رمزنگاری در رایانش ابری

معصومه رئوف فوشازده [1]، اسماعیل ملک زاده سرایی [2]،پویان صالحی [3]، مینا چوپانی سفیدی [4]
۱و۳ گروه مهندسی کامپیوتر، موسسه آموزش عالی علوم و فناوری آریان، امیر کلا بابل
۲و۴ گروه مهندسی کامپیوتر، دانشکده علامه محدث نوری،نور

چکیده

الگوریتم های رمزنگاری بسیار متعدد هستند ، اما تنها تعداد اندکی از آنها به صورت استاندارد درآمده اند. رمزنگاری دانشی است که به بررسی و شناخت اصول و روش های انتقال و ذخیره سازی اطلاعات به صورت امن می پردازد. در سال‌های اخیر استفاده از منابع بهینه برای محاسبات داده‌های عظیم مورد توجه قرار گرفته است. نیاز به استفاده از زیرساختی برای فراهم آوردن انعطاف‌پذیری، ظرفیت بالای محاسباتی و توانایی ذخیره‌ی اطلاعات در حافظه‌های مستقل از مکان ایجاد شده است که این زیرساخت، رایانش ابری نامیده می‌شود. با این حال، ذات عمومی ابر موجب بروز چالش‌های امنیتی می‌شود بعبارتی کنترل فیزیکی از اطلاعات در ابر غیرممکن است. بنابراین، رمزنگاری اطلاعات حساس و حیاتی امری ضروری است. استفاده از رمزنگاری سمت سرور در محیط‌های غیرقابل اعتمادی همچون ابر، خطرناک است. در طرف دیگر رمزنگاری سمت کاربر می‌تواند مزایای برای ابر به همراه داشته باشد اما این کار زمان‌بر است. برای حل این چالش، ما ابر خصوصی را معرفی می‌کنیم که بعنوان میانجی مورد استفاده قرار می‌گیرد. در این مقاله، روش های تخصصی پیشنهاد شده است که می تواند به طور موثر اطلاعات را از ابتدا تا انتها محافظت کند، یعنی از مالک به ابر و سپس کاربر با توجه به مفهوم XaaS ، ما رمزنگاری را بعنوان سرویسی برای حل چالش‌های امنیتی در ابر ارائه می‌کنیم که خطرات ناشی از رمزنگاری سمت سرور و نیز ناکارآمدی رمزنگاری سمت کاربر را حل می‌کند.

کلمات کلیدی: پردازش ابری، رمزنگاری، پردازش موازی، امنیت

کارشناس ارشد کامپیوتر مهندسی هوش مصنوعی
Email: shaqaieq1067@yahoo.com

۱.مقدمه

ابر به طور عمده سیستم های ذخیره سازی خارج از سیستم را مدیریت می کند که توسط شخص ثالث نگهداری می شود. امروزه با توجه به افزایش استفاده از اینترنت و اطلاعات الکترونیکی، تغییرات وسیع و ناگهانی در نوع و تعداد سیستم‌های پردازشی شرکت‌ها ایجاد شده است. این تغییرات که هرروزه بر سرعت آن افزوده می‌شود موجب استفاده از رایانش‌های دینامیک مانند رایانش ابری شده است که رایانش ابری، زیرساختی به روز رسانی شده در لحظه‌ی تقاضا است و از طرفی هزینه‌ی استفاده از این رایانش کم است بعبارتی شما به میزان استفاده خود هزینه خواهید کرد. قابلیت ارتجاعی و انعطاف‌پذیری این رایانش موجب شده است که این زیرساخت مورد توجه شرکت‌های کوچک و یا ارگان‌های خاصی مانند بهداشت یا شرکت‌های بیمه شود. ابر تحت وب، انقلابی در زندگی روزمره‌ی جوامع بشری ایجاد کرده است به طوری که ما هرروزه قادر به تعامل لا یکدیرگ با استفاده از سرویس‌های تحت وب مانند گوگل، یاهو، آمازون و غیره هستیم. از طرف دیگر با توجه ذات رایانش ابری، مهاجرت به ابر موجب بروز چالش‌هایی برای شرکت‌ها می‌شود. چالش‌های مربوط به رایانش ابری به دو دسته تقسیم می‌شوند، چالش‌های تجاری و چالش‌های مربوط به فناوری[۱]. غیر از این چالش‌ها، امنیت همیشه معماری سیستم‌های سورس باز را به چالش می‌کشد. با توجه به اینکه برنامه و اطلاعات کاربر در موقعیت ارائه دهنده‌ی ابر قرار دارد نگرانی‌های جدی‌تری در زمینه‌ی امنیت مشاهده شده است. در حالت کلی، باید اطلاعات در برابر برخی از خطرات مانند سرویس‌های مضر، تخریب اطلاعات، سرقت اطلاعات و عدم حفظ حریم خصوصی به مانند خطراتی همچون قطع ارتباط یا شنود و برنامه‌های خصمانه امن نگهداری شوند.

در ابر که هیچ کنترل فیزیکی بر روی اطلاعات وجود ندارد، رمزنگاری به عنوان بهترین راهکار برای حفاظت از اطلاعات حساس به نظر می‌رسد. در حقیقت رمزنگاری برای محرمانگی و اصالت و یکپارچگی اطلاعات مورد استفاده قرار می‌گیرد. ویژگی چند کاربری و دسترسی آسان ارائه دهندگان ابر به اطلاعات، لزوم استفاده از رمزنگاری و کنترل دسترسی را برای حفظ محرمانگی اطلاعات نمایان می‌کند.

گرچه رمزنگاری بهترین راهکار برای حفاظت از اطلاعات حساس است اما در صورت استفاده از رمزنگاری سمت کاربر، به مزایای استفاده از ابر خدشه وارد شود. همچنین نگهداری از تمامی کلیدها و گواهی‌ها در سمت کاربر امن نیست. از طرف دیگر، رمزنگاری سمت سرور در محیطی عمومی دارای معایبی است. در این مقاله EaaS[۲] را ارائه خواهیم کرد و نشان می‌دهیم که کنترل و مدیریت اطلاعات با استفاده از رمزنگاری موجب حذف مشکلات ناشی از رمزنگاری در سمت کاربر و سرور می‌شود و همینطور موجب کاهش هزینه‌های عملیاتی می‌شود .

[2] Encryption as a service

۲.رمزنگاری

رمزنگاری علم کدها و رمزهاست . یک هنر قدیمی است و برای قرنها بمنظور محافظت از پیغامهایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل م یشده، استفاده شده است تا پیغامهای آنها محرمانه بماند.
هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم . این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و م یتوانند از رمزنگاری استفاده کنند.
اغلب این مساله باید تضمین شود که یک پیغام فقط میتواند توسط کسانی خوانده شود که پیغام برای آنها ارسال شده است و دیگران این اجازه را ندارند . روشی که تامین کننده این مساله باشد" رمزنگاری "نام دارد .رمزنگاری هنر نوشتن بصورت رمز است بطوریکه هیچکس بغیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.
رمزنگاری مخفف ها و اصطلاحات مخصوص به خود را دارد . برای درک عمیق تر به مقداری از دانش ریاضیات نیاز است.

۳.مرور ادبیات

در محیط‌های غیر قابل اعتماد مانند ابر عمومی، محاسبات و ذخیره‌ی اطلاعات باید به اندازه کافی امن باشد. در این قسمت، برای اینکه یک ابر را امن و قابل اعتماد کنیم، در مورد برخی تکنیک‌های رمزنگاری که قابلیت بکارگیری در ابر را دارند بحث خواهیم کرد. علاوه بر این برای برقراری امنیت فیزیکی سنتی، متدهای مجازشناسی و احراز هویت از برخی تکنیک‌های رمزنگاری مانند رمزنگاری مبتنی بر هویت، رمزنگاری مبتنی بر ویژگی، رمزنگاری هممورفیک و رمزنگاری قابل جستجو، ایزوله کردن رمزنگاری و رمزگشایی، ترکیب رمزنگاری‌های متقارن و نامتقارن بهره خواهیم برد.

۴.رمزنگاری مبتنی بر هویت

شمیر، استفاده از هویت یک فرد برای رمزنگاری را معرفی کرد که در این روش هویت فرد مانند آدرس ایمیل با یک گواهی دیجیتالی جایگیزین می‌شود.[۲]. در [۳] بائورا از رمزنگاری مبتنی بر هویت برای ایجاد امنیت در محیط سلامت استفاده کرده است. روش پیشنهادی توسط بائورا، بر دوفاز مبتنی است. هدف از فاز یک، ایجاد ارتباطی امن مابین نهادهای مختلف حاضر مانند کاربر، ارائه‌کننده‌ی سرور و درخواست کننده‌ی اطلاعات و ابر است. برای رسیدن به این هدف، پس از تنظیمات اولیه توسط ارائه دهنده‌ی سرور، کاربر اطلاعات را با استفاده از کلید عمومی و هویت گیرنده‌ی اطلاعات رمز می‌کند. سپس تایید اصالت اطلاعات با استفاده از امضای دیجیتالی در سمت گیرنده و با هدف تقویت اصالت اطلاعات انجام می‌گیرد.
فاز دوم بر دسترسی مناسب درخواست‌کنندگات تاکید دارد. با توجه به اینکه کاربر از هویت فرد درخواست کننده‌ی اطلاعات آگاهی ندارد، اطلاعات باید بر اساس سیاست‌هایی رمز شوند و با استفاده از سیاست‌هایی به درخواست کنندگان

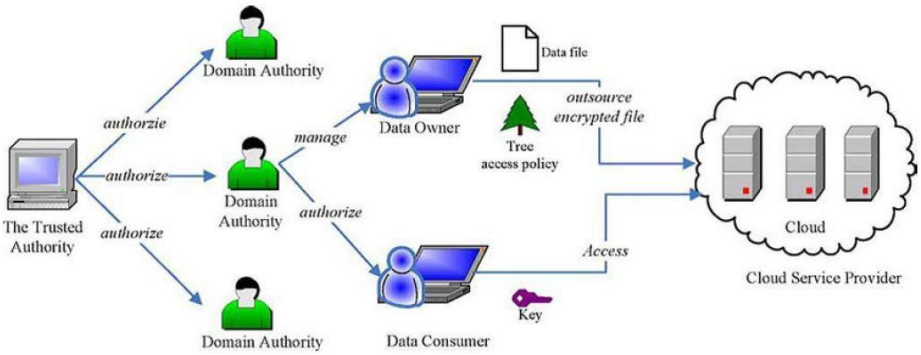
اطلاعات، دسترسی داده شود. نویسنده، درخت دسترسی طراحی کرده است که این درخت مبتنی بر نقش‌های مختلف و نیز سطح حریم خصوصی است. در این سناریو، درخواست کننده‌ی اطلاعات قادر به یادگیری ویژگی‌های غیرضروری نیست.

۵.رمزنگاری مبتنی بر ویژگی

در زمینه‌ی محاسبات قابل اعتماد، رمزنگاری مبتنی بر ویژگی برای حل چالش‌های مرتبط به کنترل دسترسی مبتنی بر نقش ایجاد شد. در این روش، متن رمز شده باید مربوط به فرمولی به نام فرمول دسترسی باشد درحالی که کلید به دسته‌ای از ویژگی‌ها مربوط می‌شود. چنانچه این ویژگی‌ها، فرمول دسترسی را راضی کنند، اجازه‌ی دسترسی به اطلاعات صادر می‌شود. این ایده برای اولین بار توسط ساهای و واترز معرفی شد[۴].

در رایانش ابری که اطلاعات رمز شده بر روی سرورهایی ذخیره می‌شوند باید کلیدهای مخفی برای کاربران مجاز فاش شوند. این عملیات، نیازمند مکانیزمی کارآمد برای مدیریت و توزیع کلید است. با توجه به وجود تعداد زیادی از کاربران مجاز و یا حذف کاربران غیرمجاز، کارآمدی سیستم کاهش خواهد یافت. از این روی، وان روش CP_ASBE که توسط بووبا [۵] ارائه شده است را بکار گرفت و تنها ساختاری سلسله مراتبی که مقیاس‌پذیری و انعطاف‌پذیری را فراهم کند به آن افزود. در یک ساختار سلسله مراتبی که در تصویر ۱ نشان داده شده است طرف سوم مورد اعتماد، شاه کلیدها را توزیع و مدیریت می‌کند و همینطور دامنه‌ی اختیارات و صاحب و مصرف‌کننده‌ی اطلاعات را برای رمزنگاری و رمزگشایی تعیین می‌کند و همینطور ایجاد نمایندگی برای استفاده از کلید در زیر دامنه‌ها را تعریف می‌کند. اطلاعات در سرورهای ارائه دهنده‌ی ابر ذخیره می‌شود. با توجه به CP_ASBE ، مالک یا مصرف کننده‌ی اطلاعات، وظایف خود را به نهادهای مورد نظر منتقل می‌کنند بنابراین مالک و یا مصرف‌کننده‌ی اطلاعات در زمان‌های ضروری آنلاین می‌شود. امنیت روش برابر با سطح امنیتی در CP_ABE است[۶].

شکل ۱. نمایش مدل سیستم سلسله مراتبی در طرح HSABE



۶.رمزنگاری هممورفیک و قابل جستجو

با ظهور رایانش ابری و ضرورت طرف مورد اعتماد سوم برای ذخیره و پردازش اطلاعات، احتمال تصادم در اطلاعات افزایش یافت. بنابراین، محققان به مدولاسیون رمزنگاری در محیط‌های غیر قابل اعتمادی چون ابر پرداختند. رمزنگاری جستجوپذیر و هممورفیک تکنیکی است که موجب می‌شود بدون رمزگشایی اطلاعات، بر روی اطلاعات پردازش انجام داده و تغییراتی اعمال کرد.

بونه، مدلی برای رمزنگاری ارائه کرده است که جستجو بر روی کلمات کلیدی را فراهم می‌کند. برای مثال، او توانست کلیدواژه‌ای را در یک ایمیل رمز شده و بدون رمزگشایی آن پیدا کند[۷].

گنتری[۸] موجب بروز انقلابی در رمزنگاری هممورفیک شد که در آن متن رمزشده از رب کلید و عدد تصادفی q بعلاوه‌ی متن اصلی بدست می‌آید. $c = p*q + m$.

هوو، روشی برای جستجوی اطلاعات ارائه کرد که در این روش درخواست‌کننده‌ی اطلاعات می‌توانند با حفظ حریم خصوصی به اطلاعات مورد نیاز خود در محیط‌های ناامن دسترسی داشته باشند. این روش به دو فاز تقسیم می‌شود. در فاز اول، نویسندگان برای جستجو بر روی اطلاعات رمز شده با استفاده از کلیدواژه‌ها، از رمزنگاری هممورفیک استفاده می‌کنند در ایت فاز، اینگونه فرض شده است که ادمین، کاربری قابل اعتماد است که تمامی درخواست‌ها را پاسخ می‌دهد. البته ادمین قادر به کسب اطلاعات در مورد کلیدواژه یا اطلاعات نیست چرا که ادمین دارای کلید خصوصی برای رمزگشایی اطلاعات نیست. در فاز دوم، آنها فرضیات اولیه در مورد ادمین را ابطال می‌کنند و سپس تمامی تختیارات اعطا شده به ادمین، به طرف مورد اعتماد سوم منتقل می‌شود. [۹]

در نهایت، سوتار و پاتیل چارچوبی در رایانش ابری با استفاده از در نظر گرفتن سه طرف ابر، کاربر و سرور ابری ارائه کرده‌اند. سپس آنها اطلاعات افراد را به سه دسته‌ی اطلاعات قابل تشخیص توسط فرد، اطلاعات حساس مانند رمز عبور و اطلاعات عمومی مانند شماره‌ی ثبت نام تقسیم کرده‌اند و در نهایت با استفاده از رمزنگاری هممورفیک، مکانیزمی برای تبادل این اطلاعات مابین سه طرف مورد نظر ارائه شده است. بنابراین گمنامی برای حفظ حریم خصوصی فراهم می‌شود. در این کار، احراز هویت توسط طرف سوم انجام می‌گیرد که کارت‌های اعتباری افراد را با کارتهای اعتباری موجود در سرور ابر مقایسه می‌کند. در این کار، نویسندگان فرض کرده‌اند که سرور ابری به اندازه کافی برای نگهداری اطلاعات کاربران امن است از این روی این روش بیشتر برای احراز هویت کاربران پیشنهاد شده است تا اینکه به پردازش اطلاعات در محیط‌های چندکاربره پیشنهاد شود[۱۰].

۷.ایزوله کردن رمزنگاری و رمزگشایی

این دسته از تحقیقات نشان می‌دهد که چگونه می‌توان اطلاعات رمز شده و کلید رمزنگاری را می‌توان در یک ابر عمومی نگهداری کرد. یک روش برای مواجهه با این مشکل، استفاده از تقسیم مجازشناسی است بطوریکه در مدیریت تجارت نیز رایج است. بعنوان مثال، یک منشی با یک حسابدار دارای توانایی‌های متفاوتی در پردازش بر روی یک سند موجود در یک شرکت است.

هووآنگ نمونه‌ای از این مدل تجاری را در ابر ارائه کرده است که در آن رمزنگاری و رمزگشایی عملیاتی جدا از ذخیره‌سازی اطلاعات است.[۱۱]. برای مثال کاربران برای مجازشناسی یک برنامه‌ی ورودی را اجرا می‌کنند، سپس زمانی‌که یک برنامه‌ی CRM[3] کاربر را به عنوان فردی مجاز تشخیص داد، این درخواست به همراه شناسه (ID)[4] کاربر به ابر ارسال می‌شود. پس از یافتن اطلاعات رمزشده‌ی مرتبط، اطلاعات و شناسه کاربر به سرویس رمزنگاری و رمزگشایی ارسال می‌شود تا اطلاعات از رمز خارج شود. این اطلاعات رمزگشایی شده، با استفاده از کانالی امن در اختیار درخواست کننده قرار می‌گیردو سپس سرویس رمزنگاری و رمزگشایی، تمامی اطلاعات مربوط به پردازش را حذف خواهد کرد.

[3] Customer Relationship Management
[4] Identity

۸.ترکیب الگوریتم‌های متقارن و نامتقارن

کونسولو راهکاری را ارائه کرد که با استفاده از ترکیب الگوریتم‌های متقارن و نامتقارن و با عملکردی بهتر از الگوریتم نامتقارن و همچنین با امنیتی بیشتر عمل می‌کند. در راهکار ارائه شده، اطلاعات باید با استفاده از یک الگوریتم رمزنگاری متقارن رمز شوند درحالی که کلید مربوطه را می‌توان با استفاده رمزنگاری نامتقارن رمز کرد. با توجه به اینکه رمزنگاری نامتقارن دارای جفت کلید عمومی و خصوصی است، تنها دارنده‌ی کلید خصوصی می‌تواند کلید متقران را از رمز خارج کند. ذخیره‌ی کلید عمومی در کنار اطلاعات موجب دسترسی به اطلاعات و کلید عمومی توسط مالک در هر نود توزیع شده در شبکه می‌شود. در این کار، اینگونه فرض شده است که عملیات رمزگشایی مشابه با ذخیره‌ی گواهی کاربر در نود کاربر صورت می‌گیرد.[۱۲]

بسیاری از تکنیک‌هایی که در بالا ارائه شد در حال حاضر فقط جنبه‌ی تئوری دارند و نیازمند زمان بسیاری برای پیاده‌سازی عملی آنها است. راهکاری که ما ارائه می‌کنیم استفاده از طرف سوم مورد اعتمادی است که رمزنگاری را بعنوان سرویسی به رایانش ابری می‌افزاید.

روش:

با توجه به ایجاد طرف سوم مورد اعتمادی در نقش ، EaaS ، باید سه مرحله را انجام دهیم. ابتدا، ابر خصوصی پیاده‌سازی کنیم سپس الگوریتمی برای رمزنگاری ارائه کنیم و در نهایت، ویژگی‌های چند رشته‌ای و مبتنی بر تعداد هسته‌های VM تعریف کنیم.

۹.پیاده‌سازی ابر خصوصی

یک ابر خصوصی به کاربران اجازه می‌دهد که بر روی زیرساخت وامنیت کنترل بیشتری داشته باشند زیرا که شبکه و دسترسی ها محدود می‌شود. علاوه بر این در یک ابر خصوصی، اطلاعات پردازش شده توسط سازمان، در برابر استفاده‌های غیرقانونی حفاظت می‌شوند و محدودیت‌های پهنای باند در حین پردازش تاثیری ندارد. اما، ابر خصوصی از منابع محاسباتی بزرگی برخوردار نیست اما با این حال به اندازه‌ای بزرگ است که مزایای رایانش ابری را به همراه داشته باشد. بنابراین، در ابر خصوصی، تقسیم بار کاری کاربر بر روی منابع با توجه به وسعت شرکت موردنظر شدنی است.[۱۳]

از طرف دیگر در یک ابر خصوصی، گروهی از کاربران وجود دارند که می‌توانند نمونه‌های خود را به اشتراک بگذارند. بنابراین، در دسترسی بودن سرویس‌ها در یک ابر خصوصی تضمین می‌شود.

برای پیاده‌سازی یک ابر خصوصی، نیازمند به کارگیری چارچوبی برای طراحی و پیاده‌سازی IaaS[۵] هستیم. تعدادی از چارچوب‌های معروف در این زمینه OpenNebula و Nimbus و OpenStack و Eucalyptus است.

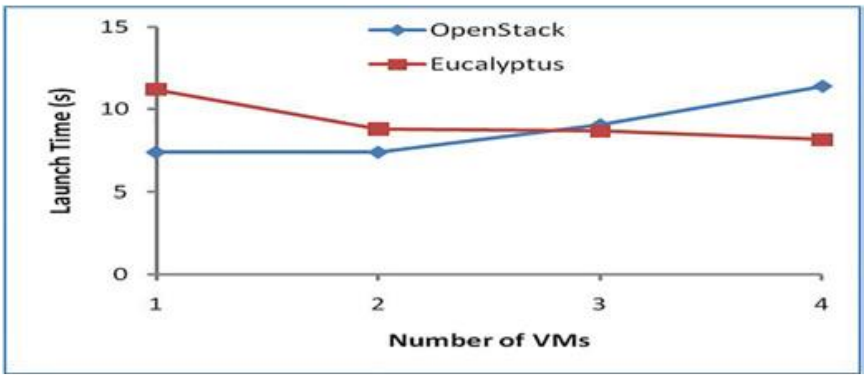
در حقیقت، چارچوب مناسب به کاربر و کاربرد موردنظر بستگی دارد. OpenNebula دارای راه‌اندازی ساده است گرچه سایر چارچوب‌ها مانند Eucalyptus در ورژن نهایی بهبود یافته‌اند. با توجه به اینکه OpenNebula دارای هیچ سیستم کش[۶] برای تصاویر نیست با این حال این چارچوب دارای سرعت توسعه‌ی پایینی است. Eucalyptus و OpenStack معمولا در زمانی که سرورها تعداد کمی هستند بسیار عالی عمل می‌کنند اما، برای سرورها و VM های با تعداد زیاد، زمان و تعداد شکست‌ها افزایش می‌یابد. Nimbus دارای شبکه‌ی مدیریتی قابل قبولی نیست و همینطور VM در این چارچوب قابل استفاده نیست و با توجه به اینکه این چارچوب حدود چهار ماه است که ارائه شده است این موضوع را می‌توان بعنوان یکی از معایب این چارچوب در نظر گرفت. سرویس‌های تحت وب آمازون، استانداردی عملی و یکی از

[5] Infrastructure as a service
[6] Cashing system

بهترین ابرهای عمومی می‌توان در نظر گرفت. قابلیت سازگاری با این سرویس را می‌توان بعنوان استانداردی ضروری در نظر گرفت. در میان این چارچوب‌ها OpenStack با EC2 و S3 سازگار نیست.[۱۴]

در [۱۵]، نویسندگان مقایسه‌ای مابین OpenStack و Eucalyptus انجام داده‌اند. آنها زمان مورد نیاز برای دسترسی به یک منبع در هنگام راه‌اندازی یک نمونه را اندازه‌گیری کرده‌اند و این المان را VM launch-time[۷] نامیده‌اند. در هنگان راه‌اندازی VM ها بصورت سری، OpenStack بسیار سریعتر عمل می‌کند اما در صورت راه‌اندازی آنها بصورت موازی، در هنگام وجود ۳، چهار و بیشتر VM ها، Eucalyptus سریعتر عمل می‌کند که در تصویر ۲ نشان داده شده است. دلیل این اتفاق این است که Eucalyptus تصاویر را برای نمونه‌های مختلف ارسال نمی‌کند. در نهایت، با توجه به مقایسه‌ی رابط این دو چارچوب، نویسندگان ادعا کردند که Horizon در OpenStack به اندازه‌ی Right Scale در Eucalyptus قوی نیست. برای مثال،یکپارچه‌سازی یک ابر خصوصی در یک ابر عمومی با استفاده از رابط مجاز است.

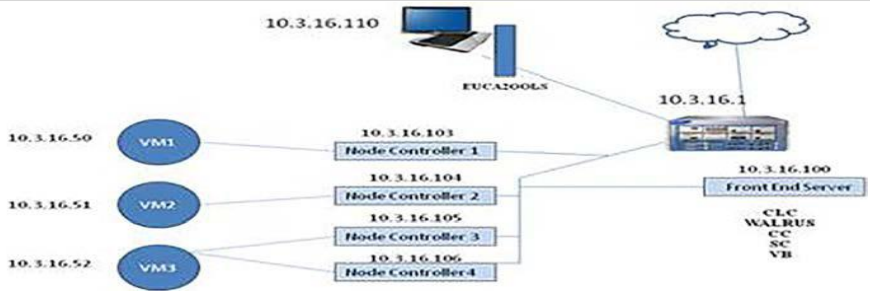
شکل ۲. نمایش زمان راه اندازی موازی VM



Eucalyptus از ۶ مولفه، کنترل‌کننده‌ی نود که در همان ماشین با نمونه‌های ماشین مجازی است و منابع ضروری را فراهم می‌کند، مولفه‌ی اختیاری VB در هنگام استفاده از VMware hypervisor، کنترل‌کننده‌ی خوشه‌بندی و ذخیره‌سازی و کنترل‌کننده‌ی ابر و walrus برای مدیریت و درخواست از مولفه‌های دیگر استفاده می‌کند. برای افزایش تعامل مابین Walrusو CLC و همین‌طور سهولت در مدیریت، تمامی مولفه‌ها به غیر از NC[۸] را در یک ماشین فیزکی که در تصویر ۳ نشان داده شده است پیاده‌سازی کرده‌ایم. مولفه‌ی کنترل کننده‌ی نود همراه با hypervisor ضروری در چهار ماشین قرار گرفتند. و در نهایت از یک لپ‌تاپ و با استفاده از EUCA2OOLS و dashboard برای مدیریت مولفه‌های ابر استفاده کردیم.

شکل ۳. نمونه خصوصی پیکربندی ابر

[7] virtuele machine
[8] Networking Computer



۱۰.کتابخانه‌ی رمزنگاری

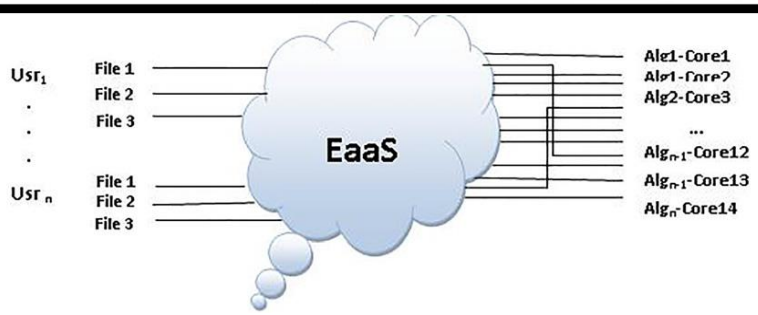
همانطور که قبلا گفته شد، رمزنگاری می‌تواند محرمانگی و اصالت اطلاعات را فراهم کند. بنابراین روش مابايد امنیت معنایی اطلاعات را در برابر حملات متن رمزشده‌ی انتخابی، جلوگیری از تخریب اطلاعات، تزریق پیام توسط مخرب را حفظ کند. با توجه به اینکه محرمانگی فقط امنیت در برابر شنود را حفظ می‌کند باید از کد احراز هویت پیام MAC[9] برای حفظ اصالت استفاده کنیم. تنها راه برای حفظ محرمانگی و اصالت، استفاده از رمزنگاری احراز هویت شده است. کتابخانه‌ی CryptoPP انواع الگوریتم‌ها و انواع مدهای رمزنگاری را شامل می‌شود بنابراین برای هدف ما مناسب است. برای ترکیب رمزنگاری و MAC ، ۳ استراتژی مختلف وجود دارد، اگر رمزنگاری در در ابتدا استفاده شود مانند پروتکل IPSEC[10]، کاملا امن در نظر گرفته می‌شود در حالی که استفاده‌ی همزمان بر روی متن اصلی همانند SSH[11] ناامن است. پروتکل SSL[12] ، رمزنگاری را پس از احراز هویت انجام می‌دهد و در بعضی از ساختارها می‌تواند امن باشد.[۱۶]

۱۱.مدل چند رشته‌ای

در سناریوی ما، چندکاربری‌ها به گروه امنیتی که از الگوریتم‌های مشابه یا متفاوت استفاده می‌کند تعلق دارد.. هر کدام از این گروه‌ها، چندین فایل دارند که می‌توانند رمزنگاری یا رمزگشایی شوند. چنانچه برنامه بصورا چندرشته‌ای نوشته نشود در EaaS عملکرد بهینه‌ای را شاهد نخواهیم شد. در حالت قبل، بسیاری از عملیات‌ها طی یک روند متوالی انجام شد که موجب استفاده‌ی بیش از حد منابع می‌شود. بنابراین ما نیازمند استفاده از پردازش موازی در برنامه‌ی خود هستیم. سهولت، انعطاف‌پذیری و قابل حمل بودن موجب شده است که OpenMP[13] بعنوان کتابخانه‌ای مناسب برای پیاده‌سازی موازی بکارگرفته شود. زمانی که یک رشته به ناحیه‌ی موازی شده وارد می‌شود، گروهی از رشته‌ها را ایجاد می‌کند. تنظیم تعداد رشته‌ها به تنظیم برخی از ویژگی‌های بولین در کتابخانه‌ی OpenMP بستگی دارد. با توجه به اینگه تعدادی VMware با هسته‌های مختلفی داریم، می‌توانیم تنظیمات مقیاس‌پذیری را با توجه به هسته‌های CPUموجود در هر VM تنظیم کنیم.از طرفی دیگر، تنظیمات مهم دیگری برای موازی‌سازی مربوط به انتخاب یک الگوریتم زمان‌بندی مناسب است. در میان چهار الگوریتم در پردازش زمان‌بندی، الگوریتم guided ، سربار کمتری را در زمان‌بندی‌های پردازشگرهای مختلف ایجاد می‌کند.

شکل ۴. چند نخی در EaaS

[9] Media Access Control
[10] Internet Protocol Security
[11] Secure Shell
[12] Secure Sockets Layer
[13] Open Multi-Processing



۱۲.نتایج و نتیجه‌گیری

در رایانش ابری که چند مالکیتی، مجازی‌سازی و ویژگی‌های برون‌سپاری موجب افزایش خطرات امنیتی می‌شود و هیچ‌گونه کنترل فیزیکی بر روی اطلاعات وجود ندارد اطلاعات را می‌توان با استفاده از رمزنگاری و مدیریت کلید و اعطای کلید به افراد مجاز، امن کرد. با این حال پیدا کردن طرف سوم مورد اعتمادی برای توزیع کلید در چنین محیطی کاری سخت است. برای حل این مشکل، باید تکنیک‌های رمزنگاری را برای محیط ابری بهینه کرد. برخی محققان با استفاده از ترکیب رمزنگاری و احراز هویت سعی در برطرف کردن این مشکل داشته‌اند. احرازهویت مبتنی بر هویت و مبتنی بر ویژگی نمونه‌ی مناسبی برای چنین تحقیقات است. برخی دیگر سعی در ارائه‌ی مدلی با استفاده از ایزوله کردن رمزنگاری و رمزگشایی ار سرویس ذخیره‌سازی در ابر داشته‌اند. راهکار دیگری که بر مدیریت کلید تاکید دارد، استفاده از ترکیب الگوریتم‌های رمزنگاری متقارن و نامتقارن است. یکی از بهترین راهکارها که محققان زیادی نیز در این زمینه فعالیت کرده‌اند استفاده از رمزنگاری هممورفیک است که تمامی عملیات‌ها در این رمزنگاری بر روی اطلاعات رمز شده صورت می‌گیرد. با این حال، این راهکار در عمل بسیار کند است.

بنابراین اولین مشکل در رایانش ابری نبود تعاملی مابین رمزنگاری سمت کاربر و سمت سرور است. رمزنگاری سمت سرور با بکارگیری منابع ابر دارای سرعت بسیار بالایی در رمزنگاری و رمزگشایی است اما این عملیات در طرف سوم غیرقابل اعتماد انجام می‌گیرد. رمزنگاری سمت کاربر دارای امنیت بالایی است اما مزایای رایانش ابری را تحت تاثیر قرار می‌دهد. پس به نظر می‌رسد که پیاده‌سازی یک ابر خصوصی بعنوان طرف سوم مورد اعتماد که رمزنگاری را بعنوان سرویسی ارائه کند می‌تواند این مشکلات را برطرف کند. در تصویر ۶، زمان برای ۶ الگوریتم انتخاب شده نشان داده شده است که این الگوریتم‌ها در سمت کاربر و با استفاده از Eaas ارائه شده بدست آمده‌اند. یک ماشین شامل پردازشگر i5_intel با 3 gb RAM انتخاب شده است و همین‌طور برای EaaS ارائه شده توسط ما یک VM با ۱۴ هسته و ۳۲ گیگا بایت RAMدر نظر گرفته شده است. تمامی آزمایش‌ها بر روی فایل متنی 300MB انجام شده است. جدول نشانگر افزایش قابل‌توجه در زمان رمزنگاری و رمزگشایی فایل مورد نظر است. این جدول نشانگر این است که روش ارائه شده‌ی ما، ۶بار بهتر از یک کامپیوتر تنها عمل می‌کند. بکارگیری منابع ابر و استفاده از چندرشته‌ای می‌تواند اصلی‌ترین دلیل این عملکرد باشد.

مراجع

[1] Yang H, Tate M. Where are we at with cloud computing?: a descriptive literature review.ACIS 2009 Procedding. 2009.
[2] Shamir A. Identity-based cryptosystems and signature schemes. Advances in cryptology, Springer;1985, p.47-53.
[3] Barua M, Liang X, Lu R, Shen X. ESPAC: Enabling Security and Patient-centric Access Control for eHealth in cloud computing.International Journal of Security and Networks; 2011; 6(2), p.67-76.
[4] Sahai A, Waters B. Fuzzy identity-based encryption. Advances in Cryptology–EUROCRYPT 2005, p. 557.
[5] Bobba R, Khurana H, Prabhakaran M. Attribute-sets: A practically motivated enhancement to attribute-based encryption. Computer Security–ESORICS 2009, p.587-604.
[6] Wan Z, Liu J, Deng R. HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing.Information Forensics and Security, IEEE; 2012; 7(2), p.743-754.
[7] Boneh D, Di Crescenzo G, Ostrovsky R, Persiano G. Public key encryption with keyword search. Advances in Cryptology-Eurocrypt 2004,Springer; 2004, p.506-522.
[8] Gentry C. Computing arbitrary functions of encrypted data. Communications of the ACM; 2010; 53(3), p.97-105.
[9] Hou S, Uehara T, Yiu S, Hui LCK, Chow K. Privacy Preserving Confidential Forensic Investigation for Shared or Remote Servers. Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Seventh International Conference on, IEEE; 2011, p.378-383.
[10]Sutar S, Patil G. Privacy Management in Cloud by making use of Homomorphic Functions. International Journal of Computer Applications;2012; 37(2), p.13-16.
[11] Hwang JJ, Chuang HK, Hsu YC, Wu CH. A business model for cloud computing based on a separate encryption and decryption service.Information Science and Applications (ICISA), International Conference on, IEEE; 2011, p.1-7.
[12] Cunsolo VD, Distefano S, Puliafito A, Scarpa M. Achieving Information Security in Network Computing Systems. Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference; 2009, p.71-77.
[13] Armbrus M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A view of cloud computing. Commun. ACM; 2010; 53(4), p.50-58.
[14] Laszewski G, Diaz J, Wang F, Fox GC. Comparison of multiple cloud frameworks. Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on, IEEE; 2012, p.734-741.
[15] Steinmetz D, Perrault BW, Nordeen R, Wilson J, Wang X. Cloud Computing Performance Benchmarking and Virtual Machine Launch Time. Proceedings of the 13th annual conference on Information technology education, ACM; 2012; p.89-90.
[16] Krawczyk H. The order of encryption and authentication for protecting communications (or: How secure is SSL?). Advances in Cryptology—CRYPTO 2001, Springer, p.310-331.