



Secure File Server Engine

اولین و تنها فایل سرور امن مستقل از سیستم عامل در کشور

دارای تاییدیه فنی از شورای عالی انفورماتیک کشور و ثبت مالکیت در مرکز توسعه فناوری رسانه های دیجیتال

« سامانه فایل سرور »



مقدمه

سامانه جامع رسان تنها فایل سرور هوشمند کاملاً بومی در کشور می باشد که در سه بخش زیر کاملاً مستقل از سیستم عامل طراحی شده است:

۱. مدیریت تعریف سطوح دسترسی به منابع
۲. پروتکل احراز هویت
۳. پروتکل ارسال و دریافت فایل

سامانه جامع رسان برای اولین بار موفق به پیاده سازی یک سیستم تعیین سطوح دسترسی هوشمند به منابع , با ویژگی های فوق العاده گشته تا کار پیاده سازی سناریو های پیچیده برای فایل سرور را به امری کاملاً آسان تبدیل کند.

استفاده از پروتکل احراز هویت بومی و عدم استفاده از پروتکل های رایج انتقال فایل نظیر **File FTP, Sharing** و پروتکل های مبتنی بر سرویس دهنده های بانک های اطلاعاتی , امنیت این سامانه را بعنوان یک فایل سرور بومی در حد بسیار بالایی قرار داده است.

یکی از دیگر ویژگی های منحصر به فرد این سامانه توانایی پیاده سازی یک معماری نوین در عرصه سیستم های جلوگیری از نشت اطلاعات می باشد.

سامانه جامع رسان دارای فایل سرور بومی خاص خود می باشد به نحوی که از هیچ پروتکل شناخته شده رایج که توسط فایل سرورهای معروف دنیا استفاده می شود کمک نمی گیرد، و این ویژگی منحصر به فرد سامانه جامع رسان را قادر می سازد تا در مقابل انبوه تهدیدهای پروتکل های فایل سروهای معروف همچون **File Sharing و FTP** و .. در امان باشد.

در ضمن در طراحی پروتکل سامانه جامع رسان سعی گشته تا تمام موارد و نقایص امنیتی فایل سرورها معروف بر طرف گردیده تا یک پروتکل امن و بومی فایل سرور بوجود آید بنابراین در هنگام استفاده از سامانه جامع رسان شما می توانید تمام درایور های کارت شبکه خود را غیر فعال کرده و صرفاً با وجود درایور **TCP/IP** بر روی کارت شبکه خود از تمام امکانات فایل سرور و پیام رسان سامانه جامع رسان بهره مند شوید.

سامانه جامع رسان بعنوان یک فایل سرور کاملا بومی و امن که در سطح برنامه نویسی بصورت TCP/IP Port Programming طراحی و کد نویسی شده است، سامانه اهراز هویت این سیستم نیز از طراحی تا پیاده سازی بصورت کاملا بومی می باشد، بخش تعیین سطوح دسترسی سامانه جامع رسان که از شاهکارهای این سامانه می باشد امکان ایجاد انواع سناریو های پیچیده یک فایل سرور را به راحتی امکان پذیر کرده است.

سطوح دسترسی در سامانه جامع رسان

تعریف سطوح دسترسی در سامانه جامع رسان بر روی کاربران صورت می گیرد نه بر روی منابع و این ویژگی مهم باعث می شود تا برای منابعی که هنوز بوجود نیامده اند دسترسی تعریف کرد.

بر همین اساس یک سطح دسترسی باید در یکی از سه بخش زیر تعریف شود:

دسترسی عمومی: دسترسی تعریف شده در این بخش به کل کاربران اعمال می شود

دسترسی بر اساس نام قسمت: دسترسی تعریف شده در این بخش به کاربران قسمت تعیین شده اعمال می گردد

کاربر خاص: دسترسی تعریف شده در این حالت بر روی یک کاربر خاص اعمال می شود

انواع دسترسی در سامانه جامع رسان

تعریف دسترسی مستقیم به منابع هدف



سطح دسترسی	مسیر
RLDW	\ STORAGE\Doc\List\EDU >نام ریشه سامانه <

اگر دسترسی فوق را برای کاربری تعریف کنیم به این معنا است که کاربر به پوشه EDU دسترسی خواندن (R)، دیدن (L) محتویات، نوشتن (W) و پاک کردن (D) دارد. وقتی کاربر به سیستم وارد می شود با کلیک کردن بر روی نام ریشه سامانه از آنجا که یک دسترسی برای او در سه لایه پایین تر از نام ریشه وجود دارد سامانه بصورت هوشمند و پویا مسیر را برای رسیدن کاربر به پوشه باز می کند به این معنی که بصورت پویا و اتوماتیک به سه پوشه Storage و Doc و List دسترسی دیدن را داده تا کاربر به مقصد تعریف شده خود برسد سپس با رسیدن به پوشه EDU سامانه دسترسی تعریف شده RLDW را اعمال می کند. در

صورتی که در سیستم های سنتی می بایست دسترسی از بالاترین پوشه در تمام لایه ها بر روی هر پوشه اعمال شود تا کاربر به انتهای مسیر برسد.

ماشین زمان



تمام تغییرات در محتوای فایل ها که می تواند توسط کاربران مختلف بر روی یکی از منابع صورت پذیرد قابل بازگشت به عقب می باشد، بطور مثال در نظر بگیرید که یک منبع اطلاعاتی را بین چند کاربر به اشتراک گذاشته اید و کاربران مدام در حال تغییر محتوای منابع به اشتراک گذاشته شده می باشند ، اکنون با این ویژگی هر یک از کاربران می توانند فایل را که بارها تغییر کرده به حالت چند روز قبل برگردانند و یا می توانند بدانند که این فایل چند بار و در هر نوبت توسط چه کسی دچار چه تغییراتی شده و در صورت لزوم ، نسخه ای از فایل را که محتوای آن، قبل از تغییرات مورد نظر آنها می باشد را دریافت کنند .

تعریف دسترسی هوشمند در مسیر های عمومی



مسیر	سطح دسترسی
STORAGE\Doc*\EDU >نام ریشه <سامانه	RLDW

در این مورد کاربر با ورود به سامانه تا پوشه Doc هدایت می شود سپس کاربر در پوشه Doc تعدادی پوشه را می بیند اما از اینجا به بعد پوشه ای برای کاربر باز می شود که در آن پوشه EDU باشد.

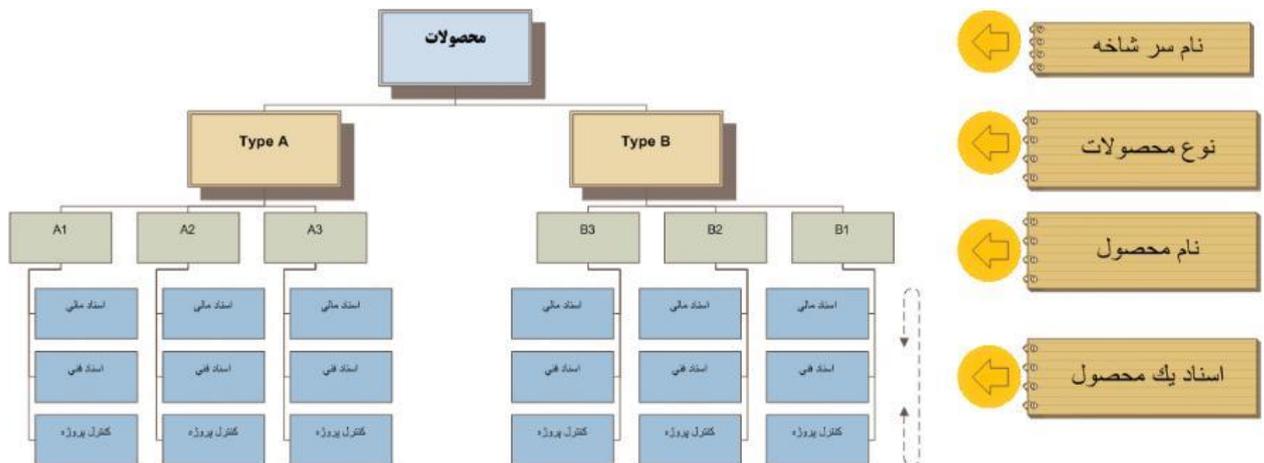
نکته ۱: می توان در مسیر از یک یا چند * استفاده کرد.

نکته ۲: کاربرد این روش در مواقعی است که یک ساختار ثابت از پوشه ها وجود دارد تا بتوان برای اعمال دسترسی به قسمتهای مختلف این ساختار از این روش استفاده کرد.

پیاده سازی یک سامانه آرشیو مستندات با این ویژگی



مطابق شکل زیر شرکتی را فرض کنید که دارای چنین طبقه بندی از نظر محصولات تولیدی خود می باشد.



اگر چارت فوق را بصورت ساختار پوشه ای در بیاوریم به بصورت زیر می توان ساختار فوق را در سامانه جامع رسان پیاده کرد ، اکنون می توان برای مسئولین مالی و فنی و کنترل پروژه دسترسی های زیر را تعریف کرد.

همانطور که مشاهده شد با تعریف سه دسترسی زیر، یک نظام دسترسی بر مبنای چارت تولیدات شرکت انجام شد، به این ترتیب که مسئولین هر بخش فارغ از نوع و نام محصول به بخش تخصصی خود دسترسی دارند و حتی با کم و زیاد شدن نوع یا تعداد محصولات شرکت نیاز به تعریف دسترسی مجدد نمی باشد.



مسیر	سطح دسترسی	کاربر
کنترل پروژه**\/محصولات\<نام ریشه سامانه>	RLDW	مدیر کنترل پروژه
مسیر	سطح دسترسی	کاربر
اسناد فنی**\/محصولات\<نام ریشه سامانه>	RLDW	مدیر فنی
مسیر	سطح دسترسی	کاربر
اسناد مالی**\/محصولات\<نام ریشه سامانه>	RLDW	مدیر مالی

تعریف دسترسی بر اساس نام کاربر



مسیر	سطح دسترسی
صندوق شخصی \ ؟ \ <نام ریشه سامانه>	RLDW

در سامانه جامع رسان بصورت پیش فرض هر کاربر در محل ریشه سامانه، یک پوشه به نام خود دارد که شامل ۴ زیر پوشه می شود:

- صندوق شخصی
- فایل های ارسالی
- فایل های دریافتی
- ورود و خروج از سازمان

بطور مثال اکنون برای اینکه برای هر کاربر دسترسی به پوشه صندوق شخصی را تعریف کنیم، دسترسی فوق را در قسمت دسترسی های عمومی (دسترسی که به تمام کاربران اعمال می شود) در صفحه مدیریت کاربران

که از طریق کنسول مدیریتی قابل اعمال است را وارد می کنیم , که در نتیجه بصورت اتوماتیک بجای علامت ؟ نام کاربری که اکنون به سیستم وارد شده قرار می گیرد و دسترسی کاربر را به پوشه صندوق شخصی را فراهم می کند.

در نتیجه با ایجاد یک دسترسی , به تعداد کاربران سامانه یک سطح دسترسی تولید می شود.

تعریف دسترسی بر اساس نام کاربر بر مبنای نام قسمت



مسیر	سطح دسترسی
اداری \ \ <نام ریشه سامانه>	RLDW

در سامانه جامع رسان در تعریف هر کاربر یک نام قسمت ، که می تواند مطابق چارت سازمانی وی باشد تعریف می شود.

در این حالت سامانه بصورت خودکار بجای عبارت **اداری | ۱** ، نام کاربرانی که نام قسمت آنها اداری باشد را قرار می دهد، همانطور که قبلا بیان شد در سامانه جامع رسان بصورت پیش فرض هر کاربر در ریشه سامانه، یک پوشه به نام خود دارد، اکنون اگر بخواهیم مدیر هر قسمت بر تمام پوشه های کارمندان خود دسترسی داشته باشد، برای آن مدیر قسمت دسترسی بالا را وارد می کنیم.

اکنون اگر فردی با دسترسی بالا به سامانه وارد شود در محل ریشه سامانه علاوه بر پوشه خود پوشه تمام افرادی را که نام قسمت آنها اداری باشد را هم می بیند

تعریف دسترسی بر اساس IP

بصورت پیش فرض برای دسترسی به منابع آی پی (IP) سیستم کاربر چک نمی شود، اما در صورت استفاده از این ویژگی خاص می توان برای منابع دارای طبقه بندی محدودیت آی پی را اعمال کرد تا حتی در صورت بدست آوردن کلمه عبور یک کاربر توسط افراد غیر مجاز ، آنها نتوانند به منابع حساس کاربر دسترسی داشته باشند، همچنین میتوان برای یک منبع یک یا چند IP مجاز برای دسترسی به آن تعریف کرد



ارسال اطلاعات بصورت رمز شده



استفاده از رمز نگاری در ارسال اطلاعات یکی از اساسی ترین راههای مقابله با سرقت اطلاعات در طول مسیر ارسال می باشد.

سامانه جامع رسان با استفاده از الگوریتم های استاندارد رمز نگاری همچنین با استفاده از یک سیستم مدیریت کلید اختصاصی ، می تواند با انتخاب کاربر ،اطلاعات را بصورت رمز و یا کشف ارسال کند.

از آنجا که سیستم های مانند VPN که ارتباط رمز شده ای را ایجاد می کنند باعث کند شدن سرعت ارتباط می شوند لذا در سامانه جامع رسان امکان رمز شدن بصورت انتخابی بعهدده کاربر می باشد که در صورت دلخواه برای منابع با سطح طبقه بندی بالا می توان از آن استفاده کرد تا در موارد غیر ضروری سرعت ارتباط کم نشود.

ایجاد "شناسه کاربر و تاریخ" برای بوجود آورنده منابع



هر گاه به پوشه ای فقط دسترسی (W) نوشتن داده شود در این حالت اگر کاربری بخواهد در آن پوشه فایل یا پوشه ای قرار دهد ابتدا توسط سامانه جامع رسان بصورت خودکار دو پوشه (اولی بنام کاربری که قصد ایجاد فایل را دارد، و دومی تاریخ و زمان ایجاد فایل) ساخته شده، سپس فایل کاربر را در انتهای آن قرار می گیرد.

پیاده سازی سیستم توزیع و جمع آوری فرم های اداری با این ویژگی



در این سناریو فایل هایی به فرمت دلخواه بعنوان فرم های اداری در اختیار کاربران قرار داده می شود و سپس کاربران با پر کردن این فرم ها نتیجه را به بخش مورد نظر تحویل می دهند.

ابتدا می بایست فرم های اداری خام را با هر نوع فرمت مانند فایل ورد و یا اکسل و یا هر نوع فرمت دیگر را در محل خاصی در سرور برای تمام کاربران یا کاربران مورد نظر ، دسترسی خواندن داد.

سپس پوشه دیگری را برای جمع آوری فرم ها در نظر گرفته ، دسترسی های زیر را بنا به خواست، در بخش دسترسی عمومی برای تمام کاربران و یا در بخش دسترسی بر اساس قسمت برای کاربران قسمت خاص وارد می کنیم.

مسیر	سطح دسترسی
? \ پوشه جمع آوری فرم ها \ <نام ریشه سامانه>	L
مسیر	سطح دسترسی
پوشه جمع آوری فرمها \ <نام ریشه سامانه>	W

دسترسی اول باعث می شود تا کاربر بتواند پوشه جمع آوری فرم ها را ببیند ولی دسترسی دیدن فرم های پر شده توسط دیگر کاربران را نداشته باشد و در صورت لزوم فقط فرم پر شده خود را ببیند.

دسترسی دوم علاوه بر اینکه مجوز نوشتن در پوشه مورد نظر را به کاربران می دهد، همانطور که در قسمت پیام رسان مشاهده خواهد شد نام کاربر ارسال کننده به همراه تاریخ ارسال را در سیستم ثبت می کند.

از این ویژگی در ایجاد یک سامانه « پیام رسان » در سامانه جامع رسان استفاده شده است



مسیر	سطح دسترسی
فایلهای در یافتی * \ <نام ریشه سامانه>	W

همانطور که قبلا اشاره شد هر کاربر بصورت پیش فرض در ریشه سامانه پوشه ای بنام خود دارد که شامل چند پوشه از جمله پوشه فایل های در یافتی می باشد با اعمال دسترسی فوق به تمام کاربران , یک سیستم پیام رسان ایجاد می شود.

در واقع وقتی کاربر از طریق نرم افزار سامانه جامع رسان فایلی را برای کاربر دیگر ارسال می کند فایل او به مسیر فایل‌های دریافتی کاربر مورد نظر ارسال می شود و کاربر دریافت کننده نیز با مشاهده این قسمت ابتدا نام فرستنده و سپس تاریخ ارسال و در انتها فایل ارسال شده را مشاهده می کند.

البته مکانیزمی در سیستم تعبیه شده تا کاربر ارسال کننده بتواند با انتخاب خود یک نسخه از فایل ارسالی را در پوشه فایل‌های ارسالی حساب خود نگهداری نماید.

