به نام حق

دانشکده فنی و مهندسی
کارشناسی ارشد مهندسی کامپیوتر نرم‌افزار
گروه مهندسی کامپیوتر و فناوری اطلاعات

گزارش درس سمینار

موضوع:

امنیت رایانش ابری

نگارش:

سیما محسنی

استاد راهنما:

جناب آقای دکتر آرش قربان نیا دلاور

آذر 1399

چکیده

این مقاله به امنیت در رایانش ابری و جنبه های کلیدی و مهم آن می پردازد. ابتدا مفاهیم اصلی و ذاتی در رایانش ابری بررسی خواهد شد، بعد از آن مسائل مربوط به امنیت و حریم خصوصی بیان می شود. خطرات مربوط به محیط های رایانش ابری تجزیه و تحلیل خواهد شد و چند راه حل برای کاهش مشکلات ارائه می گردد.

کلید واژه

رایانش ابری، امنیت، حریم خصوصی، محرمانه بودن

1. مقدمه

رایانش ابری یک نوع رایانش جدید است که به کاربر این امکان را می دهد تا صرف نظر ازنوع پلت فرم و فقط با داشتن یک پایانه ی دسترسی متصل به یک پلت فرم که دارای رایانش ابری است ، به بسیاری از برنامه های کاربردی و خدمات ، از هرنقطه، دسترسی پیدا کند[1].

این کلمه (رایانش ابری)، ایده ی یک جهان ناشناخته را نشان می دهد که فقط می توانیم آغاز و پایان آن را ببینیم. به همین دلیل کاربرد این اصطلاح (ابری)، برای این نوع جدید رایانش بسیار مناسب است. در واقع تمام زیرساخت ها و منابع رایانشی "پنهان" هستند. کاربر فقط به یک رابط استاندارد دسترسی دارد که از طریق آن طیف وسیعی از برنامه های کاربردی و خدمات در دسترس قرار می گیرد[1].

این ابر از یک زیرساخت ارتباطی تشکیل شده است که مجموعه ای از سخت افزار ، نرم افزار ، رابط ها ، شبکه های ارتباط از راه دور و دستگاه های کنترل و ذخیره سازی است ؛ به طوریکه امکان ارائه ی رایانش به عنوان یک خدمت را فراهم می سازد[2].

برای آن که این نوع رایانش امکان پذیر گردد، لازم است که همه برنامه ها و داده های کاربر درمراکز ذخیره سازی بزرگ که به عنوان مراکز داده شناخته می شوند، جمع آوری شود. زمانی که جمع آوری انجام شد، زیرساخت های کاربران و برنامه های کاربردی به شکل خدماتی که از طریق اینترنت قابل دسترسی است ، توزیع می گردد[1].

نکته ی مهم دیگر برای درک این نوع رایانش، به شرکت کنندگان ابر اشاره دارد که می توان آن ها را به سه گروه اصلی ارائه دهنده خدمات، برنامه نویس، و کاربر تقسیم کرد. ارائه دهنده خدمات مسئول تحویل، مدیریت و نظارت بر کل زیرساخت های ابر، تضمین سطح خدمات و امنیت کافی داده ها و برنامه ها است. برنامه نویس باید قادرباشد از طریق زیرساخت های ارائه شده توسط ارائه دهنده خدمات، به کاربر نهایی خدمات ارائه دهد. باشد. در حالی که کاربر نهایی مصرف کننده ای است که از امکانات ارائه شده توسط رایانش ابری استفاده خواهد کرد[1].

رایانش ابری نشان دهنده یک نوع خدمت جدید است که می تواند انواع پردازش داده ها، زیرساخت ها و ذخیره سازی داده ها را از طریق اینترنت و براساس نیاز کاربر فراهم سازد.

امنیت اطلاعات،چه برای شرکت ها وچه برای خود فرد، بیشترین اهمیت را دارد. ما همواره در معرض تهدید هستیم، چه ازسوی علل طبیعی آنها و چه عمدی.

اطلاعات داخلی اشخاص ثالث اگر به دست افراد بد خواه بیفتد، می تواند باعث درگیری و ضرر و زیان جبران ناپذیری شود و همچنین ممکن است آینده یک فرد یا بسیاری از افراد را تحت تاثیر قرار دهد. اطلاعات می تواند اتفاقات را رقم بزند، بنابراین حفظ اسرار در صورت لزوم، حیاتی است.

در یک محدوده ی رایانشی مشترک، حفاظت ازاطلاعات باید دو برابر شود. درمحیط رایانش ابری که در آن همه چیز بر روی اینترنت نگهداری می شود این نگرانی باید بشتر شود، چرا که خطرات و تهدیدها بسیار بیشتر هستند. نگرانی های اصلی در مورد رایانش ابری با توجه به امنیت، دو جنبه ی اساسی را در برمی گیرد: حریم خصوصی و امنیت.

2. ویژگی های اصلی

همگرایی طیف وسیعی از فناوری های مهم، رایانش ابری را قادر می سازد تا در میان قابلیت ها و امکانات دیگر، خدمات را به طور شفاف به کاربر ارائه دهد. از نظرفنی، زمینه های اصلی مرتبط با این حوزه عبارت اند از: سخت افزار، با ظرفیت برای مجازی سازی؛ فناوری های اینترنتی مانند وب 5.0 ، خدمات وب؛ مدیریت سیستم ها، مانند رایانش مستقل و اتوماسیون مرکز داده؛ رایانش توزیعی، به ویژه رایانش همگانی و مشبک[3].

با در نظر گرفتن این موضوع که تمرکز این مقاله بر رایانش ابری نیست ، بلکه بر امنیت است، ما هر یک از فن آوری های ذکر شده در بالا را توضیح نخواهیم داد، اما ویژگی های اصلی آن را به مختصر شرح خواهیم داد.

الف) کشش

رایانش ابری تصور منابع رایانشی بی نهایت و قابل دسترس برای استفاده را ایجاد می کند. بنابراین، کاربران از فضای ابری انتظار دارند که قادر باشد منابع را با هر مقداری و در هر زمانی ارائه دهد. انتظار می رود زمانی که درخواست برای خدمات افزایش یابد، منابع نیز به طور خودکار افزایش یابد.

ب) خود یاوری (سلف سرویس)

مصرف کننده خدمات رایانش ابری انتظاردارد منابع رایانشی را بر اساس نیاز خود و فورا به دست آورد. برای پشتیبانی از این نوع انتظار، ابرها باید امکان دسترسی سلف سرویس را برای کابران فراهم سازند به طوری که کاربران قادر به درخواست، شخصی سازی کردن ، پرداخت و استفاده ازخدمات مورد نظرخود بدون دخالت انسان، باشند.

ج) صورت حساب و اندازه گیری میزان استفاده

از آنجا که شما در درخواست و میزان استفاده از منابع و خدماتی که ضروری می دانید، مختارید، هزینه ی سرویس ها باید بر اساس میزان استفاده باشد. برای مثال، از طریق اندازه گیری میزان استفاده از پردازنده ها در چند ساعت. به همین دلیل ابرها باید منابعی را پیاده سازی کنند که به طور قطعی منجربه تجارت کارآمد خدمات شود، مانند شارژ کافی، صورت حساب، حسابداری، نظارت و بهینه سازی مصرف. اندازه گیری میزان استفاده از منابع باید به صورت خودکار و با توجه به انواع مختلف خدمات ارائه شده (ذخیره سازی، پردازش، و پهنای باند) انجام شود و بی درنگ دوباره ذخیره شود و این امکان را برای شفافیت تجاری بیشتر فراهم سازد[3].

د) دسترسی گسترده به شبکه

منابع باید از طریق شبکه در دسترس باشند. منابع همچنین باید از طریق مکانیسم های استانداردی که امکان استفاده ازمنابع را توسط پلت فرم های ناهمگون مانند گوشی های هوشمند،لپ تاپ و PDAها ایجاد می کند، قابل دسترسی باشند[4].

ه) شخصی سازسی کردن

درخدمت رسانی به کاربران متعدد، تفاوت بسیاری بین نیاز هایشان وجود دارد، که اهمیت توانایی شخصی سازی کردن منابع ابری را نشان می دهد. از خدمات زیربنایی گرفته تا خدمات مربوط به پلت فرم و خدمات نرم افزاری.

3. معماری لایه ای و انواع ابر

خدمات رایانش ابری به سه دسته تقسیم می شوند که سطح انتزاع ویژگی ارائه شده و نوع خدمات ارائه دهنده را در نظر می گیرند. سطح انتزاع ممکن است به عنوان یک لایه ی معماری دیده شود که در آن خدمات لایه های فوقانی ممکن است از خدمات لایه های پایین تر تشکیل شده باشد. این سه دسته خدمت به این شکل نام نامگذاری شده اند: زیرساخت به عنوان خدمت (IaaS)، لایه تحتانی؛ پلت فرم به عنوان خدمت (PaaS)، لایه میانی؛ نرم افزار به عنوان خدمت، لایه فوقانی.

الف) زیرساخت به عنوان خدمت (IaaS)

در این دسته، خدمات زیربنایی بر اساس تقاضا ارائه می شود، به این معنا که منابع سخت افزاری مجازی سازی شده، مانند رایانش ، ذخیره سازی و ارتباطات، ارائه می شوند. این نوع خدمت، سرورها را قادر می سازد تا نرم افزار شخصی سازی شده را اجرا نماید و بر روی سیستم عامل های مختلف کار کند. برنامه ای به عنوان یک رابط واحد برای مدیریت زیرساخت ها وجود دارد که ارتباط با میزبان ها، کلید ها، مسیریاب ها را ارتقا می بخشد و از گنجاندن تجهیزات جدید پشتیبانی می کند. همچنین از آنجا که لایه تحتانی به حساب می آید، مسئول تامین زیرساخت های لازم برای لایه های میانی و فوقانی می باشد.

ب) پلت فرم به عنوان خدمت (PaaS)

این تخت میانی است که به عنوان یک خدمت، یک محیط ارائه می شود که در آن برنامه نویس ممکن است برنامه ها را ایجاد و اجرا کند بدون آنکه نگران باشد که چند پردازنده یه چه میزان حافظه برای انجام این کار استفاده شده است. با استفاده از لایه تحتانی، یک زیر ساخت با سطح بالایی از یکپارچگی را ایجاد می کند که با سیستم عامل های مختلف، زبان های برنامه نویسی و محیط های طراحی سازگار است.

ج) نرم افزار به عنوان خدمت (SaaS)

بالاترین لایه معماری رایانش ابری مسئول تحویل برنامه های انتها به انتها(end-to-end) به کاربر نهایی است. این دسترسی را ارائه دهندگان خدمات از طریق درگاه های وب ایجاد می کنند که کاملا برای کاربر شفاف است، از این رو امکان اجرای برنامه هایی که در فضای ابری از طریق یک ماشین محلی اجرا میشود را فراهم می سازد. برای ایجاد این شفافیت، SaaS از لایه های پایین تر، PaaS و IaaS استفاده می کند.

4. مدل های پیاده سازی

پیاده سازی ابر بستگی به نیاز برنامه ای که ارائه می شود و نوع قرارداد خدمات خواهد داشت. با وجود اینکه خدمات در دسترس عموم قرار دارد و هر کاربر به تمامی انواع محتوای ابر دسترسی دارد، مدل های کسب و کار، توسعه مدل های پیاده سازی را ارتقا بخشیده اند به طوری که کنترل اطلاعات را به میزان کافی تضمین می کنند تا در فضای ابری در دسترس و دید قرار گیرد. در حال حاضر انواع پیاده سازی عبارت اند از: عمومی، خصوصی، همگانی و ترکیبی. در مدل عمومی، ابر در دسترس عموم مردم و یا گروه های بزرگ صنعتی قرار دارد. ابر توسط یک ارائه دهنده خدمات پیاده سازی شده است، که باید قادر به تضمین عملکرد و امنیت آن باشد[4]. ابرهای خصوصی منحصراً توسط یک سازمان اداره می شوند. مدیریت شبکه می تواند توسط خود سازمان یا توسط اشخاص ثالث انجام شود. اگر توسط اشخاص ثالث انجام شود، زیرساخت مورد استفاده متعلق به

کاربر است، به این ترتیب، مسئول کنترل اجرای برنامه های کاربردی در ابر است[5]. مدل همگانی با این ویژگی مشخص می شود که زیرساخت ابر توسط چندین سازمان به اشتراک گذاشته می شود. از یک جامعه خاص حمایت می کند که نگرانی های مشابه ای از جمله ماموریت، الزامات امنیتی، سیاست، و ملاحظات انطباقی را دارد.این مدل ممکن است توسط سازمان ها یا توسط اشخاص ثالث اداره شود و می تواند به صورت محلی یا از راه دور در دسترس باشد[4].در ابر ترکیبی، زیرساخت ها از دو یا چند مدل پیاده سازی تشکیل شده اند و هر ابر به عنوان یک نهاد واحد باقی می ماند، اما با استفاده از فناوری اختصاصی یا استاندارد شده متحد می شود و قابلیت انتقال داده ها و برنامه ها را تضمین می کند [4]. در صورتی که ابر ترکیبی از ابر عمومی و خصوصی ساخته شده باشد، با این ویژگی شناخته می شود که منابع ابر خصوصی می توانند از طریق ذخیره شدن در یک ابر عمومی توسعه یابند. این ویژگی، حفظ سطح خدمات حتی به هنگام نوسانات سریع در نیاز به منابع را ممکن می سازد. یکی دیگر از ویژگی های جالب این مدل استفاده از آن برای انجام کارهای دوره ای است که راحت تر در ابرهای عمومی پیاده سازی می شوند[5].

5. مزایا

از جمله مزایای رایانش ابری توانایی دسترسی به داده ها و برنامه ها از هر نقطه است. این دسترسی تا زمانی امکان پذیر است که اتصال با کیفیت به اینترنت برقرار باشد تا به کاربران پویایی و انعطاف پذیری بخشد. مدل پرداخت هزینه برای استفاده ، کاربر را قادر می سازد تا تنها هزینه ی آنچه را که نیاز دارد بپردازد، از منابع هدر رفته اجتناب کند و همچنین به لطف مقیاس پذیری، می توان در دسترس بودن منابع را افزایش داد چرا که این کاربر است که نیاز خود را تعیین می کند. این انعطاف پذیری این امکان را فراهم می سازد تا خطرات مربوط به زیرساخت ها به حداقل برسند زیرا شرکت نیازی به خرید بسیاری از منابع فیزیکی ندارد و مسئولیت زیرساخت های قراردادی را نیز به عهده نمی گیرد[5].

سایر انعطاف پذیری ها عبارت اند از سهولت استفاده از خدمات ، اشتراک گذاری منابع و همچنین قابلیت اطمینان به خدمات ، زیرا شرکت هایی که خدمات را ارائه می دهند، بر اساس شهرت و عمدتا به دلیل توانایی حفظ داده ها از طریق پشتیبان گیری، رمزنگاری و کنترل دقیق دسترسی، ارزش گذاری می شوند.

یکی دیگر از مزیت های بزرگ این است که شرکت هایی که رایانش ابری را ارائه می دهند، دسترس پذیری قراردادی اطلاعات و خدمات را صد درصد تضمین می کنند، به این معنی که هیچ وقفه ای در جریان اطلاعات یا خدمات وجود نخواهد داشت.

6. معایب

معایب اصلی این فناوری نیز از دلایل مهم برای توسعه و برجستگی آن است:

امنیت: این واضح ترین چالشی است که با آن مواجه می شویم. زیرا اطلاعاتی که قبلاً به صورت محلی ذخیره شده بودند، اکنون در فضای ابری در یک مکان فیزیکی قرار خواهند گرفت که دقیقاً مشخص نیست کجا است یا چه نوع داده هایی در حال ذخیره سازی هستند. حریم خصوصی و یکپارچگی اطلاعات پس از آن، از اهمیت فوق العاده ای برخوردار است، چرا که به ویژه در ابرهای عمومی احتمال قرار گیری در معرض حملات بسیار زیاد است. از جمله قابلیت های مورد نیاز برای جلوگیری از نفوذ اطلاعات می توان به رمزنگاری داده ها، کنترل دقیق دسترسی ، و مدیریت موثر در پشتیبان گیری اشاره کرد[6].

مقیاس پذیری یک ویژگی مهم در رایانش ابری است زیرا برنامه های کاربردی برای یک فضای ابری نیاز به مقیاس پذیری (یا کشسانی) دارند. به این ترتیب منابع مورد استفاده را می توان با توجه به درخواست ها تغییر داد. برای این که این امکان وجود داشته باشد، برنامه های کاربردی و داده های آن ها باید به اندازه کافی انعطاف پذیر باشند. این وظیفه ممکن است پیچیده باشد و معمولاً به پیاده سازی بستگی دارد[7].

قابلیت تعامل متقابل، عامل توانایی کاربران در اجرای برنامه ها و داده های خود در سراسر ابرهای مختلف است، بنابراین آنها به یک فضای ابری واحد محدود نمی شوند. این یک ویژگی بسیار مطلوب در محیط رایانش ابری است. اگرچه بسیاری از برنامه های کاربردی سعی کرده اند این عامل را در نظر بگیرند، اما به پیاده سازی استانداردها و رابط ها نیاز است تا این قابلیت انتقال امکان پذیر شود[8].

قابلیت اطمینان، با بسامدی که سیستم با آن از کار می افتد و تأثیر خرابی آن (داده از دست رفته باشد یا نه) ارتباط دارد. برنامه های کاربردی طراحی شده برای رایانش ابری باید قابل اعتماد باشند، به این معنی که باید معماری ای داشته باشند که اجازه دهد داده ها دست نخورده باقی بمانند حتی اگر در یک یا چند سرور یا ماشین مجازی که آن برنامه ها بر روی آن ها در حال اجرا هستند، خرابی یا خطا وجود داشته باشد. این ویژگی به سیاست مدیریت نسخه پشتیبان مربوط است[5].

دسترس پذیری یک نگرانی عمده است زیرا حتی سیستم های گوگل مانند Gmail در دسترس نیستند و با اینکه سیستم همیشه آنلاین است، کاربر همیشه به اینترنت نیاز دارد که خود اینترنت نیز سرویسی است که در سطح یک شبکه محلی در دسترس نیست. یک جایگزین این است که بیش از یک ارائه دهنده و در نتیجه بیش از یک ابر وجود داشته باشد تا به کاربران

اجازه دهد برنامه های خود را در فضای ابری دیگری اجرا کنند در حالی که ابر دیگر آفلاین است. با این حال، این جایگزین به اندازه ای که نیاز به قابلیت تعامل متقابل بین ابرها دارد، ساده نیست[5].

7.امنیت عمومی فناوری اطلاعات (IT)

برای درک امنیت فناوری اطلاعات، ابتدا باید سه اصل اساسی را که امنیت فناوری اطلاعات را در یک محیط رایانه ای تضمین می کند، درک کنیم. این سه اصل عبارت اند از محرمانگی، دسترس پذیری و یکپارچگی.

محرمانگی «برای حفاظت از اطلاعات در برابر دسترسی غیرمجاز توسط افراد یا برنامه های غیرمجاز در نظر گرفته شده است، در حالی که محرمانه بودن و حریم خصوصی اطلاعات آن ها را حفظ می کند»[9]، به عبارتی در یک محیط رایانه ای، اساساً به دنبال کسب اطلاعات از هر فرد یا برنامه ای است که اجازه دسترسی به آن را ندارد.

دسترس پذیری ویژگی ای است که همیشه دسترسی به اطلاعات برای استفاده ی مشروع را تضمین می کند، یعنی توسط کسانی که صاحب اطلاعات آن ها را مجاز می داند.

یکپارچگی در یک محیط رایانشی متشکل از این ایده است که کاربرانی که اجازه این کار را ندارند ، نمی توانند اطلاعات را تغییر یا تحت تأثیر قرار دهند. حفاظت از اطلاعات در برابر هر نوع تغییر، بدون اجازه صاحب یا مسئول دیگر این اطلاعات، هدف اصلی یکپارچگی اطلاعات است[9].

این به این معنی است که اطلاعات، هنگام دسترسی، باید دقیقاً همان طور باشد که آخرین بار ذخیره یا باز شده است ، بنابراین باید اقداماتی انجام شود تا این اطمینان حاصل شود که اطلاعات به طور نامناسب یا توسط افرادی که اجازه این کار را ندارند تغییر نمی کند، همانطور که باید از محتوای اطلاعات نه تنها درهنگام ذخیره سازی محافظت شود، بلکه در طول پردازش آن نیز باید از تلفات داده ها در صورت هر گونه خرابی یا توقف در سیستم جلوگیری شود.

با تحلیل تمام این اصول به راحتی می توان فهمید که چگونه با هم کار می کنند، یکدیگر را کامل می سازند و برای حفظ امنیت یک سیستم تلاش می کنند.با این وجود خوب است بدانید که سطحی که هر یک از این سه جنبه در یک محیط فناوری اطلاعات به آن رسیده است، ممکن است با توجه به نیاز شما به کسب و کار یا خدمات، جایی که در آن به کار گرفته خواهد شد و ارزش اطلاعاتی که قرار است حفظ شود، متفاوت باشد.

8. خطرات و تهدید ها

بزرگترین چالش پیش روی رایانش ابری، به ویژه برای سازمان ها، امنیت است. برای درک خطرات امنیتی بالقوه، آنها باید سرویس ابری ای را که از آن استفاده خواهند کرد به طور کامل تجزیه و تحلیل کنند. در فرایند تجزیه و تحلیل، اگر هر یک از الزامات امنیتی ذکر شده (محرمانگی ، یکپارچگی و یا دسترس پذیری) به خطر بیفتد، اثرات به وجود آمده باید ارزیابی شود. و از طریق این تجزیه و تحلیل، سازمان ها می توانند فرایندها یا داده های خود را به طور کامل یا جزئی به محیط رایانش ابری منتقل کنند.

به منظور ارزیابی خطرات امنیتی بالقوه در یک محیط رایانش ابری، لازم است خطرات امنیتی سه مدل اصلی استقرار رایانش ابری (SaaS، PaaS و IaaS) که از قبل شرح داده شده اند را درک کنیم.

خطرات اصلی ای که برای خدمات ارائه شده توسط IaaS، باید ملاحضه شوند مربوط به دسترس پذیری هستند. به طوری که می توانیم بگوییم IaaS پایه ای برای محیط های دیگر است چرا که ظرفیت لازم برای انجام فعالیت های دیگر را برای آن ها فراهم می سازد. «سطح IaaS به عنوان پایه ای برای سایر مدل های ارائه خدمات (PaaS و SaaS) عمل می کند ، و عدم امنیت در این سطح قطعاً بر مدل های ساخته شده بر روی آن نیز تأثیر می گذارد. [10]»

IaaS بخش ساختاری را ارائه می دهد و از این رو باید خرابی هایی را که ممکن است در سرورها ، تجهیزات شبکه و فضای ذخیره سازی شما اتفاق بیفتد، در نظر بگیرد. تصور کنید در حال کار بر روی سندی هستید و این سند در سروری ذخیره شده است که به هر دلیلی آفلاین می شود، خواه یک خرابی سخت افزاری ساده باشد و یا حتی یک بلای طبیعی در جایی که سرور ذخیره شده است باشد ، و باعث شود سرور از کار بیفتد.

IaaS با مجازی سازی کار می کند و این فناوری توسط کاربران مختلف، با استفاده از سرویس های مختلف، و با نیازهای مختلف، در یک دستگاه واحد استفاده می شود و می تواند مشکلاتی را ایجاد کند، زیرا ممکن است دستگاه های مجازی با توجه به امنیت کاملاً آماده نباشند [10]. یک مثال خوب برای تشخیص آنچه که در دستگاه انجام می شود، استفاده از حملات کانال جانبی است که در آن امکان انجام یک تجزیه و تحلیل آماری از سرعت ترافیک شبکه در هنگام تایپ کلیدها و همچنین در زمان تراوش های الکترومغناطیسی صفحه، وجود دارد [10] .

عامل بسیار مهم دیگری که باید مورد توجه قرار گیرد ، تلاش برای سرقت اعتبارنامه است ، جایی که افراد مخرب تلاش می کنند با کلاهبرداری رمزعبورهای کاربران قانونی سیستم را بدست آورند.

در این زمینه ، یک روش معمول که مورد استفاده قرار می گیرد فیشینگ یا تله گذاری است ،جایی که کاربران برای ارائه داده های حساب خود تحت تأثیر قرار می گیرند. یک مثال می تواند ایمیل های ارسالی با درخواست به روزرسانی نمایه برای حساب های بانکی باشد، جایی که کاربر بی اطلاع، در نهایت، اطلاعات بانکی خود را ارائه می دهد. همچنین سایت هایی وجود دارند که به همان روش های قانونی ایجاد شده اند و کاربر اطلاعات خود را با تصور اینکه این کار را در سایت اصلی انجام می دهد ، درج می کند ، اما در نهایت اطلاعات و دسترسی را برای افراد غریبه فراهم می کند.

9. چگونه امنیت را تضمین کنیم؟

اکنون چند مثال و روش ارائه می دهیم که می توان از آن ها برای به حداقل رساندن خطرات در محیط ابری استفاده کرد. کاربرانی که از سرویس ابری استفاده می کنند به تمام داده ها و اطلاعاتی که سرویس ابری برای ارائه دهنده خدمات تولید می کند اعتماد می کنند، بنابراین مهم است که اقدامات و سیاست های حفاظتی مختلفی اتخاذ شود تا در صورت هرگونه خدماتی، اطلاعات به طور کامل از دست نرود [10].

حریم خصوصی و یکپارچگی اطلاعات از اهمیت ویژه ای برخوردار هستند ، به ویژه در ابرهای عمومی که بیشتر در معرض حملات قرار می گیرند. قابلیت های مورد نیاز برای جلوگیری از نفوذ اطلاعات عبارت اند از: رمزگذاری داده ها ، کنترل دقیق دسترسی و یک سیستم موثر مدیریت پشتیبان [11].

در صورت وقوع مشکلات مربوط به دسترس پذیری خدمات، مانند یک خرابی یا یک فاجعه، ارائه دهندگان خدمات باید سیاست های احتمالی داشته باشند که قادر باشد زمان در دسترس نبودن خدمات را تا حد امکان کاهش دهد. همچنین در مواقع بحرانی تر و حتی زمانی که مشکل برای کاربران قابل مشاهده نیست.

از این نظر ، چندین استراتژی احتمالی وجود دارد ، دو سایت Hot Sites و Warm Site اصلی ترین آن ها هستند. Hot site استراتژی است که به محض بروز خطر شروع به کار می کند و مربوط به زمان تحمل پذیری موارد محافظت شده در برابر خطا است. مانند یک پایگاه داده که نمی تواند بیش از چند ثانیه از دسترس خارج شود، زیرا سایت هایی مجهز به امکاناتی وجود دارند که بتوانند نیازهای شرکت را برآورده کنند، در عین حال ، پشتیبان گیری از داده ها به صورت دوره ای برای اطمینان از یکپارچگی داده ها به Hot site ارسال می شود [9].

Warm site استراتژی است که روی اشیایی اعمال می شود که ممکن است به مدت طولانی تری در حالت عدم دسترسی، باقی بمانند. همچنین مکان هایی با زیرساخت کمی کوچک تر هستند، اما توانایشان کمتر نیست، چرا که آنها می توانند خدمات

را تا 24 ساعت از سر بگیرند و همچنین پشتیبان گیری داده ها را در یک دوره که کمی طولانی تر است انجام دهند ، این استراتژی می تواند در خدمات ایمیل مورد استفاده قرار گیرد، چرا که آنها کسب و کار را به طور جدی به خطر نمی اندازند [9].

احراز هویت، مجوز، و حسابرسی کاربران درون محیط رایانش ابری باید حداقل بیش از یک روش داشته باشد که قادر به تامین امنیت این سه مورد باشد، در این صورت می توان از صحت هویت کسی که به خدمات دسترسی دارد اطمینان حاصل کرد و مجاز است به پرونده ها و خدماتی که انتخاب می کنید و آنچه که با آنها انجام می دهید دسترسی پیدا کند. «مجوز ، فرآیند اعطا یا انکار حقوق کاربران یا سیستم ها از طریق به اصطلاح لیست های کنترل دسترسی (ACL) است که تعیین می کند چه فعالیت هایی مجاز است ، [...]» [9].

احراز هویت وسیله ای است برای اطمینان از اینکه کاربر یا شیء دور در واقع همان کسی است که ادعا می کند. این یک سرویس امنیتی ضروری است زیرا احراز هویت قابل اطمینان، کنترل دسترسی را تضمین می کند، تعیین می کند که چه کسی مجاز به دسترسی به اطلاعات است، مسیرهای حسابرسی را ممکن می سازد و مشروعیت دسترسی را تضمین کند.

سه روش برای احراز هویت کاربر وجود دارد: نام کاربری و رمز عبور، نشانه یا کارت، و تحلیل شبکیه چشم یا اثر انگشت. ترکیب تمام این روش ها، دسترسی افراد مخرب به منابع فضای ابری را از طریق عبور با نام کاربری دیگری بسیار دشوار می کند، زیرا به ندرت می توانند دو مورد از اطلاعات مورد نیاز برای دسترسی را بدست آورند.

یک سیاست خوب برای امکان دسترسی به هر نوع کاربری ، SSO (ورود یکپارچه) است . SSO شناسه منحصر به فردی است که در اختیار کاربر قرار می گیرد و حاوی تمام اطلاعات مربوط به نمایه کاربری شما است ، یعنی آنچه ممکن است انجام دهد یا ندهد و از آن در محدوده های خاص یا به عبارت دیگر در شبکه ارائه دهنده استفاده شود. این اطلاعات به سرور شناسایی که مسئول ذخیره همه این SSO ها ، پروفایل های دسترسی و سیاست دسترسی برای هر نوع کاربر و منابع سیستم است، منتقل می شود ، از آنجا سرور فدراسیون شناسایی با ارائه دهنده خدمات سرور ، IaaS، ارتباط برقرار می کند ، SaaS یا PaaS است که مشخص می کند چه چیزهایی توسط SSO قابل دسترسی و استفاده هستند.

«برای تأمین دسترسی به سطوح مختلف خدمات ، سازمان مصرف کننده ممکن است از یک سرویس ورود یکپارچه (SSO) استفاده کند که بخشی از یک فدراسیون برای تأیید اعتبار کاربران برنامه های موجود در فضای ابری است.» [9]

از این طریق می توان کاربر را وادار کرد اطلاعات خود را فقط یک بار وارد کند ، و حتی مجبور به استفاده از منابع مختلف ابر شود و دسترسی را آسان کند. زیرا تنها یک گواهی هویت وجود دارد که همچنین می تواند اصالت بیشتر و حسابرسی آسان تر از آن را تضمین کند، و فقط یک گواهی هویت برای همه دسترسی ها وجود دارد.

برای محافظت از داده های منتقل شده در حین استفاده از رایانش ابری، تکنیک های رمزنگاری باید به طور گسترده ای مورد استفاده قرار گیرند. این تکنیک شامل استفاده از الگوریتم هایی برای رمزنگاری داده های در حال انتقال است، سپس داده های رمزنگاری شده ممکن است برای گیرندگانی فرستاده شوند که نیاز به دانستن کلید یا کد مورد استفاده برای رمزگشایی آنچه دریافت شده است، خواهند داشت. رمزنگاری نشان دهنده ی مجموعه تکنیک هایی است که برای ایمن نگه داشتن اطلاعات استفاده می شوند. این تکنیک ها شامل استفاده از کلیدها و الگوریتم های رمزنگاری است.با دانستن کلید و الگوریتم استفاده شده، رمزگشایی پیام دریافتی امکان پذیر است [9].

یک راه برای اطمینان از انتقال ایمن داده ها استفاده از VPN (شبکه خصوصی مجازی) است که تونل هایی رمزنگاری شده میان دو نقطه مجاز هستند که می توانند بدون هیچ گونه تعاملی با شخص ثالث، تبادل اطلاعات کنند [9]. این یک اتصال مجازی است و بنابراین نمی تواند توسط کاربران خارج از تونل مشاهده شود ، بنابراین سطح بالاتری از حریم خصوصی و یکپارچگی داده ها را تضمین می کند.

در VPN ، مفهوم تونل زنی در جایی استفاده می شود که بسته های داده ای که برای انتقال ارسال می شوند ، از یک فرایند رمزگذاری عبور می کنند تا در صورت رهگیری از آن، رمزگشایی نشوند و اینکار همچنین توسط یک فرآیند کپسوله سازی و دریافت یک هدر اضافی انجام می شود. این هدر حاوی اطلاعات مقصد در داخل تونل است و با رسیدن به مقصد ، حذف شده و بسته داده ها نیز رمزگشایی شده و به آخرین مقصد ارسال می شود.

مدل های پیاده سازی امنیت قوی

الف) جست و جوی رمزگذاری شده

جستجوی رمزگذاری شده (رمزگذاری قابل جستجو) روشی است که بدون نیاز به کلید رمزگذاری ، قابلیت جستجو در داده های رمزگذاری شده را فراهم می سازد. این روش از دو بخش استفاده می کند: یک مشتری و یک سرور که یک پایگاه داده رمزگذاری شده D را ذخیره می کند ، جایی که مشتری دارای کلید دسترسی Q است و از آن برای به دست آوردن نتیجه پرس و جو Q (D) بدون آشکار کردن متن و نتیجه پرس و جو برای سرور، استفاده می کند. کلید دسترسی، مجموعه ای از کلمات

رمز است که با کلمات کلیدی مرتبط با سوابق جدول جستجو شده در پایگاه داده ارتباط دارد. جستجو (کوئری)، رکوردهایی را که در آن بین کلمات کلید دسترسی Q و کلمات رکوردها در جدول، مطابقت وجود داشته باشد ، برمی گرداند [12].

به عنوان نمونه ای از سناریوی استفاده از جستجوی رمزگذاری شده ، فرض کنید که یک مشتری معین بخواهد اطلاعات پزشکی رمزگذاری شده خود را در یک پایگاه داده در فضای ابری ذخیره کند تا بتواند به صورت انتخابی سوابق را بازیابی کند. مشتری مجموعه ای از کلمات کلیدی را برای هر رکورد جدول با هم مرتبط می سازد، به عنوان مثال نوع بیماری. برای استفاده از جستجوی رمزنگاری شده ،مشتری مجموعه کلمات کلیدی را که با رکوردهای جدول مرتبط هستند رمزگذاری می کند. سوابق داده های پزشکی نیز با استفاده از الگوی رمزگذاری استاندارد رمزگذاری می شوند. کلمات کلیدی و داده های پزشکی در یک جدول در پایگاه داده ذخیره می شوند. برای جستجوی سوابقی که با کلمه "دیابت" در ارتباط هستند، مشتری یک کلید جستجو Q با استفاده از کلمه "دیابت" ایجاد می کند و جستجو را به سرور می فرستد که هر کلمه کلیدی را در جدول بررسی می کند تا سوابقی را که در آن کلید جستجو و کلمه کلیدی "دیابت" وجود دارد، انتخاب نماید، و در صورت وجود، به مشتری بازگرداند. در این حالت ، سرور اطلاعاتی درباره اینکه کدام سوابق دریافت شده اند بدست می آورد، اما از محتوای این سوابق چیزی نمی داند.

در طرح های جستجوی رمزنگاری شده ممکن است از طرح های رمزنگاری مبتنی بر کلید متقارن یا کلید نامتقارن استفاده شود. طرحواره های کلید عمومی برای ویژگی های چند کاربره مناسب است که در آن هر مشتری می تواند داده ها را با استفاده از پارامترهای عمومی رمزگذاری کند ، اما فقط یک کاربر می تواند داده ها را جستوجو کند. در طرح کلید متقارن ، فقط دارنده ی کلید مخفی می تواند کلمات کلیدی را ایجاد کند [12].

ب) بازیابی اطلاعات خصوصی

برای محافظت از حریم خصوصی استاندارد دسترسی به داده ها، هر عملیات دسترسی به داده باید پنهان شود تا هر کسی که تراکنش را «تماشا» می کند، هیچ اطلاعات معنی داری دریافت نکند. بازیابی اطلاعات خصوصی (PIR) یک تکنیک جستجوی پایگاه داده عمومی رمزگذاری نشده با حفاظت در برابر نقض حریم خصوصی دسترسی کاربر است. نقض حریم خصوصی دسترسی، زمانی رخ می دهد که علاوه بر دسترسی به خصوصیات داده های آماری جمع شده، ارائه دهنده فضای ابری ممکن است به احتمال زیاد، اطلاعات خصوصی خاصی را در مورد کاربر، از داده های رمزگذاری وذخیره شده بداند [13].

پروتکل های PIR به مشتریان این امکان را می دهد که اطلاعات را از پایگاه داده های عمومی یا خصوصی بازیابی کنند بدون اینکه آشکار شود کدام سوابق بازیابی شده اند. در محافظت از محتوای جستوجوها، RIP ها ممکن است از حوزه های مهم برنامه های کاربردی مانند پایگاه داده های ثبت اختراع، پایگاه داده های دارویی، سرشماری های آنلاین، خدمات مبتنی بر مکان و تحلیل رفتاری آنلاین برای تبلیغات در شبکه، محافظت کند [13].

یک طرح PIR، پایگاه داده را به عنوان یک رشته دودویی x = x1, x2, x3,..., xn به اندازه n مدل سازی می کند. کپی های یکسان این رشته در سرورهای k ذخیره می شوند، جایی که $k \geq 2$ است. کاربران دارای شاخص i (یک عدد صحیح بین 1 تا n) هستند و همچنین خواهان به بدست آوردن مقدار بیت xi هستند. بنابراین جستجوهای تصادفی را در سرورها انجام می دهند و پاسخ هایی می گیرند که ممکن است بیت Xl را محاسبه کند. جستجوهای انجام شده در سرورها بدون در نظر گرفتن مقدار i توزیع می شوند تا سرورها اطلاعاتی در مورد i به دست نیاورند. جستوجو ها لزوماً یک بیت خاص یا مجموعه ای از بیت ها را بازیابی نمی کنند. آن ها ممکن است توابع محاسبه شده توسط سرورها را تعریف کنند ، به عنوان مثال ، یک جستجو می تواند مجموعه ای از شاخص ها را بین 1 تا n مشخص کند و پاسخ سرور می تواند XOR بیت هایی باشد که دارای این شاخص ها هستند.

مهم ترین پارامتر در طرحهای PIR، پیچیدگی ارتباط بین کاربر و سرورها است. کارآمدترین پروتکل ها، برای ارتباط با دو سرور، دارای پیچیدگی ارتباطی O (n 1 3) هستند. از آنجا که طرح های PIR از داده های رمزنگاری نشده استفاده می کنند، برای استفاده در محیط های ابری غیرقابل اطمینان، مناسب نیستند [13].

ج) محاسبات چند جانبه امن (SMC)

SMC (محاسبات چند جانبه ای امن) یک روش داده پردازی توزیعی، با تضمین حفظ حریم خصوصی است. در SMC، گروهی از ذینفعان مایلند برخی از عملکردهای مورد علاقه مشترک گروه را ارزیابی کنند و به این منظور داده های خصوصی فردی را بدون آشکار کردن این داده ها برای یکدیگر پردازش می کند. پردازش داده های مشارکتی اغلب در یک محیط ابری مورد نیاز است. پردازش داده های مشارکتی اغلب در یک محیط ابری مورد نیاز است. در پردازش توزیعی ، حزب ها ممکن است مخالفانی منفعل باشند که تلاش می کنند اطلاعات بیشتری در مورد داده ها از طرف های دیگر به دست آورند [14].

در این روش ، هر مشتری Ci دارای یک ورودی خصوصی xi است ، و همه مشتری ها یک تابع عمومی f (x1, x2, x3, ..., xn) را محاسبه می کنند بدون اینکه xi را به دیگران نشان دهند، به جز آنچه که می تواند از تابع ورودی یا خروجی [14] مشتق شود.

د) ناشناس بودن تجزیه

رمزگذاری ابزاری مفید برای محافظت از محرمانگی اطلاعات حساس است. وقتی داده ها رمزگذاری می شوند ، انجام جستجو ها به یک چالش تبدیل می شود. بنابراین ، در حالی که رمزگذاری داده ها محرمانگی را ممکن می سازد، استفاده از داده های رمزگشایی سده نسبت به داده های رمزگذاری شده بسیار راحت تر است. [15]

هنگامی که رمزگذاری به همراه پایگاه داده های رابطه ای استفاده می شود ، دو مشکل عمده ایجاد می کند. اولین مشکل این است که پایگاه داده های رابطه ای ایجاب می کنند که انواع داده ها قبل از ذخیره سازی آن ها تعریف شوند. مشکل دوم این است که جستجو ها یا توابع نمی توانند از طریق داده های رمزگذاری شده انجام شوند. شما نمی توانید محدوده های تاریخ را ارزیابی کنید یا داده های رمزگذاری شده را از نظر ارزش مقایسه کنید. ساختارهای شاخص نیز نمی توانند مورد استفاده قرار گیرند. علاوه بر این ، روشهای مبتنی بر رمزنگاری باید شامل راهبردهای تولید و توزیع کلید باشند. با این حال ، چند اشکال در مدیریت کلیدهای رمزنگاری وجود دارد ، مانند:

- نیاز به ذخیره کلیدها تا زمانی که داده ها رمزگذاری شده باشند.
- اختصاص یا لغو کلیدها برای دسترسی به داده ها توسط کاربران.
- نیاز به نگه داشتن چندین نسخه رمزگذاری شده از همان پرونده برای دسترسی به چند کاربر با استفاده از کلید عمومی [15].

بنابراین، روش های جدید برای اطمینان از حریم خصوصی داده های ذخیره شده ابری ، که مبتنی بر رمزنگاری نیستند ، در سناریوهای مختلف برنامه های کاربردی، ضروری می شوند. به این ترتیب، استراتژی حفظ حریم خصوصی داده های ذخیره شده در ابر، به نام «تجزیه» را ارائه می کنم که از تجزیه و پراکنده شدن فایل ها برای جدا کردن داده ها به اجزای غیرقابل تشخیص و ذخیره آن ها بر روی سرورهای توزیع شده در ابر استفاده می کند. علاوه بر این، رویکرد پیشنهاد شده، داده ها را رمزگذاری نمی کند تا در فضای ابری ذخیره و پردازش شوند [16].

تکنیک «تجزیه» اطلاعات مربوط به کمیت ، کیفیت و اندازه را از پرونده های داده استخراج می کند. پرونده های داده به عنوان اشیا در نظر گرفته می شوند. پرونده های داده به عنوان اشیا در نظر گرفته می شوند. هر شئ دارای سه ویژگی است که آن را مشخص می کند: کیفیت ، کمیت و اندازه. در یک فایل داده ، کیفیت توسط 256 ترکیب ممکن از 8 بیتی که بایت های تشکیل دهنده پرونده را تشکیل می دهند ، نشان داده می شود. کمیت تعداد دفعاتی است که هر بایت در پرونده پیدا می شود و اندازه ترتیب قرارگیری بایت ها در پرونده است. در یک پرونده 256 بایتی که فقط بایت های نشان دهنده حروف "A"، "B"، "C" و "D" به نسبت مساوی وجود دارد، به عنوان مثال:

بایگانی: "ABCDABCDABCDABCDABCDABCDABCD ... ABCD" (256 بایت)

اندازه :, A (1º,5º,9º,13º...253º), B (2º, 6º, 10º, 14º..., 254º)

C (3º, 7º, 11º, 15º..., 255º), D (4º, 8º, 12º, 16º, 256º) [16]

مراحل زیر مراحل تشکیل دهنده روش "تجزیه" است:

1) الگوریتم تجزیه، توالی های 256 بایتی را از پرونده داده ها می خواند. من از این به بعد به این مجموعه بایت با عنوان I-Object اشاره خواهم کرد [16].
2) این الگوریتم اطلاعات کیفی ، کمی و اندازه I-Object را استخراج می کند و این اطلاعات را در دو آرایه، هر کدام با اندازه 256 عنصر ذخیره می کند: آرایه عدد صحیح کمی-کیفی [256] و آرایع کارکتر اندازه [256]. من از این به بعد از آرایه ها به عنوان بردار نام می برم [16].
3) بردار کمی-کیفی [256] برای هر بایت مختلف موجود در I-Object ، تعداد دفعات پیدا شدن این بایت در I-Object را ذخیره می کند. به عنوان مثال ، اگر بایت 1510 = 000011112، 20 بار در I-Object وجود داشته باشد ، مقدار کمی-کیفی [15] برابر با 20 خواهد بود. اگر بایت 1510 وجود نداشته باشد ، مقدار مورد Quantity-Quality [15] صفر خواهد بود [16].

4) برای هر یک از بردارهای کمی-کیفی ، الگوریتم تجزیه، اگر المان بردار بیشتر از صفر باشد، مقدار آن را در توالی بیت های '1' تبدیل می کند.

مثال: ’111’ = VectorBits [25] ⇒ 3= Quantity-Quality [25]. اگر المان بردار کمی-کیفی برابر با صفر باشد ، VectorBits هیچ مقداری را ذخیره نمی کند [16].

5) موارد موجود در VectorBits به شرح زیر با هم ادغام می شوند:

VectorBits [0] + ‘0’ + VectorBits [1] + ‘0’ +, ... + ‘0’ + VectorBits[255]، یک بردار با المان 512 تولید می کند که به عنوان ورودی در تابعی استفاده می شود که بردار را به توالی های 8 موردی می خواند و به نمایش ASCII متناظر تبدیل می شود و یک توالی 64 بایتی ایجاد می کند که در پرونده quantity-quality.dec نوشته می شود. مثال: ‘01000001’به حرف "A" تبدیل می شود [16].

6) بردار کاراکتر اندازه گیری شده [256] برای هر المان بردار کمی-کیفی 0 <[256]، ترتیب نمایش بایت ها در I-Object را ذخیره می کند. موقعیت بایت ها از 0 تا 255 متغیر است که نشان دهنده بایت اول تا 256 ام موجود در بلوک داده ها است. بردار از مقدار اعشاری بایت برای نشان دادن مقادیر موقعیت های بایت های I-Object استفاده خواهد کرد. جدول 2.18 مثالی را نشان می دهد که در آن بایت-1، 3 بار و بایت-3، 1 بار در I-Object رخ می دهد و هیچ رخدادی از بایت های 0، 2 و 255 وجود ندارد. بردار اندازه گیری شده [256] در پرونده measure. Dec ثبت شده است [16-17].

فایل های measured.dec و quantity-quality.dec در ارائه دهندگان فناوری ابری مختلف ذخیره می شوند. در این حالت هر یک از فایل ها برای بازسازی فایل اصلی کافی نیست. به عنوان مثال، با فرض اینکه ارائه دهنده ای که صاحب فایل quantity-quality.dec است، تلاش خواهد کرد تا یک بلوک 256 بایتی از فایل اصلی را بازسازی کند[18-19].

با استفاده از روش نیروی خام برای بازسازی دنباله 256 بایتی یک I-Object ، احتمال یافتن توالی صحیح بایت ها توسط ارائه دهنده و با دانستن این که کمیت و کیفیت یک جایگشت تکراری P با المان 256 است:ذ Prob = 1/P256 n1, n2, n3...,، که در آن ... n1, n2, n3 به عنوان موارد کمی شناخته می شوند. برای یک I-Object که فقط 1 بایت کیفیت یا کمیت دارد ، احتمال آن 1/256 است. برای I-Object با 2 بایت مختلف، احتمالاً تقریباً 1/1076 است [19] [20].

هرچه مقدار اقلام کمیت یا کیفیت افزایش یابد ، احتمال یافتن ترتیب بایت به صفر می رسد. با 10 بایت مختلف در I-Object، احتمال همانگاه به 1/10256 می رسد. احتمال ترکیب مجدد I-Object با استفاده از نیروی ناخالص 1/256 است، که تقریباً 1/10506 است. هر چه فایل بزرگتر باشد، دشواری مهاجم برای بازسازی آن بیشتر می شود [21].

مزایای این روش نسبت به روش های مرسوم که از رمزنگاری، برای اطمینان از محرمانه بودن داده های ذخیره شده در فضای ابری استفاده می کنند، به شرح زیر است [22]:

1) عدم استفاده از کلیدهای رمزنگاری. (i) کاربردی بودن این روش برای راه کار های SaaS، PaaS و IaaS بدون هیچ گونه تغییری در رابط های برنامه کاربر.
2) این روش می تواند در هر فرمتی از داده های ذخیره شده (داده ها و برنامه ها) اعمال شود.
3) هیچ محدودیت حداکثری در اندازه فایل وجود ندارد که ناشناس واقع شود. این راهکار از پاکسازی داده های ابری پشتیبانی می کند ، زیرا پرونده هایی که در ارائه دهندگان مجزا در دسترس هستند اطلاعات مربوط به داده های اصلی را فاش نمی کنند. اگر کاربر فضای ابری را ترک کند، داده ها می توانند به طور خودکار حذف شوند.

11. نتیجه

برای اینکه حداقل امنیت در سیستم های رایانش ابری وجود داشته باشد، باید از یک سیستم رمزنگاری استفاده کنیم، اگر امکان پذیر نبود باید از یک مدل پراکنده سازی داده ها استفاده کنیم. علاوه بر مسئله ی اصلی امنیت اطلاعات باید به موارد زیر نیز توجه کنیم:

الف) کنترل دسترسی

با وجود دسترسی آسان بسیاری از افراد ، شما باید روش های کنترل خوبی ایجاد کنید. علاوه بر اینکه دقیقاً می دانید چه کسی مجاز است چه چیزی را ببیند ، باید بدانید که آیا همه تجهیزات استفاده شده به درستی بیمه شده اند یا خیر. ایجاد رمزهای عبور قوی و متفاوت برای هر کاربر که مرتباً تغییر می کنند از اهمیت بسیاری برخوردار است. ما باید به سرعت، کاربرانی را که دیگر عضوی از شرکت یا سازمان نیستند، حذف کنیم.

ب) سرمایه گذاری بر آگاهی کاربر

این موضوع که همه ی افراد باید از اهمیت محافظت از داده ها مطلع باشند،از اهمیت فوق العاده ای برخوردار است. باید روی آموزش ایمنی به کاربر سرمایه گذاری شود. این کار را می توان از طریق کارگاه های آموزشی با بهترین نکات عملی و با یادآوری اهمیت عدم باز کردن لینک های مشکوک و حتی دوره های مربوط به امنیت اطلاعات ، انجام داد. اقدامات کوچک مانند قفل کردن دستگاه ها به هنگام ترک میز و اطلاع از به روزرسانی های جدید آنتی ویروس ها می تواند بسیار موثر باشد.

ج) پشتیبان گیری کنید

بنابراین، مهم است که همیشه دو یا حتی سه نسخه ی پشتیبان از اطلاعات داشته باشید. این نسخه پشتیبان همچنین می تواند در فضای ابری باشد، اما در سرور دیگری غیر از سرور اصلی که قبلاً استفاده شده است.

د) استفاده از رمز گذاری

داده هایی که در فضای ابری هستند فقط توسط افرادی که برای دسترسی به آنها رمز عبور دارند قابل دسترسی هستند. اما حتی با تمام اقدامات احتیاطی در رابطه با امنیت ، هنوز هم امکان نفوذ اطلاعات وجود دارد. به همین دلیل رمزنگاری بسیار مهم است. بنابراین حتی اگر کسی بتواند به اطلاعات برسد ، نمی تواند رمزگشایی کند مگر اینکه کلید آن را داشته باشد.

References

[1] SILVA, F. H. R.,"A study on the benefits and security risks of using Cloud Computing; 2010 15f", Scientific article of conclusion of course presented at the University Centre Augusto Motta, UNISUAM-RJ.

[2] HURWITZ, Judith; BLOOR, Robin; KAUFMAN, Marcia; HALPER, Fern,"Cloud Computing for Dummies", 1. ed Indiana, U.S.: Wiley Publishing, Inc; 2010. pp. 336.

[3] BUYYA, Rajkumar; BROBERG, James; GOSCINSKI, Andrzej,"Cloud Computing – Principles and Paradigms", 1. Ed New Jersey, U.S.: John Wiley & Sons, Inc. 2011. pp. 664.

[4] MELL, Peter; GRANCE, Timothy,"The NIST Definition of Cloud Computing (Draft)", January 2011. [Online] Available: http://csrc.nist.gov/publications/drafts/800-145/Draft-SP800-145_cloud-definition.pdf.

[5] CHIRIGATI, Fernando Seabra,"Cloud Computing", Rio de Janeiro, RJ. 2009. [Online] Available:

[6] KAUFMAN, L. M. Data,"Security in the World of Cloud Computing", IEEE Security and Privacy, 7(4): pp. 61-64, 2009

[7] SUN MICROSYSTEMS, INC.,"Introduction to Cloud Computing Architecture", White Paper, 1st edition, 2009a.

[8] DIKAIAKOS, M. D.; PALLIS, G.; KATSAROS, D.; MEHRA, P.; VAKALI, A.,"Cloud Computing – Distributed Internet Computing for IT and Scientific Research", IEEE Internet Computing, 13(5): pp. 10-13, 2009.

[9] MOURATO, Joao Carlos Gomes,"Security of Information Systems", 2008. 10 f. Article (Degree in Informatics Engineering) - School of Technology and Management - Polytechnic Institute of Portalegre, Portalegre, 2008.

[10] MARCON, Arlindo; LAUREANO, Marcos; SANTIN, Altair; MAZIERO, Carlos,"Aspects of Security and Privacy in Cloud Computing Environments", [Online] Available: http://professor.ufabc.edu.br/~joao.kleinschmidt/aulas/ seg2011/nuvem.pdf

[11] NOGUEIRA, Matheus Cadori; PEZZI, Daniel da Cunha, "Computing Now is in the Clouds", [Online] Available: http://www.inst-informatica.pt/servicos/informacao-edocumentacao/dossiers-tematicos/teste-dossier-tematicono-7-cloud-computing/tendencias/a-computacao-agora-enas-nuvens

[12] Aggarwal, C. C. (2005),"On k-anonymity and the curse of dimensionality", In Proceedings of the 31st international conference on Very large data bases, pp. 901–909. VLDB Endowment.

[13] Aggarwal, C. C., Philip, S. Y.,"A condensation approach to privacy preserving data mining", pp. 183–199. Springer, 2004.

[14] CAMENISCH, J., Fischer-Hübner, S., Rannenberg, K., "Privacy and identity management for life. Springer", 2011.

[15] Cao, J., Karras, P.,"Publishing microdata with a robust privacy guarantee", Proc. VLDB Endow., 5(11): pp. 1388– 1399, 2012.

[16] Chen, K., Liu, L.,"Privacy preserving data classification with rotation perturbation", In Proceedings of the Fifth IEEE International Conference on Data Mining, pp. 589–592. IEEE Computer Society.

[17] Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M. (1998),"Private information retrieval. Journal of the ACM (JACM)", 45(6), pp. 965–981. [Clarke 1999] Clarke, R. (1999). Introduction to dataveillance and information privacy, and definition of terms.

[18] Domingo-Ferrer, J.,"A survey of inference control methods for privacy-preserving data mining, pp. 53–80. Springer, 2008.

[19] Duncan, G. T., Keller-McNulty, S. A., Stokes, S. L., "Disclosure risk vs. data utility: The ru confidentiality map", In Chance. Citeseer, 2001.

[20] Fung, B. C., Wang, K., Fu, A. W.-C., Yu, P. S.," Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques", Chapman-Hall, 2010.

[21] Fung, B. C. M., Ke, W., Yu, P. S.,"Anonymizing classification data for privacy preservation", Knowledge and Data Engineering, IEEE Transactions on, 19(5), pp. 711– 725, 2007. [22] Gionis, A., Mazza, A., Tassa, T.,"k-anonymization revisited", In Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on, pp. 744–753. IEEE, 2008.