باسمه تعالي

مدارگسترش فناوری اطلاعات

سیستم جامع مدیریت امنیت و کنترل دسترسی (پارسبان)

ITO-SACM

شماره تلفن: ۸۸۹۷۶۲۹۹ (سه خط) **شماره فکس: ۸۸۹۷۶۲۹۸**

وب‌سایت شرکت: http://www.ITOrbit.net

نشاني پست الكترونيكي شركت: info@ITOrbit.net

تعداد صفحات: ۷

تاریخ بروزرساني: ۱۳۸۶/۰۶/۰۱ **کد شناسه ITO.GEN.ACM.01**

این سند جهت معرفي سیستم جامع مدیریت امنیت و کنترل دسترسی و استفاده عمومي تهیه شده است. حفظ حقوق مطالب درج شده الزامیست.

پارسبان

امروزه امنيت سيستم‌هاي جامع نرم‌افزاري مانند امنيت قلعه‌هاي عظيم قديم است، بسيار مشكل و پر هزينه. معمولا پس از ساختن قلعه به اين نتيجه مي‌رسيدند كه اين قلعه امنيت مي‌خواهد و هزاران نگهبان لازم دارد تا ورودي‌ها و خروجي‌ها را كنترل كند و صدها نفر لازم است تا اين نگهبان‌ها را مديريت كند. طراحي اين نظام امنيتي بر عهده كارشناساني بود كه گوشه گوشه قلعه را بشناسند تا كوچكترين راه‌هاي نفوذ هم كنترل شود. اين شهرها در امنيت چنين حصاري در ايمني كامل بودند. نرم‌افزارها هم دقيقا قلعه‌هايي هستند با حفره‌هاي فراوان كه روزانه هزاران نفر تمايل دسترسي به اطلاعات موجود در آن‌را دارند، بديهي است كه اين دسترسي نياز به كنترل و مديريت دقيق دارد.

سيستم مديريت امنيت و كنترل دسترسي مدار تمامي نيازهاي امنيتي يک سيستم را تامين مي‌كند و نرم‌افزار را در حصار امنيتي پارسبان قرار مي‌دهد.

اساس کار پارسبان:

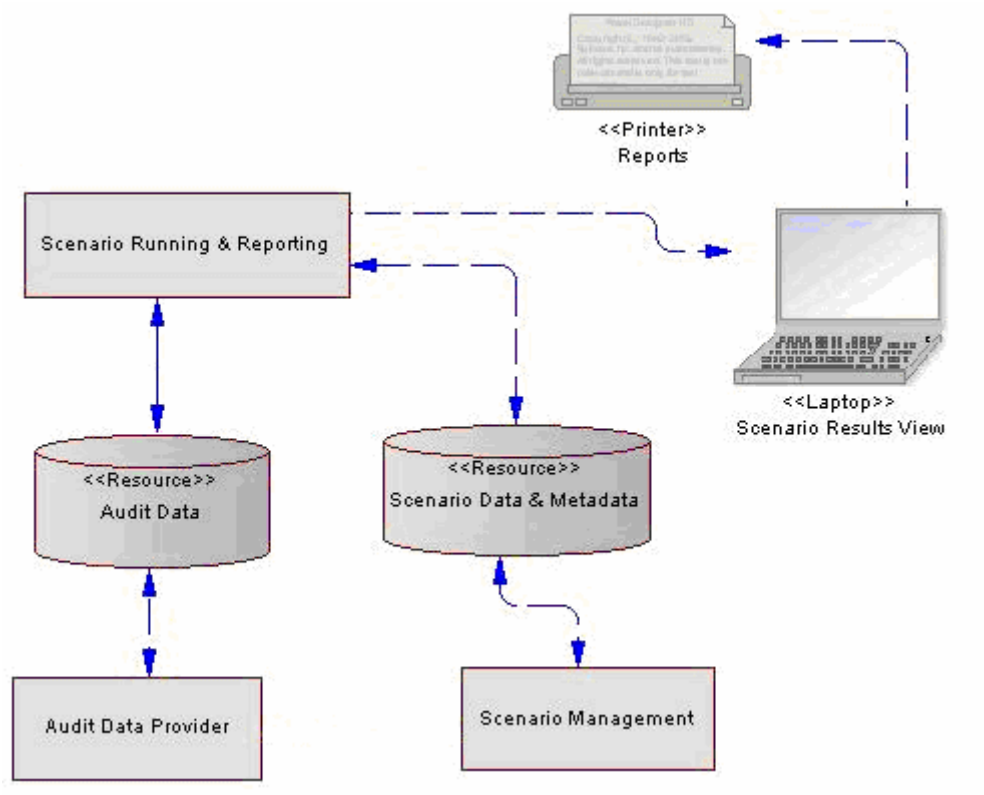
۱. **هويت شناسي**: هويت شناسی مسئول تصديق هويت كاربران را براي ورود به برنامه‌هاي كاربردي سيستم‌ها براساس شناسه كاربري و كلمه عبور تعيين‌شده است. از آنجا كه شيوه‌های بسيار زيادی مانند روش‌های بايومتريک برای تصديق هويت كاربران وجود دارد پارسبان امكان خاص ملحق‌شدن به اين روش‌ها را به سادگی فراهم می‌كند.

۲. **مجاز شناسي**: مجاز شناسي پارسبان بسته به معماري سيستم و بستر نرم‌افزاري آن در برخي موارد به صورت دستي و در برخي ديگر به شكل اتوماتيک صورت مي‌گيرد. با كنترل دسترسي كاربران به موجوديت‌ها در تمامي لايه‌هاي نرم‌افزار از پايگاه داده گرفته تا لايه واسط كاربري، ديگر ذره‌اي نگراني باقی نخواهد ماند.

۳. **نظارت و لاگ**: پارسبان تمام تلاش‌ها و عمليات‌هاي صورت گرفته در بخش‌هاي هويت‌شناسي، مجاز شناسي و راهبري امنيت را ثبت مي‌كند و هيچ عملي از چشم‌هاي نظارت و لاگ پارسبان پنهان نمي‌ماند.

كليه حقوق اين سند متعلق به شركت مدار گسترش فناوری اطلاعات است.

٤. **تحليل رويدادها**: براي بررسي رفتارهاي كاربران و رويدادهاي امنيتي، امكان تعريف سناريوهايي از رفتارهاي مشكوک و اجراي اين سناريوها به صورت دستي و يا به صورت زمان‌بندي شده و اتوماتيک وجود دارد. همچنين انباره اوليه قدرتمندی از رفتارهای مشکوک شناسایی شده به‌صورت پیش‌فرض در سیستم قرار گرفته است.



شماي كلي تحليل كننده رويدادها

٥. **نيازمندي‌هاي گروه نظارت**: هدف گروه نظارت در پارسبان، نظارت بر کار تمامی کاربران و راهبران سیستم می‌باشد. کاربران این دسته، مي‌توانند تمامي لاگهاي ثبت شده از عمليات کاربران را در حالی بررسي نمایند که اثری از رد پای‌شان بر روی سیستم باقی نماند.

٦. **كنترل دسترسي براي جزء به جزء(ريزدانه) اطلاعات**: تعجب نكنيد ! پارسبان دسترسي‌ها را در سطح سطرهاي اطلاعات هم كنترل مي‌كند، حتي بدون نياز به كنترل و دسترسي‌هاي پايگاه‌هاي داده كه مشكلات خاص خود را دارد. پارسبان اين مهم را به سادگي انجام مي‌دهد.

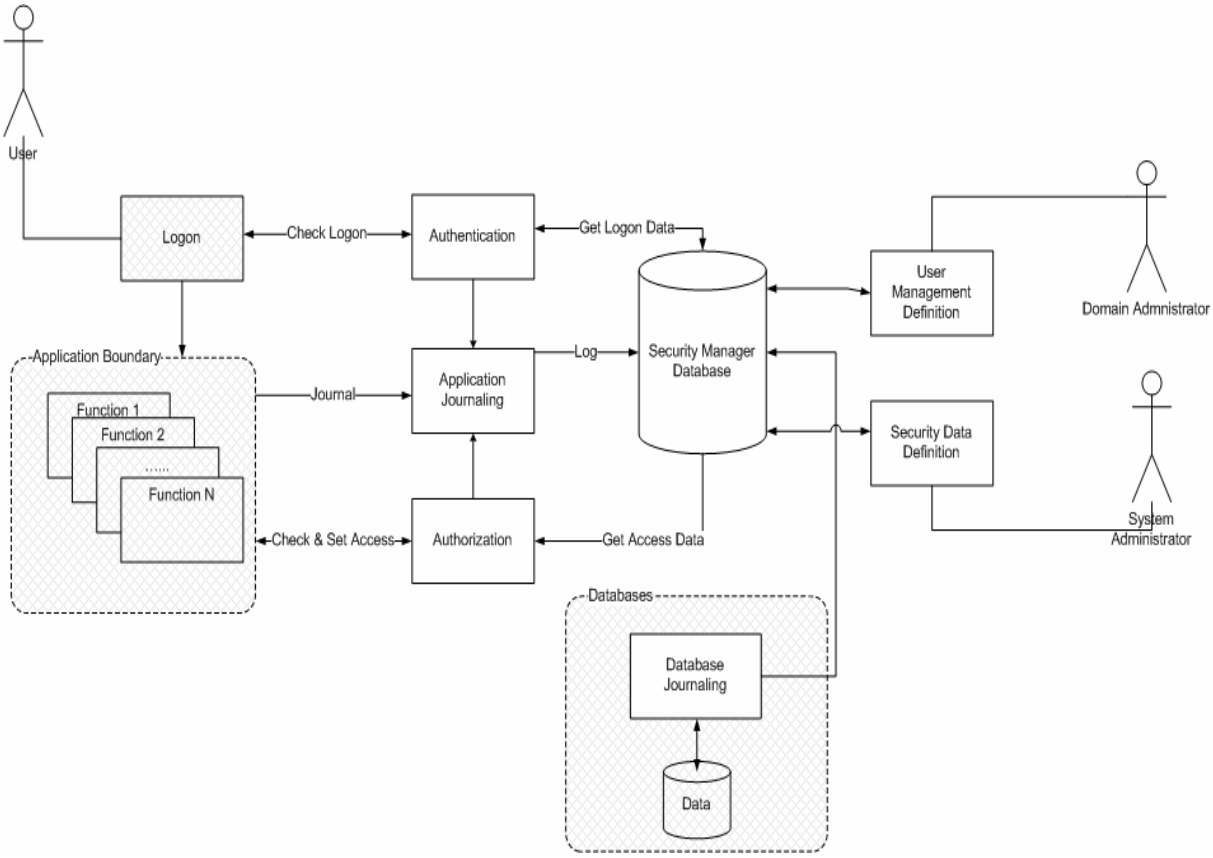
كليه حقوق اين سند متعلق به شركت مدار گسترش فناوری اطلاعات است.

۷. نرمافزار راهبري پارسبان:

- تعریف و ویرایش دامنه‌ها که می‌توانند هرگونه تقسیم‌بندی منطقی دلخواهی از سازمان باشند
- تعریف و ویرایش برنامه‌های کاربردي یکپارچه شده
- تخصیص هر سیستم به یك یا چند دامنه
- تعریف موجودیت‌هایی از سیستم که در تمامی سطوح کاربری (از لایه واسط کاربر گرفته تا پایگاه داده) باید امنیت در موردشان اعمال شود.
- تعریف روابط پدر- فرزندي (سلسله مراتبي) برای موجودیت‌هایي که در دل موجودیت‌هاي دیگر هستند، مانند منو و زیرمنو
- تعریف محدوده‌ها، بر روی جداول بانک اطلاعاتی، به منظور کنترل دسترسی رکوردهای خاص
- تعریف و ویرایش نقش‌هاي مختلف برای هر سیستم
- تعریف و ویرایش حقوق دسترسی نقش‌ها در کارکرد با سیستم‌ها (دسترسي به جداول بانك اطلاعاتي، فرم‌ها و اجزاي داخلي آن، منوها و دیگر موجودیت‌ها و محدوده‌ها)
- تخصیص حقوق دسترسي یك نقش به سایر نقش‌ها از طریق اعطای مجوز یک نقش به نقش دیگر که می‌تواند سلسله مراتبی هم باشد
- تعریف تداخل ایستا و پویا بین نقش‌ها
- تعریف و ویرایش کاربران و مدیریت آنها
- انتساب کاربران به دامنه‌ها
- تنظیم پارامترهای امنیتی دامنه‌ها
- انتساب نقش‌ها به کاربران به منظور تعیین مجوزهاي دسترسي کاربر به موجودیت‌ها یا محدوده‌های تعریف شده
- تعریف و ویرایش محدودیت‌هاي زماني و مکاني ورود کاربر به سیستم‌های کاربردي
- تعریف سناریوها براي بررسي عملیات صورت گرفته در سیستم
- تعریف برنامه زمان‌بندي برای اجراي سناریوها

کلیه حقوق این سند متعلق به شرکت مدار گسترش فناوری اطلاعات است.

نمودار بلوكي سيستم مديريت كنترل دسترسي :



استانداردهاي پياده سازي شده در پارسبان

۱. استاندارد RBAC[1]

استاندارد كنترل دسترسي بر مبناي نقش (RBAC) معتبرترين و مهمترين استاندارد در حوزه كنترل دسترسي است. از اصول و توصيه‌هاي مهم اين استاندارد كه در اكثر سيستم‌هاي مشابه مهجور مانده‌اند، مي‌توان به اصل حداقل مجوز، جداسازي وظايف ايستا و پويا، طبقه‌بندي سلسله مراتبي نقش‌ها و همچنين مفهوم مهم نشست كاري اشاره نمود كه همگي در سيستم پارسبان به صورت كامل پياده سازي شده است.

كليه حقوق اين سند متعلق به شركت مدار گسترش فناوری اطلاعات است.

۲. استاندارد BLP

استاندارد BLP يكي از معتبرترين استانداردهاي جهاني در زمينه طبقه‌بندي چند سطحي اطلاعات و اسناد به سطوحي مانند عادي، محرمانه و سري است. اين روش براي حفاظت اسناد و اطلاعات از نامحرمان كاربرد بسيار دارد، در حالی که در بسياري از سيستمها برای پوشش اين نياز، بسيار ساده انگارانه برخورد مي‌شود و موجب بروز نشت اطلاعات می‌گردد، استاندارد BLP براي حفظ محرمانگي اطلاعات راه‌كارهايي را ارائه ميدهد. اين استاندارد و همچنين توسعه‌اي از آن كه به جامعيت اطلاعات ناظر است نيز به صورت كامل در پارسبان پياده‌سازي شده است.

شناسنامه فني قسمتهاي گوناگون سيستم مديريت كنترل دسترسي پارسبان:

ITO- SACM Technical Specification	
سيستم راهبري امنيت و كنترل دسترسي– **نسخه Desktop**	
محيط اجراي برنامه : Windows به همراه NET framework 1.1. مستندات همراه : راهنمای كامل و مصور توسعه‌دهندگان و كاربران	
سيستم راهبري امنيت و كنترل دسترسي – **نسخه Web**	
محيط اجراي برنامه : J2EE Application Server مستندات همراه : راهنمای كامل و مصور توسعه‌دهندگان و كاربران	
سرويس‌هاي كنترل دسترسي	
محيط كارفرما/كارگزار	زبان برنامه‌نويسي : PL/SQL محيط مورد نياز براي اجراي برنامه :يک سرور Oracle يا SQL-Server مستندات همراه : راهنمای كامل و مصور توسعه‌دهندگان و كاربران
محيط NET.	زبان برنامه‌نويسي : C# محيط مورد نياز براي اجراي برنامه : Windows به همراه NET framework 1.1. مستندات همراه : راهنمای كامل و مصور توسعه‌دهندگان و كاربران
محيط چند لايه J2EE	زبان برنامه‌نويسي : Java محيط مورد نياز براي اجراي برنامه : يک J2EE Application Server مستندات همراه : راهنمای كامل و مصور توسعه‌دهندگان و كاربران

كليه حقوق اين سند متعلق به شركت مدار گسترش فناوری اطلاعات است.

نمونه سیستم‌های موفقی که با پارسبان یکپارچه‌سازی شده‌اند:

- سیستم راهبري سیستم مدیریت کنترل دسترسي: برنامه تحت وب در محیط **J2EE** ، با پایگاه داده اوراکل.
- سیستم آموزش دانشگاه تهران : برنامه تحت وب یکپارچه‌سازی شده در محیط **J2EE** ، با پایگاه داده اوراکل.
- سیستم شماره گذاري خودرو ناجا: برنامه تحت وب یکپارچه‌سازی شده در محیط **J2EE** ، با پایگاه داده اوراکل.
- سیستم **ERP** سایپا: برنامه‌ای با معماري خادم/مخدوم، در محیط اوراکل.
- سیستم‌هاي اطلاعات مدیریت شرکت مدار: مجموعه نرم‌افزار تحت وب، یکپارچه‌سازی شده در محیط **.NET** ، با پایگاه داده **SQL Server** .
- سیستم بودجه‌بندی و بهاي تمام شده بیمارستاني مدار: برنامه خادم/مخدوم یکپارچه‌سازی شده در محیط **.NET** ، با پایگاه داده **SQL Server** .

کلیه حقوق این سند متعلق به شرکت مدار گسترش فناوری اطلاعات است.