یک رویکرد محاسباتی آگاه از امنیت و حریم خصوصی در مورد اشتراک داده ها در محیط ابری

مصطفی المیاحی[۱]، سمیه سلطانی[۲]، سید امین حسینی سنو[۳]

[۱] گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد
almayahi@mail.um.ac.ir

[۲] گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد
somayeh.soltani@mail.um.ac.ir

[۳] دانشیار، گروه کامپیوتر، دانشکده مهندسی، دانشگاه فردوسی مشهد
hosseini@um.ac.ir

چکیده

امروزه ابرهای محاسباتی در زندگی روزمره ما نقش پر رنگی را ایفا می‌نمایند. از آنجایی که بستر ارتباطی بین کاربران و ابر عمومی، شبکه اینترنت است، برقراری امنیت داده‌های ارسال شده و حفظ حریم خصوصی کاربران تبدیل به یک چالش بزرگ شده است. در این مقاله روشی برای قابلیت ردیابی کاربرانی ارائه شده است که با استفاده از کلید خصوصی و خصیصه‌های خود اقدام به رمزگشایی داده‌های موجود در سیستم می‌کنند. روش پیشنهادی عناصر خرابکاری که از این امکان سوءاستفاده نموده و آن را در اختیار دیگران قرار می‌دهند و موجب نشت اطلاعاتی در سیستم می‌گردند را شناسایی می‌کند. همچنین روش پیشنهادی راه کاری برای امنیت سیاست‌های ارسال شده به همراه متن‌های رمز شده برای برقراری کامل ایمنی سیستم و جلوگیری از نقض حریم خصوصی مالکان داده‌ها ارائه می‌دهد. نتایج شبیه‌سازی برتری راه کار پیشنهادی در مقایسه با روش مقاله پایه از جهت میزان توانایی سیستم در یافتن عناصر خرابکار و میزان امنیت سیستم در جلوگیری از نقض حریم خصوصی کاربران را نشان می‌دهد.

کلمات کلیدی

محاسبات ابری، رمزگذاری مبتنی بر ویژگی، رمزگذاری حفظ ترتیب، حریم خصوصی، سیاست کنترل دسترسی

۱- مقدمه

محاسبات ابری به جدیدترین پیشرفت فن‌آوری مدرن محاسبات تبدیل شده است [۱]. کارهای محاسباتی بزرگ به بخش‌های کوچکتر تقسیم می‌شوند و هر بخش برای محاسبه در ابر توزیع می‌شود [۲]. از آنجا که داده‌ها در محاسبات ابری شامل اطلاعات شخصی کاربران است، امنیت آنها از اهمیت حیاتی برخوردار است [۳]. فرض می‌کنیم که سرور ابر نیمه اعتماد است، چرا که ابر فضایی باز است و همه می‌توانند به آن دسترسی پیدا کنند [۴]. مهاجمان ممکن است داده‌ها را در روند ارتباطات شنود کنند و یا حتی آنها را تغییر دهند. این می‌تواند حریم خصوصی کاربران را به خطر بیندازد [۵]. بنابراین، محافظت از حریم خصوصی در ابر بسیار مورد توجه قرار گرفته است.

کارهای تحقیقاتی متعددی در حوزه امنیت و حریم خصوصی اشتراک داده‌ها در محیط ابری وجود دارند که می‌توان آنها را از جهات مختلف دسته‌بندی کرد. مقاله‌های [۱۲-۶] متدهایی برای حفظ حریم خصوصی در محاسبات ابری ارائه داده‌اند. مقاله‌های [۱۹-۱۳] مدل‌هایی برای ارزیابی اعتماد در محاسبات ابری ارائه داده‌اند. مقاله‌های [۲۶-۲۰] بر روی مبحث

رمزگذاری مبتنی بر ویژگی در ابر تمرکز کرده‌اند. مقاله‌های [۳۰-۲۷] نیز بر روی مبحث کنترل دسترسی در ابر کار کرده‌اند.

برای محافظت از حریم خصوصی، رمزگذاری کلید عمومی به عنوان قدرتمندترین مکانیزم در نظر گرفته می‌شود [۳]. علاوه بر این ، رمزگذاری مبتنی بر ویژگی به عنوان طرح مناسب برای ابر در نظر گرفته می‌شود. رمزگذاری مبتنی بر ویژگی همچنین یک تکنولوژی بسیار مناسب برای کنترل دسترسی ایمن و انعطاف‌پذیر ریزدانه است. با این حال، بیشتر طرح‌های رمزگذاری مبتنی بر ویژگی موجود برای محاسبات ابری مناسب نیستند زیرا شامل عملیات جفت شدن پرهزینه هستند و به‌خصوص برای دستگاه‌های تلفن همراه با منابع محدود چالش بزرگی را ایجاد می‌کنند [۵].

به‌علاوه، استفاده از رمزنگاری برای حفظ حریم خصوصی کاربران، بار محاسباتی زیادی را بر کاربران تحمیل می‌نماید. یکی از روش‌هایی که موجب می‌شود این بار محاسباتی کاهش پیدا کند برون‌سپاری برخی عملیات محاسباتی می‌باشد. در اکثر کارهای تحقیقاتی، تنها عمل رمزگشایی به ابر محاسباتی سپرده می‌شود و این موجب خواهد شد هنوز بار محاسباتی سنگین مربوط به عمل رمزگذاری برعهده کاربران باقی بماند. با این حال، فن و همکاران [۲]، علاوه بر عملیات مربوط به رمزگشایی، اکثر عملیات رمزنگاری را نیز به ابر عمومی برون‌سپاری کرده‌اند که بار محاسباتی حداکثری را از روی دوش کاربران برداشته است. آنها برای انجام این کار از روش رمزنگاری CP-ABE استفاده نموده‌اند و همچنین برای منقضی شدن کاربران روشی اتخاذ کرده‌اند تا کاربران پس از اتمام کار با سیستم از آن حذف شوند و اجازه دسترسی غیرمجاز به کاربران منقضی شده داده نشود.

البته فن و همکاران به این نکته توجه نکرده‌اند که امکان نشت اطلاعاتی در سیستم بدین گونه وجود خواهد داشت که کاربران مجاز (کاربرانی که خصیصه‌هایشان مطابق با درخت سیاست موجود در داده‌ها باشد) می‌توانند این امکان خود را به دیگران منتقل نمایند. در واقع، هر کاربری که خصیصه‌هایش با درخت سیاست داده‌ها تطبیق داشته باشد می‌تواند داده‌ها را رمزگشایی نماید. حال اگر این کاربر اقدام به فروش کلید خصوصی خود کند و از این طریق حریم خصوصی داده‌ها و امنیت آنها را مورد حمله قرار دهد، روش پیشنهادی فن و همکاران تمهیداتی برای مقابله با این حمله نیندیشیده است.

از طرف دیگر، در روش فن و همکاران مشابه روش‌های دیگر CP-ABE در هر بار ارسال سیاست، این رشته به صورت متن واضح همراه متن رمز شده ارسال می‌گردد. این حالت ارسال موجب خواهد شد که اگر افراد غیرمجاز هم این پیام را دریافت کنند از روی سیاست متوجه این نکته بشوند که پیام می‌تواند توسط چه کسانی باز شود و این خود موجب نقض حریم خصوصی مالکان داده‌ها خواهد بود.

برای حل این چالش‌ها روشی در این مقاله ارائه شده است که قابلیت ردیابی کاربرانی که با استفاده از کلید خصوصی و خصیصه‌های خود اقدام به رمزگشایی داده‌های موجود در سیستم می‌نمایند، را دارد و عناصر خرابکاری که از این امکان سوءاستفاده نموده و آن را در اختیار دیگران قرار می‌دهند و موجب نشت اطلاعاتی در سیستم می‌گردند نیز یافت می‌شوند. همچنین امنیت سیاست‌های ارسال شده به همراه متن‌های رمز شده برای برقراری کامل ایمنی سیستم و جلوگیری از نقض حریم خصوصی مالکان داده‌ها در نظر گرفته شده است.

در ادامه این مقاله در بخش ۲ به مرور کارهای پیشین پرداخته می‌شود. در بخش ۳ مدل کردن مسئله ارائه می‌شود. در بخش ۴ روش پیشنهادی ارائه می‌شود. بخش ۵ نتایج آزمایشات را مورد بحث قرار می‌دهد و در بخش آخر نتیجه‌گیری مقاله آورده شده است.

۲- مدل مسئله

مدل پیشنهادی ما از پنج موجودیت تشکیل شده است که عبارتند از یک ارائه دهنده خدمات ابری (CSP)، یک مرجع صدور گواهینامه جهانی (CA)، مالک داده (DO)، کاربر داده (DU) و مراجع ویژگی (AA).

CSP مسئول ذخیره اطلاعات شامل متن رمزی، کلیدها و لیست کاربران است. سرویس دسترسی داده به DU نیز توسط CSP پشتیبانی می‌شود. CSP همچنین مسئول عملیات مربوط به لغو کاربر و لغو ویژگی است. علاوه بر این، CSP وظیفه تولید بخشی از متن رمز و پیش‌رمزگشایی را بر عهده می‌گیرد. اگر و فقط اگر ویژگی‌های DU سیاست کنترل دسترسی را برآورده کنند، CSP می‌تواند از کلیدهای درگیر برای پیش‌رمزگشایی استفاده کند. پس از آن، این قسمت از متن رمزی رمزگشایی شده برای رمزگشایی نهایی به DU ارسال می‌شود.

DO کسی است که سیاست کنترل دسترسی روی ویژگی‌ها را برای این طرح رمزگذاری و تعریف می‌کند. یک DO داده‌ها را بر اساس آن سیاست کنترل دسترسی رمزگذاری می‌کند و اگر هر DU بخواهد متن رمزی تا حدی رمزگشایی شده را از CSP دریافت کند، ویژگی‌های DU باید سیاست دسترسی را برآورده کند.

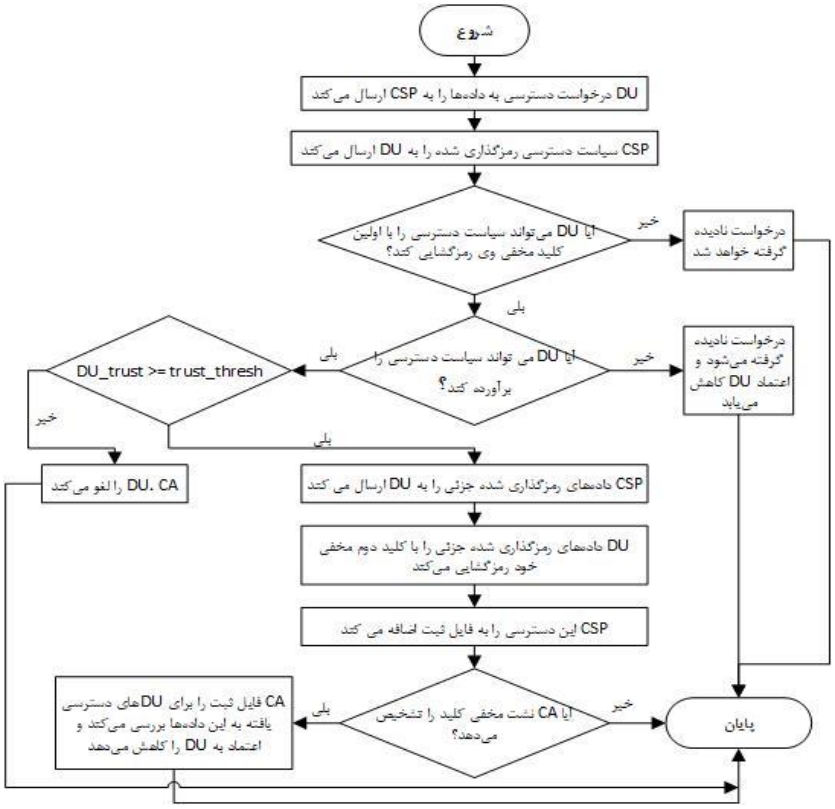
DU کسی است که می‌خواهد اطلاعات محرمانه DO را تأیید کند. اگر مجموعه ویژگی‌هایی که DU دارد سیاست دسترسی را برآورده می‌کند، CSP کلیدهای مخفی برای رمزگشایی خواهد داشت. پس از اینکه CSP تا حدی رمزگشایی کرد، DU می‌تواند متن رمزی تا حدی رمزگشایی شده را دریافت کند. سپس DU می‌تواند داده‌ها را با کلید مخفی خود بازیابی کند.

موجودیت‌های AA هیچ ارتباطی با یکدیگر ندارند. آنها مسئول ویژگی‌های کاربران هستند که به طور مستقل صادر، لغو و بروز می‌شوند. در طرح ما، هر کاربر به کلیدهای خصوصی ویژگی مربوط به ویژگی‌های درگیر نیاز دارد. AAای که ویژگی‌ها متعلق به او است، مسئول صدور این کلیدهای خصوصی ویژگی است.

CA تنها سازمانی است که به‌طور کامل در طرح ما مورد اعتماد است. همه AAها و DUها باید در CA ثبت نام کنند. CA مسئولیت عملیات راه‌اندازی طرح را بر عهده می‌گیرد و هویت سراسری برای هر کاربر صادر می‌کند. CA در هیچ محاسبه رمزگذاری و رمزگشایی در طرح دخیل نیست [۳۱].

۳- راه کار پیشنهادی

در راه کار پیشنهادی قصد داریم تا چالش امنیتی بیان شده در مقدمه مقاله را با استفاده از اضافه کردن امکان قابلیت ردیابی کاربرانی که داده‌ها را رمزگشایی می‌کنند برطرف نماییم. علاوه بر این قصد داریم تا راه حلی نیز برای مشکل امنیت سیاست‌های ارسال شده به همراه متن‌های رمز شده ارائه دهیم و نیز امکان انجام پرس‌وجوهایی مشخص مانند پرس‌وجوهای دقیق،



شکل (۱): روند انجام کار روش پیشنهادی

بازه‌ای، Min و Max بر روی داده‌های رمزشده فراهم نماییم. از این رو، راه کار پیشنهادی از سه قسمت تشکیل خواهد شد که در ادامه در مورد آنها توضیح خواهیم داد. روند انجام کار در روش پیشنهادی در شکل ۱ نشان داده شده است.

۳-۱- افزودن امکان قابلیت ردیابی کاربران سیستم

با ردیابی کاربرانی که از داده‌ها استفاده می‌کنند می‌توانیم به شناسایی عناصر خرابکار در سیستم بپردازیم. در اکثر روش‌های CP-ABE ارائه شده به این مشکل نشت اطلاعاتی کمتر پرداخته شده است. از آنجایی که کاربران متعددی می‌توانند با استفاده از خصیصه‌های خود داده‌ها را رمزگشایی کنند امکان اینکه سیستم متوجه شود چه افرادی (مجاز یا غیرمجاز) به داده‌ها دستیابی پیدا کرده‌اند بسیار مشکل است و اینکه افرادی که این عمل را انجام داده‌اند با استفاده از چه کلیدهای خصوصی توانسته‌اند داده‌ها را رمزگشایی نمایند نیز کار سختی است. برای مثال، از آنجایی که کلید خصوصی براساس خصیصه‌های کاربران تولید می‌گردد، کاربرانی که خصیصه‌های مشابهی دارند دارای کلید خصوصی مشابهی خواهند بود که در نتیجه در زمان رمزگشایی متوجه نخواهیم شد کدام کاربر اقدام به رمزگشایی نموده است. این مشکل امنیتی با عنوان نشت کلید مخفی شناخته می‌شود و راه حل آن این گونه باید باشد که با ردیابی این عناصر، خرابکاران در سیستم شناسایی شوند و در ادامه، می‌بایست این عناصر خرابکار از سیستم حذف شوند. مکانیزم پیشنهادی در قسمت ابطال نیز تغییراتی را بوجود می‌آورد تا در نهایت این عناصر خرابکار از سیستم حذف شوند.

۳-۲- افزایش امنیت سیاست‌های ارسال شده به همراه متن‌های رمزشده

در این بخش قصد داریم به برقراری امنیت در مورد سیاست‌های فرستاده شده به همراه پیام‌های متنی رمز شده بپردازیم که نشان دهنده کاربرانی است که اجازه دسترسی به اطلاعات را دارا هستند. یک راه اولیه برای این مسئله می‌تواند این باشد که برای هر ویژگی جفتی از نام و مقدار داشته باشیم و در سیاست تنها نام‌ها را قرار دهیم و مقادیر مربوط به هر ویژگی را درون متن رمزی قرار دهیم. به این ترتیب، چنانچه یک گره خرابکار به پیام و البته سیاست همراه آن دسترسی پیدا کند، از روی فیلد نام مربوط به ویژگی‌ها نمی‌تواند به اطلاعات مهمی دستیابی پیدا کند و در نتیجه حریم خصوصی کاربران نقض نخواهد شد.

۳-۳- انجام برخی پرس‌وجوهای خاص بر روی داده‌های رمز شده در ابر

یکی از مسائل حل نشده سرویس‌های ابری، امنیت داده‌های ذخیره شده است. قبل از اینکه کاربر داده به سرویس ابری اعتماد کند، باید از حفظ حریم خصوصی آنها اطمینان حاصل کند و خطر دسترسی غیرمجاز به اطلاعات توسط افراد مختلف و از جمله مالک سرویس ابری را حذف یا به حداقل برساند. طرح رمزگذاری حفظ ترتیب (OPES) یک روش رمزگذاری است که ترتیب عددی متن‌های ساده را حفظ می‌کند [۴]. طرح رمزگذاری حفظ ترتیب اجازه می‌دهد برخی پرس‌وجوها مستقیماً بدون رمزگشایی عملوندها بر روی داده‌های رمزشده انجام شود. پرس‌وجوهای تطبیق دقیق، بازه‌ای، Min،

Max و Count را می‌توان مستقیماً بر روی داده‌های رمزگذاری شده پردازش کرد. به طور مشابه، عملیات GROUP BY و ORDER BY نیز قابل پردازش است. فقط هنگام اعمال SUM یا AVG بر روی گروه، مقادیر باید رمزگشایی شوند. الگوریتم ۱ مراحل مختلف روش پیشنهادی را بیان می‌کند.

الگوریتم 1 الگوریتم پردازش درخواست ها

```
1. Input: RequestFromDUs,
2. requests=Receive_RequestFromDUs ();
3.     while (requests ? null ) do for each request
4.           Send_ EncryptedAccessPolicy(request.DU); // The CSP sends the
     encrypted access policy  back to  DU
5.           success= request.DU.Decrypt_accessPolicy (DU.secrect key);
6.           if (success==true) then
7.                 if (request.DU.Satisfy_Policy(request.DU.attributes)) then
8.                       if (request.DU.trust>= trust_thresh)) then
9.                       request.DU.Receive_PartiallyEncryptedDataOPES()
10.  request.DU.Decrypt_PartiallyEncryptedDataOPES(request.DU.secondSecretK
     ey);
11.                      addToLog file(request);
12.                      if (Detection_SecretKeyLeakage()==true) then
13.                            DecreaseTrust(request.DU);
14.                      end if
15.                else
16.                      Revoke(DU);
17.                end if
18.          else
19.                Request_ignore(request);
20.                DecreaseTrust(request.DU);
21.          end if
22.    else
23.          Request_ignore(request);
24.    end if
25.    end while
```

الگوریتم به این صورت عمل می‌کند که در خط ۲ تمام درخواست‌هایی که از تمامی DUها ارسال می‌شود در آرایه درخواست‌ها (requests) قرار داده می‌شود. در CSP و در خط سوم الگوریتم تا زمانی که درخواستی وجود داشته باشد، یعنی آرایه درخواست‌ها برابر با Null نشده باشد، برای هر درخواست کارهای زیر انجام می‌شود. در خط ۴ داده‌های دسترسی سیاست رمز شده برای DU که درخواست را داده ارسال می‌شود. بعد در خط ۶ اگر این DU بتواند این دسترسی سیاست را با کلید مخفی خود رمزگشایی کند، یعنی success==true، آن گاه در خط ۷ اگر DU بتواند سیاست دسترسی را با ویژگی‌های خودش برآورده کند و در خط ۸ اگر اعتماد DU از اعتماد آستانه بیشتر باشد آنگاه عملیات انجام می‌شود. میزان اعتماد آستانه در شبیه‌سازی برابر ۰.۵ در نظر گرفته شده است. DU می‌تواند داده رمزشده جزئی با OPES را دریافت کند و به کمک کلید مخفی دوم آن را رمزگشایی کند و در نهایت این درخواست پردازش شده در فایل log ثبت می‌شود. در خط ۱۲ اگر CSP یک نشت کلید کشف کند، به عبارتی بتواند یک تخطی از این کلید مخفی‌ها که به بیرون درز کرده کشف کند، اعتماد DU را کاهش می‌دهد. اگر DU اعتمادش از اعتماد آستانه کمتر باشد، CSP آن را ابطال می‌کند. اگر اعتماد DU از اعتماد آستانه کمتر باشد، DU را ابطال می‌کند (خط ۱۶). اگر DU نتواند سیاست را برآورده کند، درخواستش رد می‌شود و اعتمادش کاهش پیدا می‌کند (خط ۱۹و ۲۰). اگر DU نتواند سیاست دسترسی را رمزگشایی کند اینجا هم درخواست رد می‌شود (خط ۲۳).

۴- آزمایش‌ها و نتایج ارزیابی

برای شبیه‌سازی روش پیشنهادی از شبیه‌ساز iFogsim استفاده شده است. کتابخانه iFogsim مبتنی بر زبان برنامه نویسی جاوا بوده و دارای ماژول‌ها و کلاس‌هایی جهت شبیه‌سازی محاسبات مه است [۳۲]. این کتابخانه توسعه یافته شبیه‌ساز کلودسیم است و از بسیاری کلاس‌های کلودسیم بهره می‌برد. سیستم کامپیوتری که شبیه‌سازی این تحقیق در آن اجرا شده دارای پردازنده اینتل از نوع Core i7 با سرعت ۲ گیگاهرتز، حافظه RAM به اندازه ۱۲ گیگابایت و تحت سیستم عامل مایکروسافت ویندوز ۱۰ از نوع ۶۴بیتی می‌باشد.

پارامترهایی که برای شبیه‌سازی روش پیشنهادی مورد استفاده قرار گرفته است در جدول ۱ نشان داده شده است. تعداد مالک‌های داده برابر ۱۰، تعداد کاربران داده برابر ۱۰۰ و تعداد حملات برابر ۲ تا ۱۰ تا حمله درنظر گرفته شده است. همچنین نرخ کاربران متخلف (کل کاربران/کل متخلف) برابر سه مقدار ۰.۰۱، ۰.۰۵ و ۰.۱ درنظر گرفته شده است.

جدول (۱): پارامترهای شبیه‌سازی روش پیشنهادی

پارامترها	مقادیر
تعداد مالک‌های داده	۱۰
تعداد کاربران داده	۱۰۰
تعداد حملات	۲ تا ۱۰
میزان کاربران متخلف	۰.۰۱و۰.۰۵و۰.۱

برای ارزیابی راهکار پیشنهادی، نتایج به دست آمده با مقاله [۲] مقایسه می‌گردد. بدین منظور، مهمترین فاکتورهایی که نشان دهنده بهبود روش پیشنهادی خواهد بود عبارت است از:

- میزان توانایی سیستم در یافتن عناصر خرابکار
- میزان امنیت سیستم در جلوگیری از نقض حریم خصوصی کاربران
- هزینه رمزگشایی

برای ارزیابی راه کار پیشنهادی، سناریوی دسترسی به داده‌های ذخیره شده در ابر محاسباتی مورد استفاده قرار گرفته است. بدین معنی که مالکان داده‌ها قصد دارند داده‌های خود را در ابر محاسباتی به صورت ایمن ذخیره نمایند. در سمت مقابل کاربران سیستم نیز قصد دارند تا با استفاده از خصیصه‌های خود به داده‌های موجود به صورت مجاز دسترسی پیدا کنند.

۴-۱- میزان توانایی سیستم در یافتن عناصر خرابکار

با بررسی نتایج شبیه‌سازی، به این نتیجه رسیدیم که راه کار پیشنهادی در مقایسه با مقاله پایه هم در مورد معیار میزان توانایی سیستم در یافتن عناصر خرابکاری که در سیستم موجب مشکل نشت کلید مخفی شده‌اند و هم در مورد معیار میزان امنیت سیستم در جلوگیری از نقض حریم خصوصی کاربران از وضعیت بهتری برخودار است. بدین منظور، یک تعداد حمله شبیه‌سازی شده است که در این حملات هدف به دست آوردن ویژگی‌ها و همچنین کلیدهای خصوصی کاربران و داده‌ها بوده است. به این شکل که در هر حمله با توجه به ویژگی‌های کاربر، حمله کننده تلاش برای به دست آوردن کلید خصوصی کاربر می‌کند. این معیار براساس تعداد دفعاتی که کلید مخفی افشا شده به تعداد کل کلیدهای مخفی موجود به دست می‌آید. نتایج میزان کاربران متخلف در شکل ۲ آورده شده است.

شکل (۲): مقایسه میزان کاربران متخلف در روش پیشنهادی و مقاله [۲]

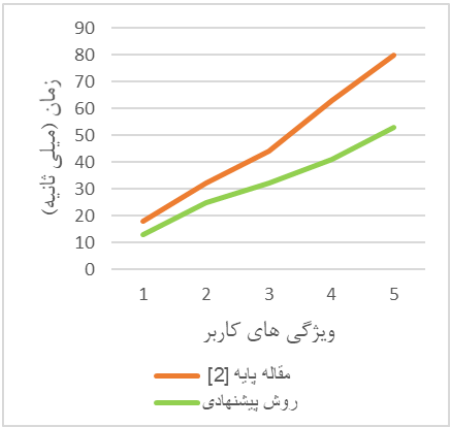
۴-۲- میزان مقاومت سیستم در مقابل حملات نقض حریم خصوصی

با بررسی نتایج شبیه‌سازی، به این نتیجه رسیدیم که راه کار پیشنهادی در مقایسه با روش مقاله پایه در مورد معیار میزان هزینه رمزگشایی از وضعیت بهتری برخودار است. دلیل برتری روش پیشنهادی این است که روش پیشنهادی اقدام به مخفی‌سازی سیاست ارسالی به همراه متن رمز شده نموده است. این مخفی‌سازی از افشای اطلاعات که منجر به نقض حریم خصوصی مالکان داده‌ها می‌شود جلوگیری به عمل آورده است. نتایج تعداد حملات موفق در شکل ۳ آورده شده است. این معیار براساس تعداد ویژگی‌هایی که افشا شده است به تعداد کل ویژگی‌های موجود به دست می‌آید.

شکل (۳): مقایسه نشت ویژگی در روش پیشنهادی و مقاله [۲]

۴-۳- هزینه رمزگشایی

شکل ۴ هزینه محاسبه مورد نیاز برای عملیات رمزگشایی کاربر در روش پیشنهادی و مقاله [۲] را نشان می‌دهد. هزینه محاسبه رمزگشایی کاربر با توجه به مجموعه ویژگی کاربر متفاوت است. هزینه محاسبه به طور متوسط از ۲۰ اجرا بدست می‌آید. با بررسی نتایج شبیه‌سازی، به این نتیجه می‌رسیم که راه کار پیشنهادی در مقایسه با روش مقاله پایه در مورد معیار هزینه محاسبه رمزگشایی از وضعیت بهتری برخودار است. دلیل برتری روش پیشنهادی این است که در روش پیشنهادی از طرح OPES استفاده شده که برای عملیات ریاضی نیاز به رمزگشایی و سپس رمزنگاری مجدد نمی‌باشد که این کار بهبود زیادی در تاخیر داشته است. طرح OPES اجازه می‌دهد عملیات مقایسه مستقیماً بدون رمزگشایی عملوندها بر روی داده‌های رمزگذاری شده اعمال شود.



شکل (۴): مقایسه هزینه زمانی روش پیشنهادی و مقاله [۲]

۵- نتیجه گیری

در این مقاله روشی برای قابلیت ردیابی کاربرانی که با استفاده از کلید خصوصی و خصیصه‌های خود اقدام به رمزگشایی داده‌های موجود در سیستم می‌نمایند و یافتن عناصر خرابکاری که از این امکان سوءاستفاده نموده و آن را در اختیار دیگران قرار می‌دهند و موجب نشت اطلاعاتی در سیستم می‌گردند ارائه شده است. همچنین امنیت سیاست‌های ارسال شده به همراه متن‌های رمز شده برای برقراری کامل ایمنی سیستم و جلوگیری از نقض حریم خصوصی مالکان داده‌ها در نظر گرفته شده است. در روش پیشنهادی از OPES استفاده شده و انجام بسیاری از پرس‌وجوها نیاز به رمزگشایی و سپس رمزنگاری مجدد ندارد که این کار باعث کاهش تاخیر شده است. با بررسی نتایج شبیه‌سازی، به این نتیجه رسیدیم که راه کار پیشنهادی در مقایسه با روش‌های موجود هم در مورد معیار میزان توانایی سیستم در یافتن عناصر خرابکاری که در سیستم موجب مشکل نشت کلید مخفی شده‌اند و هم در مورد معیار میزان امنیت سیستم در جلوگیری از نقض حریم خصوصی کاربران از وضعیت بهتری برخودار است. همچنین روش پیشنهادی در مقایسه با روش‌های موجود دارای هزینه محاسبه رمزگشایی کمتری است.

مراجع

[1] Hajibaba, M., and Gorgin, S. "A review on modern distributed computing paradigms: Cloud computing, jungle computing and fog computing." CIT. Journal of Computing and Information Technology, vol. 22, no. 2, pp. 69-84, 2014.

[2] Fan, K., Liu, T., Zhang, K., Li, H. and Yang, Y., "A secure and efficient outsourced computation on data sharing scheme for privacy computing. " Journal of Parallel and Distributed Computing, vol. 135, no. 1, pp.169-176, 2020.

[3] Waters B., "Ciphertext-Policy Attribute-based Encryption: An Expressive, Efficient, and Provably Secure Realization." International Workshop on Public Key Cryptography Springer Berlin Heidelberg, vol. 1, no. 1, pp. 53-70, 2008.

and Computer Applications, vol. 154, no. 1, pp. 102533, 2020.

[19] Sun, P. "Research on cloud computing service based on trust access control." International Journal of Engineering Business Management, vol. 12, no.1, pp. 1847979019897444, 2020.

[20] Kumar, Praveen, and P. J. A. Alphonse. "Attribute based encryption in cloud computing: a survey, gap analysis, and future directions." Journal of Network and Computer Applications, vol. 108, no. 1, pp. 37-52, 2018.

[21] Li, J., Chen, N., and Zh, Y. "Extended file hierarchy access control scheme with attribute based encryption in cloud computing." IEEE Transactions on Emerging Topics in Computing, vol. 1, no. 1, pp. 1-9, 2019.

[22] Yang, Y., Chen, X., Chen, H., and Du, X. "Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing." IEEE Access, vol. 6, no. 1, pp. 18009-18021, 2018.

[23] Gunjal, Y. S., Gunjal, M. S., and Tambe, A. R. "Hybrid attribute based encryption and customizable authorization in cloud computing." In 2018 International Conference On Advances in Communication and Computing Technology (ICACCT), pp. 187-190, 2018.

[24] Joshi, M., Joshi, K., and Finin, T. "Attribute based encryption for secure access to cloud based EHR systems." In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 932-935, 2018

[25] Zhang, L., Gao, X., Guo, F., and Hu, G. "Improving the Leakage Rate of Ciphertext-Policy Attribute-Based Encryption for Cloud Computing." IEEE Access, vol. 8, no. 1, pp. 94033-94042, 2020.

[26] Liao, Y., Zhang, G., and Chen, H. "Cost-Efficient Outsourced Decryption of Attribute-Based Encryption Schemes for Both Users and Cloud Server in Green Cloud Computing." IEEE Access, vol. 8, no. 1, pp. 20862-20869, 2020.

[27] Roy, S., Das, A. K., Chatterjee, S., Kumar, N., Chattopadhyay, S., and Rodrigues, J. J. "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications." IEEE Transactions on Industrial Informatics, vol. 15, no. 1, pp. 457-468, 2018.

[28] Sankaran, K. S., Vasudevan, N., Prakash, V. R., and Diderot, P. K. G. "Access Control based Efficient Hybrid Security Mechanisms for Cloud Storage." In 2019 International Conference on Communication and Signal Processing (ICCSP), pp. 0564-0567, 2019.

[29] Almarhabi, K. " Arbiter: a lightweight, secured and enhanced access control mechanism for cloud computing." In 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1-5, 2019.

[30] Singh, A., Chandra, U., Kumar, Sh., and Chatterjee, K. "A Secure Access Control Model for E-health Cloud." In TENCON 2019-2019 IEEE Region 10 Conference (TENCON), pp. 2329-2334, 2019.

[31] Seno, S. A. H., Budiarto, R., & Wan, T. C. (2011). A secure mobile ad hoc network based on distributed certificate authority. Arabian Journal for Science and Engineering, 36(2), 245-257.

[32] Noorani, N., & Seno, S. A. H. (2018, October). Routing in VANETs based on intersection using SDN and fog computing. In 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE) (pp. 339-344). IEEE.

[4] Soltani, S., Hadavi, M., & Jalili, R. (2011). Separating indexes from data: a distributed scheme for secure database outsourcing. The ISC International Journal of Information Security, 3(2), 121-133.

[5] Li, H., Lan, C., Fu, X., Wang, C., Li, F., and Guo, H "A Secure and Lightweight Fine-Grained Data Sharing Scheme for Mobile Cloud Computing." Sensors, vol. 20, no. 17, pp. 4720, 2020.

[6] Mohanaprakash, T. A., and Andrews, J. "Novel privacy preserving system for Cloud Data security using Signature Hashing Algorithm." In 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1-6, 2019.

[7] Oleshchuk, V. "Secure and Privacy Preserving Pattern Matching in Distributed Cloud-based Data Storage." In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 2, no. 1, pp. 820-823, 2019.

[8] Xiong, H., Zhang, H., and Sun, J. "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing." IEEE Systems Journal, vol. 13, no. 3, pp. 2739-2750, 2018.

[9] Li, Q., Tian, Y., Zhang, Y., Shen, L., and Guo, J. "Efficient Privacy-Preserving Access Control of Mobile Multimedia Data in Cloud Computing." IEEE Access, vol. 7, no. 1, pp. 131534-131542, 2019.

[10] Liu, J., Tang, H., Sun, R., Du, X., and Guizani, M. "Lightweight and Privacy-Preserving Medical Services Access for Healthcare Cloud." IEEE Access, vol. 7, no.1, pp. 106951-106961, 2019.

[11] Huang, Q., Zhang, Z., and Yang, Y. "Privacy-Preserving Media Sharing with Scalable Access Control and Secure Deduplication in Mobile Cloud Computing." IEEE Transactions on Mobile Computing, vol. 20, no. 5, pp.1951-1964, 2020.

[12] Xu, J., Wei, L., Wu, W., Wang, A., Zhang, Y., & Zhou, F. "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system." Future Generation Computer Systems, vol. 108, no. 1, pp. 1287-1296, 2020.

[13] Wang, Y., Wen, J., Zhou, W., & Luo, F. "A novel dynamic cloud service trust evaluation model in cloud computing." In 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference On Big Data Science and Engineering (TrustCom/BigDataSE), pp. 10-15, 2018.

[14] Li, W., Cao, J., Hu, K., Xu, J., and Buyya, R. "A trust-based agent learning model for service composition in mobile cloud computing environments." IEEE Access, vol. 7, no. 1, pp. 34207-34226, 2019.

[15] Rathi, S. R., and Kolekar, V. K. "Trust Model for Computing Security of Cloud." In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-5, 2018.

[16] Wu, X. "Study on Trust Model for Multi-users in Cloud Computing." IJ Network Security, vol. 20, no. 4, pp. 674-682, 2018.

[17] Saeed, O., and Shaikh, R. A. "A user-based trust model for cloud computing environment." International Journal of Advanced Computer Science and Applications, vol. 9, no. 3, pp. 337-346, 2018.

[18] Mohsenzadeh, A., Jalaly Bidgoly, A., and Farjami, Y. "A novel reward and penalty trust evaluation model based on confidence interval using Petri Net." Journal of Network