حسابرسی انسجام عمومی در داده های ابر مشترک و پویا

چکیده

محاسبه ابر سکو ذخیره حائز اهمیتی است که در حال حاضر موضوع تحقیقات است. ایـن مسـئله خـدمات متنـوعی برای کاربران خود فراهم می سازد. از میان آنها، یکی از خدمات برجسته ارائه شده ذخیره ابـر مـی باشـد کـه بـرون سپاری داده ها را به روند رو به افزایش تبدیل نموده است. اما مسئله عمده و مـرتبط، انسـجام و تفکیـک داده هـای برون سپاری شده می باشد. کاربران لازم می دانند که داده های خود در برابر هر نوع دستکاری یا دسترسی غیرمجاز، ایمن باشد. لذا روشی باید وجود داشته باشد برای تایید اینکه آیا داده ها بدون نیاز به بازیابی دست نخـورده انـد یـا خیر. این امر نیاز به حسابرسی ایمن داده ها از راه دور را تقویت می کند. این مقاله طرح حسابرسی بر اسـاس تعهـد برداری، امضا حلقه ای مبنی بر هویت و پروتکل تطابق کلید گروهی فراهم می کند کـه برگرفتـه از جفـت دوخطـی است. تحلیل آزمایشی طرح مطرح شده نشان می دهد طرح پیشنهادی هنگام مقایسه با طرح های مرتبط با خود، نیز کارآمد است.

کلید واژه: محاسبه ابر، حسابرسی انسجام عمومی، تعهد برداری، امضا حلقه ای، پروتکل تطابق کلید گروهی.

1-مقدمه

محاسبه ابر را می توان به عنوان محاسبه مبنی بر شبکه تعریف نمود که منابع و داده های پردازشی مشـترکی بـرای کاربران خود در هنگام نیاز فراهم می سازد. به ازای هر نوع ان.آی.اس.تی، آن مدلی است که امکان دسترسی جامع و طبق نیاز به منابع اشتراکی را فراهم می سازد که می توان بلافاصله آن را با حداقل تلاش مدیریتی فـراهم نمـوده و عرضه نهاد (29). این مدل برای کاربر قابلیت های متنوعی جهت ذخیره داده های خود در سرور ابر و پردازش آن در هنگام نیاز فراهم می کند. این امر سازمان ها را انگیزه می بخشد داده های خود را به سـرور ذخیـره خـارجی بـرون سپاری کرده و محدودیت های ذخیره ابزارهای محلی را بهبود بخشند و این امکان را به آنها می دهد بر توانمندهای اصلی خود تمرکز بیشتری داشته باشند. کاربر ابر می توان در هر زمان بر حسب نیاز به داده ها از هر نقطه از جهـان

دسترسی داشته باشد اما در مواردی همانند از کارافتادگی سخت افزار و غیره، سرور ممکن است به نتیجه نـامعتبری دست یابد. لذا انسجام داده ها به مسئله بزرگی برای کاربران ابر تبدیل می شود چرا که دیگر کنترل فیزیکی بر داده های برون سپاری شده ندارند. لذا برای اطمینان یابی از اینکه آیا داده ها ایمن هستند یا خیر، شیوه ای بـرای تاییـد انسجام و دسترسی آن باید برای کاربران وجود داشته باشد.

چند راه حل برای اطمینان از انسجام و دسترسی داده های ذخیره شده در سرور از راه دور مطرح شده انـد. مـولفین در مرجع (2)، (28)، (10)، (24)، (25)، (35)، (37) و (32) طرح پویا را مطرح می کنند که بر مواردی تاکید دارد که در آن فقط دارنده می تواند داده های ذخیره شده تعدیل کند. در نـرم افزارهـای (19)، (20) و (21) کـه در آن پشتیبانی امر به عنوان سکو همکاری به کار می رود، کاربران گروه چندگانه کد را به اشتراک گذاشته و می تواند آن را در هر زمان و از هر مکان تجدید نظر نموده و اجرا کنند و به آن دسترسی داشته باشند. این نوع شـبکه همکـاری طرح های حسابرسی از راه دور را غیرعملی می سازد که در آن فقط دارنده داده هـا مـی توانـد داده هـا را تعـدیل و دستکاری کند. آن باعث هزینه مازاد محاسباتی و ارتباطاتی برای دارنده داده ها می گردد و برای وی نامناسب است. اگر تایید انسجام را بتوان با فرد دیگری به جز دارنده داده ها یعنی حسابرس شخص ثالث انجام داد، آنگاه طـرح بـه طور آشکار قابل تایید است. طرح (38) به طراحی برچسب های صحه گذاری چندجمله ای می پردازد و از راهبرد به روز رسانی برچسب جایگزین برای پشتیبانی از حسابرسی عمومی استفاده مـی کنـد امـا محرمانـه بـودن داده هـای کاربران گروه در نظر گرفته نمی شود. این بدان معناست که این طرح از به روز رسانی داده و بررسی انسـجام جهـت متن ساده پشتیبانی به جای متن کدگذاری پشتیبانی می کند. با این وجود هیچ نـوع راه حلـی بـه بررسـی مسـئله بررسی انسجام عمومی با تعدیل کاربر گروه نمی پردازد. کمبود این طرح ها به ما انگیزه می دهد تـا شـیوه معتبـر و کارآمدی برای حسابرسی داده های از راه دور فراهم سازیم. در این راستا نوعی ساختاربندی مطرح می گردد که تعهد برداری را در پایگاه داده ها به کار می گیرد و از کدگذاری و کدگشایی داده ای گروهی در طـی تعـدیل و دسـتکاری پشتیبانی می کند و پروتکل تطابق کلید گروهی استفاده می کند (36). امضاهای حلقـه ای مبنـی بـر هویـت (39) برای پشتیبانی از بی نامی امضاکننده به کار می روند.

1-1 اثرگذاری ما

این مقاله روشی برای حسابرسی انسجام عمومی و موثر مطرح می کند که بر اساس طرحی در مرجع (27) می باشد. مسائل حسابرسی انسجام عمومی بیشتر مطالعه شدند و تعهد برداری برگرفته از طرح موجود (27) با امضا حلقه ای مبنی بر هویت ترکیب می شوند تا طرح بررسی انسجام داده های عمومی موثر مطرح کنند. در پایان ارزیابی عملکرد طرح مطرح شده نشان می دهد که آن موثرتر از طرح موجود است.

2-آثار مرتبط

دسترسی، انسجام و محرمانگی ویژگی های عمده داده های ذخیره شده در سرور ابر اند. آثار جدی انجام شده اند که در پی روشی برای برون سپاری ایمن داده های محلی برای سرور ذخیره و حسابرسی از راه دور اند. مولفین در مقالات (2) و (28)، طرح صحه گذاری همشکل را به کار می گیرند تا هزینه ارتباطات و محاسبه را کاهش دهند. بعدها، استانداردهای دیگر این طرح ها آماده شد تا کارایی آنها از جمله امکان حسابرسی داده های عمومی (35)، (34) و (37) و به روز رسانی داده ها (24) و (25) اصلاح گردد. در مرجع (4) طرحی پیشنهاد می گردد که از رجوع مجدد کاربر پشتیبانی می کند. اما بر این فرض ساختاربندی می شود که برخوردی وجود ندارد و بین کاربر رجوع کرده و سرور ابر رخ نمی دهد.فرض بر این است که کانال مورد تایید انحصاری بین هویت ها وجود دارد. یوان و یو طرح حسابرسی پویا در (38) پیشنهاد دادند که از روش به روز رسانی برچسب جایگزین استفاده کرده و بر مبنای برچسب های صحه گذاری چندجمله ای ایجاد می کند اما ذخیره متن کدگذاری را در نظر نمی گیرد. بنابز با همکاران (8) طرح پایگاه داده قابل تایید مطرح می کنند اما مسئله این است که تایید پذیری عمومی در آن پشتیبانی نمی گردد. مولفین شیوه جدیدی در مرجع (16) مطرح می کنند تا پایگاه داده ای ایجاد کنند که با استفاده از تعهد بردار قابل تایید می باشد که از تایید پذیری عمومی پشتیبانی می کند. این طرح پایگاه داده برون سپاری را اندازه ثابت فرض می کند و نیز آنکه کاربر دارای توانایی دستیابی به اطلاعات درباره کارکرد برون سپاری از قبل می باشد. بیکس با همکاران طرحی در (5) مطرح می کنند که دارای ویژگی هایی است که این فرض را از میان بر می دارد. امضا گروهی ابتدا در مرجع (17) معرفی شد. این روش امضا به هر عضو گروه این اجازه را می دهد تا

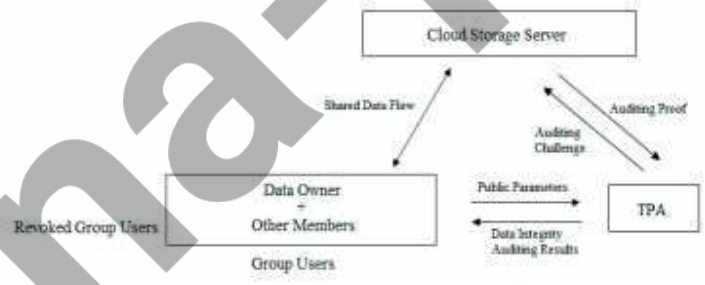
دارای کلید رمز بوده و پیامی را امضا نمایند. فقط مدیر گروه هویت امضا کننده حقیقی را می داند که هویت مورد اعتماد بوده و لذا بدین ترتیب این شکل امضا کردن بی نامی امضا کنندگان را تایید می کند. این نوع امضا در مراجع (8)، (15)، (14)، (3)، (13)، (33) مطالعه شده است. مولفین امضا گروهی را پیشنهاد کرده اند که از رجوع محلی تایید کننده در مقاله (9) پشتیبانی می کند. در طرح پیشنهادی، اطلاعات رجوع به تایید گر امضا در رجوع کاربر ارسال می گردد. به هر حال روند شروع برای تعیین گروه در این طرح مورد نیاز است که ممکن است تحت برخی شرایط عملی نباشد. ایده امضا حلقه ای در مرجع (31) معرفی گردید. طرح پیشنهاد شده در (31) بر مبنای کلید عمومی آر.اس.ای می باشد و امنیت آن در مدل رمز ایده آل تحلیل می گردد (6). مقاله (11) این طرح را بهبود بخشیده و امضا حلقه ای مطرح می کند که امنیت آن در مدل اوراکل تصادفی تحلیل می گردد (7).

3-طرح بندی مسئله

این بخش به جزئیات ساختار سیستم مطرح شده و طراحی آن می پردازد در حالی که مدل تهدید و اهداف امنیتی طرح موجود را در مرجع (27) مد نظر قرار دارد.

3-1 ساختار سیستم

طرح مطرح شده شامل سه مولفه است:کاربران گروهی، سرور ذخیره ابر و حسابرس شخص ثالث همانطور که در شکل 1 نشان داده شده است.

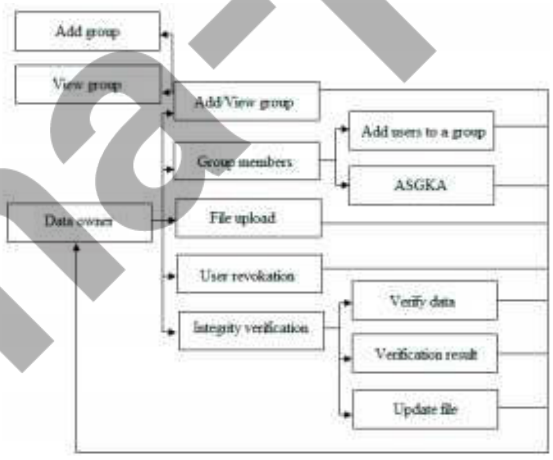


شکل 1- ساختار سیستم

- کاربران گروهی:آنها شامل دارندگان داده ها و اعضا دیگر گروه هستند که دارنده داده ها می تواند داده های ذخیره شده خود را در کنار امتیازات دسترسی، دستکاری و غیره به اشتراک بگذارد.
- سرور ذخیره ابر: آن مسئول فراهم سازی خدمات ذخیره برای کاربر ابر است. آن دارای قابلیت اعتماد نیمه بوده و لذا امکان حمله وجود دارد.
- حسابرس شخص ثالث: آن مسئول تایید انسجام داده های ذخیره شده به محض درخواست است. آن به حسابرسی فایل پرداخته و نتیجه را بازمی فرستد.

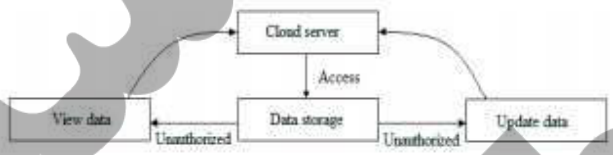
3-3 طراحی سیستم

- دارنده داده ها: اگر کاربر ابر بخواهد برخی داده ها را در بین تعدادی از کاربران به اشتراک بگذارد، آنگاه به عنوان دارنده داده ها عمل می کند. دارنده داده ها ممک ناست داده های داده های ذخیره شده خود را در بین اعضا گروه موجود به اشتراک گذارد یا گروه جدیدی ایجاد کند که فقط شامل اعضایی باشد که با آنها می خواهد داده ها را به اشتراک گذارد. اگر وی نخواهد برخی از داده های خود را با هر عضو گروه به اشتراک بگذارد، می تواند به راحتی این کار را انجام دهد. به علاوه وی دارای این حق و امتیاز است که داده های خود را با کدگذاری آنها قبل از بارگذاری در ابر ایمن سازد. شکل 2 نشان دهنده کارهایی است که دارنده داده ها می تواند انجام دهد.



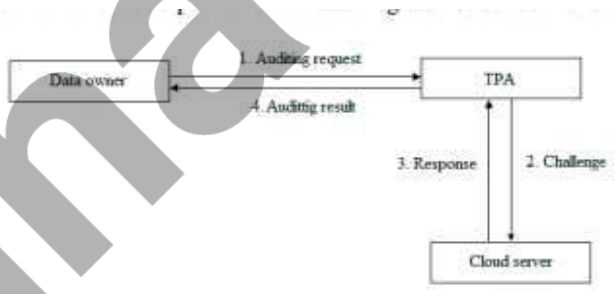
شکل 2- دارنده داده ها

- سرور ابر: سرور ابر سرور ذخیر هاز راه دورو برای داده های کاربران است. تمامی داده های بارگذاری شده توسط دارنده داده ها در این سرور ذخیره، نگهداری می شوند. چون اعتماد آن نیمه است، این امکان وجود دارد که ابر احتمالا بخواهد به داده های ذخیره شده طبق شکل 3 دست یابد. این تلاش از جانب سرور ابر پذیرفته شده نبست و این نوع دسترسی غیرمجاز به داده های ذخیره شده با هدف مشاهده یا دستکاری آنها اطلاعات دارندگان داده ها را آسیب پذیر می سازد. لذا برای پشتیبانی علیه افشا داده ها در صورت این اقدام از سوی سرور ابر، داده ها باید کد گذاری شوند قبل از اینکه در محل دور ذخیره شوند که به میزان امنیت داده های ذخیره شده می افزاید.



شکل 3- سرور ابر

- حسابرس شخص ثالث: آن مسئول تایید انسجام داده هاست هنگامی که هر عضو گروه درخواست می کند همانطور که در شکل 4 نشان داده شده است. هر زمان که درخواست تایید انسجام مطرح می شود، آن چالشی ایجاد می کند و آن را به سرور ابر می فرستد. تی.پی.ای به محض دریافت پاسخ از ابر فعالیت حسابرسی را انجام داده و نتیجه را به کاربر می فرستد.



شکل 4:حسابرس شخص ثالث

4-مطالب پایه ای

این بخش به مرور تمامی اصول اولیه به کار رفته در طرح پیشنهادی می پردازد.

4-1گروه های دوخطی

گیریم دو گروه مضرب $G_1 \& G_2$ دارای مرتبه نخست P و $g_1 \& g_2$ به عنوان مولد باشند. فرض می کنیم ψ تناظر برگرفته از G2به G1 با $\psi(g_2) = g_1$ بوده و $e : G_1 X G_2 \longrightarrow G_T$ نقشه دوخطی با ویژگی های زیر باشد:

- قابلیت شمارش: الگوریتم موثر برای محاسبه eوجود دارد.
- دو خطی: به ازای هر $u \in G_1, v \in G_2$ و $a, b \in Z_p$ $e(u^a, v^b) = e(u, v)^{ab}$
- تجزیه ناپذیری: $e(g_1, g_2) \neq 1$

4-2 مفروضات پیچیدگی

امنیت روش پیشنهادی به مفاهیم مسائلی از جمله مسئله خطی تصمیم، مسئله دیفی-هلمن قوی و مسئله دیفی-هلمن محاسباتی بستگی دارد که در زیر توصیف می شود:

- مسئله خطی تصمیم: گیریم G1 گروه چرخه ای باشد که دارای g1 به عنوان مولد و مرتبه اولpمی باشد. با توجه به $u, v, h, u^a, u^b, u^c \in G_1$ به عنوان ورودی؛ اگر $a + b = c$, خروجی آری و در غیر این صورت خیر است.

- مسئله دیفی هلمن قوی:حال دو گروه G1,G2 مرتبه اول p (حدالمقدور) در نظر می گیریم که g1 مولد گروه G1و g2مولد G2است. با توجه به $(q+2)$ام $(g_1, g_2, g_2^{\gamma}, g_2^{\gamma^2}, \ldots)$ به عنوان ورودی، جفت $(g_1^{\frac{1}{\gamma+x}}, x)$ را به عنوان خروجی تولید کنید که در آن $x \in Z_p^*$.
- مسئله دیفی-هلمن محاسباتی:گیریم G1گروه چرخشی دارای g1به عنوان مولد باشد. گیریم مرتبه اول گروه p باشد. با توجه به (g, g^x) به ازای $x \in Z_p$، g^{x^2} را به عنوان خروجی تولید کنید.

4-3 تعهد بُرداری

یکی از مهم ترین مسائل در رمزنگاری طرح تعهد است. تعهد برداری (16) از جمله آنهاست که به کاربر اجازه می دهد به مقدار انتخابی پایبند باشد، آن را از دیگران مخفی نگه دارد به شیوه ای که مقدار متعهد را بتوان بعدها افشا نمود. این طرح تعهد در دو ویژگی صدق می کند، یعنی مخفی کردن و پایبندی. لذا مقادیر اولیه ایجاد شده بر مبنای تعهد بردری در حل مسئله برون سپاری داده های قابل تایید مفید اند. این طرح تعهد شامل الگوریتم های زیر است:

- بردار تعهد.کلید مولد: با توجه به پارامتر امنیت و اندازه بردار متعهد به عنوان ورودی، این الگوریتم پارامترهایی تولید می کند که عمومی شده اند.
- بردار تعهد.محاسبه: باتوجه به پیام ورودی m و پارامترهای عمومی، آن رشته تعهد C را به ازای پیام محاسبه می کند.
- بردار تعهد.باز کردن: این الگوریتم اثباتی را ایجاد می کند که m برابر پیام متعهد i-thاست.
- بردار تعهد. تایید: این الگوریتم صحه گذاری فقط زمانی قبول می کند اثبات اینکه C ایجاد شده به ازای پیام i-th معتبر باشد.

- بردار تعهد.به روز رسانی: این الگورویتم طرح تعهد بردار ا ز سوی متعهد اجرا می شود که رشته تعهد را ایجاد کرده و می خواهد آن را با تغییر پیام i-th برابر m به m’ به روز رسانی کند. آن پیام قدیمی، پیام جدید و موقعیت i را به عنوان ورودی اتخاذ نموده و تعهد جدید به عنوان خروجی تولید می کند.

4-4 امضا حلقه ای مبنی بر هویت

امضا حلقه ای مبنی بر هویت (آی.دی) (39) ترکیبی از امضا حقله ای کلی و مورد مبتنی بر هویت است. به طور دقیق تر، این طرح اساسا امضا حلقه ای است که در آن کلید عمومی کاربر هویت امضاکنندگان است. این طحر شامل سه هویت است:امضا کننده، کاربر و عامل با اقتدار مورد اعتماد؛ و مجموعه ای از چهار الگوریتم است که در زیر توصیف می شود:

- برپاسازی: آن توسط عامل با اقتدار مورد اعتماد اجرا می شود و چند پارامتر و کلید اصلی ضمن دریافت پارامتر امنیت به عنوان ورودی تولید می کند.
- استخراج: این الگوریتم کلید خصوصی برای کاربر ایجاد می کند هنگامی که توسط عامل با اقتدار مورد اعتماد بر مبنای ورودی پارامتر، کلید اصلی و هویت دلخواه اجرا می گردد. منظور از هویت، همان هویت امضاکنندگان است و از کلید عمومی امضا کنندگان استفاده می کند.
- امضا: این الگوریتم ضمن دریافت پارامتر، کلید خصوصی امضا کننده، لیست هویت هایی که شامل هویت امضا کننده و پیام است، امضاء پیام را به عنوان خروجی ارائه می دهد.
- تایید:این الگوریتم تایید می کند آیا امضا به ازای پیام ورودی معتبر است یا خیر.

5- طرح پیشنهادی

5-1 مرور

طرح پیشنهادی بر مبنای طرح موجود در مرجع (27) است که از امضا گروهی استفاده می کند. این شکل امضا به هر عضو گروه این اجازه را می دهد تا پیام ها را از طرف کل گروه امضا کنند در حالی که بی نامی و حریم را فراهم می سازد. در گروه، مدیری وجود دارد که اعضا را به گروه اضافه می کند و می تواند امضا کننده را در حالت هر نوع منازعه افشا کند. در طرح پیشنهادی، امضا حلقه ای مبنی بر هویت به جای امضا گروهی به کار می رود. امضا حلقه ای به هر تعداد کاربران این اجازه را می دهد تا دور هم جمع شده و گروهی تشکیل دهند به منظور اینکه داده ها را در میان خود به اشتراک گذارند بودن اینکه نیاز به مدیر گروه یا هر نوع آماده سازی مازاد باشد. آن جمع آوری موقت کاربران است که در آن هر فرد می تواند تایید کند آیا امضا به واسطه فرد متعلق به مجموعه ایجاد شده است. این نوع امضا در محافظت از بی نامی مفید است چرا که روشی برای تعیین هویت امضا کننده وجود ندارد. شکل 5 نشان دهنده الگوریتم های به کار رفته در طرح پیشنهادی است:

شکل 5:طرح پیشنهادی

هر چند کار انجام شده با طرح امضا گروهی متغییر است، مسائل خاصی وجود دارد که باید بررسی شوند از جمله مدیریت کلید پیچیده، اجرا مدیر گروه، هزینه محاسبه مازاد و غیره. طرح امضا حلقه ای مبنی بر هویت به طور موفقیت آمیز به تمامی این مسائل می پردازد. تکنیک استفاده از رشته معروف عمومی درباره کاربر همانند ایمیل، شماره تلفن و غیره به عنوان کلید عمومی وی تا حدودی مثالی از مدیریت کلید است. طرح امضا حلقه ای شامل تعداد کمتر محاسبات نسبن به طرح امضا گروهی در محاسبه امضا در پیام است. به علاوه عدم حضور مدیر گروه به عنوان مزیت برای کاربران عمل می کند چرا که هر تعداد از کاربران می توانند در هر زمان گروهی را ایجاد کنند بدون اینکه نیاز به مشارکت شخص ثالث باشد.

5-2 طرح محسوس

طرح مطرح شده شامل پنج الگوریتم می باشد که شامل برپاسازی، تایید، جستجو، به روز رسانی و اثبات به روز رسانی است. اختلاف عمده با طرح موجود در تولید امضا و بخش صحه گذاری است. این بخش تعریف محسوس طرح پیشنهادی را بر مبنای تعهد برداری و امضا حلقه مبنی بر هویت مطرح می سازد. پایگاه داده ای را در نظر بگیرید که دارای چندتایی (i, m_i) می باشد که در آن i شاخص و m_i مقدار مرتبط است.تعداد nکاربر یک گروه صرفا دارای یک دارنده داده ها این پایگاه داده ها را به اشتراک می گذارد. گیریم $M = Z_p$ فضای پیام بوده و k پارامتر امنیت باشد.

- راه اندازی

1- فرض می کنیم دو گروه دو خطی G و G_T دارای مرتبه اولیه P باشند. طرح دوخطی $e : G \longrightarrow G_T$ و g به عنوان مولد G را در نظر بگیرید. برای شروع $z_1, \ldots z_q \longleftarrow Z_p$، را به طور تصادفی انتخاب کنید. حال داریم $h_i = g^{z_i}$ ، $\forall i = 1, \ldots, q$، و $\forall i, j = 1, \ldots, q, i \neq j$، $h_{i,j} = g^{z_i z_j}$ را محاسبه کنید. حال برای به دست آوردن پارامترهای عمومی PP، تعهد برداری کلید تولید توسط دارنده داده ها اجرا می شود. پارامترهای عمومی هستند. $PP = (p, q, G, G_T, H, g, (h_i)_{i\in[q]}, \{h_{i,j}\}_{i,j\in[q],i\neq j})$.

2- گروه G با تولید کنندهP را در نظر می گیریم. $s \in Z_q^*$ را به طور تصادفی انتخاب کنید و $P_{pub} = sP$. گیریم s کلید اصلی عامل بااقتدار مورد اعتماد باشد. به محض دریافت هویت به عنوان ورودی، خروجی $S_{id} = sH_1(ID)$ به عنوان کلید خصوصی مربوط به هویت و کلید عمومی برابر $Q_{id} = H_1(ID)$. می باشد. بدین ترتیب کلیدهای رمز را برای تمامی کاربران تولید می کنیم.

3- رشته تعهد و دیکر اطلاعات جانبی را با استفاده از الگوریتم محاسبه طرح تعهد بردار طبق زیر تعیین کنید:

$$C = h_1^{m_1}, h_2^{m_2}, ..., h_q^{m_q}$$
$$aux = (m_1, m_2, ..., m_q)$$

4- آنگاه برای تعیین امضا پیام ورودی m، الگوریتم امضا طرح امضا حلقه مبنی بر هویت را در تعهد اجرا کنید. عضو $A \in G$ را انتخاب کنید و $c_{k+1} = H(L \| m \| e(A, P))$. را تعیین کنید. حال دنباله حلقه را جهت تولید هدایت کنید. به ازای $i = k+1, ..., n-1, 0, 1, ..., k-1$، $T_i \in G$ را انتخاب کنید و بیابید:

$$c_{i+1} = H(L \| m \| e(T_i, P)e(c_i H_1(ID_i), P_{pub}))$$

تعیین کنید:

$$T_k = A - c_k S_{ID_k}$$

امضا پیام برابر مرتبه چندگانه $(n+1)$ است: $(c_0, T_0, T_1, ..., T_{n-1})$.

- جستجو

کاربر گروه تعهد برداری.باز کردن را برای محاسبه یک نوع اثبات از میان پیام متعهد i-th اجرا می کند:

$$\Lambda_i^t = \Pi_{j-1, j \neq i}^q \cdot h_{i,j}^{m_j^t} = (\Pi_{j=1, j \neq i}^q \cdot h_j^{m_j^t})^{z_i}$$

- تایید

1- در ورودی پیام و امضا متناظر با آن، حسابرس شخص ثالث ابتدا پایایی امضا را تایید می کند. حسابرس به ازای آن الگوریتم صحه گذاری طرح امضا حلقه ای را اجرا می کند. این الگوریتم محاسبه می کند:

$$c_{i+1} = H(L \| m \| e(T_i, P)e(c_i H_1(ID_i), P_{pub})) \text{ for } i = 0, 1, ..., n-1$$

ضمن دریافت امضا $(c_0, T_0, T_1, ..., T_{n-1})$ به عنوان ورودی & می پذیرد اگر:

$$(c_n = c_0)\ .$$

2-اگر امضاء معتبر باشد، حسابرس تعهد برداری.تایید را اجرا می کند تا تایید کند که آیا معادله زیر برقـرار است یا خیر.اگر خروجی آن یک باشد، رابطه زیر برقرار است.

$$e(C^t / h_i^{m_i^t}, h_i) = e(\Lambda_i^t, g)$$

- به روز رسانی

1-کاربر گروه پایگاه داده فعلی را برای اطمینان یابی از پایایی خود، تایید می کند.

2- برای به روز رسانی پیام m_i به m_i' ، کاربر تعهد برداری.به روز رسانی را اجرا می کند و تعهد به روز رسانی C=C′فراهم می کند. $h_i^{m'-m}$ & اطلاعات به روز رسانی شده $U = (m, m', i)$ به عنوان خروجی است.

- اثبات به روزرسانی

1-حسابرس شخص ثالث تعهد برداری.اثبات به روز رسانی را برای محاسبه اثبات به روزرسانی شده Λ_j به ازای پیام در موقعیت j اجرا می کند به طوری که این اثبات جدید با توجه به تعهد جدید C′ معتبر است کـه حـاوی پیام به روز رسانی شده m′ به عنوان پیام جدید در موقعیت j است.

2-حسابرس از اطلاعات به روز رسانی برای تولید اثبات به روز رسانی استفاده می کند. اگر $i \neq j$، تعهد به روز رسانی شده $C' = C \cdot h_i^{m'-m}$ و اثبات به روز $\Lambda_j' = \Lambda_j \cdot (h_i^{m'-m})^{z_j} = \Lambda_j' \cdot h_{j,i}^{m'-m}$ را بیابید. اگر i=j $C' = C \cdot h_i^{m'-m}$ را با اثبات باقی مانده به طور یکسان بیابید.

6-ارزیابی عملکرد

طرح پیشنهادی به حل مسائل کارکارایی طرح های حسابرسی انسجام عمومی می پردازد که در آن داده ها توسط کاربری امضا می گردد که به گروهی تعلق دارد که در آن داده ها به اشتراک گذاشته شده و هر عضو می تواند به روز رسانی داده های قابل تایید را انجام دهد. این بخش تحلیل عملکرد طرح پیشنهادی را مطرح نموده و مقایسه ای با طرح موجود انجام می دهد. فرض می شود که بلوک های ساختاری پایه ای طرح ایمن هستند.

آزمایشات در ویندوز 10 دستگاه با اینتل هسته ¢ i7-4770 CPI اجرا شده در 3.40GHz و حافظه 8 گیگ اجرا می شوند. گروهی که دارای اعضا کمتر می باشد در نظر گرفته می شود که دارای تمامی امتیازات اعطا شده از جانب دارنده داده ها باشد. نخست اینکه یک تلاش محاسباتی زمانی در مرحله شروع مورد نیاز است. آن کارآمد است چرا که منابع سرمایه گذاری شده توسط کاربر به اندازه پایگاه داده بستگی ندارد و گران ترین محاسبات به سرور ابر برون سپاری می شوند.

شکل 6- تولید امضا

شکل 6 نشان دهنده زمان صرف شده در الگوریتم های تولید امضا می باشد. طرح موجود از امضا گروهی برای محاسبه امضا در پیام استفاده می کند در حالی که طرح پیشنهادی از امضا حلقه ای بدین منظور استفاده می کند. همانطور که به گروه کوچک کاربران علاقه مند هستیم، طرح امضا حلقه ای زمان کمتری در مقایسه با مورد امضا گروهی می برد. طرح امضا گروهی نیاز به تعداد یکسانی از محاسبات صرف نظر از تعداد کاربران دارد اما طرح دیگر به تعداد کاربران بستگی دارد. آن را به وضوح می توان از گراف مشاهده نمود که طرح امضا حلقه ای به ازای تعداد کمتر کاربران دارای زمان محاسباتی کمتری در مقایسه با طرح امضا گروهی است.

شکل 7- تایید حسابرس شخص ثالث

الگوریتم تعهد برداری.باز کردن مسئول تولید اثبات پیام تعهد است و زمان صرف شده در آن نمایی از تعداد فایل ها به ازای طرح موجود و نیز پیشنهادی است. همانطور که تهداد فایل ها افزایش می یابد، هزینه مازاد محاسباتی افزایش می یابد. زمان سپری شده از جانب حسابرس شخص ثالث برای تایید فایل در شکل 8 نشان داده شده

است. به وضوح از تصویر دیده می شود که حسابرس زمان کمتری استفاده می کند تا به تایید فایل بپردازد که امضا آن با طرح امضا حلقه ای به جای طرح امضا گروهی محاسبه می شود. اما هنوز زمان سپری شده توسط حسابرس شخص ثالث تقریبا در تایید امضا تولید شده با طرح های استفاده شده یکسان است. این اختلاف کم در زمان صحه گذاری به خاطر تعداد محاسبات شامل شده در فرایند تایید می باشد. طرح دوم این مقدار مازاد را تا حدودی کاهش می دهد همانطور که در شکل مشاهده می شود.

7- نتیجه گیری

طرح پیشنهادی به طور موفقیت آمیز اجرا می شود تا حریم و انسجام داده های ذخیره شده در سرورهای ابر از راه دور حفظ گردد. طرح های مختلف به کار رفته حسابرسی ادغام داده های ایمن را تحقق می بخشند. طرح امضا حلقه ای مبنی بر هویت زمان کمتری می برد تا امضا را به ازای کاربران گروه کوچک محاسبه کند هنگامی که ب طرح امضا گروهی به کار رفته در روش موجود مقایسه می شود. به ازای گروه کوچک، تعداد محاسبات انجام شده در طرح امضا حلقه ای کمتر از مواد طرح امضا گروهی در طی تولید و نیز تایید مضا می باشد که هزینه مازاد محاسبه را کاهش می دهد. به علاوه، هویتی همانند مدیر گروه در حالت امضا حلقه وجود ندارد که به هر تعداد کاربران اجازه دهد گروهی برای اشتراک گذاری داده ها در بین خود ایجاد کنند، بر خلاف امضا گروهی که در ان مدیر گروه مسئول انجام فعالیت ها می باشد. از این رو، ترکیب این مقادیر اولیه روش پیشنهادی را مقدر می سازد پیگاه داده کدگذاری شده را به سرور ابر از راه دور برون سپاری کند و محرمانگی داده ها برای گروه کوچک فراهم می سازد. همچنین تحلیل عملکرد نشان می دهد که طرح پیشنهادی در منظر گروه کوچک در مقایسه با طرح موجود کارآمدتر است.

8- آثار آتی

طرح پیشنهادی در حال حاضر از رجوع کاربر گروه و نیز مکانیسم مسئولیت پذیری کاربر پشتیبانی نمی کند. این مسئله از جمله معایب این طرح به شمار می رود هنگامی که دارنده داده ها دیگر نمی خواهد داده های خود

را با برخی اعضا گروه به اشتراک گذارد یا زمانی که شناسایی امضا کننده پیام حائز اهمیت باشد. می توان بهبودهایی را در طرح پیشنهادی با شامل سازی این ویژگی ها فراهم آورد.