

پایگاه داده

چکیده:

پایگاه داده مجموعه‌ای از داده‌های بهم مرتبط است که توسط برنامه‌ای که DBMS نامیده می‌شود، سازماندهی می‌شود. پایگاه داده‌ها اطلاعات مهمی را برای کاربران مهیا می‌کنند. بنابراین امنیت و حفاظت از آنها از اهمیت بسیار زیادی برخوردار است. امنیت پایگاه داده‌ها به حفاظت اطلاعات و کنترل دسترسی کاربران توجه دارد. این مقاله به اصول امنیت و سیاستهای مهم در این مورد و احتیاجات امنیتی سیستمها می‌پردازد. همچنین راههایی را برای کنترل دسترسی که از مهمترین احتیاجات هر سیستم پایگاه داده‌ای است، ارائه می‌کند.

در این مقاله با معرفی چند زمینه پیشرفته مطالعاتی امروزی بعضی مشکلات حل نشده در این زمینه را نیز به خوانند معرفی می‌کند.

مقدمه :

در طی سه دهه اخیر تعداد پایگاه داده‌های کامپیوتری افزایش بسیاری داشته است. حضور اینترنت به همراه تواناییهای شبکه، دسترسی به داده و اطلاعات را آسانتر کرده است. به عنوان مثال، کاربران امروزه می‌توانند به حجم بالایی از اطلاعات در فاصله زمانی بسیار کوتاهی دسترسی پیدا کنند. به همین نسبتی که ابزارها و تکنولوژی دسترسی و استفاده از اطلاعات توسعه می‌یابند، نیاز به حفاظت اطلاعات هم بوجود می‌آید. بسیاری دولتها و سازمانها صنعتی داده‌های مهم و طبقه بندی شده‌ای دارند که باید حفاظت شوند. سازمانهای بسیار دیگری هم مثل مؤسسات دانشگاهی نیز اطلاعات مهمی در مورد دانشجویان و کارمندانشان دارند. در نتیجه تکنیکهایی برای حفاظت داده‌های ذخیره شده در سیستمهای مدیریت پایگاه داده،^۱ اولویت بالایی پیدا کرده‌اند.

در طول سه دهه اخیر، پیشرفتهای بسیاری در مورد امنیت پایگاه داده‌ها حاصل شده است. بسیاری از کارهای اولیه روی امنیت پایگاه داده‌های آماری انجام شد. در دهه ۷۰، همزمان با شروع تحقیقات روی پایگاه داده‌های رابطه‌ای، توجه مستقیماً به مسئله کنترل دسترسی^۲ بود و بیشتر از همه، کار روی مدل‌های کنترل دسترسی احتیاطی^۳ شروع شد؛ ولی در واقع تا مطالعات نیروی هوایی در ۱۹۸۲، که تلاش وسیعی برای DBMS‌های امن چند سطحی^۴ بود، کار مهمی انجام نشد.

1- DNMS

2- Access Control

3- Discretionary

4- Mandatory

در هزارهٔ جدید با حضور تکنولوژیهای مثل کتابخانه‌های دیجیتال، شبکه گستره جهانی و سیستمهای محاسباتی اشتراکی، علاقه بسیاری به امنیت نه تنها در بین سازمانهای دولتی، بلکه بین سازمانهای اقتصادی هم وجود دارد. این مقاله مروری به پیشرفتها و محصولات در سیستمهای پایگاه داده‌ای امن در بر دو زمینهٔ اجباری و احتیاطی دارد.

۲- کنترل دسترسی (مفاهیم و سیاستها):

در این بخش مفاهیم پایه در کنترل دسترسی معرفی می‌شوند. سپس در مورد سیاستهای کنترل دسترسی احتیاطی و الزامی بحث می‌شود و نهایتاً مروری داریم بر سیاستهای سرپرستی.

۲-۱- مفاهیم اساسی:

کنترل دسترسی معمولاً در مقابل، مجموعه ای از قوانین اعطای مجوز که توسط مدیران امنیتی یا کاربران براساس بعضی سیاستهای خاص ارائه می‌شوند، قرار دارد. قانون اعطای مجوز، در حالت کلی بیان می‌کند که فرد S (Subject) اجازه دارد که امتیاز P (Privilege) را بروی شیئی O (Object) بکار ببرد.

اشیاء مجاز^۱: ترکیبات غیرفعال سیستم هستند که باید در مقابل دسترسی‌های غیرمجاز محافظت شوند. اشیایی که باید به آنها متوجه شدند به مدل داده‌ای مورد استفاده بستگی دارند. به عنوان مثال، در یک سیستم عامل فایلها و دایرکتوریها اشیاء هستند. در حالیکه، در یک DBMS منابعی که باید محافظت شوند رابطه‌ها، دیدها و صفات هستند.

¹ - Authorization Object

اشخاص مجاز^۱: موجودیتهایی در سیستم هستند که اجازه دسترسی به آنها داده می شود.

اشخاص به دسته های زیر تقسیم بندی می شدند:

- کاربران: که شخصیت های مجزا و مشخصی هستند که با سیستم در ارتباطند.
- گروهها مجموعه ای از کاربران.
- نقشها^۲: مجموعه ای نامدار از امتیازها که احتیاج دارند، فعالیت خاصی را در رابطه با سیستم انجام دهند.
- سلسله عملیات^۳: که برنامه هایی را برای کاربر اجرا می کند. به طور کلی، سلسله عملیات به آدرسهای حافظه، استفاده از CPU، فراخوانی برنامه های دیگر و عملیات بروی داده اشاره می کند.

- امتیازهای مجاز^۴: انواع عملیاتی را که یک فرد می تواند روی یک شیئی در سیستم اجرا کند، بیان می کند. مجموعه این امتیازها به منابعی که باید محافظت شوند، بستگی دارد. به عنوان مثال، در یک سیستم عامل خواندن، نوشتن و اجراء از امتیازها هستند. ولی، در یک DBMS رابطه ای، انتخاب، درج، تغییر و حذف از جمله امتیازها به شمار می روند.

1- Authotization Subject

2- Role

3- process

4- Authorization privilege

۲-۲- سیاستهای کنترل دسترسی :

سیاستهای کنترل دسترسی، معیارهایی هستند که براساس آنها تعیین می شود آیا یک درخواست دسترسی باید مجاز شمرده شود یا نه. یک طبقه بندی کلی بین سیاستهای کنترل دسترسی احتیاطی و الزامی است.

۲-۲-۱- سیاستهای کنترل دسترسی احتیاطی :

سیاستهای کنترل دسترسی احتیاطی (DAC)، دسترسی افراد به اشیاء را براساس شناسه افراد و قوانین و مجوزها کنترل می کند. و قوانین برای هر فرد مجوزهایی را که می تواند برای انجام عملیات روی اشیاء بکار برد، بیان می کند. وقتی تقاضای دسترسی به سیستم می آید، مکانیسم دسترسی مشخصی می کند آیا قانونی برای تأیید این درخواست وجود دارد یا نه. اگر قانونی وجود داشت درخواست مجاز شمرده می شود در غیراین صورت رد می شود. چنین مکانیسمی احتیاطی است و در آن به اشخاص اجازه داده می شود که مجوز دسترسی به داده هایشان را به دیگران بدهند.

سیاستهای دسترسی احتیاطی انعطاف پذیری زیادی دارند. به طوری که، اجازه تعریف محدوده وسیعی از قوانین کنترل دسترسی را با استفاده از انواع مختلف مجوزها را می دهند. مثل مجوزهای مثبت و منفی و مجوزهای قوی و ضعیف. در زیر توضیح مختصری از هر کدام ارائه می شود.

• مجوزهای مثبت و منفی :

در سیستمی که مجوز مثبت دارد. هر گاه فردی بخواهد به شیئی خاصی دسترسی داشته باشد، سیستم چک می کند آیا مجوزی وجود دارد و فقط در صورت وجود، به شخص

اجازه دسترسی داده می شود. عدم وجود مجوز به معنی رو درخواست است. مشکل این خط مشی این است که، عدم وجود مجوزهای منفی حل شد که به معنی رد قطعی مجوز در چنین مواردی است.

• مجوزهای قوی و ضعیف:

بعضی مدل‌هایی که هر دو مجوز مثبت و منفی را دارند به دو دسته مجوزهای قوی و ضعیف نیز تقسیم می شوند. مجوزهای قوی (چه مثبت و چه منفی) باطل نمی شوند. در حالیکه، مجوزهای ضعیف براساس قوانین خاصی توسط مجوزهای قوی یا ضعیف دیگری می توانند باطل شوند.

۲-۲-۲- سیاستهای کنترل و دسترسی الزامی:

سیاستهای کنترل دسترسی الزامی (MAC) بیان کننده دسترسی است که افراد به اشیاء براساس رده بندی شیئی و فرد، دارند. این نوع از امنیت تحت عنوان امنیت^۱ چند لایه هم نام برده می شود. سیستمهای پایگاه داده‌ای که خصوصیات امنیت چند لایه را تأمین می کنند. DBMS های این چند لایه (MLS/DBMS) یا DBMS های مطمئن نامیده می شوند. بیشتر MLS/DBMSها براساس سیاست Bell و Lapadula، طراحی و ساخته شده‌اند. در این خط‌مشی‌ها، افراد به عنوان سطوح مجاز مطرح می شوند و می توانند در سطح مجاز خود عمل کنند. اشیاء به سطوح مجاز مطرح می شوند و می توانند در سطوح مجاز خود عمل کنند. اشیاء به سطوح حساسیت ارجاع می شوند. سطوح مجاز حساسیت را سطوح امنیت می نامند. آنچه در زیر می آید، دو قانون مهم این خط مشی است:

¹ - Multilevel Security

- ویژگی امنیتی ساده: یک فرد دسترسی خواندن یک شیئی را دارد اگر سطح امنیتی آن بر سطح امنیتی شیئی مسلط باشد.

- ویژگی ستاره: یک فرد دسترسی نوشتن یک شیئی را دارد اگر سطح امنیتی شیئی توسط سطح امنیتی فرد پوشانده شود.

شکل زیر تفاوت بین سیاستهای الزامی و احتیاطی را نشان می دهد. تحت سیاست احتیاطی یک تقاضای دسترسی مجاز شمرده می شود اگر قانونی وجود داشته باشد که دسترسی را مجاز بداند. در مقابل، دو سیاست الزامی یک دسترسی مجاز است، اگر رابطه خاصی بین سطح امنیتی شخصی که تقاضای دسترسی دارد و سطح امنیتی شیئی که مورد تقاضاست، وجود داشته باشد.

۲-۳- سیاستهای سرپرستی^۱:

یکی دیگر از ابعادی که می تواند معیاری برای مقایسه مدل های کنترل دسترسی باشد، سیاستهای سرپرستی است، که حمایت می کند. سرپرستی است. که حمایت می کند. سرپرستی به عملیات اعطا و بازپس گرفتن مجوز اطلاق می شود. ما سیاستهای سرپرستی را به صورت زیر طبقه بندی می کنیم. (۵)

سرپرستی DBA: تحت این سیاست، فقط DBA می تواند حق دسترسی بدهد یا تقاضای را برگرداند. این سیاست بسیار متمرکز است و امروزه به ندرت در DBMSها بکار می رود، مگر در ساده ترین آنها.

¹ - Aclminidtration

سرپرستی شیئی - مالک^۱: براساس این سیاست که عمدتاً توسط DBMS ها و سیستم عاملها استفاده می شود، بوجود آوردند شیئی مالک آن محسوب می شود و تنها شخص مجاز برای سرپرستی شیئی است. سرپرستی متصدی شیئی^۲ ک بر طبق این سیاست، یک شخص، نه الزاماً ایجاد کننده شیئی، مدیر سرپرستی شیئی است. براساس این سیاست حتی ایجاد کننده شیئی هم باید مجوز دسترسی به شیئی را دریافت کند.

دومین و سومین سیاست می توانند با وکالت سرپرستی و انتقال سرپرستی ترکیب شوند. وکالت سرپرستی به این معناست که مدیر یا سرپرست یک شیئی می تواند اعمال سرپرستی بروی یک شیئی را به شخص دیگری واگذار کند. بیشتر DBMS ها سیاست سرپرستی براساس سرپرستی مالک با امکان واگذاری را حمایت می کنند. باید توجه داشت که تحت خط مشی واگذاری سرپرست اولیه شیئی امتیاز سرپرستی خود را از دست نمی دهد.

انتقال سرپرستی مثل واگذاری، سرپرستی را به شخص دیگری می دهد. با این تفاوت که، سرپرست اولیه امتیاز سرپرستی خود را از دست می دهد. برای انتقال سرپرستی دو خط مشی زیر وجود دارد.

- ارجاع بازگشتی^۳: تمام مجوزهایی که در توسط سرپرستی پیشین داده شده، به صورت بازگشتی ارجاع داده می شود.

¹ - obuect-Owner

² - Object Cuarator

³ - Recursive Revoke

- انتقال واگذار کننده^۱: تمام مجوزهای که توسط سرپرستی پیشین صادر شده نگه داشته می‌شوند علاوه بر این انتقال می‌تواند با پذیرش^۲ یا بدون پذیرش به معنای این است که چنین پذیرشی احتیاج نیست. شکل زیر طبقه بندی سیاستهای سرپرستی که در این بخش در مورد آن بحث شد را نشان می‌دهد.

۳- سیستمها و مدلهای کنترل دسترسی احتیاطی:

در این بخش به بحث در مورد مدلها و سیستمهای DAC می‌پردازیم. مدلهای احتیاطی براساس معیارهای گوناگونی می‌تواند طبقه بندی شود. این بخش این مدلها را براساس DBMSهایی که تحت آن این مدلها توسعه می‌یابند به سه گروه تقسیم بندی می‌کند: مدلهای اعطای مجوز برای DBMSهای رابطه‌ای، مدلهای اعطای مجوز برای DBMSهای شیئی گرا و مدلهای اعطای مجوز برای DBMSهای فعال.

۳-۱- مدلهای اعطای مجوز برای DBMSهای رابطه‌ای:

در این بخش مروری داریم بر مدلهای اعطای مجوز که برای DBMSهای رابطه‌ای ساخته شده‌اند و با شرح مدل System R شروع می‌کنیم. مدل System R یک حادثه مهم در تاریخ مدلهای اعطای مجوز است. اهمیت مدل سیستمهای R از آنجایی است که بسیاری DBMSهای تجاری مکانیزم اعطای مجوز را براساس آن توسعه دادند.

در این مدل اشیایی که باید محافظت شوند جدولها و دیدهایی هستند که اشخاص، امتیازهای گوناگون نسبت به آنها دارند. امتیازهایی که این مدل حمایت می‌کند شامل،

¹ - Grantor Transfer

² - acceptance

انتخاب (Select) برای انتخاب تاپلها از جدول، به روز رسانی (Update) برای تغییر تاپلهای یک جدول، درج و حذف (Delete,insert) برای افزودن یا حذف کردن تاپلهای جدول، حذف جدول (drip) برای پاک کردن کل یک جدول. گروه و نقش در این مدل حمایت نمی شوند. این مدل امکانات سرپرستی تا متمرکز را حمایت می کند. هرگاه شخصی جدولی را بوجود می آورد. امتیازی را نسبت به آن بدست می آورد. مالک جدول می تواند تمام امتیازها را بر جدول اعمال کند.

این مدل ارجاع بازگشتی دارد، به این معنا که وقتی شخصی مجوز جدولی را از کاربر دیگری می گیرد. تمام مجوزهایی که قبلاً به او داده شده ارجاع می شود.

۲-۳- مدلهای اعطای مجوز برای DBMS های شیئی گرا:

امروزه DBMS های شیئی گرا و شیئی - رابطه ای از مهمترین زمینه های تحقیق در موزه DB هستند. دلیل این اهمیت این است که آنها بسیار مناسب برای کاربردهای پیشرفته مثل CAD/CAM، مولتی مدیا و کاربردهای نقشه کشی هستند. چون این برنامه ها احتیاج به مدلهای داده ای غنی تری نسبت به مدلهای رابطه ای دارند. احتیاجات سیستمهای DBMS ها هم متفاوت از سیستمهای رابطه ای است و این باعث می شود مدلهای سنتی برای DBMS های رابطه ای، برای سیستمهای شیئی گرا کافی نباشد. با وجود رشد علاقه و توجه به ODBMS ها، تحقیقات برای مدلهای اعطای مجوز برای ODBMS ها هنوز در مراحل اولیه است. اگرچه طرحهای بسیاری وجود دارد. تنها مدلهای Orion و Iris مدلهای قابل مقایسه با مدلهای RDBMS ها دارند.

۱-۲-۳- مدل Orion:

مدل اعطای مجوز Orion، مجوزهای مثبت و منفی و همچنین قوی و ضعیف را حمایت می‌کند. مجوز قوی همیشه اولویت بیشتری نسبت به مجوز ضعیف دارد. مجوزها به جای کاربران تکی به نقشها داده می‌شوند و یک کاربر مجاز است عملی را روی یک شیئی انجام دهد، اگر نقشی وجود داشته باشد که اجازه این کار را داشه‌ته باشد. نقشها، اشیاء و امتیازها تحت یک سلسله مراتب سازماندهی می‌شوند و یکسری قوانین انتشار یا تکثیر اعمال می‌شود :

- اگر یک نقش مجوز دسترسی به یک شیئی را داشته باشد تمام نقشهای بالاتر از آن در سلسله مراتب همان مجوز را دارند.

- اگر یک نقش مجوز منفی برای دسترسی به یک شیئی را داشته باشد تمام نقشهای بعداز آن همان مجوز منفی را خواهند داشت.

قوانین انتشار یکسانی برای امتیازها هم تعریف می‌شدند. نهایتاً قوانین انتشار بر یک شیئی اجازه مجوزهایی را می‌دهد که از مجوزهای شیئی که، منقطعاً با آن در ارتباط است، مشتق شده باشد. به عنوان مثال مجوز خواندن یک کلاس، مجوز خواندن تمام نمونه‌های آن را صادر می‌کند.

۳-۲-۲- مدل Iris:

در مدل Iris، صفات و متدها هر دو به عنوان تابع تعریف می‌شدند و تنها امتیازی که توسط مدل حمایت می‌شود، فراخوانی تابع است. یک فرد که امتیاز فراخوانی یک تابع را دارد مجاز برای فراخواندن آن تابع است. فردی که ایجاد کننده یک تابع است، مالک

آن محسوب می شود و به طور خودکار امتیاز فراخوانی آن را دریافت می کند. علاوه بر این مالک یک تابع می تواند امتیاز فراخوانی تابع را به افراد دیگر هم بدهد. این اعطای امتیاز می تواند شامل شرایط هم باشد، که به شخصی که امتیاز را می گیرد اجازه می دهد که آن را به دیگران هم بدهد.

این مدل اجازه می دهد که یک امتیاز هم به گروه و هم به کاربر داده شود یا گرفته شود. یک کاربر می تواند متعلق به چندین گروه باشد. توابع مشتق شده تحت عنوان توابع دیگر تعریف می شوند. علاوه بر این، گروه ها می توانند تو در تو باشند. مدل Iris دو خط مشی برای حفاظت از توابع مشتق شده دارد.

تحت خط مشی که مجوز استاتیک نامیده می شود، فردی که تقاضای اجرای یک تابع مشتق را دارد. فقط باید اجازه فراخوانی تابع مشتق را داشته باشد. در خط مشی دیگر، مجوز دینامیک، فراخواننده هم باید مجوز فراخوانی تابع مشتق را داشته باشد و هم مجوز برای فراخوانی تمام توابعی که تابع مشتق آنها را اجراء می کند. هنگام ایجاد یک تابع مشتق باید مشخص کنیم که از کدامیک از این دو خط مشی برای بررسی تقاضاهای اجراء استفاده کنیم.

این مدل همچنین دو مفهوم برای کنترل دسترسی تعریف می کند: توابع نگهبان^۱ و توابع پراکسی^۲.

1- guard

2- proxy

توابع نگهبان، ابزاری برای گذاشتن پیش شرط در فراخوانی یک تابع و در نتیجه محدود کردن دسترسی به توابع هستند. تابعی که تابع نگهبان به آن اشاره می کند تابع هدف نامیده می شود. یک تابع هدف اجراء می شود. اگر تابع نگهبان مربوط به آن موفق ارزیابی شود. مهمترین مزیت تابع نگهبان این است که دسترسی به یک تابع محدود می شود، بدون اینکه لازم باشد کد تابع تغییر کند. توابع پراکسی، پیاده سازی های مختلفی از یک تابع مشخص را برای افراد مختلف، فرد یا گروه، تأمین م کند. وقتی یک تابع مورد درخواست واقع می شود، تابع پراکسی مناسب به جای تابع اصلی اجراء می شود.

۳-۳- مدلهای اعطای مجوز برای DBMS های فعال :

پایگاه داده های فعال با یک سیستم قانونمند که DBMS را قادر می سازد با تریگر کردن قانونها نسبت به حوادث عکس العمل نشان دهد، تعریف می شوند. قوانین اعمالی را توصیف می کند که می خواهیم به صورت خودکار در هنگام رخ دادن حادثه خاصی یا ارضاء شدت شرط خاصی در DB اجراء شوند. به عنوان یک مثال از این مدل در ادامه امکانات سیستم Starbust را شرح می دهیم.

Starbust یک نمونه از سیستم پایگاه داده ای رابطه ای توسعه پذیر است که در مرکز تحقیقاتی Almaden در IBM تولید شده است. Starbust بوسیله یک زبان قانونمند توصیف می شود. مدل اعطای مجوز آن سلسله مراتبی و از نوع امتیازها را که در DB می تواند اعمال شود، حمایت می کند. در این سلسله مراتب عناصر بالاتر، انواع پائین تر را پوشش می دهند. مثالهایی از انواع امتیازها، کنترل است که تمام امتیازهای دیگر یعنی Attach و Alter ، Write را پوشش قوانین توسط محدودیتهای زیر اداره می شوند.

- ایجاد کننده یک قانون بر جدول T، باید هر دو امتیاز Attach و Read را از جدول T داشته باشد.
- عوامل عمل و شرایط قانون ایجاد شده در برابر امتیازات ایجاد کننده چک می شود. اگر قسمتی از شرایط یا نحوه عملکرد قانون شامل عباراتی شود که ایجاد کننده اجازه اجرای آنها را نداشته، عملیات ایجاد شده مجاز شمرده نمی شود.
- فردی که متقاضی حذف یک قانون T بر روی جدول T است باید امتیاز کنترل و یا امتیاز Attach و کنترل را روی جدول T داشته باشد.
- فرد متقاضی تغییر قانون باید امتیاز Alter را روی قانون داشته باشد.

۳-۴- کنترل دسترسی احتیاطی در DBMS های تجاری:

در این بخش، توضیح می دهیم که چگونه DAC در سیستم شیئی رابطه ای اوراکل اعمال می شود. در اوراکل، امتیازها به هر دو گروه کاربران و نقشها داده می شود. نقشها در یک سلسه مراتب سازمان دهی شده اند و یک نقش تمام امتیازات نقشهای زیر خود در سلسله مراتب را بدست می آورد. یک کاربر ممکن است مجاز برای ایفای چند نقش در یک فاصله زمانی باشد. با هر نقشی ممکن است یک کلمه عبور همراه شود. تا از استفاده غیرمجاز امتیازها جلوگیری کند.

مجموعه ای از پیش تعریف شده از امتیازها فراهم است که می تواند به هر کدام از نقشها در اوراکل تغییر داده شود. وقتی یک فرد نقشی را ایجاد می کند، نقش به طور خودکار با اختیارات سرپرستی¹ به ایجاد کننده داده می شود، که به او اجازه می دهد نقش را به

¹ - admin options

نقشی دیگر بدهد یا از او بگیرد و این کار را می توان با اختیارات سرپرستی یا بدون آن باشد. ارواکل همچنین گروه خاص، عمومی^۱ را حمایت می کند که برای هر فردی قابل دسترسی است. امتیازها در پایگاه داده ارواکل به دو بخش تقسیم می شوند: امتیازات سیستم و امتیازات شیئی. امتیازات سیستم به فرد اجازه می دهد، اعمال سیستمی و یا عملی را روی داده خاصی انجام دهد. بیش از ۶۰ محدود از امتیازات سیستمی مهیاست. مثالی از این امتیازها، امتیاز حذف تاپل از هر جدولی در DB است. به علت اینکه امتیازات سیستمی قدرتمند هستند، اغلب فقط به DBA یا تولید کنندگان برنامه های کاربردی داده می شدند. مثل نقشها این امتیازات می توانند با اختیارات سرپرستی داده شوند و اگر شخصی امتیاز سیستمی با اختیارات سرپرستی را داشته باشد می تواند این امتیاز را به افراد دیگر بدهد یا از آنها بگیرد.

امتیازات شیئی به فرد اجازه می دهد. یک عمل خاص را روی شیئی مشخص در DB انجام دهد. امتیازات حذف یا درج تاپل در یک جدول مشخص، مثالی از این امتیازهاست. وقتی فردی شیئی را در شمای خودش ایجاد می کند، به طور اتوماتیک تمام امتیازات شیئی را در مورد آن شیئی مثل حق دادن این امتیاز به دیگران را دریافت می کند. اگر این اعطا امتیاز آن باشد، مزد دریافت کننده می تواند این امتیاز را به دیگران دم بدهد. امتیاز شیئی فقط توسط شخصی که آن را اعطاء کرده بازگردانده می شود. بازگشت و ارجاع این امتیاز بازگشتی است.

۴- امنیت چندلایه در سیستمهای پایگناه داده ای:

¹- public

در این بخش به شرح جنبه‌های امنیت چندلایه در امنیت دائمی برای سیستم‌های پایگاه داده‌ای می‌پردازیم. بخش اول به طور کلی بروی سیستم‌های رابطه‌ای متمرکز است.

مسئله‌ای که باید مورد توجه قرار بگیرد این است که محصولات قابل توجه دیگری هم برای امنیت چندلایه برای سیستم‌های توزیع شده^۱، نامتجانس^۲ و یکپارچه^۳ است. ما در این بخش به بحث در مورد بعضی از این پیشرفته‌ها می‌پردازیم.

۴-۱- مدل داده‌ای رابطه‌ای چند لایه :

در یک پایگاه داده چند لایه، تمام داده‌ها به سطح امنیتی یکسانی منسوب نمی‌شوند. اگر چنین پایگاه داده‌ای بر اساس مدل رابطه‌ای باشد، اشیاء طبقه بندی شده ممکن است شامل کل DB، رابطه‌ها، تاپلها، صفات و عناصر داده‌ها می‌باشد. دسترسی به چنین اشیایی توسط سیاست الزامی که در بخش ۲ صحبت آن شد، اداره می‌شود. یک DBMS چند لایه باید DB چندلایه را از دسترسی غیرمجاز یا تغییر توسط افراد در سطح امنیتی دیگر محافظت کند. یک پایگاه داده رابطه‌ای چند لایه، DB چندلایه را به عنوان مجموعه‌ای از رابطه‌ها تعریف می‌کند و چنین مدلی، مدل داده‌ای چندلایه رابطه‌ای نامیده می‌شود.

هدف طراحان پایگاه داده‌های رابطه‌ای چند لایه تعریف نسخه‌های گوناگون از موجودیت، عمل یا حادثه یکسان در سطوح امنیتی مختلف بدوت تعارض با قوانین امنیتی و جامعیتی است. یکی از مکانیزم‌های ارائه شده، چند نمونه ای بودن^۴ است. این مکانیزم

1- Distributed
2- heterogeneous
3- Federated
4- polinstiation

اجازه می دهد دو تاپل با کلید اولیه یکسان در یک DB در سطح مختلف امنیتی وجود داشته باشند. اگرچه، وجود دو تاپل با کلید اولیه یکسان متناقض خصوصیت جامعیت موجودیتی در مدل داده ای رابطه ای استاندارد است. مثال زیر را در نظر بگیرید:

EMP یک رابطه با صفات زیر است:

DEPT \neq , NAME, SALARY, SS \neq

در این رابطه، SS \neq کلید اولیه است فرض کنیم شخصی تاپل زیر را ابتدا در EMP درج می کند:

(000, Jphn, 60k, 120)

و سپس فرد دیگری نه از همان طبقه، تاپل زیر را وارد کند.

(000, John, 20k, 120)

اگر این تاپل پذیرفته شود تاپل چند نمونه ای¹ است.

اخیراً بحثهای بسیاری در مورد چند نمونه ای بودن وجود دارد. عده ای معتقدند چند نمونه ای بودن لازم است اگر ما قصد طراحی پایگاه داده های چند لایه با ضریب اطمینان بالا را داریم و عده ای بر این عقیده اند که جامعیت DB اهمیت بیشتری دارد و چند نمونه ای بودن با آن در تناقض است. سیستمهایی که در اینجا بحث می کنیم انواع مختلفی از مدل داده ای چند لایه را ارائه داده اند و همه خصوصیات امنیتی را که در این بخش در مورد آنها صحبت شد را ارضاء می کنند و چند نمونه ای بودن هم در بسیاری مدلها وجود دارد.

¹ - polyinstantiated

۲-۴- معماری :

در این بخش مدل‌های مختلف کنترل دسترسی که برای DBMS/MLS ها تولید شده‌اند، بررسی می‌کنیم. در حالیکه DBMS ها باید با انواع مختلف موارد امنیتی به عنوان سیستم عامل‌های قابل اطمینان در تعامل باشند، خصوصیات DBMS ها است که سطح امنیتی آنها را در مقابل آنچه سیستم عامل‌های سنتی انجام می‌دهند. معرفی می‌کند. به عنوان مثال اشیاء در DBMS ها تمایل دارند در سائزهای چندگانه باشند و بتوانند دانه دانه باشند. این با سیستم‌هایی که در آنها دانه دانه بودن وجود ندارد در تناقض است (به عنوان مثال فایلها یا سگمنت‌ها).

همچنین تفاوت‌های عملیاتی آشکاری بین سیستم عاملها و DBMS ها وجود دارد که چگونگی برخورد با مسئله امنیت را تحت تأثیر قرار می‌دهد. سیستم عاملها تمایل به تعامل با افرادی دارند که تلاش برای دسترسی به بعضی اشیاء دارند DBMS ها اشیاء را بین کاربران تقسیم می‌کنند و برای کاربران ابزار ارتباط با اشیاء داده‌ای گوناگون را فراهم می‌کنند. همچنین به طور کلی DBMS ها وابسته به سیستم عامل برای تأمین منابع هستند. بنابراین طراحی DBMS ها باید در راستای چگونگی برخورد سیستم عامل با مسئله امنیت باشد.

تفاوت بین نحوه عملکرد و احتیاجات امنیتی DBMS ها و سیستم عاملها به این معناست که راه‌های سنتی که برای تأمین امنیت سیستم‌هایی که با این سیستم عاملها بخوبی کار می‌کردند، نیاز دارند برای DBMS ها تغییر داده شدند. در حال حاضر هیچ معماری به تنهایی مورد قبول یا مورد استفاده در تولید DBMS/MLS ها نیست. گسترده وسیعی از

خط مشی‌ها برای طراحی و ساخت DBMS/MLS ارائه شده است. بعضی نظریه‌ها در این مورد عبارتند از:

• معماری *Single-kernel*

در این مدل کنترل دسترسی تماماً به عهده سیستم عامل است و DBMS نقشی در آن ندارد.

• معماری *Distributed*

بر طبق این خطی مشی چندین ماشین انتهایی^۱ DBMS و یک ماشین ابتدایی^۲ مطمئن وجود دارد که انتهایی‌ها از طریق آن با هم در ارتباطند.

• معماری *Trusted-Subject*

در این خط مشی که گاهی دو هسته‌ای^۳ هم نامیده می‌شود، براساس سیستم عامل عمل نمی‌کند و DBMS کنترل دسترسی را به عهده دارد.

• معماری *Integrity-lock*

در این معماری یک انتهایی DBMS مطمئن با دسترسی به تمام داده‌ها DB و یک ابتدایی نامطمئن که با کاربرها ارتباط برقرار می‌کند و یک انتهایی نامطمئن که استفاده از تکنولوژی پنهان سازی را فراهم می‌کند. در این خط مشی مهم است که عناصر نامطمئن از هم جدا باشند. بنابراین می‌توان مطمئن بود که هیچ دو عنصر نامطمئن خارج از نظارت فیلتر مطمئن با هم ارتباط ندارند.

¹ - back-end

² - Front-end

³ - Dual-kernel

• معماری Extended-Kernel

گسترشی بر مدل اول است. در این معماری سیستم عامل همچنان دو راه حل MAC و DAC را به کار می‌برد. در این مدل TDBMS بعضی راه‌حلهای مکمل برای فراهم کردن کنترل دسترسی را اضافه می‌کند.

۳-۴- محصولات تجاری:

از سال ۱۹۸۸ محصولات DBMS/MLS ها تولید شده اند. گرچه تعدادی از آنها هرگز به بازار نیامدند. در این بخش مروری داریم بر بعضی محصولات تجاری بین سالهای ۱۹۸۸ تا ۱۹۹۳.

• TRUDATA

نسخه اولیه TRUDATA در سالهای آخر دهه ۸۰ براساس معماری Integrity-lock به بازار آمد. TRUDATA از ماشین Britton lee به عنوان انتهایی نامطمئن و سیستم AT7T 3B2V/MLS به عنوان ابتدایی استفاده می‌کند.

• Secure Sybase

Secure SQL Server که متعلق به شرکت Sybase است، سیستم مبتنی بر معماری Trusted-Subject با معماری CIS^۱ است. در موارد اولیه قسمت مشتری معماری بروی Ultrix، SE/VMS یا SUN MLS اجرائی می‌شد و قسمت خدمتگذار بروی Ultrix و

¹ - Client/Server

چون Ultrix سیستم مطمئنی نبود، بنابراین محیط سیستم عاملی امنی به حساب نمی آمد و در نتیجه کنترل دسترسی به DBMS داده شد.

• *Trusted Oracle*

تلاش DBMS اوراکل در بین کارهایی که انجام شده یکتاست و به گونه ای است که هر دو معماری Trusted-Subject, Single-kernel را ارضاء می کند. Single-lernel در نسخه های اولیه اوراکل توسط سیستم عاملها SE/VMS و HP/VX که این DB روی آنها اجراء می شد، تأمین می گردید. اوراکل مطمئن چند نمونه ای بودن برای عمل درج را حمایت می کند.

۵- زمینه های تحقیق :

بسیاری محیط های کاربردی پیشرفته مثل کتابخانه های دیجیتال توزیع شده، سیستم های اطلاعاتی ناهمگون^۱، سیستم های همکار^۲، برنامه های کاربردی Work flow ۳ وعده احتیاجات کنترل دسترسی بسیار زیادی دارند، به طوری که مکانیزم های کنترل دسترسی امروزه نمی توانند پاسخگوی این نیازها باشد. در بسیاری موارد یا سازمان مجبور به بکارگیری سیاست خاصی برای کنترل دسترسی به صورت دستی است یا باید این سیاستها توسط برنامه کاربردی پیاده سازی شوند، که هر دو موقعیت آشکارا غیر قابل

¹- heterogeneous

²- Cooperative

قبول است. در این بخش احتیاجات کنترل دسترسی در سه زمینه مهم امروزی مطرح می شود:

• کتابخانه های دیجیتال:

- مکانیزم تشخیص انعطاف پذیر افراد.

- کنترل دسترسی Content-base به مولتی مدیا و داده های

ساختار نیافته.

- دسترسی های از راه دور و دسترسی به کتابخانه های توزیع

شده.

- کپی کردن و استفاده کردن از اطلاعات.

• سیستم های مدیریتی *Work flow*

- کنترل دسترسی Role-base

- محدودیتهای اعطای مجوز بروی نقشها و کاربران.

• شبکه جهانی *WWW*

- استراتژی مفید برای ذخیره سازی مجوزها.

- عملیات سرپرستی.

- مدل های اعطای مجوز برای XML

۶- جمع بندی

در این مقاله مروری داشتیم بر سیستمهای پایگاه داده ایمن. مفاهیم اساسی در کنترل دسترسی همچنین سیاستهای MAL و DAC معرفی شدند. مروری داشتیم بر سیاستهای سرپرستی ارائه شده و امنیت الزامی مدلهای داده‌ای، معماریها، محصولات تجاری و صحبت کوتاهی شد در مورد محصولات و تمایلات امروزی.

محصولاتی در این مقاله معرفی شدند. در مورد ساختار آنها صحبت مختصری شد، این محصولات هر ساله بهبود می‌یابند. بنابراین برای اطلاعات به روزتر خواننده باید به کاتالوگ فروشندگان با تولید کنندگان این محصولات مراجعه کند.

جهت سیستمهای پایگاه داده ای به سوی محصولات تحت وب پیش می‌رود و سیستمهای پایگاه داده دیگر سیستمهای مستقل نخواهد بود. آنها در حال یکی شدن با کاربردهای مختلفی مثل مولتی مدیا، تجارت الکترونیکی، سیستمهای کامپیوتری سیار و کتابخانه های دیجیتال هستند. موارد امنیتی برای چنین سیستمهای بسیار مهم است. علاوه بر این امنیت در سیستمهای work folw موضوع تحقیق بسیاری از افراد است. و رقابت شدیدی برای فرموله کردن سیاستها در چنین سیستمهای وجود دارد. تکنولوژیهای جدید مثل داده کاوی^۱ به حل مشکل امنیتی کمک خواهند کرد و به طور کلی DB همچنان در تکاپو خواهد بود و پیشرفت خواهد کرد و مسئله امنیت آن نمی تواند فراموش شود.

۲- مراجع

1- Data Mining

[1] Mario Piattini , and oscar Diaz, Advance Data base Technology A and Design, Briston: Artech House, 2000.

[2] Bertino, E., and E., Ferrari, “Adiminstration Policies in a Ualtipolicy Authorization System,” Proc . 10th IFIP Working conf. On Data base Security, Lake Tahoe, CA, Aug. 1997.

[3] Bell, D., and L.Lapadula, “Secure Computer systems,” ESD-TR-75-306, Hanscom Air Force Base, Bedford, MA, 1975.