الگوریتم رمزنگاری جدید جهت افزایش امنیت داده در معماری رایانش ابری

میلاد رجبی پنبه چوله، کارشناسی ارشد، روزبهان ساری
Milad.rajabipn@gmail.com
مجید ابوطالبی، استادیار، هیئت علمی دانشکده فنی آزاد ساری
Majidaboutalebi@gmail.com

چکیده

با پیشرفت فناوری IT و همچنین رایانش ابری لزوما وجود یک معماری جامع و امن برای چنین محیطی دائما خودنمایی می کند، که دراین بین سازمان NIST به عنوان یکی از مهمترین موسسه ملی فناوری استاندارد در رایانش ابری بوده که با هدف اندازه گیری به وجود آمده است که رهبران این موسسه را سازمان های فدرال و پلیسی تشکیل می دهند. این گزارش تغییراتی برروی معماری NIST به وجود آمده با هدف افزایش محرمانگی داده، مشکل اصلی این معماری افشای اطلاعات در مقابل نفوذ هکر به این معماری بوده است که با اضافه نمودن یک الگوریتم رمزنگاری(صفت) در قسمت ابتدا و انتهای ابر دلال در معماری این مشکلات رفع گردید،الگوریتم رمزنگاری صفت CP-ABE بر اساس 3 مرحله ایمن سازی انجام می دهد، در فاز اول برای راه اندازی و تولید کلید می باشد در فاز دوم مربوط به رمزگذاری و کدگذاری داده و فاز سوم برای بازگشایی و استخراج داده خواهد بود. و در مرحله پیاده سازی ما با نرم افزار شبیه سازی اکلیپس که نوع زبان برنامه نویسی جاوا می باشد و الگوریتم پیشنهادی را با دو الگوریتم از نوع متقارن مقایسه نمودیم، و همچنین در انتها معماری پیشنهادی SNIST را با معماری پایه که NIST باشد در اکلیپس پیاده سازی نمودیم که نتایج نشان دهنده این بوده که طرح پیشنهادی ما افزایش گذردهی و محرمانگی نسبت به معماری پایه را دارا بوده است.

کلیدواژه‌ها: رایانش ابری، معماری ان آی اس تی، الگوریتم سی پی ای بی ایی

1- مقدمه

امروزه رایانش ابری [1] به عنوان یکی از کلیدی ترین ابزار در صنعتی سازی فعالیت های مهندسی بالاخص مهندسی نرم افزار و فناوری اطلاعات مطرح است. این فناوری به دلیل آن که مبتنی بر ابزار شبکه و مخصوصا اینترنت می باشد، باعث شده است تا تولیدات مهندسی کامپیوتر همواره در دسترس باشند. از سوی دیگر رایانش ابری امکان برون سپاری بسیاری از خدمات مهندسی را برای سازمان ها فراهم اورده است. از اینروست که مسئله امنیت درمحیط های رایانش ابری به چالشی اصلی بدل شده است. رایانش ابری، یک مدل رایانشی است که بر پایه شبکه‌های رایانه‌ای مانند اینترنت دایر شده است و به ارایه الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی (شامل زیرساخت، نرم‌افزار، بستر، و سایر منابع رایانشی) می پردازد[2] . به عنوان مثال آنچه یک ارائه‌دهنده خدمات نرم‌افزاری رایانش ابری ارائه می‌کند، برنامه‌های کاربردی تجاری آنلاین است که از طریق مرورگر وب یا نرم‌افزارهای دیگر به کاربران ارائه می‌شود. نرم‌افزارهای کاربردی و اطلاعات، روی سرورها ذخیره می‌گردند و براساس تقاضا در اختیار کاربران قرار می‌گیرد. جزئیات از دید کاربر مخفی می‌مانند و کاربران نیازی به آشنایی یا کنترل در مورد فناوری زیرساخت ابری که از آن استفاده می‌کنند ندارند. رایانش ابری به عنوان یک فناوری غالب در صنعت کامپیوتر و مخصوصا نرم افزار تبدیل شده است. این فناوری باعث رواج صنعت نرم افزار شده است، به گونه ای که با استفاده از آن، کاربران و مشتریان می توانند به راحتی به خدمات متنوع نرم افزاری دسترسی داشته باشند و به راحتی با تغییر و پیکربندی مجدد این خدمات، نیازهای متفاوت و جدید خود را برطرف نمایند. همزمان با توسعه صنعت نرم افزار و رشد تصاعدی مشتریان و علاقه مندی آنها به فناوری رایانش ابری، امنیت به عنوان یک معیار تعیین کننده از اهمیت دوچندانی برخوردار گردید. زیرا از طریق این فناوری مشتریان اغلب به خدمات نرم افزاری و سخت افزاری ای دسترسی داشتند که محل ارایه خدمات در مکانی به غیر از سازمان درخواست کننده بود. امروزه امنیت به عنوان یکی از مهمترین چالش های فناوری رایانش ابری، مورد مطالعه اغلب محققان می باشد. مهمترین گام در تامین امنیت، تشخیص تهدیدات احتمالی و ارایه فرآیندهای امنیتی و محافظتی لازم می باشد. در این راستا برای فناوری رایانش ابری سازمان های استاندارد گزار معماری های متفاوتی ارائه کرده اند که هر یک از نظر سطح امنیتی با توجه به لایه های امنیتی موجود در معماری ویژگی های خاص خود را دارد. این پژوهش با بررسی الگوریتم های رمزنگاری و سیاست های امنیتی رایج به ارائه یک معماری امن برای فناوری رایانش ابری می پردازد . طبیعی است که این معماری علاوه بر افزایش سطح امنیتی باید کاهش محسوسی در معیار های کارایی نداشته باشد[3].

2- بیان مسئله

امروزه فناوری از رایانش ابری به عنوان یکی از مهمترین دستاوردهای علم کامپیوتر که زمینه ساز صنعتی شدن این رشته را فراهم نموده است، یاد می گردد. در این فناوری ابر، ابزاری است جهت برون سپاری خدمات و باعث فراهم آمدن امکان استفاده تخصصی تر و کاراتر از منابع می گردد. فناوری رایانش ابری در دو بخش ذخیره و بازیابی اطلاعات و پردازش آنها کاربردهای فراوانی یافت. بنابراین و به تدریج شرکت ها و موسسات پیشرو به ارایه معماری های استانداری در این زمینه اقدام نمودند. در این بین موسسه NIST یکی از مهمترین موسسات استاندارد گذار در این زمینه می باشد. حفظ امنیت داده یکی از مهمترین دغدغه های کاربران و مشتریان در محیط های رایانش ابری می باشد. افزایش سطح محرمانگی داده یکی از راهکارهای رایج برای افزایش امنیت به شما می رود. رمزنگاری به عنوان یکی از مهمترین راهکارهای افزایش محرمانگی داده مد نظر می باشد. برای این منظور با استفاده از تکنیک رمزنگاری و سایر تکنیک های رایج می توان داده ها را به طریقی کاملا خصوصی و خاص منظوره برای مشتریان خاص ذخیره نمود. این پژوهش ضمن به بررسی معماری های رایج رایانش ابری، به پیشنهاد یک معماری سفارشی شده بر مبنای معماری های موجود می پردازد به گونهای که، با افزایش سطح خصوصی سازی داده بتوان بدون کاهش معنا دار سایر معیارهای کیفی همچون کارایی، امنیت داده ها را تا سطح موثری افزایش داد.

3- اهمیت و ضرورت تحقیق

امروزه دو موضوع امنیت و کارایی رایانش ابری، مهمترین دغدغه های موجود در فناوری رایانش ابری می باشد. این دغدغه ها از آن جهت اهمیت یافته اند که بدون تامین آنها میزان استقبال مشتریان به این فناوری به نحو موثری کاهش می یابد.

4- پیشینه تحقیق

4-1 **اقای لی فن وی و همکارانش** [4] در سال 2013 به ارائه راهکارای برای امنیت و محرمانگی در ذخیره سازی و محاسبات در رایانش ابری می پردازد، رایانش ابری یک ظهور به عنوان یک الگوی محاسباتی جدید بوده که با هدف قابلیت اعتماد و سفارش و تضمین کیفیت خدمات برای کاربران در محیط رایانش ابری می باشد. در این پژوهش یک محرمانگی و محاسباتی امن برای پروتکل حسابرسی یا Sec cloud ارائه گردیده شده است، تایید دسته ای و تکنیک های نمونه گیری احتمالی که تجزیه تحلیل داده شده، دقیق بدست می آورد. اندازه نمونه مطلوب هزینه را به حداقل می رساند. یکی از کارهای دیگر در این پژوهش که به صورت کاربردی در رایانش ابری می باشد محیط تجربی هست که secHFS به عنوان یک بستر پیاده سازی در sec cloud می باشد. محاسبات ابری با توجه به گستردگی و تحقیقاتی که انجام گردیده است به دو مسئله رو به رو شده است یک امنیت در ذخیره سازی و دوم امنیت در محاسبات می باشد، امنیت در ذخیره سازی ابر اساسا به مسائل بیرون سپاری و یا خارج منابع اشاره می کند.

4-2 **اقای هونگ کیو لانگ و همکارانش** [5] در سال 2013 به ارائه راهکاری طرح امن و حفظ محرمانگی DRM با استفاده از رمزنگاری همریختی در محاسبات ابری می پردازد،

در این قسمت یک چارچوب مدیریت حقوقی دیجیتال که به صورت کارآمد استفاده خواهد کرد که اجازه خواهد داد محتوای مطالب رمزنگاری شود در سرورهای متمرکز تا اجازه دهد کاربران استفاده کنند از مطالب که مطالب دارای مجوز باشد یعنی مجوز صادر شود (از طرف سرور این مجوز ها صادر می شود)، علاوه بر این روشی ارائه داده شده طرحی از محتوای کلید امن توزیع شده که مبتنی خواهد بود بر افزودنی هوموروفیک که استفاده خواهد کرد از کلید های عمومی برای تکنیک رمزنگاری.

4-3 **اقای یانجی ژانگ و لین لی و همکارانش** در سال 2016 به اطمینان از ویژگی و محرمانگی در رمزگشایی سریع برای برون سپاری امنیت داده های تلفن در رایانش ابری , ارائه گردیده است نگرانی مربوط به امنیت و محرمانگی در رایانش ابری به چشم می آید که با استفاده از AES رمزنگاری مبتنی بر ویژگی که با استفاده از رمزکردن و پنهان کردن متن در مراحل رمزنگاری مشکل دسترسی غیر مجاز کاربران و محرمانگی را حل گردیده است که این طرح پیشنهاد شده معروف هست به بازی بعد از رمزگشایی که محاسباتی انجام می گردد و این نوع از رمزگذاری نامتقارن می باشد و دارای کلید خصوصی می باشد.

4-4 **آقای کی خان** و همکارانش در سال 2016 به امنیت و کارایی طرح اشتراک گذاری داده در فضای ابر ارائه گردیده است که این مدل امینت را افزایش می دهد و محرمانگی آن هم بالا می باشد و از کلیدها برای انتقال و رمزنگاری استفاده میکند نقطه قوت این مدل در سرعت و پشتیبانی تعداد بالا کاربران می باشد و ضعفش هم در لغو کاربران ثبتنام شده می باشد که بعد لغو به اطلاعات دسترسی نداشته باشد[6] .

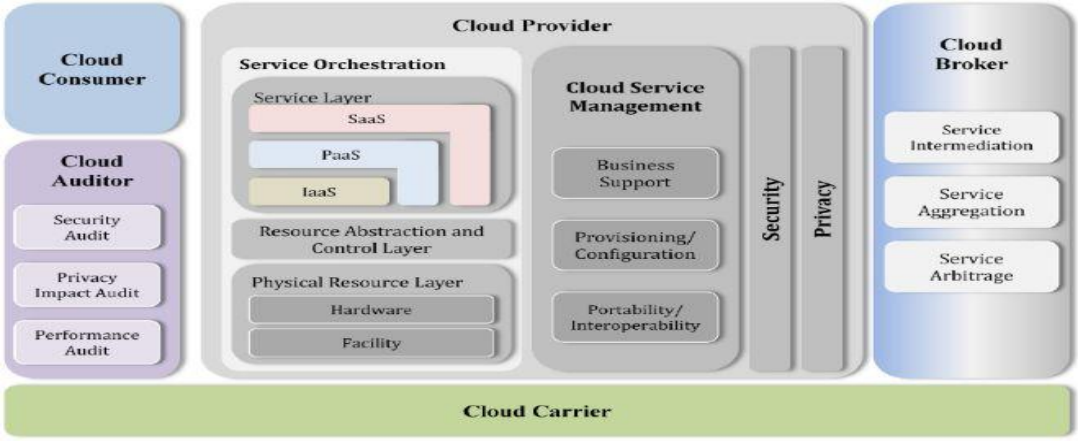
4-5 **آقای یازان الجورودی و مزلیناصالح** و همکارانش در سال 2016 روش نوآوری در حفظ حریم خصوصی برای مجموعه داده های افزایشی در رایانش ابری ارائه گردیده است , نگرانی های مربوط به حریم خصوصی و امنیت در رایانش ابری وجود دارد که اطلاعاتی مانند اطلاعات پزشکی و اقتصادی که نباید کاربران غیر مجاز دسترسی داشته باشد که با استفاده از عملکرد و ارزیابی در حریم خصوصی باعث بهبود لزومات محرمانگی شده است[7].

5- مطالب اصلی و پیشنهادی

در این بخش ما ابتدا رایانش ابری و معماریNIST و الگوریتم صفات CP-ABE را تعریف و بررسی خواهیم کرد، و بعد از تعریف و بررسی طرح پیشنهادی خود را با شکل ارائه خواهیم داد.

رایانش ابری، یک مدل رایانشی است که بر پایه شبکه‌های رایانه‌ای مانند اینترنت دایر شده است و به ارایه الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی (شامل زیرساخت، نرم‌افزار، بستر، و سایر منابع رایانشی) می پردازد.

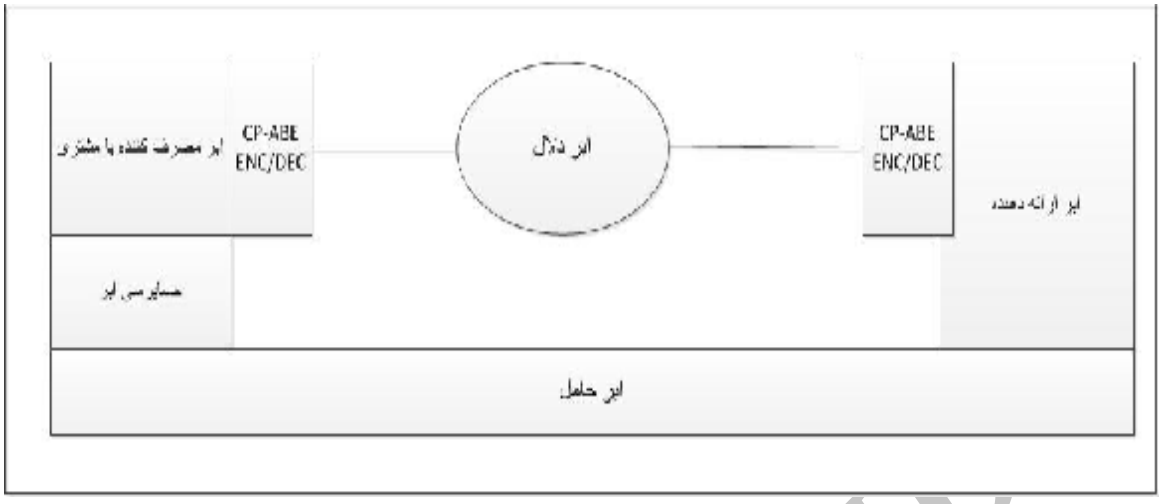
معماری NIST، موسسه ملی استاندارد و فناوری در ایالات متحده می باشد که با هدف اندازه گیری دقیق و استاندارد های مربوط به زیرساخت کشور می باشد که توسط سازمان های فدرال و پلیسی رهبری می گردد[8] .



شکل 1: معماری NIST

الگوریتم صفات CP-ABE سیاست متن رمزشده صفات مبتنی بر رمزنگاری که از نوع رمزنگاری نامتقارن(جفت کلیدی) می باشد مبدا و مقصد از کلیدهای متفاوت استفاده می شود با هدف اینکه جلوی گیری از افشای اطلاعات کند و همچنین هکر نتواند نفوذ به این معماری داشته باشد.

هدف از این پژوهش جلوگیری از افشای اطلاعات در معماری NIST بوده است، زمانی که اطلاعات از کاربر توسط دلال به سرور انتقال پیدا می کند و همچنین بلعکس، توسط هکر ها مورد نفوذ قرار گرفته می شود و باعث افشای اطلاعات و سرویس ها می شود، ما در این پژوهش با اضافه نمودن یک صفت CP-ABE به معماری NIST در قسمت ابتدا و انتهای ابر دلال باعث به وجود آمدن معماری جدیدی به نام SNIST گردید است که باعث افزایش امنیت و محرمانگی در این معماری جدید نسبت به معماری پایه یعنی NIST گردیده است. معماری SNIST پیشنهادی بر مبنای معماری NIST طراحی شده است. این معماری به جهت افزایش سطح محرمانگی و امنیت یک مولفه رمزنگاری را در دو سوی ابر دلال افزوده است. همانگونه که در شکل 2 نشان می دهیم این مولفه بدون آنکه تغییری در سایر مولفه های موجود ارائه دهد تنها به افزایش یک لایه به انجام یک مرحله رمزنگاری بر مبنای الگوریتم CP-ABE میپردازد. الگوریتم CP-ABE یک الگوریتم رمزنگاری مبتنی بر صفت می باشد. صفات بکار گرفته شده برای رمزنگاری پیام،کلید توضیح داده خواهد شد.یکی از مهمترین چالش ها در معماری SNIST آن است که مولفه CP-ABE بتواند بدون تغییر فرمت داده ها، داده های مناسب را به هر دوی سوی مشتری و ارائه دهنده ارسال کند. شکل زیر شمای کلی از طرح پیشنهادی ارائه گردیده می باشد.



شکل2: معماری ارائه شده SNIST

5-1 بررسی مولفه CP-ABE

مولفه CP-ABE وظیفه رمزنگاری و یا بازگشایی رمز داده های اماده تحویل و یا دریافتی ابر دلال را بر عهده دارد. داده های انتقالی از سوی مشتری به تهیه کننده و یا بالعکس در قالب XML می باشد. سیاست متن رمز شده- صفاتی مبتنی بر رمزنگاری می باشد که با استفاده از این الگوریتم می خواهیم افزایش امنیت در معماری NIST به وجود بیاوریم. سیاست های متن رمز شده صفاتی مبتنی بر رمزنگاری از طریق تکنیک های رمزنگاری انجام می شود که در ابتدا متن رمز شده را از طریق کلید رمز میکند و در پایان هم از طریق کلید، از نوع همان الگوریتم بازگشایی می کند.. مهمترین نکته در انجام عملیات رمزنگاری بحث کلید می باشد چون رمزنگاری از دو طریق صورت می گیرد[9] .

- رمزنگاری متقارن(تک کلیدی)
- رمزنگاری نامتقارن(کلید خصوصی یا دو کلیدی)

طرح پیشنهادی ما از طریق رمزنگاری نامقارن عمل می کند یعنی جفت کلیدی که در ابتدا متن ساده را با یک کلید رمز می کند و در انتها با کلید دیگر رمزگشایی می کند تا بدین صورت امنیت کار را بشدت افزایش دهد، البته کارایی هم تحت تاثیر این کار قرار می گیرد و افزایشی نداشته و چون رابطه مستقیمی بین افزایش امنیت و کارایی وجود دارد می توان نتیجه گرفت که کارایی دچار کاهش خواهد شد، اما این کار صورت گرفته بشدت امنیت را افزایش می دهد، یک از مزایای الگوریتم رمزنگاری نامتقارن این است که وقتی به آن حمله صورت بگیرد بشدت مقاوم تر از الگوریتم های متقارن یا تک کلیدی می باشد اما الگوریتم های نامتقارن پیچیده تر و محاسبات سنگین تری نسبت به الگوریتم های متقارن دارد، و یکی دیگر از مزایای رمزنگاری

نامتقارن این است که مشکلات توضیح کلید را حل نموده تا هکر نتواند به راحتی به کلید آن متن رمز شده دسترسی داشته باشد و افشای اطلاعات کند که این یکی از مشکلات اساسی در رمزنگاری متقارن بوده است.

2-5 روش کار الگوریتم CP-ABE

برای ایجاد عملیات رمزنگاری ما 3 فاز داریم. در فاز اول راه اندازی عملیات، در فاز دوم رمزگذاری صفات موجود یا داده، در فاز سوم رمزگشایی داده و بازیابی آن به حالت اول، که هر کدام را در ادامه بررسی خواهیم کرد.

فاز اول راه اندازی، راه اندازی توسط مراکز ساخت و مدریت کلید انجام می شود، که برای ساخت کلید از سه طریق امکان پذیر می باشد، اول از طریق سرورهای کلود، دوم از طریق مراکز مجاز کلید، و سوم از طریق کاربران صورت می گیرد، که وقتی کلید راه اندازی گردید در پایان به ما کلید عمومی PK و کلید اصلی MK را به ما می دهد، و همچنین به کاربرانی که عضو می باشند یک شناسه منحصر به فرد ID می دهد تا سطح دسترسی داده را مشخص نماید یعنی هر کاربر اجازه دسترسی داده و افشای اطلاعات را نداشته باشد. پس در فاز اول یعنی راه اندازی ما کلید عمومی و خصوصی را بدست آوردیم و هدف از این کار در رمزگشایی و رمزنگاری استفاده خواهیم نمود.

$$\text{SETUP} \rightarrow PK.MK \qquad -(1)$$

فاز دوم رمزگذاری، در این بخش جهت مکانیسم ها و شیوه های ذخیره سازی و امن کردن داده ها از آغاز و انتقال امن آنها به ابر در قالب رمزنگاری شده بکار برده می شود که به برسی و نوع کار و مراحل آن در ادامه می پردازیم، الگوریتم رمزگذاری بر اساس صفات CP-ABE یعنی سیاست های متن رمز شده- صفاتی مبتنی بر رمزنگاری ابتدا در انجام رمزگذاری کلید عمومی PK و M پیام و CSK پرامترهای امن را رمز می کند و خروجی متن رمز شده ناخوانی به نام CT به ما می دهد که این پیام به صورت ناخوانی می باشد تا اطلاعات و داده دارای امنیت باشد. نکته مهم برای رمز گذاری عضو بودن کاربران می باشد و برای دسترسی کاربران به پیام یا داده ها باید عضو و شماره منحصر به فرد شناسایی داشته باشند، در غیر این صورت کاربران عضو نمی باشند و اجازه دسترسی نخواهند داشت.

$$\text{Encryption} \quad (PK, M, CSK) \rightarrow CT \qquad -(2)$$

فاز سوم رمزگشایی ، در این مرحله از عملیات رمزنگاری که مرحله آخر می باشد برای بازگشایی اطلاعات، داده و سرویس ها می باشد، الگوریتم بازیابی صفات CP-ABE ابتدا، متن رمزشده CT و کلید امن SK به عنوان ورودی می باشد و خروجی M یعنی پیام به ما تحویل می دهد.

کاربران عضو می توانند به متن ساده و پیام بعد از رمزگشایی دسترسی داشته باشد که مسائل مانند سطح دسترسی و محرمانگی داده و سرویس اتفاق می افتد، یعنی هر کاربری نتواند به داده ها دسترسی داشته باشد.

$$\text{Decryption} \quad CT, SK \rightarrow M \qquad -(3)$$

5-3 ارتباط دلال با CP-ABE

در شکل2 نشان داده شده ارتباط دلال را با مولفه قبل و مولفه بعد در معماریSNIST مشخص گردیده است که همانطور که مشاهده گردیده شده ارتباط دلال از طریق رمزنگاری صفات CP-ABE به ابرهای مصرف کننده و ارائه دهنده صورت می پذیرد، در این معماری انتقال داده از طریق صفات داده و یا صفات سرویس در قالب XML انتقال پذیری صورت می گیرد. نحوه ارتباط ابر مصرف کننده با الگوریتم رمز صفات از طریق سه لایه Paas-Saas-Laas انجام می شود که هر کدام از این لایه وظایف خاص خود را دارا می باشد و بعد از عملیات رمزگذاری و انتقال داده توسط دلالان عملیات رمزگشایی انجام می گردد که نحوه ارتباط الگوریتم های صفات با ابرهای ارائه دهنده باز هم از طریق سه لایه Paas-Saas-Laas صورت می گرد که داده ها و یا سرویس ها از طریق عملیات رمزنگاری با قالب XML انتقال و انجام می گردد.

5-4 گام های کلی راهکار

در ابتدا باید اشاره شود که گام های زیر بر اساس مدل ارایه شده رمزنگاری صفات که جهت افزایش سطح محرمانگی داده و تامین امنیت اطلاعات و همچنین ایجاد حداقل سربار بر روی معماری مربوطه انجام می گیرد:

1. به محض آنکه فرایند تایید هویت کاربر و میزان دسترسی کاربران به داده ها با موفقیت طی بشود، مرحله راه اندازی صورت می گیرد یعنی اماده رمزگذاری صفات و یا داده می شود.
2. پس از اینکه راه اندازی صورت گرفت، داده و یا سرویس اماده عملیات رمزنگاری توسط CP-ABE می باشد.
3. جهت رمزگشایی داده نیز عملیات در جهت معکوس انجام می گیرد، که متن رمز شده به متن خام تبدیل می شود.
4. مقدار MAC مربوط به داده ها نیز با استفاده از الگوریتم MAC جهت برسی یکپارچگی داده ها محاسبه می شود.
5. در صورتیکه مقدار MAC تولید شده برابر با مقدار فرستاده شده باشد، یکپارچگی داده تایید می شود.

6- نتیجه و جمع بندی

در این پژوهش ارائه شده ابتدا برسی های لازم درباره رایانش ابری و مفاهیم اولیه بحث گردیده که از جمله مزایای آن می توان به کاهش هزینه ها، افزایش دسترسی پذیری، مدیریت آسان و فضای ذخیره سازی نامحدود اشاره نمود. از سوی دیگر رایانش ابری مانند هر تکنولوژی دیگر، با تهدیدات و چالش هایی روبرو است که تصمیم گیری برای استفاده و گسترش آن را سخت و مبهم می سازد. از جمله چالش ها و تهدیدات رایانش ابری می توان به مواردی نظیر آسیب پذیری، خطرات امنیتی، عملکرد و قابلیت دسترسی اشاره نمود.

یکی از استفاده های اصلی از رایانش ابری ذخیره سازی داده ها است. رایانش ابری به کاربران خود اجازه می دهد مقداری زیادی از داده ها را در مراکز داده ای گسترده و مقیاس پذیری قرار دهند که در همه جا قابل دسترس هستند. در واقع داده های ذخیره شده را در محیطی باز مثل اینترنت منتشر می کند. نکته مهم و قابل اهمیت در رایانش ابری با رشد کاربران ابر، فعالیت های مخرب نیز افزایش می یابند، بنابراین نیاز به خدمات امن و پایدار ضروری است. امنیت یک مفهوم کلی در مباحث فناوری اطلاعات می باشد. هدف امنیت اطلاعات، محافظت اطلاعات و سامانه های اطلاعاتی از دسترسی و استفاده غیر مجاز، افشا، تغییر یا خرابی است.

رایانش ابری از معماری های مختلفی برخوردار می باشد که در این گزارش بحث اصلی بروی معماری NIST و اجزای آن بوده است. در این معماری هدف اصلی ما ایجاد امنیت و افزایش سطح محرمانگی داده و دسترسی ها در معماری NIST بوده است به عبارت دیگر هدف اصلی این پژوهش افزایش امنیت، سرعت و عملکرد داده های ذخیره شده در معماری NIST رایانش ابری است. موارد و پارامترهای تاثیر گذار بر امنیت بسیار زیاد می باشد از جمله عوامل موثر برای اطمینان از امنیت داده می توان به رمزنگاری، محرمانگی و سطح دسترسی به داده برای کاربران اشاره کرد. بر همین اساس در این پایان نامه یک چارچوب جهت تامین امنیت داده ها و افزایش سطح دسترسی در معماری پیشنهاد شده است که مربوط به ایمن سازی ابرهای دلال می باشد. برای این منظور چندین مکانیزم و تکنیک جهت حفاظت از اطلاعات مهم در برابر دسترسی های غیرمجاز، بکار گرفته شده است. در واقع روش پیشنهادی به سه فاز تقسیم گردیده فاز نخست برای راه اندازی و اختصاص شماره منحصر بفرد به کاربران. در فاز دوم به رمزگذاری داده ها در معماری مربوط ابر پرداخته شده است و با توجه به نوع صفات سرویس و یا صفات داده رمز انجام می شود . در فاز سوم به رمزگشایی داده و بازیابی آن می پردازد که نکته مهم با همان الگوریتم که رمز شده است رمزگشایی انجام می شود اما کلید های آن متفاوت بوده است، و بحث دسترسی کاربران هم بعد از رمزگشایی پیش خواهد آمد که هر کاربری به داده رمزگشایی شده دسترسی نخواهد شد چون در مرحله راه اندازی به کاربران مجاز شماره منحصر بفرد داده ایم و در این مرحله پایانی کاربرانی که شماره منحصر بفردی دارا می باشند می توانند به داده ها دسترسی داشته باشند. این الگوریتم رمزنگاری صفات CP-ABE به عنوان یک راهکار بهینه جهت رمزنگاری و رمزگشائی داده ها و سرویس استفاده می شود و با استفاده از آن داده ها و سرویس ها از سمت ابرهای حسابرس تا ابرهای حامل و ابرهای دلال یا کارگزار رمزنگاری و ایمن نمود. در پیاده سازی با اکلیپس جاوا به این نتیجه رسیدیم که در معماری پایه NIST نسبت به معماری ارائه شده SNIST دارای تفاوت های بوده است که مربوط به اضافه نمودن صفت در معماری ارائه شده است که طرح پیشنهادی زمان اجرا افزایش می یابد اما گذردهی با محرمانگی داده افزایش می یابد.

7- دستاوردها و پیشنهادها

در این پژوهش ما با توجه به پیشنهاد ارائه شده و ایمن سازی توانستیم امنیت و محرمانگی داده را با استفاده از تکنیک های رمزنگاری افزایش دهیم و همچنین این افزایش امنیت را می توانم در معماری ibm بوجود بیاوریم .

8- تقدیر تشکر

تقدیر تشکر، از دانشگاه اصفهان برای فرصت دادن به بنده، و همچنین استاد عزیزم دکتر مجید ابوطالبی که در این پژوهش مرا یاری کرده اند، و تقدیر تشکر از پدر و مادر عزیزم که هر چه دارم از دعاهای خیرشان می باشد.

9- مراجع

[1] اندروس تائن باوم-مارتن فان استین,(1392) سیستم های توزیع شده، اصول و روش ها, ویرایش دوم. تهران.

[1] Qinlong Huang, Yixian Yang, Mansuo Shenc , 29 September 2016 , ***Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing***, page9-page16 , Accepted.

[2] Lu Zhou, Youwen Zhu, Aniello Castiglione***, Efficient k-NN query over encrypted data in cloud with limited key-disclosure and offline data owner***, *Computers & Security* (2016), http://dx.doi.org/doi: 10.1016/j.cose.2016.11.013.

[3] L. M. Thain D, Tannenbaum T, ***Distributed computing in practice***, pp. 17–24, 2005.

[4] Gentzsch W. Sun grid Engine, ***towards creating a compute power symposium on cluster computing and the grid***, 2001.

[5] Daniel Nurmi and et al, ***A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to useful systems***, comput. sci. tech, 2008.

[6] K. Han, Q. Li, and Z. Deng, ***Security and efficiency data sharing scheme for cloud storage***, Chaos,.

[7] L. S. Mather T, Kumaraswarmy S, ***loud security and privacy: an enterprise perspective on risks and complianc***, 2009.

[8] Dongyoung Koo , Junbeom Hur , Hyunsoo Yoon , December 2012 , ***Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage***, page3-page9 , elsevier.