برون‌سپاری امن داده‌های ابری با استفاده از تسهیم راز مبتنی بر مشبّکه

طاهره غفاری[۱]، کارشناس ارشد؛ شقایق بختیاری چهل‌چشمه[۲]، استادیار

۱- گروه مهندسی کامپیوتر- واحد شهرکرد- دانشگاه آزاد اسلامی - شهرکرد - ایران - tahere_ghafari81@yahoo.com
۲- گروه مهندسی کامپیوتر - واحد شهرکرد- دانشگاه آزاد اسلامی - شهرکرد - ایران - sh.bakhtiari@iaushk.ac.ir

چکیده: در برون‌سپاری داده، مدیریت داده‌ها به‌عنوان یک سرویس به سرویس‌دهنده‌ای بیرونی واگذار می‌شود. ولی مسائل امنیتی مربوط به داده‌های برون‌سپاری شده چالش‌های فراوانی در این زمینه ایجاد می‌کند. تاکنون پژوهش‌های فراوانی در جهت افزایش امنیت انجام شده است که هرکدام مزایا و معایب مربوط به خود را دارد. در این پژوهش با فرض غیرقابل‌اعتماد بودن سرویس‌دهنده‌های بیرونی در ابر و با تکیه بر روش‌های رمزنگاری و تسهیم راز، روشی ارائه شده است تا امنیت داده‌های برون‌سپاری شده در پایگاه داده‌های ابری را فراهم آورد و آن‌ها را از دسترس سرویس‌دهنده‌های بیرونی غیرقابل‌اعتماد، مخفی نگاه دارد. در روش پیشنهادی، تسهیم راز مبتنی بر مشبّکه نیز به کار گرفته شده است تا علاوه بر حل نمودن معایب مربوط به روش تسهیم راز شامیر، امنیت کوانتومی را نیز فراهم کند. ارزیابی روش پیشنهادی، امنیت داده‌های برون‌سپاری شده را به‌خوبی اثبات می‌کند. همچنین نشان می‌دهد که زمان اجرا روش پیشنهادی نسبت به روش‌های پیشین بهبود یافته است. در ضمن در این روش اطلاعات به تعداد سرویس‌دهندگان تفکیک می‌شوند و هر قسمت به یک سرویس‌دهنده ارسال می‌گردد و بدین طریق با حذف تکرار داده‌ها از پهنای باند و حافظه کمتری استفاده می‌شود.

واژه‌های کلیدی: برون‌سپاری داده، پایگاه داده ابر، تسهیم راز، مشبّکه ، محرمانگی

Secure Outsourcing Cloud Data using Lattice-based Secret Sharing

T. Ghafari[1], MSc; S. Bakhtiari Chehelcheshmeh[2], Assistant Professor

1- Department of Computer Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran,
Email: tahere_ghafari81@yahoo.com
2- Faculty of Computer Engineering, Shahrekord Branch, Islamic Azad University, Shahrekord, Iran,
Email: sh.bakhtiari@iaushk.ac.ir

Abstract: In the outsourcing of the data, the management of the data is delegated as a service to the external service provider. However, security issues related to outsourced data create many challenges in this regard. So far, many studies have been done to increase security, each with its own advantages and disadvantages. In this research, assuming the unreliable external service providers in the cloud and relying on cryptographic mechanisms and secret sharing techniques, a method has been proposed to provide the security of outsourcing data, and even provide them with keep hidden from external trusted service providers. In the proposed method, lattice-based encryption is also used. Using lattice encryption, data security is strongly guaranteed against quantum attacks. The evaluation of the proposed method in this paper explains the security of outsourced data. It is also shown that runtime, bandwidth and memory usage of the proposed method are improved compared to previous methods. Meanwhile, in this way, the information is broken down into the number of service providers and each part is sent to a service provider, thereby reducing the bandwidth and memory by eliminating the repetition of the data.

Keywords: Outsourcing Data, Cloud database, Secret Sharing, Lattice, Confidentiality

تاریخ ارسال مقاله:
تاریخ اصلاح مقاله:
تاریخ پذیرش مقاله:
نام نویسنده مسئول: شقایق بختیاری چهل چشمه
نشانی نویسنده مسئول: ایران - شهرکرد- رحمتیه- دانشگاه آزاداسلامی واحد شهرکرد - دانشکده مهندسی فنی و مهندسی-گروه کامپیوتر.

۱ -مقدمه

محاسبات ابری مدلی برای دسترسی آسان و مناسب به شبکه و منابع محاسباتی مشترک است که می‌تواند در حداقل زمان ممکن و حداقل تعامل با ارائه‌دهنده سرویس در اختیار استفاده‌کنندگان قرار گیرد[۱]. حجم زیاد اطلاعات موجود در شرکت‌ها و سازمان‌ها، پایگاه داده‌های ابر را برای استفاده‌کنندگان بسیار جذاب کرده است[۲]. پایگاه داده ابری، پایگاه داده توزیع‌شده‌ای است که از طریق آن می‌توان اطلاعات را در ابر میزبان یعنی ابری که ارائه‌دهنده سرویس‌ها است، ذخیره کرد[۳].

ایده برون‌سپاری داده و مدیریت آن توسط سرویس‌دهنده‌های بیرونی، منجر به ارائه روش‌هایی برای نگهداری و مدیریت امن داده در محیط‌های غیرقابل‌اعتماد گردیده است. بااین‌حال نیازمندی‌های امنیتی، تحقق برون‌سپاری داده‌ها را بر روی ابر به چالش می‌کشد. اطمینان از امنیت داده‌های برون‌سپاری شده در ابر یکی از پراهمیت‌ترین مسائل مربوط به محاسبات ابر و استفاده از پایگاه داده‌های ابری است. در[۴] نشان داده شده است که دغدغه بیش از ۷۰ درصد از افراد در مورد امنیت داده‌هایشان در پایگاه داده‌های ابری است. درواقع نگرانی‌های امنیتی مانعی بزرگ برای استفاده از ابر هستند و چون هنوز از امنیت داده‌های برون‌سپاری شده در آن، اطمینان صد در صد وجود ندارد برخی سازمان‌ها و کاربران تمایلی به استفاده از این تکنولوژی ندارند. بنابراین از بزرگ‌ترین چالش‌های امنیتی ابرها این است که مالک داده، نسبت به مکانی که داده‌هایش در آن قرار داده شده است کنترلی ندارد. به همین دلیل پژوهش برای ارائه راه‌حل‌های برقراری امنیت برای داده‌های برون‌سپاری شده بسیار ضروری است. ازآنجایی‌که تضمین امنیت قوی یکی از ویژگی‌های متمایز رمزنگاری مشبّکه است، در این پژوهش نیز طرحی مبتنی بر مشبّکه ارائه می‌گردد که یکی از ویژگی‌های بارز آن فراهم کردن امنیت در برابر حملات کامپیوترهای کوانتومی می‌باشد. همچنین در طرح پیشنهادی، برای حفظ هر چه بیشتر امنیت اطلاعات، با استفاده از ساختار تسهیم راز به تفکیک اطلاعات و ارتباط بین آن‌ها پرداخته می‌شود.

این مقاله به این شرح است: در بخش ۲ تعدادی از کارهای پیشین آورده شده است، در بخش ۳ روش پیشنهادی شرح داده شده است . در بخش ۴ روش پیشنهادی با برخی روش‌ها مقایسه و ارزیابی شده است و در نهایت، در بخش آخر نتیجه‌گیری و کارهای آتی آمده است.

۲ -کارهای پیشین

چور و همکاران، پژوهشی انجام دادند که در آن از مسئله تسهیم راز برای دستیابی به ارسال هم‌زمان پیام در سیستم‌های غیر هم‌زمان که در مقابل خطا تحمل‌پذیر هستند استفاده شده است. آن‌ها به این مسئله اشاره کرده‌اند که روش شامیر، در برابر خطا تحمل‌پذیر نبوده و در حالتی که توزیع‌کننده خراب شود راهی برای اثبات درستی وجود ندارد [۵].

در مقاله [۶] که توسط هادوی و همکاران ارائه شد، مقادیر یک ویژگی با استفاده از طرح آستانه سفارشی تسهیم راز به چندین بخش تقسیم‌بندی می‌شود و با استفاده از ساختار شاخص‌گذاری درخت B^+ روی صفات قابل جستجو، مقادیر آن‌ها را به‌عنوان نتایج پرس‌وجو تقسیم‌بندی می‌کنند و آن‌ها را به‌عنوان مقادیر راز در سمت سرویس‌گیرنده بازیابی و بازسازی می‌کنند. همچنین از طرح تسهیم راز مطرح شده در الگوریتم شامیر، برای تأیید صحت نتایج پرس‌وجوها استفاده می‌کنند. رویکرد استفاده شده در مقاله آن‌ها زمان اجرای بیشتری نسبت به بسیاری از رویکردهای دیگر دارد، همچنین به دلیل استفاده از تسهیم راز شامیر مشکلات طرح شامیر را دارد و در برابر حملات کوانتومی آسیب‌پذیر است.

آگراوال و همکاران در [۷] از تسهیم راز برای حفظ محرمانه بودن اطلاعات برون‌سپاری شده استفاده کردند. آن‌ها همچنین توابع درهم‌ساز[۱] را برای تکثیر چندجمله‌ای توزیع‌شده و تسهیم داده به کاربردند. در این مقاله برای رمزنگاری داده‌های عددی و اجرای پرس‌وجوهای بازه‌ای از روش رمزنگاری مبتنی بر حفظ ترتیب استفاده شده است. درحالی‌که راه‌حل آن‌ها به‌خوبی انواع پرس‌وجوها را پشتیبانی می‌کند، ولی اگر سرویس‌دهنده‌ها غیرقابل‌اعتماد باشند در معرض استنتاج آماری قرار می‌گیرند.

در [۸] یک پرس‌وجو در چهار مرحله پردازش می‌شود. وقتی کاربر پرس‌وجویی ارسال می‌کند سرویس‌گیرنده آن پرس‌وجو را به پرس‌وجویی که قابل‌اجرا روی داده‌های رمز شده سمت سرویس‌دهنده باشد تبدیل می‌کند. سپس سرویس‌دهنده آن را اجرا می‌کند و نتیجه را برای سرویس‌گیرنده ارسال می‌کند. ایده اصلی این پژوهش استفاده از bucketing و شاخص‌گذاری مقادیر است. برای حفظ محرمانگی، داده‌ها قبل از برون‌سپاری رمزنگاری می‌شوند، ولی زمان اجرای پرس‌وجو در آن نسبتاً زیاد است.

جلیلی و همکاران در [۹] با استفاده از طرح آستانه تسهیم راز شامیر، یک راز را بین n سرویس‌دهنده به اشتراک می‌گذارند و داده‌ها را برون‌سپاری می‌کنند. آن‌ها برای تحقیق خود بر روی داده‌های عددی تمرکز کرده‌اند، درحالی‌که داده‌های غیرعددی هم باید بررسی شوند. همچنین فرض کرده‌اند که سرویس‌دهنده، صادق ولی کنجکاو است، ولی باید این موضوع هم در نظر گرفته شود که ممکن است سرویس‌دهنده‌ها برای حفظ محرمانگی و صحت داده‌ها غیرقابل‌اطمینان باشند.

در [۱۰] از روش رمز کردن به‌وسیله توابع هم‌ریخت به‌عنوان روشی برای رمزنگاری استفاده می‌شود، در رمزنگاری هم‌ریخت، حاصل انجام یک عمل روی داده‌های رمز شده، معادل رمز شده نتیجه همان عمل، روی داده‌های اصلی است. رمزنگاری هم‌ریخت که به‌عنوان راه‌حلی کلیدی برای برون‌سپاری امن محاسبات مطرح شده است، با مشکل اصلی پیچیدگی و سربار اجرایی بالایی روبه‌رو است و تنها

پرس‌وجوهای ساده محاسباتی با توجه به کارآیی روش پیشنهادی، قابل‌اجرا هستند.

راه‌حل‌های موجود رمزنگاری تمام داده‌ها از مقدار کلید، بدون در نظر گرفتن سطح محرمانه بودن اطلاعات که به‌نوبه خود هزینه و زمان پردازش را افزایش می‌دهد، استفاده می‌کردند. بنابراین لو آی توالب و همکاران در [۱۱]، یک مدل محاسبات ابری امن بر اساس طبقه‌بندی داده‌ها ارائه دادند. مدل پیشنهاد شده توسط آن‌ها سربار و زمان پردازش موردنیاز برای حفاظت از داده‌ها را با استفاده از روش‌های امنیتی مختلف با مقادیر کلیدی متغیر برای تأمین سطح مناسب محرمانگی موردنیاز برای داده‌ها به حداقل می‌رساند. روش پیشنهادی این مقاله با الگوریتم‌های رمزنگاری مختلف مورد آزمایش قرار گرفت. نتایج شبیه‌سازی نشان داد که چارچوب آن‌ها دارای زمان پردازش مناسبی است درحالی‌که اطمینان به محرمانه بودن اطلاعات و یکپارچگی نیز حفظ شده است. این روش با استفاده از طبقه‌بندی داده‌ها به‌صورت خودکار انجام شد، ولی روش‌هایی که از الگوریتم‌های مختلف رمزنگاری مانند کلید نامتقارن عمومی، رمزنگاری RSA و رمزنگاری منحنی بیضوی استفاده می‌کنند درجه بالاتری از محرمانگی و امنیت فراهم می‌کنند.

راه‌حل ارائه شده در مقاله [۱۲] محرمانه بودن اطلاعات ذخیره شده در پایگاه داده‌های ابری که غیرقابل‌اطمینان هستند را تضمین می‌کند. در این مقاله همه داده‌های برون‌سپاری شده برای سرویس‌دهنده‌های ابر از طریق الگوریتم‌های رمزنگاری RSA و AES[۲] رمزنگاری شده‌اند که اجازه اجرای پرس‌وجوهای SQL[۳] استاندارد در داده‌های رمزنگاری شده را می‌دهند. طراحی معماری با استفاده از الگوریتم RSA است که برای داده‌ها بسیار امن است، داده‌های بسیار مهم با استفاده از RSA و داده‌های باقی‌مانده با استفاده از AES رمزنگاری شده‌اند. راه‌حل موجود در این مقاله اجازه می‌دهد تا دسترسی مستقیم، مستقل و هم‌زمان به پایگاه داده ابری مهیا شود و حتی تغییرات ساختار بانک اطلاعاتی را پشتیبانی کند. همچنین متکی به هیچ پروکسی که نشان‌دهنده یک نقطه شکست یا گلوگاه سیستم است، نمی‌باشد. در طرح پیشنهادی این مقاله، امکان خواندن و نوشتن هم‌زمان اطلاعات، که ساختار پایگاه داده‌های رمزنگاری را تغییر می‌دهد، پشتیبانی می‌شود. اما روش رمزنگاری RSA، سربار را افزایش می‌دهد.

در [۱۳] از گواهینامه‌های پویا استفاده شده است. در این روش با توجه به طراحی یا اهمیت جایگاه کاربران در سازمان‌ها برای آن‌ها سلسله مراتبی در سیستم ایجاد می‌شود. با توجه به نقش و جایگاه کاربران، حق دسترسی برای اجرای پرس‌وجو و همچنین کار با سیستم پایگاه داده ایجاد می‌شود. هرزمانی که کاربر پرس‌وجویی را برای دسترسی به سیستم بانک اطلاعاتی اجرا می‌کند، یک گواهینامه دیجیتالی تولید می‌شود. این گواهینامه یک کلید تصادفی سمت کاربر ایجاد می‌کند و فقط درصورتی‌که این کلید با کلید سمت سرویس‌دهنده یکسان باشد کاربر می‌تواند به کار خود ادامه بدهد. اما در این روش ممکن است مجوز حق دسترسی مربوط به کاربری فاش شود یا این‌که حتی کاربر مجاز هم ممکن است از داده‌ها سوء استفاده کند.

در [۱۴]، یک مدل امنیتی پیشنهاد شده است که شامل متدهای امنیت داده بر اساس رمزنگاری، بازیابی اطلاعات خصوصی، توزیع اطلاعات خصوصی و پراکندگی اطلاعات به‌جای رمزنگاری است. مدل پیشنهاد شده ۴ لایه دارد که هرکدام از آن‌ها برای برقراری اطمینان از امنیت داده‌های ابر مربوط به خود است. لایه اول مسئول احراز هویت کاربران است، لایه دوم برای دستیابی به سرویس‌های نرم‌افزاری و فضای ذخیره‌سازی در ابر مورد استفاده قرار می‌گیرد، لایه سوم مدیریت پایگاه داده، سرویسی کارآمد و قابل‌اطمینان را در ابر فراهم می‌کند و لایه چهارم، لایه ذخیره‌سازی است. همچنین برای امنیت بیشتر سه فاز ثبت، ورود و احراز هویت تعریف شده است. در این روش به دلیل این‌که با ارسال پیام رمزشده به سیستم یا کاربر، کلید خصوصی متفاوتی تولید می‌شود، این اطمینان وجود دارد که هنگام جستجوی کلید به‌وسیله یک متجاوز، کلید آشکار نخواهد شد. بااین‌وجود این تکنیک برای کارآمد بودن در زمینه امنیت، نیاز به بهبود بیشتری دارد.

در طرح پیشنهادی مقاله [۱۵] عملیات رمزنگاری از طریق محاسبات جبری و تغییرات نهایی پیکسل‌ها انجام می‌گردد و سپس کلید رمز مطابق با طرح تسهیم راز شامیر به اشتراک گذاشته می‌شود، البته این طرح برای تصاویر در نظر گرفته شده است.

در [۱۶] و [۱۷] به‌جای استفاده از رمزنگاری، طرح خود را بر اساس الگوریتم تسهیم راز شامیر ارائه دادند که معایب مربوط به تسهیم راز شامیر را دارا هستند.

علاوه بر مسائل ذکر شده، ضعف امنیتی و آسیب‌پذیری در لایه‌های مختلف سیستم‌های نرم‌افزاری نیز، منجر به بسیاری حملات امنیتی برعلیه سیستم‌های نرم‌افزاری می‌شود. برای بهبود امنیت مؤلفه‌های مختلف سیستم، باید به شناسایی و رفع آسیب‌پذیری پرداخت. در مقاله [۱۸] طی بررسی‌های انجام‌شده جهت شناسایی آسیب‌پذیری، معیار توسعه‌دهنده‌ای برای فایل‌های آسیب‌پذیر ارائه شده است که این معیار می‌تواند به‌خوبی فایل‌های آسیب‌پذیر را شناسایی کند.

۳- روش پیشنهادی

معمولاً در سیستم‌های رمزنگاری یک کلید یا راز دسترسی به بسیاری از اطلاعات مهم را امکان‌پذیر می‌سازد. بنابراین اگر چنین کلیدی از دست برود، یعنی شخصی که کلید را می‌داند از دسترس خارج شود یا کلید روی کامپیوتری باشد که خراب شده باشد، دسترسی به اطلاعات غیرممکن می‌شود. ازاین‌رو برای حل این مشکل می‌توان از تسهیم راز استفاده کرد. ایده اصلی تسهیم راز، تقسیم کلید یا راز و توزیع هر

بخش از آن به یک شرکت‌کننده مورد اطمینان است. بازیابی کلید نیز از طریق ترکیب سهام مربوطه نزد زیرمجموعه خاصی از شرکت‌کنندگان امکان‌پذیر است.

همان‌طورکه در بخش ۳ بیان شد، اکثر روش‌های قبلی ارائه شده برای حفظ محرمانگی داده‌های برون‌سپاری شده ابری مبتنی بر روش تسهیم راز[۴] شامیر هستند و معایب زیر را دارا هستند. یکی از مهم‌ترین معایب آن‌ها احتمال تقلب اعضا یا حضور دشمن در مرحله بازیابی راز[۵] است. طرح شامیر، می‌تواند توسط هر یک از افراد شرکت‌کننده در مرحله بازیابی راز مورد تهدید قرار گیرد. بنابراین توانایی تحمل تقلب در مرحله بازیابی راز را ندارد[۲۱- ۱۹]. با استفاده از خاصیت کشف و تصحیح خطا در کدهای MDS[۶]، حتی درصورتی‌که تعداد افراد از حد موردنظر بیشتر نباشند این امکان وجود دارد که با انجام تقلب، راز به دست آید[۲۲].

از طرفی می‌توان نشان داد که تسهیم راز شامیر هم‌ارز تسهیم راز آستانه‌ای با استفاده از کد رید- سولومون است[۲۳]. بنابراین، حتی در صورت استفاده از تسهیم راز شامیر، می‌توان از روش کدگشایی رید- سولومون برای بازیابی راز در حضور افراد متقلب استفاده کرد.

از طرف دیگر، با رشد سریع کامپیوترها و در دسترس بودن حافظه‌های کامپیوتری فراوان و به‌طور خاص پدیدار شدن کامپیوترهای کوانتومی، به شکل چشم‌گیری دنیای رمزنگاری تغییر پیدا کرد و الگوریتم‌های کوانتومی فراوانی برای حل مسائل سخت و پیچیده مطرح شد[۲۴]. بنابراین روش تسهیم راز شامیر در برابر حملات کوانتومی آسیب‌پذیر می‌باشند[۲۵].

از الگوریتم‌های کوانتومی برای رمزگذاری و رمزگشایی و به‌خصوص برای شکستن سیستم‌های رمزنگاری استفاده می‌شود. الگوریتم‌های کوانتومی روش‌هایی مانند روش شامیر را به‌راحتی می‌شکنند، بنابراین با توجه به این‌که در آینده‌ای نه‌چندان دور کامپیوترهای کوانتومی به بازار خواهند آمد به روشی نیاز است که نسبت به شامیر خیلی امن‌تر باشند. رمزنگاری مشبّکه [۷] که هنوز هم یک حوزه پژوهشی نوین و بسیار فعال برای طراحی سیستم‌های رمزنگاری است، بسیار کارآمد و تضمین‌کننده امنیت است[۲۶]. تمام نتایج حاصل شده در مورد رمزنگاری مشبّکه از لحاظ تئوری موردتوجه قرار گرفته است. می‌توان گفت رمزنگاری مشبّکه تنها ساختار رمزنگاری شناخته شده‌ای است که از طریق آن برقراری امنیت در بدترین حالت پیچیدگی در محاسبات، قابل‌اثبات است. در عمل اکثر توابع رمزنگاری مشبّکه به‌منظور جلوگیری در مقابل حملات به کار می‌روند[۲۷].

ازآنجایی که تضمین امنیت قوی یکی از ویژگی‌های متمایز رمزنگاری مشبّکه است، در این مقاله نیز طرحی مبتنی بر مشبّکه پیشنهاد خواهد شد که یکی از ویژگی‌های بارز آن فراهم کردن امنیت در برابر حملات کامپیوترهای کوانتومی است. همچنین در طرح پیشنهادی، برای حفظ هر چه بیشتر امنیت اطلاعات، با استفاده از ساختار تسهیم راز به تفکیک اطلاعات و ارتباط بین آن‌ها پرداخته می‌شود. در ادامه به توضیح طرح پیشنهادی پرداخته خواهد شد.

در ضمن برخلاف دیگر روش‌ها، در روش پیشنهادی نیازی به ارسال کل جدول برای n سرویس‌دهنده و به دنبال آن ذخیره و تکرار n بار اطلاعات نیست بلکه در این روش جدول حاوی اطلاعات به n قسمت شکسته و برای هر سرویس‌دهنده فقط تعدادی از ستون‌های رمز شده ارسال می‌شود، بنابراین به میزان قابل‌توجهی حافظه مصرفی کاهش می‌یابد و چون برای هر سرویس‌دهنده فقط چند ستونی که به‌عنوان سهم آن‌ها در نظر گرفته شده، ارسال می‌شود، نسبت به روش‌های دیگری که کل جدول برای هر سرویس‌دهنده فرستاده می‌شود، به پهنای باند کمتری نیاز است.

۳ ـ ۱ ـ معماری روش پیشنهادی

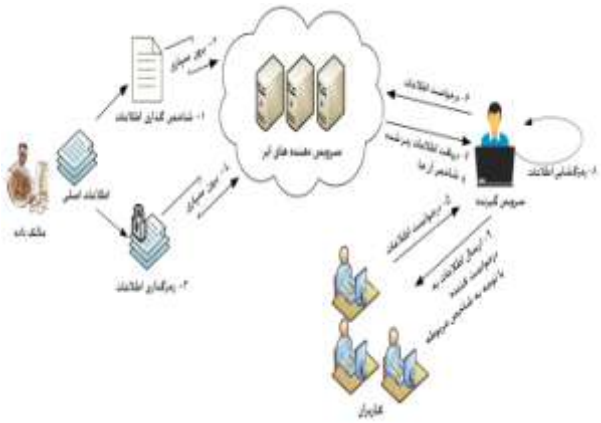
در طرح پیشنهادی ابتدا باید اطلاعات رمزنگاری شوند و سپس برون‌سپاری گردند. در این طرح به دلیل فراهم کردن امنیت بیشتر اطلاعات، از مشبّکه و ضرب ماتریس‌ها استفاده می‌شود. بنابراین در نخستین گام‌ها تمامی اطلاعات رمزنگاری و سپس از طریق یک کانال امن ارتباطی به‌تمامی اعضای شرکت‌کننده ارسال می‌شوند. حال با ارسال پرس‌وجویی از طرف یک کاربر، اطلاعات مربوط به‌تمامی شرکت‌کنندگان بازیابی می‌شود. در این زمان، اطلاعات موردنظر باید رمزگشایی شوند. رمزگشایی نیز بر مبنای مشبّکه انجام می‌شود. رمزگشایی به کمک یک کلید شکل خواهد گرفت. در طرح پیشنهادی، کلید نیز باید برون‌سپاری گردد. کلید به‌اندازه تعداد اعضای شرکت‌کننده یا همان سرویس‌دهنده‌های داده تقسیم می‌شود، هرکدام از اعضا باید یک سهمی[۸] از آن در اختیار داشته باشند. برای رمزگشایی اطلاعات رمز شده، نیاز هست همه اعضا سهم خود را ارسال کنند تا بتوان کلید را به دست آورد. کلید یا همان راز به‌هیچ‌وجه فقط از طریق تعدادی از اعضا، قابل‌دستیابی نیست و در همین راستا اطلاعات قابل رمزگشایی نمی‌باشند. همان‌طورکه بیان شد در طرح پیشنهاد شده هم رمزنگاری و هم رمزگشایی اطلاعات به کمک ضرب ماتریس‌ها انجام می‌شود. به‌منظور یافتن سریع‌تر پاسخ پرس‌وجوی ارسال شده از سمت کاربران، اطلاعات توسط درخت B^+ شاخص‌گذاری می‌شوند. به کمک درخت B^+ مشخص می‌شود که پاسخ پرس‌وجو متعلق به کدام قسمت از اطلاعات است و همان قسمت به کاربر ارسال خواهد شد. قابل ذکر است که رمزنگاری و رمزگشایی از طریق تسهیم راز، نسبت به روش‌های دیگر بسیار کارآمدتر است. شکل ۱ چشم‌اندازی از نمای کلی معماری طرح پیشنهادی را نشان می‌دهد.

همان‌گونه که در شکل ۱ نشان داده شده است موجودیت‌های به کار گرفته شده در طرح پیشنهادی به شرح زیر هستند:

- مالک داده[۹]: اطلاعات اصلی را رمزگذاری و شاخص‌گذاری می‌کند و آن‌ها را به ترتیب به سرویس‌دهنده داده و سرویس‌دهنده شاخص ارسال می‌کند.

- سرویس‌گیرنده[۱۰]: پرس‌وجوها را از کاربران دریافت می‌کنند و برای ارسال پاسخ به آن‌ها، اطلاعات رمز شده را از سرویس‌دهنده‌های داده دریافت و آن‌ها را رمزگشایی می‌کنند، سپس به کمک سرویس‌دهنده شاخص پاسخ مربوط به پرس‌وجوی کاربران را برای آن‌ها ارسال می‌کند.
- کاربران[۱۱]: درخواست‌کنندگان اطلاعات از ابر می‌باشند.
- سرویس‌دهنده داده[۱۲]: سرویس‌دهنده‌ای که اطلاعات رمزشده و کلید در آن ذخیره می‌شود.
- سرویس‌دهنده شاخص[۱۳]: مسئول نگهداری اطلاعات شاخص‌گذاری شده است. این سرویس‌دهنده تعیین می‌کند که مقدار شرط پرس‌وجو مربوط به کدام سطر یا ستون ماتریس است.

علائم و نمادهایی که در طرح پیشنهادی مورد استفاده قرار گرفته است، به‌طور خلاصه در جدول ۱ آورده شده است.



شکل ۱: نمای کلی معماری طرح پیشنهادی

جدول ۱: علائم و نمادهای استفاده شده در طرح پیشنهادی

$wt(x)$	تابع مربوط به وزن همینگ رشته x با مختصات غیرتهی
$t_j^{(i)}$	iامین عنصر بردار j
λ	ماتریسی متشکل از بردارهای ستونی $\lambda_1 \lambda_2$ ... و λ_n با مقادیری بر اساس وزن همینگ[۱۴]
B	ماتریسی شامل مقادیر اصلی اطلاعات
C	ماتریس مقادیر رمزنگاری شده
e	ماتریس واحد شامل بردارهای ستونی و همانی e_1 تا e_n
e_i	iامین بردار ستونی همانی ماتریس e
v_i	iامین شرکت‌کننده برای دریافت سهم
a	ماتریس کلید یا راز (مورد استفاده در زمان بازیابی مقادیر اصلی)
b_i	iامین ستون ماتریس B
c_i	iامین ستون ماتریس C
DS_i	iامین سرویس‌دهنده داده

۲ ۳ مفروضات روش پیشنهادی

اولین و مهم‌ترین نیاز در برون‌سپاری امن داده، حفظ محرمانگی داده‌های برون‌سپاری شده نزد سرویس‌دهنده بیرونی است. روش ارائه شده برای حفظ محرمانگی و امنیت اطلاعات باید در برابر حملات آماری مبتنی بر تکرار مقاوم باشد، زیرا مهاجم ممکن است از اطلاعات برای افزایش آگاهی خود در مورد داده‌ها استفاده کند.

بر این اساس، معمولاً طرح پیشنهادی این پژوهش و همچنین همه طرح‌های تسهیم‌رازی که محرمانگی داده را مد نظر قرار می‌دهند، فرضیاتی به شرح زیر خواهند داشت:

سرویس‌دهنده‌های داده درست‌کار ولی کنجکاو هستند، یعنی به‌درستی پرس‌وجوهای دریافتی را روی داده‌های برون‌سپاری شده اجرا و پاسخ صحیح را برای سرویس‌گیرنده ارسال می‌کنند. بااین‌وجود فرض می‌شود که سرویس‌دهنده‌ها تلاش می‌کنند تا اطلاعات خود را در مورد داده‌های برون‌سپاری شده افزایش دهند.

سرویس‌دهنده‌های داده ممکن است از قبل در مورد داده‌های برون‌سپاری شده آگاه داشته باشند. فرض می‌شود سرویس‌دهنده‌ها در مورد الگوی پرس‌وجوهای وارد شده چیزی نمی‌دانند.اگر مهاجمی کنترل سرویس‌دهنده را در اختیار بگیرد ممکن است توانایی‌اش در حد سرویس‌دهنده باشد.همچنین فرض می‌شود سرویس‌گیرنده‌ها که ماشین واسطی هستند و کاربران پرس‌وجوی خود را از طریق آن‌ها به سیستم ارسال می‌کنند، مورد اعتماد هستند و اطلاعات محرمانه را برای موجودیت‌های غیرقابل‌اعتماد از جمله سرویس‌دهنده‌ها افشا نمی‌کنند. در ضمن تصور می‌شود که کاربران دارای اعتبارات یکسانی برای دسترسی به داده‌ها هستند و با ارسال پرس‌وجو از طریق یک سرویس‌گیرنده می‌توانند اطلاعات موردنظرشان را بازیابی کنند.

در قسمت ذیل نیز تعاریفی در مورد تسهیم راز و امنیت آن آورده شده است:

تعریف-۱. یک طرح تسهیم راز روشی برای به اشتراک‌گذاری یک راز x بین مجموعه‌ای از اعضای $v = \{v_1, v_2, \dots, v_n\}$ است، به‌طوری‌که تنها زیرمجموعه مجاز از اعضا بتواند راز x را بازیابی کنند[۲۸].

تعریف-۲. یک طرح تسهیم راز برای برون‌سپاری داده به شرطی امن است که رابطه‌ای بین مقادیر اصلی و سهم‌های متناظر با آن‌ها برای سرویس‌دهنده درست‌کار ولی کنجکاو مشاهده نشود[۹].

تعریف-۳. یک طرح تسهیم راز برای برون‌سپاری داده امن است اگر با احتمال این‌که مهاجمی که یک سهم داده را در اختیار داشته باشد، یافتن مقدار راز متناظر با آن سهم از میان مجموعه رازهای ممکن برای او امکان‌پذیر نباشد[۲۹].

ازآنجایی‌که روش پیشنهاد شده در این مقاله بر مبنای سیستم رمزنگاری مشبّکه ارائه شده است، نسبت به روش‌های دیگر به‌خصوص روش [۹] که بر مبنای تسهیم راز شامیر است، امن‌تر است. همان‌طورکه قبلاً نیز بیان شد، هرچند روش شامیر از نظر تسهیم راز

امنیت بالایی فراهم می‌کند اما این روش و روش‌هایی که مبتنی بر آن ارائه شده‌اند، توسط الگوریتم‌های کوانتومی شکسته می‌شوند[۲۵].
رمزنگاری مشبّکه یکی از مطمئن‌ترین روش‌های شناخته شده برای حفظ امنیت اطلاعات و جلوگیری از حملات کوانتومی است. امنیت روش پیشنهادی بر مبنای امنیت رمزنگاری مشبّکه است که امنیت آن در مرجع[۲۷] اثبات شده است. بنابراین روش پیشنهادی این مقاله امنیت در مقابل حملات کوانتومی را فراهم می‌کند.

۳ ۳ -شرح روش پیشنهادی

در روش پیشنهادی ماتریسی به نام B در نظر گرفته می‌شود که تمامی مقادیر اصلی اطلاعات در آن قرار داده می‌شود. ازآنجایی‌که مهم‌ترین هدف طرح پیشنهادی در این پژوهش و به‌طورکلی در همه طرح‌های برون‌سپاری داده‌ها، حفظ امنیت اطلاعات است و درهرصورت این امکان وجود دارد که هنگام برون‌سپاری، امنیت اطلاعات به خطر بیفتد، بنابراین باید اطلاعات را قبل از برون‌سپاری و توزیع بین شرکت‌کنندگان رمزنگاری کرد. در طرح پیشنهاد شده برای توزیع اطلاعات از روش تسهیم راز آستانه‌ای (n, n) استفاده می‌شود[۳۰]. بنابراین برای بازیابی اطلاعات باید تمامی n شرکت‌کننده حضور داشته باشند که این خاصیت مربوط به مشبّکه بودن طرح است. در ضمن ماتریس دیگری به نام a به‌عنوان کلید یا راز در نظر گرفته می‌شود، کلید نیز همچون مقادیر رمز شده باید بین تمامی شرکت‌کنندگان توزیع شود. هنگام رمزگشایی اطلاعات به بازیابی کلید و همچنین اطلاعات رمز شده نیاز است. عملیات مربوط به طرح پیشنهادی طی فازهایی انجام می‌گیرد. توضیح فازها در بخش بعدی آمده است.

۳ ۳ ۱ -فازهای روش پیشنهادی

طرح پیشنهاد شده در این پژوهش شامل سه فاز رمزگذاری[۱۵]، فاز تفکیک[۱۶] و توزیع[۱۷] داده‌های رمز شده و در نهایت فاز بازیابی[۱۸] راز است، این فازها باید به ترتیب یکی پس از دیگری انجام شود تا عملکرد طرح پیشنهادی به‌خوبی میسر گردد، فازها به‌صورت زیر تشریح می‌شوند:

۳-۳-۱-۱- فاز رمزگذاری

در این فاز ماتریسی با نام دلخواه λ در نظر گرفته می‌شود، مقادیر این ماتریس شامل صفر و یک است که مقادیر آن بر اساس وزن همینگ و با استفاده از تابع $wt(x)$ تعیین می‌شود. مقادیر اصلی اطلاعات به کمک معادله $C = \lambda.B$ رمزنگاری می‌شوند. بنابراین C یک ماتریس شامل مقادیر رمز شده است. درواقع مالک داده هر ستونی از این ماتریس را به‌صورت $C_i = \lambda.B_i$ محاسبه می‌کند، در نهایت ترکیب تمامی ستون‌ها ماتریس C را تشکیل می‌دهد.

۳-۳-۱-۲- فاز تفکیک داده‌های رمز شده و توزیع آن‌ها

اکنون باید تمامی داده‌های رمز شده به همه شرکت‌کنندگان یعنی $v = \{v_1, v_2, \dots, v_n\}$ ارسال شوند. چنانچه همه ستون‌های ماتریس C که شامل داده‌های رمز شده هستند، برای همه سرویس‌دهنده‌های داده ارسال شود، حجم اطلاعاتی که هر سرویس‌دهنده داده نگه می‌دارد بسیار زیاد می‌شود، بنابراین می‌توان تعداد کل ستون‌ها را به‌اندازه تعداد سرویس‌دهنده‌های داده تقسیم کرد و هر قسمت را به‌عنوان یک سهم به هر سرویس‌دهنده داده ارسال کرد. به‌طورکلی هر سهم یک یا تعدادی بردار ستونی از مقادیر رمز شده است. در این فاز مالک داده تفکیک و توزیع اطلاعات رمزنگاری شده را انجام می‌دهد. با انجام این مراحل کار توزیع و برون‌سپاری اطلاعات به پایان می‌رسد.

۳-۳-۱-۳- فاز بازیابی راز و رمزگشایی مقادیر رمز شده

برای بازیابی اطلاعات یک ماتریسی به نام a به‌عنوان کلید یا راز در نظر گرفته می‌شود، ماتریس a بین مجموعه اعضای $v = \{v_1, v_2, \dots, v_n\}$ به اشتراک گذاشته می‌شود، هر قسمتی از کلید باید در اختیار یک شرکت‌کننده یا همان سرویس‌دهنده داده قرار گیرد، یعنی تمامی اعضا سهمی از راز خواهند داشت. برای بازیابی، تمامی سهم‌ها موردنیاز هستند به‌طوری‌که با در دسترس نبودن یکی از شرکت‌کنندگان کلید غیرقابل دسترس می‌شود.

ماتریس a توسط مالک داده به دست می‌آید، مقادیر ماتریس a باید طوری در نظر گرفته شود که حاصل‌ضرب ماتریس λ در ماتریس a برابر با ماتریس همانی e شود. e_i به‌عنوان iامین ستون ماتریس همانی e است، این ماتریس یک بردار n بعدی واحد است. با جایگذاری e_i و λ در معادله (۱) مقادیر ماتریس a به دست می‌آید.

$$e_i = \left[\lambda_{k_1}, \dots, \lambda_{k_n}\right].\left[a^i_{k_1}, \dots, a^i_{k_n}\right] \quad 1 \le i \le n \qquad (۱)$$

پس از محاسبه ماتریس a، این ماتریس نیز مانند ماتریس C به تعداد سرویس‌دهنده‌های داده تقسیم شده و هر قسمت یا سهم می‌بایستی از طریق یک کانال امن ارتباطی به هر سرویس‌دهنده داده ارسال شود. حال با ارسال پرس‌وجو از طرف یک کاربر مجاز، به کمک معادله (۲) مقادیر ماتریس B یا همان اطلاعات اصلی، بازیابی می‌شود.

$$B = \left[a_{k_1}, \dots, a_{k_n}\right].\left[c_{k_1}, \dots, c_{k_n}\right] \qquad (۲)$$

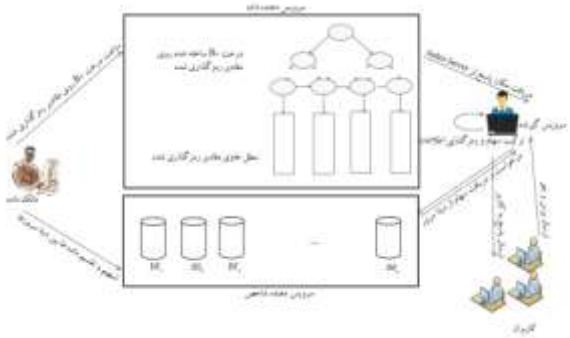
برای بازیابی هرکدام از مقادیر اصلی اطلاعات، باید همه شرکت‌کنندگان سهم خود را به موجودیتی به نام ترکیب‌کننده ارسال کنند. در اینجا سرویس‌گیرنده‌ای که کاربر پرس‌وجوی خود را به او ارسال کرده است و در حقیقت واسط بین کاربر و سرویس‌دهنده داده است، که نقش ترکیب‌کننده را ایفا می‌کند. وظیفه ترکیب‌کننده، دریافت تمامی سهام از تمامی سرویس‌دهنده‌های داده و ترکیب آن‌هاست. ترکیب‌کننده باید سهام مربوط به ماتریس C را با هم ترکیب

کند تا ماتریس C حاصل شود. به‌طور مشابه با دریافت سهام مربوط به ماتریس a، این ماتریس نیز به دست می‌آید.

پس از بازیابی و رمزگشایی اطلاعات، با استفاده از ساختار شاخص‌گذاری[19] درختB^+ روی صفات قابل جستجو، مکان اطلاعات درخواست شده، به‌عنوان نتیجه پرس‌وجو مشخص می‌شود و در نهایت اطلاعات مربوط به مکان به‌دست‌آمده توسط درختB^+ به کاربر موردنظر ارسال می‌گردد. اطلاعات شاخص‌گذاری شده و همچنین درختB^+ در سرویس‌دهنده‌ای به نام سرویس‌دهنده شاخص قرار دارند.

۳ ۴ -وظایف و روابط بین موجودیت‌های معماری طرح پیشنهادی

روش پیشنهادی با انجام کارهایی که بر عهده موجودیت‌های مطرح شده در معماری پیشنهادی می‌باشند به نتیجه می‌رسد. برای موفقیت‌آمیز بودن روش پیشنهادی باید موجودیت‌ها با هم در ارتباط باشند و هرکدام از آن‌ها بر اساس نیاز موجودیت دیگر، وظایف مربوط به خود را انجام بدهند تا مراحل مربوط به روش پیشنهادی طی شود. شکل ۲ دیاگرام عملکرد طرح پیشنهادی و ارتباطات بین موجودیت‌ها را نشان می‌دهد.



شکل ۲: روابط بین موجودیت‌ها

با توجه به شکل، جزئیات وظایف و روابط بین موجودیت‌ها به شرح زیر است:

- مالک داده: مالک داده با استفاده از معادله $C = \lambda.B$ مقادیر اصلی را رمزگذاری می‌کند. سپس تعداد ستون‌های ماتریس C را به تعداد سرویس‌دهنده‌های داده تقسیم و هر قسمت را برای یک سرویس‌دهنده داده ارسال می‌کند. برای مقادیر رمز شده ستون‌هایی که قرار است در شرط پرس‌وجو استفاده شوند، یک درختB^+ ساخته می‌شود که هر برگ آن به یک سطل حاوی مقادیر نگه داشته شده در سرویس‌دهنده‌های داده اشاره دارد. درواقع مالک داده از طریق درختB^+ اطلاعات را شاخص‌گذاری می‌کند. همچنین مقدار راز را محاسبه می‌کند و پس از سهم‌بندی راز، سهام مربوط به سرویس‌دهنده‌های داده را برای آن‌ها ارسال می‌کند.
- سرویس‌دهنده شاخص: این سرویس‌دهنده سطل مربوط به مقدار شرط پرس‌وجو را از طریق درختB^+ پیدا می‌کند و آن را برای سرویس‌گیرنده ارسال می‌کند. یعنی مشخص می‌کند که مقدار شرط پرس‌وجو مربوط به کدام سطر یا ستون ماتریس است. مسئولیت هر جستجو بر عهده درختB^+ است.
- سرویس‌دهنده داده: مسئولیت نگهداری اطلاعات رمز شده را بر عهده دارد. همچنین سهام مربوط به راز در اختیار سرویس‌دهنده داده قرار می‌گیرد. در نهایت هنگام رمزگشایی و بازیابی اطلاعات، هر سرویس‌دهنده داده سهام مربوط به خود را به سرویس‌گیرنده ارسال می‌کند.
- سرویس‌گیرنده: سرویس‌گیرنده تقریباً با بیشتر موجودیت‌های طرح پیشنهادی در ارتباط است. سرویس‌گیرنده پرس‌وجویی را از کاربر دریافت می‌کند، سپس تمامی سهام، چه سهام مربوط به اطلاعات و چه سهام مربوط به کلید را از همه سرویس‌دهنده‌های داده درخواست می‌کند، پس از دریافت سهام، آن‌ها را با هم ترکیب می‌کند و بعد از آن اطلاعات را رمزگشایی می‌کند، همچنین از سرویس‌دهنده شاخص مکان مربوط به پاسخ پرس‌وجو را درخواست می‌کند و اطلاعات مربوط به همان مکان را برای کاربر ارسال می‌کند.

۴ -ارزیابی روش پیشنهادی

به علت وجود برخی مشکلات در روش‌های پیشین، در بخش ۳ روشی برای برقراری هر چه بهتر امنیت بر مبنای تسهیم راز و با استفاده از مشبّکه ارائه گردید. در این بخش نیز ابتدا به توضیح مختصری در مورد امنیت حاصل از رویکرد پیشنهادی پرداخته خواهد شد و سپس ارزیابی روش پیشنهادی با چند روش ذکر شده مورد بررسی قرار می‌گیرد.

۴-۱ بازدهی[20]

در این مقاله به‌منظور بررسی نتایج پیاده‌سازی، از نرم‌افزار Oracle 11g به‌عنوان سرویس‌دهنده‌ای برای میزبانی داده‌ها استفاده شده است. نرم‌افزار مدیریت پایگاه داده روی یک سیستم عامل ویندوز ۱۰ با پردازنده‌ای ۱/۸ گیگاهرتزی و مدل corei5 و حافظه اصلی با ظرفیت ۴ گیگابایت نصب شده است. برنامه‌نویسی مربوط به شبیه‌سازی نیز با زبان جاوا و نسخه JDK8 انجام شده است. در ضمن عملیات شبیه‌سازی روی مجموعه داده‌های واقعی که حدود یک میلیون رکورد در یک جدول پایگاه داده هستند اجرا شده است.

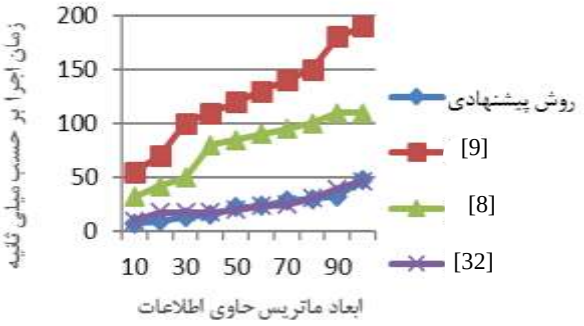
همچنین یک نرم‌افزار طراحی و در سمت سرویس‌گیرنده نصب شده است تا کار ترجمه و بازسازی نهایی نتایج پرس‌وجوها را انجام دهد. سرویس‌گیرنده از طریق یک شبکه محلی به سرویس‌دهنده‌های

میزبان داده که در آن‌ها سهم‌های ارسال شده یا درواقع داده‌های رمز شده ذخیره شده‌اند، متصل می‌شود.

ممکن است ابرها به‌صورت سیار باشند، در ابرهای سیار، قدرت محاسباتی دستگاه‌های سیار با واگذاری بخش‌هایی از نرم‌افزار به ابر، افزایش می‌یابد. هدف از تخصیص وظایف در واگذاری یک نرم‌افزار، کمینه‌سازی دو معیار زمان کل اجرا و انرژی مصرفی و همچنین تأمین کیفیت سرویس موردنظر برنامه کاربردی می‌باشد که در مقاله [۳۱] به این موضوع پرداخته شده است.

در این بخش، نتیجه پیاده‌سازی و ارزیابی روش پیشنهادی در محیط عملیاتی شبیه‌سازی شده، گزارش شده است. برای اطمینان از صحت طرح پیشنهادی، اجرای برنامه مربوطه بیش از ۱۰ بار تکرار گردید. شکل ۳ نتایج حاصل از اجرای برنامه را نشان می‌دهد.

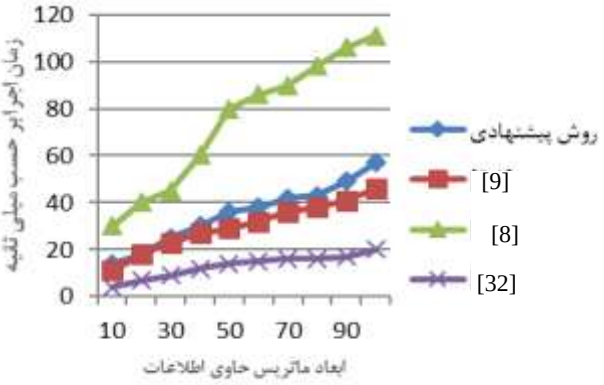
با بالا رفتن ابعاد ماتریس(جدول پایگاه داده)، زمان اجرای عملیات نیز افزایش پیدا می‌کند که تقریباً در همه روش‌ها با افزایش حجم اطلاعات زمان اجرای عملیات نیز افزایش می‌یابد. ولی درواقع رویکرد طرح پیشنهادی برای مقایسه با چند طرح [۸]، [۹] و [۳۲] بیان شده در بخش ۳ پیاده‌سازی شده است. عملیات اصلی روش پیشنهاد شده و هر روش دیگری که از شیوه رمزنگاری استفاده می‌کند، شامل مراحل رمزگذاری و رمزگشایی است، بنابراین زمان اجرای این دو عملیات در روش‌های مختلف با روش پیشنهاد شده مقایسه می‌شود. شکل ۴ نموداری حاصل از مقایسه زمان اجرای عملیات رمزکردن در روش‌های موردنظر است. هرچند این شکل نشان می‌دهد که روش پیشنهاد شده در این مقاله تقریباً زمان اجرای کمتری نسبت به بقیه روش‌ها دارد، اما توضیحات آورده شده در ادامه، کارآیی این روش را بهتر نشان می‌دهد.



شکل ۴: مقایسه روش پیشنهادی با سه روش دیگر در مرحله رمزنگاری

با توجه به پاسخ‌های به‌دست‌آمده پس از چندین بار تکرار اجرای برنامه درستی مقادیر در روش پیشنهادی تأیید می‌شود. پژوهش [۹] که مربوط به هادوی و همکاران است بیشترین زمان اجرا را دارد، البته نویسندگان این مقاله این مسئله را قبول دارند ولی به دلیل امنیتی که روش آن‌ها ایجاد می‌کند زمان اجرای بالای آن را نیز پذیرفته‌اند. روش پیشنهاد شده در این مقاله، هم‌زمان اجرای کمتری دارد و هم امنیت لازم را برقرار می‌کند. روش [۸] نیز پس از [۹] بیشترین زمان اجرا را دارد. روش [۳۲] زمان اجرای کمتری نسبت به روش‌های [۸] و [۹] دارد و زمان اجرای آن تقریباً برابر با طرح پیشنهادی است ولی عیب آن این است که از اجرای پرس‌وجوهای مختلف پشتیبانی نمی‌کند.

شکل ۵ نتیجه مقایسه مرحله رمزگشایی روش‌های ذکر شده با روش پیشنهادی را نشان می‌دهد. با توجه به شکل، روش مطرح شده در مقاله [۸] بیشترین زمان اجرا را در مرحله رمزگشایی به خود اختصاص می‌دهد و روش مقاله [۳۲] کمترین زمان اجرا را دارد ولی چنانچه قبلاً نیز گفته شد، در این روش امکان اجرای پرس‌وجوهای مختلف وجود ندارد. زمان اجرای روش پیشنهادی این مقاله کمی بیشتر از روش [۹] است، ولی همان‌طورکه در مرحله رمزگذاری نیز اشاره شد این روش بر مبنای تسهیم راز شامیر ارائه شده است و همین مسئله بیان‌گر مقاوم نبودنش در مقابل حملات کوانتومی می‌شود. بنابراین ارزیابی روش پیشنهادی با دیگر روش‌ها در مرحله رمزگشایی نیز نتیجه قابل قبولی را نشان می‌دهد.



شکل ۵: مقایسه روش پیشنهادی با سه روش دیگر در مرحله رمزگشایی

۵ -نتیجه‌گیری و کارهای آتی

در این مقاله یک روش پیشنهادی به‌منظور افزایش سطح امنیت اطلاعات پایگاه داده‌های ابری با استفاده از ساختار تسهیم راز و به‌کارگیری مشبّکه ارائه شد. در روش پیشنهادی ابتدا اطلاعات رمز شده و سپس با استفاده از تسهیم راز تقسیم‌بندی شده و پس از آن به سرویس‌دهنده‌های بیرونی ارسال شدند. ایده تسهیم راز برای تفکیک اطلاعات و ایجاد امنیت بیشتر برای آن‌ها می‌باشد. با توجه به مقاومت رمزنگاری مبتنی بر مشبّکه در مقابل حملات کوانتومی و امنیت آن، به‌کارگیری آن در جهت افزایش بیشتر امنیت اطلاعات تأثیری مثبت داشت. در نهایت طرح پیشنهادی شبیه‌سازی و پیاده‌سازی گردید. با ارزیابی نتایج به‌دست‌آمده مشخص شد که روش پیشنهادی علاوه بر فراهم آوردن حفظ محرمانگی داده‌های برون‌سپاری شده، زمان اجرای کمتری نسبت به بقیه روش‌های مقایسه شده دارد. همچنین به دلیل این‌که در روش پیشنهادی مسئله تکرار داده‌های ارسالی برای سرویس‌دهنده‌ها وجود ندارد و کل اطلاعات جدول برای هر سرویس‌دهنده ارسال نمی‌شود، حافظه مصرفی و در راستای آن پهنای

باند کمتری برای ارسال اطلاعات به سرویس‌دهندگان، استفاده می‌شود. در بیشتر روش‌های موجود در زمینه کنترل دسترسی، حداقل قابلیت دسترسی یعنی امکان خواندن اطلاعات در نظر گرفته شده است. بنابراین یکی از مسائلی که در آینده می‌توان آن را مورد بررسی قرار داد، تعیین خط‌مشی‌های کنترل دسترسی پیچیده‌تر برای بهبود عملیات مربوط به پایگاه داده ابری و به‌طورکلی همه پایگاه داده‌ها است. بنابراین باید به مسئله حق دسترسی عملیات نوشتن برای پایگاه داده‌هایی که دارای چندین مالک می‌باشند توجه شود. از ایده‌های دیگر برای آینده استفاده از روش تسهیم راز مبتنی بر مشبّکه است که آستانه‌اش (n,t) باشد.

پیوست

مثال عددی برای اثبات درستی روش پیشنهادی

در این بخش مراحل انجام فازهای طرح پیشنهادی و عملکرد موجودیت‌ها با یک مثال بیان خواهد شد. اگر ماتریس B مقادیر زیر را داشته باشد و $wt(x)=3$ در نظر گرفته شود، یعنی مقادیر ماتریس λ به شکل زیر باشد، آنگاه مالک داده می‌تواند با استفاده از فرمول $c_i=\lambda.b_i$ مقادیر ماتریس C که همان مقادیر رمز شده هستند را به دست آورد.

$$\lambda=\begin{bmatrix}1&0&1&1\\1&1&0&1\\1&1&1&0\\0&1&1&1\end{bmatrix}\quad B=\begin{bmatrix}7&9&8&4\\6&3&3&0\\5&9&0&5\\4&4&2&3\end{bmatrix},$$

$$c_1=\lambda.b_1=\begin{bmatrix}16\\17\\18\\15\end{bmatrix},$$

$$c_2=\lambda.b_2=\begin{bmatrix}22\\16\\21\\16\end{bmatrix},$$

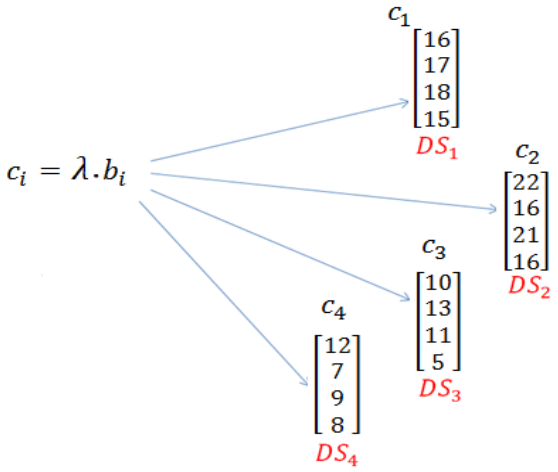
$$c_3=\lambda.b_3=\begin{bmatrix}10\\13\\11\\5\end{bmatrix},$$

$$c_4=\lambda.b_4=\begin{bmatrix}12\\7\\9\\8\end{bmatrix}$$

به‌این‌ترتیب اطلاعات رمزنگاری می‌شوند. ماتریس C شامل بردارهای ستونی به‌دست‌آمده در بالا است که از ترکیب آن‌ها ماتریس زیر حاصل می‌شود.

$$C=\begin{bmatrix}16&22&10&12\\17&16&13&7\\18&21&11&9\\15&16&5&8\end{bmatrix}$$

اکنون زمان توزیع مقادیر اصلی است، همان‌طورکه پیش از این شرح داده شد به دلیل کاهش حجم اطلاعات برای هر سرویس‌دهنده داده، محتویات ماتریسی که حاوی اطلاعات رمز شده است، بین سرویس‌دهنده‌های داده تقسیم می‌شود. بنابراین طبق آن‌چه پیش از این گفته شد باید تعداد کل ستون‌ها بین تعداد سرویس‌دهنده‌های داده تقسیم شود، با توجه به تعداد ستون‌های مربوط به مقادیر در مثال و فرض این‌که تعداد سرویس‌دهنده‌های داده ۴ تا باشند، هر ستون به یک سرویس‌دهنده داده ارسال می‌گردد. شکل ۶ توزیع سهام بین سرویس‌دهنده‌های داده را نشان می‌دهد. همان‌طورکه قابل‌مشاهده است هر ستون به یک سرویس‌دهنده داده ارسال شده است.



شکل ۶: توزیع سهام بین سرویس‌دهنده‌های داده

حال نوبت به حساب کردن ماتریس a می‌رسد، همان‌طورکه قبلاً گفته شد ماتریس a برای رمزگشایی مقادیر، موردنیاز است. با داشتن مقادیر ماتریس λ و با توجه به همانی بودن ماتریس e و جایگذاری این دو ماتریس در معادله $e=\lambda.a$، ماتریس a قابل‌محاسبه است.

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}=\begin{bmatrix}1&0&1&1\\1&1&0&1\\1&1&1&0\\0&1&1&1\end{bmatrix}.a$$

سرانجام با محاسبات ریاضی مربوط به ماتریس‌ها، ماتریس a با مقادیر زیر حاصل می‌شود.

$$a=\begin{bmatrix}\frac{1}{3}&\frac{1}{3}&\frac{1}{3}&\frac{-2}{3}\\\frac{-2}{3}&\frac{1}{3}&\frac{1}{3}&\frac{1}{3}\\\frac{1}{3}&\frac{-2}{3}&\frac{1}{3}&\frac{1}{3}\\\frac{1}{3}&\frac{1}{3}&\frac{-2}{3}&\frac{1}{3}\end{bmatrix}$$

در طرح پیشنهادی این پژوهش، ماتریس a به‌عنوان کلید یا همان راز در نظر گرفته می‌شود، این ماتریس نیز همانند ماتریس C باید به تعداد سرویس‌دهنده‌های داده تقسیم و هر سهمی از آن به یک

سرویس‌دهنده داده ارسال شود، البته ماتریس a به دلیل حفظ امنیت، سهم‌بندی می‌شود، درصورتی‌که سهم‌بندی ماتریس C به دلیل کاهش حجم اطلاعات موجود در سرویس‌دهنده‌های داده است.

با ارسال یک پرس‌وجو از سمت کاربر ابتدا باید سهام مربوط به مقادیر رمز شده از سمت سرویس‌دهنده‌های داده بازگردانده شوند، ترکیب‌کننده سهام را با هم ترکیب می‌کند تا ماتریس C به دست آید. سپس سهام مربوط به راز یعنی ماتریس a بازیابی و ترکیب می‌شوند. با جایگذاری مقادیر این دو ماتریس در معادله $B = a.C$، اطلاعات اصلی یا درواقع مقادیر ماتریس B به دست می‌آید.

$$B = \begin{bmatrix} \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & \frac{-2}{3} \\ \frac{-2}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{-2}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{-2}{3} & \frac{1}{3} \end{bmatrix} \cdot \begin{bmatrix} 16 & 22 & 10 & 12 \\ 17 & 16 & 13 & 7 \\ 18 & 21 & 11 & 9 \\ 15 & 16 & 5 & 8 \end{bmatrix} = \begin{bmatrix} 7 & 9 & 8 & 4 \\ 6 & 3 & 3 & 0 \\ 5 & 9 & 0 & 5 \\ 4 & 4 & 2 & 3 \end{bmatrix}$$

اکنون با توجه به مکانی که درخت B^+ تعیین می‌کند، مقادیر مربوط به نتیجه پرس‌وجو به کاربر ارسال می‌گردد. همان‌طورکه مشاهده شد اطلاعات با به‌کارگیری روش مشبّکه و ضرب ماتریس‌ها رمزگذاری و سپس رمزگشایی شدند.

مراجع

[1] P. Mell and T. Grance, "Effectively and Securely Using the Cloud Computing Paradigm," NIST, Information Technology Laboratory, pp. 304-311, 2009.

[2] G. Rossman, L. McMillan, E. White, Y. Deniz, B. Gourley, "Survey finds database in the cloud taking over in enterprises," OCTOBER 29, 2015, http://openstackdbaas.ulitzer.com/node/3523973, 2015.

[3] B. Furht and A. Escalante, "Handbook of cloud Computing," Springer Publishing Company, Incorporated, 2010.

[4] J. Kendrick, "The rapidly accelerating cloud-enabled enterprise," [Online]. Available:http://www.oracle.com/us/products/database/2015.-ioug-survey-db-manageability-2542988.pdf, 2015.

[5] B. Chor, S. Goldwasser, S. Micali and B. Awerbuch, "Verifiable secret sharing and achieving simultaneity in the presence of faults," In Proceedings of the 26th IEEE Symposium on the Foundations of Computer Science, pp. 383-395, 1985.

[6] M.A. Hadavi, M. Noferesti, R. Jalili, and E. Damiani, "Database as a Service: Towards a Unified Solution for Security Requirements," IEEE 36th International Conference on Computer Software and Applications Workshops (COMPSACW), 2012.

[7] D. Agrawal, A. E. Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities," In IEEE 25th International Conference on Data Engineering, pp. 1709–1716, 2009.

[8] H. Hacigumu, B. Iyer, C. Li and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," SIGMOD '02, USA, pp. 216–227, June, 2002.

[9] M. A. Hadavi and R. Jalili, "Secure Data Outsourcing Based on Threshold Secret Sharing: Towards a More Practical Solution," in Proc. VLDB PhD Workshop. Singapore, pp. 54-59, 2010.

[10] Y. Yu, L. Jussipekka and P. Benjamin, "A Study on the Security of Privacy Homomorphism," International Journal of Network Security, In Information Technology: New Generations, Vol.6, No.1, pp. 33–39, IEEE, 2006.

[11] L. Tawalbeh, S. Nour, R. Al-Qassas and F. AlDosari, "A Secure Cloud Computing Model based on Data Classification," In Procedia Computer Science pp. 1153–1158, 2015.

[12] A. Jayadar and R. Arunachalam, "Secure Cloud DBaaS by Client and Server side Encryption, " In International Journal of Science and Research, 2319-7064, 2013.

[13] M. Singh and M. Alka, "A Dynamic Approach For Data Base Security," International Journal of Computer Science and Mobile Computing, Vol. 3, Issue. 5, pp. 1247–1253, 2014.

[14] K. Munir, "Security Model for Cloud Database as a Service (DBaaS)," Cloud Technologies and Applications (CloudTech), International Conference on. IEEE, 7336974, 2015.

[15] A.K. Chattopadhyay, A. Nag and K. Majumder, "Secure Data Outsourcing on Cloud Using Secret Sharing Scheme," International Journal of Network Security, Vol.19, No.6, PP.912-921,2017.

[16] D. Agrawal, K. S. Candan and W. S. Li, "Information and Software as Services," LNBIP, Springer, Heidelberg, Vol. 74, pp. 57–80, 2011.

[17] X. Tian, C. Sha, X. Wang and A. Zhou, "Privacy Preserving Query Processing on Secret Share Based Data Storage," In. DASFAA 2011. Part I. LNCS, Vol. 6587, pp. 108–122, Springer, Heidelberg, 2011.

[۱۸] جمیله شفیعی و اشکان سامی، «بهبود امنیت با استفاده از معیارهای استخراج شده از مخازن نرم افزاری- معیار فعالیت توسعه‌دهنده»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۵، شماره ۳، پاییز ۱۳۹۴.

[19] R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-SolomonCodes Comm -of ACM," Yol.24, No.9, pp. 83–84, 1981.

[20] K. Okada and K. Kurosawa, "MDS secret sharing scheme secure against cheaters," IEEE Trans, on Information Theory, I T-46, pp. l078-1081, 2000.

[21] J. Pieprzyk and X. Zhang, "Ideal ThresholdS chemesfr orn MDS Codes," pp. 253–2632, 2003.

[22] A. Behnad and T. Euclid, "Sharing the secret fingerprint tolerant of fraud with the help of decoding the list," Fifteenth of Iran's Electrical Engineering Conference, 2007.

[23] S. Mahajan and G. Singh, "Reed-Solomon Code Performance for M-ary Modulation over AWGN Channel," International Journal of Engineering Science and Technology (IJEST), Vol. 3, No. 5, May, 2011.

[24] N. Stolanov and M. Bozhilova, "A Study of Lattice-Based Cryptography," Conference Paper, 5-th

international scientific conference on defensive technologies-oteh 2012, at elgrade, Serbia, 2012.

[25] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," In Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on IEEE, pp. 124–134, 1994.

[26] R. Bayer and E. M. McCreight, "Organization and maintenance of large ordered indexes," Vol. 1, Issue. 3, pp. 173–189, 1972.

[27] R. Bansarkhani and M. Meziani, "An Efficient Lattice-Based Secret Sharing Construction, pp. 160–168, 2012.

[28] A. Shamir, "How to share a secret," In Communications of the ACM, Vol.22, pp. 612–613, 1979

[29] J. L. Dautrich and C. V. Ravishankar, "Security Limitations of Using Secret Sharing for Data Outsourcing," Vol. 7371, pp. 145–160, 2012.

[30] A. Toshinori, "Efficient (k,n) Threshold Secret Sharing Schemes Secure Against Cheating from n − 1 Cheaters," Vol. 4586, pp. 133–142, 2007.

[۳۱] محمدعلی نعمت‌بخش، سیمین قاسمی فلاورجانی و بهروز شاهقلی قهفرخی، «تخصیص وظایف چندهدفه در واگذاری به ابر سیار»، مجله مهندسی برق دانشگاه تبریز، جلد ۴۶، شماره ۴ ،زمستان ۱۳۹۵.

[32] M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," pp. 420–436, 2006.

زیرنویس‌ها

[1] Hash
[2] Advanced Encryption Standard
[3] Structure Query Language
[4] Secret sharing
[5] Secret Recovery
[6] Maximum Distance Separable
[7] Lattice
[8] Share
[9] Data Owner
[10] Client
[11] Users
[12] Data Server
[13] Index Server
[14] Haming
[15] Encryption
[16] Seperation
[17] Distribution
[18] Recover
[19] Indexing
[20] Performance