APJ. 5(1):24-33, Spring 2024

Arman Process Journal (APJ)

Homepage: armanprocessjournal.ir

A Methodological Perspective on Effective Access Control for Distributed Databases

M. Asadi*[*,1] , Z. Khodadadi[2]

[1] *Computer Engineering Department, Islamic Azad University, Khodabandeh Branch, Tehran, Iran*

[2] *Computer Engineering Department, Islamic Azad University, Khodabandeh Branch, Tehran, Iran*

ABSTRACT

Received: 23 January 2023
Accepted: 11 May 2024

KEYWORDS:
Distributed Database,
Database Management System,
Access Control,
Methodological Approach,

[1] Corresponding author
ma.asadi2020@gmail.com

Distributed databases have evolved dramatically since their inception in the early 1970s. These databases are developed in different geographical locations and are organized by a decentralized database management system, which increases the flexibility and speed of data access. These databases generally provide vital information to their users. Therefore, their security and protection is very important. The security of these databases mainly focuses on information protection and especially user access control. Therefore, this article deals with the principles of security and important policies in the field of access control. Previous access control approaches are mainly limited and centralized and are usually not efficient for distributed applications in new technology platforms. Therefore, according to the necessity of the research, in this article, we investigate a methodological and comprehensive perspective that, by integrating existing access control methods, will provide the ability to make distributed and flexible use effective in distributed spaces.

NUMBER OF REFERENCES 23

NUMBER OF FIGURES 0

NUMBER OF TABLES 0

نشریه تخصصی آرمان پردازش، دوره ۵، شماره ۱، بهار ۱۴۰۳

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

دیدگاه متدولوژیک کنترل دسترسی موثر برای پایگاه داده های توزیعی

مریم اسدی*[1] و زهرا خدادادی[2]

دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد خدابنده، زنجان، ایران

دانشکده مهندسی کامپیوتر، دانشگاه آزاد اسلامی، واحد خدابنده، زنجان، ایران

چکیده

پایگاه‌های داده توزیعی از زمان پیدایش در اوایل دهه هفتاد میلادی به طور چشمگیری تکامل یافته‌اند. این پایگاهها در مکان‌های مختلف جغرافیایی توسعه می یابند و توسط سیستم مدیریت پایگاه داده نامتمرکز سازماندهی می گردند که این امر باعث افزایش سرعت دسترسی به داده‌ها می‌شود. این پایگاه داده‌ها عموما اطلاعات حیاتی را برای کاربراشان مهیا می‌کنند. لذا امنیت و حفاظت از آنها از اهمیت بسیار زیادی برخوردار است. امنیت این پایگاه داده‌ها عمدتا به حفاظت اطلاعات و بویژه کنترل دسترسی کاربران توجه دارد. لذا این مقاله به اصول امنیت و سیاستهای مهم در حوزه کنترل دسترسی می پردازد. رویکردهای کنترل دسترسی قبلی عمدتا بصورت محدود و متمرکز ارائه گردیده اند، و معمولا برای کاربردهای توزیع شده در بسترهای فناوری جدید کارا نمی باشند. لذا بنا به ضرورت تحقیق، در این مقاله به ارائه دیدگاه متدولوژیک و جامعی می پردازیم که با یکپارچه سازی روش های کنترل دسترسی موجود، توانمندی موثرسازی استفاده توزیع شده و انعطاف پذیر را در فضاهای توزیع شده فراهم نماید.

واژگان کلیدی:

پایگاه داده توزیعی،
سیستم مدیریت پایگاه داده،
کنترل دسترسی،
دیدگاه متدولوژیک،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۲۳

مقدمه

اخیرا حضور دائمی اینترنت به همراه توانائیهای شبکه، دسترسی به داده و اطلاعات را آسانتر کرده است و کاربران امروزه می‌توانند به حجم بالایی از اطلاعات در فاصلهٔ زمانی بسیار کوتاهی دسترسی پیدا کنند. پایگاههای داده در حوزه ساخت و توسعه برنامه های کاربردی و خدمات توزیعی نقش بسیار برجسته و مهمی دارند و همچنین درصورتی که توسط یک سیستم مدیریت پایگاه داده[1] نظارت شوند به میزان قابل توجهی از قابلیت توزیع بهره می‌برند. در دهه های اخیر تعداد پایگاه داده‌های توزیعی افزایش بسیاری داشته است. پایگاه داده‌های توزیع شده، بر خلاف دیتابیس‌هایی که در یک ماشین واحد تعبیه شده‌اند، قابل افزایش مقیاس هستند، کارایی زیادی دارند و شفافیت داده‌ها نیز در آن‌ها ملموس است [۱]. پایگاه داده‌های توزیع شده اساساً سیستم‌های توزیع شده‌ای به حساب می‌آیند که در آن‌ها دستگاه‌های محاسباتی یا عنصرهای پردازشی از طریق یک شبکه مثل اینترنت با هم ارتباط برقرار می‌کنند و با هم هماهنگ و همگام می‌شوند تا قابلیت‌های عملکردی بسیاری از اجزا را به عنوان عملکردی واحد و یکتا به کاربر ارائه دهند [۲]. به همان نسبتی که ابزارها و تکنولوژی دسترسی و استفاده از اطلاعات توسعه می‌یابند و کاربرد پایگاه داده های توزیعی در ارائه خدمات محسوس تر و ملموس تر می گردد، نیاز به حفاظت اطلاعات در این پایگاههای داده نیز ضرورت می یابد. 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 داده های ذخیره شده در سیستمهای مدیریت پایگاه داده توزیعی، اولویت بالایی پیدا کرده‌اند. با توجه به اینکه سیستم‌های توزیع شده پایگاه داده نرم‌افزارهایی عموما کاربردی تجاری هستند، لازم است در آن‌ها کنترل دسترسی ایمن و سختگیرانه ای فراهم شده باشد. بسیاری محیط‌های کاربردی پیشرفته مثل کتابخانه‌های دیجیتال توزیع شده، سیستمهای اطلاعاتی ناهمگون[2]، سیستمهای همکار[3]، برنامه‌های کاربردی Work flow و غیره احتیاجات کنترل دسترسی بسیار زیادی دارند، به طوری که مکانیزمهای کنترل دسترسی امروزه نمی‌توانند 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 قبول است. در این بخش احتیاجات کنترل دسترسی در سه زمینه مهم امروزی که در حوزه تمرکز پژوهش حاضر است به همراه کارکردهای مرتبط، مطرح می‌شود :

- کتابخانه های دیجیتال :
  - ـ مکانیزم تشخیص انعطاف پذیر افراد.
  - ـ کنترل دسترسی Content-base به مولتی مدیا و داده‌های ساختار نیافته.
  - ـ دسترسی‌های از راه دور و دسترسی به کتابخانه‌های توزیع شده.
  - ـ کپی کردن و استفاده کردن از اطلاعات.
- سیستمهای مدیریتی جریان کار:
  - ـ کنترل دسترسی Role-base
  - ـ محدودیتهای اعطای مجوز بروی نقشها و کاربران.
- شبکه جهانی وب:
  - ـ استراتژی مفید برای ذخیره سازی مجوزها.
  - ـ عملیات سرپرستی.
  - ـ مدلهای اعطای مجوز برای XML

در مقالات جدید، پیشرفتهای بسیاری در مورد امنیت پایگاه داده‌ها حاصل شده است. بسیاری از کارهای اولیه، روی امنیت پایگاه داده‌های آماری انجام شد. در دهۀ ۷۰، همزمان با شروع تحقیقات روی پایگاه داده‌های رابطه‌ای، توجه مستقیماً به مسئله کنترل دسترسی[4] بود و بیشتر از همه، کار روی مدلهای کنترل دسترسی احتیاطی[5] شروع شد. در حالی که، در سالهای پایانی دهۀ ۷۰، کار بروی امنیت الزامی[6] ولی در واقع تا مطالعات نیروی هوایی در ۱۹۸۲، که تلاش وسیعی برای DBMS های امن چند سطحی[7] بود، اقدامات اساسی و مهمی انجام نشد. در هزارۀ جدید با حضور تکنولوژیهایی 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 [۳]. این مقاله مروری به پیشرفتها و محصولات در سیستمهای پایگاه داده‌ای امن با تمرکز بر کنترل دسترسی در دو زمینۀ اجباری و احتیاطی دارد و دیدگاه متدولوژیکی درجهت کنترل دسترسی موثر برای پایگاه داده های توزیعی ارائه می نماید.

دیدگاه متدولوژیک کنترل دسترسی در پایگاههای داده توزیعی

پایگاه‌های داده توزیع‌شده در مکان‌های مختلف جغرافیایی پخش می‌شوند که این امر باعث افزایش سرعت دسترسی به داده‌ها می‌شود. داده‌ها در مدل توزیع شده می‌توانند بر روی چندین رایانه مختلف ذخیره و یا در شبکه‌های مختلفی پراکنده شوند. پایگاه‌های داده توزیع‌شده می‌توانند همگن یا ناهمگن باشند .در مدل همگن تمام موقعیت‌های جغرافیایی دارای زیربنای سخت‌افزاری، سیستم‌عامل و نرم‌افزارهای مشابه یا یکسانی هستند اما در مدل ناهمگن، هر موقعیت جغرافیایی

[1] Database Management System (DBMS)
[2] - heterogeneous
[3] - Cooprative

[4] - Access Control
[5] - Discretionary
[6] - Mandatory
[7] - Multilevel

دارای سیستم‌عامل و امکانات سخت‌افزاری و نرم افزاری متفاوتی است . Apache Ignite، Apache Cassandra، Apache HBaseو Amazon SimpleDBاز جمله معروف‌ترین پایگاه‌های داده توزیع‌شده هستند. با افزایش حجم داده‌ها در دنیای اینترنت، پایگاه‌های داده توزیعی نیز با چالش‌های بیشتری روبه‌رو می‌شوند و مدیران پایگاه‌های داده باید توجه به این مسئله داشته باشند [۵-۴]. یکی از مهم ترین این چالش ها چالش امنیتی و بخصوص کنترل دسترسی موثر در پایگاه داده های توزیعی می باشد که بنا به ضرورت تحقیق در این حوزه، در این راستا قصد داریم دیدگاه متدولوژیکی ارائه نمائیم.

دراین بخش دیدگاه متدولوژیک کنترل موثر دسترسی در پایگاههای داده توزیعی بیان می گردد. سپس در مورد سیاستهای کنترل دسترسی موردنیاز در این دیدگاه بحث می شود. 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. اشیاء مجازترکیبات 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 [۶]. به عنوان مثال، در یک سیستم عامل فایلها و دایرکتوریها اشیاء هستند. در حالیکه، در یک DBMS منابعی که باید محافظت شوند رابطه ها، دیدها و صفات هستند. اشخاص مجاز نیز موجودیتهایی در سیستم هستند که اجازهٔ دسترسی به آنها داده می‌شود. کاربران شخصیتهای مجزا و مشخصی هستند که با سیستم در ارتباطند. گروهها مجموعه ای از کاربران و نقشها مجموعه‌ای نامدار از امتیازها که احتیاج دارند، فعالیت خاصی را در رابطه با سیستم انجام دهند می باشند. سیاستهای کنترل دسترسی، معیارهایی هستند که براساس آنها تعیین می‌شود آیا یک درخواست دسترسی باید مجاز شمرده شود یا نه. دیدگاه متدولوژیک کنترل دسترسی در پایگاههای داده توزیعی دیدگاهی جامع است که همه ابعاد مساله کنترل دسترسی را درنظر داشته و رویکردی یکپارچه جهت اعمال و نظارت بر کنترل دسترسی موثر در پایگاه داده های توزیعی ایجاد می نماید. یکی از ابعاد مهم این دیدگاه متدولوژیک سیاست گذاری های کنترل دسترسی می باشد که یک طبقه بندی پایه در این حوزه سیاستهای کنترل دسترسی احتیاطی و الزامی است [۷].

سیاست کنترل دسترسی احتیاطی :

سیاستهای کنترل دسترسی احتیاطی، دسترسی افراد به اشیاء را براساس شناسه افراد، قوانین و مجوزها کنترل می‌کند. قوانین برای هر فرد، مجوزهایی را که می‌تواند برای انجام عملیات روی اشیاء بکار برد، بیان می‌کند. وقتی تقاضای درخواستی به سیستم می‌آید، مکانیسم دسترسی مشخصی می‌کند آیا قانونی برای تأیید این درخواست وجود دارد یا نه. اگر قانونی وجود داشت درخواست مجاز شمرده می‌شود، در غیراین صورت رد می‌شود. چنین مکانیزمی احتیاطی است و در آن به اشخاص اجازه داده می‌شود که مجوز دسترسی به داده‌هایشان را به دیگران بدهند [۸]. 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 می‌دهند. مثل مجوزهای مثبت و منفی و مجوزهای قوی و ضعیف. در سیستمی که مجوز مثبت دارد. هرگاه فردی بخواهد به شیئی خاصی دسترسی داشته باشد، سیستم چک می‌کند آیا مجوزی وجود دارد و فقط در صورت وجود، به شخص اجازه دسترسی داده می‌شود. عدم وجود مجوز به معنی رد درخواست است. مشکل این خط مشی این است که، عدم وجود مجوز به معنای جلوگیری از دسترسی شخص به شیئی در آینده نیست [۹]. این مشکل توسط مجوزهای منفی حل شد که به معنی رد قطعی مجوز در چنین مواردی است. بعضی مدلهایی که هر دو مجوز مثبت و منفی را دارند به دو دسته مجوزهای قوی و ضعیف نیز تقسیم می‌شوند. مجوزهای قوی (چه مثبت و چه منفی) باطل نمی‌شوند. در حالیکه، مجوزهای ضعیف براساس قوانین خاصی توسط مجوزهای قوی یا ضعیف دیگری می‌توانند باطل شوند.

سیاست کنترل دسترسی الزامی:

سیاستهای کنترل دسترسی الزامی بیان کننده دسترسی است که افراد به اشیاء براساس رده بندی شیئی و فرد دارند. این نوع از امنیت تحت عنوان امنیت چند لایه[1] هم نام برده می‌شود. سیستمهای پایگاه داده‌ای که خصوصیات امنیت چند لایه را تأمین می‌کنند، DBMS های امن چند لایه مطمئن نامیده می‌شوند. دراین خط‌مشی‌ها، افراد به عنوان سطوح مجاز مطرح می‌شوند و می‌توانند در سطح مجاز خود عمل کنند. اشیاء به سطوح حساسیت ارجاع می‌شوند. سطوح مجاز حساسیت دسترسی را سطوح امنیتی مرتبط می‌نامند. آنچه در زیر می‌آید، دو قانون مهم این خط مشی است [۱۰]:

- ویژگی امنیتی ساده : یک فرد دسترسی خواندن یک شیئی را دارد اگر سطح امنیتی آن بر سطح امنیتی شیئی مسلط باشد.
- ویژگی ستاره : یک کاربر مجاز دسترسی نوشتن یک شیئی را دارد اگر سطح امنیتی شیئی توسط سطح امنیتی فرد پوشش داده شود.

تحت سیاست احتیاطی یک تقاضای دسترسی مجاز شمرده می‌شود اگر قانونی وجود داشته باشد که دسترسی را مجاز بداند. در مقابل، در 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 [۱۱].

[1] - Multilevel Security

سیاستهای سرپرستی:

یکی دیگر از ابعادی که می تواند معیاری برای مقایسه مدلهای کنترل دسترسی باشد، سیاستهای سرپرستی است، که حمایتگر می باشند. سرپرستی به عملیات اعطا و بازپس گرفتن مجوز اطلاق می‌شود. سیاستهای سرپرستی را به صورت زیر طبقه بندی می‌کنیم [۱۳-۱۲]:

- سرپرستی DBA : تحت این سیاست، فقط DBA می‌تواند حق دسترسی بدهد یا تقاضایی را برگرداند. این سیاست بسیار متمرکز است و امروزه به ندرت در DBMSها بکار می‌رود، مگر در ساده ترین آنها.
- سرپرستی شیئی - مالک: براساس این سیاست که عمدتاً توسط DBMSها و سیستم عاملها استفاده می‌شود، بوجود آوردند شیئی مالک آن محسوب می‌شود و تنها شخص مجاز برای سرپرستی شیئی است.
- سرپرستی متصدی شیئی: بر طبق این سیاست، یک شخص، نه الزاماً ایجاد کننده شیئی، مدیر سرپرستی شیئی است. براساس این سیاست حتی ایجاد کنندهٔ شیئی هم باید مجوز دسترسی به شیئی را دریافت کند.

دومین و سومین سیاست می‌توانند با وکالت سرپرستی و انتقال سرپرستی ترکیب شوند. وکالت سرپرستی به این معناست که مدیر یا سرپرست یک شیئی می‌تواند اعمال سرپرستی بروی یک شیئی را به شخص دیگری واگذار کند. بیشتر DBMSها سیاست سرپرستی براساس سرپرستی مالک با امکان واگذاری را حمایت می‌کنند. 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 می‌دهد. با این تفاوت که سرپرست اولیه امتیاز سرپرستی خود را از دست می‌دهد. عموما برای انتقال سرپرستی دو خط مشی زیر وجود دارد:

- ارجاع بازگشتی[1] : تمام مجوزهایی که توسط سرپرستی پیشین داده شده، به صورت بازگشتی ارجاع داده می‌شود.
- انتقال واگذار کننده[2] : تمام مجوزهای که توسط سرپرستی پیشین صادر شده نگه داشته می‌شوند.

علاوه براین انتقال می‌تواند با پذیرش یا بدون پذیرش باشد. پذیرش به معنای این است که شخصی که سرپرستی به او واگذار می‌شود باید صریحاً این مسؤولیت را بپذیرد. انتقال بدون پذیرش به معنای این است که چنین پذیرشی احتیاج نیست.

مدلهای کنترل دسترسی احتیاطی در دیدگاه متدولوژیک

دراین بخش به بررسی و بحث در مورد مدلها و سیستمهای کنترل دسترسی احتیاطی یا 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 DBMS های رابطه‌ای، مدلهای اعطای مجوز برای DBMS های شیئی گرا و مدلهای اعطای مجوز برای DBMS های فعال [۱۵-۱۴].

مدلهای اعطای مجوز برای DBMSهای رابطه‌ای

دراین 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. دراین 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، انتخاب برای انتخاب تاپلها از جدول، به روز رسانی برای تغییر تاپلهای یک جدول، درج و حذف برای افزودن یا حذف کردن تاپلهای جدول، حذف جدول برای پاک کردن کل یک جدول. گروه و نقش دراین مدل حمایت نمی‌شوند. این مدل امکانات سرپرستی نامتمرکز را حمایت می‌کند. هرگاه شخصی جدولی را بوجود می‌آورد. امتیازی را نسبت به آن بدست می‌آورد. مالک جدول می‌تواند تمام امتیازها را بر جدول اعمال کند. این مدل ارجاع بازگشتی دارد، به این معنا که وقتی شخصی مجوز جدولی را از کاربر دیگری می‌گیرد. تمام مجوزهایی که قبلاً به او داده شده ارجاع می‌شود [۱۶].

مدلهای اعطای مجوز برای DBMSهای شیئی گرا

امروزه DBMSهای شیئی‌گرا و شیئی رابطه‌ای از مهمترین زمینه های تحقیق در حوزه پایگاه داده هستند. دلیل این اهمیت این است که آنها بسیار مناسب برای کاربردهای پیشرفته مثل CAD/CAM، مولتی مدیا و کاربردهای نقشه‌کشی هستند. چون این برنامه‌ها احتیاج به مدلهای داده‌ای غنی‌تری نسبت به مدلهای رابطه‌ای دارند. احتیاجات سیستمهای DBMSها هم متفاوت از سیستمهای رابطه ای است و این باعث می‌شود مدلهای سنتی برای DBMSهای رابطه‌ای، برای سیستمهای شیئی‌گرا کافی نباشد. با وجود رشد علاقه و توجه به ODBMSها، 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.

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

[1] - Recursive Revoke

[2] - Grantor Tronsfer

وجود داشته باشد که اجازه این کار را داشته باشد. نقشها، اشیاء و امتیازها تحت یک سلسله مراتب سازماندهی می‌شوند و یکسری قوانین انتشار یا تکثیر اعمال می‌شود [۱۷]:

- اگر یک نقش مجوز دسترسی به یک شیئی را داشته باشد، تمام نقشهای سلسله مراتب بالاتر از آن در سلسه 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 می‌شوند. نهایتاً قوانین انتشار بر یک شیئی اجازهٔ مجوزهایی را می‌دهد که از مجوزهای شیئی که، منقطاً با آن در ارتباط است، مشتق شده باشد. به عنوان مثال مجوز خواندن یک کلاس، مجوز خواندن تمام نمونه‌های آن را صادر می‌کند.

مدل Iris

در مدل Iris ، صفات و متددها 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 می‌شود و به طور خودکار امتیاز فراخوانی آن را دریافت می‌کند. علاوه براین مالک یک تابع می‌تواند امتیاز فراخوانی تابع را به افراد دیگر هم بدهد. این اعطای امتیاز می‌تواند شامل شرایط هم باشد، که به شخصی که امتیاز را می‌گیرد اجازه می‌دهد که آن را به دیگران هم بدهد. این مدل اجازه می‌دهد که یک امتیاز هم به گروه و هم به کاربر داده شود یا گرفته شود. یک کاربر می‌تواند متعلق به چندین گروه باشد. توابع مشتق شده تحت عنوان توابع دیگر تعریف می‌شوند. علاوه براین، گروهها می‌توانند تو در تو باشند. مدل Iris دو خط مشی برای حفاظت از توابع مشتق شده دارد. تحت خط مشی که مجوز استاتیک نامیده می‌شود، فردی که تقاضای اجرای یک تابع مشتق را دارد. فقط باید اجازه فراخوانی تابع مشتق را داشته باشد. در خط مشی دیگر، مجوز دینامیک، فرا خواننده هم باید مجوز فراخوانی تابع مشتق را داشته باشد و هم مجوز برای فراخوانی تمام توابعی که تابع مشتق آنها را اجراء می‌کند. 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 می‌کند: توابع نگهبان[1] و توابع پراکسی[2]. 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 می‌کند تابع هدف نامیده می‌شود. یک تابع هدف اجراء می‌شود، اگر تابع نگهبان مربوط به آن موفق ارزیابی شود. مهمترین مزیت تابع نگهبان این است که دسترسی به یک تابع محدود می‌شود، بدون اینکه لازم باشد کد تابع تغییر کند. توابع پراکسی، پیاده سازی‌های مختلفی از یک تابع مشخص را برای افراد مختلف، فرد یا گروه، تأمین می‌کند. وقتی یک تابع مورد درخواست واقع می‌شود، تابع پراکسی مناسب به جای تابع اصلی اجراء می‌شود [۱۸].

مدلهای اعطای مجوز برای DBMSهای فعال

پایگاه داده‌های فعال با یک سیستم قانونمند که DBMS را قادر می‌سازد با تریگر کردن قانونها نسبت به حوادث عکس‌العمل نشان دهد، تعریف می‌شوند. قوانین اعمالی را توصیف می‌کند که می‌خواهیم به صورت خودکار در هنگام رخ دادن حادثه خاصی یا ارضاء شدن شرط خاصی در DB اجراء شوند. به عنوان یک مثال از این مدل در ادامه امکانات سیستم Starbust را شرح می‌دهیم. Starbust یک نمونه از سیستم پایگاه داده‌ای رابطه‌ای توسعه پذیر است که در مرکز تحقیقاتی Almaden در IBM تولید شده است. Starbust بوسیلهٔ یک زبان قانونمند توصیف می‌شود. مدل اعطای مجوز آن سلسله مراتبی است و از انواع امتیازها که در پایگاه داده توزیعی می‌تواند اعمال شود، حمایت می‌کند. دراین سلسله مراتب عناصر بالاتر، انواع پائین‌تر را پوشش می‌دهند. مثالی از انواع امتیازها، کنترل است که تمام امتیازهای دیگر یعنی Write، Alter و Attach را پوشش می‌دهد. وقتی یک جدول ایجاد می‌شود مالک آن امتیاز کنترل آن را دریافت می‌کند. ایجاد و تغییر قوانین توسط محدودیتهای زیر اداره می‌شوند [۱۹]:

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

کنترل دسترسی احتیاطی در DBMSهای تجاری

دراین بخش، توضیح می‌دهیم که چگونه DAC در سیستم شیئی رابطه‌ای اوراکل اعمال می‌شود. در اوراکل، امتیازها به هر دو گروه کاربران و نقشها داده می‌شود. نقشها در یک سلسه مراتب سازمان دهی شده‌اند و یک نقش تمام امتیازات نقشهای زیر خود در سلسله مراتب را بدست می‌آورد. یک کاربر ممکن است مجاز برای ایفای چند نقش در یک فاصلهٔ زمانی باشد. با هر نقشی ممکن است یک کلمه عبور همراه

[1] - Guard

[2] - Proxy

شود. تا از استفاده غیرمجاز امتیازها جلوگیری کند. مجموعه‌ای از پیش تعریف شده از امتیازها فراهم است که می‌تواند به هر کدام از نقشها در اوراکل تغییر داده شود. وقتی یک فرد نقشی را ایجاد می‌کند، نقش به طور خودکار با اختیارات سرپرستی[1] به ایجاد کننده داده می‌شود، که به او اجازه می دهد نقش را به نقشی دیگر بدهد یا از او بگیرد و این کار را می‌تواند با اختیارات سرپرستی یا بدون آن باشد. پایگاه اوراکل همچنین گروه خاص، عمومی[2] را حمایت می‌کند که برای هر فردی قابل دسترسی است. امتیازها در پایگاه داده اوراکل عموما به دو بخش کلی تقسیم می‌شوند [۲۱-۲۰]:

- امتیازات سیستم: 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 برنامه‌های کاربردی داده می‌شدند. مثل نقشها این امتیازات می‌توانند با اختیارات سرپرستی داده می‌شوند و اگر شخصی امتیاز سیستمی با اختیارات سرپرستی را داشته باشد می‌تواند این امتیاز را به افراد دیگر بدهد یا از آنها بگیرد.
- امتیازات شیئی: به فرد اجازه می‌دهد، 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 می‌کند، به طور اتوماتیک تمام امتیازات شیئی را در مورد آن شیئی مثل حق دادن این امتیاز به دیگران را دریافت می‌کند. اگر این اعطا امتیاز همراه با اختیار اعطاء آن باشد، فرد دریافت کننده می‌تواند این امتیاز را به دیگران دم بدهد. امتیاز شیئی فقط توسط شخصی که آن را اعطاء کرده بازگردانده می‌شود. بازگشت و ارجاع این امتیاز بازگشتی است.

امنیت چندلایه در سیستمهای پایگاه داده‌ای

دراین بخش به شرح جنبه‌های امنیت چندلایهٔ 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[3]، نامتجانس[4] و یکپارچه[5] است. ما دراین بخش به بحث در مورد بعضی از این پیشرفتها می‌پردازیم.

مدل داده‌ای رابطه‌ای چند لایه

دریک پایگاه دادهٔ چند لایه، تمام داده‌ها به سطح امنیتی یکسانی منسوب نمی‌شوند. اگر چنین پایگاه داده‌ای براساس مدل رابطه‌ای باشد، اشیاء طبقه بندی شده ممکن است شامل کل DB، رابطه‌ها، تاپلها، صفات و عناصر داده‌ای باشد. دسترسی به چنین اشیایی توسط سیاست الزامی که در بخش قبل بحث 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 بدون تعارض با قوانین امنیتی و جامعیتی است. یکی از مکانیزمهای ارائه شده، چند نمونه ای بودن[6] است. این مکانیزم اجازه می‌دهد 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 داده‌ای رابطه‌ای استاندارد است [۲۲].

اخیراً بحثهای بسیاری در مورد چند نمونه ای بودن وجود دارد. عده‌ای معتقدند چند نمونه‌ای بودن لازم است اگر ما قصد طراحی پایگاه داده های چندلایه با ضریب اطمینان بالا را داریم و عده‌ای براین عقیده‌اند که جامعیت DB اهمیت بیشتری دارد و چند نمونه‌ای بودن با آن در تناقض است. سیستمهایی که در این مقاله بحث می‌کنیم انواع مختلفی از مدل داده‌ای چند لایه را ارائه داده اند و همه خصوصیات امنیتی را که دراین بخش در مورد آنها صحبت شد را ارضاء می‌کنند و چند نمونه‌ای بودن هم در بسیاری مدلها وجود دارد.

معماری های مرتبط در دیدگاه متدولوژیک

دراین بخش مدلهای مختلف کنترل دسترسی که برای MLS/DBMS ها تولید شده‌اند، بررسی می کنیم. در حالیکه DBMSها باید با انواع مختلف موارد امنیتی به عنوان سیستم عاملهای قابل اطمینان در تعامل باشند، خصوصیات DBMS هاست 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 سایزهای چندگانه باشند و بتوانند دانه دانه باشند. این با سیستمهایی که در آنها دانه دانه بودن وجود ندارد در تناقض است. 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

---

1 - Admin Options
2 - Public
3 - Distributed
4 - hetrogeneous
5 - Fedrated
6 - polyinstantiation

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 نحوهٔ عملکرد و احتیاجات امنیتی DBMS ها و سیستم عاملها به این معناست که راه حلهای سنتی که برای تأمین امنیت سیستمهایی که با این سیستم عاملها بخوبی کار می‌کردند، نیاز دارند برای DBMS ها تغییر داده شوند. در حال حاضر، هیچ معماری به تنهایی مورد قبول یا مورد استفاده در تولید MLS/DBMS ها نیست. گسترده وسیعی از خط مشی‌ها برای طراحی و ساخت MLS/DBMS ارائه شده است. بعضی نظریه‌ها دراین مورد عبارتند از [۲۳و۱۸-۱۹]:

- معماری **Single-kernel**: دراین مدل کنترل دسترسی تماماً به عهدهٔ سیستم عامل است و **DBMS** نقشی در آن ندارد.
- معماری **Distributed**: بر طبق این خطی مشی چندین ماشین انتهایی[1] **DBMS** و یک ماشین ابتدایی[2] مطمئن وجود دارد که انتهایی از طریق آن با هم در ارتباطند.
- معماری **Trusted-Subject**: دراین خط مشی که گاهی دو هسته‌ای[3] هم نامیده می‌شود، براساس سیستم عامل عمل نمی کند و **DBMS** کنترل دسترسی را به عهده دارد.
- معماری **Integrity-lock**: دراین معماری یک انتهایی سیستم مدیریت پایگاه داده 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. دراین خط مشی مهم است که عناصر نامطمئن از هم جدا باشند. بنابراین می توان مطمئن بود که هیچ دو عنصر نامطمئن خارج از نظارت فیلتر مطمئن با هم ارتباط ندارند.
- معماری **Extended-Kernel**: این معماری اساسا گسترشی بر مدل اول است. دراین معماری سیستم عامل همچنان دو راه حل **MAC** و **DAC** را به کار می‌برد. دراین مدل **TDBMS** بعضی راه‌حلهای مکمل برای فراهم کردن کنترل دسترسی را اضافه می‌کند.

نتیجه گیری

در دهه های اخیر تعداد پایگاه داده‌های توزیعی افزایش بسیاری داشته است. پایگاه داده‌های توزیع شده، بر خلاف دیتابیس‌هایی که در یک ماشین واحد تعبیه شده‌اند، قابل افزایش مقیاس هستند، کارایی زیادی دارند و شفافیت داده‌ها نیز در آن‌ها ملموس است. کنترل دسترسی در سیستم های توزیع شده به دلیل مشارکت تعداد زیاد دستگاه ها و افراد از اهمیت زیادی برخوردار است و حفظ همخوانی و یکپارچگی داده ها و سطح مناسب دسترسی افراد به داده ها یک اصل مهم به شمار می آید. دراین مقاله دیدگاه متدولوژیک کنترل دسترسی موثر در پایگاه داده توزیعی ایمن را مطرح نمودیم. براین اساس، ابعاد این دیدگاه متدولوژیک و مفاهیم اساسی در کنترل دسترسی همچنین سیاستهای مختلف دسترسی معرفی شدند و همچنین مروری داشتیم بر سیاستهای سرپرستی ارائه شده و امنیت الزامی، مدلهای داده‌ای، معماری ها و محصولات تجاری. به عنوان رویکردهای آتی لازم به ذکر است، تکنولوژیهای جدید مثل داده کاوی به حل مشکلات امنیتی و کنترل موثر دسترسی پایگاه داده های توزیعی کمک خواهند کرد و به طور کلی پایگاه داده های توزیعی همچنان در تکاپو خواهد بود و مسئله امنیت بیش از پیش اهمیت می یابد.

مراجع

[1] Al-Sayid NA, Aldlaeen D. Database security threats: A survey study. In2013 5th international conference on computer science and information technology 2013 Mar 27 (pp. 60-64). IEEE.

[2] Chica JC, Imbachi JC, Vega JF. Security in SDN: A comprehensive survey. Journal of Network and Computer Applications. 2020 Jun 1;159:102595.

[3] Uzunov AV, Fernandez EB, Falkner K. Securing distributed systems using patterns: A survey. Computers & Security. 2012 Jul 1;31(5):681-703.

[4] Uzunov AV. A survey of security solutions for distributed publish/subscribe systems. Computers & Security. 2016 Aug 1;61:94-129.

[5] Tan YS, Ko RK, Holmes G. Security and data accountability in distributed systems: A provenance survey. In2013 IEEE 10th

[1] - Back-end
[2] - Front-end
[3] - Dual-kernel

[14] Dekker MA, Etalle S. Audit-based access control for electronic health records. Electronic notes in theoretical computer science. 2007 Feb 8;168:221-36.

[15] Inukollu VN, Arsi S, Ravuri SR. Security issues associated with big data in cloud computing. International Journal of Network Security & Its Applications. 2014 May 3;6(3):45.

[16] McCollum CJ, Messing JR, Notargiacomo L. Beyond the pale of MAC and DAC--Defining new forms of access control. InProceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy 1990 May 1 (pp. 190-190). IEEE Computer Society.

[17] Kulkarni S, Urolagin S. Review of attacks on databases and database security techniques. International Journal of Emerging Technology and Advanced Engineering. 2012 Nov;2(11):253-63.

[18] Curtis LH, Weiner MG, Boudreau DM, Cooper WO, Daniel GW, Nair VP, Raebel MA, Beaulieu NU, Rosofsky R, Woodworth TS, Brown JS. Design considerations, architecture, and use of the Mini-Sentinel distributed data system. Pharmacoepidemiology and drug safety. 2012 Jan;21:23-31.

[19] Mazurek ML, Arsenault JP, Bresee J, Gupta N, Ion I, Johns C, Lee D, Liang Y, Olsen J, Salmon B, Shay R. Access control for home data sharing: Attitudes, needs and practices. InProceedings of the SIGCHI Conference on Human Factors in Computing Systems 2010 Apr 10 (pp. 645-654).

[20] Ryutov T, Zhou L, Neuman C, Leithead T, Seamons KE. Adaptive trust negotiation and access control. InProceedings of the tenth ACM symposium on Access control models and technologies 2005 Jun 1 (pp. 139-146).

[21] Ullah F, Edwards M, Ramdhany R, Chitchyan R, Babar MA, Rashid A. Data exfiltration: A review of external attack vectors and countermeasures. Journal of Network and International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing 2013 Nov 13 (pp. 1571-1578). IEEE.

[6] Santos, R.J., Bernardino, J. and Vieira, M., 2011, April. A survey on data security in data warehousing: Issues, challenges and opportunities. In *2011 IEEE EUROCON-International Conference on Computer as a Tool* (pp. 1-4). IEEE.

[7] Gupta N, Agrawal R. Challenges and security issues of distributed databases. InNoSQL 2017 May 19 (pp. 251-270). Chapman and Hall/CRC.

[8] Benantar M. Access control systems: security, identity management and trust models. Springer Science & Business Media; 2005 Dec 9.

[9] Colombo P, Ferrari E. Privacy aware access control for big data: A research roadmap. Big Data Research. 2015 Dec 1;2(4):145-54.

[10] Bertino E, Ferrari E. Big data security and privacy. InA comprehensive guide through the Italian database research over the last 25 years 2017 May 31 (pp. 425-439). Cham: Springer International Publishing.

[11] Metoui N, Bezzi M, Armando A. Risk-based privacy-aware access control for threat detection systems. Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXVI: Special Issue on Data and Security Engineering. 2017:1-30.

[12] Abouelmehdi K, Beni-Hssane A, Khaloufi H, Saadi M. Big data security and privacy in healthcare: A Review. Procedia Computer Science. 2017 Jan 1;113:73-80.

[13] Paananen H, Lapke M, Siponen M. State of the art in information security policy development. Computers & Security. 2020 Jan 1;88:101608.

Computer Applications. 2018 Jan 1;101:18-54.

[22] Panda BN. Query processing in multilevel secure database systems. North Dakota State University; 1993.

[23] Sharma PK, Singh S, Jeong YS, Park JH. Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. IEEE Communications Magazine. 2017 Sep 8;55(9):78-85

تعارض منافع

«هیچ‌گونه تعارض منافع توسط نویسندگان بیان نشده است»