطات را در بطن شبکه با کمک سرویس‌های امن رمزنگاری برقرار می‌کند. برای عملکرد صحیح و کامل IPSec، هر دو طرف فرستنده و گیرنده باید یک کلید عمومی را به اشتراک بگذارند که به‌واسطه استفاده از پروتکل "مدیریت کلید" عملی می‌شود. این پروتکل به گیرنده این اجازه را می‌دهد تا یک کلید عمومی را به دست آورده و فرستنده را بر اساس امضای دیجیتال احراز هویت نماید.
فناوری کلید عمومی **(Public Key Technology)** شامل استانداردها، نرم‌افزارها و سرویس‌هایی است که مرکز صدور گواهی دیجیتال (Certificate Authority(CA)) از آنها برای تولید کلیدها و گواهی‌های دیجیتال استفاده می‌کنند. این کلیدها و گواهی‌های دیجیتال دسترسی امن به اطلاعات را فراهم می‌کنند.	**X.509** X.509 یک استاندارد ITU-T است که به طور گسترده برای تعریف گواهی دیجیتال در زیرساخت کلید عمومی (PKI) استفاده می‌شود. این استاندارد فرمت گواهی کلید عمومی، لیست گواهی‌های لغوشده، ویژگی گواهی‌ها و روش اعتبارسنجی مسیر گواهی را مشخص می‌کند. تاکنون سه نسخه از این استاندارد منتشر شده است. این استاندارد برای اولین بار در سال ۱۹۸۸ به‌عنوان قسمتی از استاندارد سرویس‌های دایرکتوری ITU X.500 منتشر شد. این استاندارد در سال ۱۹۹۳ مورد بازبینی مجدد قرار گرفت و به ساختار آن دو فیلد اضافه و به‌عنوان نسخه دوم منتشر شد. هدف از افزودن این دو فیلد، پشتیبانی از کنترل دسترسی به دایرکتوری بود. این استاندارد سپس مورد بازبینی مجدد قرار گرفت و در RFC2459 به ساختار آن تعدادی فیلد توسعه افزوده و سپس به‌عنوان نسخه سوم منتشر شد. هدف از افزودن این فیلدهای توسعه، ذخیره کردن اطلاعات اضافی در مورد گواهی دیجیتال مثل کاربردهای آن است. به طور کلی در حال حاضر اصطلاح X.509 تنها برای نسخه سوم این گواهی به کار می‌رود. تاکنون برای نسخه سوم این گواهی چندین RFC از جمله RFC 4325، RFC 4630 و RFC 5280 منتشر شده است. در هر یک از این‌RFCها تعدادی فیلد توسعه به استاندارد X.509 افزوده شده است. پروتکل‌ها و استانداردهای ذیل از X.509 پشتیبانی می‌کنند: TLS/SSL, S/MIME , IPsec, SSH, HTTPS, EAP, LDAP, Trusted Computing Group, CableLabs, WS-Security, XMPP, Microsoft Authenticode, OPC UA

استانداردهای سرویس	مثال
	(Online Certificate Status Protocol) OCSP پروتکل تعیین وضعیت گواهی برخط (OCSP) یک پروتکل اینترنت برای پی بردن به وضعیت ابطال یک گواهی دیجیتال X.509 است. این پروتکل در RFC6960 تعریف شده است و در قسمت استانداردهای اینترنت جای دارد. پروتکل OCSP به‌عنوان جانشینی برای لیست ابطال گواهی(CRL) مطرح می‌باشد.
	(Server-based Certificate Validation Protocol) SCVP پروتکل معتبرسازی گواهینامه مبتنی بر خدمتگزار (SCVP) یک پروتکل اینترنتی است که هم مسیر بین یک گواهینامه دیجیتال X.509 و یک ریشه مورد اعتماد را تعیین می‌نماید و هم اعتبار مسیر را با توجه به سیاست معتبرسازی مشخص تعیین می‌نماید.
تشخیص و جلوگیری از نفوذ **(Intrusion Detection & Prevention)** سیستم‌های جلوگیری از نفوذ که با نام سیستم‌های تشخیص و جلوگیری از نفوذ هم شناخته می‌شوند، ابزاری برای امنیت شبکه هستند که فعالیت‌های موجود در شبکه یا سیستم را برای تشخیص و جلوگیری از فعالیت‌های مخرب تحت نظر می‌گیرند. وظایف اصلی یک سیستم جلوگیری از نفوذ شامل شناسایی فعالیت‌های مخرب، ثبت اطلاعات در مورد این فعالیت‌ها، اقدام به مسدود و متوقف کردن این فعالیت‌ها و ثبت گزارش کارهای انجام شده توسط خود سیستم می‌شوند. سیستم‌های جلوگیری از نفوذ حالت ارتقاء یافته سیستم‌های تشخیص نفوذ محسوب می‌شوند، چرا که هر دو این سیستم‌ها فعالیت‌های شبکه و یا سیستم را برای یافتن فعالیت‌های مخرب نظارت می‌کنند. تفاوت اصلی این سیستم‌ها با سیستم‌های تشخیص نفوذ در این است که این سیستم‌ها می‌توانند به‌صورت فعال مانع از فعالیت‌های مخرب شده یا آنها را متوقف کنند. به‌طور دقیق‌تر می‌توان گفت که یک سیستم جلوگیری از نفوذ توانایی انجام کارهایی مانند ارسال هشدار، دور ریختن بسته‌های مخرب، مسدود کردن ارتباط از طرف آدرس‌های متخاصم را دارد. این سیستم‌ها همچنین توانایی اصلاح خطاهای CRC ، اصلاح ترتیب بسته‌ها، جلوگیری از مسائل ترتیب بسته TCP و پاکسازی گزینه‌های ناخواسته در لایه انتقال و شبکه را دارند. سیستم‌های جلوگیری از نفوذ به چهار نوع سیستم‌های جلوگیری از نفوذ مبتنی بر شبکه (NIPS)، سیستم‌های جلوگیری از نفوذ بی‌سیم (WIPS)،	**ابزارهای تشخیص و جلوگیری از نفوذ** تعدادی از ابزارهایی که برای تشخیص و جلوگیری از نفوذ مورد استفاده قرار می‌گیرند در ذیل آمده است. برای انواع مختلفی همچون NIPS، WIPS، NBA و HIPS ابزارهای مختلف دیگری نیز وجود دارد. ▪ DefensePro ▪ Kismet ▪ ACARM-ng ▪ AIDE ▪ Bro NIDS ▪ Fail2ban ▪ OSSEC HIDS ▪ Prelude Hybrid IDS ▪ Samhain ▪ Snort ▪ Suricata ▪ McAfee Network Security Manager ▪ Pytbull ▪ IBM Security Network Intrusion Prevention System ▪ IPS-1 ▪ TippingPoint IPS ▪ Strata Guard ▪ StoneGate IPS ▪ iPolicy Intrusion Prevention Firewall ▪ ParsIPS ▪ Dragon IPS ▪ Sourcefire Next Generation IPS

استانداردهای سرویس	مثال
تجزیه و تحلیل رفتار شبکه (NBA)، سیستم‌های جلوگیری از نفوذ مبتنی بر میزبان (HIPS) تقسیم می‌شوند. اکثر ابزارهای جلوگیری از نفوذ از یکی از سه روش مبتنی بر امضاء، مبتنی بر آنومالی آماری و تجزیه و تحلیل پروتکل مبتنی بر حالت استفاده می‌کنند.	
پویشگر آسیب‌پذیری **(Vulnerubility Scanner)** پویشگر آسیب‌پذیری یک برنامه کامپیوتری است که به‌منظور دسترسی به ضعف‌های برنامه‌های کاربردی، شبکه‌ها و سیستم‌های کامپیوتری طراحی شده است. انواع مختلفی از پویشگرهای آسیب‌پذیری وجود دارد که با توجه به اهداف ویژه‌ای که بر روی آن تمرکز دارند، از یکدیگر متمایز می‌شوند. در حالی که عملکردها بین انواع مختلف پویشگرهای آسیب‌پذیری، تفاوت ایجاد می‌کند اما همه آنها در یک هدف اصلی با هم مشترک هستند و آن برشمردن آسیب‌های موجود در یک یا چند هدف است. پویشگرهای آسیب‌پذیری از اجزای اصلی مدیریت آسیب‌پذیری هستند. این پویشگرها نرم‌افزارهایی هستند که یک پایگاه‌داده بزرگ از کدهای مخرب برای آسیب‌پذیریهای شناخته شده دارند و آنها را با سرعت زیادی به ترتیب روی هدف مورد نظر تست کرده و آسیب‌های موجود را شناسایی می‌کنند. شناسایی آسیب‌ها کمک می‌کند که نفوذهایی که از این آسیب‌ها استفاده می‌کنند را تست کرده و زمینه مقابله با آسیب‌پذیری‌ها و نفوذهای ناشی از آنها را فراهم کنیم. شناسایی آسیب‌پذیری‌ها می‌تواند به‌صورت کاملاً خودکار توسط پویشگرهای آسیب‌پذیری صورت گیرد، درحالیکه تست نفوذ (Penetration Test) پیچیده‌تر بوده و علاوه بر استفاده از ابزارهای پویشگر آسیب‌پذیری نیاز به دخالت عوامل انسانی مجرب و آگاه در این زمینه دارد.	**ابزارهای پویشگر آسیب‌پذیری** تعدادی از ابزارهایی که برای شناسایی آسیب‌پذیری و تست نفوذ مورد استفاده قرار می‌گیرند در ذیل آمده است. برای موارد مختلفی همچون کاربردهای وب، شبکه، پورتها و غیره ابزارهای مختلف دیگری نیز وجود دارد. ▪ Acunetix ▪ Aircrack-ng ▪ Arachni ▪ Back Track ▪ BeEF ▪ Burpsuite ▪ Cain & Abel ▪ Canvas ▪ CORE Impact ▪ Dradis ▪ Ettercap ▪ HconSTF ▪ Hydra ▪ IBM AppScan ▪ IronWASP ▪ John The Ripper ▪ Metasploit ▪ Nagios ▪ Nessus ▪ Netsparker ▪ Nikto ▪ Nmap ▪ OpenVAS ▪ PunkSPIDER(scanner powered by PunkSCAN) ▪ Retina ▪ SATAN ▪ Secunia PSI ▪ SHODAN ▪ Social Engineer Toolkit ▪ Sqlmap ▪ Sqlninja ▪ Veracode ▪ w3af ▪ WebScarabNG ▪ Wireshark ▪ Zed Attack Proxy (ZAP)

استانداردهای سرویس	مثال
دایرکتوری سرویس (Directory Service) دایرکتوری سرویس شامل پروتکل‌ها و استانداردهایی است که امکان ذخیره‌سازی و سازمان‌دهی اطلاعات مربوط به کاربران و منابع یک شبکه کامپیوتری را فراهم کرده و به مدیر شبکه این امکان را می‌دهند که دسترسی کاربران به منابع شبکه را مدیریت نماید. دایرکتوری سرویس در عین حال به‌عنوان یک لایه محافظ بین کاربران و منابع مشترک شبکه عمل می‌کند. دایرکتوری سرویس‌ها معمولاً از اجزای اصلی در طراحی امنیت سیستم‌های اطلاعاتی می‌باشند و به همین دلیل دارای ساختار بسیار دقیقی در خصوص کنترل دسترسی هستند. هریک از منابع در شبکه به‌عنوان یک شئ در دایرکتوری سرویس محسوب می‌گردند. اطلاعات مربوط به هر منبع شبکه تحت عنوان خصیصه شئ مربوط به آن منبع در دایرکتوری سرویس ذخیره می‌شود. سطح امنیت اطلاعات هر شئ می‌تواند به نحوی تعیین شود که فقط کاربرانی قابلیت دسترسی به آنها را داشته باشند که دارای مجوز لازم هستند.	**پروتکل LDAP (Lightweight Directory Access Protocol)** پروتکلی است که برای دسترسی و به‌روزرسانی دایرکتوری‌های توزیع‌شده مورد استفاده قرار می‌گیرد. این پروتکل مجموعه‌ای از پروتکل‌ها و روش‌ها، برای دسترسی به اطلاعات شاخه‌های توزیع‌شده است. پروتکل LDAP از استانداردهای موجود در X.500 پیروی می‌کند و بر خلاف X.500 از TCP/IP پشتیبانی می‌کند که برای استفاده از اینترنت مفید است. پروتکل LDAP سبک‌تر از X.500 است و به همین دلیل گاهی به آن X.500 Lite نیز گفته می‌شود. این پروتکل در سال ۱۹۹۰ توسط کارگروه مهندسی اینترنت (IETF) عرضه شد، تا پیاده‌سازی X.500 در پست الکترونیکی را آسان نماید. LDAP یک پروتکل ارتباطی را مشخص می‌کند که در آن یک پیام از سرویس‌گیرنده، برای استفاده و دسترسی به اطلاعات یک دایرکتوری X.500، به سرویس‌دهنده ارسال می‌گردد. اکثر سرویس دهندگاه LDAP از نسخه ۳,۰ آن استفاده می‌کنند. دایرکتوری‌ها اغلب با یک مدل ارتباطی خدمتگزار- مشتری قابل دسترسی هستند. برنامه‌ای که در خواست خواندن، یا ایجاد تغییر در دایرکتوری را دارد، به طور مستقیم نمی‌تواند چنین کاری را انجام بدهد بلکه با استفاده از یک سرویس میانی قادر به انجام این کار خواهد بود. به این صورت که یک API فراخوانی می‌شود و آن API ، پیامی به یک فرآیند دیگر می‌فرستد و آن فرآیند با استفاده از TCP/IP به اطلاعات دسترسی خواهد داشت. پورت استاندارد برای ارتباط امن، پورت ۶۳۶ و برای حالت عادی ۳۸۹ است. تلاش برای استفاده از XML در LDAP و استفاده در وب سرویس‌ها، منجر به زبانی به نام DSML شده است. این زبان به استفاده کنندگان از دایرکتوری‌ها این امکان را می‌داد، که بدون نوشتن Interface برای کار با APIهای مربوطه، به دایرکتوری‌ها دسترسی داشته و بتوانند با آنها کار کنند. **ابزارهای LDAP به‌صورت نرم‌افزارهای مشتری:** Admin4, Apache Directory Server/Studio, COGNITUM , FusionDirectory, Jxplorer, JXWorkBench, LDAP Account Manager, phpLDAPadmin, SLAMD, RoundCube, Teleform, Kofax Capture, web2ldap, Gosa, Atlassian Crowd, LDAP Admin Tool, Evolution, KAddressBook, Ldapscripts, Contacts, Directory Utility, Workgroup Manager, Active Directory Explorer, LDAP Admin, LDAP Administrator, Veeam Explorer for Microsoft Active Directory, Powershell, Softerra Adaxes **ابزارهای LDAP به‌صورت نرم‌افزارهای خدمتگزار:**

استانداردهای سرویس	مثال
	389 Directory Server, Active Directory, Apache Directory Server, Apple Open Directory, CA Directory, Critical Path Directory Server, DirX Directory, FreeIPA, IBM Tivoli Directory Server, ldapjs, Mandriva Directory Server, Nexor Directory, NetIQ eDirectory, OpenBSD ldapd, OpenDJ , OpenDS, OpenLDAP, Smart User Repository, Oracle Directory Server Enterprise Edition, Oracle Internet Directory, Oracle Unified Directory, RadiantOne, Red Hat Directory Server, Samba4 , Slapd , Sun Java System Directory Server, UnboundID Directory Server, Univention Corporate Server, ViewDS Directory Server, Virtual Identity Server **ابزارهای LDAP به‌صورت میان‌افزار:** Json2Ldap, Rest2LDAP, DSML gateway
انتقال امن **(Secured Transport)** شامل پروتکل‌های امنیتی است که در لایه انتقال شبکه استفاده می‌شوند و انتقال امن اطلاعات بر روی شبکه و اینترنت را فراهم می‌کنند.	**پروتکل‌های SSL/TLS** لایه سوکت‌های امن SSL (Secure Sockets Layer) پروتکلی است که توسط شرکت Netscape برای ارسال و دریافت سندهای خصوصی از طریق اینترنت توسعه یافته است. SSL از یک کلید خصوصی برای رمزنگاری اطلاعاتی که بر روی یک ارتباط SSLمنتقل می‌شوند استفاده می‌نماید. پروتکل امنیتی لایه انتقال TLS (Transport Layer Security) بر پایه SSL بنا شده است. پروتکل TLS توسط IETF برای رمزنگاری ارتباطات انتها به انتها استاندارد شده است. هدف از استفاده TLS در لایه انتقال، امن نمودن تراکنش‌های ارتباطی در لایه کاربرد است. TLS برای اطمینان از هویت طرف مقابل و تبادل کلید متقارن از گواهی X.509 و رمزنگاری نامتقارن استفاده می‌کند. این پروتکل امنیت انتقال داده‌ها را در اینترنت برای مقاصدی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی، پیام‌های فوری اینترنتی و صدا بر روی IP فراهم می‌کند. اکثر وب‌گاه‌ها برای امن کردن ارتباطات بین خدمتگزارانشان و مرورگرهای وب از پروتکل TLS استفاده می‌کنند. پروتکل‌های TLS و SSL در لایه انتقال استفاده می‌شوند و می‌توانند در شبکه‌های سیار و سیمی پیاده‌سازی شوند.
امنیت XML **(XML Security)** شامل استانداردها، پروتکل‌ها و ابزارهایی است که یک چارچوب مشترک و قوانین پردازشی مناسب برای پاسخگویی	**Xenc (XML encryption)** استاندارد Xenc توسط کنسرسیوم وب جهان‌گستر (W3C) و کارگروه مهندسی اینترنت (IETF) برای رمزنگاری اسناد XML و فراهم کردن محرمانگی در این اسناد ارائه شده است. این استاندارد این امکان را فراهم می‌کند که تنها بخش‌های حساس رمز شده و هر بخش نیز

استانداردهای سرویس	مثال
به نیازهای امنیتی XML تعریف می‌کنند. این استانداردها و ابزارها مفاهیم و فناوری‌های امنیت و رمزنگاری و همچنین فناوری‌های XML را با هم یکپارچه کرده تا راهکاری عملی، قابل‌گسترش و انعطاف‌پذیر برای پاسخگویی به نیازهای امنیتی فراهم کنند.	توسط کلید جداگانه‌ای رمز گردد.
	(XML signatures) XML-SIG استانداردهای مبتنی بر XML است که توسط کنسرسیوم وب جهان‌گستر (W3C) برای امضاهای دیجیتال و صحت اسناد XML مورد استفاده قرار می‌گیرند.
	(XML-Key Management Specification) XKMS استانداردهای مبتنی بر XML است که توسط کنسرسیوم وب جهان‌گستر (W3C) برای توزیع و ثبت کلیدهای عمومی (Public Key) مورد استفاده قرار می‌گیرند.
	(Security Assertion Markup Language) SAML زبان SAML (زبان نشانه‌گذاری توافق امنیتی) زبانی استاندارد مبتنی بر XML است که برای تبادل داده‌های احراز هویت (Authentication) و مجازشماری (Authorization) بین بخش‌های مختلف مورد استفاده قرار می‌گیرد. SAML توسط کمیته فنی سرویس‌های OASIS تولید شده است.
	(eXtensible Access Control Markup Language) XACML زبان XACML (زبان نشانه‌گذاری کنترل دسترسی قابل گسترش) زبانی استاندارد است که برای تعریف سیاست‌های کنترل دسترسی خصوصیت‌مبنا (Attribute-based) مورد استفاده قرار می‌گیرد. از اهداف XACML افزایش تعامل‌پذیری بین پیاده‌سازی‌های کنترل دسترسی است که توسط تولیدکننده‌های مختلف ارائه می‌شود. این زبان توسط سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) ارئه شده است.
	IBM alphaWorks XML Security ابزاری است که شرکت IBM برای فراهم کردن سازوکار کنترل دسترسی در اسناد XML ارائه کرده است.
	Phaos XML Security Suite ابزاری است که شرکت Paos برای فراهم کردن امضای دیجیتال و رمزنگاری در اسناد XML ارائه کرده است.
	WS-Security & WS-Trust توسعه‌ای از پروتکل SOAP است که برای امنیت وب‌سرویس‌ها از XML-SIG و Xenc استفاده می‌کند. استاندارد WS-Trust نیز توسعه‌ای از استانداردهای خانواده WS-Security است که چارچوبی برای درخواست و ارسال امن نشانواره (Token) در ارتباطات وب‌سرویس ارائه می‌دهد.

استانداردهای سرویس	مثال
امنیت از راه دور (Remote Security) شامل روش‌ها یا پروتکل‌هایی است که میان دو کامپیوتر یک ارتباط امن و غیر قابل نفوذ ایجاد می‌کنند. این روش‌ها و پروتکل‌ها امکان احراز هویت را بین دو کامپیوتر راه دور فراهم کرده و دو کامپیوتر می‌توانند بر روی یک شبکه یا اینترنت اطلاعات را به‌صورت رمزشده و غیر قابل شنود مبادله کنند. در واقع این روش‌ها و پروتکل‌ها تمام امکاناتی که پروتکل Telnet فراهم می‌کند را به‌صورت امن در اختیار کاربران قرار می‌دهند.	**(Secure Shell) SSH** پوسته امن (SSH) یک پروتکل اینترنتی است که امکان تبادل اطلاعات با استفاده از یک کانال امن را بین دو دستگاه متصل در شبکه ایجاد می‌کند. دو نسخه اصلی این پروتکل به نام‌های SSH1 و SSH2شناخته می‌شود. در ابتدا بر روی سیستم‌های مبتنی بر یونیکس و لینوکس برای دسترسی به حساب‌های پوسته استفاده شد. SSH جایگزینی برای Telnet و سایر پوسته‌های ارتباط از راه دور غیر امن ایجاد شده است. هربار که داده‌ای از طرف کامپیوتر به شبکه فرستاده می‌شود، به‌صورت خودکار توسط SSH رمزنگاری می‌شود. هنگامی که داده به مقصد خود می‌رسد به‌صورت خودکار رمزگشایی می‌شود. نتیجه‌ای که خواهد داشت رمزنگاری نامرئی خواهد بود. بدین صورت کاربران نهایی درگیر پروسه رمزنگاری و رمزگشایی نخواهند شد و از ارتباط امن خود می‌توانند به خوبی استفاده کنند. امنیت سیستم رمزنگاری SSH با استفاده از الگوریتم‌های پیچیده و مدرن تضمین می‌شود. تا آنجا که امروزه در سیستم‌های حیاتی و بسیار حساس از این سیستم استفاده می‌شود. به‌صورت معمول محصولاتی که از SSH استفاده می‌کنند از دو بخش خدمتگزار و مشتری تشکیل می‌شوند. مشتری با استفاده از تنظیمات خدمتگزار مربوطه به آن وصل می‌شوند و خدمتگزار وظیفه تأیید هویت و قبول یا رد ارتباط را به عهده دارد. تشابه نامSecure Shell با محیط‌هایی مانند Bourne shell و یا C Shell نشان دهنده این نیست که SSH نیز محیطی است که وظیفه تفسیر فرامین برای سیستم‌عامل را بر عهده دارد. **ابزارهای پشتیبانی کننده از مشتری SSH:** Admin Hands, AbsoluteTelnet, Bitvise SSH, Client/Tunnelier, Cisco CLI Analyzer, ConnectBot, CRAX Commander, DameWare, Dropbear, JuiceSSH, MindTerm, MobaXterm, eSSH Client, Private Shell, ProxyCap, lsh, OpenSSH, PACManager, PenguiNet, PuTTY, Reflection for Secure IT, Salt, SecureCRT, ShellCraft, SSH Tectia Client/ConnectSecure, SunSSH, Terminals CodePlex, Tera Term, TN3270 Plus, Token2Shell, TtyEmulator, Win32-OpenSSH, Xshell, ZOC Terminal **ابزارهای پشتیبانی کننده از خدمتگزار SSH:** Apache MINA SSHD, Bitvise SSH Server (formerly WinSSHD), Copssh, CrushFTP Server, Dropbear, freeSSHd SSH Server, GoAnywhere MFT, KpyM SSH Server, lsh, Maverick Legacy Server, MobaSSH SSH Server, OpenSSH, Pragma Fortress SSH Server, Tectia SSH Server, PowerShell Server, SilverSHielD, Georgia

استانداردهای سرویس	مثال
	SoftWorks SSH Server, Syncplify.me Server, TinySSH, SFTPPlus
سایر مؤلفه‌های امنیت **(Other Security Components)** شامل پروتکل‌ها و مؤلفه‌هایی است که استفاده از آنها برای رسیدن به اهداف امنیتی همچون محرمانگی، صحت داده‌ها و قابلیت‌دسترسی الزامی است. این پروتکل‌ها و مؤلفه‌ها با توجه به استانداردهای امنیتی و اسناد راهبردی در زمینه امنیت فضای تولید و تبادل اطلاعات ایران قابل استخراج است.	**مدیریت شناسه و دسترسی** شامل سطح گسترده‌ای از محصولات، برنامه‌های کاربردی، سکوها و مؤلفه‌هایی است که شناسایی و اطلاعات وابسته به موجودیت‌ها (شامل افراد، برنامه‌های کاربردی و سخت‌افزارها) را مدیریت کرده و امکان دسترسی موجودیت‌های مجاز به منابع صحیح در زمانی صحیح و بنا به دلایلی صحیح را فراهم می‌کنند. احراز هویت، مجازشماری، مدیریت رمزعبور، شناسایی یگانه، دایرکتوری سرویس، کارت‌های دیجیتال، شناسه‌های دیجیتال، توکِن‌های امنیتی، پروتکل SAML، WS-Security، WS-Trust و OAuth نمونه‌های از فناوری‌ها و استانداردهای مرتبط با مدیریت شناسه و دسترسی هستند.
	محرمانگی شامل مؤلفه‌هایی است که برای حفاظت داده‌های ارسال شده در مقابل حملات غیرفعال مورد استفاده قرار می‌گیرند. بدین ترتیب پیام به شکلی ساخته و ارسال می‌شود که فقط توسط گیرنده‌های مورد نظر قابل شناسایی و خواندن باشد. این مؤلفه‌ها می‌توانند برای حفاظت از جریان ترافیک در مقابل تحلیل نیز مورد استفاده قرار گیرند. این کار مستلزم این است که حمله‌کننده نتواند مبداء، مقصد، تعداد دفعات ارسال پیام، یا سایر ویژگی‌های ترافیک را در امکانات ارتباطی مشاهده نماید. در بحث محرمانگی ارتباطات باید فقط "فرستنده" و "گیرنده مورد نظر فرستنده" قادر باشند به محتوای اطلاعات رد و بدل شده دست یابند و آن را بفهمند. برای جلوگیری از حملات احتمالی، نظیر استراق سمع، می‌توان داده‌های ارسالی را رمزنگاری کرد.
	الگوریتم رمزنگاری شامل الگوریتم‌ها و توابع ریاضی است که در پروتکل‌های رمزنگاری مورد استفاده قرار می‌گیرند. این الگوریتم‌ها و توابع را می‌توان به‌صورت

استانداردهای سرویس	مثال
	زیر دسته‌بندی کرد: ▪ توابع بدون کلید (توابع درهم‌ساز و تبدیل‌های یک‌طرفه) ▪ توابع مبتنی بر کلید (الگوریتم‌های کلید متقارن مانند 3DES و AES، الگوریتم‌های کلید نامتقارن مانند RSA و الگوریتم‌های امضای دیجیتال)

۲-۴ حوزه زیرساخت و سکوی سرویس

حوزه زیرساخت و سکوی سرویس(Infrastructure and Platform Area) شامل مجموعه‌ای از سکوهای تحویل و پشتیبانی، زیرساخت‌ها و نیازمندی‌های سخت‌افزاری است که برای پشتیبانی از ساخت، نگهداشت و قابلیت‌دسترسی مؤلفه‌های سرویس مورد نیاز هستند.

پایگاه‌داده/ذخیره‌سازی (Database/Storage)

پایگاه‌داده/ذخیره‌سازی شامل برنامه‌هایی است که برای ذخیره‌سازی، تغییر و استخراج اطلاعات از پایگاه‌داده‌ها مورد استفاده قرار می‌گیرند. این طبقه روش‌ها و دستگاه‌هایی که برای ذخیره‌سازی حجم عظیمی از داده‌ها مورد استفاده قرار می‌گیرند را نیز شامل می‌شود.

جدول ۲-۱۳ مثال‌هایی از پایگاه‌داده‌ها و دستگاه‌های ذخیره‌سازی

استانداردهای سرویس	مثال
پایگاه‌داده‌ها (Databases) شامل مجموعه‌ای از اطلاعات سازماندهی شده است، به‌طوریکه برنامه‌های کامپیوتری می‌توانند به سرعت هر داده دلخواهی را در آن انتخاب کرده و مورد استفاده قرار دهند. سیستم‌های مدیریت پایگاه‌داده (DBMS) کاربردهای نرم‌افزاری هستند که ابزارهایی را برای دسترسی، ذخیره‌سازی، مدیریت، تحلیل و بالا بردن کارایی پایگاه‌داده‌ها فراهم می‌کنند.	**RDBMS (Relational Database Management System)** یک سیستم مدیریت پایگاه‌داده رابطه‌ای (RDBMS) سیستمی است که داده را طبق مدل رابطه‌ای مدیریت می‌کند. مدل رابطه‌ای در سال ۱۹۷۰ توسط ریاضیدانی به نام Edgar.F.Codd طراحی شد. مدل داده پیشنهادی یک مدل منطقی بر مبنای ریاضیات است که از منطق گزاره‌ها و تئوری مجموعه‌ها به‌عنوان زیربنا استفاده شده است. یک پایگاه داده رابطه‌ای پایگاه‌داده‌ای است که با مدل رابطه‌ای مطابقت داشته باشد و به‌صورت مجموعه‌ای از جدول‌هایی که از دید کاربر قابل درک هستند دیده می‌شود. سیستم‌های مدیریت پایگاه‌داده رابطه‌ای پرکاربرد عبارتند از: ▪ Oracle Database ▪ Microsoft SQL Server ▪ MySQL (Oracle Corporation) ▪ IBM DB2 ▪ IBM Informix ▪ SAP Sybase Adaptive Server Enterprise ▪ SAP Sybase IQ ▪ Teradata
	OODBMS (Object-Oriented DBMS) یک سیستم مدیریت پایگاه‌داده شئ‌گرا (OODBMS) سیستمی است که در آن اطلاعات به‌صورت اشیاء (همانند زبان‌های برنامه‌سازی شئ‌گرا) بازنمایی می‌شود. این سیستم‌ها متفاوت از سیستم‌های مدیریت پایگاه‌داده رابطه‌ای است که مبتنی بر جداول هستند. برخی از

استانداردهای سرویس	مثال
	سیستم‌های مدیریت پایگاه‌داده شئ‌گرا عبارتند از: ▪ caché ▪ ConceptBase ▪ Db4o ▪ GemStone/S ▪ NeoDatis ODB ▪ ObjectDatabase++ ▪ ObjectDB ▪ Objectivity/DB ▪ ObjectStore ▪ ODABA ▪ OpenAccess ▪ OpenLink Virtuoso ▪ Perst ▪ Picolisp ▪ siaqodb ▪ Twig ▪ VelocityDB ▪ Versant Object Database / JPA / FastObjects ▪ Volante ▪ WakandaDB ▪ Zope Object Database
	(Object-Relational DBMS) ORDBMS یک سیستم مدیریت پایگاه‌داده شئ‌گرا–رابطه‌ای (ORDBMS) ترکیبی از دو سیستم مدیریت پایگاه داده رابطه‌ای و شئ‌گرا است. ORDBMS در واقع یک سیستم مدیریت پایگاه‌داده رابطه‌ای است که مفاهیم شئ‌گرا (مانند کلاس، شئ، وراثت) به‌صورت مستقیم در شماها و درخواست‌های آن پشتیبانی می‌شود. برخی از سیستم‌های مدیریت پایگاه‌داده شئ‌گرا–رابطه‌ای عبارتند از: ▪ Adaptive Server Enterprise ▪ CUBRID ▪ DB2 ▪ Greenplum Database ▪ Informix ▪ Caché ▪ Microsoft SQL Server ▪ Oracle Database ▪ PostgreSQL ▪ OpenEdge Advanced Business Language Virtuoso Universal Server ▪ VMDS (Version Managed Data Store) ▪ WakandaDB ▪ Zope Object Database
دستگاه‌ها و سیستم‌های ذخیره‌سازی (Storage Devices and Systems)	**(Network Attached Storage) NAS** دستگاه NAS (ذخیره‌سازی پیوست‌شده به شبکه) مجموعه‌ای از هارد دیسک‌ها است که از قابلیت ذخیره‌سازی اطلاعات در قالب

استانداردهای سرویس	مثال
دستگاه‌ها و سیستم‌هایی هستند که برای فراهم کردن دسترسی به ذخیره‌سازی‌های مشترک بر روی شبکه طراحی شده‌اند. این دستگاه‌ها قابلیت‌های توسعه‌داده شده‌ای را با هزینه کم نسبت به خدمتگزارهای فایل (File Servers) **برای شبکه فراهم می‌کنند.**	پروتکل‌های ذخیره‌سازی NFS و CIFS پشتیبانی می‌کند. کلیه دستگاه‌های NAS با استفاده از ساختار آدرس IP قابل دسترس هستند و در واقع همیشه به یک شبکه مبتنی بر پروتکل TCP/IP و دارای آدرس IP متصل می‌شوند. با توجه به اینکه پروتکل‌های دسترسی به NASپروتکل‌های مبتنی بر فایل هستند، مشتری‌ها به فایل‌ها و منابعی که بر روی NAS قرار می‌گیرد در قالب فایل و تحت شبکه دستری پیدا می‌کنند. از NAS برای مدیریت متمرکز فایل‌های سازمانی استفاده می‌شود. با توجه به ذخیره‌سازی اشتراکی که به‌صورت شبکه‌ای فراهم می‌شود، پیچیدگی‌های مدیریتی خدمتگزارهای فایل کاهش پیدا کرده، محدودیت فضای روی دیسک‌های محلی کاهش پیدا کرده، ساختار ذخیره‌سازی اطلاعات بهبود پیدا می‌کند. NAS ها معمولاً از نظر اندازه کوچکتر از SANها هستند و تعداد هارد دیسک‌های کمتری دارند.
	(Storage Area Network) SAN بر خلاف NASها در دستگاه‌های ذخیره‌سازی SAN پروتکل‌های دسترسی بر اساس فایل نیست و بر اساس دسترسی سطح بلوکی (Block Level Access) ایجاد می‌شوند. نمونه‌هایی از این پروتکل‌های دسترسی iSCSI و Fiber Channel هستند که دسترسی به اطلاعات در شبکه در قالب بلوک‌های اطلاعاتی را فراهم می‌کنند. دستگاه‌هایی که با استفاده از ساختار دسترسی سطح بلوکی به SAN دسترسی پیدا می‌کنند خودشان فایل‌ها و سیستم فایل خودشان را مدیریت می‌کنند. SAN در واقع خودش یک شبکه است. شبکه‌ای که تمام مخازن ذخیره‌سازی و خدمتگزارها را به هم متصل می‌کند.
	هَدوپ(Hadoop) هدوپ یک نرم افزار متن باز تحت لیسانس آپاچی است که با جاوا برنامه‌نویسی شده و برای تقسیم بندی و توزیع فایل‌های متمرکز به‌کار می‌رود. این نرم‌افزار چارچوبی را برای پردازش توزیع‌شده روی مجموعه‌ای از داده‌های حجیم فراهم می‌کند و این عملیات توسط یک مدل برنامه‌نویسی ساده بر روی سیستم خوشه‌ای (Clustering) انجام می‌گیرد. طراحی این نرم‌افزار به‌شکلی است که می‌تواند بر روی هزاران سرور محاسبات یا عملیات ذخیره‌سازی اطلاعات را به‌صورت محلی انجام دهد. هَدوپ شامل یک سیستم فایل توزیع شده با قابلیت گسترش(HDFS) است که بتواند داده‌های در اندازه پتابایت را پشتیبانی نماید و یک موتور با قابلیت مقیاس‌پذیری بسیار بالا (MapReduce) که نتایج را به‌صورت دسته‌ای محاسبه نماید.

خدمتگزارهای تحویل (Delivery Servers)

خدمتگزارهای تحویل سکوهایی هستند که اطلاعات را برای برنامه‌های کاربردی درخواست‌کننده فراهم می‌کنند. این سکوها شامل سخت‌افزارها، سیستم‌عامل‌ها، نرم‌افزارهای خدمتگزار و پروتکل‌های شبکه می‌شود.

جدول ۲-۱۴ مثال‌هایی از خدمتگزارهای تحویل

استانداردهای سرویس	مثال
خدمتگزار وب **(Web Server)** خدمتگزارهای وب کامپیوترهایی هستند که سرویس‌های وب جهانی را بر روی اینترنت فراهم می‌کنند. این خدمتگزارها شامل سخت‌افزارها، سیستم‌عامل‌ها، نرم‌افزارهای خدمتگزار وب، پروتکل‌های TCP/IP و محتوای وب (صفحه وب) هستند. اگر خدمتگزار وب به‌صورت محلی مورد استفاده قرار بگیرد و به‌صورت عمومی نباشد، ممکن است به‌عنوان خدمتگزار اینترانت (Interanet Server) شناخته شود.	**Apache** Apache یک خدمتگزار وب متن باز است که توسط گروهی از برنامه‌سازان با نام گروه Apache گسترش یافته است. اولین نسخه Apache در سال ۱۹۹۵ توسعه پیدا کرده است. با توجه به متن باز بودن این خدمتگزار وب که تحت مجوز GNU است، هر کسی می تواند با توجه به نیاز خود آن را با خدمتگزار خود تطبیق دهد. کتابخانه بسیار بزرگی برای Apache وجود دارد. از جنبه‌های مختلف، توسعه Apache معادل توسعه سیستم عامل Linux است. نسخه اولیه Apache برای Unix نوشته شده بود ولی در حال حاضر نسخه‌هایی برای OS/2,Windows و سایر سکوها نیز وجود دارد.
	(Internet Information Services) IIS IIS خدمتگزار وبی است که ارائه دهنده آن شرکت Microsoft است. در واقع IIS مجموعه‌ای از سرویس‌های اینترنتی است که به‌صورت یکجا نمایش داده شده است. طبق آخرین آماری که منتشر شده بعد از خدمتگزار وب Apache بیشترین محبوبیت را بین کاربران دارد. این خدمتگزار وب در محیطهایی غیر از Windows کار نمی‌کند.
	Nginx Nginx خدمتگزار وبی است که ارائه دهنده آن شرکت Nginxاست. این خدمتگزار رایگان بوده، حجم پایین و کارایی بسیار بالایی داشته و تحت مجوز BSD منتشر می‌شود. یکی از بزرگترین مزیت‌های این خدمتگزار، پشتیبانی بسیار عالی از فایل‌های ایستا است. Nginx سرعت پاسخگویی بسیار بالایی دارد و در بازدیدهای بسیار بالا عملکرد عالی دارد.
خدمتگزار برنامه‌کاربردی **(Application Server)** خدمتگزار برنامه‌کاربردی هم یک چارچوب نرم‌افزاری است که	**خدمتگزارهای برنامه‌کاربردی** تعدادی از خدمتگزارهای برنامه‌کاربردی عبارتند از: ▪ Geronimo

استانداردهای سرویس	مثال
تسهیلاتی را جهت ایجاد برنامه‌های کاربردی وب فراهم می‌کند و هم محیط خدمتگزاری را برای اجرای آنها مهیا می‌سازد. خدمتگزارهای برنامه‌کاربردی به‌صورت مجموعه‌ای از مؤلفه‌ها (که از طریق APIها در اختیار توسعه‌دهندگان قرار می‌گیرند) عمل می‌کنند. این مؤلفه‌ها برای برنامه‌های کاربردی وب معمولاً در محیط‌های مشابهی اجرا شده و کار اصلی آنها ساخت صفحات پویا است. خدمتگزارهای برنامه‌کاربردی با فراهم کردن سرویس‌های مختلف این امکان را برای توسعه‌دهندگان فراهم می‌کند که تنها روی پیاده‌سازی منطق کسب‌وکار متمرکز شوند.	▪ Glassfish ▪ JBoss ▪ Jetty ▪ JOnAS ▪ NetDynamics ▪ Powertier ▪ Resin ▪ Sapphire/Web ▪ Silverstream ▪ Sybase EAS ▪ Synergy ▪ tcServer ▪ Tomcat ▪ Weblogic ▪ WebSphere ▪ Wildfly
خدمتگزار درگاه **(Portal Server)** خدمتگزار درگاه یک خدمتگزار برنامه‌کاربردی است که نرم‌افزارهای درگاه یا کاربردهای درگاه را اجرا می‌کند.	**خدمتگزارهای درگاه** تعدادی از خدمتگزارهای درگاه عبارتند از: ▪ IBM WebSphere Portal ▪ Microsoft SharePoint ▪ Oracle Application Server Portal ▪ SAP Enterprise Portal ▪ Sun Java System Portal Server
خدمتگزار محتوا **(Content Server)** خدمتگزار محتوا شامل یک انباره امن، متمرکز، انعطاف‌پذیر و مبتنی بر وب است که کلیه مراحل چرخه حیات محتوا (شامل ساخت، تأیید، انتشار، جستجو، انقضاء و بایگانی) را مدیریت می‌کند. این خدمتگزار سرویس‌های مرکزی همچون سرویس‌های کتابخانه، جستجو، امنیت، شخصی‌سازی، گردش‌کاری، ورودی کاربر و مدیریت را فراهم می‌کند.	**خدمتگزارهای محتوا** تعدادی از خدمتگزارهای محتوا عبارتند از: ▪ Adobe Content Server ▪ Calibre Content Server ▪ Cisco TelePresence Content Server ▪ FatWire Content Server ▪ OpenText Content Server ▪ Oracle Content Server ▪ SAP Content Server ▪ Tandberg Content Server ▪ Treeno Content Server
خدمتگزار رسانه **(Media Server)** خدمتگزار رسانه مدیریتی بهینه برای فایل‌های مبتنی بر رسانه (مانند جریان‌های صدا و تصویر و تصاویر دیجیتال) فراهم می‌کند.	**خدمتگزارهای رسانه** تعدادی از خدمتگزارهای رسانه عبارتند از: ▪ atmosph3re ▪ Darwin Streaming Server ▪ Firefly Media Server ▪ Flash Media Server ▪ Flumotion Streaming Server ▪ FreeJ video streamer for Icecast ▪ Icecast ▪ IIS Media Services ▪ Logitech Media Server ▪ Nimble ▪ Open Broadcaster Software

استانداردهای سرویس	مثال
	▪ PlayOn ▪ Plex ▪ PS3 Media Server ▪ QuickTime Broadcaster ▪ Red5 ▪ SHOUT ▪ Sirannon ▪ Steamcast ▪ Subsonic ▪ TVersity Media Server ▪ Unreal Media Server ▪ VideoLAN ▪ Vidiator Xenon Streaming Server ▪ WebORB Integration Server ▪ Windows Media Encoder ▪ Windows Media Services ▪ Wowza Streaming Engine

سکوهای پشتیبان (Support Platforms)

سکوهای پشتیبان شامل معماری‌های سخت‌افزاری و نرم‌افزاری هستند که لایه‌های زیرین یک سیستم کامپیوتری را تشکیل می‌دهند. سکو در ابتدا تنها برای معماری‌های سخت‌افزاری به کار برده می‌شد.

جدول ۲-۱۵ مثال‌هایی از سکوهای پشتیبان

استانداردهای سرویس	مثال
موبایل/بی‌سیم **(Mobile/Wireless)** شامل سکوهایی است که برای انتقال‌های موبایل و بی‌سیم مورد استفاده قرار می‌گیرند. تکنیک‌های انتقال مختلفی همچون امواج مادون قرمز، امواج مایکروویو، امواج رادیویی و امواج نوری برای انتقالات بی‌سیم مورد استفاده قرار می‌گیرند.	**(Java 2 Platform, Micro Edition) J2ME** سکویی است که شرکت Sun برای دستگاه‌های موبایل و بی‌سیم طراحی کرده و هدف آن ارائه نرم‌افزارهایی است که مستقل از سکوی کاری مقصد و سیستم‌عاملِ اجرا کننده آن(که در دنیای دستگاه‌های موبایل، تنوع بیشتری دارند)، به ارائه خدمات بپردازند.
مستقل از سکو **(Platform Independent)** شامل توصیفاتی از سیستم عامل است که توانایی اجرا بر روی هر سکو و سیستم‌عاملی را دارند.	**Hypervisor** اصطلاح Hypervisor برای اولین بار توسط شرکت IBM در سال ۱۹۵۶ معرفی شد که به اشتراک‌گذاری حافظه RAM کامپیوتر می‌پرداخت. Hypervisor یک مدل از مجازی‌سازی سخت‌افزاری (Hardware Virtualization) است که امکان اجرا و استفاده از چندین سیستم‌عامل مهمان را در یک زمان واحد بر روی یک سیستم میزبان فراهم می‌کند. در این حالت سیستم‌عامل‌های مجازی نصب شده همانند هر سیستم عامل واقعی امکان استفاده از منابع سخت‌افزاری موجود در یک سیستم را دارا خواهند بود. Hypervisor در حقیقت اشاره به تأمین نیازمندی‌های

استانداردهای سرویس	مثال
	سخت‌افزاری سیسم‌عامل‌های مهمان و مدیریت ارتباط بین آنها و میزان بهره‌مندیشان از منابع سخت افزاری را دارد. از Hypervisor با عنوان (Virtual Machine Manager(VMM)) نیز یاد می‌شود.
	(Java 2 Platform Enterprise Edition) J2EE J2EE (ارائه شده توسط شرکت Sun) و .Net (ارائه شده توسط شرکت Microsoft) دو تا از چارچوب‌های معماری محاسبات توزیع‌شده مشهور هستند. J2EE حمل‌پذیری برای یک زبان (زبان Java) بر روی چندین سیستم‌عامل و سکوی سخت‌افزاری را فراهم می‌کند.
	Linux یک سیستم‌عامل متن باز است که بر روی سکوهای سخت‌افزاری مختلف اجرا می‌شود.
	Eclipse مجموعه‌ای از پروژه‌های متن باز است که بر روی Equinox OSGi run-time ساخته شده‌اند.
وابسته به سکو **(Platform Dependent)** شامل توصیفاتی از سیستم عامل است که تنها توانایی اجرا بر روی یک سکو یا سیستم‌عامل مشخص را دارند.	**Windows** خانواده سیستم‌عامل‌های Windows توسط شرکت Microsoft ارائه شده است.
	Mac OS سیستم‌عامل مبتنی بر Unix که شرکت Apple آنرا مبتنی بر استانداردهای صنعتی ارائه کرده است.
	.Net J2EE (ارائه شده توسط شرکت Sun) و .Net (ارائه شده توسط شرکت Microsoft) دو تا از چارچوب‌های معماری محاسبات توزیع‌شده مشهور هستند. چارچوب .Net از تعداد زیادی از زبان‌ها پشتیبانی می‌کند ولی اجرای آن با سیستم‌عامل Windows و سخت‌افزارهای Intel گره خورده است.

زیرساخت/سخت‌افزار (Hardware/Infrastructure)

زیرساخت/سخت‌افزار شامل دستگاه‌های فیزیکی، تسهیلات و استانداردهایی است که جهت محاسبات و شبکه‌بندی بین سازمان‌ها به‌کار گرفته می‌شوند.

جدول ۲-۱۶ مثال‌هایی از زیرساخت‌ها و سخت‌افزارهای قابل استفاده

استانداردهای سرویس	مثال

استانداردهای سرویس	مثال
کامپیوترها/خدمتگزارها **(Computers/Servers)** شامل انواع مختلفی از ماشین‌های قابل برنامه‌ریزی است که توانایی پاسخ به مجموعه‌ای از دستورات و اجرای برنامه‌ها را دارند.	**خدمتگزار سازمانی (Enterprise Server)** کامپیوتر یا دستگاهی است که بر روی شبکه، منابع شبکه و برنامه‌های کاربردی مشترک را برای چندین کاربر مدیریت می‌کند.
	Mainframe کامپیوتر خیلی بزرگی است که توانایی پشتیبانی ازصدها یا هزاران کاربرِ همزمان را داشته و از برنامه‌های همزمان نیز پشتیبانی می‌کند.
دستگاه‌های فناوری تعبیه‌شده **(Embedded Technology Devices)** شامل دستگاه‌ها و بخش‌های مختلفی است که یک کامپیوتر یا خدمتگزار را می‌سازند. همچنین شامل دستگاه‌هایی است که کار خاصی را خارج از یک کامپیوتر یا خدمتگزار انجام می‌دهند.	**RAM (Random Access Memory)** RAM (حافظه با دسترسی تصادفی) نوعی حافظه برای ذخیره‌سازی موقت اطلاعات کامپیوتری است. یک RAM به داده‌های ذخیره شده اجازه می‌دهد تا مستقیماً در هر مرحله تصادفی در دسترس باشند.
	دیسک سخت (Hard Disk) مربوط به سطحی از کامپیوتر است که داده‌ها بر روی آن ذخیره می‌شوند. دیسک سخت وسیله‌ای است با یک یا چند صفحه که سطح آنها با موادی پوشش داده شده که بتوان داده‌ها را به طور مغناطیسی بر روی آنها ضبط نمود. این وسیله علاوه بر صفحه‌های مذکور حاوی هدهای خواندن/نوشتن، سازوکار تعیین محل هد و موتوری است که در محفظه‌ای جای داده می‌شود تا از آلودگی‌های خارجی در امان باشد.
	ریزپردازنده (Microprocessor) ریزپردازنده تراشه کوچکی است که می‌تواند عملیات حسابی و منطقی را انجام دهد. این تراشه‌ها از تعداد بسیار زیادی ترانزیستور ساخته شده‌اند. ریزپردازنده قلب هر کامپیوتر است که به‌عنوان واحد پردازشگر مرکزی نیز شناخته شده است. ریزپزدازنده یک دستگاه محاسبه‌ای کامل است که بر روی یک تراشه واحد ساخته می‌شود و مجموع دستورهای دستگاه را اجرا می‌کند.
	RAID (Redundant Array of Independent Disks) فناوری RAID (آرایه چندگانه دیسک‌های مستقل)، پیوند دادن چند دیسک سخت جداگانه در چارچوب یک آرایه برای دستیابی به کارایی، پایایی و گنجایشی بیش از یک دیسک بزرگ و گران است. همچنین کل این آرایه برای سیستم‌عامل میزبان، به‌گونه‌ای یکپارچه رفتار می‌کند.
دستگاه‌های جانبی **(Prepherials)** شامل دستگاه‌های کامپیوتری است که به کامپیوتر وصل شده و ظرفیت و کاربری آن را بالا می‌برند، اما جزء قطعات اصلی کامپیوتر به حساب نمی‌آیند. دستگاه‌های جانبی می‌توانند درونی	**چاپگر (Printer)** چاپگر یکی از تجهیزات جانبی کامپیوتر است که متن یا تصویر ایجاد شده به وسیله کامپیوتر را بر روی کاغذ یا رسانه مشابه دیگری حک می‌کند. انواع چاپگرها عبارتند از چاپگر ماتریس سوزنی، چاپگر لیزری، چاپگر جوهرافشان، چاپگر تماسی و چاپگر غیرتماسی.

استانداردهای سرویس	مثال
یا بیرونی باشند و به وسیله کابل یا بدون کابل (مثلاً از طریق امواج رادیویی) به کامپیوتر متصل شوند.	**پویشگر (Scanner)** وسیله‌ای برای تصویربرداری از اسناد کاغذی یا اسناد مشابه است. پویشگرها دستگاه‌هایی برای ورود عکس یا متن به کامپیوتر می‌باشند و کمپانی‌های تولید کننده پویشگر معمولاً همان کمپانی‌های تولیدکننده چاپگرها هستند. پویشگرها شمایلی مانند دستگاه فتوکپی دارند. در محفظه‌ای که در آن کاغذ قرار می‌گیرد تصویر یا متن مورد نظر در کامپیوتر وارد می‌شود.
	فکس (Fax) طرح اصلی فکس در ۱۹۰۲ در آلمان اختراع شد. فکس‌های اداری از اوایل ۱۹۸۰ رایج شد. فکس تصویری از یک مدرک (یک یا چند صفحه متن یا تصویر) را به دستگاه فکسِ دیگر می‌فرستد. این دستگاه تصویر مدارک فرستاده شده توسط دستگاه های فکسِ دیگر را هم چاپ می‌کند. ماشینی که تصویر را می‌فرستد الگوی نقاط روشن و تاریک مدرک را به سیگنالِ الکتریکی تبدیل می‌کند. این سیگنال از طریق شبکه تلفن به دستگاه گیرنده می‌رسد که سیگنال را به‌صورت اولیه‌اش بر می‌گرداند. می‌توان مدار الکترونیکی کوچکی به کامپیوتر شخصی اضافه کرد که به کامپیوتر امکان دهد به‌صورت دستگاه فکس عمل کند. به این صورت می توان متن و تصویرهای موجود در کامپیوتر را به دستگاه فکسِ دیگری فرستاد یا متن و مدارکی را که بر روی صفحه نمایش کامپیوتر ظاهر می‌شود دریافت و در حافظه کامپیوتر ذخیره کرد یا آن را به کمک چاپگر کامپیوتر چاپ کرد.
	دوربین دیجیتال (Digital Cammera) یک دستگاه الکترونیکی است که برای گرفتن عکس و ذخیره آن به‌جای فیلم عکاسی از حسگرهای حساس به نور معمولاً از نوع CCD یا CMOS استفاده می‌کند و تصویر گرفته شده توسط سنسور طی چند مرحله به حافظه دوربین برای استفاده فرستاده می‌شود.
	وب‌کم (Webcam) وب‌کم دوربین کوچکی است که معمولاً از طریق پورت یواس‌بی (USB) به کامپیوتر وصل می‌شود و از طریق آن می‌توان فیلم یا عکس را به کامپیوتر منتقل کرد. با توجه به خصوصیات وب‌کم از آن می‌توان برای گفتگوهای اینترنتی، کنفرانس از راه دور و غیره استفاده کرد. ضمناً از آن می‌توان به‌عنوان چشم الکترونیکی برای بازرسی کردن خانه، حیاط و محیط‌های مختلف استفاده نمود.
	بلندگو (Speaker)

استانداردهای سرویس	مثال
	دستگاهی است که وظیفه‌ی انتقال صوت به بیرون از کامپیوتر را دارا است. این دستگاه بیشتر دارای یک آمپلی‌فایر(تقویت‌کننده الکترونیکی) داخلی با قدرت کم است.
	دستگاه‌های کمک کننده (Assistive Devices) شامل دستگاه‌هایی است که به کاربران اجازه می‌دهد که اطلاعات را با استفاده از رسانه‌هایی غیر از رسانه‌های معمول وارد کامپیوتر کنند. این دستگاه‌ها برای دسترسی بیشتر افراد معلول مورد استفاده قرار می‌گیرند. نمونه‌ای از این دستگاه‌ها برای تشخیص گفتار مورد استفاده قرار می‌گیرد که امکان تبدیل صحبت افراد به کلمات متنی را فراهم می‌کند.
شبکه گسترده **(Wide Area Network)** شبکه گسترده یک شبکه کامپیوتری است که ناحیه جغرافیایی نسبتاً وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر). این شبکه‌ها معمولاً از امکانات انتقال خدمت‌دهندگان عمومی مانند شرکت‌های مخابرات استفاده می‌کند. به‌عبارتی دیگر، این شبکه‌ها از مسیریابها و لینک‌های ارتباطی عمومی استفاده می‌کنند. بزرگ‌ترین و شناخته‌شده‌ترین مثال از یک شبکه گسترده شبکه اینترنت است. اغلب جهت پیاده‌سازی شبکه‌های گسترده از خطوط اجاره‌ای استفاده می‌شود. در هر انتهای خط اجاره‌ای یک دستگاه مسیریاب قرار داده می‌شود که از یک طرف به شبکه محلی و از طرف دیگر به‌وسیله یک هاب به آن سوی شبکه گسترده متصل است.	**رِله فریم (Frame Relay)** رِله فریم یک فناوری لایه دوم شبکه‌های گسترده محسوب می‌شود که فرایند محصورسازی (Encapsulation) بسته‌های IP و ارسال آنها در شبکه را انجام می‌دهد. در این فناوری بر خلاف شبکه‌های LAN امکان ارسال پیام‌ها به‌صورت Broadcast به تمام دستگاه‌ها وجود نداشته و در دسته‌بندی (None Broadcast Multi Access(NBMA)) قرار می‌گیرد.
	حالت انتقال ناهمگام (Asynchronous Transport Mode(ATM)) ATM به پالس‌های ساعت وابستگی نداشته و در رده شبکه‌های اتصال‌گرا تقسیم‌بندی می‌شود. جهت برقراری اتصال در این مدل، در آغاز بسته‌ای به‌سوی مقصد ارسال می‌شود. این بسته مسیر خود را بین مسیریاب‌های مختلف پیدا کرده و مدار مجازی را تشکیل می‌دهد. هر یک از این اتصال‌ها (که از این به بعد آن را می‌توان اتصال فیزیکی در نظر گرفت) دارای یک شماره شناسایی هستند. در این مدل اطلاعات به‌صورت بسته‌های ۵۳ بایتی(سلول) ارسال می‌گردد. این بسته‌ها از دو بخش سرآیند و داده‌های کاربر تشکیل شده‌اند. در بخش سرآیند که ۵ بایت است اطلاعاتی همچون شماره شناسایی اتصال ذخیره می‌گردد. ATMها سرعت بالایی دارند و بسته‌ها را در یک مسیر و به ترتیب ارسال می‌کنند. مدل مرجع ATM برخلاف مدل مرجع OSI و مدل مرجعTCP/IP ، مدلی سه بعدی است و دارای سه لایه فیزیکی، لایه ATM و لایه انطباق ATM است.
	(Multi Protocol Label Switching) MPLS MPLS (سوییچینگ برچسب چند پروتکلی) یک فناوری انتقال داده در بستر شبکه گسترده است که از برچسب‌گذاری برای ارسال بسته‌ها استفاده می‌کند. یک بسته در هنگام ورود به شبکه MPLS بر اساس آدرس IP مقصد برچسب‌گذاری شده و در طول مسیر لایه

استانداردهای سرویس	مثال
	دوم و بر اساس برچسب زده شده هدایت می‌شود تا به مقصد برسد. MPLS در یک لایه خاص از مدل OSI قرار نمی‌گیرد و عملکرد آن بین لایه دوم و سوم قرار دارد. به همین خاطر آن را به‌عنوان پروتکل لایه دوونیم (۲/۵) معرفی می‌کنند. برچسب‌ها بین مسیریاب‌ها پخش می‌شوند و آنها را قادر می‌سازد که بدون در نظر گرفتن آدرس IP اقدام به ارسال بسته‌ها کنند. نکته قابل توجه این است که امروزه سرویس VPN مبتنی بر فناوری MPLS امکان ایجاد شبکه‌های اختصاصی مجازی در گستره شبکه IP/MPLS در مراکز استان‌های کشور را برای مشتریان فراهم می‌نماید.
شبکه محلی **(Local Area Network)** شبکه محلی (LAN) یک شبکه کامپیوتری است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمان‌ها را پوشش می‌دهد. از مشخصات تعریف‌شده شبکه‌های محلی در مقایسه با شبکه‌های گسترده (WAN) می‌توان به سرعت (نرخ انتقال) بسیار بالاتر آنها، محدوده جغرافیایی کوچکتر و عدم نیاز به خطوط استیجاری مخابراتی اشاره کرد. دو فناوری اترنت (Ethernet) و وای‌فای (Wi-Fi) رایج‌ترین فناوری‌هایی هستند که امروزه استفاده می‌شوند. فناوری‌های آرکنت (ARCNET) و توکِن‌رینگ (Token Ring) و بسیاری از روش‌های دیگر نیز در گذشته مورد استفاده بوده‌اند.	**اترنت (Ethernet)** اترنت یکی از فناوری‌های مبتنی بر فِریم در شبکه‌های کامپیوتری برای شبکه‌های محلی است. این فناوری از دهه ۱۹۹۰ تاکنون به کارگرفته شده است و جایگزین استانداردهایی همچون توکِن‌رینگ (Token Ring) و آرکنت (ARCNET) شده است. این فناوری وضعیت سیم‌کشی و استانداردهای سیگنالینگ در لایه فیزیکی و همچنین قالب‌های آدرسی همچون MAC را معین می‌کند.
	وای‌فای (Wi-Fi) نام اولیه و رسمی این فناوری شبکه محلی بی‌سیم (WLAN) است. این نام به مرور زمان و با تبلیغات قوی اتحادیه وای‌فای در سطح بازار کمتر استفاده می‌شود. وای‌فای نامی تجاری است که توسط اتحادیه وای‌فای (Wi-Fi Alliance) ثبت شده و علامتی است که این اتحادیه به محصولاتی که مورد تأیید این اتحادیه جهت کار در شبکه محلی بی‌سیم تحت استاندارد IEEE 802.11 است اعطاء می‌کند. با این فناوری، ارتباطی با قدرتی بیشتر از بلوتوث ایجاد می‌شود. ارتباط وای‌فای بیشتر بر پایه ارتباط شبکه اینترنت به‌صورت بی‌سیم تأکید می‌کند و همین امر باعث محبوبیت بسیار زیاد آن شده است. با استفاده از این فناوری به‌راحتی در مسافرت، هواپیما یا هتل می‌توان از طریق کامپیوتر یا تلفن همراه به اینترنت متصل شد.
	توکِن‌رینگ (Token Ring) فناوری توکن‌رینگ در اواسط سال ۱۹۸۰ میلادی توسط شرکت IBM معرفی شد. مشخصات و ویژگی‌های توکن‌رینگ را به‌صورت اختصاصی استاندارد IEEE 802.5 تعیین می‌کند.
	شبکه محلی مجازی (Virtual LAN (VLAN)) یک VLAN مجموعه‌ای از نودهایی است که در یک دامنه انتشار (Broadcast Domain) قرار دارند. VLAN همان صفات شبکه

استانداردهای سرویس	مثال
	فیزیکی را دارد، اما به ایستگاه‌ها اجازه می‌دهد تا با هم گروه‌بندی شوند، حتی اگر آنها در یک بخش از شبکه واقع نشده باشند. با استفاده از VLAN می‌توان پیکربندی دوباره شبکه را به‌صورت نرم‌افزاری انجام داد و نیازی به جابجایی فیزیکی دستگاه‌ها نیست. VLANها برای ارائه سرویس‌های تقسیم‌بندی که به‌صورت سنتی توسط مسیریاب‌ها در تنظیمات شبکه فراهم می‌شد، ایجاد شده‌اند. از مشکلات VLAN میتوان به مقیاس‌پذیری، امنیت و مدیریت آن اشاره کرد.
استانداردها/دستگاه‌های شبکه **(Network Devices/Standards)** استانداردها/دستگاه‌های شبکه شامل گروهی از ایستگاه‌ها (کامپیوترها، تلفن‌ها و سایر دستگاه‌ها) است که برای تبادل اطلاعات با استفاده از تسهیلات ارتباطاتی به یکدیگر متصل می‌شوند. اتصالات می‌تواند از طریق کابل‌ها و به‌صورت همیشگی باشد یا از طریق خطوط تلفن یا سایر خطوط و به‌صورت موقتی باشد. رسانه‌های انتقال نیز می‌تواند به‌صورت فیزیکی (به‌عنوان مثال کابل‌های فیبر نوری) یا بی‌سیم (به‌عنوان مثال ارتباط ماهواره‌ای) باشد	**هاب (Hub)** هاب، یکی از تجهیزات متداول در شبکه‌های کامپیوتری و ارزانترین روش اتصال دو یا چند کامپیوتر به یکدیگر است. هاب در اولین لایه مدل مرجع OSI فعالیت می‌نماید. هاب‌ها فریم‌های داده را نمی‌خوانند (کاری که سوئیچ و یا روتر انجام می‌دهند) و صرفاً این اطمینان را ایجاد می‌نمایند که فریم‌های داده بر روی هر یک از پورت‌ها، تکرار خواهد شد. گره‌هائی که یک اترنت و یا Fast Ethernet را با استفاده از قوانین CSMA/CD به اشتراک می‌گذارند، عضو یک دامنه برخورد (Collision Domain) مشابه می‌باشند.
	سوییچ (Switch) سوئیچ یک وسیله ارتباط از راه دور است که پیام‌ها را از هر وسیله‌ای که به آن وصل شده دریافت می‌کند و سپس آن را تنها برای دستگاه هدف ارسال می‌کند. این کار سوئیچ را هوشمندتر از هاب می‌کند (که پیغامی را دریافت کرده و آن را برای تمام دستگاه‌های موجود در شبکه ارسال می‌کند). سوییچ معمولاً به دستگاه چند پورته‌ای اطلاق می‌شود که پردازش و انتقال داده را در لایه دوم مدل OSI انجام می‌دهد. سوئیچ‌هایی که معمولاً در لایه سوم یا بالاتر پردازش را انجام می‌دهند، معمولاً سوئیچ چند لایه یا سوئیچ لایه سه خوانده می‌شوند. اولین سوئیچ اترنت، توسط Kalpana در سال ۱۹۹۰ معرفی شده است.
	مسیریاب (Router) دستگاه کامپیوتری شبکه‌ای (یا یک کامپیوتر) است که بسته‌های داده را بر روی یک شبکه به هم پیوسته برای رسیدن به مقصدشان، هدایت می‌کند. مسیریاب جهت اتصال دو یا چند شبکه محلی به هم یا اتصال چندین خط شبکه بزرگ به هم مورد استفاده قرار می‌گیرد. مسیریاب می‌تواند انواع مختلف شبکه را به هم وصل کند. عمل مسیریابی در لایه سوم مدل OSI رخ می‌دهد.

استانداردهای سرویس	مثال
	(Network Interface Card) NIC NIC یا کارت شبکه، یکی از مهمترین عناصر سخت افزاری در زمان پیاده‌سازی یک شبکه کامپیوتری است. هر کامپیوتر موجود در شبکه (سرویس گیرندگان و سرویس دهندگان) نیازمند استفاده از یک کارت شبکه است. کارت شبکه، ارتباط بین کامپیوتر و محیط انتقال (نظیر کابل‌های مسی یا فیبر نوری) را فراهم می‌نماید.
	Transceiver دستگاهی است که نام آن از ترکیب دو کلمه انتقال‌دهنده (Transmitter) و دریافت‌کننده (Receiver) گرفته شده است و برای انتقال و دریافت سیگنال‌های آنالوگ و دیجیتال مورد استفاده قرار می‌گیرد. Transceiver مسئولیت تبدیل یک نوع سیگنال یا کانکتور به نوع دیگری را برعهده دارد.
	دروازه (Gateway) در شبکه، دروازه به سیستمی گفته می‌شود که توانایی آن را دارد تا دو شبکه متفاوت را که از دو پروتکل متفاوت تشکیل شده است را به یکدیگر متصل کند. بسته به نوع پروتکلی که در شبکه پشتیبانی می‌شود، دروازه می‌تواند در هر سطح از مدل OSI کار خود را انجام دهد. به این دلیل که دروازه‌ها عملیات انتقال را در چندین لایه مدل OSIانجام می‌دهند، می‌توان دروازه‌ها را جزء پیچیده‌ترین دستگاه‌ها شبکه برشمرد.
	Integrated Services Digital Network (ISDN) ISDN شامل سرویس‌های دیجیتالی است که می‌توانند به‌طور همزمان ویدئو، داده و صوت را پشتیبانی نمایند. استانداردهای ISDN توسط اتحادیه بین المللی مخابرات (ITU) تعریف می‌شود. خطوط ISDNدر واقع خطوط تلفن معمولی است. ISDN شامل دو نوع BRI و PRI است.
	Digital Subscriber Line (DSL) DSL (خط دیجیتال مشترک) از دسته فناوری‌هایی است که انتقال مخابراتی اطلاعات داده را به وسیله سیم‌های ارتباطی در یک شبکه تلفنی محلی فراهم می‌آورد. DSL شاخه‌ای از فناوری است که اطلاعات را از طریق شبکه کابلی تلفن محلی انتقال می‌دهد. DSL ابتدا برای یک حلقه ارتباطی دیجیتال شکل گرفت. در بازاریابی ارتباطات رادیویی اصطلاح DSL با معنی خط اشتراک دیجیتال نامتقارن (ADSL) قابل فهم و شناخته شده است که متداول‌ترین شیوه استفاده از فناوری DSL است.
	فایروال (Firewall)

استانداردهای سرویس	مثال
	به سیستم‌هایی اطلاق می‌شود که شبکه خصوصی یا کامپیوترهای شخصی را در مقابل نفوذ مهاجمین، دسترسی‌های غیرمجاز، ترافیک‌های مخرب و حملات هکری خارج از آنها محافظت می‌کند. فایروال‌ها می‌توانند ترافیک ورودی و خروجی شبکه را کنترل و مدیریت کرده و با توجه به قوانینی که در آنها تعریف می‌شود به کاربر یا برنامه‌های کاربردی خاصی اجازه ورود، خروج و دسترسی به یک سیستم خاص را بدهند. قوانینی که در یک فایروال وجود دارد بر اساس نیازمندی‌های امنیتی یک سازمان تعیین می‌شود. فایروال‌ها می‌توانند به‌صورت نرم‌افزاری یا سخت‌افزاری مورد استفاده قرار گیرند.
ویدئوکنفرانس **(Video Conferencing)** ویدئوکنفرانس به مفهوم برقراری ارتباط زنده صوتی و تصویری بین نقاط مختلف جغرافیایی دور و نزدیک است. به‌عبارت دیگر ویدئوکنفرانس فناوری است که افراد در مکان‌های مختلف با فواصل مختلف را قادر می‌سازد تا صوت و تصویر همدیگر را به‌صورت زنده دریافت کرده و همانند جلسات حضوری با یکدیگر ارتباط داشته و تبادل‌نظر نمایند. ویدئوکنفرانس می‌تواند با امکانات افزوده دیگری همانند تبادل اسناد و مدارک، اشتراک در تهیه مدارک، ارسال عکس‌ها و غیره نیز همراه باشد.	**پایانه (Terminal)** پایانه یا ترمینال تنها جزء ضروری شبکه ویدئوکنفرانس است. پایانه شامل تمام اجزائی است که کاربر برای ارتباط ویدئوکنفرانسی نیاز دارد. این اجزاء شامل کُدک (Codec) برای کدگذاری و کدگشایی اطلاعات، دوربین برای دریافت تصویر، میکروفون برای دریافت صدا، صفحه نمایش برای نمایش تصویر، بلندگو برای پخش صدا و امکانات اختیاری دیگر مثل تخته وایت‌برد دیجیتال برای استفاده در برنامه‌های کاربردی آموزش از راه دور می‌باشد. ترمینال‌های ویدئوکنفرانس از نظر حجم کاربرد به سه دسته ترمینال‌های Desktop، ترمینال‌های Set-top و ترمینال‌های Rollabout تقسیم می‌شوند.
	MCU (Multipoint Control Unit) MCU (واحد کنفرانس چند نقطه‌ای) جزئی از شبکه ویدئوکنفرانس است که امکان برقراری ارتباط همزمان بین بیش از دو پایانه را فراهم می‌آورد.MCU شامل دو بخش MC (Multipoint Contoller) و MP (Multipoint Processor) است. MC وظیفه کنترل و مدیریت کنفرانس و MP وظیفه ادغام و سوییچ‌کردن جریان‌های ویدئویی و صوتی رسیده از پایانه‌ها را به عهده دارد. MCU به‌طور منطقی جزئی جدا در شبکه ویدئو کنفرانس به‌شمار می‌رود ولی ممکن است از نظر فیزیکی، ادغام شده در یک ترمینال باشد. این گونه MCUها توانایی برقراری ارتباط بین سه تا هفت پایانه را دارا هستند و به‌طور معمول پاسخگوی نیاز اکثر کاربران می‌باشند. در صورت نیاز به ظرفیت بیشتر، از روش Cascade کردن MCUها و یا از MCUهای خارجی استفاده می‌شود.
	کُدک (Codec) مغز اصلی پایانه ویدئوکنفرانس است که کلیه تجهیزات (مثل دوربین،

استانداردهای سرویس	مثال
	میکروفون ، نمایشگر و تجهیزات جانبی) به آن متصل می‌شوند و عهده‌دار مسئولیت اصلی کار و فشرده‌سازی و بازگشایی بسته‌های اطلاعاتی می باشد. در پایانه‌های سخت‌افزاری این بخش همان قطعه‌ای است که کابلِ کلیه تجهیزات به آن متصل می‌گردد و در پایانه‌های نرم‌افزاری، کامپیوتر به‌علاوه نرم‌افزارِ ویدیوکنفرانس نقش کُدک را دارد.
	H.320 از استانداردهای ITU برای پایانه‌های ویدئو کنفرانس است که از خطوط تلفن ISDN یا شبکه‌های (Leased SCN) استفاده می‌کند. این استاندارد در سال ۱۹۹۰ تدوین گردید و با استقبالی فراوان روبرو شد. با تدوین استاندارد H.323 در سال ۱۹۹۶ و توسعه شبکه‌های کامپیوتری، H.320 جای خود را به این استاندارد جدید وگذار نمود و در جایگاه دوم از نظر محبوبیت قرار گرفت.
	H.323 استاندارد مصوب ITU برای پایانه‌های ویدئو کنفرانس در شبکه‌های پاکتی (PBN) از جمله شبکه‌های کامپیوتری مبتنی بر TCP/IP و شبکه اینترنت است. این استاندارد نخست در سال ۱۹۹۶ تصویب گردید و در مدت کوتاهی توانست به جایگاه ویژه‌ای در بازار ویدئوکنفرانس دست یابد.

مهندسی نرم‌افزار (Software Engineering)

مهندسی نرم‌افزار فناوری‌هایی را که مربوط به ساخت سیستم‌های نرم‌افزاری می‌شود پوشش می‌دهد. همچنین راهکارهای فنی که از موارد مدیریتی همچون تست، مدلسازی و نسخه‌بندی پشتیبانی می‌کنند در طبقه مهندسی نرم‌افزار قرار می‌گیرند. مهندسی نرم‌افزار در مدل مرجع فناوری به معماری‌های فنی مؤلفه‌ها مربوط می‌شود و فرایندهای مهندسی را شامل نمی‌شود.

جدول ۲-۱۷ مثال‌هایی از فناوری‌های قابل به‌کارگیری در مهندسی نرم‌افزار

استانداردهای سرویس	مثال
مدلسازی **(Modeling)** مدلسازی از فرایند نمایش موجودیت‌ها، داده‌ها، منطق کسب‌وکار و قابلیت‌ها برای کمک به مهندسی نرم‌افزار پشتیبانی می‌کند.	**زبان مدلسازی یکپارچه (Unified Modeling Language (UML))** UML زبان مدلسازی همه‌منظوره استاندارد در زمینه مهندسی نرم‌افزار است که توسط گروه OMG ایجاد شده است. با استفاده از UML می‌توان تقریباً هر گونه برنامه‌کاربردی که ممکن است بر روی هر ترکیبی از سخت‌افزار، سیستم عامل، زبان برنامه‌سازی و شبکه اجرا شود را مدلسازی نمود. طراحی بر پایه مفاهیم شئ‌گرایی UML سبب

استانداردهای سرویس	مثال
	می‌شود که ذاتاً با محیط‌ها و زبان‌های برنامه‌سازی شئ‌گرا سازگاری کامل داشته باشد، اگرچه می‌توان از آن برای مدلسازی برنامه‌های غیر شئ‌گرا نیز استفاده نمود. تعدادی از ابزارهای UML عبارتند از: ▪ ArgoUML ▪ Astah ▪ ATL ▪ Borland Together ▪ BOUML ▪ CaseComplete ▪ ConceptDraw PRO ▪ Creately for UML ▪ Dia ▪ Eclipse UML2 Tools ▪ Edraw Max ▪ Enterprise Architect ▪ Gliffy ▪ Lucidchart ▪ MagicDraw ▪ Microsoft Visio ▪ Modelio ▪ MyEclipse ▪ NClass ▪ NetBeans ▪ objectiF ▪ Open ModelSphere ▪ Papyrus ▪ PlantUML ▪ Poseidon for UML ▪ PowerDesigner ▪ Prosa UML Modeller ▪ Rational Rhapsody ▪ Rational Rose XDE ▪ Rational Software Architect ▪ Rational Software Modeler ▪ Rational System Architect ▪ RISE ▪ Real Time Developer Studio ▪ Software Ideas Modeler ▪ StarUML ▪ Umbrello UML Modeller ▪ UML Designer ▪ UMLet ▪ UModel ▪ Visual Paradigm for UML ▪ yEd
	Computer Aided Software Engineering (CASE) CASE (مهندسی نرم‌افزار به کمک کامپیوتر) گستره‌ای وسیع از نرم‌افزارها و ابزارهای مورد استفاده برای طراحی و پیاده‌سازی

استانداردهای سرویس	مثال
	برنامه‌های کاربردی است. ابزارهای CASE مشابه ابزارهای طراحی به کمک کامپیوتر (CAD) هستند. این ابزارها برای توسعه نرم‌افزار با کیفیت بالا، بدون نقص و قابل نگهداری به کار برده می‌شوند. این ابزارهای نرم‌افزاری اغلب با روش‌های توسعه سیستم‌های اطلاعاتی با کمک ابزارهای خودکار که در فرایند توسعه نرم‌افزار می‌توانند مورد استفاده قرار بگیرند استفاده می‌شوند. در واقع ابزارهایی مانند CASE جهت کمک به مهندسان نرم‌افزار در طول چرخه حیات نرم‌افزار ایجاد شده‌اند تا به تحلیل، طراحی، برنامه‌سازی، آزمون و تست، نگهداری و غیره نرم‌افزار کمک کنند. برخی از ابزارهای CASE عبارتند از: ▪ Artiso Visual ▪ DB-MAIN ▪ iGrafx FlowCharter ▪ MetaEdit+ ▪ Microsoft Visio ▪ OmniGraffle ▪ Rational Rose ▪ SmartDraw ▪ ArgoUML ▪ Visible Analyst
	(Business Process Model & Notation) BPMN مجموعه‌ای از علائم، نشانه‌ها و شیوه‌ای استاندارد برای مدل‌سازی فرایندهای کسب‌وکار است و یکی از ابزارهای اصلی در مدیریت فرایندهای کسب‌وکار محسوب می‌شود. نسخه BPMN 2.0 در سال ۲۰۱۱ توسط گروه OMG ارائه شده است. برخی از ابزارهای BPMN عبارتند از: ▪ ABACUS ▪ Activiti Modeler ▪ ActiveVOS ▪ ADONIS (software) ▪ Agiles BPMS & ECM ▪ Altova UModel ▪ ARCWAY Cockpit ▪ ARIS Express ▪ AuraPortal ▪ Axon.ivy Designer ▪ BeePMN ▪ Bizagi BPM Suite ▪ Bizagi Process Modeler ▪ BiZZdesign Architect ▪ BPMN Visio Modeler ▪ BPMN Web Modeler ▪ Bonita BPM ▪ Borland Together ▪ bpmn.io ▪ Camunda Modeler

استانداردهای سرویس	مثال
	▪ Cubetto ▪ Cubetto Toolset ▪ Eclipse BPMN2 Modeler ▪ jBPMN ▪ Edraw Max ▪ Enterprise Architect ▪ Genexus WorkFlow ▪ GenMyModel ▪ Yaoqiang BPMN Editor ▪ HP Process Automation ▪ IBM BlueWorks Live ▪ IBM Process Designer ▪ IBM Rational System Architect ▪ iGrafx Flowcharter, iGrafx Process ▪ inspire smart process Modeller ▪ Imixs-BPMN ▪ Innovator for Business Analysts ▪ IYOPRO ▪ jBPM ▪ Logizian ▪ LucidChart ▪ MagicDraw ▪ ModelFoundry ▪ myInvenio ▪ iServer ▪ Pegasystems ▪ process4.biz BPM ▪ Microsoft Visio ▪ Modelio ▪ OmniGraffle ▪ Papyrus ▪ ProcessCraft ▪ ProcessMaker ▪ Process Modeler for Microsoft Visio ▪ QPR ProcessDesigner ▪ QUAM ▪ RunaWFE ▪ SemTalk ▪ Signavio Process Editor ▪ Software Ideas Modeler ▪ Stages ▪ SYDLE SEED Community ▪ TIBCO ActiveMatrix ▪ Triaster ▪ Visible Analyst ▪ W4 BPMN+ ▪ W4 Web Modeler ▪ yEd ▪ Intellileap Solutions
(Business Process Execution Language) BPEL	

استانداردهای سرویس	مثال
	زبان WS-BPEL (Web Services BPEL) که عموماً به‌عنوان BPEL شناخته می‌شود، زبان اجرای فرایندهای کسب‌وکار است که جهت توصیف کنش‌ها در فرایندهای کسب‌وکار با استفاده از وب‌سرویس‌ها مورد استفاده قرار می‌گیرد. به‌عبارت دیگر اطلاعات فرایندها در BPEL با استفاده از واسط وب‌سرویس‌ها صادر و وارد می‌گردد. زبان BPEL استاندارد سازمان پیشبرد استانداردهای اطلاعاتی ساختیافته (OASIS) بوده و مبتنی بر XML است که سیستم مدیریت فرایندهای کسب‌وکار می‌تواند با آن فرایندها را اجرا کند. این استاندارد در همنواسازی سرویس‌های وب (Web Service Orchestration(WSO)) به‌کار می‌رود. تعدادی از ابزارهای BPEL عبارتند از: ▪ ExpressBPEL ▪ ActiveVOS ▪ Apache ODE ▪ BizTalk Server ▪ iBolt Server ▪ Open ESB ▪ Oracle BPEL Process Manager ▪ OW2 Orchestra ▪ Parasoft BPEL Maestro ▪ Petals BPEL Engine ▪ SAP Exchange Infrastructure ▪ Virtuoso Universal Server ▪ WebSphere Process Server
	مدل موجودیت–ارتباط (Entity-Relationship(ER)) مدل ER در سال ۱۹۷۶ طراحی شده است. این مدل یک مدل ادراکی داده است که دنیای واقعی را به‌صورت موجودیت‌ها و وابستگی‌های بین آنها نمایش می‌دهد. در مدل ER ساختار پایگاه‌داده به‌صورت یک دیاگرام به تصویر کشیده می‌شود که ارتباط منطقی موجودیت‌ها را به‌صورت یک نمودار ترسیمی نمایش می‌دهد. مدل ER به‌عنوان ابزاری برای طراحی پایگاه‌داده بسیار موفق است و کمک بسیار خوبی برای طراحی، پیاده‌سازی، بهینه‌سازی و اشکال‌زدایی برنامه‌های پایگاه‌داده است. برخی از ابزارهای مدل ER عبارتند از: ▪ Avolution ▪ ConceptDraw PRO ▪ Creately ▪ Edraw Max ▪ ER/Studio ▪ ERwin ▪ MagicDraw ▪ ModelRight ▪ Navicat Data Modeler ▪ OmniGraffle ▪ Oracle Designer

استانداردهای سرویس	مثال
	▪ PowerDesigner ▪ Prosa Structured Analysis Tool ▪ Rational Rose ▪ Software Ideas Modeler ▪ Sparx Enterprise Architect ▪ SQLyog ▪ System Architect ▪ Toad Data Modeler ▪ Visual Paradigm ▪ yEd
محیط توسعه یکپارچه **(Integrated Development Environment (IDE))** محیط توسعه یکپارچه (IDE) یک کاربرد نرم‌افزاری است که تسهیلات جامعی را برای برنامه‌سازان کامپیوتری جهت توسعه نرم‌افزارها فراهم می‌کند. این محیط همه یا قسمت زیادی از اشیاء مورد نیاز برای ساخت یک برنامه را تحت زبان برنامه‌سازی خاص دارا است و مراحل تولید یک برنامه نرم‌افزاری را ساده‌تر و سریع‌تر می‌کند. بعضی از محیط‌های IDE تسهیلات زیادی را در مراحل توسعه نرم‌افزار مانند طراحی، پیاده‌سازی، تست، اشکال‌زدایی و گسترش فراهم می‌کنند. برای بیشتر زبان‌های برنامه‌سازی انواع رایگان و تجاری از محیط‌های IDE ارائه شده است.	**محیط‌های توسعه یکپارچه برای زبان Java** برخی از محیط‌های توسعه یکپارچه برای زبان Java عبارتند از: ▪ Anjuta ▪ BlueJ ▪ DrJava ▪ Eclipse JDT IBM ▪ Geany ▪ Greenfoot ▪ IntelliJ IDEA ▪ JBuilder ▪ JCreator ▪ JDeveloper ▪ jGRASP ▪ KDevelop ▪ MyEclipse ▪ NetBeans ▪ Rational Application Developer ▪ Servoy ▪ Understand ▪ Xcode (Apple) **محیط‌های توسعه یکپارچه برای زبان C/C++** برخی از محیط‌های توسعه یکپارچه برای زبان C/C++ عبارتند از: ▪ Anjuta ▪ AppCode (IntelliJ IDEA) ▪ C++Builder ▪ Code::Blocks ▪ CodeLite ▪ Dev-C++ ▪ Eclipse CDT ▪ Geany ▪ GNAT Programming Studio ▪ JetBrains CLion ▪ KDevelop ▪ LabWindows/CVI ▪ LccWin32 ▪ Microsoft Visual Studio ▪ Microsoft Visual Studio Express

استانداردهای سرویس	مثال
	▪ MonoDevelop ▪ NetBeans C/C++ pack ▪ OpenWatcom ▪ Oracle Solaris Studio (formerly Sun Studio) ▪ Pelles C ▪ Philasmicos Entwickler Studio ▪ Qt Creator ▪ Rational Software Architect (Eclipse IBM) ▪ Ultimate++ TheIDE ▪ Understand ▪ Xcode (Apple)
	محیط‌های توسعه یکپارچه برای زبان C# برخی از محیط‌های توسعه یکپارچه برای زبان C# عبارتند از: ▪ Microsoft Visual Studio ▪ MonoDevelop ▪ SharpDevelop ▪ Understand
	محیط‌های توسعه یکپارچه برای JavaScript برخی از محیط‌های توسعه یکپارچه برای JavaScript عبارتند از: ▪ Anjuta ▪ Brackets ▪ Aptana Studio ▪ Codeanywhere ▪ CodeLite ▪ Eclipse Web Tools ▪ Komodo IDE / Edit ▪ NetBeans ▪ Nodeclipse NTS ▪ NuSphere PhpED ▪ Oracle JDeveloper ▪ Servoy ▪ Visual Studio ▪ WebStorm
	محیط‌های توسعه یکپارچه برای PHP برخی از محیط‌های توسعه یکپارچه برای PHP عبارتند از: ▪ Adobe Dreamweaver ▪ Aptana Studio ▪ CodeLite ▪ Codelobster ▪ Eclipse PDT ▪ Geany ▪ HTML-Kit ▪ KDevelop ▪ Komodo IDE / Edit ▪ NetBeans ▪ PHPEclipse (Eclipse) ▪ PhpED Professional

استانداردهای سرویس	مثال
	▪ PHPEdit ▪ PhpStorm (IntelliJ IDEA) ▪ Quanta Plus ▪ RadPHP (formerly Delphi for PHP) ▪ Zend Studio
	محیط‌های توسعه یکپارچه برای Python برخی از محیط‌های توسعه یکپارچه برای Python عبارتند از: ▪ Anjuta ▪ eric ▪ Geany ▪ IDLE ▪ IntelliJ IDEA ▪ Koding ▪ Komodo IDE ▪ KDevelop ▪ MonoDevelop ▪ nbPython (plug-in for NetBeans ▪ Ninja-IDE ▪ PIDA ▪ PyCharm ▪ PyDev (plug-in for Eclipse and Aptana) ▪ PyScripter ▪ Python Tools for Visual Studio ▪ PythonAnywhere ▪ Pyzo ▪ SourceLair ▪ Spyder ▪ Stani's Python Editor ▪ Understand ▪ Thonny ▪ Wing IDE
مدیریت تست **(Test Management)** فناوری است که از یکپارچه‌کردن کلیه فعالیت‌ها و نتایج تست پشتیبانی می‌کند. فعالیت‌های مدیریت تست شامل برنامه‌ریزی تست، طراحی تست (موردهای تست)، اجرای تست، گزارش‌دهی تست، پوشش کدها و توسعه‌های اکتشافی می‌شود. دو رویکرد کلی زیر را می‌توان برای تست نرم‌افزار در نظر گرفت: ▪ **تست جعبه‌سیاه (Blackbox Testing)** در این رویکرد، تست تمامی مکانیسم‌های داخلی یک سیستم نادیده گرفته می‌شود و روی خروجی تولید شده تمرکز می‌شود. به این رویکرد تست	**تست واحد(Unit Testing)** در این نوع تست یک واحد یا یک گروه از واحدهای مرتبط با هم تست می‌شود. این نوع تست زیر مجموعه تست جعبه‌سفید است. **تست یکپارچه‌سازی(Integration Testing)** این نوع تست این امکان را می‌دهد که چند نوع مؤلفه مختلف را کنار یکدیگر تست کنیم. در این صورت حتی می‌توان وابستگی‌های میان سخت‌افزار و نرم‌افزار را نیز آزمایش کرد. این نوع تست زیر مجموعه تست جعبه سیاه است. **تست کارکردی(Functional Testing)** در این تست اطمینان حاصل می‌شود که عملکرد برنامه درست است. توجه شود که در این نوع تست برخلاف آزمون واحد می‌توان عملکرد یک سیستم را تست کرد و محدود به تست یک واحد از سیستم

استانداردهای سرویس	مثال
کارکردی (Functional) نیز گفته می‌شود. ▪ **تست جعبه سفید (Whitebox Testing)** در این رویکرد، تست با مکانیستم داخلی یک سیستم سر و کار دارد. به این نوع رویکرد تست ساختاری (Structural) نیز گفته می‌شود.	نمی‌شود. این نوع تست زیر مجموعه تست جعبه‌سیاه است. **تست سیستم(System Testing)** این نوع تست اجازه می‌دهد که از عملکرد برنامه در محیطهای مختلف اطمینان حاصل شود (مثل سیستم عامل های مختلف). این نوع تست زیر مجموعه تست جعبه‌سیاه است. **تست فشار (Stress Testing)** این نوع تست عملکرد برنامه را در شرایط نامطلوب و تحت فشار مورد بررسی قرار می‌دهد. این نوع تست زیر مجموعه تست جعبه‌سیاه است. **تست عملکرد و کارایی(Performance Testing)** تست عملکرد و کارایی که در مجموعه تست جعبه‌سیاه جای می‌گیرد این اطمینان را می‌دهد که برنامه عملکرد و کارایی لازم را در یک مدت زمان مشخص دارا است. **تست قابلیت استفاده (Usability Testing)** این تست زیر مجموعه تست جعبه‌سیاه است. این تست از دیدگاه مشتری انجام می‌شود و در واقع مشخص‌کننده برخی فاکتورها مانند فاکتورهای زیر است: آیا برنامه کاربر پسند است؟ آیا برنامه ساده و قابل یادگیری است؟ آیا برنامه جذاب طراحی شده است؟ **تست پذیرش(Acceptance Testing)** این نوع تست معمولاً از طرف مشتری انجام می‌شود. هدف از این تست، مشخص کردن این است که آیا برنامه نیازهای مشتری را پاسخ می‌دهد و آیا برنامه همان چیزی است که مشتری می‌خواهد. **تست رگرسیون(Regression Testing)** این نوع تست به‌منظور ارزیابی صحت عملکرد سیستم بعد از تغییرات استفاده می‌شود. این نوع تست زیرمجموعه تست جعبه سیاه است. **تست بِتا(Beta Testing)** تستی است که توسط کاربر نهایی یا یک تیم خارج از تیم توسعه انجام می‌شود. هدف تست بِتا پوشش دادن خطاهای غیر منتظره است. این نوع تست زیر مجموعه تست جعبه سیاه است. **تست قابلیت اطمینان(Reliability Testing)** تستی است که تأیید می‌کند که سیستم در زمانی که خرابی یا شرایط غیرعادی رخ می‌دهد به‌صورت صحیح به سیستم‌های افزونه یا کامپیوترهای آماده‌باش سوییچ کرده و به‌صورت صحیح ترمیم می‌شود.

استانداردهای سرویس	مثال
	تست پیکربندی (Configuration Testing) تستی است که اطمینان حاصل می‌کند که برنامه‌کاربردی یا سیستم می‌تواند تمام متغیرهای سخت‌افزار و نرم‌افزار و نیازمندی‌های که تعریف شده است را اداره کند.
	تست نصب (Installation Testing) تستی است که تأیید می‌کند که فرایند نصب نرم‌افزار در محیط‌های متفاوت و شرایط مختلف درست کار می‌کند.
	تست چرخه کسب‌وکار (Business Cycle Testing) تقلیدی (Emulation) از فعالیت‌های انجام‌شده در یک دوره زمانی مشخص است که مربوط به برنامه‌کاربردی است که در حال تست است.
مدیریت پیکربندی نرم‌افزار **(Software Configuration Management)** مدیریت پیکربندی نرم‌افزار عبارت است از مجموعه‌ای از فعالیت‌های پیگیری و کنترل که در طول فرایند توسعه نرم‌افزار اجرا می‌گردد. این فعالیت‌ها با شروع یک پروژه مهندسی نرم‌افزاری آغاز می‌شوند و تنها زمانی پایان می‌یابند که نرم‌افزار از کار می‌افتد. فرایند مدیریت پیکربندی یکی از فرایندهای پشتیبان مهم در طول توسعه نرم افزاراست که به‌منظور برنامه‌ریزی و کنترل فعالیت‌های لازم در آن، ضروری است. از آن‌جایی که تغییر می‌تواند در هر زمانی رخ دهد، فعالیت‌های مدیریت پیکربندی نرم‌افزار می‌تواند شامل شناسایی تغییر، کنترل تغییر، حصول اطمینان از این که تغییر به‌درستی اجرا می‌شود و گزارش تغییر به کسانی که علاقمند به دانستن آن هستند، باشد. مدیریت پیکربندی با پشتیبانی نرم‌افزار که فعالیت‌های آن تنها پس از تحویل نرم‌افزار به مشتری و استفاده از آن به وقوع می‌پیوندند، متفاوت است.	**مدیریت نسخه (Version Management)** مدیریت نسخه مربوط به کنترل و پیگیری نسخه‌های فایل‌های مختلف در طول پروژه نرم‌افزاری می‌شود و می‌تواند شامل قابلیت‌هایی همچون برچسب‌زنی (Labeling)، انشعاب (Branching)، ادغام (Merging)، مقایسه محتوای نسخه‌ها و مدیریت امنیت باشد.
	پیگیری نقص (Defect Tracking) پیگیری نقص مربوط به شناسایی، انتساب و مدیریت نقص‌های کشف شده در یک برنامه کاربردی، محصول یا راهکار می‌شود. ابزارهای پیگیری نقص، داده‌های قابل جستجویی از نقص‌ها برای شناسایی نقص‌ها و خطاهای مرتبط را فراهم می‌کنند.
	مدیریت تغییر (Change Management) مدیریت تغییر مربوط به تغییر کدها و محتوای برنامه‌های کابردی در طول چرخه حیات توسعه نرم‌افزار می‌شود.
	پیگیری موضوع (Issue Tracking) مربوط به ایجاد، تخصیص، پیگیری و منظم‌تر کردن کارها است. اگرچه پیگیری موضوع محدودیت‌هایی را ایجاد می‌کند، اما در نهایت بهره‌وری را بالاتر خواهد برد. اصولاً ابزارهای پیگیری موضوع از هر کسی یا هر سمتی می‌خواهند تا هر درخواستی را از هر شخصی دارد از طریق این ابزارها ایجاد و پیگیری کند.
	مدیریت Release مدیریت Release فرایند مدیریت، برنامه‌ریزی، زمانبندی و کنترل مربوط به یک نرم‌افزار است که در مراحل و محیط‌های مختلفی ساخته می‌شود.

استانداردهای سرویس	مثال
	Requirements Management and Traceability مدیریت و ردگیری نیازمندی‌ها شامل کشف، ذخیره‌سازی و انتشار اطلاعات است. مدیریت و ردگیری نیازمندی‌ها با استفاده از مستندسازی، اندازه‌گیری و تحلیل انحراف‌هایی که در نیازمندی‌های پروژه صورت گرفته، هزینه‌های توسعه نرم‌افزار و مخاطرات مربوطه را کاهش می‌دهد. ردگیری نیازمندی‌ها مؤلفه جدایی‌ناپذیری در پیاده‌سازی کیفیت نرم‌افزار محسوب می‌شود. ردگیری نیازمندی‌ها، چگونگی برآورده کردن نیازمندی‌ها و همچنین تغییراتی که در نیازمندی‌ها رخ می‌دهد را پیگیری می‌کند.
سایر موضوعات مهندسی نرم‌افزار **(Other Issues of Software Engineering)** شامل سایر فناوری‌ها، تکنیک‌ها و استانداردهایی است که برای ساخت و تهیه سیستم‌های نرم‌افزاری مورد استفاده قرار می‌گیرند.	**Commercial Off The Shelf (COTS) Software** شامل نرم‌افزارهای آماده تجاری هستند. این نرم‌افزارها باید از استانداردهای باز و صنعتی پشتیبانی کرده و از تعامل‌پذیری بالایی با سایر محصولات برخوردار باشند. همچنین دسترسی راحت به آموزش و تغییر پارامترها برای شخصی‌سازی در استفاده‌های محلی در آنها باید لحاظ شده باشد.
	Programming language for Application Development شامل زبان‌های برنامه‌سازی است که برای توسعه کاربردهای نرم‌افزاری به‌کار گرفته می‌شوند. این زبان‌ها باید قابلیت حمل کدها و قابلیت همکاری بین کدها را فراهم کنند. همچنین این زبان‌ها باید با مرورگرهای وب و چارچوب‌های توسعه برنامه‌های کاربردی پذیرفته شده سازگار باشند.
	سیستم مدیریت محتوا Content Management System (CMS) سیستم مدیریت محتوا یک سیستم نرم‌افزاری است که به کمک آن محتوا مدیریت می‌شود و شامل نرم‌افزارهایی است که نظام قابل مدیریتی را در ثبت، بروزرسانی و بازیابی محتوا فراهم می‌آورند. این سیستم‌ها الزاماً وابسته به وب نیستند و سیستم‌های مدیریت محتوای وب‌سایت‌ها تنها نمونه‌ای از سیستم‌های مدیریت محتوا هستند. در ایران، به علت گسترش سیستم‌های مدیریت محتوای وب‌سایت‌ها، عبارت CMS تنها به سیستم‌های مدیریت وب‌سایت اطلاق می‌شود. بنابراین می‌توان گفت سیستم مدیریت محتوا چرخه‌زندگی صفحات وب‌سایت را از لحظه ایجاد تا زمان انقراض در بر می‌گیرد و به صاحبان این وب‌سایت‌ها، که لزوماً آشنا با مباحث تخصصی اینترنت، وب و برنامه‌نویسی تحت وب نیستند، اجازه می‌دهد تا بتوانند سایت‌های خود را به‌نحوی حرفه‌ای مدیریت کنند. جوملا (Joomla)، وُرد پِرس (Wordpress) و دروپال (Drupal) نمونه‌هایی از بهترین سیستم‌های مدیریت محتوا محسوب می‌شوند.

فصل سوم

اصول پیاده‌سازی مدل مرجع فناوری

۳ اصول پیاده‌سازی مدل مرجع فناوری

در این بخش تعدادی از اصول که برای استفاده و پیاده‌سازی مدل مرجع فناوری و انتخاب و تعیین مصادیق استانداردهای سرویس باید در نظر گرفته شود ارائه می‌شود.

۳-۱ پشتیبانی از استانداردها و معماری‌های باز

استفاده از فناورهایی که از استانداردها و معماری‌های باز پشتیبانی می‌کنند باید دارای اولویت بیشتری باشد. در این راستا موارد زیر را باید در نظر گرفت:

- فناوری‌هایی که دارای معماری‌ها و استانداردهای باز هستند توسط شرکت‌ها و فروشندگان بیشتری ارائه و پشتیبانی شده و این امکان را فراهم می‌کنند که سازمان‌ها برای تهیه آنها دارای قدرت انتخاب بیشتری باشند. این موضوع سبب صرفه‌جویی اقتصادی برای سازمان‌ها و انعطاف‌پذیری بیشتر برای سیستم‌ها و شبکه‌های آنها می‌شود. همچنین تغییرات غیرقابل پیش‌بینی در توانایی‌ها و استراتژی‌های یک شرکت آسیب کمتری به مشتری‌های آن شرکت می‌رساند.
- استفاده از شبکه‌های با معماری باز و فروشندگانی بی‌طرف انعطاف‌پذیری و سازگاری بیشتری را فراهم کرده و به سازمان‌ها این اجازه را می‌دهد که پاسخ سریعتری به تغییر در نیازمندی‌های کسب‌وکار بدهند.
- استفاده از استانداردها و معماری‌های باز و صنعتی سازگاری بیشتری را برای استقرار، مدیریت و توسعه شبکه‌ها فراهم کرده و به سازمان‌ها این اجازه را می‌دهد که پاسخ سریعتری به تغییر در نیازمندی‌های کسب‌وکار بدهند.

۳-۲ تعامل‌پذیری

سیستم‌ها باید طوری طراحی، توسعه و تقویت شوند که امکان به اشتراک‌گذاری داده‌ها و فرایندها به شکلی مؤثر و برای اهدافی مناسب در داخل سازمان‌ها و بین شرکا فراهم شود. در این راستا موارد زیر را باید در نظر گرفت:

- تحلیلگران سیستم‌ها باید تأثیراتی که طراحی، توسعه و تقویت مربوط به حوزه و استفاده هر یک از برنامه‌های کاربردی بر کل سازمان دارند را در نظر بگیرند.
- به ابزارهای جدید و مناسبی برای به اشتراک‌گذاری داده‌ها و همچنین آموزش جهت استفاده مناسب از این ابزارها نیاز است.
- درک این موضوع ضروری است که در بسیاری از مواقع داشتن هم تعامل‌پذیری و هم امنیت بین محصولات مختلفی که حتی به ظاهر از استانداردهای تعامل‌پذیری پشتیبانی می‌کنند غیرممکن است.

- نیاز به کارگروهای داخلی برای تهیه راهنماهای تعامل‌پذیری وجود دارد.
- استفاده از پروتکل‌های متداول و پرکاربرد جهت افزایش تعامل‌پذیری ضروری است

۳-۳ استفاده از فناوری‌های جدید و اثبات‌شده صنعتی

سازمان‌ها باید پیشرفت فناوری را رصد کرده و از جدیدترین فناوری‌هایی که توانایی خود را به اثبات رسانده‌اند بهره بگیرند. در این راستا موارد زیر را باید در نظر گرفت:

- همواره باید تحلیلی کامل و دقیق از راهکارهای شبکه وجود داشته باشد.
- باید معیارهایی برای ارزیابی فروشندگان و شرکت‌های ضعیف و همچنین فناوری‌های ناکارآمد ایجاد شود.
- اکتشاف فناوری‌های نوین شبکه و نتایج حاصل از بررسی آنها باید به خوبی مدیریت شود.
- مدیریت سبد فناوری[۹] در سازمان‌ها باید ایجاد شود تا مدیریت نظام‌مندی بین سرمایه‌گذاری‌ها، پروژه‌ها و دپارتمان‌های فناوری اطلاعات هر سازمان حاصل شود.

۳-۴ مقیاس‌پذیری، قابلیت دسترسی، پشتیبان‌گیری و بایگانی

فناوری‌های انتخاب شده باید از تغییرات و رشدهای ایجاد شده در نیازمندی‌ها پشتیبانی کنند. برای این منظور نیاز است که برنامه‌های کاربردی و فناوری‌هایی به‌کار گرفته شود که در مقابل تغییرات تطبیق‌پذیر بوده و برای پاسخگویی به افزایش و کاهش نیازمندی‌ها مقیاس‌پذیر باشند. باید از خدمتگزارها، حافظه‌ها و شبکه‌هایی استفاده کرد که توانایی اداره بارِ کاری مربوط به کاربران، برنامه‌های کاربردی و داده‌ها را داشته باشند. زیرساخت فناوری نباید دارای نقطه شکست واحد[۱۰] در پشتیبان و بایگانی باشد و داده‌ها و منابع سیستم‌ها باید همیشه در دسترس باشند. برای این منظور نیاز است سیاست‌های دقیقی در راستای پشتیبان‌گیری و بایگانی‌کردن اتخاذ شود. در راستای مقیاس‌پذیری، قابلیت‌دسترسی، پشتیبانی و بایگانی موارد زیر را باید درنظر گرفت:

- سیستم‌ها باید در زمانی که خرابی یا شرایط غیرعادی رخ می‌دهد به‌صورت صحیح به سیستم‌های افزونه یا کامپیوترهای آماده‌باش سوییچ کرده و به‌صورت صحیح ترمیم شوند.
- سیستم‌ها باید همه درخواست‌ها را اداره کرده و پاسخی مناسب برای آنها ارائه کنند. این موضوع شامل مدیریت خطاها و استثناءها نیز می‌شود.
- در هنگاه رخداد خطا تمام تراکنش‌ها و داده‌ها باید ترمیم شوند.

---

[۹] Technology Portfolio Management

[۱۰] Single Point of Failure

- سکوها باید از ترمیم خرابی‌ها پشتیبانی کنند.
- باید به‌صورت منظم سلامتی سیستم‌ها کنترل شود. برای این منظور استفاده از ابزارهای کنترل و نظارت متمرکز جهت کنترل و نظارت بر سلامتی سیستم‌ها و توافقات سطح سرویسی که از پیش تعریف شده‌اند ضروری است.

۳-۵ تغییرات بر اساس نیازهای کسب‌وکار

تغییرات در برنامه‌های کاربردی و فناوری‌ها باید برای پاسخ به نیازهای کسب‌وکار باشد. این اصل در مقابل تغییر کسب‌وکار به خاطر انتخاب یک فناوری جدید قرار دارد.

پیوست‌ها

پیوست الف: واژه‌نامه

در این بخش واژگان تخصصی که در این سند استفاده شده است، به همراه ترجمه آن آورده شده است.

فارسی	انگلیسی
تست پذیرش	Acceptance Testing
کانال‌های دسترسی	Access Channels
فعالیت	Activity
تلفن آنالوگ	Analogue Telephony
تحلیلی	Analytic
ضد ویروس	Anti-Virus
برنامه‌کاربردی	Application
لایه کاربرد	Application Layer
بایگانی	Archival
حالت انتقال ناهمگام	Asynchronous Transport Mode (ATM)
خصوصیت- مبنا	Attribute-based
احراز هویت	Authentication
مجازشماری	Authorization
اتوماسیون	Automation
قابلیت‌دسترسی	Availability
پشتیبان‌گیری	Backup
تست جعبه‌سیاه	Blackbox Testing
دسترسی سطح بلوکی	Block Level Access
دامنه انتشار	Broadcast Domain
دلال	Broker
گذرگاه	Bus
کسب‌وکار	Business
تست چرخه کسب‌وکار	Business Cycle Testing
منطق کسب‌وکار	Business Logic
مرکز صدور گواهی دیجیتال	Certificate Authority (CA)
مدیریت تغییر	Change Management
مدیر ارشد اطلاعاتی	Chief Information Officer (CIO)

فارسی	انگلیسی
طبقه‌بندی	Classification
همکاری	Collaboration
دامنه برخورد	Collision Domain
ارتباطات	Communications
پذیریش	Compliance
مؤلفه	Component
مهندسی نرم‌افزار به کمک کامپیوتر	Computer Aided Software Engineering (CASE)
محرمانگی	Confidentiality
تست پیکربندی	Configuration Testing
سازگاری	Consistency
محفظه	Container
رِندِر	Content
خدمتگزار محتوا	Content Server
چندسکویی	Cross-platform
توسعه سفارشی و بومی	Customization Development
داشبورد	Dashboard
انبار داده	Data Warehouse
پایگاه‌داده	Database
داده– محور	Data-Centric
پیگیری نقص	Defect Tracking
وابسته	Dependent
توصیف	Description
خط دیجیتال مشترک	Digital Subscriber Line (DSL)
تلفن دیجیتال	Digital Telephony
کشف	Discovery
توزیع	Distribution
پست الکترونیکی	Electronic Mail
دستگاه فناوری تعبیه‌شده	Embedded Technology Device
کدگذاری	Encoding
غنی‌سازی	Enrichment
سازمان	Enterprise
تبادل	Exchange

فارسی	انگلیسی
صریح	Explicit
بیرونی	External
قالب	Format
کارکردی	Functional
تست کارکردی	Functional Testing
دروازه	Gateway
رایانش سبز	Green Computing
مجازی‌سازی سخت‌افزاری	Hardware Virtualization
میزبانی	Hosting
ترکیبی	Hybrid
ضمنی	Implicit
مستقل	Independent
اثبات‌شده صنعتی	Industry Proven
زیرساخت	Infrastructure
تست نصب	Installation Testing
محیط توسعه یکپارچه	Integrated Development Environment (IDE)
یکپارچه‌سازی	Integration
تست یکپارچه‌سازی	Integration Testing
صحت	Integrity
هوش	Intelligence
سیستم تلفن گویا	Interactive Voice Response (IVR)
اتصالات متقابل	Interconnections
واسط	Interface
داخلی	Internal
تعامل‌پذیری	Interoperability
تشخیص و جلوگیری از نفوذ	Intrusion Detection and Prevention
پیگیری موضوع	Issue Tracking
برچسب‌زنی	Labeling
قانونگذاری	Legislation
شبکه محلی	Local Area Network
حداکثر واحد انتقال	Maximum Transmission Unit
اندازه‌گیری	Measurement

فارسی	انگلیسی
خدمتگزار رسانه	Media Server
ادغام	Merging
پیام	Message
فرازبان	Meta Language
میان‌افزار	Middleware
نظارت	Monitoring
سوییچینگ برچسب چند پروتکلی	Multi-Protocol Label Switching
نزدیک به بلادرنگ	Near-real-time
ذخیره‌سازی پیوست‌شده به شبکه	Network Attached Storage (NAS)
شیء	Object
سیستم مدیریت پایگاه‌داده شئ‌گرا	Object-Oriented Database Management System (OODBMS)
سیستم مدیریت پایگاه‌داده شئ‌گرا–رابطه‌ای	Object-Relational Database Management System (ORDBMS)
پروتکل تعیین وضعیت گواهی برخط	Online Certificate Status Protocol (OCSP)
هستی‌شناسی	Ontology
متن باز	Open Source
استاندارد باز	Open Standard
همنواسازی	Orchestration
بسته	Packet
نقطه به نقطه	Peer-to-Peer (P2P)
تست نفوذ	Penetration Test
تست عملکرد و کارایی	Performance Testing
دستگاه‌های جانبی	Peripherals
دستیار دیجیتالی شخصی	Personal Digital Assistant
شخصی‌سازی	Personalization
سکو	Platform
خدمتگزار درگاه	Portal Server
محرمانگی	Privacy
فرایند	Process
کلید عمومی	Public Key
ناشر– متقاضی	Publish-subscribe

فارسی	انگلیسی
صف‌بندی	Queuing
حافظه با دسترسی تصادفی	Random Access Memory (RAM)
آرایه چندگانه دیسک‌های مستقل	Redundant Array of Independent Disks (RAID)
تست رگرسیون	Regression Testing
سیستم مدیریت پایگاه‌داده رابطه‌ای	Relational Database Management System (RDBMS)
تست قابلیت اطمینان	Reliability Testing
امنیت از راه دور	Remote Security
گزارش‌دهی	Reporting
مدیریت و ردگیری نیازمندی‌ها	Requirements Management and Traceability
مسیریاب	Router
قوانین	Rules
مقیاس‌پذیری	Scalability
شِما	Schema
پوسته امن	Secure Shell
لایه سوکت‌های امن	Secure Sockets Layer
انتقال امن	Secured Transport
امنیت	Security
معنایی	Semantic
خدمتگزار	Server
پروتکل معتبرسازی گواهینامه مبتنی بر خدمتگزار	Server-based Certificate Validation Protocol (SCVP)
حوزه دسترسی و تحویل سرویس	Service Access and Delivery Area
حوزه سرویس	Service Area
طبقه سرویس	Service Category
نیازمندی‌های سرویس	Service Requirements
استاندارد سرویس	Service Standard
سرویس پیام کوتاه	Short Message Services (SMS)
نقطه شکست واحد	Single Point of Failure
سرویس‌های شبکه‌های اجتماعی	Social Networking Services
مدیریت پیکربندی نرم‌افزار	Software Configuration Management
ذخیره‌سازی	Storage
تست فشار	Stress Testing

فارسی	انگلیسی
ساختاری	Structural
مدیریت سبد فناوری	Technology Portfolio Management
دورسنجی	Telemetry
پایانه	Terminal
نشانواره	Token
تبدیل	Transformation
انتقال‌دهنده	Transmitter
لایه انتقال	Transport Layer
زبان مدلسازی یکپارچه	Unified Modeling Language (UML)
آدرس یکسان منبع	Uniform Resource Identifier (URL)
تست واحد	Unit Testing
تست قابلیت استفاده	Usability Testing
مدیریت نسخه	Version Management
عمودی	Vertical
ویدئوکنفرانس	Video Conferencing
شبکه محلی مجازی	Virtual LAN (VLAN)
شبکه خصوصی مجازی	Virtual Private Network (VPN)
امضای ویروس	Virus Signature
صدا روی پرتکل اینترنت	Voice over IP (VoIP)
پویشگر آسیب‌پذیری	Vulnerability Scanner
کامپیوتر پوشیدنی	Wearable Computer
استانداردهای دسترسی وب	Web Access Standards
مرورگر وب	Web Browser
خطوط راهنمای دسترس‌پذیری وب	Web Content Accessibility Guidelines (WCAG)
تست جعبه‌سفید	Whitebox Testing
شبکه گسترده	Wide Area Network
بی‌سیم	Wireless
گردش‌کاری	Workflow