بسم الله الرحمن الرحيم

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر گرایش نرم‌افزار

کنترل دسترسی در پایگاه‌های داده متحرک با استفاده از عامل‌های متحرک

استاد راهنما:

دکتر احمد براآنی

پژوهشگر:

امین صداقتی

۱۳۸۸/۱۰/۲۷

شهریور ماه ۱۳۸۸

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر گرایش نرم‌افزار آقای امین صداقتی تحت عنوان

کنترل دسترسی در پایگاه‌های داده متحرک با استفاده از عامل‌های متحرک

در تاریخ ۱۳۸۸/۶/۲۸ توسط هیأت داوران زیر بررسی و با درجه خوب به تصویب نهایی رسید.

۱- استاد راهنمای پایان نامه	دکتر احمد براآنی	با مرتبه ی علمی استادیار	امضا
۲- استاد داور داخل گروه	دکتر بهروز ترک لادانی	با مرتبه ی علمی استادیار	امضا
۳- استاد داور خارج از گروه	دکتر مهدی برنجکوب	با مرتبه ی علمی استادیار	امضا

امضای مدیر گروه

سپاسگزاری

با سپاس فراوان از جناب آقای دکتر احمد براآنی، به خاطر تمام کمک‌ها و راهنمایی‌های دلسوزانه‌اش و با سپاس از تمامی اساتید گروه *کامپیوتر* که فرصت و شرایط تکمیل این پروژه را برای من فراهم آوردند.

تقدیم به پدر و مادر عزیزم

چکیده

پیشرفت های اخیر در زمینه سخت‌افزارها و تکنولوژی‌های ارتباطی منجر به افزایش حیرت‌انگیز کامپیوترهای همراه شده است. با توجه به این موج جدید در جریان انتقال و دسترسی به اطلاعات، می توان سال-های پیش‌رو را عصر محاسبات همراه و شکل جدیدی از تجارت الکترونیک، یعنی تجارت همراه دانست. با ظهور کامپیوترهای قابل حمل قدرتمندتر، مفهوم دسترسی مطمئن و به‌هنگام به منابع اطلاعاتی به سرعت در حال تغییر است. کاربران خواسته‌های جدیدی دارند: آن ها می‌خواهند تا در هر زمان و در هر مکان، به هر اطلاعاتی که نیاز دارند دسترسی مطمئن و امنی داشته باشند. این بر عهده مکانیسم‌های کنترل دسترسی است که این خواسته را برآورده کنند.

رواج وسایل محاسباتی متحرک، آن‌ها را به اهدافی دوست‌داشتنی برای توسعه کدهای بدخواه و تلاش‌های خرابکارانه تبدیل کرده است و این حملات به پایگاه‌های داده روز به روز بیشتر می‌شوند. از سوی دیگر تحرک-پذیری، محدودیت‌ها و ویژگی‌های خاص خودش را نسبت به محیط‌های ثابت دارا می‌باشد که از آن جمله می‌توان به انفصالات پی‌درپی و جابجایی کاربران اشاره کرد. این ویژگی ها ابعاد جدیدی از امنیت را مطرح می‌کنند. آن‌ها منجر به تأخیر در دسترسی کاربر به داده‌های درخواستیش و درنتیجه تغییر در شرایط دسترسی کاربر به آن داده‌ها می‌شوند. بنابراین، مکانیسم‌های کنترل دسترسی می‌بایست این تغییرات را به‌صورت پویا و انعطاف‌پذیر پوشش دهند. اما، روش‌هایی که در حال حاضر در این حیطه به کار می‌روند نتوانسته‌اند به طور کامل با این محدودیت‌ها و ویژگی‌ها سازگار شوند.

در این پروژه روشی ارائه می‌دهیم که با بهره‌گیری توامان از عامل‌های متحرک و شکلی از کنترل دسترسی مبتنی بر نقش در قالب لیست‌های قابلیت، شیوه‌ای از دسترسی پویا، انعطاف‌پذیر و مطمئن به پایگاه‌های داده متحرک را فراهم می‌سازد. روش پیشنهادی با بهره‌گیری از خاصیت تحرک‌پذیری عامل‌ها، تأثیر انفصالات پی در پی و جابجایی وسایل متحرک و تأخیر ناشی از آن‌ها را نیز تعدیل کرده است.

کلیدواژه: پایگاه داده متحرک، کنترل دسترسی، عامل متحرک، مجوزدهی، لیست قابلیت

فهرست مطالب

عنوان صفحه

عنوان | صفحه

عنوان | صفحه

فصل سوم: پایگاه های داده متحرک

عنوان | صفحه

فصل چهارم: مروری بر روش‌های کنترل دسترسی در پایگاه‌های داده متحرک

فصل پنجم: روش پیشنهادی

عنوان | صفحه

فصل ششم: ارزیابی روش پیشنهادی

عنوان | صفحه

فهرست شکل‌ها

عنوان — صفحه

عنوان | صفحه

فهرست جدول‌ها

عنوان **صفحه**

فصل اول: مقدمه

۱-۱ مقدمه

در سال‌های اخیر، شاهد پدیده جهانی شدن و رشد روزافزون تبادل اطلاعات هستیم. پیش‌بینی می‌شود تعداد وسایل تبادل اطلاعات از ۲.٤ بیلیون در سال ۲۰۰٦ به ۲۳ بیلیون در سال ۲۰۰۸ برسد و در سال ۲۰۱۲ این رقم به یک تریلیون خواهد رسید. از این حجم عظیم وسایل، قسمت زیادی متحرک خواهند بود. از طرفی، تکنولوژی بی‌سیم، تمامی جنبه‌های مختلف زندگی ما را تحت تأثیر قرار داده است و کاربردهای وسایل متحرک و همراه، به طور روزافزون در حال افزایش است. در این میان افزایش امنیت و جامعیت اطلاعات، با حفظ سرعت دسترسی، اهمیت زیادی دارد. به این ترتیب، با این حجم عظیم تبادلات، یافتن روشی برای کنترل دسترسی با کمترین سربار اضافی روی سرورها، اهمیت حیاتی دارد.

هنگامی که از یک پایگاه اطلاعاتی امن صحبت می‌شود، منظور پایگاه داده ای است که نیازهای امنیتیِ محرمانگی، جامعیت و در دسترس بودن را برآورده کند. مکانیسم‌هایی چون کنترل دسترسی، محدودیت‌های جامعیت معنایی و مکانیسم‌های بازیابی برای ایجاد یک بانک اطلاعاتی امن به کار می‌روند.

یکی از روش‌های برقراری امنیت در پایگاه داده، به منظور حفظ محرمانگی داده‌ها، "کنترل دسترسی" است که عبارتست از اجازه دادن یا رد کردن حق استفاده یک نفر از یک چیز. هدف کنترل دسترسی، کنترل

اَعمال اشخاص است تا از ایجاد خسارت در داده‌ها و منابع جلوگیری شود. سیاست‌ها و مدل‌های کنترل دسترسی در پایگاه داده را معمولاً به دو گروه تشخیصی و اجباری تقسیم می‌کنند. در مدل تشخیصی یک کاربر می‌تواند سیاست امنیتی را برای یک شیء تعیین کند اما در مدل اجباری سیاست‌های امنیتی در داخل سیستم ایجاد می‌شوند و کاربران نمی‌توانند آنها را تغییر دهند. بدین ترتیب در کل مدل‌های مختلف کنترل دسترسی باید این سرویس‌ها را ارائه دهند: شناسایی و احراز اصالت، اجازه، و رسیدگی و بازرسی.

یک سیستم پایگاه داده متحرک عبارتست از یک سیستم پایگاه داده توزیع‌شده که خاصیت تحرک‌پذیری به آن افزوده شده است. یک شبکه بی‌سیم مجموعه ای از سلول‌های بی‌سیم است که به یک شبکه ثابت متصل شده‌اند یا به طور کلی‌تر مجموعه‌ای از سلولهای بی‌سیم متصل به شبکه ثابت، می‌باشد. در سیستم‌های قابل حمل، بدلیل خواص شبکه‌های بی‌سیم با پیچیدگی‌های بیشتر و محدودیت‌هایی در مقایسه با سیستم‌های سنتی مواجه می‌شویم که هر کدام از آن‌ها به یکی از شش گروه زیر مربوط می‌شوند:

۱) تحرک‌پذیری دستگاه‌ها

۲) اتصال به شبکه‌ای با پهنای باند محدود، و در نتیجه ارتباطات کند بین دستگاه‌ها

۳) احتمال بسیار زیاد انفصال دستگاه‌های متحرک

٤) محدودیت‌های پردازش، منابع و قدرت، و درنتیجه قدرت محاسباتی و حجم ذخیره‌سازی محدود

٥) استقرار داده‌ها در تعداد زیادی از منابع (متحرک و ثابت)

٦) وجود کپی‌های چندگانه از داده‌ها در دستگاه‌های مختلف

چهار ویژگی اول خاص پایگاه های داده متحرک و دو ویژگی آخر، از ویژگی‌های پایگاه های داده توزیع شده می‌باشند. یک سیستم پایگاه داده با این محدودیت‌ها را یک "سیستم دسترسی به پایگاه داده متحرک" می‌نامند. در این سیستم‌ها کم و بیش و بدون در نظر گرفتن وسیله سخت‌افزاری، جایگاه داده‌ها، و نوع دسترسی به داده‌ها، تمامی کاربران نیازهای مشابهی دارند: دسترسی مطمئن و سریع به انواع مختلف داده‌ها. خواص و محدودیت‌های خاص پایگاه‌های داده متحرک سبب شده‌اند تا کنترل دسترسی در پایگاه‌های داده متحرک پیچیده‌تر شود، و نیازها و نگرانی‌های جدیدی در ارتباط با امنیت اطلاعات در پایگاه‌های داده مطرح شوند:

۱) با توجه به خاصیت تحرک‌پذیری مکان کاربر باید از دید سایرین پنهان باشد.

۲) با وجود تحرک کاربر، باید بتواند اطلاعات مورد نیازش را در مکان جدید دریافت کند.

۳) احتمال شنود و سرقت اطلاعات در حین انتقال بسیار بالاست.

٤) با وجود انفصال‌های متناوب، وسیله متحرک باید بدون وقفه و اشکال، عملکرد خود را انجام دهد.

٥) حرکت کاربر و انفصالات پی‌درپی در شبکه بی‌سیم سبب تأخیر در تحویل داده‌ها و در نتیجه تغییر در شرایط زمینه و متعاقباً تغییر در مجوزها می‌شود. کنترل دسترسی می‌بایست این شرایط را به طور پویا کنترل کند.

٦) گم شدن واحدهای متحرک ممکن است سبب از دست دادن محرمانگی داده‌ها شود.

٧) با توجه به هزینه بالای ارتباطات و محدودیت حافظه در وسایل متحرک، مدل‌های کنترل دسترسی باید تا حد امکان کوچک باشند.

٨) با توجه به محدودیت منابع در وسایل متحرک، پردازش‌ها می‌بایست سبک باشند.

٩) وجود کپی‌های چندگانه از داده‌ها و توزیع‌شدگی داده‌ها می‌توانند سبب ناسازگاری و ناکارایی پروتکل‌های امنیتی شوند.

روش کنترل دسترسی در مواجهه با این موارد باید از حدی مناسب از پویایی و انعطاف‌پذیری برخوردار باشد. در این پروژه به دنبال راه حلی برای کنترل دسترسی در پایگاه های داده متحرک هستیم تا نیازها و ویژگی-های خاص این سیستم‌ها را پوشش دهد. در این نوع از شبکه ها، مجموعه‌ای از کاربران متحرک با ابزارهای همراهشان را داریم که می‌خواهند به پایگاه‌های داده‌ای که در شبکه پخش شده‌اند دسترسی پیدا کنند. این پایگاه‌های داده در یک سرور پایگاه‌داده مستقر می‌باشند. در محیط‌های متحرک و پایگاه‌های داده متحرک با محیطی پویا مواجه هستیم، محیطی که مدام در حال حرکت و تغییر است. بهترین ابزار برای کار در این محیط ابزاری است که بتواند این پویایی و حرکت را دنبال کند. حرکت و پویایی از ویژگی‌های عامل‌های متحرک می‌باشند. از طرفی یکی دیگر از اهداف در این محیط، کارکردن بدون وقفه و به طور مستقل است که عامل‌ها با خاصیت خودکاری و استقلالشان می‌توانند برای این منظور ابزاری مناسب باشند. از طرفی عامل‌ها می توانند در شرایط اضطراری خود و یا عامل‌های دیگر را از بین ببرند و این خاصیتی مفید است که در شرایط انفصال یا گم شدن واحد متحرک می‌تواند مفید باشد.

به همین دلایل در روش پیشنهادی در این پروژه، از عامل ها برای کنترل دسترسی بهره می‌بریم. هر کاربر برای انجام عملیات، عاملی تولید می‌کند، کارها را به او می‌سپارد و او را به سمت سرور (فراهم کننده خدمات موردنظر) می‌فرستد. عامل حتی در صورت انفصال تولیدکننده‌اش، به کار خود ادامه می دهد و پس از اتمام عملیات، منتظر اتصال تولیدکننده اش می شود، سپس به خانه بازمی‌گردد و نتایج را گزارش می‌دهد.

کارهای زیادی در زمینه امنیت در پایگاه های داده متمرکز انجام گرفته که از آن جمله می‌توان به مدل مبتنی بر هویت، مدل مبتنی بر نقش، مدل مبتنی برقابلیت، و چندین و چند مدل دیگر اشاره کرد. اما، تلاش‌های کمی در ارتباط با کنترل دسترسی در پایگاه‌های داده متحرک و ویژگی‌های خاص امنیتی در آن‌ها، صورت گرفته‌اند. مدل‌هایی که امروزه برای کنترل دسترسی در پایگاه‌های داده متحرک به کار می‌روند، در واقع تغییر یافته مدل‌های به کار رفته در پایگاه‌های داده متمرکز هستند.

۱-۲ اهداف تحقیق

بدست آوردن امنیت بالا و البته با الگوریتمی سبک و توزیع‌شده، آرزوی بسیاری از نهادها و سازمان‌های اقتصادی است. از جمله می‌توان به بانک‌ها، موسسات کارت‌های اعتباری، فروشگاه‌های الکترونیک، موسسات تحقیقاتی و خبری، و در کل هر گروه یا سازمانی که می‌خواهد "در هر زمان و هر کجا" اطلاعاتی مهم و ارزشمند ارائه کند، اشاره کرد. با تحقق این هدف، و جلب اعتماد اکثریت افراد در جامعه، گسترش سریعی در ابزارهای همراه شکل خواهد گرفت.

اما، همانطور که در بخش قبل نیز گفته شد کنترل دسترسی در محیط‌های متحرک با ضعف‌های زیادی مواجه است. به همین دلیل، در این پروژه به دنبال ایجاد یک مکانیسم کنترل دسترسی هستیم تا با بهره‌گیری از خواص عامل‌های متحرک، و با وجود محدودیت‌های پایگاه‌های داده متحرک، در بالاترین سطح، امنیت پایگاه داده را تامین کند:

- عامل‌ها می‌توانند وارد یک ایستگاه شده، پرس‌وجوی مورد نیازشان را پردازش کنند و تنها اطلاعات حاصل را انتقال دهند، و به این ترتیب از انتقال حجم وسیعی از اطلاعات جلوگیری کنند و همچنین محدودیت‌های منابع در یک واحد متحرک را بپوشانند.
- عامل‌ها می‌توانند به صورت پویا تغییرات در مقادیر زمینه‌ها را پیگیری کنند تا از اعتبار مجوزها حتی پس از تأخیر (ناشی از انفصال و جابجایی) اطمینان حاصل کنند.
- عامل‌ها با حرکت در بین سرورهای محلی ثابت، خود را به واحد متحرک می‌رسانند و به او ملحق می‌شوند.

در کل هدف، ارائه یک مدل کنترل دسترسی سبک، پویا و انعطاف‌پذیر در پایگاه‌های داده متحرک است.