به نام خدا

ملاحظات پدافند غیرعامل در سامانه بانک اطلاعاتی(DBMS)

فهرست:

مقدمه

از آنجائیکه امروزه وجود ابزارهای ذخیره سازی و بازیابی اطلاعات نظیر سامانه مدیریت پایگاه‌داده، در دسترسی کاربران به نیازهای اطلاعاتی شان ضروری است، مواردی همچون حفظ امنیت اطلاعات در سامانه های مدیریت پایگاه‌داده و قابل دسترس بودن سامانه های ملی برای کاربران از جمله موارد مرتبط با پدافند غیر عامل است.

سامانه مدیریت پایگاه‌داده[۱] به عنوان یکی از عناصر حیاتی در نظام اطلاعات الکترونیکی هر کشور محسوب می شود. همزمان با افزایش تمرکز سازمان ها و مجامع دولتی و غیر دولتی بر سامانه های مدیریت پایگاه‌داده، تهدیدات حوزه اطلاعات سازمانی بیش از پیش شده است. این مطلب تاکیدی بر این نکته خواهد بود که اطلاعات در هر سازمان به یک عنصر با ارزش و به نوعی به یکی از اساسی ترین دارایی های هر سازمان تبدیل شده است. با توجه به گسترش فناوری اطلاعات و تاکید بر کاهش آسیب‌پذیری در مقابل تهدیدات دشمن، می بایست در گام نخست اقدامات و ملاحظاتی را در جهت بررسی ملاحظات پدافند غیر عامل در طراحی سامانه مدیریت پایگاه‌داده انجام داد.

---

[۱] DataBase Management System

فصل ۱ - تاریخچه

در جدول ذیل به طور خلاصه مهمترین و ارزشمندترین پیشرفت‌ها در سامانه مدیریت پایگاه‌داده بیان شده است:

ردیف	تاریخ	عنوان/ رخداد	سازمان اقدام کننده
۱	پیش از ۱۹۶۰ میلادی	اولین سامانه مدیریت پایگاه‌داده به نام IDS و بیان مدل شبکه‌ای	Charles Bachmann Honeywell
۲	۱۹۶۰ میلادی	سامانه مدیریت اطلاعات و مدل سلسله مراتبی داده	پروژه Apollo در IBM
۳	۱۹۶۵ میلادی	سامانه ذخیره داده یکپارچه و مدل داده شبکه‌ای	General Electric
۴	۱۹۷۱ میلادی	مدل CODASYL و استاندارد سازی بیشتر مدل شبکه‌ای	Data Base Task Group
۵	دهه ۱۹۷۰ میلادی	سامانه مدیریت پایگاه‌داده رابطه‌ای	Edgar Codd
۶	دهه ۱۹۷۰ میلادی	توسعه System R بر اساس تحقیقات Codd	IBM
۷	دهه ۱۹۷۰ میلادی	توسعه سامانه مدیریت پایگاه‌داده رابطه‌ای Ingres	دانشگاه Berkely

ردیف	تاریخ	عنوان/ رخداد	سازمان اقدام کننده
۸	دهه ۱۹۷۰ میلادی	توسعه زبان SEQUEL و توسعه زبان پرس‌وجوی ساخت یافته	IBM
۹	۱۹۷۶ میلادی	انتشار مدل موجودیت داده (ER)	Peter Chen
۱۰	۱۹۷۶ میلادی	انتشار اولین سامانه مدیریت پایگاه‌داده رابطه‌ای	Honeywell Information SYSTEM
۱۱	۱۹۷۹ میلادی	انتشار اولین نسخه تجاری سامانه مدیریت پایگاه‌داده	Oracle
۱۲	اواخر ۱۹۸۰ میلادی	بیان ایده پایگاه‌داده شیء گرا	-
۱۳	۱۹۸۵ میلادی	۱۳ قانون Codd	Edgar Codd
۱۴	دهه ۱۹۹۰	بیان ایده سامانه مدیریت پایگاه‌داده شیء- رابطه‌ای	Micael Stonebraker، Eugene Wang
۱۵	دهه ۱۹۹۰	انباره‌داده OLAP	-
۱۶	نیمه دوم دهه ۹۰	ظهور سامانه مدیریت پایگاه‌داده متن‌باز مانند MySQL، PostgreSQL و غیره	-

ردیف	تاریخ	عنوان/ رخداد	سازمان اقدام کننده
۱۷	سال ۲۰۰۰ تاکنون	سامانه‌های مدیریت پایگاه‌داده خاص منظوره مانند GeoDatabase، bioDatabase	-
۱۸	سال ۲۰۰۰ تاکنون	بیان اهمیت و کاربردهای داده‌کاوی از اطلاعات موجود در پایگاه‌داده با هر مدل داده‌ای	-
۱۹	سال ۲۰۰۵ میلادی	بیان اهمیت امنیت در داده‌کاوی (Privacy preserving)	Srikant ،Agrawal (۲۰۰۰)
۲۰	سال ۱۳۸۷ شمسی	ارائه ملاحظات پدافند غیرعامل در طراحی و مطالعه نمونه الگوی سامانه مدیریت پایگاه‌داده	سازمان پدافند غیرعامل ایران

فصل ۲ - کاربرد بانک اطلاعاتی و نقش آن در جامعه اطلاعاتی

در این بخش به برخی از مهمترین کاربردهای نوین پایگاه‌داده اشاره می کنیم.

۲-۱- پایگاه‌داده چند رسانه‌ای:

امروزه با توجه به رشد روزافزون در زمینه ذخیره و بازیابی اطلاعات چندرسانه ای شامل صوت، عکس و فیلم و عدم کارایی سامانه‌های مدیریت بانک اطلاعاتی معمول برای نگهداری و ویرایش این گونه داده‌ها، نیاز به استفاده از پایگاه‌داده چندرسانه‌ای امری اجتناب ناپذیر است.

۲-۲- پایگاه‌داده بلادرنگ:

پایگاه‌داده بلادرنگ یک سامانه پردازشی است که برای اداره بارهای کاری که وضعیت آن‌ها بطور پیوسته درحال تغییر می باشد، طراحی شده است.

۲-۳- پایگاه‌داده فضایی:

از این نوع پایگاه‌داده جهت نگهداری، ایجاد، پردازش و شبیه سازی اشیاء و اجسام در فضای چند بعدی استفاده می‌شود.

۲-٤- پایگاه‌داده زمانی:

بسیاری از کاربردهای پایگاه‌داده که در ذات خود زمانی هستند مانند سامانه‌های سوابق پزشکی، مدیریت اموال، سیستم‌های حمل و نقل و سیستم‌های مدیریت پروژه می‌توانند بر اساس پایگاه‌داده زمانی پیاده‌سازی شوند.

۲-٥- پایگاه‌داده سیار:

پیشرفت‌های اخیر در زمینه تکنولوژی بیسیم[۱]منجر به محاسبات سیار[۲] گردیده، که مبحث جدیدی در زمینه پردازش و انتقال داده است.

۲-٦- پایگاه‌داده XML:

پایگاه‌داده XML اجازه می‌دهد که داده های با فرمت XML ذخیره شوند. در این نوع پایگاه‌داده می‌توان داده ها را در معرض انواع عملیات مرتبط با داده قرار داد.

---

[۱] Wireless

[۲] Mobile Computing

۲-۷- پایگاه‌داده موازی:

سامانه پایگاه‌داده موازی یکی از سامانه‌هایی است که به دنبال بهبود کارآیی از طریق پیاده‌سازی موازی عملیات مختلف، مانند بارگذاری داده، ساختن شاخص‌ها و پرس‌وجوها است. سامانه‌های موازی سرعت پردازش و عملیات ورودی/خروجی را به‌وسیله استفاده از پردازنده‌ها و دیسک‌ها به‌صورت موازی بهبود می‌بخشند.

۲-۸- پایگاه‌داده توزیع شده:

همانطور که از نام آن مشخص است داده در این نوع پایگاه‌داده در سایت‌های مختلف نگهداری شده و هر سایت نوعاً توسط سامانه مدیریت پایگاه‌داده‌ای که می‌تواند مستقل از بقیه سایت‌ها اجرا شود، مدیریت می‌گردد.

۲-۹- پایگاه‌داده مقیم در حافظه:

در پایگاه‌داده مقیم در حافظه، داده در حافظه اصلی بار می شود نه حافظه جانبی (دیسک). بدلیل ناچیز بودن زمان دسترسی در حافظه و سریعتر بودن نسبت به انجام عملیات ورودی/خروجی بر روی دیسک ها، می تواند برای کاربردهای بلادرنگ مورد استفاده قرار گیرد.

۲-۱۰- پایگاه‌داده استنتاجی:

سامانه‌های پایگاه‌داده استنتاجی بر اساس قوانین[۱] و حقایق[۲] ذخیره شده در پایگاه‌داده خود می توانند استنتاج کنند. برای تعامل با پایگاه‌داده استنتاجی نیاز به یک زبان توصیفی داریم تا مشخص کند چه چیزی باید انجام شود. عموماً در این مورد از زبان Data log که توانایی مشخص کردن پرس و جوها و قوانین و حقایق در پایگاه‌داده استنتاجی را دارد، استفاده می شود.

۲-۱۱- پایگاه داده بیولوژیکی:

پایگاه‌داده بیولوژیکی مجموعه ای از اطلاعات جمع آوری شده از علوم طبیعی است. این مجموعه اطلاعات شامل حوزه های تحقیق ژنومی، پروتئینی، متابولیسم ها، و غیره است. این اطلاعات به طور کلی کارکردهای ژن ها، ساختار آن ها، تاثیرات آزمایشات مختلف و نتایج حاصل از آن ها و نیز شباهت های ترتیبی و ساختاری بیولوژیکی را در خود ذخیره می نمایند.

---

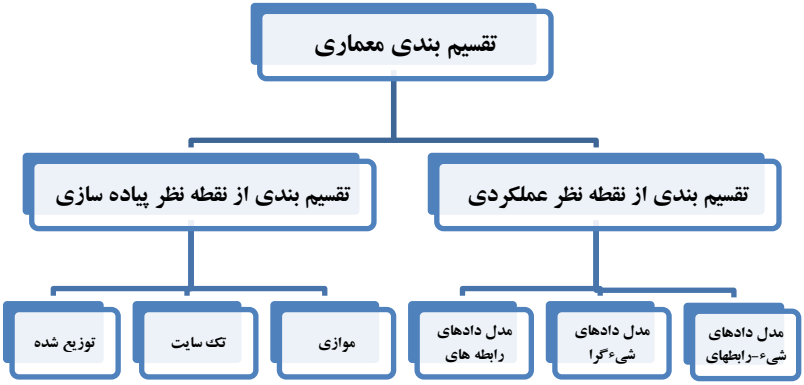
[۱] Rules

[۲] Facts

فصل ۳ - معماری بانک اطلاعاتی

۳-۱- طبقه‌بندی سامانه مدیریت پایگاه‌داده:

ارائه یک معماری برای سامانه مدیریت پایگاه‌داده مبتنی بر نیاز است (خاص منظوره). نمی توان یک معماری واحد و همه منظوره برای پوشش همه نیازها ارائه کرد. هر سازمانی متناسب با نیازهای خود از یک معماری خاص استفاده می کند. به عنوان مثال معماری سامانه های مدیریت پایگاه‌داده در حوزه نظامی متفاوت از معماری آن در سامانه های مدیریت پایگاه‌داده کسب و کار است. با این حال سامانه های مدیریت پایگاه‌داده از دو منظر عملکرد[۱] و پیاده سازی[۲] قابل دسته بندی است.



[۱] Functionality

[۲] Implementation

شکل ۱. تقسیم بندی معماری از مناظر عملکردی و پیاده سازی

۳-۱-۱- سامانه‌های مدیریت پایگاه‌داده از منظر عملکرد:

بررسی معماری از منظر عملکرد مبتنی بر مدل داده ای است که سامانه بر اساس آن شکل گرفته است. متناسب با هر مدل داده، یکسری مؤلفه در سامانه وجود دارد که ممکن است در سامانه هایی با مدل های داده دیگر متفاوت باشد. امروزه تنها به سه مدل زیر توجه می شود:

- مدل داده رابطه ای[۱]:

مبتنی بر مفهوم رابطه در نظریه مجموعه ها است. در این مدل تمامی موجودیت ها و روابط بین آن ها به شکل رابطه (جدول) نمایش داده می شود.

- مدل داده شیء گرا[۲]:

این مدل به منظور تعامل با زبان های برنامه نویسی شیء گرا طراحی شده است. به طور کلی در زمانی که نیازهای تجاری در نرم افزار حکمفرماست، نیازمند کارایی بالایی هستیم و ساختار داده نیز ساختاری پیچیده است، این نوع مدل از کارآمدی بسیار بالایی برخوردار است.

---

[۱] Relational

[۲] Object Oriented

❖ مدل داده شیء- رابطه ای[۱]:

این مدل به منظور رفع تمامی مشکلات مدل رابطه ای (عدم توانایی در تعریف نوع داده ای جدید و تعاملات کاربردی جدید) و شیءگرا (پیچیدگی بیش از حد SQL و عدم پیاده سازی یکسان) به کار گرفته شده است. این مدل، مفاهیم ساده موجود در مدل داده رابطه ای را با توانایی تعریف نوع داده جدید و متدهای شیء گرایی تلفیق می کند.

۳-۱-۲- سامانه‌های مدیریت پایگاه‌داده از منظرپیاده‌سازی:

از منظر پیاده سازی، سامانه های مدیریت پایگاه‌داده را می توان به سه دسته کلی زیر تقسیم کرد:

❖ پایگاه‌داده متمرکز یا تک سایت[۲]:

در این نوع پیاده‌سازی، داده و سامانه مدیریت پایگاه‌داده تنها بر روی یک کامپیوتر قرار دارند، لذا تنها یک نسخه از پایگاه‌داده اجرا می شود.

---

[۱] Object Relational

[۲] Single-Site

- پایگاه‌داده نامتمرکز یا توزیع‌شده[۱]:

داده در این نوع پایگاه‌داده، در سایت‌های مختلف نگهداری می شود و هر سایت به نوعی توسط سیستم مدیریت پایگاه‌داده ای که می تواند مستقل از بقیه سایت‌ها اجرا شود، مدیریت می گردد.

- پایگاه‌داده موازی[۲]:

سامانه پایگاه‌داده موازی یکی از سامانه‌هایی است که به منظور افزایش کارآیی، از موازی سازی عملیات مختلف مانند بارگذاری داده، ساختن شاخص‌ها و پرس‌وجوها استفاده می‌کند.

۳-۲- مؤلفه‌های اساسی یک سامانه مدیریت پایگاه‌داده:

۳-۲-۱- مولفه های معماری از منظر نرم‌افزاری:

بر اساس تعریف سیستم مدیریت پایگاه‌داده و بر مبنای نگاه نرم افزاری، می‌توان سه رکن پایگاه‌داده، سیستم مدیریت پایگاه‌داده و ابزارهای تحلیل را مانند شکل ۲ به صورت سه لایه مجزا، کلان و مرتبط با یکدیگر بیان نمود.

---

[۱] Distributed

[۲] Parallel

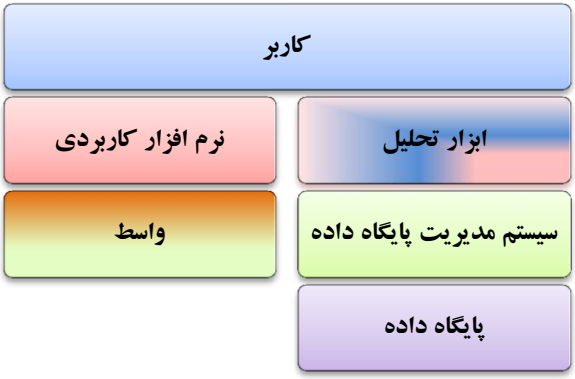
کاربران تنها از طریق لایه سیستم مدیریت پایگاه‌داده و ابزار های تحلیل با پایگاه‌داده در ارتباط بوده و توانایی برقراری ارتباط مستقیم با آن را ندارند. البته بسیاری از متخصصین به این اصل معتقدند که کاربران می توانند از طریق برنامه های کاربردی توسعه یافته توسط مهندسین نرم افزار، با پایگاه‌داده ارتباط مستقیم برقرار کنند.

شکل ۲. جایگاه واسط نرم افزاری در مدل سه لایه نرم افزاری

اساس این گزارش بر این اصل استوار است که برقراری ارتباط میان برنامه کاربردی با پایگاه‌داده تنها از طریق یکسری واسط ارتباطی نرم افزاری مانند ODBC، JDBC وADO (در بسیاری از منابع از آن به عنوان یک پروتکل ارتباطی یاد می شود، اما ما در نگاه کلان آن را واسط ارتباطی می نامیم) صورت می‌پذیرد که در درگاه های ورودی و خروجی مابین برنامه کاربردی و سیستم مدیریت پایگاه‌داده قرار دارد. در شکل۳ جایگاه واسط نرم افزاری در مدل سه لایه نرم افزاری نشان داده شده است.

نکته قابل توجه در مورد ابزارهای تحلیل این است که ابزارهای تحلیل باید قابلیت تعامل با سیستم مدیریت پایگاه‌داده را داشته باشند. در مدل بالا، ابزارهای تحلیل همانند برنامه‌های کاربردی دیده شده و هیچ تقابلی با مدل بیان شده در شکل۳ ندارند.

همچنین کانال ارتباطی برای تبادل اطلاعات مابین سامانه مدیریت پایگاه‌داده و پایگاه داده نیز می‌بایست از طریق یک کانال امن صورت گیرد.



شکل ۳. سطوح انتزاعی سیستم مدیریت پایگاه‌داده

۳-۲-۲-مولفه های معماری از منظر نماهای مختلف داده

داده درون پایگاه‌داده نشان دهنده موجودیت های درون/میان سازمانی و روابط موجود میان آن ها است. به طور مثال دانشگاه دارای موجودیت هایی مانند کلاس، درس، استاد و غیره است.

یک مدل داده ای[۱]، مجموعه ای از ساختارهای توصیف داده سطح بالاست که بسیاری از جزئیات ذخیره سازی داده در سطح پایین را محو می‌کند. هر سیستم مدیریت پایگاه‌داده مبتنی بر یک مدل داده ای است. از جمله مدل های داده ای می‌توان به موارد زیر اشاره کرد:

- مدل سلسله مراتبی[۲]
- مدل شبکه ای[۳]
- مدل رابطه ای
- مدل شی گرا
- مدل شی- رابطه ای

در محصولاتی مانند IMS شرکت IBM، از مدل سلسله مراتبی پشتیبانی می شود. در محصولاتی مانند IDS و IDMS از مدل

---

[۱] Data Model

[۲] Hierarchical

[۳] Network Model

شبکه ای پشتیبانی می شود. در محصولاتی مانند DB۲، Oracle، Sybase، Teradata، Paradox MS SQL Server از مدل رابطه ای پشتیبانی می شود. در محصولاتی مانند Object Store و Versant از مدل شی ءگرا پشتیبانی می شود. در محصولاتی مانند Oracle ، Object Store، Informix Versant و محصولاتی از شرکت IBM از مدل شیء- رابطه ای پشتیبانی می شود.

بنابر استاندارد ANSI/SPARC دریک سامانه مدیریت پایگاه داده، داده در سه سطح انتزاعی توصیف می شود. این سه سطح عبارتند از سطوح مفهومی، فیزیکی و خارجی.

همانطور که در شکل ۴ نشان داده شده است، شمای مفهومی[۱] یا منطقی[۲] به توصیف داده های ذخیره شده در قالب مدل داده سیستم مدیریت پایگاه‌داده می پردازد. شمای فیزیکی[۳] یا داخلی، مشخص کننده جزئیات فیزیکی بیشتری است. شمای خارجی[۴] نیز عموماً بر حسب مدل داده ای توصیف می شود با این تفاوت که این شمای[۵] متناسب با نیاز گروهی خاص، سفارشی و پیکربندی شده است.

---

[۱] Conceptual schema

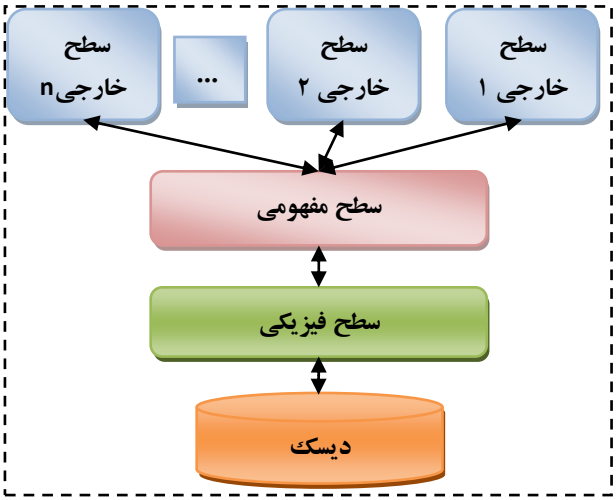
[۲] Logical schema

[۳] Physical schema

[۴] External schema

[۵] به توصیفی از داده توسط یک مدل داده در اصطلاح **شمای**[۵] گفته می شود.

هر سامانه مدیریت پایگاه‌داده دارای یک شمای فیزیکی، یک شمای مفهومی و تعداد بیشماری شمای خارجی می باشد.



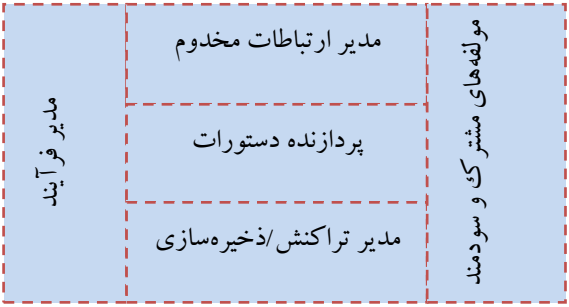
شکل ۴. سطوح انتزاعی سیستم مدیریت پایگاه داده

۳-۲-۳-مولفه های معماری از منظر کارکردها و مؤلفه‌های درونی

در منابع متعدد، سامانه مدیریت پایگاه‌داده را با سه جزء اصلی آن یعنی مدیریت تراکنش/ذخیره سازی، پردازنده پرس و جو و منبع ذخیره سازی می شناسند. هر کدام از این سه مؤلفه خود دارای زیرمؤلفه های دیگری است.

با توجه به شکل ۵، سامانه مدیریت پایگاه‌داده از پنج مؤلفه اصلی تشکیل شده است. این مؤلفه‌ها عبارتند از:

- مدیر ارتباطات مخدوم[۱]
- مدیر فرایند[۲]
- پردازنده دستورات[۳]
- مدیر تراکنش / ذخیره سازی[۴]
- مدیر مؤلفه های مشترک و برنامه های سودمند[۵]



شکل ۵. نمای سطح کلان معماری مؤلفه‌ای

[۱] Client Communication Manager

[۲] Process Manager

[۳] Statement Processor

[۴] Transaction/Storage Manager

[۵] Shared component & utility tools

به منظور تعامل با سامانه مدیریت پایگاه‌داده، اولین کار برقراری ارتباط از جانب یک واسط ارتباطی است. این واسط ارتباطی می بایست ابتدا به مدیر ارتباطات مخدوم متصل گردد. یکی از روش های امن سازی، استفاده از پروتکل های امن جهت برقراری ارتباط با مدیر ارتباطات مخدوم است. بسیاری از سامانه های مدیریت پایگاه‌داده با حملات عدم دسترس پذیری[۱] مواجه می شوند که می بایست با استفاده از معیارهایی، این حملات کشف و از آن جلوگیری شود.

پس از دریافت دستور و عبور از مدیر ارتباطات مخدوم، یک ریسمان[۲] از جانب سامانه مدیریت پایگاه‌داده به آن اختصاص داده می شود؛ این کار توسط مدیر فرایند صورت می گیرد. یکی از مهمترین وظایف این بخش کنترل ورود[۳] است.کنترل ورود، عملیات نظارت و کنترل درخواست ها و تعداد ارتباطات مجاز را مدیریت می کند.

پس از انجام این کار، دستور توسط پردازنده دستورات قابل اجرا است. در این بخش ابتدا کنترل می شود که آیا کاربر مجاز به انجام

---

[۱] DoS

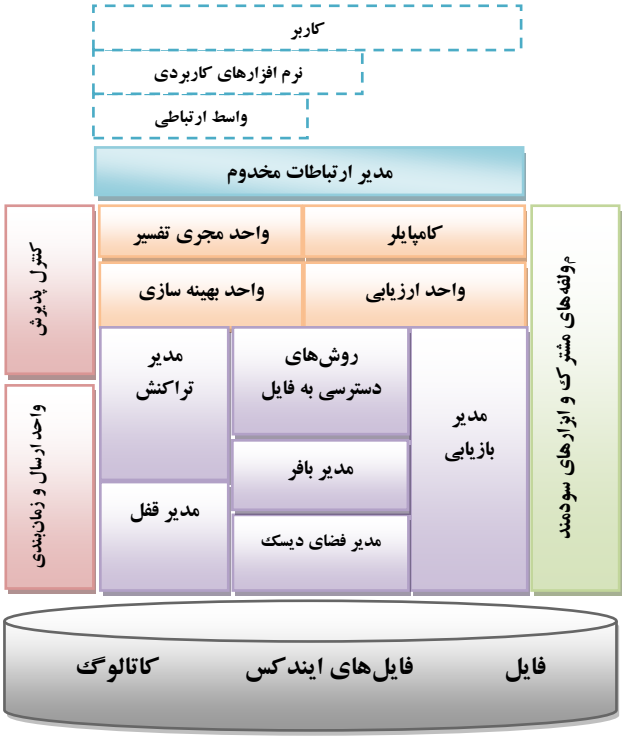
[۲] Thread

[۳] Admission Control

این دستورات هست یا خیر. سپس دستورات کامپایل شده و به یک تفسیر اجرا[۱] تبدیل می شود. این تفسیرخود نیازمند بهینه سازی است. این تفسیر بهینه شده[۲] توسط بخشی به نام واحد اجرای تفسیر، اجرا می گردد. تفسیر بدست آمده نیازمند چند واکشی داده از پایگاه‌داده است. این کار توسط مدیر تراکنش/ذخیره سازی که مدیریت تمامی دسترسی ها به داده و دستکاری آن را بر عهده دارد، انجام می گیرد.

[۱] Execution explanation

[۲] Optimized



شکل ۶. زیر مؤلفه‌ها در معماری یک سیستم مدیریت پایگاه‌داده

یک مدیر بافر[۱] در این بخش وجود دارد که در مورد زمان و نحوه مبادله داده‌ها میان دیسک و حافظه تصمیم گیری می کند. دو بخش مهم دیگر این مؤلفه مدیر قفل[۲] که وظیفه مدیریت دستورات

[۱] Buffer manager

[۲] Lock Manager

همروند و مدیر ثبت وقایع[۱] که اطمینان از پایداری[۲] تراکنش ها را بر عهده دارند.

۳-۲-٤-سایر مؤلفه‌ها:

در بسیاری از سامانه‌های مدیریت پایگاه‌داده علاوه بر مؤلفه‌های توضیح داده شده، ابزارهای سودمند دیگری وجود دارد که باعث افزایش قابلیت های هر سامانه مدیریت پایگاه‌داده می گردد. برخی از این مؤلفه ها در ادامه به صورت مختصر مورد بررسی قرار گرفته است.

❖ سرویس‌های انعکاس[۳]:

برخی مواقع، کپی کردن پایگاه‌داده در سرتاسر یک شبکه و بروز رسانی متوالی آن ها بسیار مفید است. این سرویس به منظور فراهم کردن کارکردهای عملی از سامانه مدیریت سامانه پایگاه‌داده توزیع شده در محیط های جغرافیایی پراکنده به کار می رود.

❖ مدیر کاتالوگ[۱]:

---

[۱] Log manager

[۲] Durability

[۳] Replication Services

کار این مؤلفه، نگهداری اطلاعات فراداده[۲] است. بسیاری از سامانه‌های تجاری امروزی با روش های مختلف مانند کنترل دسترسی، از دسترسی نابجای کاربران به اطلاعات کاتالوگ آن جلوگیری می کنند.

❖ مؤلفه تخصیص حافظه[۳]:

سامانه مدیریت پایگاه‌داده به منظور انجام بسیاری از کارهای دیگر خود نیازمند تخصیص حافظه است. مکانیزم تخصیص حافظه پایگاه‌داده تجاری مبتنی بر مفهوم[۴] است. حافظه ای از این دسته، بیانگر ساختمان داده ای در حافظه است که لیستی از حافظه های مجازی متوالی را در خود نگهداری می کند. به این حافظه مجازی متوالی در اصطلاح مخزن حافظه[۵] اتلاق می شود.

❖ زیر سامانه مدیریت دیسک[۶]:

---

[۱] Catalog manager

[۲] فرا داده، اطلاعات کنترلی و مدیریتی در مورد داده اصلی را شامل می‌شود.

[۳] Memory Allocator

[۴] Context-Based

[۵] Memory Pool

[۶] Disk Management Subsystems

وظیفه زیر سامانه مدیریت دیسک تعامل با انواع دیسک هاست. سامانه های مدیریت پایگاه‌داده ترجیح می دهند که یا به صورت مستقیم با دستورات ورودی/خروجی با دیسک تعامل برقرار کنند یا از سیستم فایل خود استفاده نمایند. بسیاری از سامانه‌های مدیریت پایگاه‌داده به منظور ایمن نمودن خود در مقابل افشای اطلاعات از روش های رمزنگاری استفاده می کنند.

۳-۳- امنیت در سامانه مدیریت پایگاه‌داده:

امروزه سازمان ها بیش از پیش وابسته به اطلاعاتی هستند که افراد، منابع و امور سازمان را مدیریت می کنند. بنابراین تخلف در امنیت اطلاعات ممکن است کل سیستم را به خطر اندازد. همه روزه با توجه به تلاش محققان در مورد ساخت یک سیستم کامپیوتری امن، گزارشاتی مبنی بر انواع روش‌های نفوذ و سوء استفاده از سیستم، در منابع متعدد منتشر می گردد.

امنیت پایگاه داده یعنی محافظت از تلاش های تبهکارانه برای سرقت[۱]، تغییر[۲] و یا تخریب[۳] داده های پایگاه‌داده.

---

[۱] Disclosure

[۲] Alternation

[۳] Destruction

امنیت[۱] از جمله مفاهیمی است که باید در تمام لایه های یک سیستم کامپیوتری اعم از سخت افزار، شبکه، سیستم عامل، بانک اطلاعات و... لحاظ شود. تأمین امنیت هر سازمان به صورت خاص[۲] انجام می شود.

۳-۳-۱- اهداف امنیت:

هنگام صحبت از یک پایگاه‌داده امن معمولاً سه هدف در رابطه با آن طرح می شود:

الف- محرمانگی[۳]: محرمانگی به معنای عدم دسترسی و مشاهده کاربران غیر مجاز به اطلاعات تعریف می شود. به عنوان مثال یک فرد نباید اجازه مشاهدهٔ اطلاعات سایر افراد را داشته باشد.

ب- جامعیت[۴]: کاربران مجاز می توانند فقط داده های مجاز را بصورت مجاز تغییر دهند. به عنوان مثال دانشجویان می توانند نمرات خود را ببینند اما اجازه تغییر آن را ندارند. جامعیت به صورت جلوگیری از تغییر، حذف و یا دخالت ناخواسته و نادرست در اطلاعات نیز تعریف می شود.

---

[۱] Security

[۲] Ad-hoc

[۳] Confidentiality

[۴] Integrity

ج- دسترس‌پذیری[۱]: عملکرد سیستم نباید به صورت ناخواسته، حتی لحظه ای قطع شود. به عنوان مثال استاد درسی که اجازه تغییر نمرات را دارد همواره باید بتواند این عمل را انجام دهد.

برای رسیدن به سه هدف فوق باید سیاست‌های امنیتی واضح و مشخصی تدوین شود. به عبارت دیگر باید به طور کامل و صریح روشن شود که چه بخش یا بخش‌هایی از داده ها باید محافظت شوند و چه کاربرانی اجازه دسترسی به چه قسمت‌هایی از داده ها را دارند.

۳-۳-۲- گام‌های اساسی در تأمین امنیت پایگاه‌داده:

برای برقراری امنیت در سامانه پایگاه‌داده، ابتدا با کمک مکانیزم های تصدیق هویت کاربر[۲] مثل کلمهٔ عبور[۳] اطمینان حاصل می کنیم که کاربر وارد شده به سیستم یک کاربر مجاز است. البته این امکان نیز وجود دارد که کاربری غیرمجاز بتواند به نحوی مجوز ورود را به دست آورد (مثلاً از کلمهٔ عبور یک کاربر مجاز استفاده کند). از این جهت، تهدیدات امنیتی یک سامانه پایگاه‌داده را به دو دسته داخلی و خارجی تقسیم بندی می کنیم .

---

[۱] Availability

[۲] Authentication

[۳] Password

در مرحله بعد که مطمئن هستیم کاربری که وارد سیستم شده اجازه ورود داشته است، با مکانیزم های کنترل دسترسی (مجوز دهی به کاربر)، فقط مجوزهای دسترسی به داده هایی مشخص را به او تخصیص می دهیم.

اما این کاربر مجاز ممکن است روی همان داده های مجاز خود نیز تغییرات غیر مجاز انجام دهد (مثل انتساب مقداری منفی برای سن یک فرد). مقابله با چنین تهدیداتی به تضمین جامعیت سیستم بر می گردد که با قرار دادن قیود جامعیت و استفاده از مکانیزمهایی همچون Assertion[۱]، Trigger[۲] و... از داده های بانک اطلاعات مراقبت می شود.

۳-۳-۳-رمزنگاری و تاثیر آن در امنیت سامانه مدیریت پایگاه‌داده:

در سامانه مدیریت پایگاه‌داده از رمزنگاری به عنوان آخرین خط دفاعی نام برده می شود. رمزنگاری در حقیقت پوشاندن یک پیام عادی با استفاده از قواعد و قوانین ریاضی است. امروزه مفاهیم پیشرفته ریاضی در رمزنگاری نقشی مهم دارند. برای رمز کردن یک پیام عادی[۳] نیاز به یک کلید داریم که بتوانیم بر اساس آن و الگوریتم رمزنگاری متن عادی خود را به صورت پیام رمز شده

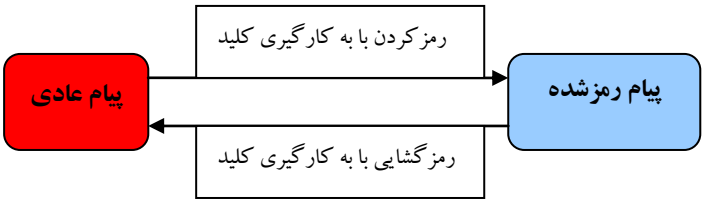
---

[۱] تایید ادعا

[۲] تصدیق

[۳] Plain Text

درآوریم. مراحل کار رمز شدن یک متن عادی در شکل ۷ نشان داده شده است.



شکل ۷. نحوه عملکرد رمزنگاری بااستفاده از کلیدها

برخی از اهداف که می توان با استفاده از رمزنگاری درسامانه مدیریت پایگاه داده به آنها رسید در زیر آمده است.

- تصدیق هویت کاربر وارتباط امن
- امنیت سامانه و شبکه
- کنترل دسترسی
- جلوگیری از استنتاج
- نگهداری جامعیت و پوشیدگی
- محافظت از داده های خصوصی در مقابل دسترسی های کاربران غیر مجاز در کنترل دسترسی سلسله مراتبی

فصل ٤ - نیازها و ویژگی‌های بانک اطلاعاتی

سامانه مدیریت پایگاه‌داده[۱] به عنوان یکی از پیچیده‌ترین سامانه‌های نرم‌افزاری در قیاس با سایر سامانه‌های نرم‌افزاری دیگر از قبیل کامپایلر، سیستم عامل و... است.
مهمترین موارد قابل طرح در طراحی یک سامانه مدیریت پایگاه‌داده عبارتند از:

۱) سامانه مدیریت پایگاه‌داده، زبان پایگاه‌داده و غیره نباید هیچ یک از قوانین پایه ای ریاضیات را نقض کنند (همانگونه که در مدل رابطه‌ای در مورد مجموعه‌ها رعایت می‌شود).
۲) نمایش داده‌ها و شیوه دسترسی به داده‌ها باید از دید کاربر پنهان باشد. بجز قابلیت‌های محدودی که به DBA[۲] ارائه می‌شود، پس از ایجاد ساختارهای داده‌ای، مسئولیت نگهداری، به‌روز درآوردن، حذف و... برعهده سامانه مدیریت پایگاه‌داده است و نه کاربر یا DBA.
۳) مرزهای دقیق سامانه مدیریت پایگاه‌داده باید در دو زمینه جداسازی دقیق انجام دهد:

---

[۱] Data Base Management System (DBMS)

[۲] Data Base Administrator

الف) کاربردها و قابلیت‌های مربوط به کارایی (مثلاً شاخص‌ها)

ب) قابلیت‌های منطقی و معنایی[۱] (مثلاً کلید[۲] و یکتا بودن آن)

به طور کلی کاربر نباید درگیر مورد اول شود. مثلاً اگر DBA شاخص[۳] را حذف کند نباید در منطق آن خدشه‌ای وارد شود.

۴) ممانعت از قفل کردن طولانی مدت غیرمجاز

ممکن است گاهی داده کاربر برای مدت زمان بسیار طولانی قفل شود که به منظور پرهیز از این رویداد DBA می‌تواند برای آنها فرصت[۴] تعیین کند.

۵) مسائل تعامدی[۵] در طراحی سامانه مدیریت پایگاه‌داده

هر گونه به‌کارگیری یک قابلیت درکنار قابلیتی دیگر در طراحی سامانه مدیریت پایگاه‌داده باید دلایل شفاف، غیراحساسی، منطقی و قابل دفاع داشته باشد.

۶) شاخص‌های مبتنی بر دامنه

---

[۱] Semantic & Logic

[۲] Key

[۳] Index

[۴] Timeout

[۵] Orthogonal

برای سامانه مدیریت پایگاه‌داده سفارشی و وابسته به نرم‌افزار، امکان ایجاد و حذف شاخص‌های مبتنی بر دامنه به کاربران مجاز ارائه می‌شود که می‌تواند در سامانه مدیریت پایگاه‌داده مبتنی بر سخت‌افزار خاص نیز منجر به افزایش کارایی گردد.

۷) آمارهای پایگاه‌داده

نحوه به‌روز شدن اطلاعات آماری پایگاه‌داده که توسط واحدهای مختلف از جمله در بهینه‌سازی پرس‌وجو استفاده می‌شود و تصمیم در مورد اینکه توسط چه کاربری، با چه تناوبی و... انجام گردند و نیز نحوه به‌کارگیری آنها.

۸) ممانعت اتوماتیک در برابر عملکرد نادرست[۱]

در صورت وقوع شرایطی که در آن برخی از تراکنش‌ها ساقط[۲] شوند، سامانه مدیریت پایگاه‌داده باید دقت کند که این ساقط شدن، اثر مخرب روی پایگاه‌داده به جای نگذارد.

۹) ترمیم اتوماتیک درصورت عملکرد نادرست

۱۰) امکان ایجاد انواع داده جدید بر اساس انواع داده توکار سامانه

۱۱) سادگی

---

[۱] Malfunction

[۲] Fail

۱۲) دسترسی‌ها به پایگاه‌داده از طریق زبان های پایگاه‌داده

۱۳) امکان تعریف توابع[۱]

۱۴) اجرای اتوماتیک دستورات بدون توقف یا شکست

مواردی از این قبیل که ناشی از عواملی نظیر کمبود حافظه یا تعداد زیاد پارامترها و... است.

۱۵) بایگانی[۲] اطلاعات به طور خودکار و دوره‌ای

۱۶) پرهیز از عملگرهای پرهزینه و جایگزینی آنها با عملگرهای مؤثرتر

۱۷) مسئولیت سامانه مدیریت پایگاه‌داده در قبال رمز گذاری و رمزگشایی داده ها

۱۸) چند زبانی بودن (ارتباط دو جانبه بین سامانه مدیریت پایگاه‌داده و زبانهای برنامه‌نویسی)

---

[۱] Function

[۲] Archive

فصل ۵ – استانداردهای بانک اطلاعاتی

با توجه به عدم وجود استاندارد رسمی خاص در زمینه طراحی و ارزیابی سامانه مدیریت پایگاه‌داده، سعی شده است به استانداردهایی که لزوماً خاص سامانه های مدیریت پایگاه داده نیست ولی به نوعی با آن مرتبط است، در جدول ذیل اشاره گردد.

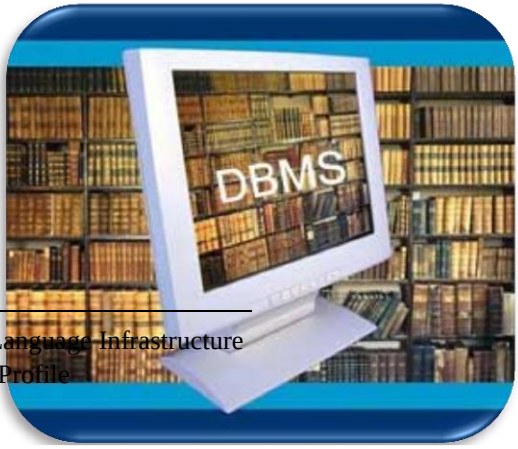
نام استاندارد	طراحی	پیاده سازی	ارزیابی	امنیتی	کشور/سازمان ارائه کننده	توضیحات
FIPS	✓	✓	✓		آمریکا / NIST[۱]	مرتبط با درون نگاری ماژول های رمزنگاری در سیستم های کامپیوتری و مخابراتی است
ISO/IEC ۱۵۴۰۸ (CC)[۲]	✓	✓	✓		ISO	

[۱] National Institute of Standards and Technology

[۲] Common Criteria

نام استاندارد	طراحی	پیاده سازی	ارزیابی	امنیتی	کشور/سازمان ارائه کننده	توضیحات
ITSEC	✓	✓	✓		فرانسه آلمان هلند انگلستان	بوسیله استاندارد *common criteria* جایگزین شد
TCSEC	✓	✓	✓		آمریکا / وزارت دفاع	بوسیله استاندارد common criteria جایگزین شد
Ansi/x۳/ Sparc		✓	✓	✓		مدلی سه لایه ای قابل استفاده در *طراحی* DBMS
ODMG	✓		✓	✓	Object Data Management Group	استاندارد مربوط به پایگاه داده های شی و نگاشت های مرتبط شی – رابطه ای
SQL: ۲۰۰۳	✓		✓	✓	ANSI ISO	یک استاندارد برای زبان پرس و جوی ساخت یافته (استاندارد SQL: ۲۰۰۶ نیز توسط ISO تدوین گردیده که ویژگی اصلی آن پشتیبانی جامع و کاملتر از XML می باشد)
JDBC	✓		✓	✓	SUN Microsystems	استاندارد ارتباطی با پایگاه داده

نام استاندارد	طراحی	پیاده سازی	ارزیابی	امنیتی	کشور/سازمان ارائه کننده	توضیحات
ODBC	✓		✓	✓	ISOMicrosoft SQL Access Group X/Open Group Simba Technology	استاندارد ارتباطی با پایگاه داده
XQuery	✓		✓	✓	W۳C	استفاده از پرس و جوهای XML
CLI[۱]	✓		✓	✓	Microsoft ISO/IEC ۲۳۲۷۱ ECMA -۳۳۵	استانداردی برای زیربنای زبان معمول
DBMS PP[۲]	✓	✓	✓		Oracle	نمایه محافظتی برای مشخص کردن نیازمندی‌های سامانه‌های مدیریت پایگاه داده در سازمان



[۱] Common Language Infrastructure
[۲] Protection Profile

فصل ٦ - ملاحظات پدافند غیر عامل

ملاحظات پدافند غیر عامل که باید در این حوزه رعایت شوند به اختصار در ذیل آورده شده است:

❖ به دلیل عدم توانایی سامانه مدیریت پایگاه‌داده رابطه ای در تأمین نیاز کاربردهای جدید همچون چندرسانه ای و بلادرنگ و ناتوانی آن در تعریف انواع داده جدید از جانب کاربر، همچنین عدم وجود استاندارد واحد در سامانه‌های مدیریت پایگاه‌داده شیء-گرا و پیچیدگی زبان انحصاری SQL آن، بسیاری از رویکردهای مطالعاتی و تجاری امروز مبتنی بر سامانه مدیریت پایگاه‌داده شیء- رابطه‌ای است. بدین منظور، ساخت سامانه مدیریت پایگاه‌داده مبتنی بر مدل داده ای شیء رابطه ای الزامی است.

❖ از آنجا که توزیع و تکرار داده ها در سایت‌های مختلف منجر به افزایش دسترس‌پذیری و قابلیت اطمینان سامانه مدیریت پایگاه‌داده می‌شود، لذا سامانه مدیریت پایگاه‌داده ملی باید به صورت نامتمرکز یا توزیع شده پیاده سازی شود.

❖ کانال ارتباطی مابین سامانه مدیریت پایگاه‌داده و خود پایگاه‌داده می بایست از طریق کانال ارتباطی امن صورت گیرد. مکانیزم امن سازی مناسب همچون رمزگذاری در این بستر ضروری است.

می بایست مکانیزم هایی مبنی بر رمزگذاری در فرستنده و گیرنده از جانب سامانه مدیریت پایگاه‌داده تعبیه شود.

❖ استفاده از یک واسط ارتباطی ایمن به منظور تعامل با سامانه مدیریت پایگاه‌داده ضروری بوده و این سامانه می بایست به صورت بومی طراحی و پیاده سازی شود.

❖ مدیر ارتباطات مختوم می بایست از مکانیزم های کشف حملات عدم دسترس پذیری استفاده نماید.

❖ سیستم فایل مورد استفاده سامانه مدیریت پایگاه‌داده ملی لازم است سیستم فایل تعبیه شده ملی باشد.

❖ به منظور جلوگیری از دسترسی هر کاربر عادی به کاتالوگ سامانه مدیریت پایگاه‌داده که بخش حیاتی هر سامانه است، می بایست مکانیزمی مانند کنترل دسترسی، تمامی تعاملات کاربران با آن را کنترل کند. در بسیاری از سامانه‌ها ثبت وقایع در مورد تعاملات کاری کاربران و کاتالوگ بکار گرفته می‌شود تا در مواقع اضطراری سامانه به وسیله آن به حالت معمول باز گردد.

❖ به منظور حفظ امنیت بیشتر در سامانه مدیریت پایگاه‌داده، می توان زیر سامانه مدیریت دیسک را به یک الگوریتم رمزنگاری مجهز نمود. این روش روند کشف اطلاعات توسط اشخاص/سامانه‌های دیگر را غیر ممکن یا حداقل بسیار کند می کند.

❖ به منظور افزایش قابلیت اطمینان سامانه مدیریت پایگاه‌داده، پایداری و دسترس‌پذیری آن از سرویس های انعکاس استفاده می‌شود. در میان روش های انعکاس، روش مبتنی بر ثبت وقایع نسبت به سایر روش ها کارآمدتر است.

❖ در مکانیزم تهیه نسخه پشتیبان بهتر است که داده ایمن گردد. داده ایمن می تواند توسط عملیات رمزگذاری یا استفاده از امضای دیجیتالی حاصل شود.

❖ مدیریت امنیت سامانه مدیریت پایگاه‌داده ملی لازم است به صورت نامتمرکز (توزیع شده) باشد.

❖ بررسی دقیق درخواست های ورودی به سامانه مدیریت پایگاه‌داده برای جلوگیری از تهدیداتی نظیر SQL Injection لازم است.

❖ سامانه مدیریت پایگاه‌داده ملی بهتر است تحت سیستم عامل‌های مختلف (اعم از ۳۲ بیتی و ۶۴ بیتی) قابل به کارگیری باشد.

❖ بهتر است سامانه مدیریت پایگاه‌داده دارای امکانات کافی جهت پردازش و جستجو در انواع داده از جمله متن باشد.

❖ زبان پیاده‌سازی سامانه مدیریت پایگاه‌داده ملی بهتر است یک زبان توسعه یافته ملی باشد.

❖ بهتر است سامانه مدیریت پایگاه‌داده ملی مبتنی بر سیستم عامل توسعه یافته ملی باشد.

❖ از آنجا که واسط پایگاه‌داده، به عنوان یک backdoor، ضریب امنیتی را پایین می آورد، پیشنهاد می شود از واسط پایگاه‌داده ملی استفاده شود.

❖ در انتخاب یک سامانه برای ایجاد یک بستر انتخاب صحیح نوع لیسانس بسیار حیاتی است.

❖ مکانیزم تصدیق هویت کاربر بهتر است استفاده از نام کاربری/ رمز عبور باشد.