کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش مهارت های کاربردی در تدوین و چاپ مقاله

اصول تنظیم قراردادها

مقاله نویسی علوم انسانی

2nd INTERNATIONAL CONFERENCE ON
RESEARCH IN SCIENCE AND TECHNOLOGY
Istanbul-Turkey 14 March 2016
RSTCONF
دومین کنفرانس بین المللی
پژوهش در علوم و تکنولوژی
ترکیه - استانبول ۲۴ اسفند ۱۳۹۴

حفظ حریم خصوصی برای ذخیره سازی ایمن در ابر

علی نصیریان پور
دانشجوی ارشد، دانشکده فنی مهندسی، گروه مهندسی کامپیوتر و فنآوری اطلاعات، دانشگاه آزاد اسلامی واحد خمین،
alinasirian2008@gmail.com

حمید پایگذار
عضو هیئت علمی دانشکده فنی مهندسی، گروه مهندسی کامپیوتر گرایش نرم‌افزار، دانشگاه آزاد اسلامی واحد خمین،
paygozarh@gmail.com

چکیده

رایانش ابری مناسب بر روی تقاضا ی دسترسی به شبکه به یک منبع مشترک از منابع محاسباتی قابل تنظیم را فراهم می کند . این منابع را می توان به سرعت با کارایی بالا و حداقل سربار مدیریت مستقر نمود . پلت فرم ابر (بستر نرم افزار) محاسباتی ناامن از نظر کاربران ابری است، سیستم باید مکانیسم های را طراحی کنند که نه تنها محافظت از اطلاعات حساس محاسبات با داده های رمزگذاری شده را قادر می سازد ، بلکه کاربران را از رفتارهای مخرب محافظت کند با فعال کردن امکان اعتبار سنجی از نتیجه محاسبات . در این مقاله ، ما یک طرح رمزگذاری داده جدید به نام جایگذاری بیت لایه ای(لایه لایه) پیشنهاد می کنیم ، که برای بازیابی بسته حساس به زمان در حضور از دست دادن bursty (انفجاری- پشت سر هم) طراحی شده است . این سرعت بالا طرح بازیابی اطلاعات با احتمال از دست دادن حداقل و با استفاده از یک طرح اصلاح خطا رو به جلو که مسئول رسیدگی به از دست دادن bursty را دارا باشد . روش ارائه شده در بازیابی خسارات تک قلو تقریبا بلافاصله و از تلفات داده bursty است بسیار کارآمد می باشد .

واژگان کلیدی: رایانش ابری ، تمامیت داده ها ، بازیابی اطلاعات ، جایگذاری بیت لایه ای، امنیت

۱. مقدمه

امروزه سازمان ها به طور فزاینده ای به دنبال رایانش ابری به عنوان یک تکنولوژی جدید انقلابی امیدوار کننده برای کاهش هزینه های توسعه و نگهداری و هنوز هم دستیابی به خدمات بسیار قابل اعتماد و الاستیک . فن آوری ابر یک روند رو به رشد است و هنوز هم تحت بسیاری از آزمایشات است .ابر وعده مزایای هزینه های زیادی، چابکی و مقیاس پذیری به کسب و کار است . (Lilibridge et al,2003)

تمام داده های کسب و کار و نرم افزارها بر روی سرورها در یک مکان ارجاع (اشاره) از راه دور به عنوان مراکز داده ذخیره می شود . محیط زیست مرکز داده های اجازه می دهد تا شرکت ها به منظور اجرای برنامه های کاربردی سریع تر، با قابلیت اداره مدیریت آسان تر و تلاش نگهداری کمتر و سرعت بیشتر در مقیاس منابع (مانند سرورها، ذخیره سازی، و شبکه) برای دیدار با نوسان نیازهای کسب و کار است . مرکز داده ها در محیط ابر دارای اطلاعات است (اطلاعاتی را نگه می دارد) که کاربران نهایی به طور سنتی تر بر روی کامپیوتر خود ذخیره می کنند. این افزایش نگرانی در مورد حفاظت از حریم خصوصی کاربراست چرا که کاربران باید اطلاعات خود را برون سپاری کنند. (Wang et al,2011)

حرکت داده ها به خدمات (سرویس های) متمرکز می تواند بر حریم خصوصی و امنیت تعاملات کاربران با فایل های ذخیره شده در فضای ذخیره سازی ابری تاثیر بگذارد . استفاده از زیرساخت های مجازی به عنوان یک سکوی پرتاب ممکن است حملات جدید به داده های کاربران را معرفی نماید .

تمامیت (یکپارچگی) داده ها به عنوان دقت و انسجام از داده های ذخیره شده در غیاب هر گونه تغییر به داده ها بین دو به روز رسانی از یک فایل یا رکورد تعریف شده است . خدمات ابر باید به تضمین یکپارچگی داده ها و ارائه اعتماد به حریم خصوصی کاربر بپردازد.

اگر چه برون سپاری اطلاعات به ابر از لحاظ اقتصادی برای هزینه و پیچیدگی بلند مدت در مقیاس بزرگ ذخیره سازی داده ها جذاب است، آن را فاقد ارائه تضمین قوی از تمامیت (یکپارچگی) داده ها و در دسترس بودن ، ممکن است مانع پذیرش گسترده آن توسط هر دو شرکت و کاربران فردی ابر باشد. (Wang et al,2011)

رایانش ابری در درجه اول به شمار نگرانی های حریم خصوصی می آید ، زیرا ارائه دهنده خدمات در هر نقطه در زمان، ممکن است به داده هایی که بر روی ابر می باشد دسترسی داشته باشد (پیدا کند) . ارائه دهنده خدمات ابر می تواند به طور تصادفی یا به عمد برخی از اطلاعات را از سرور ابر تغییر دهد و یا حذف کند.

از این رو، سیستم باید نوعی مکانیزم برای اطمینان از یکپارچگی داده ها داشته باشد. در حال حاضر مدل امنیت ابر بر اساس این است فرض که کاربر / مشتری باید به ارائه دهنده اعتماد کند.

این است که به طور معمول توسط یک توافقنامه سطح خدمات (SLA : service level agreement) اداره می شود که به طور کلی به تعریف ارائه متقابل و انتظارات و تعهدات کاربرمی پردازد.

به منظور حصول اطمینان از یکپارچگی و در دسترس بودن داده ها در ابر و اجرای با کیفیت از سرویس (خدمات) ذخیره سازی ابر ، روش های کارآمد است که قادر می سازد بر روی تقاضا تایید صحت داده ها از طرف کاربران ابر باید طراحی شود.

با این حال، این واقعیت است که کاربران دیگر مالکیت فیزیکی داده ها را در ابر پذیرش مستقیم از شکلهای هندسی اولیه رمزنگاری سنتی به منظور حفاظت از یکپارچگی داده ها را ممنوع کرده است. (Wang et al,2011)

از این رو، تایید صحت ذخیره سازی ابر باید بدون دانش صریح و روشن از تمام (کل) فایل های داده انجام شود. (Bowers et al,2009) (Shah et al,2008) (Filho and Barreto,2006) (Wang et al,2011)

داده های ذخیره شده در ابر نه تنها ممکن است قابل دسترسی باشند بلکه غالبا به طور مرتب و مکرر توسط درج، حذف، اصلاح، الحاق، و غیره به روزرسانی می شوند .

بنابراین، امری ضروری است برای حمایت از ادغام این ویژگی پویا به تضمین صحت ابر ذخیره سازی ، که باعث می شود حتی طراحی سیستم بیشتر به چالش کشیده شود . (Wang et al,2009) (Wang et al,2011)در این مقاله، ما یک روش برای رمزگذاری و بازیابی اطلاعات در صورت خرابی را تجزیه و تحلیل می کنیم.

A. سهم ما

سهم اصلی این مقاله عبارتند از :

- پروتکل پاسخ به چالش در کار ما بیشتر، محل خطا داده ها فراهم می کند.
- ما یک روش کارآمد برای رمزگذاری داده های منتقل شده و ذخیره شده در ابر پیشنهاد می کنیم.
- در نهایت، ما یک روش بازیابی اطلاعات کارآمد و تجزیه و تحلیل عملکرد پیشنهاد می کنیم برای بازیابی اطلاعات از دست رفته در ابر ارائه شده است.

B. پیش فرض

در این مقاله، ما فرض می کنیم که این طرح امن(ایمن) پشتیبانی وعملیات پویا کارآمد بر روی بلوک های داده ها، از جمله: بروز رسانی، حذف و اضافه.

بقیه این مقاله به شرح زیر سازماندهی شده است . بخش دوم توصیف کار مرتبط است. بخش سوم مدل سیستم و فرمولاسیون را معرفی می کند. سپس ما شرح مفصلی از طرح های ما در بخش چهارم ارائه می کنند. بخش پنجم تجزیه و تحلیل امنیتی می دهد. بخش ششم جزئیات بیشتر در بازیابی داده ها (اطلاعات) را فراهم می کند و بخش هفتم در ارزیابی عملکرد، بخش هشتم به مرور کار مرتبط و نتیجه گیری وسخن پایانی از کل مقاله.

۲ . کار مرتبط

طرح توزیع موثر و انعطاف پذیر با پشتیبانی از داده های پویا صریح (واضح – روشن) برای اطمینان از صحت داده های کاربران در ابر توسط C. وانگ، Q. وانگ، K. رن، و W. لو در July ۲۰۰۹ پیشنهاد (ارائه) شده است. C. وانگ، Q. وانگ، K. رن، و W. لو در پاک شدن کد تصحیح در تهیه و توزیع فایل برای ارائه اضافی و تضمین قابلیت اعتماد و اطمینان داده ها تکیه می کنند.

این ساخت و ساز ممکن است به شدت به کاهش ارتباطات و سربار ذخیره سازی در مقایسه با تکنیک های توزیع فایل های مبتنی بر تکرار سنتی باشد .

طرح آنها رسیدن به بیمه صحت ذخیره سازی و همچنین محلی سازی خطا داده است که، هر زمان که فساد داده در طول تایید صحت ذخیره سازی شناسایی شده است ، طرح خود را تقریبا می توانید تضمین محلی سازی به طور همزمان از خطاهای داده کنبد.

بعدها در ماه May سال ۲۰۱۱، کانگ وانگ، کیان وانگ ، Kui رن، ونیجنگ لو کار خود را توسعه داده و اجازه می دهد تا کاربر به حسابرسی ابر ذخیره سازی با ارتباطات بسیار سبک وزن و محاسبه هزینه ، طرح پیشنهادی بسیار کارآمد و انعطاف پذیر در برابر شکست بیزانس، حمله اصلاح داده های مخرب، و حتی حملات تبانی سرور است .

مدل رسمی " اثبات بازیابی " (POR) برای حصول اطمینان از یکپارچگی داده ها از راه دور توسط A. Juels و J. برتون S. Kaliski در اکتبر سال ۲۰۰۷ توضیح داده شد. طرح آنها ترکیبی از دو روش تست (چک کردن) نقطه و کد تصحیح خطا برای اطمینان از هر دو مالکیت(در اختیار داشتن) و بازیابی فایل ها در بایگانی(بر روی آرشیو) یا سیستم های خدمات پشتیبان . H.Shacham و B.Waters در سال ۲۰۰۸ بر روی این مدل ساخته شده و ساخته شده یک تابع خطی تصادفی مبتنی برتایید (Authenticator - تایید کننده اعتبار) Homomorphic که قادر می سازد به تعداد نامحدودی از پرس وجو ها و نیاز به سربار ارتباطات کمتری داشته باشم . (Shacham and Waters,2008)

چارچوب بهبود یافته برای پروتکل های POR است که تعمیم کار هر دو Juels و Shacham را نشان داده است . (Bowers et al,2009)

همه این طرح ها با تمرکز بر روی داده های استاتیک می باشد . اثربخشی طرح های آنها عمدتا بر اساس مراحل پیش پردازش که کاربر قبل از برون سپاری فایل داده F انجام می دهد. هر گونه تغییردر محتویات F، حتی چند بیت، باید از طریق انتشار کد تصحیح خطا انجام شود، در نتیجه معرفی محاسبات قابل توجه (معنی دار) و پیچیدگی ارتباطات توسط باورز در سال ۲۰۰۹ پیشنهاد شد.

"در اختیار داشتن داده ها قابل اثبات " (PDP : provable data possession) مدل برای حصول اطمینان از در اختیار داشتن فایل در انبارهای غیر قابل اطمینان توسط Ateniese و همکاران تعریف شده بود .(Ateniese et al,2007)

طرح آنها با کلید عمومی مبتنی بر بر چسب Homomorphic برای حسابرسی فایل داده مرده استفاده قرار می گیرد ، بنابراین ارائه (فراهم کردن) اثباتپذیری عمومی است .

با این حال، طرح آنها نیازمند به سربار محاسبات به اندازه کافی است که می تواند برای کل فایل گران قیمت باشد.

پس از آن (بعدها) ، در کار بعدی آنها در سال ۲۰۰۸، به توصیف یک طرح PDP که تنها از رمزنگاری کلید متقارن استفاده می کند می پردازند .

این روش سربار کمتری نسبت به طرح قبلی آنها دارد و اجازه می دهد برای به روز رسانی بلوک، حذف و اضافه در فایل ذخیره شود، که این نیز(همچنین) در کار ما حمایت می شده است.

با این حال، تمرکز طرح آنها بر سناریوی تک سرور می باشد واین فساد داده کوچک را حل نمی کند، ترک هر دو سناریو توزیع و بازیابی خطا داده مسئله ناشناخته.است

معنای جدید و کارآمد از چند جمله ای به اندازه ورودی (یعنی کلید ویا داده) توسط M.A.shah ، Swaminathan R.، و M. بیکر در سال ۲۰۰۸ در "حسابرسی حفظ حریم شخصی و استخراج محتویات دیجیتال "مطرح شد.

تهدید اصلی از حسابرس این می باشد که ممکن است اطلاعات مهم که از اینسو و آنسو جمع شده از فرایند حسابرسی باشد که می تواند سازش(مصالحه) تضمین حفظ حریم خصوصی ارائه شده توسط سرویس باشد.

به عنوان مثال، حتی چند بیت از یک فایل که حاوی سابقه پزشکی می باشد می تواند نشان دهد که آیا یک مشتری دارای یک بیماری است .

برای اطمینان از حفظ حریم خصوصی، استانداردهای مختلف برای رمزگذاری داده ها و کلید رمزنگاری وجود دارد . برای داده ها، سیستم متکی بر (1) قدرت طرح رمزگذاری و (2) خاصیت دانش صفر از پروتکل برای حسابرسی کلید رمزنگاری می باشد.

برای اطمینان از یکپارچگی فایل در سراسر(میان) چندین سرور توزیع شده، با استفاده از پاک شدن کد نویسی و بلوک در سطح چک یکپارچگی فایل ، توسط TSJ شوارتز و EL میلر در سال ۲۰۰۹ پیشنهاد شد.

با این حال، طرح آنها تنها فایل های داده ایستا (ثابت) را در نظر می گیرد .به منظور بررسی یکپارچگی(تمامیت) داده ها با استفاده از مخلوط مبتنی بر RSA برای در اختیار داشتن داده ها در شبکه های به اشتراک گذاری فایل نظیر به نظیر توسط DLG فیلو و PSLM بارتو در سال 2006 تعریف شده است .

با این حال، پیشنهاد آنها نیازمند به توان رساندن بیش از کل فایل داده ها می باشد، که به وضوح برای سرور غیر عملی است هر زمان که فایل بزرگ باشد.

۳ . مدل سیستم و مشکل فرمولاسیون

سیستم پیشنهادی دارای سه نهاد مهم می باشد:

کاربر:

از کاربران ذخیره داده ها در ابر و برای تمام محاسبات خود بر روی داده های ذخیره شده در سرور ابر بستگی دارد . کاربر ممکن است یک فرد یا سازمان است .

ارائه دهنده خدمات ابر :(CSP)

(CSP : Cloud Service Provider) شامل منابع و تخصص در ساخت و مدیریت توزیع شده سرورهای ذخیره سازی ابر، صاحب و عمل و اجاره سیستم های رایانش ابری زندگی می کنند.

حسابرس شخص سوم:(TPA : Third Party Auditor)

TPA دارای تخصص و قابلیت های که کاربران ممکن است نداشته باشند، برای ارزیابی، حسابرسی مورد اعتماد است و در معرض خطر ابتلا به خدمات ذخیره سازی ابر به نمایندگی از کاربران پس از درخواست از کاربران.

یک نهاد خاص برای اطمینان از امنیت و قابلیت اعتماد و اطمینان به سرور ابر در نظر گرفته شده است ، که به عنوان مدل دشمن به آن اشاره می شود .

دشمن به طور مداوم علاقه مند به فساد کشاندن فایل داده های ذخیره شده کاربر بر روی سرورهای فردی است .

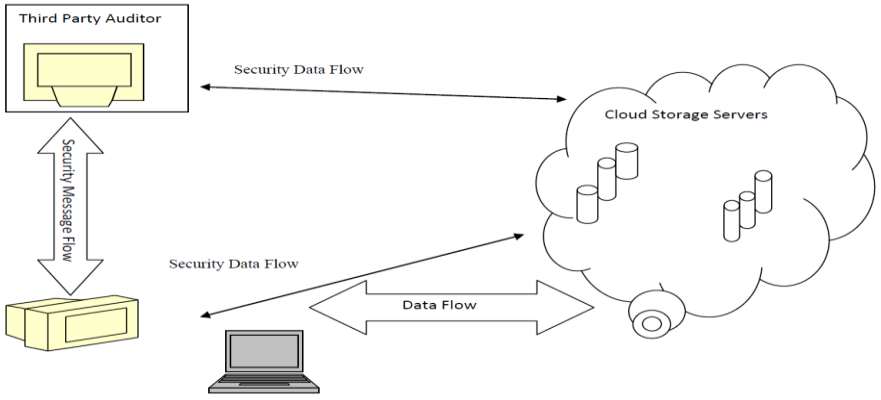
هنگامی که یک سرور تشکیل شده است، یک دشمن می تواند فایل های داده های اصلی را با تغییر و یا معرفی داده های تقلبی خود آلوده کند برای جلوگیری از این که داده های اصلی توسط کاربر بازیابی شود .معماری شبکه پیشنهادی برای ابر ذخیره سازی داده ها در شکل ۱ نشان داده شده است.

در سیستم ابر ذخیره سازی داده ها، کاربران داده های خود را در ابر ذخیره می کنند و دیگر دارای داده های محلی نمی باشد . بنابراین، صحت و در دسترس بودن فایل های داده که بر روی سرورهای ابر توزیع شده ذخیره می شود، باید تضمین شده باشد . یکی از مسائل کلیدی این است که به طور موثر، شناسایی (تشخیص) هر گونه اصلاح داده های غیر مجاز و فساد، احتمالا به علت سازش سرور است.

از این رو، آن است که حضور TPA برای ارزیابی، حسابرسی الزامی می باشد و در معرض خطر ابتلا به خدمات ذخیره سازی ابر است. به منظور رسیدگی به این مشکلات، طرح اصلی ما برای حصول اطمینان از ابر ذخیره سازی داده ها در این بخش ارائه شده است.

قسمت اول از این بخش اختصاص داده شده است به بررسی ابزارهای اساسی از نظریه کدگذاری که در طرح ما برای توزیع فایل در سراسر سرورهای ابر مورد نیازاست .

نرم افزارهای تبدیل کننده (کد گذار) FEC معمولا با چند تایی (تاپل) (m , k) پارامترگذاری می شود .برای هر یک از دنباله های خروجی از بسته های داده، در مجموع (m + k) داده ها و بسته های تصحیح خطا به روی کانال فرستاده می شوند، و در نتیجه سر بار رمزگذاری k / m است .



شکل ۱ : معماری ابر ذخیره سازی داده ها

اطلاعات کار برکنار شده (زائد) را نمی توان تولید و ارسال نمود تا زمانی که تمام بسته های داده ای برای ارسال در دسترس باشند . در نتیجه ، زمان تاخیر بازیابی بسته توسط نرخی که در آن فرستنده داده ها را انتقال می دهد ، تعیین می شود . تولید بسته های تصحیح خطا کمتر از بسته های داده در فرستنده است و نه یک گزینه قابل دوام ، حتی اگر نرخ داده ها در این کانال کم باشد، گیرنده و یا شبکه می تواند عامل را در نزدیکی ظرفیت کامل با داده ها از فرستنده های دیگر و FEC در معرض ضرر و زیان bursty می باشد.

۴ . شرح مفصل

شرح مفصل ماژول های مهم از این مقاله را پوشش می دهد.

A . آماده سازی توزیع فایل

کد تصحیح پاک شدن ممکن است برای تحمل شکست های متعدد (چند گانه) در سیستم های ذخیره سازی توزیع شده مورد استفاده قرار گیرد. در ابر ذخیره سازی داده ها، ما بر روی این روش تکیه می‌کنیم برای پراکنده کردن داده‌های زائد فایل F که در سراسر مجموعه ای از d سرور(سرویس دهنده) توزیع شده است .

در روش ترک بین لایه ای (Interleaving) برای تعیین بردارهای برابری افزونگی c از بردارهای داده r استفاده می‌شود به گونه ای که بردارهای داده r اصلی را می توان از هر r خارج از r + c داده و بردار برابری بازسازی نمود .با قرار دادن هر یک از بردارهای r + c در سرور های مختلف ، فایل داده های اصلی می تواند از شکست هر c از r + c سرورهای بدون از دست دادن داده ها زنده بماند، با یک فضای سربار c / r .

بردارهای فایل داده r اصلاح نشده همراه با بردار توازن(برابری) C در سراسر r + c سرورهای مختلف توزیع شده است.

کاربر فایل کد گذاری شده توسط ضرب F با A بدست می آورد که عبارت است از :

$$\mathbf{G = F \cdot A} = (G(1),G(2), \ldots, G(m),G(m+1),. , G(n)) = (F1, F2, \ldots, Fm, G(m+1), \ldots, G(n)),$$

که در آن F فایل واقعی است و A از یک ماتریس Vandermonde مشتق شده است، یک ماتریس با شرایط یک تصاعد هندسی در هر ردیف (سطر) است.

برای ترک بین(interleave) شاخصی از ۳، اولین بلوک حاوی شماره بسته های داده ((0,3,6,...(r-1).c) ، دوم با شماره بسته های داده (1,4,7,..,((r-1).c)+1) و سوم با شماره بسته های داده (2,5,8,...((r-1).c)+2) است.

B . پیاده سازی TPA

کاربر می تواند وظیفه حسابرسی را به یک حسابرس شخص سوم مستقل واگذار کند، ساخت ابر ذخیره سازی برای عموم قابل اثبات است . برای TPAموثر، فرایند حسابرسی باید بدون آسیب پذیری های جدید ، حریم خصوصی داده ها را درسمت کاربر به ارمغان بیاورد.

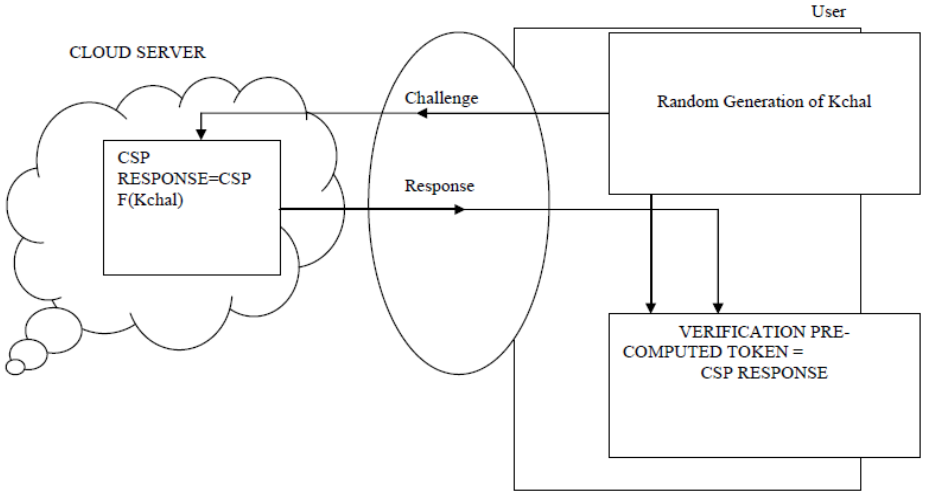
یعنی، TPA نباید محتوای داده های کاربرها را از طریق حسابرسی داده های محول (واگذار) شده یاد بگیرد .این طرح پیشنهادی می تواند از حفظ حریم خصوصی حسابرس شخص سوم حمایت کند. (Shah et al,2007)

حسابرسی TPAباید بدون آسیب پذیری های جدید معرفی کند زمانی که کاربر مسئولیت حسابرسی را به TPA واگذار می کند، او تمام ویژگی های مورد نیاز برای تایید سرور ابر که به یک شیوه ی امن رمزگذاری شده است را ارسال می کند .

TPA تایید سرور ابر برای کاربر و اشتراک نتایج تضمین صحت برای سرور ابر که برای تایید درخواست کاربرمی باشد.

۵ . تجزیه و تحلیل امنیت

برای رسیدن به اطمینان از صحت ذخیره سازی داده ها و محلی سازی خطا در داده ها به طور همزمان، این مقاله بر روی یک طرح پروتکل پاسخ به چالش متمرکزاست .



شکل ۲ : پروتکل پاسخ چالش (Challenge Response Protocol)

A . چالش ایجاد رمز

ایده اصلی این است- هنگامی که یک فایل در ابر توزیع شده ، کاربر قبل از محاسبه تعداد معینی از نشانه تأیید کوتاه بر بردار فردی $(j \{1, . . . , n\})$ G^j ، هر یک از پوشش نشانه رمز یک زیر مجموعه تصادفی از بلوک های داده ها است که درسرورهای مختلف ابر توزیع شده است .

بعدها، هنگامی که کاربر می خواهد از صحت ذخیره سازی برای داده ها در ابر مطمئن شود ، او سرورهای ابر را با مجموعه ای از تولید تصادفی شاخص های بلوک به چالش می کشد .

پس از دریافت چالش، هر محاسبه سرور ابر یک "امضا" کوتاه (خلاصه) بالای (بر فراز) بلوک های مشخص شده می باشد و آنها را به کاربر برمی گرداند.ارزش این امضا باید با نشانه های مربوطه به قبل از محاسبه توسط کاربر مطابقت داشته باشد.

فرض کنید که اگر کاربر بخواهد سرور ابر را t بار(در زمان t) برای اطمینان از صحت ذخیره سازی داده ها به چالش بکشد ، کاربر باید قبل از محاسبه نشانه تأیید X برای هر $(j \{1, . . . , n\})$ G^j ،یک کلید چالش k_{chal} و یک کلید جایگشت ارشد (اصلی) K_{prp} داشته باشد . برای تولید رمز i^{th} برای سرور j ، کاربر به شرح زیر عمل می کند:

۱ . مشتق یک مقدار چالش تصادفی i و یک کلید جایگشت $K^{(i)}_{prp}$ بر اساس K_{PRP} .

۲ . محاسبه مجموعه ای از r انتخاب شاخص به طور تصادفی .

۳ . محاسبه رمز V^j_i با استفاده از ارزش چالش های تصادفی.

پس از تولید رمز، کاربر هرکدام از، نگه داشتن نشانه های از پیش محاسبه شده به صورت محلی و یا ذخیره سازی آنها به صورت رمزگذاری شده در سرورهای ابر را انتخاب می کند .

B . تأیید صحت

مقادیر پاسخ از سرور(سرویس دهنده) برای هر چالش نه تنها برای تعیین صحت ذخیره سازی توزیع شده است ، بلکه (اما همچنین) حاوی مطالب و اطلاعات برای قرار دادن خطای داده های بالقوه نیز می باشد .

در این روش از i^{th} پاسخ به چالش برای تایید بیش از d سرور(سرویس دهنده) است که به صورت زیر توضیح داده شده است :

- کلید جایگشت به هر سرور را کاربر نشان می دهد.
- سرور نگهداری(ذخیره سازی) بردار $G^{(j)}$ جمع آن در K ردیف ، توسط شاخص کلید جایگشت در یک ترکیب خطی مشخص شده است .
- پس از دریافت ترکیبی خطی از تمام سرور ها(سرویس دهنده ها)، کاربر از ارزش های کور (کم مقدار- کم ارزش) دور می گردد .
- پس از تایید کاربر، مقادیر دریافتی باقی مانده یک کلمه کد معتبر است که توسط ماتریس مخفیP تعیین می شود .

۶ . بازیابی اطلاعات

FEC اطلاعاتی است که معمولا به دستگاه های ذخیره سازی انبوه برای فعال کردن بازیابی از داده های خراب شده (فاسد)اضافه شده است.

افزونگی اجازه می دهد تا گیرنده به شناسایی تعداد محدودی از اشتباهات که ممکن است در هر نقطه از پیام رخ دهد ، و اغلب به تصحیح این اشتباهات بدون ارسال مجدد می پردازد .

دو چالش ها در استفاده از FEC نرخ حساسیت و حساسیت پشت سرهم (sensitivity.Burst) میباشد .

ترک میانی(Interleaving) در یک روش کدگذاری استاندارد برای مبارزه با از دست دادن پشت سرهم (bursty) استفاده می شود ، که در آن بسته های تصحیح خطا از بلوک های متلاشی شده(گسسته - مجزا) متناوب از داده ها به جای استفاده از بسته های متوالی تولید شده است.

به عنوان مثال، با ترک بین (Interleave) شاخصی از ۴، رمزگذار بسته های اصلاح به طور جداگانه سه بلوک مجزا را ایجاد می کند .

اولین بلوک حاوی شماره بسته های داده (0,4,,...(m-1).4) ، دوم با شماره بسته های داده (1,5,7,..,((m-1).4)+1) ، سوم با شماره بسته های داده (2,6,8,...((m-1).4)+2) و بلوک چهارم شامل (3,7,…((m-1).4)+3) ترک بین (Interleaving) به FEC تحمل پشت سر هم می افزاید، اما تشدید حساسیت آن نسبت به سرعت ارسال .

با ترک بین (Interleave) شاخصی از i و یک نرخ رمزگذاری (m, k)، فرستنده مجبور به صبر (m-1) + 1 . i برای بسته های اطلاعاتی قبل از ارسال هر گونه افزونگی (تفاوت) اطلاعات است .

۷ . نتیجه گیری و آینده کار (کار آینده)

رایانش ابری در حال کسب محبوبیت قابل توجهی در سال های اخیر برای منافع خود است از نظر انعطاف پذیری، مقیاس پذیری، قابلیت اطمینان، و مقرون به صرفه می باشد .

با وجود تمام وعده ها با این حال، رایانش ابری دارای یک مشکل است: امنیت .

در این مقاله، ما مشکلات امنیت داده ها در ابر ذخیره سازی داده ها را مورد مطالعه قرار دادیم ، که در اصل یک سیستم ذخیره سازی توزیع شده بود.

طرح توزیع موثر و قابل انعطاف برای اطمینان از صحت داده های کاربران در سرورهای ابری پیشنهاد شده است.

اگر این تایید صحت ، مصرف منابع بیش از حد در سمت کاربر است، این کار را می توان به حسابرس شخص ثالث واگذار و نشانه های از قبل محاسبه شده می توانند یا در دستگاه محلی کاربر و یا سرور ابر در فرمت های رمزگذاری شده باشد.

توسط امنیتی دقیق و تجزیه و تحلیل عملکرد، ما نشان می دهیم که طرح ما در بازیابی تقریبا بلافاصله تلفات تک قلو و بازیابی از تلفات داده پشت سرهم (bursty) بسیار کارآمد است.

ما چند جهت ممکن برای تحقیقات آینده در این زمینه در ذهن مجسم می کنیم . ما به عنوان کار آینده بر روی کاهش تاثیر در حفظ کلید چالش در فضای محلی کاربر تمرکز می کنیم .

برای این کار ما می توانیم کلید چالش را به چند کلید قطعات جزئی تقسیم کنیم و آن کلید را در سرور های مختلف ابر حفظ کنیم و در عین حال از امنیت و شفافیت داده ها اطمینان بیابیم . این ممکن است فضای سربار و تایید متقابل ممکن از فرآیند تایید ازیک TPA توسط دیگر TPAs را کاهش دهد.

- منابع انتهای مقاله:

C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in cloud computing,” in Proc. of IWQoS’09, July 2009, pp. 1–9.

Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE transactions on Services Computing, 06 May 2011.

D. L. G. Filho and P. S. L. M. Barreto, “Demonstrating Data Possession and Uncheatable Data Transfer,” Cryptology ePrint Archive, Report 2006/150, 2006, http://eprint.iacr.org/.

G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. of CCS’07, Alexandria, VA, October 2007, pp. 598–609.

M. A. Shah, R. Swaminathan, and M. Baker, “Privacy-preserving audit and extraction of digital contents,” Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.

H. Shacham and B. Waters, “Compact proofs of retrievability,” in Proc. of Asiacrypt’08, volume 5350 of LNCS, 2008, pp. 90–107.

K. D. Bowers, A. Juels, and A. Oprea, “Proofs of retrievability: Theory and implementation,” in Proc. of ACM workshop on Cloud Computing security (CCSW’09), 2009, pp. 43–54.

M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to keep online storage services honest,” in Proc. of HotOS’07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.

M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, “A cooperative internet backup scheme,” in Proc. of the 2003 USENIX Annual Technical Conference (General Track), 2003, pp. 29–41.

کارگاه‌های آموزشی مرکز اطلاعات علمی

آموزش مهارت های کاربردی در تدوین و چاپ مقاله

اصول تنظیم قراردادها

مقاله نویسی علوم انسانی