تحلیل چالش‌های امنیتی و تاثیر آن بر رایانش ابری

سمیه سلطان باغشاهی[۱]، لیلا سلطان باغشاهی[۲]، احمد خادم زاده[۳] و سام جبه داری[۴]
[۱] دانشگاه آزاد اسلامی واحد تهران شمال- دانشکده فنی و مهندسی- گروه مهندسی کامپیوتر ، Sbaghshahi@yahoo.com
[۲] دانشگاه آزاد اسلامی واحد تهران جنوب- دانشکده فنی و مهندسی- گروه مهندسی کامپیوتر ، Lbaghshahi@yahoo.com
[۳] پژوهشگاه ارتباطات و فناوری اطلاعات- تهران- ایران ، Zadeh@Itrc.ac.ir
[۴] Sjabbehdari@gmail.com

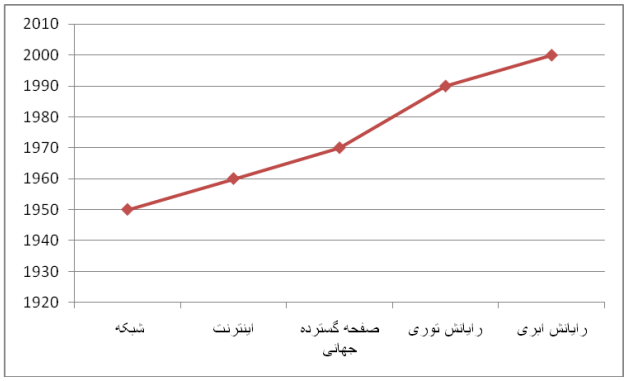
چکیده- رایانش ابری یک تکنولوژی جدیدی نیست؛ بلکه یک روش جدید برای ارائه منابع محاسباتی و یک مدل برای ارائه سرویس از طریق اینترنت می‌باشد. در واقع رایانش ابری توانایی بهره‌وری و صرفه‌جویی در منابع *IT* و افزایش توان محاسباتی را فراهم می‌کند، به طوری که توان پردازشی به ابزاری با قابلیت دسترسی همیشگی تبدیل می‌شود. اگرچه رایانش ابری مزایای زیادی دارد؛ ولی امنیت در ابر بسیار حائز اهمیت است. در این مقاله ابتدا یک بینش کلی نسبت به رایانش ابری و سرویس‌های ارائه شده در آن فراهم می‌شود، سپس تکنولوژی‌های مجازی‌سازی برای ساخت مخازن اشتراکی منابع مورد بحث قرار گرفته و در ادامه مسائل و چالش‌های امنیتی موجود در رایانش ابری به همراه روش‌های کاهش این چالش‌ها بیان می‌شود. همچنین یک بررسی مقایسه‌ای از تاثیر این چالش‌ها بر مزایای رایانش ابری انجام می‌شود.

کلید واژه‌ها- رایانش ابری، مجازی‌سازی، چندمستاجری

۱. مقدمه

امروزه پیشرفت و توسعه مرزهای دانش به گسترش تکنولوژی‌های محاسباتی وابسته شده است. به عنوان نقطه آغاز این تکنولوژی‌ها می‌توان به تشکیل شبکه کامپیوتری اشاره کرد که در آن تنها چندین کامپیوتر به هم متصل شده بودند. پس از آن این شبکه‌های کوچک به یکدیگر متصل شدند و اینترنت را به وجود آوردند که در اینترنت شبکه‌ها به اشتراک گذاشته شدند. در آن زمان به بستری برای تبادل اطلاعات از طریق اینترنت نیاز بود که مفهوم صفحه گسترده جهانی(WWW[۱]) شکل گرفت که از طریق آن اطلاعات در میان کاربران به اشتراک گذاشته شد. در این راستا تکنولوژی جدیدی به نام رایانش توری[۲] شکل گرفت که در آن منابع از راه دور به اشتراک گذاشته شدند و هدف آن افزایش کارایی و توان پردازشی بود. در عصر حاضر با روش جدیدی به نام رایانش ابری روبرو هستیم که در این روش سرویس‌ها از طریق اینترنت به اشتراک گذاشته می‌شوند. در شکل ۱ سیر تکاملی رایانش ابری نشان داده شده است [۱].

شکل ۱- سیر تکاملی رایانش ابری



با توجه به رشد روز افزون تکنولوژی‌ها و تنوع نیاز کاربران در حوزه فناوری اطلاعات، جایگاه رایانش ابری نمود بیشتری پیدا می‌کند. چرا که گسترش زیر ساخت محاسباتی در هر سازمان نیازمند صرف هزینه و زمان و نیروی انسانی بسیاری است که گاهی در توان عملیاتی یک سازمان نمی‌گنجد. از این رو سازمانها

[1]- World Wide Web
[2]- Grid Computing

برای پیشبرد اهداف خود تمایل به استفاده از چنین تکنولوژی‌هایی دارند. ولی اغلب نمی‌توانند هیچ تضمینی در خصوص امنیت اطلاعات و برنامه‌های کاربردی خود که نزد سرویس‌دهندگان ابر (CSP[3]) می‌باشد، حاصل کنند. البته راهکارهای امنیتی توسط ارائه دهندگان برای تضمین امنیت اطلاعات مشتریان اعمال می‌شود. ولی به دلیل اینکه همه چیز در ابر کاملا شفاف[4] است و کاربران هیچ اطلاعی از این مکانیزم‌ها ندارند، گاهی مسئله را سخت و دشوار جلوه می‌دهد.

رایانش ابری از بستر اینترنت برای اتصال به میزبان شبکه، زیرساخت‌ها، برنامه‌های کاربردی و ارائه سرویس‌های قابل اعتماد استفاده می‌کند. در ابر هر سرویسی با توجه به نیاز مشتری ارائه می‌شود. در مجموع می‌توان ابر را ترکیبی از فناوری‌های موجود، سیستم‌های توزیع شده، چند پردازنده‌ای، تکنولوژی‌های مجازی سازی و شبکه‌های مبتنی بر فضای ذخیره‌سازی داده‌های توزیع شده معرفی کرد.

با وجود اینکه تعاریف زیادی از رایانش ابری وجود دارد، ولی می‌توان گفت یک اتفاق نظر کلی هم در صنعت محاسبات و هم در دانشگاه وجود دارد که منابع مورد نیاز و سرویس‌ها در سراسر اینترنت را فراهم می‌کند. این نوع محاسبات به سازندگان و توسعه‌دهندگان اجازه می‌دهد تا برنامه‌های کاربردی مورد نظر خود را نوشته و در محیط ابر اجرا کنند.

انواع سرویس‌ها در ابر به سه دسته تقسیم می‌شوند:

- زیر ساخت به عنوان سرویس(Iaas[5])
- platform به عنوان سرویس(Paas[6])
- نرم افزار به عنوان سرویس(Saas[7])

از جمله مزایایی که می‌توان برای رایانش ابری برشمرد، کیفیت سرویس، قابلیت اطمینان، مدیریت از راه دور، کاهش هزینه، کارایی، قابلیت اعتماد و شهرت و غیره می باشد.

[3]- cloud service provider
[4]- Transparency
[5] - Infrastructure as a service
[6] - Platform as a service
[7] - Software as a service

علاوه بر داشتن مزایا، رایانش ابری دارای معایبی مانند وابسته بودن توان پردازشی به پهنای باند، امنیت حریم خصوصی، حالت نگهدار نبودن و غیره می‌باشد [۲].

۲. به کارگیری تکنولوژی مجازی سازی در رایانش ابری

در رایانش ابری، ارائه‌دهندگان سرویس‌های ابری، از یک زیرساخت مجازی برای ارائه سرویس به مشتریان خود استفاده می‌کنند. در واقع مشتریان با استفاده از این تکنیک به منابع اشتراکی دست خواهند یافت و منابع فیزیکی مانند Cpu، حافظه و... به صورت مجازی در اختیار مشتریان قرار می‌گیرد. در این تکنولوژی به هر مشتری یک ماشین مجازی (VM)[8] اختصاص داده می‌شود.

۲,۱. انواع مجازی سازی

ماشین مجازی، مدیر حافظه مجازی (VMM)[9]، Hypervisor و یا سیستم عامل میزبان ، مجموعه کوچکی از کامپوننت‌هایی هستند که در یک محیط مجازی مورد نیاز هستند. انواع محیط‌های مجازی عبارتند از:

- مجازی سازی نوع اول

محیط‌هایی هستند که به آنها Full Virtualization گفته می شود که لایه مجازی با دو لایه سخت افزار و Hypervisor ارتباط دارد.

- مجازی سازی نوع دوم

این نوع هم Full Virtualization هست ولی با این تفاوت که به جای Hypervisor، لایه مجازی با سیستم عامل میزبان در ارتباط است.

۲,۲. انواع آسیب پذیری های محیط مجازی

علاوه بر اینکه استفاده از این تکنولوژی مزایای زیادی دارد ولی تهدیدات بیشماری علیه آن وجود دارد که برخی از آنها به شرح ذیل می‌باشد:

–Shared Clipboard

[8]- Virtual Machine
[9]-Virtual Memory Manager

–Keystroke Logging
–نظارت VM از طریق ماشین میزبان
–نظارت ماشین مجازی از طریق ماشین مجازی دیگر
–Backdoor های ماشین مجازی [۳].

۳. تهدیدات امنیتی موجود در رایانش ابری و راه حل کاهش آنها

رایانش ابری با وجود داشتن مزایای زیاد، همواره دارای تهدیدات امنیتی بیشماری برای اطلاعات درحال تبادل است که باعث می‌شود مشتریان از بهره بردن از مزایای ابر باز بمانند. برخی از این تهدیدات در ادامه آورده شده است.

۳,۱. تهدیدات داخلی

این نوع تهدیدات از درون سازمان‌های ارائه دهنده سرویس به وجود می‌آیند. به این معنی که مشتریان داده‌های مهم و حیاتی خود را در فضای ابر میزبان ذخیره می‌کنند. اگر کارکنان سازمان به علت داشتن دسترسی به این داده‌ها، از اطلاعات مشتریان سوء استفاده کنند، شرکت ارائه دهنده ابر شهرت خود را در بین مشتریان از دست خواهد داد [۴].

از روش‌های مقابله با این چالش می‌توان به اجرای دقیق مدیریت زنجیره تامین، شفافیت شیوه‌های مدیریتی، امنیت اطلاعات و وجود یک سیستم گزارش‌گیری از نقص‌های امنیتی برای جلوگیری از انواع حمله‌ها اشاره کرد.

۳,۲. تهدیدات خارجی

با وجود اینکه تهدیدات داخلی برای ارائه‌دهندگان ابر یک تهدید بزرگ است ولی تهدیدات خارجی هم می‌تواند تاثیر بسیار زیادی داشته و باعث بروز خسارت‌هایی به سیستم و فرآیندهای آن شود. نقاط ضعف یک سازمان ارائه دهنده می‌تواند راهی برای مهاجمان خارج از سازمان باز کرده و باعث حملات مخرب خارجی شود، به طور مثال مهاجمان می‌توانند از ضعف API[۱۰] ها و کانال‌های ارتباطی استفاده کرده و سازمان را مورد حمله قرار دهند.

برای حفاظت سازمان در برابر چنین تهدیداتی استفاده از فایروال‌ها و سیستم‌های تشخیص و پیشگیری از نفوذ بسیار ضروری است. همچنین پیاده‌سازی یک Honey Pot [۱۱] و استفاده از قانون AAA[۱۲] ضروری است.

۳,۳. کنترل دسترسی

در رایانش ابری داده‌های مشتریان در مکان ناشناخته‌ای که از دید کاربران پنهان است ذخیره می‌شود و مشتریان هیچ گونه کنترل و مدیریتی روی داده‌های حیاتی خود ندارند و هیچ گونه آگاهی از مکانیزم امنیتی که توسط ارائه دهنده پیاده‌سازی شده، ندارند. از دست دادن کنترل روی داده‌های حیاتی و سرویس‌های بحرانی و حساس می‌تواند در هر سازمانی اختلال ایجاد کند.

عدم کنترل روی داده‌های حساس از سوی مشتریان ممکن است باعث از دست رفتن داده‌ها شود. این امر موجب از بین رفتن نام تجاری و شهرت سازمان‌های ارائه دهنده ابر شود.

برای کاهش مشکلات کنترل دسترسی و افزایش دسترس پذیری و کارایی، ایجاد یک توافق نامه‌ای در سطح سرویس (SLA)[۱۳] بین سرویس دهنده و مشتری الزامی است.

همچنین استفاده از یک احراز هویت بسیار قوی و فرآیند مجوز دهی، منجر به کاهش این چالش می‌شود.

منظور از احراز هویت قوی این است که سازمان‌ها برای کاربران خود از روش Single Sign On استفاده کنند تا کاربران برای دسترسی به همه سرویس‌ها و برنامه‌های کاربردی مورد نظر در هر قسمت از محیط ابر از یک احراز هویت واحد استفاده کنند.

[10]- Application Program Interface

[10]- یک تکنولوژی که درون یک شبکه قرار می‌گیرد و هر نوع ارتباط با این تکنولوژی به منزله حضور یک خرابکار در شبکه است.

[12]- Authentication & Authorization & Accounting

[13]- Service Level Agreement

۳,۴. وقفه در سرویس دهی

ماهیت اصلی رایانش ابری ارائه سرویس است، هر گونه اختلال در ارائه سرویس می‌تواند منجر به قطع سرویس و از بین رفتن شهرت سازمان ارائه دهنده ابر شود.

اگر مهاجمان بتوانند به اعتبارنامه ورود سازمان سرویس دهنده و اعتبار نامه ورود مشتریان دسترسی پیدا کنند می‌توانند داده را تغییر داده، سرویس‌ها را مورد حمله قرار داده و آنها را متوقف کنند.

ازجمله حمله‌هایی که می‌توان در این چالش‌ها برشمرد، حمله‌های DOS ، DDOS، Phishing ، Froud و... است.

این تهدید در اثر وجود ثبت نام نسبتا ضعیفی است که در محیط رایانش ابری به وجود می‌آید که می‌تواند باعث حمله هکرها به سیستم شود. در واقع ثبت نام بدین معنی است که به هر مشتری برای دریافت سرویس‌ها یک حساب کاربری معتبر از سوی سرویس دهنده داده می‌شود.

یکی از راه‌حل‌های موجود برای کاهش این چالش، عدم به اشتراک‌گذاری حساب کاربری بین مشتریان یک ارائه دهنده است که با استفاده از یک احراز هویت چندعامله انجام می‌شود.

ارائه دهنده ابر باید بتواند دائما ترافیک شبکه مشتری را بازرسی کند و با یک سیستم پیشگیری از نفوذ بتواند از هر اقدام خرابکارانه‌ای جلوگیری کند [۴].

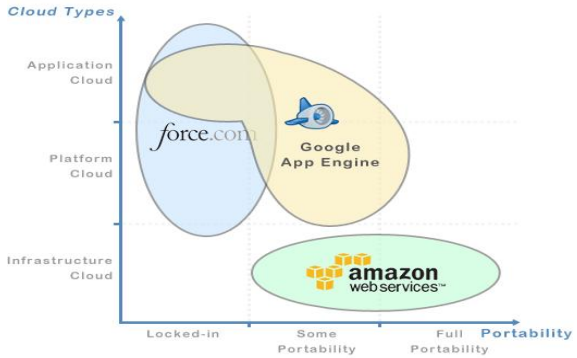
۳,۵. چند مستاجری[۱۴]

سرویس‌ها در ابر به کاربران متعددی ارائه می‌شوند. از این رو چند مستاجری مفهوم اصلی ابر است. ارائه دهنده، برنامه کاربردی و سخت افزار فیزیکی خود را برای اجرای ماشین مجازی مشتریان به اشتراک می‌گذارد. کاربران برای ارائه دهنده در حکم مستاجر هستند. هر ماشین در اختیار یک کاربر قرار می‌گیرد و این باعث بروز حمله ماشین‌های مجازی به همدیگر می‌شود. برای غلبه بر این مشکل می‌توان از راه حل‌هایی نظیر دفاع در عمق که همان دفاع از زیر ساخت مجازی ابر در لایه‌های مختلف است، استفاده کرد. در واقع در یک محیط ابری باید یک دفاع لایه بندی شده برای حفاظت از محیط وجود داشته باشد. رویکرد دفاع در عمق تضمین می‌کند که تهدیدات مجبور به عبور از بیش از یک لایه هستند. از این رو سرویس دهندگان می‌توانند تعدادی از تهدیدات را در مراحل اولیه و قبل از انتشار در محیط ابر شناسایی و مسدود کنند [۴].

۳,۶. قابلیت حمل

هر ارائه دهنده سرویس در ابر، برای تعامل با مشتریان خود یک سری قوانین خاص خود را دارد که مشتری بر اساس چنین قوانینی داده‌ها و برنامه‌های خود را نزد ارائه دهنده ذخیره می‌کند. از آنجا که همه سازمان‌های ارائه دهنده سرویس از یک استاندارد مشترک تبعیت نمی‌کنند؛ بنابراین امکان مهاجرت مشتریان از یک ارائه دهنده به ارائه دهنده دیگر در ابر امکان پذیر نیست که به این موضوع Lock in گفته می‌شود.

به عنوان مثال می‌توان مقایسه قابلیت حمل در بین سه ارائه دهنده Google، Amazon و Force را در شکل ۲ نمایش داد.



شکل ۲- مقایسه قابلیت حمل در بین سه ارائه دهنده

همانطور که در شکل ۲ نشان داده شده است قابلیت حمل درآمازون از نظر زیرساخت رایانش ابری از بقیه بیشتر می‌باشد.

برای افزایش قابلیت حمل در بین ارائه‌دهندگان لازم است که یک استاندارد جامع تعریف شود و تمامی ارائه دهندگان موظف به رعایت این استاندارد شوند.

۳,۷. انتقال اطلاعات

زمانی که مشتریان اطلاعات خود را در ابر منتقل می‌کنند، این اطلاعات برای سازمان ارائه دهنده سرویس قابل دسترسی است، از این رو ممکن است مورد سوء استفاده قرار گیرد. همچنین ممکن است این اطلاعات در حین انتقال در ابر توسط یک

[۱۴]- Multi-Tenancy

خرابکار که در حال کنترل ترافیک شبکه است به سرقت برود. بنابراین برای امنیت اطلاعات در حال تبادل دو روش وجود دارد: در روش اول از رمزنگاری اطلاعات استفاده می‌شود به این معنی که مشتری اطلاعات خود را با استفاده از الگوریتم‌های رمزنگاری رمز نموده و برای ارائه دهنده ارسال نماید. در روش دوم می‌توان از مکانیزم‌های امنیتی VPN یا SSH Tunneling استفاده نمود.

۳,۸. API های ناامن

ارتباط بین مشتریان و ارائه دهندگان ابر از طریق API ها انجام می شود. وظیفه API، تامین و مدیریت سرویس‌هایی است که قرار است در ابر ارائه شود. APIهای ضعیف می‌توانند سازمان‌های ارائه دهنده را در معرض تهدیدات امنیتی مختلفی مانند دسترسی ناشناس، مجوز نامناسب و ... قرار دهند[۵].
به منظور کاهش چنین مشکلاتی بهتر است از یک احراز هویت قوی و کنترل دسترسی مناسب استفاده شود.

۳,۹. رابط مدیریت دسترسی از راه دور

دسترسی مشتریان به سرویس‌ها در ابر از طریق رابط‌هایی در اینترنت انجام می‌شود و مجموعه بزرگی از منابع از این طریق در اختیار مشتریان قرار می‌گیرد. یک نقطه ضعف بسیار مهم در این زمینه، آسیب‌پذیری مرورگرهای وب است که می‌تواند تهدید جدی را در بر داشته باشد.
یک راه برای مقابله با این تهدید استفاده از پروتکل امن HTTPS برای ارائه دسترسی از راه دور است. راه دیگر بررسی نقاط آسیب‌پذیری مرورگرهاست و اینکه به طور مکرر باید مرورگرها به روزرسانی شوند [۴].
جدول ۱ مقایسه‌ای بین راه حل‌های موجود برای چالش‌های امنیتی را نشان می‌دهد.

جدول۱- مقایسه راه حل چالش های امنیتی

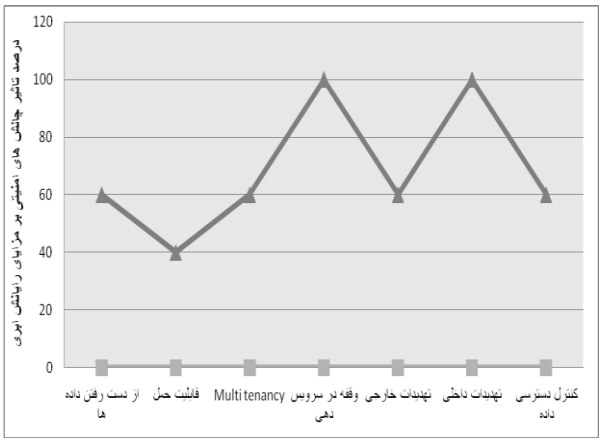
راه حل ها / چالش های امنیتی	مدیریت امنیت	سیستم گزارش گیری	فایروال	IDS & IPS	SLA	احراز هویت چندعاملی	دفاع درعمق	استانداره سازی	رمزنگاری	استفاده از پروتکل های امن	به روزرسانی مرورگرها
تهدیدات داخلی	✓	✓									
تهدیدات خارجی			✓	✓							
کنترل دسترسی					✓	✓					
وقفه در سرویس دهی			✓	✓		✓					
چندمستاجری							✓				
قابلیت حمل								✓			
انتقال داده						✓			✓	✓	✓
نامن API						✓				✓	✓
رابط مدیریت دسترسی از راه دور						✓				✓	✓

۴. مقایسه و ارزیابی تاثیر چالش‌های امنیتی بر مزایای رایانش ابری

همانگونه که بیان شد رایانش ابری یک روش جدیدی برای ارائه منابع محاسباتی است که دارای مزایا و معایب بسیاری است که در بالا به آنها اشاره شد.
چالش‌های امنیتی که در این مقاله مورد بررسی قرار گرفت می‌تواند بر روی مزایای رایانش ابری تاثیر منفی بگذارد. در جدول ۲ تاثیر این چالش‌ها مورد تحلیل و ارزیابی قرار گرفته است.

جدول ۲- تاثیر چالش‌های امنیتی بر مزایای رایانش ابری

چالش‌های امنیتی / پارامترهای ارزیابی	کنترل دسترسی داده	تهدیدات داخلی	تهدیدات خارجی	وقفه در سرویس دهی	Multi tenancy	قابلیت حمل	از دست رفتن داده ها
کیفیت سرویس	no	yes	no	yes	yes	no	yes
قابلیت اطمینان سرویس	no	yes	no	yes	no	no	no
کارایی سرویس	yes	yes	yes	yes	yes	yes	yes
دسترس پذیری سرویس	yes	yes	yes	yes	yes	no	no
قابلیت اعتماد و شهرت سرویس دهنده	yes	yes	yes	yes	no	yes	yes



شکل ۳- تاثیر چالش های امنیتی بر مزایای رایانش ابری

شکل ۳ نشان می دهد، چالش تهدیدات داخلی و وقفه در سرویس‌دهی دارای بیشترین تاثیر بر روی مزایای رایانش ابری می‌باشند.

۵. نتیجه گیری

رایانش ابری یک فضایی بزرگ و پیچیده شامل سخت‌افزارها و نرم‌افزارها و امنیت آن است. موفقیت یا شکست سرویس‌های

ابری به احساس اعتماد کاربران بستگی دارد . اعتماد به اینکه داده‌ها وفرآیندهایشان آیا در یک محیط امن و ایمن و با حفظ حریم خصوصی حفاظت می‌شود.

در این مقاله به حیاتی‌ترین بخش که حصول اطمینان از یک محیط امن است، اشاره شده که شامل یک دید پایه‌ای به سیاست‌های امنیتی سخت افزار و نرم افزار است.

در آینده انتظار می‌رود یک درجه بالایی از رایانش ابری وجود داشته باشد و این نکته حائز اهمیت است که حمله کننده‌ها به دلیل وجود داده‌ها و منابع بسیار زیاد در ابر همیشه یک تهدید جدی هستند .

مسئله مهم دیگر که در آینده باید بیشتر به آن توجه شود، استفاده از استانداردهای باز برای جلوگیری از مشکلات ناسازگاری و Lock-in است. به علاوه هنوز هیچ استاندارد امنیتی خاصی برای رایانش ابری وجود ندارد.

مراجع

[1] I. Bojanova, A. Semba, “Analysis of Cloud Computing Delivery Archtecture Models” , workshops of International Conference on Advanced Information Networking and Application, PP.453-458, 2011

[2] E. Mathise, “Security Challenges and Solutions in Cloud Computing”, Proc. 5th IEEE . Int. Conf. on Digital Ecosystems and Technologies,PP. 208-212, 2011

[3] Ronald L.Krutz, Russell Dean Vines, “Cloud Computing Security” Wiley Publishing, Inc, PP 153-165, 2010

[4] A. Behl ,“Emerging Security Challenges in Cloud Computing”, word congress on Information and Communication Technologies, PP. 217-222, 2011

[5] H. Tianfield, “Cloud Computing Archtectures” , 2011 IEEE International Conference on Systems, Man, and Cybernetics (SMC), PP.1394-1395, 2011

[6] K. Povic, Z. Hocenski, “Cloud Computing Security issues and Challenges”, Proceedings of the 33rd International Convention, PP.344-349, 2011

[7] A. Tripathi, A. Mishra, “Cloud Computing Security Consideration”, 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), PP.1-5, 2010