

نرم افزاری سبزاندیشان
تأمین امنیت سیستم های شخصی و سرورهای سازمانی
(ضد ویروس - سیستم عامل)
www.sabzandishan.ir



۲۰۷

ماهنامه

کامپیوتری

ISSN 1022 - 4082

www.rayanehmag.net

علمی / فنی / تخصصی کامپیوتر

ملشین های انسان نما

هوش مصنوعی

۱۲ گام به سوی انتخاب یک کامپیوتر شخصی

اینترنت از طریق کابل برق

به دنیای گوگل خوش آمدید...

پشتیبان گیری آنلاین

استیف بی سیم چیست؟

مدیریت یکپارچه سازی در گرید

پروتکل اس اس ال

امنیت استراتژیک

امنیت در لینوکس با استفاده از iptables

سرگرمی های سه بعدی

آر میاش بزرگترین افسانه های فن آوری

امنیت در سیستم عامل

لینوکس

با استفاده از

iptables

پارس دیتا
www.parsdata.com

Web Hosting

Server's Location: Canada, Iran.

Platforms: Windows, Linux.

Security: Hardware Firewall Layer, Protected by up-to-date Software Firewall, Permission Settings, Password Protection, Symantec Security Software.

General Features: Control Panel (Helm for Windows, DirectAdmin for Linux), Search Engine Submission, Burstable Bandwidth, Virus Scanning.

Technical Features: DNS Management, Sub-Domains, Dedicated IP Address, Virtual Directory, URL Front Page Extensions, 24x7 FTP Access, Anonymous FTP, Custom Error Pages, Dedicated Application Programming Languages: ASP 3.0, ASP.NET (1.1 / 2.0 / 3.5 / 4.0), PHP (4.x / 5.x), Perl 5.x, Python 3.x, ColdFusion, Compiled CGI and SSI, SHTML / DHTML.

Emails: Separated Email Space, Web Mail, POP3 / SMTP / IMAP4 / LDAP3, Catchall, Live up-to-date Unlimited Forwarding / Aliases / Auto Responders / Vacation Message, Send / Receive HTML formatted Spell Checking, Address Book, Personal Calendar, Processing Rules.

Databases: MS-SQL 2000, MS-SQL 2005, MS-SQL 2008, MySQL, MS Access, Oracle.

Database Tools: Web-Based Management and Web-Based Backup/Restore for SQL-2000/2005/2008 Components: Crystal Reports.

General Components: MS XML / MSWC, CDONTS / CDOYS, ADO / ADO NET, SOAP Toolkit.

ASP Components: AspUpload, AspJpeg, AspEmail, AspEncrypt, AspGrid, AspUser, w3 JMail, aspSmartUpload, aspSmartImage, aspSmartMail, ABCUpload, Dundas Upload, AspQMail, ImageSize.

Multimedia: Flash (FLV), Flash Media Server, Shockwave, Media Streaming Audio/Video.

WebSite Statistics: Web Statistics (Live), Counter, Raw Logs Access, Quota Reporting.

Backup: @Weekly (Backup Server) @Monthly (Mirrored HDD).

Guarantee: First Week Money Back Guarantee.

Technical Support: 24 Hours Phone, Fax, Ticket/Email.

► www.parsdata.com

DOI: 10.5281/zenodo.15254174

سال بیست و یکم - بهمن ۸۹ - ۲۳۰ صفحه - ۱۵۰۰ تومان

آیا می دانید بسته طلایی سرورهای ایران اچ پی
خیال شما را از همه نظر راحت می کند؟



سرورهای ارجیتهال
اچ پی با

پاسخگوی سریع
۰۲۱-۸۳۶۳

پیام کوتاه
۳۰۰۰۸۳۶۳

web iranhp.ir
falnic.com



مکمل اعتبار برند اچ پی
گارانتی ایران اچ پی

iranhp.ir

- رایانه مجله ای مستقل است و به هیچ شرکت و موسسه ای وابسته نیست.
- استفاده کامل از مقالات چه در کتب و مجلات و چه در سایت ها و وبلاگها بدون اجازه کتبی ممنوع است و پیگرد قانونی دارد.
- استفاده قسمتی از یک مقاله با ذکر مأخذ بلامانع است.
- رایانه در حکم و اصلاح مطالب رسیده آزاد است.
- نظر نویسنده مقاله لزوماً نظر رایانه نیست.
- لطفاً مقالات ارسالی را با خط خوانا و در یک روی صفحه بنویسید و در صورت امکان تایپ نمایید. چنانچه مطلب ارسالی ترجمه می باشد حتماً یک کپی از اصل مطلب را ضمیمه نمایید.
- مقالات خود را می توانید به آدرس الکترونیکی ماهنامه و یا سردبیر ارسال کنید.

ماهنامه (rayaneh@rayanehmag.net)

سردبیر (rayaneh_editor@yahoo.com)

صاحب امتیاز و مدیر مسئول

دکتر ابوالفضل ذوالفقاری

سر دبیر

پویا عباداللهی واحد

مدیر سازمان آگهی ها

خانم ناصری

مدیر اجرایی و گرافیکست

حامد ذوالفقاری

تلفن و فاکس

۸-۸۹۹۲۹۶۶-۸

۲۲۸۶۲۴۴۵-۲۲۸۶۲۵۲۴

صندوق پستی

۱۳۴۴۵ / ۸۷۶

آدرس

تهران/ خیابان فاطمی/ خیابان پروین اعتصامی/ لعل غربی/شماره ۳

لیتوگرافی

پارسیان/ ۶۶۴۲۳۵۶۰

چاپ رنگی

ستاره سبز/ ۶۶۲۹۹۳۷

چاپ متن

بهمن/ خیابان دماوند/ شماره ۱۰۲ / ۷۷۳۳۸۱۱۰



صفحه ۹۸



صفحه ۷۳



صفحه ۴۶



صفحه ۳۱

<http://www.rayanehmag.net>

E/mail:rayaneh@rayanehmag.net

مدیریت یکپارچه سازی اطلاعات در گرید

چکیده

از زمان ظهور شبکه های توزیع شده فرصت های عملی بسیاری برای شناسایی و ثبت رویدادها در زمان وقوع بوجود آمده و همچنین تلاش های برای شناسایی رویدادها و حل مشکلات ذخیره اطلاعات از قبیل به روز بودن و سندیت، صرف شده است. در این رابطه مشکل ها و نقص هایی در رسیدن به سطح بهینه نگهداری سوابق پولی، مالی و حسابداری وجود دارد. در جهت این امر باید در توزیع سیستم های اطلاعاتی در محیط شبکه، دقت شود و یک سری اطلاعات پیوسته و روز آمد شده را در دست داشت و نباید هیچ محدودیتی برای تهیه مفروضات و مبانی استفاده از آنها توسط اداره کننده، گروه مدیریت یا سایت اعمال شود. گرید (از جمله مجموعه سیستم ها در اشتراک اطلاعات) که توسط لن فوسترو کارل کسلمان مطرح شده، تا با برقراری یک ارتباط ایمن، راه را برای پردازش مشترک با استفاده از منابع و اطلاعات سازمان های مجازی هموار سازد. **واژگان کلیدی:** گرید، ساختار ایمن، ارتباطات ایمن، پردازش مشترک

مقدمه

با توجه به گسترش سازمان خدمات دهنده الکترونیکی، که به اشتراک و در اختیار قرار دادن منابع در محیط های مجازی فعالیت دارند، امنیت و اعتماد برای طرفین مشارکت کننده در این محیط حائز اهمیت است. بنا براین جهت شناسایی و شناخت از محیط های مزبور باید ساختار این محیط ها را بررسی کنیم. با گسترش ساختارهای گوناگون محیط های یکپارچه اطلاعاتی چون، پایگاه های اطلاعاتی شبکه های مجازی، شبکه های خصوصی، شبکه های گسترده و افزایش دامنه اشتراک اطلاعات در محدوده مجازی، نیاز به بررسی این محیط به منظور افزایش حس اعتماد - (طرفین مشارکت کنندگان) احساس می شود.

نگارنده

گرید به سیستم هایی گفته می شود که در جهت مدیریت و یکپارچه سازی منابع و سرویسها توزیع شده در میان کنترل کننده های محدوده استفاده می شود. گرید در سازمان مجازی در مقایسه گروه های شخصی، منابع وابسته و خدمات در جهت یک هدف مشترک قرار گرفته است. جهت

پاسخگویی به نیاز یکپارچگی اطلاعات و مدیریت کنترل کار در میان سازمان های مجازی ایجاد گشته است. گرید محاسباتی یک ساختار سخت افزاری یا نرم افزاری که فراهم کننده یک محدوده مورد اعتماد، پایدار، فراگیرنده و ارزان جهت دستیابی به امکانات و ظرفیت های بلااستفاده یا مازاد بر نیاز فعلی مشارکت کنندگان در سیستم را ایجاد نماید.

در این راستا گرید به طور پویا و دینامیک به گردآوری اطلاعات منابع از سازمان های مجازی (VO) فعالیت دارد و تهیه کننده خدماتی است که به صورت یکپارچه منابع را مدیریت و نمایش دهد.

همانطور که در نمایه شماره ۱ مشاهده می گردد منابع اطلاعاتی در گرید می تواند شامل یک یا چند منبع باشد. در این سیستم کاربر نهایی میتواند اطلاعات مورد نظر خود را بسادگی پیدا کرده و بکارگیرد. منابع اطلاعاتی که در گرید در دسترس افراد قرار می گیرند از تنوع بسیار برخوردارند که شامل: گرید اطلاعاتی، دایرکتوری، تخصیص منابع، توسعه نرم افزار، مدیریت اجرایی، اطلاعات منابع در دسترس و زمانبندی اطلاعات می باشد. در این شبکه نرم افزارها و خدمات ارائه شده قابلیت ارتباط بین منابع مختلف اطلاعاتی و تجزیه و تحلیل و دسته بندی آنها با توجه به نیاز مدیریت فراهم می باشد. این ارتباط از طریق ویژگی ها و قابلیت های شبکه های رایانه ای در تجزیه و تحلیل و توزیع اطلاعات تحت عنوان میان افزار گرید صورت می گیرد.

در ضمن ایمنی داده ها را در این سازمان ها تضمین می کند. از جمله پروژیه ای که از ساختار گرید استفاده می کنند می توان به:

الف) SETI@home یکی از مشهورترین چرخه پردازش شبکه است که از ۳ میلیون کامپیوتر استفاده کرده تا بتواند اطلاعات زنجیره ای به دست آورد.

ب) پروژه شناخته شده دیگر distributed.net است که در ۱۹۹۷ شروع شد و تعداد ۱۱۰۰ پروژه موفق در توزیع اطلاعات، در سوابقش مشاهده می شود.

ج) تسهیلات کامپیوترهای پیشرفته ناسا، در الگوریتم های وراثت شناختی، چرخه پردازش گر Condor را به کار می گیرد که در حدود ۳۵۰ ایستگاه کاری خورشیدی و (SGL) اجرا می کند.

د) تا ۲۷ آوریل ۲۰۰۷ طرح یکپارچه سازی اطلاعات در سازمان ها، بر اساس آن شبکه mp تشکیل شده و محصول چرخه پردازش

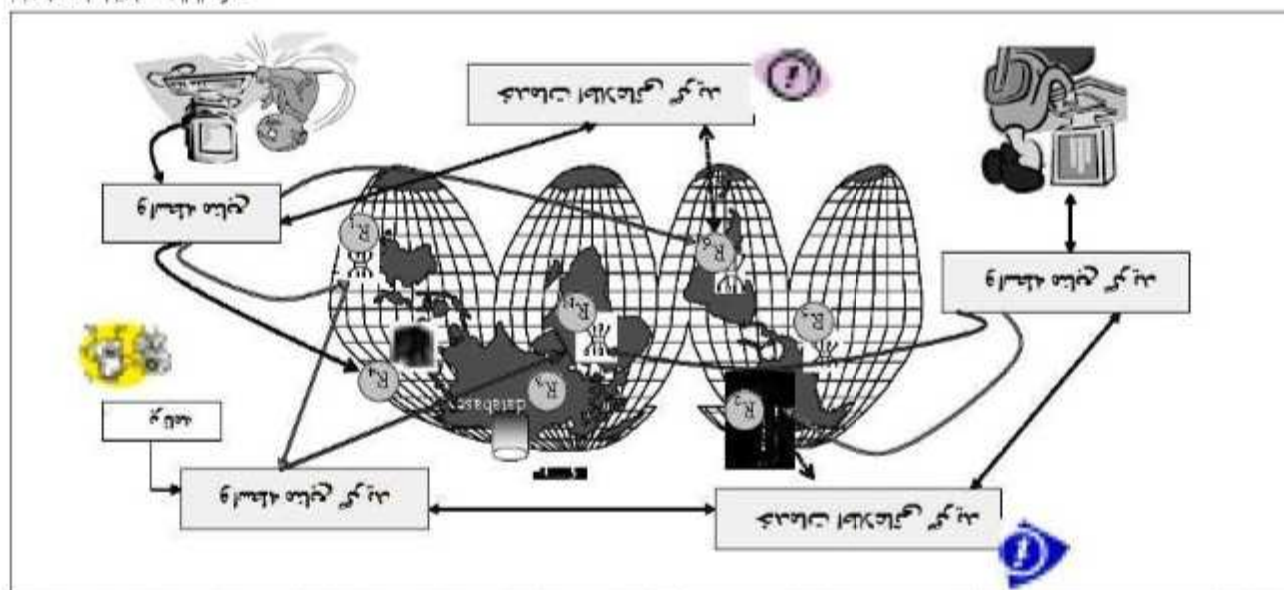
دستیابی به داده‌های مورد نیاز برای جستجو به سرعت و به روشی مناسب انجام می‌دهد. این امر به کاربران اجازه می‌دهد تا به راحتی به داده‌های مورد نیاز خود دسترسی پیدا کنند. در این زمینه، استفاده از سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای می‌تواند به بهبود کارایی و کاهش هزینه‌ها کمک کند. همچنین، استفاده از روش‌های نوین برای پردازش و تحلیل داده‌ها می‌تواند به کشف بینش‌های جدید و اتخاذ تصمیمات بهتر کمک کند. در نهایت، استفاده از سیستم‌های امنیتی و کنترل دسترسی می‌تواند به محافظت از داده‌ها و جلوگیری از سوءاستفاده کمک کند.

در این مقاله، ما به بررسی سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای می‌پردازیم. ما به بررسی مزایا و معایب این سیستم‌ها می‌پردازیم و به روش‌های نوین برای پردازش و تحلیل داده‌ها می‌پردازیم. همچنین، ما به روش‌های نوین برای محافظت از داده‌ها و جلوگیری از سوءاستفاده می‌پردازیم. در نهایت، ما به نتیجه‌گیری می‌پردازیم و پیشنهاداتی برای بهبود سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای ارائه می‌دهیم.

در این مقاله، ما به بررسی سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای می‌پردازیم. ما به بررسی مزایا و معایب این سیستم‌ها می‌پردازیم و به روش‌های نوین برای پردازش و تحلیل داده‌ها می‌پردازیم. همچنین، ما به روش‌های نوین برای محافظت از داده‌ها و جلوگیری از سوءاستفاده می‌پردازیم. در نهایت، ما به نتیجه‌گیری می‌پردازیم و پیشنهاداتی برای بهبود سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای ارائه می‌دهیم.

در این مقاله، ما به بررسی سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای می‌پردازیم. ما به بررسی مزایا و معایب این سیستم‌ها می‌پردازیم و به روش‌های نوین برای پردازش و تحلیل داده‌ها می‌پردازیم. همچنین، ما به روش‌های نوین برای محافظت از داده‌ها و جلوگیری از سوءاستفاده می‌پردازیم. در نهایت، ما به نتیجه‌گیری می‌پردازیم و پیشنهاداتی برای بهبود سیستم‌های توزیع‌شده و استفاده از شبکه‌های رایانه‌ای ارائه می‌دهیم.

شکل ۱: معماری سیستم توزیع‌شده



است، در ادامه بیان می شود، که در این خصوص استانداردهای ایمنی از بعد تکنولوژی اطلاعات چون: ساختار خدمات ایمنی از بعد یکپارچه سازی OSI و ساختار خدماتی گرید باز OGSA فراهم شده است، همچنین استفاده از تکنیک هایی برای بیان و تدوین شیوهای کاربردی مجاز، در حال گسترش است.

ساختار ایمنی، محیط های مجازی اطلاعات

ساختارهای ایمنی اطلاعات دارای استاندارد مشخص و در عین حال دقیق برای سامانه های مجازی است. این ساختارها عموماً بر دو موضوع تاکید دارند.

الف) به طور پیش فرض، بر برقراری ارتباطات بر مبنای مجوزهای متقابل و دو جانبه که از خطوط ایمن و مورد اعتماد طرفین است، صورت گیرد، تاکید دارند. این امر نقش گواهینامه های ایمنی که تعیین کننده شرایط را برای ارتباطات است را مطرح می سازد.

ب) تدوین موافقتنامه دستیابی به موضوع مورد مشارکت: ایجاد یک توافق ساده برای رسیدن به اهداف موضوع و استفاده از پروتکل های ایمنی نظیر زبان توضیحی خدمات وب، روابط چند جانبه خدمات وب که ارتباط بین واحدها در ایستگاه های کاری مختلف را متناسب با قواعدخاص هر سرویس و مبادله گر پیام، میسر می سازد، از جمله موارد مورد بحث در ساختار های ایمنی اطلاعات است. در ذیل برخی از این مکانیسم ها تشریح می شود:

۱- زبان توضیحی خدمات وب (WSDL)

این بر مبنای زبان گزارشگری تجاری است که برای توضیح دادن خدمات وب استفاده می شود. خدماتی که به عنوان مجوز از نقاط پایانی شبکه یا پورت تعریف گردیده و فراهم کننده یک ساختار خاص برای رونوشت ها با توجه به هدف مربوطه است. این زبان خلاصه ای از پیام های مرتبط و پیوسته در جهت ارتباط استفاده می کند، تا حداقل استاندارد ها برای استفاده از اطلاعات در شبکه مشخص شود.

۲- خطوط ارتباطی: خطوط ارتباطی بین مشترکین (در محدوده مشارکتی) باید همواره از نظر اعتبار، ایمنی و اطمینان از لحاظ برقراری ارتباط صحیح مورد بررسی قرار گیرد. چه بسا ارتباط بین این مشترکین در این محیط (با وجود امضا توافقتنامه) غیر ایمن، غیر مجاز و در جهت سو

استفاده از منابع مشارکتی سازمان باشد.

به همین منظور، استانداردهای ایمنی گرید مطرح شده است که از دو اصل زیر پیروی می کند.

۱- ساختار سرویس گرید باز (OGSA) این مشخصه در سال ۲۰۰۲ توسط SETI@home به شرح زیر پیشنهاد گردیده است:

الف) به طور پیش فرض، برقراری ارتباطات بر مبنای مجوزهای متقابل و دو جانبه که از خطوط ایمن و مورد اعتماد طرفین است، صورت گیرد، اما نباید نقش گواهینامه ها و خطوط ایمنی که شرایط را برای ارتباطات ایمن فراهم می نماید، نادیده گرفت.

ب) سوآپ (موافقتنامه دستیابی به موضوع مورد مشارکت). ایجاد یک محیط دستوری ساده برای رسیدن به اهداف موافقتنامه ها و استفاده از پروتکل های ایمنی چون زبان توضیحی خدمات وب، روابط چند جانبه خدمات وب که ارتباط بین واحدها در ایستگاههای کاری مختلف را متناسب با قواعدخاص هر سرویس و مبادله گر پیام، میسر می سازد.

با استفاده از سیستم های تعبیه شده در پایگاه اطلاعاتی، نحوه برقراری ارتباطات، سطوح دسترسی به اطلاعات و مجوز دهی در این سرویس، نظارت و خطاهای آن را بازگو می نماید.

با توجه به اینکه در محدوده مشارکت اطلاعات و منابع از یک سیستم تطبیق پذیر برای افزایش امنیت استفاده می شود، نظارت کننده برای بررسی این شیوه کنترلی از روش های ویژه ای نظیر هوش مصنوعی در ارزیابی و بررسی ساختار ایمنی استفاده می نماید.

با توجه به موارد بحث شده، به اصول ایمنی از دیدگاه الکس لیو توجه نمایید، زیرا که پیروی از این اصول راه را برای یک ساختار کنترلی بهینه هموار می سازد.

پروسیس سرویس مجازی ایمنی اطلاعات

با استفاده از سیستم های تعبیه شده در پایگاه اطلاعاتی، نحوه برقراری ارتباطات، سطوح دسترسی به اطلاعات و مجوز دهی در این سرویس، نظارت و خطاهای آن را بازگو می نماید.

با توجه به اینکه در محدوده مشارکت اطلاعات و منابع از یک سیستم تطبیق پذیر برای افزایش امنیت استفاده می

شود، نظارت کننده برای بررسی این شیوه کنترلی از روش های ویژه ای نظیر هوش مصنوعی در ارزیابی و بررسی ساختار ایمنی استفاده می نماید.

با توجه به موارد بحث شده، به اصول ایمنی از دیدگاه الکس لیو توجه نمایید، زیرا که پیروی از این اصول راه را برای یک ساختار کنترلی بهینه هموار می سازد.

نمایه شماره ۲ بطور خلاصه فرایند دریافت، ذخیره سازی، فهرست بندی و تجزیه و تحلیل اطلاعات در گرید را نمایش می دهد. همانطور که ملاحظه می شود کاربرد می تواند به نتایج تجزیه و تحلیل اطلاعات در سیستم از طریق رایانه و نرم افزار مربوطه دست یافته و آنها را در جهت اهداف مورد نظر خود بکار گیرد.

باز، خدماتی که به طور پیش فرض اجرا می شود و خدماتی با بالاترین سطح سوء استفاده را مشخص و محدود کنید.

۱۱. به طور واضح مسئولیت‌ها را مشخص نماید. (در سطح سازمان و در سطح دستیابی به اطلاعات)

۱۲- بررسی سیستم را تداوم بخشید ، جهت یک سیستم ایمن ، شما نیاز دارید که تغییرات بوجود آمده سیستم خود را ثبت نمایید و نقاط ضعف و قوت خود از حسابرس که به شیوه مستمر با شما همکاری می نماید جویا شده و از راه حل هایی که در اختیار شما قرار می دهد، استفاده نماید.

۱۵. آموزش را فراموش ننمایید، آموزش استفاده کنندگان مجاز از سیستم، موقعیت امنی شما را بهبود می بخشد.

زیر بنا و تعیین کننده نوع شبکه، روش های پردازش اطلاعات در شبکه کامپیوتری است. به بیان دیگر، روش های پردازش اطلاعات در شبکه، مبنای انواع شبکه های کامپیوتری است. روش های پردازش

۱. پیوندهای ضعیف در سیستم را رفع نمایید: زمان بیشتری برای رفع نقص پیوندها و شکاف های سیستم بگذارید، شاید متجاوزان از همین شکافها و پیوندهای ضعیف بتوانند سیستم را مورد هجوم قرار دهند.

۳. حداقل برتری دادن (امتیاز خاصی بخشیدن) در سازمان : اجازه ندهید که هرکسی به رمزهای عبوردست یابد. اجازه ندهید که هرکسی بتواند به سیستم وارد شده (حتی برای زمان کوتاهی) و آن را مدیریت نماید.

۴. تقسیم وظایف به طور بخش به بخش : از بخش های مختلف برای وظایف متفاوت استفاده کنید.

۶. رمزها و اسرار را مخفی سازید. به امنیت با اِبهام، اعتماد نکنید، این پیش فرض را برای خود قرار ندهید. که «تجاوزان کدایمنی شما را نمی‌دانند».

۸. حداقل کردن سطح تجاوز و حمله به سازمان، تعداد راههای ارتباطی

اطلاعات در شبکه به سه صورت: متمرکز، غیر متمرکز، اشتراکی انجام می شود. در پردازش متمرکز، تمام پردازش ها در کامپیوتر مرکزی انجام می شود و برای سازمانهای با ساختار متمرکز مناسب بوده که نیاز به کامپیوتر های بزرگ (از لحاظ قدرت محاسباتی و پردازش) دارد. پردازش غیر متمرکز بیشتر در کامپیوترهای شخصی انجام می شود و به جای استفاده از یک کامپیوتر مرکزی مشترک، هر کاربر می تواند با کامپیوتر

شخصی خود، اطلاعات را مورد پردازش قرار دهد، تفاوت پردازش متمرکز و پردازش غیر متمرکز در این است که پردازش اطلاعات در کامپیوترهای کاربران یا پایانه انجام می شود و امکان توزیع سخت افزار ها را در سطح سازمان ایجاد می نماید.

در محدوده های مشارکتی سیستم های گنبد، این امکان فراهم شده که، پردازش غیرمتمرکز یا پراکنده افزون بر اشتراک منابع، فایل ها و اطلاعات صورت گیرد و مشارکت کنندگان بتواند اطلاعات را به طور مشترک پردازش نمایند. (در این محیط، یک مشارکت کننده می تواند برای پردازش از اطلاعات سایر مشارکت کنندگان استفاده نماید که این پردازش دارای ویژگی های زیر است:

- ۱) همکاری و اشتراک منابع در انجام پردازش
- ۲) وجود یک شبکه پیوسته برای تبادل اطلاعات منابع بین مشارکت کنندگان
- ۳) ایجاد فایل های مشترک جهت پردازش مشترک
- ۴) وجود یک محیط ایمن جهت پردازش، بدون یک اداره کننده یا میانجی پردازش

گروه مدیریت سیستم گنبد

این گروه مدیریتی در ایجاد یک پایگاه اشتراک منابع، تسهیلات انتقال اطلاعات در سیستم و همچنین ایجاد شیوه های محلی و موازی در انتقال با کیفیت اطلاعات و ترکیب منابع، کمک بسزایی می نماید. این گروه سبب کنترل متمرکز سیستم شده که دانش کاملی از حالات سیستم، تقاضای کاربران و کنترل های جامع و کامل بر روی اجزا

گروه مدیریت سیستم گنبد در ایجاد یک پایگاه اشتراک منابع، تسهیلات انتقال اطلاعات در سیستم و همچنین ایجاد شیوه های محلی و موازی در انتقال با کیفیت اطلاعات و ترکیب منابع، کمک بسزایی می نماید. این گروه سبب کنترل متمرکز سیستم شده که دانش کاملی از حالات سیستم، تقاضای کاربران و کنترل های جامع و کامل بر روی اجزا مشارکت کنندگان در سیستم را دارد. این گروه از هدف های پروتکل ها و توافق نامه ای ایمنی که از سیستم پشتیبانی می کند، کاملاً آگاه است. مشخص کردن مکان و زمان دسترسی مشارکت کنندگان به اطلاعات در محدوده از جمله وظایف این گروه است کیفیت قابل توجه ای از این خدمات در محدوده مشارکتی همواره برقرار است.

مشارکت کنندگان در سیستم را دارد، این گروه از هدف های پروتکل ها و توافق نامه ای ایمنی که از سیستم پشتیبانی می کند، کاملاً آگاه است. مشخص کردن مکان و زمان دسترسی مشارکت کنندگان به اطلاعات در محدوده از جمله وظایف این گروه است. کیفیت قابل توجه ای از این خدمات در محدوده مشارکتی همواره برقرار است. نتیجه گیری:

گنبد را می توان تجربه ای جدید در تحقیقات علمی مجازی دانست که نیازمند مدیریت گسترده بر اطلاعات

می باشد. در این مقاله گوشه هایی از این فرایند را مورد نقد و بررسی قرار دادیم ولی از آنجاییکه گنبد جزء مفاهیم و ساختارهای جدید می باشد لذا تحقیقات بیشتری در این رابطه مورد نیاز است تا ویژگی بیشتری از این ساختار مورد ارزیابی قرار گیرد. با توجه به اینکه فرصتهایی تازه توسط گنبد پیش روی مدیران قرار می گیرد لذا بررسی و ارزیابی این سیستمها

بصورت مستمر از اهمیت بسزایی برخوردار است. **رایانه**

منابع:

۱. آریا ناصر، حسابرسی شبکه های کامپیوتری، مرکز تحقیقات تخصصی حسابداری و حسابرسی سازمان حسابرسی، تهران، دی ۱۳۸۰، ص ۱۷ - ۱۹.
۲. تابنده احمد، کاربرد سازمان مجازی در کسب و کار، ماهنامه تدبیر، سال هفدهم، شماره ۱۷۲
3. Foster, Ian, What is the Grid? A Three Point Checklist, Argonne National Laboratory & University of Chicago, July 20, 2002
4. AlexX.Liu //www.cse.msu.edu/~alexliu2132, Engineer Building Department of Computer Science and Engineering, Michigan State University
5. Security for Grid Services by Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman, Steven Tuecke (Universities of Chicago, Southern California & Argonne National Laboratory) 2005