

سید الشہداء



دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه‌ی کارشناسی ارشد رشته‌ی مهندسی کامپیوتر گرایش نرم افزار

کنترل دسترسی در پایگاه‌های داده متحرک با استفاده از عامل‌های متحرک

استاد راهنما:

دکتر احمد برآنی

پژوهشگر:

امین صداقتی

۱۳۸۸/۱۰/۲۷

تعمیر مدارک
اطلاعات مدارک علمی بزرگ

شماره بور ماه ۱۳۸۸

۱۲۹۸۷۰

کلیه حقوق مادی مترتب بر نتایج مطالعات، ابتکارات
و نوآوری های ناشی از تحقیق موضوع این پایان نامه
متعلق به دانشگاه اصفهان است.



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 برآنی

با مرتبه‌ی علمی استادیار

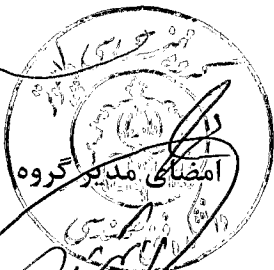
۲- استاد داور داخل گروه دکتر بهروز ترک‌لادانی

با مرتبه‌ی علمی استادیار

۳- استاد داور خارج از گروه دکتر مهدی برنجکوب

با مرتبه‌ی علمی استادیار

امضا
امضا
امضا



سپاسگزاری

با سپاس فراوان از جناب آقای دکتر احمد برآنی، 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 سخت افزارها و تکنولوژی های ارتباطی منجر به افزایش حیرت انگیز کامپیوترهای همراه شده است. با توجه به این موج جدید در جریان انتقال و دسترسی به اطلاعات، می توان سال-های پیش رو را عصر محاسبات همراه و شکل جدیدی از تجارت الکترونیک، یعنی تجارت همراه دانست. با ظهور کامپیوترهای قابل حمل قدرتمندتر، مفهوم دسترسی مطمئن و به هنگام به منابع اطلاعاتی به سرعت در حال تغییر است. کاربران خواسته های جدیدی دارند: آن ها می خواهند تا در هر زمان و در هر مکان، به هر اطلاعاتی که نیاز دارند دسترسی مطمئن و امنی داشته باشند. این بر عهده مکانیسم های کنترل دسترسی است که این خواسته را برآورده کنند.

رواج وسایل محاسباتی متحرک، آن ها را به اهدافی دوست داشتنی برای توسعه کدهای بدخواه و تلاش های خرابکارانه تبدیل کرده است و این حملات به پایگاه های داده روز به روز بیشتر می شوند. از سوی دیگر تحرک-پذیری، محدودیت ها و ویژگی های خاص خودش را نسبت به محیط های ثابت دارا می باشد که از آن جمله می توان به انفصالات پی در پی و جابجایی کاربران اشاره کرد. این ویژگی ها ابعاد جدیدی از امنیت را مطرح می کنند. آن ها منجر به تأخیر در دسترسی کاربر به داده های درخواستی و در نتیجه تغییر در شرایط دسترسی کاربر به آن داده ها می شوند. بنابراین، مکانیسم های کنترل دسترسی می بایست این تغییرات را به صورت پویا و انعطاف پذیر پوشش دهند. اما، روش هایی که در حال حاضر در این حیطه به کار می روند نتوانسته اند به طور کامل با این محدودیت ها و ویژگی ها سازگار شوند.

در این پروژه روشی ارائه می دهیم که با بهره گیری توأمان از عامل های متحرک و شکلی از کنترل دسترسی مبتنی بر نقش در قالب لیست های قابلیت، شیوه ای از دسترسی پویا، انعطاف پذیر و مطمئن به پایگاه های داده متحرک را فراهم می سازد. روش پیشنهادی با بهره گیری از خاصیت تحرک پذیری عامل ها، تأثیر انفصالات پی در پی و جابجایی وسایل متحرک و تأخیر ناشی از آن ها را نیز تعدیل کرده است.

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

فهرست مطالب

صفحه

عنوان

فصل اول: مقدمه

۱ ۱-۱ مقدمه	
۴ ۲-۱ اهداف تحقیق	
۵ ۳-۱ ساختار پروژه	

فصل دوم: مفاهیم کلی امنیت

۶ ۱-۲ مقدمه	
۷ ۲-۲ نیازمندی‌های یک محیط امن	
۷ ۱-۲-۲ محرمانگی داده‌ها	
۸ ۲-۲-۲ جامعیت داده‌ها	
۸ ۳-۲-۲ در دسترس بودن	
۹ ۳-۲ ساخت یک محیط امن	
۹ ۱-۳-۲ تهدیدات و تهاجم‌ها	
۱۰ ۱-۱-۳-۲ تهدیدات فیزیکی و تهدیدات منطقی	
۱۱ ۲-۱-۳-۲ تهدیدات عمدی و تهدیدات غیر عمدی	
۱۱ ۳-۱-۳-۲ گروه بندی تهدیدات بر اساس هدف اصلی هجوم	
۱۱ ۴-۱-۳-۲ فعال یا گذرا	
۱۱ ۵-۱-۳-۲ کلاس بندی SHIREY	
۱۲ ۲-۳-۲ مروری بر برخی روش های هجوم	
۱۲ ۱-۲-۳-۲ تجسس مخفیانه	
۱۲ ۲-۲-۳-۲ تغییرات (جزئی و یا کلی)	
۱۳ ۳-۲-۳-۲ کلاهبرداری یا بالماسکه	
۱۳ ۴-۲-۳-۲ انکار اصل موضوع	
۱۳ ۵-۲-۳-۲ تخریب نرم افزار و سرریز بافر	
۱۳ ۶-۲-۳-۲ حمله یا پاسخ	
۱۴ Wardialing ۷-۲-۳-۲	

عنوان

صفحه

۱۴	۸-۲-۳-۲ مهندسی اجتماعی.....
۱۴	۹-۲-۳-۲ تاخیر.....
۱۴	۱۰-۲-۳-۲ انکار خدمت/ انکار خدمت توزیع شده.....
۱۵	۱۱-۲-۳-۲ حمله به رمزهای عبور.....
۱۵	۱۲-۲-۳-۲ هجوم کدهای بدخواه.....
۱۵	۱۳-۲-۳-۲ در پشتی.....
۱۶	۳-۳-۲ سیاست امنیتی.....
۱۷	۴-۳-۲ مکانیسم امنیتی.....
۱۸	۴-۲ کنترل دسترسی.....
۱۹	۱-۴-۲ شناسایی و احراز اصالت.....
۲۱	۱-۱-۴-۲ Kerberos.....
۲۳	۲-۱-۴-۲ پروتکل احراز اصالت مجادله‌ای.....
۲۳	۳-۱-۴-۲ گواهی‌ها.....
۲۴	۴-۱-۴-۲ نام کاربری و کلمه عبور.....
۲۴	۵-۱-۴-۲ نشانه‌ها.....
۲۵	۶-۱-۴-۲ احراز اصالت چند عاملی.....
۲۵	۷-۱-۴-۲ احراز اصالت متقابل.....
۲۶	۸-۱-۴-۲ مقیاس‌های بیولوژیکی.....
۲۶	۲-۴-۲ مجوزدهی.....
۲۷	۳-۴-۲ بازرسی و رسیدگی.....
۲۷	۴-۴-۲ تکنیک‌های کنترل دسترسی.....
۲۸	۱-۴-۴-۲ کنترل دسترسی اجباری.....
۲۸	۱-۱-۴-۴-۲ کنترل دسترسی BLP.....
۲۹	۲-۱-۴-۴-۲ مدل Biba.....
۳۱	۲-۴-۴-۲ کنترل دسترسی تشخیصی.....
۳۱	۱-۲-۴-۴-۲ ماتریس کنترلی دسترسی.....
۳۳	۲-۲-۴-۴-۲ لیست‌های کنترلی دسترسی.....

عنوان

صفحه

۳۴	لیست‌های قابلیت ۳-۲-۴-۴-۲
۳۴	لیست‌های کنترل دسترسی تکثیر شده ۴-۲-۴-۴-۲
۳۵	مدل HRU ۵-۲-۴-۴-۲
۳۶	مدل قفل‌ها و کلیدها ۶-۲-۴-۴-۲
۳۷	کنترل دسترسی مبتنی بر حلقه ۷-۲-۴-۴-۲
۳۸	کنترل دسترسی مبتنی بر خصوصیات ۸-۲-۴-۴-۲
۳۹	مدل دیوارچین ۹-۲-۴-۴-۲
۴۱	کنترل دسترسی مبتنی بر نقش ۳-۴-۴-۲
۴۶	جمع‌بندی ۵-۲

فصل سوم: پایگاه‌های داده متحرک

۴۷	۱-۳ مقدمه
۴۹	۲-۳ محاسبات متحرک
۵۰	۱-۲-۳ معماری یک سیستم متحرک
۵۱	۲-۲-۳ تکنولوژی‌های پایه در ارتباطات بی‌سیم
۵۳	۳-۲-۳ انواع تحرک‌پذیری
۵۳	۴-۲-۳ محدودیت‌های تحرک‌پذیری
۵۴	۱-۴-۲-۳ سرعت پایین ارتباطات
۵۴	۲-۴-۲-۳ ناهمگونی و عدم یکنواختی سرعت ارتباطات
۵۴	۳-۴-۲-۳ پویایی توپولوژی شبکه
۵۴	۴-۴-۲-۳ انفصال‌های پی در پی شبکه
۵۴	۵-۴-۲-۳ مخاطرات ذاتی
۵۴	۶-۴-۲-۳ منابع محدود
۵۵	۷-۴-۲-۳ عمر باتری محدود
۵۵	۸-۴-۲-۳ صفحه نمایش کوچک
۵۵	۹-۴-۲-۳ مقیاس‌پذیری
۵۵	۱۰-۴-۲-۳ تنش
۵۶	۱۱-۴-۲-۳ شفافیت تحرک‌پذیری برای کاربران

۵۶	۳-۲-۴-۱۲ کپی‌شدگی و کش‌شدگی داده‌ها
۵۶	۳-۳ پایگاه‌های داده توزیع‌شده
۵۸	۳-۴ پایگاه‌های داده متحرک
۵۹	۳-۴-۱ معماری پایگاه داده متحرک
۶۲	۳-۴-۲ مدهای عملیاتی یک واحد متحرک در یک پایگاه داده متحرک
۶۳	۳-۵ مسائل جدید در پایگاه‌های داده متحرک
۶۴	۳-۶ جمع‌بندی

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

۶۶	۴-۱ مقدمه
۶۷	۴-۲ نیازمندی‌های امنیتی در محیط‌های متحرک
۶۹	۴-۳ هنر ایمن‌سازی سیستم متحرک
۷۱	۴-۴ مروری بر روش‌های کنترل دسترسی در پایگاه‌های داده توزیع‌شده
۷۲	۴-۴-۱ احراز اصالت
۷۴	۴-۴-۱-۱ RADIUS
۷۶	۴-۴-۲-۱ خانواده سرویس‌دهنده‌های احراز اصالت TACACS
۷۷	۴-۴-۳-۱ SPX
۷۸	۴-۴-۲ مجوزدهی
۸۲	۴-۵ روش‌های کنترل دسترسی در پایگاه‌های داده متحرک
۸۲	۴-۵-۱ مدل شمای مختصر توسعه یافته
۸۴	۴-۵-۲ سازگاری امنیتی
۸۶	۴-۶ جمع‌بندی

فصل پنجم: روش پیشنهادی

۸۸	۵-۱ مقدمه
۹۱	۵-۲ نمادهای مورد استفاده
۹۳	۵-۳ تعریف مسئله
۹۴	۵-۴ شناسایی و احراز اصالت متقابل

۹۷	۵-۵ مدیریت جابجایی
۹۸	۶-۵ مقدماتی بر مکانیسم پیشنهادی
۱۰۱	۱-۶-۵ ساختار لیست قابلیت
۱۰۳	۲-۶-۵ آغازسازی لیست قابلیت
۱۰۵	۳-۶-۵ مدیریت تغییرات
۱۰۸	۴-۶-۵ بررسی مجوزها در سرور محلی
۱۰۸	۵-۶-۵ بررسی و جمع‌بندی روش ارائه شده
۱۰۹	۷-۵ کنترل دسترسی مبتنی بر عامل‌های متحرک
۱۱۰	۱-۷-۵ مروری بر عامل‌های متحرک
۱۱۱	۲-۷-۵ ارائه مدلی براساس عامل‌های متحرک
۱۱۲	۱-۲-۷-۵ گام اول: آغازسازی و نصب اولیه واحد متحرک
۱۱۴	۲-۲-۷-۵ گام دوم: آغاز به کار وسیله متحرک
۱۱۵	۳-۲-۷-۵ گام سوم: اجرای یک پرس‌وجو
۱۱۶	۴-۲-۷-۵ گام چهارم: پردازش پرس‌وجو و بررسی مجوزها در سرور محلی
۱۱۸	۵-۲-۷-۵ گام پنجم: مدیریت جابجایی وسیله متحرک
۱۲۰	۶-۲-۷-۵ گام ششم: بازگشت و تحویل نتایج به واحد متحرک
۱۲۱	۸-۵ جمع‌بندی

فصل ششم: ارزیابی روش پیشنهادی

۱۲۲	۱-۶ مقدمه
۱۲۳	۲-۶ ارزیابی میزان پوشش ویژگی‌های خاص سیستم‌های متحرک
۱۲۳	۱-۲-۶ انفصالات پی‌درپی
۱۲۴	۲-۲-۶ جابجایی و حرکت
۱۲۴	۳-۲-۶ زمینه‌ها
۱۲۵	۴-۲-۶ راهبری و مقیاس‌پذیری
۱۲۵	۵-۲-۶ محدودیت‌های قدرت
۱۲۶	۶-۲-۶ محدودیت‌های حافظه
۱۲۶	۷-۲-۶ محدودیت‌های پهنای باند و سرعت ارتباطات

عنوان

صفحه

۱۲۶	۸-۲-۶ شفافیت در دسترسی
۱۲۷	۹-۲-۶ سایر موارد
۱۲۸	۳-۶ ارزیابی موفقیت سیستم در نیل به اهداف تعیین شده
۱۲۹	۴-۶ بررسی امنیتی پروتکل‌ها
۱۳۱	۱-۴-۶ بررسی امنیتی عامل‌ها
۱۳۳	۲-۴-۶ بررسی امنیتی لیست‌های قابلیت
۱۳۳	۵-۶ ارزیابی روش پیشنهادی از لحاظ کارایی و عملکرد
۱۳۶	۱-۵-۶ گام اول: آغازسازی و نصب اولیه واحد متحرک
۱۳۸	۲-۵-۶ گام دوم: آغاز به کار وسیله متحرک
۱۳۹	۳-۵-۶ گام سوم: اجرای یک پرس‌وجو
۱۳۹	۴-۵-۶ گام چهارم: پردازش پرس‌وجو و بررسی مجوزها در سرور محلی
۱۴۰	۵-۵-۶ گام پنجم: مدیریت جابجایی وسیله متحرک
۱۴۰	۶-۵-۶ گام ششم: تحویل نتایج به واحد متحرک
۱۴۱	۷-۵-۶ نتایج بررسی گام به گام
۱۴۳	۶-۶ تحلیل اندازه لیست‌های قابلیت
۱۴۶	۱-۶-۶ بهبود در کاربری لیست‌های قابلیت
۱۵۰	۷-۶ نقاط ضعف و چالش‌ها
۱۵۰	۸-۶ کارهای مرتبط
۱۵۱	۹-۶ جمع‌بندی

فصل هفتم: جمع‌بندی و کارهای مرتبط در آینده

۱۵۲	۱-۷ مقدمه
۱۵۲	۲-۷ مروری بر مطالب
۱۵۴	۳-۷ راهکارهای آینده
۱۵۶	منابع و مآخذ

فهرست شکل‌ها

صفحه	عنوان
۲۲	شکل ۱-۲ مسیر شناسایی برای دسترسی در حوزه Kerberos
۲۲	شکل ۲-۲ دسترسی به منبع در حوزه Kerberos
۳۰	شکل ۳-۲ مقایسه مدل Biba و BLP
۳۲	شکل ۴-۲ نمونه‌ای از ماتریس کنترل دسترسی
۳۳	شکل ۵-۲ لیست‌های کنترل دسترسی مربوط به ماتریس شکل ۴-۲
۳۳	شکل ۶-۲ لیست قابلیت مربوط به فاعل‌های رضا، علی، و پیام از ماتریس دسترسی شکل ۴-۲
۳۷	شکل ۷-۲ مدل کنترل دسترسی مبتنی بر حلقه و نحوه افزایش امتیازها
۳۹	شکل ۸-۲ نمونه‌ای از معماری سه سطحی اشیاء در مدل دیوار چین
۴۰	شکل ۹-۲ نحوه اعمال قانون خواندن در مدل دیوار چین
۴۰	شکل ۱۰-۲ نحوه اعمال قانون نوشتن در مدل دیوار چین
۴۲	شکل ۱۱-۲ انتساب‌های اجازه‌ها بین مولفه‌های مدل Core RBAC
۴۸	شکل ۱-۳ حجم تبادل داده‌ها در فاصله ۲۰۰۳ تا ۲۰۰۸ با تفکیک روش
۵۱	شکل ۲-۳ معماری شبکه بی سیم
۵۷	شکل ۳-۳ شمایی از یک سیستم پایگاه‌داده توزیع شده
۵۸	شکل ۴-۳ شمای کلی یک پایگاه داده متحرک
۶۰	شکل ۵-۳ معماری یک پایگاه داده متحرک
۶۰	شکل ۶-۳ معماری کلاینت سرور در سیستم پایگاه داده متحرک
۶۱	شکل ۷-۳ معماری C-SA-S
۶۱	شکل ۸-۳ معماری C-CA-S
۶۱	شکل ۹-۳ معماری C-I-S
۶۳	شکل ۱۰-۳ مدهای عملیاتی یک واحد متحرک
۷۳	شکل ۱-۴ استفاده از سرورهای خارجی در احراز اصالت
۷۶	شکل ۲-۴ جریان ترافیک در احراز اصالت دسترسی با RADIUS
۸۰	شکل ۲-۴ مفاهیم منطقی سیاست راهبری در محیط یک سازمان چند دامنه‌ای
۸۱	شکل ۴-۴ معماری SSM
۸۳	شکل ۳-۴ شمای مختصر توسعه یافته با استفاده از عامل‌های متحرک

عنوان

صفحه

شکل ۴-۶	میانجی‌گری در دسترسی به وسیله مولفه سازگاری	۸۵
شکل ۵-۱	فضای مسئله	۹۳
شکل ۵-۲	شمایی از فرایند کنترل دسترسی	۹۴
شکل ۵-۳	فرایند کلی عمل احراز اصالت	۹۵
شکل ۵-۴	ساختارهای اصلی مراجع اعتباردهی	۹۶
شکل ۵-۵	مکانیسم ساده برای مدیریت جابجایی	۹۸
شکل ۵-۶	یک لیست قابلیت با سه نقش	۱۰۳
شکل ۵-۷	شمای کلی مرحله آغازسازی	۱۰۴
شکل ۵-۸	پروتکل آغازسازی سیستم مدیریت نقش‌ها و مجوزها	۱۰۵
شکل ۵-۹	مدیریت تغییرات و به روز رسانی لیست قابلیت	۱۰۶
شکل ۵-۱۰	پروتکل به‌روزرسانی لیست‌های قابلیت و مدیریت تغییرات	۱۰۷
شکل ۵-۱۱	پروتکل مجوزدهی در سرور محلی	۱۰۸
شکل ۵-۱۲	شمای کلی مدل کنترل دسترسی مبتنی بر عامل	۱۱۱
شکل ۵-۱	شمای کلی گام آغازسازی	۱۱۳
شکل ۵-۲	پروتکل آغازسازی مبتنی بر عامل	۱۱۳
شکل ۵-۳	شمای کلی یک واحد متحرک پس از آغازسازی	۱۱۳
شکل ۵-۴	رول اجرای یک پرس‌وجو در یک واحد متحرک	۱۱۵
شکل ۵-۵	پروتکل اجرای یک پرس‌وجو در یک واحد متحرک	۱۱۶
شکل ۵-۶	عامل پرس‌وجو	۱۱۶
شکل ۵-۷	مذاکرات عامل پرس‌وجو و عامل سرور محلی در سرور محلی	۱۱۷
شکل ۵-۲۰	پرازش پرس‌وجو	۱۱۸
شکل ۵-۸	مدیریت جابجایی در دسترسی مبتنی بر عامل	۱۱۹
شکل ۵-۹	پروتکل بازگشت به واحد متحرک	۱۲۰
شکل ۶-۱	لیست قابلیت شکل ۵-۶ بخش‌بندی شده براساس زمینه مکان	۱۴۷
شکل ۶-۲	درخت بخش‌بندی لیست قابلیت	۱۴۸
شکل ۶-۳	درخت بخش‌بندی شکل ۶-۱	۱۴۹

فهرست جدول‌ها

صفحه	عنوان
۹۱	جدول ۱-۵ نمادهای مورد استفاده
۱۳۹	جدول ۲-۶ پیچیدگی زمانی وظایف یک عامل پرس‌وجو در گام چهارم
۱۴۰	جدول ۳-۶ پیچیدگی زمانی وظایف یک عامل سرور محلی در گام چهارم
۱۴۴	جدول ۴-۶ نمونه‌ای از شکل دسترسی کاربران به پایگاه‌های داده

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 ۲.۴ بیلیون در سال ۲۰۰۶ 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 امنیتی 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

اعمال 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 توزیع شده که خاصیت تحرک پذیری به آن افزوده شده است. یک شبکه بی‌سیم مجموعه‌ای 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) تحرک پذیری دستگاه‌ها

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

(۳) احتمال بسیار زیاد انفصال دستگاه‌های متحرک

(۴) محدودیت‌های پردازش، منابع و قدرت، و در نتیجه قدرت محاسباتی و حجم ذخیره‌سازی محدود

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

(۶) وجود کپی‌های چندگانه از داده‌ها در دستگاه‌های مختلف

چهار ویژگی اول خاص پایگاه‌های داده متحرک و دو ویژگی آخر، از ویژگی‌های پایگاه‌های 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 تحرک پذیری 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 شتود و سرقت اطلاعات در حین انتقال بسیار بالاست.

- ۴) با وجود انفصال‌های متناوب، وسیله متحرک باید بدون وقفه و اشکال، عملکرد خود را انجام دهد.
- ۵) 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.
- ۶) گم شدن واحدهای متحرک ممکن است سبب از دست دادن محرمانگی داده‌ها شود.
- ۷) با توجه به هزینه بالای ارتباطات و محدودیت حافظه در وسایل متحرک، مدل‌های کنترل دسترسی باید تا حد امکان کوچک باشند.
- ۸) با توجه به محدودیت منابع در وسایل متحرک، پردازش‌ها می‌بایست سبک باشند.
- ۹) 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 پایگاه‌های داده متحرک هستیم تا نیازها و ویژگی‌های خاص این سیستم‌ها را پوشش دهد. در این نوع از شبکه‌ها، 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، کار کردن بدون وقفه و به طور مستقل است که عامل‌ها با خاصیت خودکاری و استقلالشان می‌توانند برای این منظور ابزاری مناسب باشند. از طرفی عامل‌ها می‌توانند 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 عامل‌ها برای کنترل دسترسی بهره می‌بریم. هر کاربر برای انجام عملیات، عاملی تولید می‌کند، کارها را به او می‌سپارد و او را به سمت سرور (فراهم‌کننده خدمات موردنظر) می‌فرستد. عامل حتی در صورت انفصال تولیدکننده‌اش، به کار خود ادامه می‌دهد و پس از اتمام عملیات، منتظر اتصال تولیدکننده‌اش می‌شود، سپس به خانه بازمی‌گردد و نتایج را گزارش می‌دهد.

کارهای زیادی در زمینه امنیت در پایگاه‌های داده متمرکز انجام گرفته که از آن جمله می‌توان به مدل مبتنی بر هویت، مدل مبتنی بر نقش، مدل مبتنی بر قابلیت، 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 توزیع شده، 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، پرس و جوی 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 پوشانند.
- 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.