دانشگاه بوعلی سینا
گروه کامپیوتر

پروژه ی پایانی درس سیستم های توزیعی

عنوان

امنیت در رایانش ابری

نگارش
نرگس رضایی
محمد پیشدار

استاد راهنما
دکتر مهدی سخایی نیا

شهریور 1395


بسم الله الرحمن الرحيم

چکیده

رایانش ابری یک فناوری نوظهور در علم رایانه و ارتباطات می باشد . و به دلیل ماهیت وجود اطلاعات کاربران در سازمان ارائه دهنده ی این فناوری ، امنیت اطلاعات کاربران یکی از چالش ها و موانع اصلی گسترش استفاده از این فناوری می باشد . هدف از این پژوهش بررسی چالش ها و نگرانی های امنیتی موجود و راه حل های ارائه شده در جهت رفع این نگرانی ها می باشد . در این پژوهش ابتدا مفهوم رایانش ابری ، ساختار ، انواع آن سپس چالش ها و نگرانی های امنیتی مطرح در این زمینه شرح داده شده است .در ادامه راه حل های ارائه شده برای رفع این نگرانی ها بررسی شده است . با بررسی این نگرانی ها و راه حل های ارائه شده می توان به این نتیجه رسید که هنوز نگرانی های امنیتی در رایانش ابری وجود دارند و به طور کامل حل نشده اند اما با افزایش امنیت در رایانش ابری معادله بین مزایای استفاده از رایانش ابری و عدم استفاده به علت نگرانی های امنیتی تغییر خواهد کرد و حرکت به سوی استفاده گسترده تر از این فناوری صورت می پذیرد .

واژه های کلیدی:

رایانش ابری ، امنیت رایانش ابری ، تهدیدات امنیتی رایانش ابری ، اقدامات امنیتی رایانش ابری ، مجازی سازی ، ذخیره سازی

فهرست عناوین

صفحه

1
فصل اول
مقدمه

1.1 مقدمه

محدودیت های سخت افزاری و نرم افزاری همیشه یه عنوان یکی از موانع و چالش ها ی سازمان های حوزه فناوری اطلاعات و ارتباطات بوده است . در سال اخیر دانشمندان حوزه ی فناوری اطلاعات و ارتباطات به فکر پیاده سازی ایده ی سرویس های شهری از جمله گاز ، برق و آب در حوزه ی رایانه ها افتاده اند . همانطور که کاربران سرویس های شهری بدون اینکه بدانند سرویس آنها از کجا و به چه شکل تامین می گردند ، تنها از طریق خط لوله کشی و یا پریز برق سرویس خود را دریافت می نمایند ؛ کاربران و سازمان ها در حوزه ی فناوری اطلاعات نیز می توانند از طریق بستر شبکه نیاز های خود را رفع نمایند و به ازای مصرف خود هزینه پرداخت نمایند . این ایده در حوزه ی فناوری اطلاعات و ارتباطات تحت عنوان مفهوم رایانش ابری مطرح می شود . رایانش ابری بر پایه شبکه های کامپیوتری بنا شده است و مکانیزمی است که به کاربران امکان انجام محاسبات پیچیده و سنگین را در هر زمان و مکانی می دهد بدون اینکه کاربران نیاز به تهیه نرم افزار و یا سخت افزار پر هزینه داشته باشند . این مکانیزم به بسیاری از نیازهای کاربران پاسخ داده است و خدمات زیادی را برای آنها فراهم کرده است . با معرفی مفهوم رایانش ابری به جهانیان ، متخصصان در ابتدا ضعف عمده این فناوری را امنیت آن دانستند . این ضعف باعث عقب نشینی بسیاری از سازمان ها در برابر این فن آوری می گردد . کاربران ، اطلاعاتی از زیر ساخت و مکانیزم های فنی ابر ندارند و حتی شماری از مدیران بین المللی حاضر به سپردن اطلاعات مهم خود به شرکت های ارائه دهنده ی ابر نیستند . در رایانش ابری هر کاربر لازم می داند که بداند داده ها کجا قرار می گیرند ، آیا حق دسترسی به داده ها حفاظت شده است ، آیا ارائه دهنده سرویس ابری از مقررات لازم پیروی می نماید و ... . پژوهش های انجام شده در دانشگاه IDCI کانادا حاکی از

آن است که درصد زیادی از مدیران IT امنیت را مهمترین چالش پیش روی استفاده از ابر ذکر کرده اند . در سال های اخیر تحقیقات و پیشرفت های زیادی برای رفع نگرانی های امنیتی صورت گرفته است که در این پژوهش ضمن معرفی ابر به برخی از این چالش ها و راه حل های مطرح شده برای آنها پرداخته می شود .

در فصل دوم این پژوهش به معرفی رایانش ابری و سرویس دهندگان آن پرداخته ایم . همچنین انواع رایانش ابری و مزایا و معایبی که دارد به اختصار بیان شده است . در فصل سوم امنیت رایانش ابری مورد بحث قرار می گیرد . در این فصل ابتدا در رابطه با امنیت ابر صحبت شده است ، سپس تهدیدات امنیتی ای که برای ابرها وجود دارد به طور مختصر توضیح داده شده است . در مقابل این تهدیدات اقدامات امنیتی ای نیز بیان شده که به شرح آنها پرداخته ایم . بخش های بعدی این فصل شامل ایده های مطرح شده برای امنیت ابر در حوزه های مجازی سازی ابر و ذخیره سازی داده ها می باشد .

2
فصل دوم
رایانش ابری

1.2 رایانش ابری چیست ؟

ابر اساسا می تواند به بسیاری از نیاز های کاربران (پرسنل سازمان یا کاربران عمومی) پاسخ داده و خدمات مختلف را برای آنان فراهم نماید [2]. مؤسسه ملی فناوری و استانداردها [1] یک تعریف از این فناوری ، که پوششی کلی از جنبه های مختلف را نمایش می دهد، ارائه داده است : رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع محاسباتی قابل مثل شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها ، که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا کمترین نیاز به دخالت مستقیم فراهم‌کننده ی سرویس ، به سرعت فراهم شده یا آزاد گردد [3] . همچنین می توان رایانش ابری را چنین نیز تعریف کرد : دسترسی به نرم افزار اجرا شده بر روی سخت افزاری که متعلق به بعضی از فراهم کنندگان سرویس است و هزینه ی این سرویس ، به ازای هر آنچه که استفاده می شود ، پرداخت می شود [2].

مهم ترین هدفی که یک ابر می تواند داشته باشد ، نگهداری اطلاعات در مکانی خارج از محیط فیزیکی است . این داده ها به صورت توزیع شده بر روی مراکز ذخیره سازی رایانش ابری ذخیره می شوند . مراکز ذخیره سازی مجموعه ای از سرورها هستند که به انواع دستگاه های ذخیره سازی فایلی و بلوکی تقسیم می شوند . بنابراین در محاسبات ابری ، داده ها کمتر بر روی سرور ها و کامپیوتر های شخصی قرار می گیرند .

[1] NIST

2.2 انواع رایانش ابری

انواع مختلفی از ابرها وجود دارد که شما می توانید بسته به نیازی که دارید از آنها استفاده کنید. ابرها در پردازش ابری بر اساس نوع سرویس و تعاملی که دارند به بخش های زیر تقسیم می شوند :

- ابر عمومی[1] : ابرعمومی توسط هر مشتری که به اینترنت دسترسی دارد قابل دسترسی است و مشتری از این طریق به فضای ابر متصل می شود [4].در واقع این نوع ابر ، رایانش ابری را با یک معنای سنتی بیان می کند. معمولا کاربرانی که از سرویس های ابر عمومی استفاده می کنند ، بصورت ماه به ماه مبالغی را به ازای پهنای باند مصرفی و سرویسی که دریافت می کنند پرداخت می کنند. کاربران در چنین حالتی نیازی به خریداری سخت افزارها و دستگاه های ذخیره سازی اطلاعات و سایر موارد ندارند و این در واقع همان ماهیتی است که مقیاس پذیری ابر را نشان می دهد . در صورت نیاز به سرویس و خدمات بیشتر ، بلافاصله از سایر منابع ، خدمات مورد نیاز کاربر تامین می شود. ابر عمومی برای استفاده عمومی می باشد و جایگزین یک گروه صنعتی بزرگ است که مالک آن یک سازمان بوده و فروشنده ی سرویس‌های ابری است .
- ابر خصوصی[2] : این ابر یک نوع رایانش ابری است که که برای یک گروه ویا سازمان با محدودیت های خاص ایجاد شده است [4] . در واقع توسط یک سازمان به خصوص ایجاد شده است که تنها برای یک مشتری کار می کند و برای استفاده داخلی می باشد .
- ابر گروهی[3] : این ابر در جایی به وجود می آید که چندین سازمان نیاز مشترک داشته باشند [4] . به

[1] Public Cloud

[2] Private Cloud

[3] community cloud

عبارتی ، این ابر به دنبال این است که با به اشتراک گذاشتن زیرساخت ، از مزایای رایانش ابری بهره‌مند گردد .

- ابر ترکیبی[1] : این ابر ترکیبی از ابرهای عمومی ، خصوصی و یا گروهی می باشد [4]. یک ابر ترکیبی یا ابر آمیخته ، متشکل از چندین ارائه دهندهٔ داخلی و یا خارجی است که گزینهٔ مناسبی برای بیشتر مؤسسات تجاری می‌باشد .

3.2 مزایا و معایب محاسبات ابری

ابر به عنوان یک ایده ی نو و الگویی تازه برای عرضه ، مصرف و تحویل خدمات رایانشی ، مزایای فراوانی برای مصرف کنندگان دارد . از جمله مزایای رایانش ابری :

- عملکرد بهتر : با توجه به اینکه هیچ گونه برنامه و یا فایلی روی کامپیوتر محلی بارگذاری نمی شود ، بنابراین کاربر تاخیری را مشاهده نمی کند [4].
- هزینه کم : این نقطه یکی از مزایای مالی محاسبات ابری است. پردازش با استفاده از محاسبات ابری ، بدون نیاز به خرید تجهیزات قدرتمند و گران قیمت انجام می شود . همچنین هزینهٔ توسعهٔ نرم‌افزاری را کاهش داده و فرایند را مقیاس پذیرتر می‌نماید. رایانش ابری ، مشتریان را از هزینه های سخت‌افزاری، نرم‌افزار ی و خدمات و همچنین از درگیری با نصب و نگهداری نرم‌افزارهای کاربردی ، آزاد می کند [4] .
- به روز رسانی خودکار نرم افزار : با استفاده از محاسبات ابری ، کاربر نگرانی ای در رابطه با به روز رسانی و ارتقا نرم افزار ندارد . حتی این امر هیچ هزینه ی اضافی را به او تحمیل نمی کند [4] .

[1] Hybrid Cloud

- ظرفیت ذخیره سازی بی حد : ابر فضای ذخیره سازی نامحدودی را به کاربر ارائه می دهد و همچنین کاربر می تواند در هر زمانی این فضا را با هزینه ی بسیار کمی افزایش دهد [4] .
- افزایش امنیت داده ها : همه ی داده ها به صورت متمرکز در ابر ذخیره می شوند و هیچ نگرانی ای در رابطه با خرابی دیسک وجود ندارد . بنابراین به دلیل تمرکز داده‌ها و منابع امنیتی بیشتر و پیچیده‌تر ، امنیت افزایش می‌یابد [4] .
- دسترسی آسان در هر جا : کاربر می تواند در هر نقطه به اسناد خود دسترسی داشته باشد . به عبارتی کاربران می‌توانند در هر مکانی و با هر دستگاهی (مثل کامپیوتر شخصی و یا تلفن همراه) به وسیلهٔ یک مرورگر وب از راه اینترنت به سامانه‌ها دسترسی داشته باشند [4] .

محاسبات ابری نیز همانند بسیاری از نوآوری های دیگر ، علاوه بر مزایایی که دارد ، شامل معایبی نیز می باشد . این معایب به اختصار شامل موارد زیر است :

- نیاز به اتصال به اینترنت برای استفاده از محیط ابری لازم است .
- با اتصال به اینترنت با سرعت کم ، استفاده از محیط ابری مشکل می شود .
- حتی اگر کاربر اتصال سریع به اینترنت داشته باشد، ممکن است در محیط ابر دچار تاخیر شود .
- داده های کاربر به طور صد در صد در ابر ذخیره میشود . در واقع یک نوع چالش حریم خصوصی و امنیت داده وجود دارد .

4.2 سرویس دهندگان اصلی رایانش ابری

تعداد خدمات ابر هر روزه در حال افزایش است. این خدمات می تواند ارائه امکانات تهیه نسخه پشتیبان باشد و یا ارائه امکانات دسترسی از راه دور .

در این قسمت به تشریح مختصر سه نوع از خدمات ابر می پردازیم .

سرویس‌های برنامه ی کاربردی ابری[1] یا نرم‌افزار به عنوان سرویس (SAAS) ، نرم افزاری که میزبانی آن بر عهده ی فراهم کننده ی سرویس ابر می باشد را فراهم می کند . این نرم افزار از طریق مرورگر وب قابل دسترسی است و همه چیز توسط سرویس دهنده ی ابر کنترل می گردد . بر خلاف نرم افزار سنتی در این روش می توان نرم افزار را بین کاربران به صورت اجاره ای به اشتراک گذاشت و کاربران تنها برای میزانی که استفاده دارند ، هزینه پرداخت نمایند [2] . می توان به این صورت بیان کرد که یک کپی از نرم افزار خریداری می شود که به روی دستگاه کاربر نصب می شود . نمونه هایی از ارائه دهندگان که از سرویس saas استفاده می کنند فیس بوک ، salesforce.com و ... می باشند [4] .

- سرویس‌های زیرساخت ابری[2] یا زیرساخت به عنوان سرویس (IaaS)، این زیرساخت قابلیت های پردازشی (نظیر cpu ، حافظه ، شبکه و ..) را توسط ابر ، برای کاربران فراهم می کند . کاربر زیرساخت ابر را مدیریت نخواهد کرد و این مدیریت توسط فراهم کننده ی سرویس انجام می شود . همچنین مشتری تنها در سطح سیستم عامل کنترل را انجام می دهد . در این سرویس زیر ساخت بدون در گیری کاربر با پیچیدگی های اساسی زیر ساخت ، به صورت بهینه در اختیار وی قرار می گیرد [2] . کاربران به جای خرید سخت‌افزار و نرم‌افزار و فضای مرکز داده و یا

[1] Software As A Service

[2] Infrastructure as a Service

تجهیزات شبکه، همهٔ این زیر ساخت‌ها را به صورت یک سرویس کامل می‌خرند.

- سرویس‌های بستر ابری[1] یا بستر به عنوان سرویس (PaaS) ، بستر را به صورت مجموعه ای از محیط های پیاده سازی یا محیط مجازی ، با استفاده از مرورگر وب فراهم می کند . برنامه نویسان نرم افزار می توانند بدون نصب محیط برنامه نویسی ، برنامه ی خود را در محیط ابر به راحتی گسترش بدهند . استفاده کننده ، هیچ مدیریت و کنترلی بر روی زیر ساخت ابر ندارد و تنها می تواند پیکر بندی و محیط برنامه نویسی را کنترل نماید [2]. سرویس بستر ابری ، استقرار برنامه‌های کاربردی و مدیریت لایه‌های نرم‌افزاری و سخت‌افزاری زیرین را بدون هزینه و پیچیدگی خرید آسان می‌سازد . نمونه هایی از ارائه دهندگان برنامه های کاربردی با استفاده از PaaS عبارتند از : Microsoft Azure ، Google app engine و ... . [4]

[1] Platform as a Service

3
فصل سوم
امنیت رایانش ابری

1.3 امنیت ابر

در قسمت های قبل ، ابر به عنوان یکی از موضوعات جدیدی که بسیار مورد توجه عموم مردم قرار گرفته است ، بیان شد . علاوه بر این به این موضوع نیز اشاره شد که داده ها در رایانش ابری به صورت توزیع شده در مراکز ذخیره سازی رایانش ابری ، ذخیره می شوند . با این وجود یکی از مشکلات عمده ای که رایانش ابری با آن مواجه است ، چگونگی حفاظت از داده ها در این محیط و برقراری امنیت در فرایندهای کاربران است . اگر چه امنیت مطلق ، یک آرزوی دست نیافتنی است و برای تامین امنیت در شبکه ها و رایانه ها هیچ تضمینی وجود ندارد ، اما با این حال ، امنیت داده ها و کارایی برنامه های کاربردی ای که روی ابر انجام می شود ، برای کاربران از اهمیت ویژه ای برخوردار است .

نگرانی های امنیتی در رایانش ابری ناشی از عدم کنترل و یا کنترل کم کاربر است . نبود اطمینان و اعتماد نیز عامل افزایش این نگرانی ها می باشد چرا که اعتماد بحثی است که نگرانی های امنیتی در رایانش ابری را تشدید می کند و این موضوع به طور مستقیم با صحت و اعتبار فراهم کننده ی سرویس مرتبط می باشد . اجاره دادن همزمان منابع نیز می تواند باعت ایجاد نگرانی گردد . در ابر یک کاربر ممکن است تمام سرور را در اختیار خود ببیند ، ولی در باطن چنین نیست و منابع ممکن است در اختیار تعداد زیادی کاربر قرار بگیرد [2] .

کاربرانی که از محاسبات ابری استفاده می کنند ، بایستی از تهدیدات امنیتی ای که در چنین شبکه هایی می تواند رخ دهد، آگاه باشند . این به این دلیل است که رایانش ابری به منظور ارائه ی دسترسی به منابع مورد نیاز از شبکه استفاده می نماید ، بنابراین هر گونه خطر امنیتی ای که ممکن است در یک شبکه رخ دهد ، احتمال آن برای رایانش ابری نیز بایستی در نظر گرفته شود . از دیدگاه شبکه ای تحقیقات گسترده و نسبتا

جامعی برای تامین امنیت محاسبات ابری صورت گرفته است . علاوه بر این ، برای تامین محاسبات ابری لازم است مسائل امنیتی و فن آوری های مرتبط در تمام زمینه های زیر ساختی رایانش ابری در نظر گرفته شود . این مسائل امنیتی که در رابطه با زیر ساختها می باشد تنها محدود به شبکه نبوده ، بلکه در رابطه با پایگاهای داده ، سیستم عامل ها ، مجازی سازی ، برنامه ریزی منابع ، مدیریت تراکنش ها ، توازن بار ، کنترل همزمانی و مدیریت حافظه ها نیز می باشد [5].

نگرانی کاربران در رابطه با امنیت محاسبات ابری بیشتر مربوط به محل ذخیره سازی داده می باشد . علاوه بر این مایلند بدانند چه کسی و یا کسانی به این داده ها دسترسی دارند . بنابراین می توان گفت مهمترین جنبه امنیتی محاسبات ابری مربوط به محرمانگی داده ها و حفظ حریم خصوصی می باشد . وقتی داده کاربر در اختیار ارائه دهنده ی فضای ابری قرار می گیرد ، این داده می تواند بدون اطلاع کاربر و به وسیله ارائه دهنده ی سرویس مورد دسترسی قرار بگیرد و یا حتی دچار تغییر شود .

تمامی این مسائل ، امنیت رایانش ابری را به عنوان یکی از چالش های مهم بیان می کند .

2.3 تهدیدات امنیتی و اقدامات امنیتی در رایانش ابری

با توجه به اینکه محاسبات ابری یکی از مدل های محاسباتی مفید برای ارائه دهندگان خدمات ، ارائه دهندگان ابر و مصرف کنندگان ابر است و نیز دارای مزایای بی شماری است ، اما توجه به اینکه امنیت مهمترین موضوعی است که به منظور استفاده گسترده از رایانش ابری باید مورد توجه قرار گیرد، ارائه دهندگان رایانش ابری را ملزم می کند که چالشهای امنیتی متداول را شناسایی کنند . علاوه بر این آنها باید بتوانند

سامانه های ارتباطی پیشین را برطرف نموده و همزمان با آن به مباحث دیگری که توسط الگوی رایانش ابری معرفی میگردد، بپردازند . برخی از تهدیدات امنیتی ، برای اطلاعات در حال تبادل که باعث می شوند مشتریان از بهره بردن از مزایای ابر باز بمانند عبارتند از:

- تهدیدات داخلی[1] : همان طور که از نام این تهدید پیداست ، از درون سازمانها به وجود می آیند . بسیاری از تهدیدات امنیتی از این نوع تهدید هستند . این تهدید برای بسیاری از مشتریان و مصرف کنندگان ابر ممکن است ایجاد شود . مشتریان داده های مهم خود را در فضای ابر میزبان ذخیره میکنند و در صورتی که کارکنان سازمان از اطلاعات مشتریان سوء استفاده کنند، شرکت ارائه دهنده ابر اعتبار خود را در بین مصرف کنندگانش از دست خواهد داد .[7]
- حملات مخرب خارجی[2] : اطلاعات محرمانه به طریقی که محو شده و تغییر شکل داده اند ، می بایستی منتشر شوند ، چرا که انتشار واضح داده امنیت آن را به خطر می اندازد . تهدیدات خارجی از جمله مسائل مربوط به هر سازمان است و از جمله چالش های به روز در زیرساخت ابر می باشد . این نوع تهدید می تواند برای ارائه دهندگان ابر تهدید بزرگی باشد و باعث بروز خسارتهایی به سیستم و فرآیندهای آن شود . نقاط ضعف سازمان ارائه دهنده این امکان را به مهاجمان خارج از سازمان می دهد که راهی پیدا کرده و باعث حملات مخرب خارجی شود . ممکن است تهدیدات خارجی به اندازه ی تهدیدات داخلی مضر نباشند اما با این وجود نمی توان از آنها چشم پوشی کرد چرا که با اتفاق افتادن این امر به صورت طولانی ، سیستم مشتریان خود را از دست می دهد [7]. اگر کاربری که در حال استفاده از منابع ابر هست ، کاربری

[1] Insider Threats

[2] Outside Malicious Attacks

خرابکار باشد ، می تواند به سرور یا داده های سایر کاربران حمله نماید [2] .

- از دست رفتن داده[1] : یک سازمان در مواقعی که اطلاعات خود را به ابر منتقل می کند ، انتظار همان جامعیت داده و امنیتی را از ابر دارد که خود سازمان آن را برای خود فراهم کرده بود . به عبارتی ،بایستی در ابر از دسترسی اشخاص غیز مجاز به داده های حساس جلوگیری شود . می توان گفت ابرها چند مستاجری[2] هستند به این معنی که سرویس ها در ابر به کاربران متعددي ارائه می شوند . بنابراین کنترل دسترسی در حدی نیست که خود سازمان برای خود ایجاد می کرد و ممکن است پدیده ی گم شدن داده ها و اطلاعات و یا انشار آنها اتفاق بیفتد [7] .
- اختلال در سرویس دهی[3] :محیط ابر مسئول امنیت مشتری و سازمان و نیز حفظ اطلاعات آنها می باشد . هر سازمان و سرویس دهنده دارای یک گواهی ورود می باشد . گواهی ورود برای هر مشتری در حین عمل ثبت نام صادر می گردد . در صورتی که مهاجم بتواند به گواهی ورود سازمان سرویس دهنده و مشتری دسترسی پیدا کند می تواند داده ها را تغییر داده و یا سرویس ها را مورد حمله قرار دهد که این امر باعث از دست دادن مشتریان سازمان و تضعیف روحیه کارکنان سازمان خواهد شد . هدف اصلی که رایانش ابری دنبال می کند ارائه سرویس می باشد . بنابراین هرگونه نقض در ارائه یک سرویس باعث قطع شدن سرویس و از بین رفتن اعتبار سازمان خواهد شد . این نوع تهدید به علت ثبت ضعیف مشتری است که راه حمله هکر را باز می کند [7] .

[1] Data Loss

[2] multi tenant

[3] Service Disruptions

- چند مستاجری[1] : یکی از ویژگی های بارز محاسبات ابری چند مستاجری است و برای ارائه دهندگان ابر یک مزیت محسوب می شود . این ویژگی محدودیت های امنیتی مربوط به خود را دارد . چند مستاجری مفهوم اصلی ابر است چرا که سرویسها در ابر به کاربران متعددی ارائه میشوند . کاربران برای ارائه دهنده در حکم مستاجر هستند . ارائه دهنده برای اجرای ماشین مجازی مشتریان ، برنامه کاربردی و سخت افزار فیزیکی خود را به اشتراک میگذارد . هر ماشین در اختیار یک کاربر قرار میگیرد و این باعث بروز حمله ی ماشینهای مجازی به همدیگر میشود[7] . در ابر یک کاربر ممکن است تمام سرور را در اختیار خود ببیند . ولی در باطن چنین نیست . و منابع ممکن است در اختیار تعداد زیادی کاربر قرار بگیرد بنابراین ، اجاره همزمان منابع نیز می تواند باعث ایجاد نگرانی گردد [2].

چندین اقدام امنیتی برای امنیت در پردازش ابري پیشنهاد شده است که ما در این بخش به اختصار به تشریح این خدمات می پردازیم . هر يك از اين خدمات، شامل تكنيك هاي مختلف براي تقويت امنيت در محيط ابري مي باشند .

- مجازي سازي[2] : هر كاربري مي تواند از يك محيط كاملاً جدا و مجازي شده استفاده كند [6] .
- شبكه خصوصي مجازي[3] (VPN) : تبادل داده ها بين ارائه دهندگان ابر و كاربران با استفاده از يك VPN امن مي باشد [6] .

[1] Mutlitenancy

[2] Virtualization

[3] Virtual Private Network

- فدرال هويت[1] : اين توانايي را دارد كه در سراسر حوزه هاي امنيتي با استفاده از اظهارات يك ارائه دهنده ، امضای ديجيتالي ايجاد كند [6] .
- خدمات سياسي[2]: تعريف سياست هاي ارزيابي تصميم گيري براي ارائه خدمات در ابر است كه به عواملي مانند قابليت اطمينان، امنيت و ... بستگی دارد [6] .

در بين اقدامات مطرح شده بالا ، مجازي سازي كليدي براي فعال كردن محيط در محاسبات ابري است در يك محيط چند كاربر مي توانند فرآيندهاي مربوط به سازمانها را انجام دهند . مشكلي كه در برنامه هاي كاربردي و يا سيستم عامل مي تواند منجر به نقض انزوا شود ، اختصاص جداگانه ماشين هاي فيزيكي و يا ماشين هاي مجازي جداگانه به سازمان هاي متعدد است . يكي از نياز هاي ضروري ارائه دهنده ابر كشش سريع است ، جايي كه منابع مي تواند به آن اضافه يا حذف شود، كه بستگي به نوع تقاضاي سازمان و مشتري دارد. ارائه دهندگان خدمات ابري مي توانند توسط سرورهاي مجازي جديد ، دستگاه هايي را اضافه يا حذف كنند . يكي ديگر از استفاده هاي مجازي قابل حمل بودن آن است . انتقال ماشين هاي مجازي از يك دستگاه فيزيكي به دستگاه ديگر هنگامي كه كار تعمير و نگهداري مورد نياز است ، به آساني انجام مي شود . سازمان ها ممكن است راه حل هايي براي امنيت مجازي سازي در ابرهاي عمومي ارائه دهند كه مي توانند از نرم افزارهايي بر روي ماشين مجازي به منظور افزايش حفاظت و حفظ تماميت رعايت سرورها و برنامه هاي كاربردي استفاده كنند . برخي از آنها عبارتند از فايروال tسيستم هاي تشخيص نفوذ وپيشگيري ، نظارت بر تماميت ، ورود به سيستم براي بازرسي و درون گرايي ايمن.

- فايروال ها ، يك سيستم طراحي شده براي جلوگيري از دسترسي غير مجاز از يك شبكه خصوصي است كه با كاهش

[1] Federated Identity

[2] Policy Services

سطح حمله به يك سرور مجازي در محيط هاي ابري رايانه كمك كند .استقرار فايروال بر روي VM با سياست هاي امنيتي سازمان، ممكن است انزواي ماشين مجازي، دستيابي به فيلتر كردن داده ها در سطح پورت ها، تفكيك داده ها براي تجزيه و تحليل تمام پورتكل هاي مبتني بر IP ،انواع قالب و غيره را پوشش دهد. از حملاتي مانند DOS مي تواند جلوگيري كند. فايروال ها همچنين براي تنظيم سياست هاي مختلف رابط هاي شبكه بكار مي روند[6]. در بخش 3.3 به تشریح روشی می پردازیم که به صورت ترکیبی از فایروال و VPN به بررسی امنیت ابر می پردازد .

- تشخيص نفوذ و پيشگيري (IPS/IDS) ، مي تواند آسيب پذيري هاي تازه كشف شده در هر دو برنامه كاربردي و سيستم عامل در حال اجرا در VM را تشخيص دهد. اين حفاظت در برابر سوء استفاده از تلاش براي سازش ماشين مجازي را فراهم مي آورد IPS/IDS.هايي هستند كه براساس تكنيك هاي هوش مصنوعي بوجود آمده اند كه ممكن است در مورد آسيب پذيري هاي جديد بصورت پويا عمل كند [6] .

- نظارت بر تماميت ، شامل فايل هاي نظارت، سيستمي و رجيستري براي تغييرات است. فايل هاي نرم افزاري و فايل هاي سيستم بحراني را مي توان براي تشخيص تغييرات مخرب و غير منتظره بكار برد كه مي تواند بين منابع محاسباتي و سيگنالهاي مانيتور شده سازش ب . رقرار كند يكپارچگي نرم افزارهاي مانيتور شده بايد در سطح ماشين مجازي اعمال شود[6] .

- ورود به سيستم براي بازرسي ، ابر را قادر مي سازد تا رفتارهاي مشكوك را تشخيص دهد . بازرسي كردن ، براي جمع آوري logهاي مربوط به سيستم عامل و برنامه هاي كاربردي و تجزيه و تحليل آنها براي حوادث امنيتي صورت می گيرد . با اين كار ، استخراج كارآمد از حوادث امنيتي مرتبط اين فايل ها ، به درستی انجام می شود . فايل log مي تواند به يك سيستم امنيتي مستقل و يا اطلاعات امنيتي و

مدیریت رویدادهای سیستم (SIEM) و یا سرور لاگینگ متمرکز براي تجزیه و تحلیل ، فرستاده شود . این نکته حائز اهمیت است که نظارت بر یکپارچگي و قابلیت ورود به بخش بازرسي باید در ماشین مجازي استفاده شود[6].

- درون گرایي ایمن راه حلی است که برای تامین امنیت ابر ارائه شده است . در محاسبات ابري ممکن است تصاویر از یك ابر به دیگري حرکت کند ، یك راه حل مؤثر این است که سیستم عامل مهمان در هر یك از ماشین هاي مجازي اجرا شود و امنیت سیستم عامل مهمان بدون تکیه بر قابلیت هاي سیستم عامل مهمان بررسی شود . این راه حل ، درون گرایي امن است[6] .

3.3 ارائه روش امنیتی با استفاده از فایروال و VPN

چاندراشکار[1] و همکاران [5] تاثیر فایروال و VPN را برای امنیت ابر بررسی کردند . هدف از این سیستم ، ارائه اطلاعات امن به ابر و نیز دریافت اطلاعات امن از ابر می باشد . از جمله فناوری های استفاده شده برای ارائه امن اطلاعات ، VPN می باشد . با استفاده از VPN ، زیر شبکه های خصوصی و امن می توانند به راحتی استفاده شود . این قاعده به طور گسترده ای در شبکه های سیمی محلی[2] ، شبکه های بی سیم محلی[3] و شبکه های دسترسی از راه دور اعمال می شود . VPN با کمک پروتکل امنیتی اینترنت[4] پیاده سازی می شود . این امر می تواند به عنوان یک روش مناسب برای پیاده سازی VPN در نظر گرفته شود . پروتکل امنیتی اینترنت و VPN مورد تجدید نظر قرار گرفته و به روشی مناسب پیاده سازی شده اند تا بتوانند

[1] A. M. Chandrashekhar

[2] LAN

[3] WLAN

[4] IPsec

استاندارد قوی امنیتی با میزان قابل قبولی از محرمانگی داده ها ، احراز هویت و کنترل دسترسی صرف نظر از رسانه انتقال را فراهم نمایند . فایروال به طور پیوسته با VPN مورد استفاده واقع شده است . فایروال یک سیستم فیلترینگ بسته های داده می باشد که بین شبکه های داخلی و جهان خارج قرار گرفته است . دلیل استفاده از فایروال به همراه VPN این است که برای سالیان طولانی فایروال ها در شبکه های بزرگ عمومی مورد استفاده واقع شده است و مکان آغازین مهمی در توسعه ی استراتژی های امنیتی بوده اند و رایانش ابری نیز می تواند به عنوان یک شبکه عمومی در نظر گرفته شود .

این پژوهش شامل تعدادی سناریو است که کارایی و عملکرد سیستم را در حالات مختلف مورد بررسی قرار می دهد . رایانش ابری با VPN و بدون VPN پیاده سازی شده است و تاثیر فایروال با VPN در سیستم برای تامین امنیت ابر در سناریو های مختلف آنالیز و تحلیل می شود . هر سناریو با سه نوع برنامه کاربردی انتقال فایل[1] ، مرور وب[2] و برنامه های کاربردی پست الکترونیک ضمیمه شده است . در سناریو ها ، دو سرور به نمایندگی از دو دپارتمان قرار دارد . تاثیر فایروال و VPN بر رایانش ابری از نقطه نظر توان خروجی ، بار تاخیر و ترافیک دریافتی مورد بررسی قرار گرفته است .

نتایجی که ازین تحقیقات صورت گرفته داده شده است به صورت زیر می باشد :

- ادغام شبکه خصوصی مجازی VPN با فایر وال در رایانش ابری توان عملیاتی را کاهش می دهد . به این علت که تعداد بیت های منتقل شده در هر ثانیه کمتر از تعداد بیتهای منتقل شده در رایانش ابری بدون VPN است چون VPN همراه فایروال به سرور اجازه ی هر دسترسی را نخواهد داد .

[1] FTP

[2] HTTP

- تاخیر در سیستم بدون VPM کمی بیشتر از تاخیر در سیستم با VPN است .
- هیچ ترافیک دریافتی و ارسالی برای برنامه پست الکترونیکی در رایانش ابری با فایروال بدون VPN وجود ندارد .چون فایروال مانع هر گونه دسترسی پست الکترونیکی به سرور خواهد شد و وجود VPN در سیستم به ایستگاهای کاری ویژه اجازه خواهد داد که به سرور دسترسی پیدا کنند .
- در برنامه های مرورگر وب ، ترافیک ارسالی و دریافتی در رایانش ابری با VPN و بدون VPN وجود خواهد داشت چراکه VPN و فایروال فقط از دسترسی به سرور برای برنامه پست الکترونیک و نه سایر برنامه های کاربردی وب جلوگیری می کند .

4.3ارئه روش امنیتی برای سرویس های ذخیره سازی در محاسبات ابری

داده ها در محاسبات ابری بر اساس نوع تقاضای کاربر ، توسط سرویس های ذخیره سازی ، ذخیره می شوند . کاربران بوسیله ی ارائه دهندگان خدمات ابری ، در مورد در دسترس بودن و تمامیت داده هایشان اطمینان حاصل می کنند . از آنجا که کاربران نمی توانند یک کپی محلی از داده های خارجی خود ذخیره کنند ، ارائه دهندگان خدمات مجبور هستند رفتار غیر متعهدانه ای نسبت به کاربران ابری داشته باشند . آنها حتی می تواند برای حفظ شهرت، سعی کنند حوادث مربوط به از دست رفتن داده ها را مخفی نگه دارند . در حالی که این خدمات دارای مزایای بی شماری هستند، اما به دلیل مالکیت فیزیکی اطلاعات ، تهدیدات امنیتی زیادی برای داده ها در ابرها وجود دارد .

سوگانیا [8] و همکاران ، برای حل این مشکل ، یک مکانیسم نظارت بر تمامیت ذخیره سازی توزیع شده را پیشنهاد دادند . این روش با استفاده از نشانه رمز هوموورفیک[1] و اطلاعات رمزی توزیع شده می باشد که به کاربران اجازه می دهد تا با هزینه های ارتباطاتی و محاسباتی بسیار کم ، بر ذخیره سازی ابری نظارت کنند . این ایده با پشتیبانی از داده های پویای صریح ، برای اطمینان از دقت و در دسترس بودن داده های کاربر در ابر ، یک طرح تائید کننده ی ذخیره سازی توزیع شده ی کارآمد و انعطاف پذیر پیشنهاد که این امر باعث افزایش صحت ذخیره سازی ابری می شود و همچنین اجازه می دهد تا مکان خطای داده ها شناسایی شده و بد عمل کردن سرور سریع تر تشخیص داده شود .

مدلی که در این سیستم استفاده می شود شامل کاربر ، سرور ابری[2] و حسابرس دیگران[3] می باشد . در این مدل ، فرض شده که همه ی کانال های ارتباطی ، نقطه به نقطه قابل اعتماد هستند که در عمل می تواند با سربار کمی به دست آمده باشد . در بخش اول این ایده ، به بررسی ابزارهای اساسی نظریه رمز گذاری در فایل های برنامه توزیعی که مورد نیاز سرورهای ابری است ، پرداخته است و رمز نگاری مورد استفاده نیز هوموورفیک می باشد . در بخش دوم یک پروتکل پاسخ برای بررسی ذخیره سازی مناسب داده ها و نشاندار کردن سرورهای خراب ، بدست می آید. روش بازیابی فایل و عیب یابی بر اساس پاک کردن کد تصحیح کننده نیز توصیف شده که این کار با استفاده از تابع hash صورت گرفته است . در نهایت ، طرز عمل اشخاص ثالث[4] را با مقدار کمی تغییر در اصل روشهای بازرسی ، توصیف می کند . این قسمت از طرح به حسابرسی شخص

[1] homomorphic

[2] Cloud Server

[3] Auditor of others

[4] Third Party

ثالث[1] (TPA) معروف است به این معنی که در صورتی که کاربر برای صحت داده ها ، منابع و یا امکانات لازم را نداشته باشد می تواند این کار را به یک حسابرس مستقل خارجی واگذار کند ، طوری که ذخیره سازی ابری قابل تأیید عموم باشد . یک TPA موثر باید بدون ایجاد هرگونه آسیب پذیری جدید برای حفظ حریم خصوصی داده های کاربر ، فرایند بازرسی را انجام دهد. به این معنا که TPA نباید از طریق نمایندگان حسابرسی داده ها از محتوای داده های کاربر با خبر شود . با استفاده از این گزینه می توان نشان داد که تنها با یک تغییر جزئی ، پروتکل می تواند حسابرسی حفظ حریم خصوصی را توسط یک بازرس شخص ثالث پشتیبانی کند . سیستم پیشنهادی از طریق اجرای احراز هویت حسابرسی شخص ثالث TPA بر خطرات امنیتی غلبه می کند. TPA اطلاعات کاربر از قبیل رمز عبور کاربر ، تاریخ و زمان داده ها را ذخیره می کند. جاهایی که الگوریتم های رمز نگاری و رمز گشایی داده ها بارگیری و تخلیه می شوند ، پیش بینی شده است . اگر هیچگونه تغییری در داده ها وجود نداشته باشد ، این موضوع به اطلاع کاربر TPA رسانده می شود. این امر امنیت بیشتر ، در دسترس بودن و یکپارچگی (تمامیت) بیشتر را تضمین می کند . نتایج حاصل از این طرح عبارتند از :

- کاربران از اینکه اطلاعاتشان دست نخورده و به صورت مناسب در ابر ذخیره شده و نگهداری می شوند ، اطمینان کامل دارند . این امر درست بودن عمل ذخیره سازی می باشد.
- تشخیص دادن سرورهایی که به درستی عمل نمی کنند.
- در این طرح از داده های پویا پشتیبانی می شود . هنگامی که کاربران داده های ذخیره شده را در ابر حذف ، اضافه و یا تغییر می دهند ، باز هم همان سطح اطمینانی که در درست بودن ذخیره سازی وجود داشت ، حفظ می شود.

[1] Third Party Audit

- قابلیت اطمینان در این طرح وجود دارد چرا که اثر خطای داده ها و یا خرابی سرور به حداقل مقدار خودش کاهش داده شده است .
- این طرح باعث می شود کاربران با حداقل بار اضافی ، درست بودن ذخیره سازی را چک کنند.

5.3ارایه یک چهار چوب[1] در انتقال و ذخیره سازی داده ها در رایانش ابری

فرض کنید در حال راه اندازی یک وب می باشید . بسیار برای شما پیش آمده است که برای طراحی وب خود از چهارچوب های آماده استفاده کرده اید . مزیت چنین چهارچوب هایی کاهش تعداد خطاها در حین پیاده سازی می باشد . برای طراحی امنیت یک ابر نیز می توان از یکسری چهار چوب های امنیتی استفاده کرد . در صورتی که پیاده سازی ابر بر اساس این چهارچوب های امنیتی صورت بگیرد ، چالش های امنیتی بسیاری رفع خواهند شد . چهار چوب ها می توانند به عنوان راهنمایی ، رای دستیابی به سطوح بالای امنیتی و هم چنین افزایش افزایش سرعت عمل بالا در در پیاده سازی ، مورد استفاده قرار می گیرند . ی دانیم که یک چهارچوب ، به طراحان این اجازه را می دهد که زمان خود را بیشتر صرف نیازمندی‌های نرم افزار ، بنابراین سودمندی و کارایی را افزایش می‌دهد.

در این بخش ، به معرفی یک ایده برای چالش های امنیتی در انتقال و ذخیره سازی داده ها ر رایانش ابری [1] تمرکز کرده ایم .

چهارچوب در محاسبات ابری با توجه به شکل (1) ، شامل اجزای زیر می باشد . فلش ها در این ساختار نشان دهنده ی ارتباط هستند .

[1] Framework

- کاربر[1] : کاربران می توانند به امکانات سمت کلاینت با ویژگی های مختلف احراز هویت بر اساس مرکز تصدیق هویت ، دسترسی داشته باشند .
- پورتال خدمت به مشتریان[2] : کاربر با امضای دیجیتال منحصر به فرد خود وارد سیستم ابر می شود و همچنین با کنترل دسترسی اطلاعات وی به اشتراک گذاشته می شود. بررسی اجزای دیگر در فراهم کننده های سرویس ابر عمل صورت میگیرد .
- ورود به سیستم به صورت فردی[3] : یک کاربر ممکن است چندین نام کاربری و کلمه عبور یکسان در چندین ابر داشته و این مشکل میتواند باعث نگرانی گردد . برای مقابله با این مشکل از امضای منحصر به فرد دیجیتال استفاده می گردد .
- مدیریت امنیت[4] : ابر یک فرایند برای بررسی احراز هویت کاربران و سرویس ها براساس ویژگی ها و گواهی نامه های اعتباری وجود دارد .
- مدیریت سرویس[5] : یک نمایش خودکار سرویس برای تضمین وجود ویژگی های موجود بودن همیشگی و کارایی سرویس می باشد .
- مدیریت اطمینان[6] : به طبیعت ابر مربوط است و بیان کننده ی این است که سرویس باید با اطمینان تجمیع گردد . این مورد مستقل از سرویس می باشد .

[1] Client

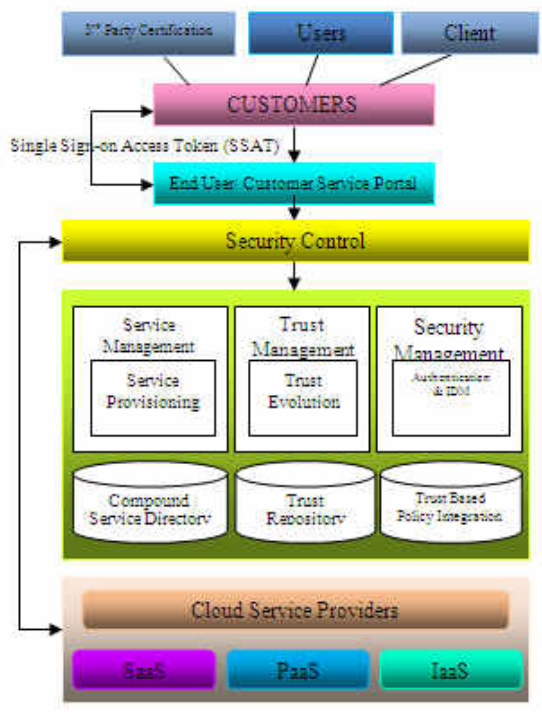
[2] Customer service portal

[3] Single Sign – on

[4] Security Management

[5] Service Management

[6] Trust Management



شکل (1) : ساختار چهارچوب امنیتی

در سال های اخیر چهارچوب های متعددی جهت تشخیص و مقابله با حملات بر ضد رایانش ابری ، با تمرکز بر جنبه های امنیتی و خصوصی سازی مطرح شده است . کورنر[1] و همکاران یک سیستم مدیریت اعتبار را برای اعتبار سنجی ارائه دادند . آنها این کار را توسط چند تابع امتیاز دهی بر روی یک سناریو از کاربردهای توزیع شده پیاده سازی کردند . سیستم پیشنهاد شده توسط کورنر ، تعداد دفعات خطایابی را روی سیستم کاهش می دهد . سان[2] و همکاران نیز یک مدل تجاری کسب و کار از زیر ساخت ابر را که برای امنیت رایانش ابری در دامنه ی قابل دسترسی عمومی اینترنت بود ، بر اساس استاندارد Fisma ارائه کردند . بیشتر این چهارچوب هایی که ارائه شده اند ، روی جنبه های خاصی از امنیت و خصوصی سازی توجه داشته اند . اما همواره ، سازمان ها به دنبال چهارچوبی بوده اند که بسیاری از جنبه های رایانش ابری امن ، خصوصی

[1] Corner

[2] Sun

سازی ، ریسک ها و حملات ، آسیب پذیری ها و نگرانی ها در رایانش ابری را در بر بگیرد . ایده و طراحی اسردهار[1] شامل این گزینه های ذکر شده می باشد .

در چهارچوب معرفی شده توسط اسردهار ، از استانداردهای OpenID و OAuth استفاده می کند . این استانداردها برای خصوصیت های محیطابری و سیساست های حفظحریم خصوصی تعریف شده اند که کاربر را قادر به حراز هویت به صورت غیر متمرکز می سازند . در این ایده از زبان XACML[2] اسفاده شده است . این زبان ، یک زبان کنترل یافته و مبتنی بر XML است که برای مدیریت سیاست حفظ حریم خصوصی ، پیاده سازی ها و تصمیم گیری استفاده می شود . XACML برای کنترل دسترسی و مجوز خدماتیمبتنی بر سیاست در محیط ابری مناسب است . پروتکل پیشنهادی XACML برپایه ابر به صورت زیر است :

- هنگامی که کاربر یک درخواست به سرور ابر می فرستد ، یک فایل Request.xml از طرف کاربر به سرور ابری فرستاده می شود .
- سرویس ابری از دسترسی کاربر به منابع جلوگیری می کند .
- سرور ابری یک Policy.xml را برای صاحبان سرویسی که می توانند این فایل را تعریف کنند، نگه میدارد .
- ابر یک تابع PDP را برای صدور مجوز نگهداری می کند و توسط آن یک Response.xml تولید می کند .

چهارچوب پیشنهادی ، چارچوبی برای شناسایی نیازمندی های امنیتی، حملات، تهدیدهاو نگرانی مربوط به استقرار ابرها می باشد .

[1] Sreedhar

[2] eXtensible Access Control Markup Language

4
فصل چهارم
جمع‌بندي و نتيجه‌گيري

مزایای رایانش ابری برای سازمان ها و کاربران آن به هیچ وجه قابل انکار نیست . اما نگرانی های امنیتی اطلاعات کاربران همواره به عنوان مانعی بر سر راه گسترش این فناوری بوده است . در این پژوهش پس از بررسی این چالش ها و نگرانی های امنیتی در دسته های مشخص راه حل ها یی که تا کنون برای افزایش امنیت رایانش ابری مطرح شده است را شرح دادیم . اعمال این راه حل ها باعث افزایش امنیت و خصوصی سازی اطلاعات کاربران در استفاده از ابر می گردد . ولی می توان گفت نگرانی های امنیتی هنوز به طور کامل از بین نخواهند رفت . اما قطعا با افزایش امنیت معادله ی بین مزایا ی رایانش ابری و و عدم استفاده به علت نگرانی های امنیتی تغییر خواهد کرد . و حرکت به سوی پذیرش این فناوری صورت می پذیرد .

منابع و مراجع

[1]. Sreedhar Acharya B, M. Siddappa, “A Novel Method of Designing and Implementation of Security Challenges in Data Transmission and Storage in Cloud Computing”, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 4 (2016) pp 2283-2286.

[2] . L. Dashora, A. Jain, G. Savner, A. Patidar, V. Singh, “cloud computing and security issues in cloud”, international journal of research in computer application and robotics, Vol.4 Issue 5, Pg.: 6-13, May 2016, ISSN 2320-7345.

[3] . Peter Mell, Tim Grance, 2009, NIST definition of cloud computing : version 15, National Institute of Standards and Technology, http://csrc.nist.gov/groups/SNS/cloud-computing/.

[4] . Anurag S. Barde, “Cloud Computing and Its Vision 2015!! ”, International Journal of Computer and Communication Engineering, Vol. 2, No. 4, July 2013.

[5] . A. M. Chandrashekhar, Sahana K2, Yashaswini K3 , “Securing Cloud Environment using Firewall and VPN”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 1, January 2016, ISSN: 2277 128X.

[6] . K.Chadha, A.Bajpai, “Security Aspects of Cloud Computing”, International Journal of Computer Applications (0975 – 8887), Volume 40– No.8, February 2012.(125).

[7] . A. Behl ,“Emerging Security Challenges in Cloud Computing”, word congress on Information and Communication Technologies, PP. 217-222, 2011(128).

[8] . S.Suganya, P.Damodharan,“ Enhancing Security for Storage Services in Cloud Computing”, International Journal of Scientific and Research Publications, Volume 3, Issue 6, June 2013, ISSN 2250-3153 .

Bu Ali Sina University

Project end of the course distributed systems
Computer Department

Title

Security in the Cloud

By

Narges Rezai

Mohammad Pishdar

Supervisor

Dr. Sakhaei nia

August , 2016