یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

تقاضای ایجاد امنیت برای محاسبات ابری

حمداله غمگین[1]

[1]دانشگاه پیام نور،تهران ،ایران. **hamghamgin@yahoo.com**

چکیده

همیشه قدرت امنیت از منابع IT سرچشمه گرفته و تعداد مشکلات را برای استفاده افزایش می دهد . نه تنها به خاطر تامین امنیت کافی ، بلکه برای کاهش مصرف IT و مشکلات استفاده از آن ، تقاضای ایجاد امنیت برای خدمات امنیتی مختلف در محاسبات ابری ، پیشنهاد شده است . معماری که از سیاست امنیتی گرفته شده است بر پایه ی سه ورودی شکل می گیرد .برای مثال : خطر دسترسی به شبکه ، انواع خدمات و سطح امنیت بر اساس این ورودی ها ، سیاست امنیتی می تواند پارامتر های امنیت را تولید کند ، که برای پیکر بندی مکانیسم های امنیتی (الگوریتم های امنیتی و پروتکل ها) در تمام دامنه های امنیت برای پشتیبانی از خدمات خاص استفاده می شوند . معماری می تواند نیاز های امنیتی مختلف کاربران و خدمات محاسبات ابری تحقق بخشد .هدف بر روی تقاضا ، معماری امنیت فعال برای پشتیبانی از سرویس در محاسبات ابری با سه دامنه ی امنیتی ارائه شده است : دامنه ی امنیت شبکه ، دامنه ی امنیت خدمات ، و دامنه ی امنیت ذخیره سازی ،معماری می تواند مصرف IT را در امنیت کاهش دهد و استفاده از آن را برای کاربر آسان تر کند .

کلمات کلیدی:

محاسبات ابری،امنیت،لایه ها

۱.مقدمه

محاسبات ابری یک نمونه از محاسبه ی امیدوار کننده است که به تازگی از هر دو بخش دانشگاه و صنعت توجه ویژه ای به آن می شود . به طور کلی یکی ، از نظر خدماتی که می تواند به طور سریع ارائه دهد پرداخت برای استفاده، کاهش هزینه ها ، مقیاس پذیری ، تامین سریع برنامه ها در داخل اینترنت ، مورد بحث قرار می گیرد .با ترکیب مجموعه ها و تکنیک های موجود از منطقه ی تحقیق مواردی مانند معماری خدمات گرا (SOA) و مجازی سازی ، لیست خدمات در بخش های Saas(نرم افزار خدمات) و paas(پلت فرم خدمات) و laas(زیر ساخت خدمات) ، طبقه بندی می شود محاسبات ابری به راه حل های تجاری موفقیت آمیز مختلفی ، همانند amazon Ec2/s3، گوگل و force .com. توسعه داده شده است . با این حال امنیت ، جدیترین چالش در محاسبات ابری است . برای کاربر بسیار مشکل است که به طور کامل به محاسبات ابری اعتماد داشته باشد و این به این دلیل است که ان ها در مورد چگونگی ذخیره ی داده های خود و حفاظت از ان ها اطلاعاتئ کمی دارند . Hayes به این نکته اشاره می کند که هیچ راهی برای دانستن این که آیا ارائه دهندگان ابر به درستی اطلاعات یک مشتری را پاک سازی می کنند ؟ یا فقط آن ها را به دلایل نا شناخته ذخیره سازی می کنند ؟در حال حاضر ، تحقیقات در مورد امنیت ابر هنوز در مطالعات مقدماتی مانده است . برای پردازش داده ها ، راج و همکارانش ، پیشنهاد دادند که منابع کاربران مختلف باید در طول پردازش داده ها تفکیک شود .بنابراین داده های کاربری که به ویروس آلوده شده است ، ویروس ها نمی توانند در دادههای سایر کاربران توزیع یابند .[2],[1] برای ذخیره سازی داده ها ، یک حسابرسی شخصی ثالث یشنهاد شده است که از دسترسی داده های ذخیره شده در ابر اطمینان حاصل نماید . این موثرترین راه برای کنترل داده های مورد استفاده با ویزگی های مبتنی بر داده ها و بهبود محاسبات ابری است .در بخش اعتماد به زمینه ی مدیریت ، برخی از کارشناسان در نظر دارند که باید سیاست های امنیتی متعدد در شناسایی کاربر و مدیریت آن ها صورت بگیرد و آن سیاست باید توانایی جلوگیری از نفوذ به داده ها توسط کاربران غیر مجاز را داشته باشد .در آمازون مدیران امتیاز دسترسی به داده های مشتریان و سیستم عامل مشتریان را ندارند . اگر دسترسی به منابع مشتری برای مدیران لازم باشد تمام دسترسی ها باید وارد سیستم شده و به طور معمولی حساب رسی شوند . به هر حال همه ی این تحقیقات به طور عمده به تهدید امنیتی خاص متمرکز شده و راه حل امنیتی فردی را ارائه می دهد[3] .در حقیقت خدمات مختلف همان پلت فرم محاسبات ابری را به اشتراک می گذارند ولی نیازمندی های امنیتی آن ها همیشه متفاوت است . تعدادی از آن ها خدماتی با اطلاعات عمومی هستند که تنها نیاز به امنیت خاص دارد ، بقیه خدماتی با اطلاعات حساس اند که نیاز به امنیت شدید دارند .در بخش دانش ما ، هیچ گونه معماری امنیتی برای برآوردن چنین نیازمندی های امنیتی متنوع ، وجود ندارد

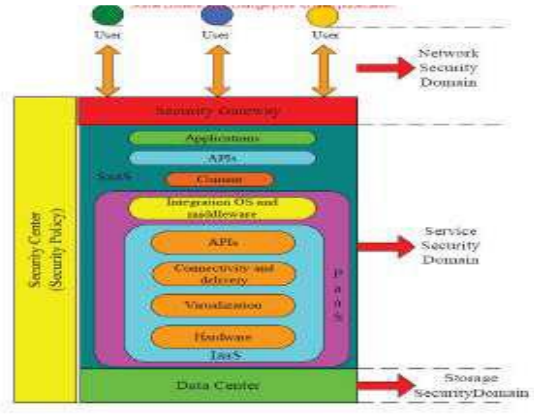
۲. سیستم های موجود

برای کاربر بسیار دشوار است که به طور کامل به محاسبات ابری اعتماد کند و دلیل ان کمبود دید به داده هایی است که آن ها ذخیره و پشتیبانی می کنند .این یک راه ماثر برای ارائه دهندگان محاسبات ابری نیست که از قوی ترین نوع امنیت ها برای خدمات محاسبات ابری

استفاده کنند ، چراکه خدمات امنیتی همیشه از منابعی مانند رایانه ها و حافظه و پهنای باند استفاده می کنند و سختی استفاده از آن را افزایش می دهند .بدیهی است که استفاده از قدرت بالای امنیت برای تمام خدمات محاسبات ابری، امکان پذیر نیست . اگرچه احراز هویت چند عاملی ، سخت تر از روش تک عاملی است اما آن سختی استفاده را برای کاربری که مسئول رسیدگی به احراز هویت است را افزایش داده و بنابراین توجه خدمات کاربر را کاهش می دهد[4] . تهدیدهای اصلی ان عبارتنداز:شناسایی هویت،حمله ی میانی وحمله ی خدماتی . همچنین تهدیدهای اصلی شامل ایجاد فرآیند خدمات ، خدمات زیر نظر کنترل غیر قانونی و وقفه در فرآین خدمات توسط هکر ها ، است .

۳. سیستم پیشنهادی

استفاده از کنترل دسترسی به داده ها برای بهبود امنیت شبکه ، موثر است . در زمینه ی اعتماد به مدیریت ، تعدادی از کارشناسان معتقدن که باید سیاست امنیت چند جانبه در احراز هویت و شناسایی مدیران استفاده شود و سیاست ها باید قادر به جلوگیری از نفوذ به داده ها توسط افراد غیر مجاز باشند .با توجه به منابع مصرف ، یکی از مزایای مهم محاسبات ابری این است که می تواند منابع IP بیشتری را ذخیره سازی نماید و خدمات ارزان تری نسبت به سیستم های سرور سنتی ارائه دهند .بر روی تقاضا ، معماری امنیت فعال برای پشتیبانی خدمات در محاسبات ابری با سه دامنه ی امنیتی ارائه داده شده است.دامنه ی امنیت شبکه ، دامنه ی امنیت خدمات ، و دامنه ی امنیت ذخیره سازی . معماری می تواند مصرف منابع ITرا کاهش داده و استفاده از آن را برای کاربر آسان سازد.برای پلت فرم ابری ، خدمات و ذخیره سازی الزاما با همان سیستم عامل ارائه داده نمی شوند .آن ها میتوانند ارائه دهندگان مختلف معرفی نمایند و یا به طور بالقوه متعلق به ارائه دهندگان ابرخصوصی باشند . تقسیم دامنه های امنیتی می توانند با چندین اپراتور در رابطه باشند . از دیدگاه پارامترهای ورودی ، تنها سه ورودی نیاز به پیکر بندی دارند .



شکل ۱. حوزه های امنیت در ابر معماری محاسبات

هنگامی که یک سرویس خاص داده شده باشد ، ورودی ها با انواع خدمات و خطر دسترسی به شبکه می تواند به طور خودکار توسط پلت فرم مشخص و ثابت نگه داشته شود . تنها ورودی های بخش امنیت توسط کاربر پیکر بندی می شود . به این معنی که وروی ها ، امکان پذیر ، قابل کنترل و قابل تنظیم اند .از دیدگاه سه دامنه ی امنیتی ،اگر بخواهیم سیستم های شبکه ی سنتی را در محاسبات ابری تکامل ببخشیم ، فرمت عملکرد مکانیزم های امنیتی در تمام دامنه ها لازم نیست چراکه ویژگی های تقاضا به طور عمده توسط سیاست امنیت ، مستقر شده اند . پیشنهاد تقاضا برای معماری امنیت سه لایه دارد اولین لایه ، لایه ی ورودی است که دارای سه ورودی به نام های سطح امنیت ، خطر دسترسی به شبکه و نوع خدمات است . لایه ی دوم لایه ی سیاست است که پارامترهای امنیتی را برای مکانیسم امنیت در تمام دامنه ها بر اساس آن سه ورودی تعیین می کند . لایه ی آخر مکانیسم امنیتی است که از خدمات خاص بر پایه ی پارامترهای امنیتی لایه ی دوم ، پشتیبانی میکند .[6][5]

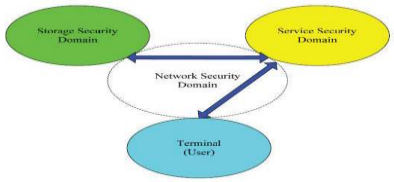
۴. نیاز به امنیت

وجود قدرت امنیت در بسیاری از خدمات ضروری است . همانند خدمات تجاری و بانک داری الکترنیکی و غیره ..... اما تعداد دیگری از خدمات مانند آن ها نیاز به قدرت امنیت ندارند ، مانند اطلاعات عمومی برای کاربران عمومی . به منظور تحقق این شرایط مختلف امنیتی به سادگی می توانیم از راه حل های قدرت امنیتی برای پشتیبانی تمام خدمات سیستم های شبکه استفاده کنید که به طور عمده در سیستم های سرور سنتی استفاده می شوند .به هر حال ، این برای ارائه دهندگان محاسبات ابری راه حل مناسبی نیست که از امنیت قوی برای تمام خدمات محاسبات ابری ، استفاده کنند .چراکه همیشه خدمات امنیتی از منابعی مانند رایانه ، حافظه و پهنای باند مصرف کرده و استفاده از ان را سخت تر می کنند .اگر ما از خدمات و داده ها بیشتر از حد مورد نیاز امنیتی پشتیبانی کنیم ، مقدار زیاد منابع IT در محاسبات ابری به هدر می رود .از طرفی دیگر ، زمانی که امنیت افزایش می یابد ، همیشه کاربر برای ارائه ی خدمات نیاز به اپراتور پیچیده تری دارد تا اینجا ، قدرت امنیتی ، مقدار اپراتوری راکه برای شکستن الگوریتم امنیت و پروتکل نیاز است را اندازه گیری می کند . برای مثال ، احراز هویت امنیتی توسط احراز هویت چند عاملی ، پشتیبانی می شود .در این حالت ، نه تنها کاربر باید رمز عبور داشته باشد بلکه باید دارای کارت هوشمند و حتی اثر انگشت باشد . در نتیجه استفاده از قدرت امنیتی بالا برای تمام خدماتمحاسبات ابری امکان پذیر نیست[7] .بنابراین ، خدمات محاسبات ابری نیاز به تقاضای راه حل های امنیتی با تنظیم خودکار آن راه حل ها دارند .اینجا تقاضای امنیت به معنی نقاط قدرت امنیت متمایز کننده است که به طور خودکار می تواند بر اساس خطرات دسترسی شبکه ، نوع خدمات و سطح امنیت پیکر بندی شده توسط کاربر ارائه داده شود .که نه تنها قادر به تامین امنیت کافی است ، بلکه مصرف را کاهش داده و استفاده از آن را دشوارتر می سازد.

۵. دامنه ی امنیت

معماری امنیت برای سیستم شبکه های خاص ,ما همیشه نیاز به تقسیم شبکه و سیستم به چند حوزه ی امنیتی داریم که میتواند استقرار راه اساس معماری ساده تر کند.در اینجا بیانیه ی حوزه ی امنیتی از سیاست امنیتی مکانیزم مشابهی دارد.در این مقاله, حل های امنیتی را بر

معماری امنیتی ما به سه حوزه ی امنیتی تقسیم میشود و هر کدام از انها در سیاست امنیتی مشابه استفاده میشوند. با توجه به چرخه ی عمر داده برای یک برنامه ,ان همیشه در یکی از سه حالت اصلی باقی میماند: داده در انتقال شبکه, داده در پلت فرم خدمات و اطلاعات در ذخیره سازی.ر وضعیتی مکانیزم امنیتی مختلفی را نیاز دارد.الگوریتم های امنیتی و پروتکل ها برای حفظ کردن داده.سه قلمرو امنیتی با شبکه ی حوزه ی امنیتی,خدمات حوزه ی امنیتی و ذخیره سازی حوزه ی امنیتی پیشنهاد میشود.معماری سیستم,حوزه ی امنیتی در معماری محاسبات ابر را نشان میدهدمرکز امنیتی برای مدیریت محاسبات شبکه مسئول است که سایت امنیتی برای فراهم کردن تقاضای امنیتی مورد استفاده قرار میگیرد.حوزه ی شبکه حوزه ی امنیتی اشاره دارد به حفاظت که داده در وضعیت انتقال است.تهدید اصلی ان شامل شناسایی است.مکانیزم های امنیتی مثل رمز نگاری,تشخیص نفوذ,ترافیک تمییز ضروری هستند.به عنوان مثال,لایه های ساخت و حمله به سرویس (پروتکل و اغلب در این حوزه استفاده میشوند .دروازه ی امنیتی , یکی از نهادهای مهم در این TLS) ,لایه ی حمل امنیت (SSL) سوکت امن حوزه است که به واسطه ی تمام ارتباطات و سیستم , کنترل ریزدانه از طریق ماشین های کنترلی دسترسی را قادر میسازد . اگر آن یک نیاز) حمله) دروازه ی امنیتی میتواند بلافاصله ارتباط را محدود و یا حتی قطع کندبنابراین , حمله DDOSمخرب است (انکار توزیع از سرویس (ی مخرب می تواند به طور موثر مانع شود . اگر تقاضا حقوقی است , ارتباط با پروتکل امنیتی برقرار شود



شکل ۲. رابطه میان حوزه های امنیتی

SaaS, PaaS, LaaSخدمات حوزه ی امنیت بدان معنا است که داده در خدمات پلت فرم شکل ۲ با توجه به رابطه میان حوزه ها میشود . حفاظت

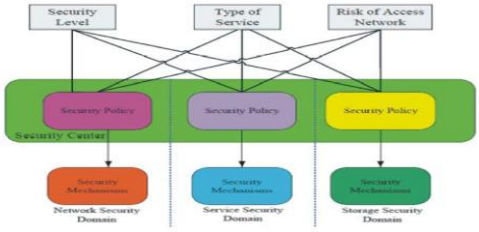
تهدید اصلی آن شامل فرآیند خدمات ساخت , خدمات تحت کنترل قانونی و وقفه ی فرآیند خدمات توسط هکرها است .همانطور که مشاهده شد

مکانیزم امنیتی مثل تصدیق , اختیارات , بررسی آسیب پذیری به انزوای داده و تشخیص ویرووس ضروری هستند .به منظور جلوگیری از صدمه تامین میکند . ذخیره سازی حوزه LaaS , PaaS , SaaSی ویروس و ربودن دیگر کاربران , خدمات حوزه ی امنیتی , خدمات هر کاربر را با ی امنیت اشاره به حفاظت داده در وضعیت ذخیره سازی دارد .تهدید اصلی آن شامل دسترسی های غیر مجاز , تغییر یا ربودن اطلاعات است مکانیزم امنیتی مثل رمزنگاری , کنترل دسترسی و یکپارچگی ضروری هستند . داده های حساس رمز گذاری میشوند و با سطح دسترسی [8]. مختلف مشخص میشوند .بسیار مهم است که از پشتیبان استفاده کند و تکنیک های بازیابی داده برای حفاظت کردن داده . ارتباط سه حوزه ی

امنیتی در شکل ۲ نشان داده شده است . همه ی حوزه های امنیتی با یکدیکر در ارتباط هستند .شبکه ی حوزه ی امنیتی پلی است که دو حوزه ی دیگر را با کاربران به هم متصل میکند . اطلاعات توسط یکی از سه حوزه در تمام چرخه ی عمر محافظت می شود . مزایای طراحی حوزه ی امنیت مشهود هستند.اول , سه حوزه ی امنیتی میتواند همه ی روش های داده را در طول چرخه ی حیات پوشش می دهد . دوم ,در هر حوزه ی امنیتی , تهدید امنیت آن ها و مکانیزم های امنیتی مشابه هستند .

۶. درخواست های امنیتی معماری

درخواست های امنیتی در شکل ۳ نشان داده شده است . معماری به سه لایه ی ,لایه ی ورودی , لایه ی سیاست و لایه ی مکانیزم امنیتی تقسیم میشود .لایه ی ورودی سه ورودی دارد : سطح امنیتی , نوع خدمات و خطر دسترسی به شبکه .لایه ی سیاست سه واحد سیاست دارد که با سه حوزه ی امنیتی مطابقت دارد . لایه ی مکانیزم امنیتی همه ی مکانیزم های امنیتی را در هر حوزه ی امنیتی نشان میدهد .کار سیاست امنیتی برای تولید پارامترهای امنیتی با توجه به ورودی ها است . این پارامتر های امنیتی برای مکانیزم های امنیتی درایو برای , بسیاری از SA توسط محاسبه ی ابر در شبکه ی حوزه ی امنیتی IPSecحفاظت خدمات خاص استفاده می شود .به عنوان مثال , استفاده می شود .(نوعی پروتکل ,روش بسته بندی , الگوریتم رمز گذاری و چرخه ی زندگی کلید مخفی) IPSecپارامترهای امنیتی پارامترهای امنیتی را از سیاست امنیتی شبکه ی حوزه ی امنیتی می گیرد . پس از آن , پارامتر های امنیتی از درایو IPSec.مکانیزم امنیتی برای حفاظت داده در شبکه ی حوزه ی امنیتی جریان دارد.در لایه ی ورودی , سطح امنیتی برنامه ای از سیستم کامپیوتر IPSEC از SA است , پردازش اطلاعات با برخی از حساسیت ها , اجازه ی دسترسی همزمان توسط کاربران با گواهی عدم سوء پیشینه ی امنیتی خاص و نیاز به دانش و جلوگیری کاربران از بدست آوردن دسترسی به اطلاعات است که آن ها فاقد مجوز هستند .این از قدرت امنیتی متفاوت است , اولی اشاره به مشکل برای شکستن یک سیستم دارد که قدرت امنیت و خطر سیم را متصل میکند .از آنجایی که هر یک از این سه ورودی ها میتوانند قدرت و ترکیب مکانیزم های امنیتی را تحت تاثیر قرار دهند , سیاست امنیتی برای تاثیر قیاس استفاده می شود و ترکیبی از پارامتر های امنیتی را تولید می کند .مثل خروجی هایی که درایو مکانیزم های امنیتی خدمات را با قدرت خاص محافظت می کنند .



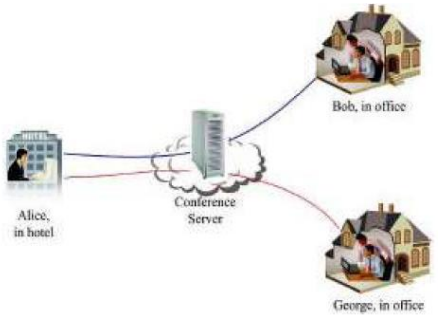
شکل ۳. بر روی تقاضا معماری امنیتی

۱.۶. مزایای استفاده از رویکرد جدید

هر حوزه ی امنیتی با انواع تهدید امنیتی مشابه روبه رو است و با مکانیزم های امنیتی مشابه مستقر است که به معنی آن است که هر حوزه می تواند روی مسئله ی خود تمرکز کند . تقسیم حوزه ی امنیتی طراحی امنیت سیاسی را ساده تر و عملی تر میسازد .برای پلت فرم ابر , شبکه ی خدمات و ذخیره سازی لزوما توسط اپراتور مشابه ارائه نشده است . آنها می تواند با ارائه دهندگان مختلف یا جزئی که متعلق به ارائه دهنده ی . از دیدگاه [13][12]ابر خصوصی میباشد را فراهم کنند .تقسیم حوزه های امنیتی میتواند تا حد زیادی با اپراتور های چندگانه بهره مند شود پارامتر های ورودی , فقط سه ورودی از خدمات و خطر دسترسی به شبکه می تواند به صورت خودکار با پلت فرم مشخص شود .فقط داده ی از سطح امنیتی توسط کاربر پیکر بندی می شود . به این منظور , ورودی ها امکان پذیر , قابل کنترل و قابل تنظیم هستند . از دیدگاه سه حوزه ی امنیتی , اگر می خواهیم سیستم شبکه ی سنتی را با محاسبه ی ابر استنتاج کنیم , توسعه ی عملکردی از مکانیزم های سیستم در هر حوزه ضروری نیستند تا جایی که ویژگی های تقاضا به طور عمده از سیاست امنیتی مستقر شده اند .بنابراین , مکانیزم امنیتی موجود در شبکه می تواند شامل این معماری , بدون تغییرات پایه ای باشد .آن میتواند به طور کامل از منابع شبکه ی موجود استفاده کند و وقتی محاسبه ی ابر مستقر است , سرمایه گذاری را ذخیره کند .

۷. کاربر سناریو

شکل ۴ مثالی برای توضیح کاربرد از تقاضای امنیت ابر را نشان میدهد .در این کاربرد سناریو ,آلیس,باب و جورج کارکنان یک شرکت میباشند.آلیس در هتل میماند.باب و جورج هر دو در اداره هستند.آلیس کنفرانس ویدیویی با باب را آغاز میکند و مکالمه ی متن جورج به بحث در مورد مسائل به مربوط به کسب و کار میباشد



شکل ۴. تقاضای امنیت برای کنفرانس مبتنی بر ابری

.تقاضای امنیت به سه ورودی نیاز دارد با نوع خدمات,خطر دسترسی شبکه و سطح امنیت. به عنوان آغاز کننده ی کنفرانس,الیس سطح امنیتی بالا را برای کنفرانس ویدئو و گفتگوی متن تنظیم میکند.خدمات و خطر دسترسی به شبکه به طور خودکار توسط محاسبه ی شبکه پیکربندی خدمات,تصدیق در حوزه ی امنیت خدمات و محرمانه بودن در شبکه ی حوزه ی امنیتی برای حفظ کنفرانس [9]میشود.با توجه به نوع ویدیویی استفاده میشود.تصدیق,محرمانگی و یکپارچگی برای حفظ گفتگوی متن استفاده میشود. به هرحال,از آنجایی که آلیس در منطقه ی عمومی واقع است.او با خطرامنیتی بیشتری نسبت به جورج و باب در اداره مواجه است.به این منظور محاسبه ی تقسیمات شبکه باید قوی تر پیکربندی شود.امنیت برای آلیس در محیطی ناامن تر از باب و جورج است.بنابراین در سمت آلیس , آلیس باید توسط پلت فرم محاسبه ی شبکه تصدیق کند با شناسایی چند عامل در خدمات حوزه ی امنیت و داده در شبکه ی حوزه ی امنیت جریان رمزنگاری شود.

تنها تصدیق ساده در خدمات حوزه ی امنیتی شامل رمز ضروری است و جریان داده در شبکه ی حوزه ی امنیت میتواند از خطر دسترسی به شبکه بکاهد.علاوه بر این,جریان داده میتواند در ذخیره سازی حوزه ی امنیت رمزنگاری و ذخیره شود.اگرچه قدرت امنیت برای خدمات مشابه در شبکه ی دسترسی مختلف متفاوت است.سطح امنیتی مشابه میتواند رضایت بخش باشد. سیاست امنیتی تمام این تنظیمات را به طور [10]خودکار نتیجه گیری کنترل میکند.

۸. نتیجه گیری

در این مقاله نیاز امنیت گوناگون را از کاربران و خدمات در محاسبه ابر تجزیه و تحلیل کردیم و اشاره کردیم که امنیت تقاضا ضروری است صرفه جویی میکند.ما پلت فرم محاسبات ابر را با سه حوزه ی IT.زیرا نه تنها میتواند برای استفاده راحت تر باشد بلکه در مصرف منابع امنیتی و هدف معماری امنیتی به سه لایه تقسیم کردیم .اولین لایه , لایه ی ورودی است که سه ورودی با سطح امنیتی و خطر دسترسی به شبکه و نوع خدمات دارد .لایه ی دوم لایه ی سیاست است که پارامترهای امنیتی برای مکانیزم های امنیتی در هر حوزه ی امنیت بر اساس سه ورودی تعیین میشود .آخرین لایه مکانیزم های امنیتی است که خدمات خاص را بر اساس پارامترهای امنیتی از لایه ی دوم را حفظ میکند .علاوه بر این اجرا میتواند آگاه کننده باشد و به مرکز صدورت بازگشت است . در این مورد برخی از حفاظت های امنیتی قوی می تواند خدمات زیاد محاسبه ی ابر را تبدیل کند

.

منابع

[1]. Armbrust, M., A. Fox, R. Griffith, A.D. Joseph,R. Katz, A. Konwinski, G. Lee, A. Patterson,A. Rabkin, .Stoicaand M. Zaharia, 2010. A view ofcloud computing, Communications of the ACM,53(4): 50-58
[.2]. Takabi, H., J.B.D. Joshi and G.J. Ahn, 2010.Security and privacy challenges in cloud computingenvironments, Computer, 8(6): 24-31.
[3]. Subashini, S. and V. Kavitha, 2011. A survey onsecurity issues in service delivery models of cloud computing", Journal of Network and Computer
Applications, 34(1): 1-11.
[4]. Wang, C., K. Ren, W.J. Lou and J. Li, 2010.Toward publicly auditable secure cloud datastorage services, IEEE Network, 24(4): 19-24.
[5]. Wang, Q., C. Wang, K. Ren W.J. Lou and J. Li, 2011.Enabling public auditability and data dynamics for storage security in cloud computing, IEEETransactions on Parallel and Distributed Systems,
22(5): 847-859.
[6]. Hu, L.K., S. Yi and X.Y. Jia, 2010. A semantics basedapproach for cross domain access control, Journal of internet technology, 11(2): 279-288.
Middle-East J. Sci. Res., 20 (2): 241-246, 2014
[7]. Pallis, G., 2010. Cloud computing the new frontier
[8]. Lua, R.P. and K.C. Yow, 2011. Mitigating DDoS Technologies, ICT 2013.attacks with transparent and intelligent fast-flux
[9]. Anyong Chen is a professor at the Shenzhen labyrinths", Indian Journal of Science andUniversity, China. His research interests include Technology, 6(6).
network security and artificial intelligence.
[10]. Yang Wang is a graduate student at the Shenzhen Journal, 28(2): 250-253.
[11]. Kerana Hanirex, D. and K.P. Kaliyamurthie, 2013. 28(2): 205-211.
[12]. Khanaa, V., K. Mohanta and T. Saravanan, 2013. Indian Journal of Science and Technology, 20. Tatyana Nikolayevna Vitsenets, 2014. Concept and
6(suppl 6): 4845- 4847.
[13]. Kumar Giri, R. and M. Saikia, 2013. Multipath routing Journal of Scientific Research, 19(5): 620-624.