مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»
سال اول، شماره ۳، پاییز ۱۳۹۲، ص ۷۲-۶۳

تأمین محرمانگی و تمامیت داده برون‌سپرده با استفاده از تسهیم راز آستانه‌ای

محمدرضا آذریون[۱]، مصطفی حق‌جو[۲]، مجید غیوری ثالث[۳*]

۱- دانشجوی کارشناسی ارشد، دانشکده کامپیوتر دانشگاه علم وصنعت ایران ۲- استادیاردانشکده کامپیوتر دانشگاه علم وصنعت ایران،

۳- استادیار دانشکده فناوری اطلاعات و ارتباطات دانشگاه امام حسین(ع)

(دریافت: ۹۱/۰۷/۲۹، پذیرش: ۹۱/۱۲/۲۰)

چکیده

در مدل برون‌سپاری داده‌ها، مالک داده، عملیات مربوط به مدیریت داده را به یک سرویس‌دهنده خارجی می‌سپارد تا پرس‌وجوهای کاربران را دریافت کرده و به آنها پاسخ دهد. داده‌ها برای مالکان بسیار با اهمیت است، حال آنکه ممکن است سرویس‌دهنده خارجی قابل اعتماد نباشد. بنابراین، حفظ محرمانگی و همچنین تمامیت داده‌ها باید کاملاً مورد توجه قرار گیرد. حفظ محرمانگی داده‌ها به این معناست که سرویس‌دهنده خارجی از محتوای داده برون‌سپرده اطلاعی نیابد و تمامیت نیز یعنی مجموع داده‌هایی که به‌عنوان جواب برای کاربر ارسال می‌شود، دقیق و کامل باشد. روش‌های مختلفی برای تأمین این اهداف ارائه شده که هر کدام دارای معایب و مزایایی است. به‌عنوان مثال، می‌توان به استفاده از رمزنگاری، تسهیم داده‌ها و بازیابی محرمانه اطلاعات اشاره کرد. در این مقاله، روشی مبتنی رویکرد تسهیم داده‌ها ارائه شده که کارایی بهتری نسبت به روش‌های قبلی دارد و برخی از مشکلات آنها را مرتفع می‌نماید. در روش پیشنهادی، علاوه بر تأمین محرمانگی داده‌ها، تمامیت پرس‌وجوها نیز تأمین می‌شود.

واژه‌های کلیدی: پایگاه‌داده، برون‌سپاری، امنیت، توزیع داده.

۱. مقدمه

با توسعه روزافزون اینترنت، گرایش شدیدی به پذیرش و اطمینان به تکنولوژی‌های مبتنی بر اینترنت و وب به‌وجود آمده است. رایانش ابری[۱]، در حال عمومیت یافتن در دنیای تجاری است و در آن، قابلیت‌های مختلف محاسباتی، به‌عنوان سرویس به مشتریان داده می‌شود. بنابراین نیاز مشتریان با استخدام افراد متخصص در این زمینه‌ها یا مدیریت و نگهداری نرم‌افزارهایی که این سرویس‌ها را می‌دهند، به این ترتیب برطرف می‌شود.

یکی از دلایل موفقیت ارائه سرویس در اینترنت، حذف تأثیر اندازه یک سازمان، در میزان موفقیت تجاری آن است. مثال خوبی که در این‌مورد می‌توان زد، مرکز داده[۲] است که برای مشتریان، زیرساخت‌های فیزیکی مورد نیاز را برای میزبانی[۳] فراهم می‌کند. این زیرساخت‌ها می‌تواند شامل مواردی همچون ارتباطات با پهنای باند بالا، قابلیت‌های نظارتی و امنیتی باشد. به این ترتیب مراکز داده، نیاز سازمان‌ها و شرکت‌های کوچک به پرداخت هزینه سرمایه‌ای بالا، برای ایجاد زیرساختی در مقیاس جهانی را مرتفع می‌کند. مدل مرکز داده، مؤثر و اجرایی بوده است زیرا به یک سازمان با هر اندازه، اجازه می‌دهد تا میزان سرویس را متناسب با میزان رشدش، افزایش و یا در صورت شکست، کاهش دهد. در چند سال اخیر، شتاب زیادی در ارائه نوآوری در الگوهای جدید تجاری مشاهده می‌شود و مراکز داده نقش مهمی در این فرآیند ایفا کرده‌اند.

علاوه بر زیرساخت فیزیکی که برای پشتیبانی از کاربردهای تحت وب مورد نیاز هستند، چنین کاربردهایی نیاز به مدیریت داده[۴] نیز دارند. به‌عنوان مثال،کاربردهای تجارت الکترونیکی برای هر کاربر، به‌منظور ایجاد امکان تحلیل‌های دقیق تجاری و علایق کاربران، اطلاعات یا کارنامه‌ای[۵] ذخیره می‌کنند. چنین موارد استفاده‌ای، موجب رشد سریع میزان داده مرتبط با این کاربردها شده است. ذخیره‌سازی و بازیابی چنین داده‌هایی باعث به‌وجود آمدن چالش‌های بزرگی، به‌ویژه برای شرکت‌ها و سازمان‌های کوچک می‌شود، زیرا هزینه مدیریت داده‌ها ۵ تا ۱۰ برابر بیشتر از هزینه ذخیره‌سازی آنها است [۱]. به‌علاوه، مدیریت داده در سمت کاربر، نیازمند مهارت بالایی در مورد کار کردن با تکنولوژی‌هایذخیره‌سازی، مدیریت خطا و عیب‌یابی، تحمل خرابی و به‌روزرسانی نرم‌افزار DBMS یا DSMS و سیستم عامل است. این در حالی است که بیشتر سازمان‌ها ترجیح می‌دهند که به‌جای پرداختن به مسائل مدیریت داده، منابع با ارزش و نیروی مهندسی را بر کاربرد تجاری خود متمرکز کنند. با توجه به دلایل ذکر شده، برون‌سپاری داده‌ها یا پایگاه داده در قالب سرویس[۶]، به‌عنوان خط فکری جدیدی در مدیریت داده‌ها مطرح می‌شود که در آن، سرویس‌دهنده پایگاه داده[۷]، مسئولیت مدیریت داده‌ها را بر عهده

* ایمیل نویسنده پاسخگو: ghayoori@ihu.ac.ir

[1] Cloud Computing
[2] Data Center
[3] Hosting

[4] Data Management
[5] Log
[6] Database As A Service
[7] Database Service Provider (Dbsp)

می‌گیرد و نیاز مالک داده را در مورد خریداری سخت‌افزاری برای به‌کارگیری DBMS، تخصیص پهنای باند شبکه و استخدام پرسنل حرفه‌ای برای اجرای سیستم، مرتفع می‌سازد.

اینکه سرویس‌دهنده پایگاه داده، ذخیره‌سازی امن داده را با هزینه اندک تضمین می‌کند، از دید سازمان‌ها و شرکت‌ها بسیار جذاب است. به‌علاوه چنین سرویسی می‌تواند از طریق اینترنت، دسترسی جهانی به داده‌ای را فراهم نماید که در سایت‌های قابل اطمینان و امن ذخیره شده است. شرکت یا سازمان می‌تواند داده خود را برون‌سپاری کند و کارمندانش به‌جای جابه‌جا کردن داده که خطر از بین رفتن آن وجود دارد، قطع نظر از مکانشان، به آن دسترسی داشته باشند.

در روش برون‌سپاری، سه نوع موجودیت مالک داده[1] یا DO، سرویس دهنده[2] یا SP و کاربر وجود دارد. مالک داده، عملیات مربوط به پایگاه داده‌اش را به یک (یا چند) سرویس‌دهنده، با توان و ابزار محاسباتی لازم برای پشتیبانی از پردازش پیشرفته پرس‌وجو، می‌سپارد. کاربران پرس‌وجوهای خود را به‌طور مستقیم به سرویس دهنده می‌فرستند.

برون‌سپاری برای تمام موجودیت‌های دخیل در آن، سودمند است: ۱- مالک داده نیازی ندارد برای به‌کارگیری DBMS منابعی را خریداری کند یا منابع موجود را به آن اختصاص دهد، ۲- سرویس دهنده می‌تواند با سرویس دادن به چند مالک داده، کسب درآمد کند و ۳- کاربر می‌تواند داده را از سرویس بهتر و حرفه‌ای‌تری از سرویس دهنده و با تأخیر کمتری دریافت کند. به‌علاوه، با توجه به اینکه مالک داده دیگر گلوگاه یا SPF[3] نیست، سیستم قوی‌تر می‌شود.

هرچند رویکرد برون‌سپاری مزایای اقتصادی و تکنیکی قابل توجهی دارد، اما متأسفانه موفقیت مراکز داده را به‌دست نیاورده است. دلیل اصلی آن این است که قوانین اخیر دولتی، رقابت بین شرکت‌های مختلف و سرقت داده‌ها، شرکت‌ها را مجبور به استفاده از تکنیک‌های حفظ محرمانگی و تمامیت داده‌ها نموده است. استفاده از یک سرویس پایگاه داده خارجی، باید مشابه کاربرد مشتری سرویس‌دهنده معمولی باشد که در آن سرویس‌دهنده‌ها و مشتریان صادق‌اند و مشتریان در به اشتراک‌گذاری داده‌هایشان با سرویس‌دهنده درنگ نمی‌کنند. اما معمولاً اینگونه نیست و در نتیجه لازم است به کاربران اطمینان داده شود که محرمانگی داده‌ها توسط سرویس‌دهنده تأمین می‌شود و همچنین باید امکان بررسی صحت نتایج برگشتی برای آنها فراهم شود. ممکن است سرویس‌دهنده خارجی قابل اعتماد نباشد و در عین حال داده‌ها برای صاحبانشان و کاربران بسیار با اهمیت باشد، بنابراین، محافظت از آنها در مقابل مهاجمان باید کاملاً مورد توجه قرار گیرد. این سؤال که «چگونه باید از داده‌های برون‌سپرده در برابر مهاجمان محافظت شود»، بسیار مورد علاقه محققان است.

باید توجه کرد که در اینجا «مهاجمان»، شامل مهاجمان خارجی و کاربران غیرقابل اعتماد در سمت سرویس‌دهنده می‌باشد. وجود کاربران غیرقابل اعتماد در سمت سرویس‌دهنده، تکنیک‌های سنتی امنیت پایگاه داده را بی‌اثر می‌کند که حتی با صرف نظر از آن، می‌توان هدف نهایی مالکان را به این صورت بیان کرد که آنها تمایل دارند برون‌سپاری داده‌ها از دیدشان شفاف باشد و سیستم، مانند یک پایگاه داده معمولی عمل کند. کاربران می‌خواهند با داده‌های برون‌سپرده، بدون نگرانی از فاش شدن آن، کار کنند. همچنین می‌خواهند پرس‌وجوهایشان با کارایی بالا و به درستی اجرا شود.

۲. تکنیک‌های مختلف برون‌سپاری

هر کدام از روش‌های مختلفی که برای تأمین محرمانگی و تمامیت داده‌ها ارائه شده است، دارای معایب و مزایایی است. این روش‌ها معمولاً به‌صورت مجزا به دو حوزه مختلف تأمین محرمانگی داده‌ها و تضمین تمامیت پرس‌وجوها پرداخته‌اند. در حوزه نخست، هدف این است که محتوای داده‌ها برای سرویس‌دهنده خارجی فاش نگردد و در حوزه دوم هدف این است که داده‌ها در برابر دست‌کاری‌های احتمالی سرویس‌دهنده محافظت شوند و همچنین پرس‌وجوهای کاربران به‌طور کامل اجرا شوند تا در نتیجه تمامیت پایگاه‌داده مخدوش نگردد. این رویکردها را می‌توان به سه دسته عمده: استفاده از رمزنگاری، بازیابی محرمانه اطلاعات و تسهیم داده‌ها تقسیم نمود.

در رویکردهای مبتنی بر رمزنگاری [۵- ۲] قبل از اینکه داده‌ها به سرویس‌دهنده خارجی سپرده شوند، باید رمزنگاری گردند. اما این کار باعث به‌وجود آمدن چالش جدیدی در مورد جستجو روی داده رمزنگاری شده می‌شود. روش‌هایی که در این زمینه ارائه شده‌اند، علاوه بر محدودیت‌های خاصی مانند نیاز به تغییر هسته DBMS، از مشکل پایین بودن کارایی رنج می‌برند. رویکرد بازیابی محرمانه اطلاعات[۸- ۶] فقط جنبه محرمانگی کاربران را تأمین می‌کند و محرمانگی داده‌ها و تمامیت پرس‌وجوها را پوشش نمی‌دهد. به‌علاوه، پیچیدگی بالا عملاً استفاده از آن را غیرممکن ساخته است [۲]. سومین رویکرد پیشنهاد شده در این زمینه، استفاده از تسهیم داده‌ها است. در این رویکرد، داده‌ها بر روی چند سرویس‌دهنده توزیع می‌شوند و برای دسترسی به آنها باید به همه یا حداقل تعدادی ازسرویس‌دهنده‌ها دسترسی داشت [۳].

با بررسی روش‌های موجود، ملاحظه می‌شود که هنوز راه‌حل صحیح و در عین حال مقرون به‌صرفه‌ای در مورد تأمین محرمانگی و تمامیت داده‌ها در رویکرد برون‌سپاری ارائه نشده است. دیفی[4] که از پیشگامان عرصه رمزنگاری است و الگوریتم معروف

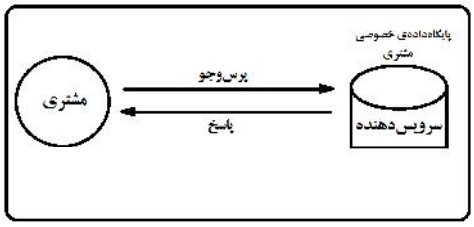
[1] Data Owner
[2] Service Provider
[3] Single Point Of Failure
[4] Whitefield Diffie

دیفی هلمن به نام او مشهور است، به‌تازگی در مصاحبه‌ای بیان کرد: «تکنیک‌های موجود، بیشتر منافع اقتصادی به‌دست آمده از برون‌سپاری را خنثی می‌کند و نشان اندکی از عملی شدن دارد». سیون که از محققین فعال در زمینه برون‌سپاری است، در یک بررسی مفصل در سال ۲۰۱۰، نشان داد که این ادعا کاملاً درست است و حتی در اغلب موارد، برون‌سپاری پرهزینه‌تر از تهیه DBMS و استفاده از پایگاه‌داده به شکل معمول آن است [۴].

در مقاله حاضر، روشی بر مبنای رویکرد تسهیم داده‌ها ارائه شده که کارایی بهتری نسبت به روش‌های قبلی داشته و برخی از مشکلات آنها را نیز مرتفع می‌نماید. در روش پیشنهادی علاوه بر تأمین محرمانگی داده‌ها، تمامیت آنها نیز با فرض متحد نشدن تمامی سرویس‌دهنده‌های پاسخ‌دهنده با یکدیگر، تأمین می‌شود. ادامه این مقاله به ترتیب زیر است: در بخش ۲ به بررسی مدل‌های مختلف برون‌سپاری پرداخته می‌شود. در بخش ۳ ابتدا به بررسی روش تسهیم رمز شمیر پرداخته و سپس روش پیشنهادی بیان خواهد شد. در بخش ۴ روش پیشنهادی با روش‌های مشابه مقایسه و بخش ۵ نیز به جمع‌بندی و ارائه کارهای آتی اختصاص دارد.

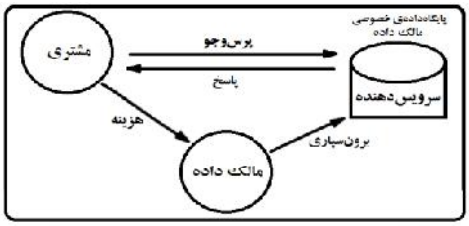
۳. مدل‌های مختلف برون‌سپاری

دو مدل مختلف برای برون‌سپاری داده‌ها وجود دارد. در اولین مدل که SSO[1] نام دارد، مالک داده، مشتری منحصر به‌فرد و یکتا است که داده‌هایش را به یک پایگاه داده خارجی سپرده است. در این مدل، مالک داده نگران محرمانگی داده‌هایش در برابر سرویس‌دهنده خارجی است. همچنین با توجه به اینکه سرویس‌دهنده خارجی ممکن است به‌درستی عمل نکند، مالک داده نگران تمامیت پرس‌وجوهایی که ارسال می‌کند نیز هست. به این معنی که مالک داده باید اطمینان یابد که داده‌هایش توسط سرویس‌دهنده دست‌کاری نشده است. شکل **۱** این مدل دسترسی را نشان می‌دهد.



شکل ۱: مدل SSO

در مدل دوم که SSCO[2] نام دارد، مالک داده، داده‌هایش را برون‌سپاری می‌کند و از مشتریان برای دسترسی به داده‌ها و اطلاعات، هزینه دریافت می‌کند. این مدل، با توجه به مباحث امنیتی، پیچیدگی خاصی دارد. در این مدل، مالک نگران محرمانگی داده‌ها و مشتری نگران تأمین محرمانگی و تمامیت پرس‌وجوهایش هم در مقابل مالک داده و هم در مقابل سرویس‌دهنده خارجی است. به‌علاوه، مالک داده نیز هنگامی که برای به‌روزرسانی، به داده‌های برون‌سپرده‌اش بر روی سرویس‌دهنده دسترسی پیدا می‌کند، نقش کاربر را ایفا می‌کند و در نتیجه، محرمانگی کاربر و تمامیت پرس‌وجوها نیز برای مالک داده اهمیت پیدا می‌کند. شکل **۲** این مدل دسترسی را نشان می‌دهد.



شکل۲: مدل SSCO

مدل مفروض در مقاله حاضر، مدل اول (SSO) است. همان‌طور که ذکر شد، در این مدل، مالک داده یا تنها مشتری موجود است، یا مشتریان همگی مورد اعتماد او هستند و در مورد نحوه برون‌سپاری داده‌ها اطلاعی به سرویس‌دهنده نخواهند داد، زیرا مالک داده همواره نگران محرمانگی داده‌ها وتمامیت پرس‌وجوها است.

۴. روش پیشنهادی

روش پیشنهادی، بر مبنای روش آگروال است. در این روش بر اساس رویکرد تسهیم داده‌ها، چند سرویس‌دهنده وجود دارد (بیش از ۲ عدد) و برای بازیابی اطلاعات باید حداقل به سه سرویس‌دهنده دسترسی داشت. این روش برای مدل SSO کاربرد دارد که در آن، مالک داده تمایل دارد داده‌هایش را به سرویس‌دهنده خارجی بسپارد و سپس پرس‌وجوها توسط خود یا کاربران مورد اعتمادش بر روی این سرویس‌دهنده به‌اجرا درآیند.

همان طور که پیش‌تر ذکر شد، روش پیشنهادی، مبتنی بر تقسیم داده (یا رمز) به چند قسمت و توزیع قسمت‌ها بر روی سرویس‌دهنده‌های مجزا است. در ادامه، ابتدا روش تسهیم رمز شمیر [۵] و سپس روش تغییر یافته پیشنهادی بررسی خواهد شد.

۴-۱. روش تسهیم رمز شمیر

هدف، تقسیم داده D به چند قسمت $D_1, D_2, \ldots, D_n$ است به‌نحوی که:

۱- با آگاهی از هر k عدد دلخواه از D_iها، D به‌راحتی قابل محاسبه باشد.

۲- با آگاهی از هر k-1 یا کمتر D_i، D کاملاً نامشخص بماند (به این معنا که تمامی مقادیر ممکن برای آن، دارای احتمال برابر باشند).

[1] Secure Storage Outsourcing
[2] Secure Storage And Computing Outsourcing

چنین طرحی، یک طرح آستانه‌ای (k,n)[1] نامیده می‌شود. طرح‌های آستانه‌ای، برای کاربردهایی مناسب است که در آنها گروهی از کاربرانی که به هم اعتماد ندارند، قرار است با یکدیگر همکاری کنند.

طرح مورد نظر بر اساس درون‌یابی چندجمله‌ای‌هاست. با داشتن k نقطه در فضای دوبعدی به‌صورت $(x_1,y_1), \dots, (x_k,y_k)$، با مقادیر x_i متمایز، تنها یک چندجمله‌ای $q(x)$ از درجه k-1 به قسمی که $q(x_i) = y_i$ برای هر i وجود دارد، می‌باشد. بدون از دست دادن کلیت، می‌توان فرض کرد که داده D یک عدد است (یا می‌تواند به یک عدد تبدیل شود). برای تقسیم D به قطعات D_i، یک چندجمله‌ای از درجه k-1 انتخاب می‌شود ($q(x) = a_0 + a_1x + \dots a_{k-1}x^{k-1}$) که در آن، $a_0 = D$ و سایر ضرایب به‌صورت دلخواه انتخاب می‌شوند.

D_iها به‌صورت $D1 = q(1)\ ,\ Di = q(i),\ Dn = q(n)$ محاسبه می‌شوند. در نتیجه با داشتن هر زیرمجموعه kتایی از این مقادیر Di، می‌توان ثوابت $q(x)$ را با درون‌یابی محاسبه کرده و سپس مقدار $D = q(0)$ را محاسبه کرد.

از سوی دیگر، حتی داشتن k-1 عدد از این مقادیر، برای محاسبه D کافی نیست. برای اینکه این ادعا دقیق‌تر بیان شود از محاسبات پیمانه‌ای[2] به‌جای محاسبات حقیقی استفاده می‌شود. مجموعه اعداد صحیح در پیمانه یک عدد اول، محدوده‌ای را تشکیل می‌دهد که درون‌یابی در آن امکان‌پذیر است.

با داشتن مقدار D، یک عدد اول p انتخاب می‌شود که از هر دو D و n بزرگ‌تر باشد. ضرایب $q(x)$ به‌صورت تصادفی از بین اعداد [0,p) انتخاب می‌شوند و $D1,\dots,D_n$ به پیمانه p محاسبه می‌شوند.

فرض کنید مهاجمی به k-1 عدد از این n قطعه دست یافته باشد، برای هر مقدار کاندید D در (0,p) می‌تواند به‌طور دقیق یک چندجمله‌ای $q(x)$ از درجه k-1 به‌قسمی که در آن q(0)=D و q(i)=Diبرای k-1 مقدار داده شده، بسازد. طبق تعریف، این p چندجمله‌ای ممکن، دارای احتمال برابر می‌باشند و بنابراین، مهاجم در مورد مقدار واقعی D چیزی به‌دست نمی‌آورد. اگر مقدار D بزرگ باشد، می‌توان آن را به بلوک‌های کوتاه‌تری (که به‌صورت مجزا پردازش می‌شوند) شکست تا از عملیات ریاضی پیچیده اجتناب شود. از آنجا که کوچک‌ترین مقدار قابل استفاده برای p، n+1 است، این بلوک‌ها نمی‌توانند به مقدار دلخواه کوچک باشند.

۴-۲. شیوه استفاده از تسهیم رمز

در روش پیشنهادی، با داشتن ۳ نقطه در فضای دوبعدی، با مقادیر x_i متمایز، یک چندجمله‌ای $q(x)$ از درجه ۲ به قسمی که $q(x_i) = y_i$ برای هر i باشد، تشکیل داده می‌شود. برای تقسیم D به قطعات Di، یک چندجمله‌ای درجه ۲ انتخاب کرده ($q(x) = a_0 + a_1x + a_2x^2$) که در آن، $a_0 = D$ و D_iها را همان‌گونه که در بالا ذکر شد به این صورت محاسبه می‌شود: $D1 = q(1), \dots, D2 = q(2), \dots, Dn = q(n)$. دقت شود که n پارامتر سیستم است و مقدار آن دلخواه (و البته بیش از ۲) است. با داشتن هر زیرمجموعه ۳ تایی از این مقادیر D_i، $D = q(0)$ را با استفاده از روش لاگرانژ محاسبه می‌کنیم. نکته مهمی که باید در نظر گرفته شود این است که برای اجرای پرس‌وجوها، ضروری است که داده‌ها به‌ترتیب بر روی هر سرویس‌دهنده ذخیره شوند.

به طور دقیق‌تر، برای هر دو مقدار دلخواه V_iو V_j در دامنه مورد نظرکه $V_i>V_j$ باشد، می‌خواهیم $Share(Vi,m) > Share(Vj,m)$ برقرار باشد که در آن $Share(Vi,m) = ax_m^2 + bx_m + V_i$ برقرار باشد. برای رعایت کردن این خاصیت، انتخاب مقادیر a و b اهمیت زیادی پیدا می‌کند.

در ادامه، روش پیشنهادی برای انتخاب a و b ارائه و درستی آن اثبات می‌شود. روش کار به این صورت است که هر داده V_i به دو قسمت $\left\lfloor \frac{V_i}{10} \right\rfloor$ و $(10\left\lfloor \frac{V_i}{10} \right\rfloor - V_i)$ تقسیم کرده و دو قسمت مزبور را به ترتیب به‌عنوان مقدار a و b در نظرگرفته می‌شود. (نماد $\lfloor\ \rfloor$ تابع ریاضی کف[3] را نشان می‌دهد).

لم:

در رابطه $Share\ (V_i,m)=ax_m^2 + bx_m + V_i$ که در آن، $a=\left\lfloor \frac{V_i}{10} \right\rfloor$ و $b=(10\left\lfloor \frac{V_i}{10} \right\rfloor - V_i)$، کافی است مقادیر x_m بزرگ‌تر یا مساوی ۶ باشد تا رابطه $Share\ (Vi,m) > Share\ (Vj,m)$ به ازای هر $Vi>Vj$ برقرار گردد.

اثبات:

$$V_i>V_j \Rightarrow Share(V_i,m) > Share(V_j,m) \Leftrightarrow$$
$$a_ix_m^2 + b_ix_m + V_i > a_jx_m^2 + b_jx_m + V_j \Leftrightarrow$$
$$\left\lfloor \frac{V_i}{10} \right\rfloor x^2 + (10\left\lfloor \frac{V_i}{10} \right\rfloor - V_i)x + V_i > \left\lfloor \frac{V_j}{10} \right\rfloor x^2 +$$
$$(10\left\lfloor \frac{V_j}{10} \right\rfloor - V_j)x + V_j \Leftrightarrow \left(\left\lfloor \frac{V_i}{10} \right\rfloor - \left\lfloor \frac{V_j}{10} \right\rfloor\right)x^2 -$$
$$\left((V_i - 10\left\lfloor \frac{V_i}{10} \right\rfloor) - (V_j - 10\left\lfloor \frac{V_j}{10} \right\rfloor)\right)x + (V_i - V_j) > 0$$

اگر ضریب x^2 همواره مثبت باشد، اطمینان داریم که عبارت فوق از نقطه‌ای به بعد، صعودی خواهد بود. اما برای یافتن این نقطه، بدترین حالت ضرایب در نظر گرفته می‌شود. یعنی کمترین مقدار برای ضرایب با علامت مثبت و بیشترین مقدار برای ضرایب با علامت منفی. با توجه به نکته فوق، مقدار عبارت $\left(\left\lfloor \frac{V_i}{10} \right\rfloor - \left\lfloor \frac{V_j}{10} \right\rfloor\right)$ حداقل برابر ۱ است.

بیشترین مقدار عبارت $\left((V_i - 10\left\lfloor \frac{V_i}{10} \right\rfloor) - (V_j - 10\left\lfloor \frac{V_j}{10} \right\rfloor)\right)$ که به معنی تفاضل یکان‌های V_i و V_j است نیز ۹ می‌باشد (به‌عنوان مثال در حالتی که V_i برابر ۲۹ و V_j برابر ۱۰ باشد). در چنین حالتی مقدار عبارت $(V_i - V_j)$ حداقل ۱۹ است، در نتیجه می‌توان نامساوی آخر

[1] (K,N) Threshold Scheme
[2] Modular
[3] Floor

را به نامساوی $x^2 - 9x + 19 > 0$ کاهش داد. ریشه‌های معادله $x^2 - 9x + 19 = 0$ عبارتند از $x_1 = ۳/۳۸$ و $x_2 = ۵/۶$. برای $x \in (۳/۳۸, ۵/۶)$مقدار عبارت کوچک‌تر از صفر و برای سایر xها، بزرگ‌تر از صفر خواهد بود. در نتیجه کافی است مقدار x حداقل برابر کوچک‌ترین عدد صحیح بزرگ‌تر از ۶/۵، یعنی عدد ۶ باشد. به این ترتیب اطمینان خواهیم داشت که رابطه مورد نظر یعنی $V_i>V_j \Rightarrow$ $Share(V_i,m) > Share(V_j,m)$ برقرار است.

اکنون فرض می‌شود سه مقدار D_1، D_2 و D_3 از سه سرویس‌دهنده بازیابی شده‌اند. سه نقطه در فضای دوبعدی داریم: $(x_1,D_1),(x_2,D_2),(x_3,D_3)$. طبق روش لاگرانژ، سهمی‌ای که از این سه نقطه می‌گذرد به صورت زیر محاسبه می‌شود:

$$D = q(0) = D_1\frac{x_2.x_3}{(x_1-x_2)(x_1-x_3)} + D_2\frac{x_1.x_3}{(x_2-x_1)(x_2-x_3)} + D_3\frac{x_1.x_2}{(x_3-x_1)(x_3-x_2)}$$

همان‌طور که قبلا ذکر شد، چندجمله‌ای‌ها به‌گونه‌ای انتخاب شده‌اند که $D = q(0)$ باشد. در نتیجه نیازی به محاسبه $q(x)$ در حالت کلی نداشته و مقدار D را به‌طور مستقیم به‌صورت زیر محاسبه می‌شود:

$$D = q(0) = D_1\frac{x_2.x_3}{(x_1-x_2)(x_1-x_3)} + D_2\frac{x_1.x_3}{(x_2-x_1)(x_2-x_3)} + D_3\frac{x_1.x_2}{(x_3-x_1)(x_3-x_2)}$$

پس از بررسی کلیت کار از لحاظ تئوری، در ادامه، مراحل کار به ترتیب بررسی می‌شود.

۴-۳. ذخیره‌سازی داده‌ها

در فاز ذخیره‌سازی داده‌ها بر روی سرویس‌دهنده‌های خارجی، به‌جای هر داده D، داده‌های D_i بر روی n سرویس‌دهنده مورد استفاده، ذخیره می‌شود. مقدار D_i برابر است با حاصل یک چندجمله‌ای درجه ۲ به صورت $q(x) = a_0 + a_1x + a_2x^2$ که ضرایب آن به ترتیب از چپ به راست عبارتند از: D، $\left\lfloor\frac{D}{10}\right\rfloor$ و $D - 10\left\lfloor\frac{D}{10}\right\rfloor$. در واقع داده به دو بخش شکسته شده و بخش‌های ایجاد شده به‌عنوان ضرایب چندجمله‌ای استفاده می‌شوند.

مقدار x، پارامتری است که به سرویس‌دهنده‌ای که قرار است داده مورد نظر بر روی آن ذخیره گردد، منتسب می‌شود (و البته مقدار آن برای تمام داده‌ها برابر است). این پارامتر یک مقدار صحیح و بزرگ‌تر یا مساوی ۹ است. تنها چیزی که لازم است مالک داده‌ها نگه دارد، مقدار x منتسب به هر سرویس‌دهنده است. به این ترتیب کار مدیریت داده‌ها به سرویس‌دهندهٔ خارجی سپرده می‌شود.

۴-۴. روش ارسال پرس‌وجو

برای ارسال پرس‌وجویی غیر از پرس‌وجوهای بازه‌ای، کافی است کاربر به‌ازای هر مقدار داده D که در پرس‌وجو وجود دارد، تشکیل معادله دهد و سپس با توجه به مقدار x که به هر سرویس‌دهنده منتسب شده است، برای هر سرویس‌دهنده مقدار چندجمله‌ای مربوط به D را محاسبه نماید. سپس به هر یک از n سرویس‌دهنده، پرس‌وجوی جدید را که مقادیر داده آن با مقادیر جدید جایگزین شده است ارسال نماید. مثلا پرس‌وجوی «اطلاعات کارمندانی که D واحد حقوق می‌گیرند» با پرس‌وجوی «اطلاعات کارمندانی که D_i واحد حقوق می‌گیرند» جایگزین و برای سرویس‌دهنده i $(1 \le i \le n)$ ارسال می‌شود ($D_i = Share(V_i,m) = ax_m^2 + bx_m + V_i$).

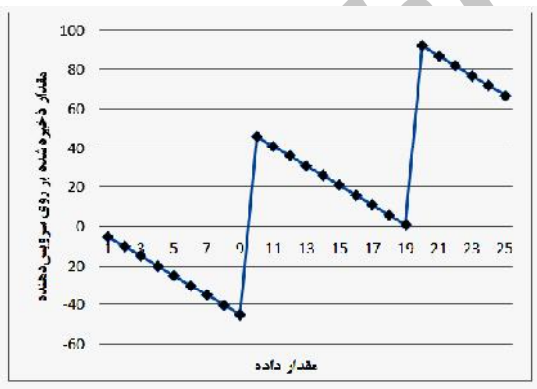
برای پرس‌وجوهای بازه‌ای، رویه اندکی متفاوت است. اگر به رفتار چندجمله‌ای‌های ایجاد شده به‌ازای مقادیر مختلف داده دقت شود، در می‌یابیم که هر بازه موجود در این نوع پرس‌وجوها باید به یک تا سه بازه در پرس‌وجوی جدید تبدیل گردد. این مطلب در سه حالت جداگانه بررسی می‌شود.

حالت اول: کران پایین و بالای بازه پرس‌وجو، هر دو در یک پله از شکل **۳** باشند، مثلاً L=2 و U=7 باشد. در این حالت بازه (L,U) در پرس‌وجوی کاربر، به بازه share (U,m) و share(L,m) در پرس‌وجوی ارسالی به سرویس‌دهنده m تبدیل می‌شود. دقت کنید که در اینجا share(U, m) از share (L,m) کوچک‌تراست.

حالت دوم:کران پایین و بالای بازه پرس‌وجو، در دو پله متوالی از شکل **۳** باشند. مثلاً L=2 و U=12 باشد. در این حالت بازه (L,U) در پرس‌وجوی کاربر، به دو بازه:

1. [share $(10\left\lfloor\frac{L}{10}\right\rfloor + 9,m)$,share(L,m))
2. (share (U,m) , share$(10\left\lfloor\frac{U}{10}\right\rfloor,m)$]

در پرس‌وجوی ارسالی به سرویس‌دهنده m تبدیل می‌شود.

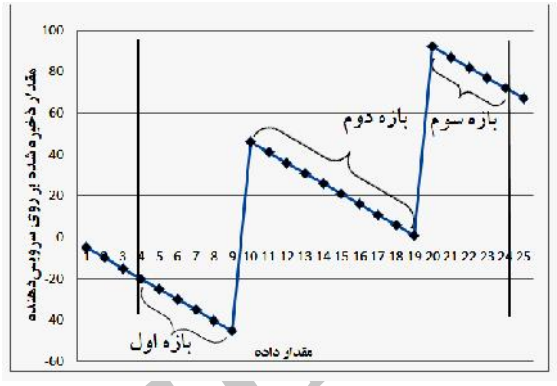


شکل ۳: رفتار چندجمله‌ای‌های ایجاد شده

حالت سوم: کران پایین و بالای بازه پرس‌وجو، در دو پله غیر متوالی (با فاصله دلخواه) باشند. در این حالت که پیچیده‌ترین حالت ممکن است، در پرس‌وجوی کاربر بازه (L,U) شامل سه بازه زیر می‌باشند :

1. [share$(10\left\lfloor\frac{L}{10}\right\rfloor + 9,m)$,share(L,m))
2. [share$((10\left\lfloor\frac{L}{10}\right\rfloor + 19,m)$, share$(10\left\lfloor\frac{U}{10}\right\rfloor - ۱۰,m)$]
3. (share(U,m) , share$(10\left\lfloor\frac{U}{10}\right\rfloor,m)$]

در پرس‌وجوی ارسالی به سرویس‌دهنده m تبدیل می‌شود. برای وضوح بیشتر به شکل **۴** مراجعه کنید. بازه مشخص شده بین دو خط عمودی، بازه پرس‌وجوی کاربر را نشان می‌دهد. شکل **۵** نیز الگوریتم تبدیل بازه پرس‌وجوی کاربر را نشان می‌دهد.



شکل ۴: تبدیل بازه پرس‌وجوی کاربر به بازه پرس‌وجو روی سرویس‌دهنده

```
Algorithm RangeMap
Input: Range (L,U)
Output: Mapped Range(s)
Begin
if (b ≤(۱۰ ⌊L/10⌋+ 9 ) then
Return (share(U,m) , share(L,m))
else if (U≤ ۱۰ ⌊L/10⌋+ 19 ) then Return
[share((۱۰ ⌊L/10⌋+ 9 ,m),share(L,m)) AND
(share(U,m) , share(۱۰⌊U/10⌋,m)]
elseReturn [share(۱۰ ⌊L/10⌋+
9,m),share(L,m)) AND
[share(((۱۰ ⌊L/10⌋+ 19 ,m),
share(۱۰⌊U/10⌋ − ۱۰,m)] AND
(share(U,m) , share(۱۰⌊U/10⌋,m)].
End.
```

شکل ۵: الگوریتم تبدیل بازه پرس‌وجو

۴-۵. روش بازیابی داده‌ها

برای بازیابی داده‌ها، از نتایج برگشتی ۳ سرویس‌دهنده استفاده و سهمی‌ای را که از سه نقطه $(x_1,D_1),(x_2,D_2),(x_3,D_3)$ می‌گذرد، درون‌یابی می‌شود. فرمول مورد استفاده همان طور که در بالا به دست آمد به‌صورت زیر است:

$$D = q(0) = D_1 \frac{x_2.x_3}{(x_1-x_2)(x_1-x_3)} + D_2 \frac{x_1.x_3}{(x_2-x_1)(x_2-x_3)} + D_3 \frac{x_1.x_2}{(x_3-x_1)(x_3-x_2)}$$

لازم به ذکر است که در فرمول بالا، عبارات $\frac{x_2.x_3}{(x_1-x_2)(x_1-x_3)}$، $\frac{x_1.x_3}{(x_2-x_1)(x_2-x_3)}$ و $\frac{x_1.x_2}{(x_3-x_1)(x_3-x_2)}$ برای هر ترکیب سه‌تایی خاص از سرویس‌دهندها ثابت هستند و ربطی به مقدار داده بازگشتی ندارند. در نتیجه برای حفظ کارایی، مالک داده‌ها می‌تواند آنها را یک بار محاسبه و مقادیرشان را نگهداری کند. این کار می‌تواند برای همه ترکیبات مختلف از سرویس‌دهنده‌ها تکرار شود. مثلاً در حالتی که $n = 4$، تعداد ترکیبات ممکن از سرویس‌دهنده‌ها برابر C_3^4 است که مساوی ۴ می‌باشد. در نتیجه مالک داده در مجموع ۱۲ عدد را نگهداری می‌کند که تعدادی قابل چشم‌پوشی است. با توجه به آنچه ذکر شد، مقدار داده برون‌سپرده به‌راحتی بازیابی می‌شود.

۴-۶. بررسی تمامیت

در یک تقسیم‌بندی، سرویس‌دهنده‌ها را می‌توان در دو دسته معتمد[1] و غیر معتمد[2] جای داد. سرویس‌دهنده‌های غیرمعتمد به نوبه خود به دو دسته‌ی تنبل[3] و معاند[4] تقسیم می‌شوند.

در صورتی که سرویس‌دهنده معتمد باشد، نیازی به بررسی تمامیت وجود ندارد. در صورتی که سرویس‌دهنده معاند باشد، ممکن است مقادیر داده را پیش از ارسال برای کاربر دست‌کاری نماید. طبق روش پیشنهادی، این‌گونه تغییرات به صورت زیر کشف می‌شود: پس از درون‌یابی و محاسبه مقدار D، چندجمله‌ای $q(x)$ به‌طور مجدد برای D در سمت کاربر تشکیل می‌شود و مقدار آن به‌ازای x مربوط به یکی از سرویس‌دهنده‌هایی که در پاسخ پرس‌وجو شرکت کرده‌اند، محاسبه می‌شود. مقدار محاسبه شده، باید با مقداری که توسط سرویس‌دهنده مزبور برگردانده شده، برابر باشد. در واقع با چنین روشی درمی‌یابیم که آیا داده بازگردانده شده در بین مقادیر برون‌سپرده وجود داشته است یا خیر. به طور دقیق‌تر، شرط برقراری صحت داده‌ها به صورت زیر است:

$$\forall\, q(0), (Share(q(0)), m) = D_i$$

متأسفانه، سرویس‌دهنده ممکن است تنها به دست‌کاری داده‌های موجود اکتفا نکند، بلکه به‌اصطلاح تنبلی کند و تعدادی متفاوت با تعداد واقعی را برگرداند. در چنین حالتی مقایسه نتایج برگشتی سرویس‌دهنده‌ها امکان‌پذیر است و با فرض اینکه حداکثر یک سرویس‌دهنده دچار خطا باشد، با توجه به مسئله شکست بیزنتاین[5]، قابل تحمل است. به این ترتیب که به اکثریت نتایج نگاه می‌کنیم و با این فرض که همه سرویس‌دهنده‌ها با هم متحد نشده‌اند، حداقل می‌توان نادرستی نتیجه دریافتی را کشف کرد. به طور دقیق‌تر:

$$\forall i \text{and} j \neq i \text{contributedinanswering}, |A_i(Q)| = |A_j(Q)|$$

$A_i(Q)$، مجموعه جابی است که سرویس‌دهنده i در پاسخ به پرس‌وجوی Q برگردانده است. همچنین سرویس‌دهنده ممکن است داده صحیحی که شرط پرس‌وجو را برآورده نمی‌کند، بازگرداند.

در این موارد نیز، با فرض این که همه سرویس‌دهنده‌ها با هم

[1] Trusted
[2] Untrusted
[3] Lazy
[4] Malicious
[5] Byzantine Failure

متحد نشده‌اند، پس از درون‌یابی و بازیابی مقدار بازگشتی، چندجمله‌ای مربوط به آن تشکیل می‌شود و در صورتی که با مقدار دریافتی از سرویس‌دهنده برابر نباشد، نادرستی مقدار دریافتی آشکار می‌شود. در اینجا نیز شرط برقراری تمامیت به‌طور دقیق مشابه حالت اول است.تا آنجا که اطلاع داریم، تاکنون یک روش جامع و در عین حال کارا در این زمینه ارائه نشده و بهترین متدی که در این زمینه یافت شده، متد هَبِر است [۶] که یک به‌روزرسانی ساده در آن، از مرتبه $O(k \log n)$ است (n، اندازهٔ کل پایگاه داده و K، تعداد رکوردهای به‌روزرسانی شده می‌باشد).

۵. تحلیل روش پیشنهادی

مقایسه میزان کارایی دو پروتکل که هر دو برای انجام یک وظیفه طراحی شده‌اند، از سه جهت میزان سربار محاسباتی، سربار حافظه و سربار ارتباطی قابل انجام است.

از لحاظ سربار محاسباتی، طرح‌های مبتنی بر رمزنگاری، بر اساس مسائل پیچیده محاسباتی شکل گرفته‌اند و در نتیجه نیازمند عملیات پیچیده‌ای مانند به توان رساندن اعداد بزرگ (در مقیاس ۱۰۰۰ بیت) هستند. در مقابل، محاسبه D_iها در روش ارائه شده بسیار کاراست و سربار بسیار کمی دارد. محاسبه D_i ها همان‌گونه که در فصل قبل ذکر شد، تنها شامل تقسیم داده به دو بخش و سپس محاسبه چندجمله‌ای مربوط است. البته مقداری سربار در تبدیل انواع داده غیرعددی نیز وجود دارد که آن هم تنها شامل چند ضرب و جمع متوالی است.

همچنین، در مقایسه با روش تسهیم داده‌ای که در مرجع [۱۰] ارائه شده نیز، روش ارائه شده جز در مورد پرس‌وجوهای بازه‌ای کارایی بهتری دارد. زیرا در [۱۰] برای حفظ ترتیب داده‌ها، از توابع درهم سازی بر مبنای محاسبات ممیز شناور استفاده شده، در حالی که در روش پیشنهادی، حفظ ترتیب داده‌ها با ضرایب پیشنهاد شده و حداقل مقدار منتسب به هر سرویس‌دهنده، تضمین شده است. مورد دیگر اینکه در [۱۰] برای بازیابی مقادیر بازگشتی ازسرویس دهنده ها، دستگاه معادلات چندمجهولی حل می‌شود، درحالی که نیازی به این محاسبه در حالت کلی نیست و استفاده از درون‌یابی لاگرانژ برای این‌کار بسیار مناسب‌تراست و کارایی بهتری دارد.

از لحاظ سربار حافظه یا سربار ذخیره‌سازی، طرح‌های مبتنی بر رمزنگاری، به استثنای طرح‌های مبتنی بر منحنی‌های بیضوی مثل ElGamal رمزهایی با طول حداقل ۱۰۲۴ بیت می‌سازند. در صورتی که بخواهیم از خصوصیات هم‌ریختی[1] طرح‌های رمزنگاری استفاده کنیم [۷] باید اعداد ۳۲ بیتی معمولی را نیز در قالب ۱۰۲۴ بیتی رمزنگاری کنیم. در صورت استفاده از طرح‌های مبتنی بر منحنی‌های بیضوی نیز ناچاریم هر بیت را در قالب حداقل ۱۶۰ بیت رمزنگاری کنیم [۸]. در مقابل، تسهیم داده‌ها برای هر فیلد از داده، n سهم تولید می‌کند. هر یک از این سهم‌ها ممکن است از داده اصلی بزرگ‌تر باشند. اما تمام این n سهم ایجاد شده را نباید به‌عنوان سربار در نظر گرفت، بلکه در واقع سربار، k-1 سهم به‌ازای هر فیلد داده است. زیرا n-k سهم، تنها در جهت بالا بردن دسترسی‌پذیری[2] داده، ذخیره شده‌اند. در مقایسه با روش‌تسهیم داده‌ای که در [۱۰] ارائه شده است، سربار ذخیره‌سازی دو روش تفاوتی نداراز لحاظ سربار ارتباطی، در روش‌های مبتنی بر رمزنگاری، غالباً یک فوق‌مجموعه از جواب پرس‌وجوی کاربر ایجاد می‌شود و در سمت کاربر، بعد از رمزگشایی فیلتر می‌شود تا مجموعه نتایج صحیح تولید شود. به اطلاعات اضافی ارسال شده، ارسال‌های ناصحیح[3] گفته می‌شود. واضح است که به‌دلیل وجود اطلاعات اضافی در سمت کاربر، کاربر باید اطلاعات را فیلتر کند و اطلاعات مورد نیاز خودش را بردارد. در واقع کاربر هنوز هم باید نقش پایگاه داده را البته در مقیاسی کوچک‌تر ایفا کند و این مطلب برخلاف هدف برون‌سپاری می‌باشد. در مقابل، در روش‌تسهیم داده‌ها هیچ‌گونه ارسال ناصحیح وجود ندارد.

۵-۱. مقایسه امنیت روش پیشنهادی و روش آگروال

همان‌گونه که شمیر در مقاله خود توضیح داده است، مهاجم بدون همکاری حداقل k سرویس‌دهنده، هیچ اطلاعاتی از محتوای داده‌ها ندارد. اما در صورت همکاری k سرویس‌دهنده، امنیت روش شمیر و بالتبع روش پیشنهادی و روش آگروال مخدوش می‌شود. البته برای مخدوش شدن امنیت، اطلاع دقیق از k+2 داده ضروری است. مهاجم باید از مقادیر اصلی داده و مقدار دقیق منتسب به هر داده بر روی تمام سرویس‌دهنده‌ها آگاه باشد. روش حمله در مرجع [۹] توضیح داده شده است، اما حفظ ترتیب داده‌ها بر روی سرویس‌دهنده نیز می‌تواند امنیت آن را مخدوش نماید. برای نشان دادن این موضوع مثالی از یک حالت بسیار ساده ذکر می‌شود. فرض کنید مالک داده برای برون‌سپاری داده‌ها از چندجمله‌ای $q(x)=3x+D$ استفاده می‌کند و مقدار x منتسب به سرویس‌دهنده مورد نظر نیز برابر ۵ است. در نتیجه $f(D)=15+D$ می‌باشد. حال اگر سرویس‌دهنده از هر طریق از محتوای دو مقدار داده مطلع گردد، مثلاً بداند که $q(4)=19$ و $q(7)=22$، به‌راحتی بااستفاده از روش لاگرانژ، منحنی‌ای که از این دو نقطه می‌گذرد و در اینجا یک خط ساده است را تقریب می‌زند.

$$f(D) = 19\frac{D-7}{4-7} + 22\frac{D-4}{7-4} = D + 15;\ R^2=1$$

ملاحظه می‌شود که رابطه بین مقادیر اصلی و مقادیر ذخیره شده، با داشتن تنها دو نقطه آشکار می‌شود. مقدار R^2 که میزان برازندگی چندجمله‌ای تخمینی سرویس‌دهنده را بیان می‌کند نیز طبق محاسبه زیر، برابر ۱ است. به این معنی که چندجمله‌ای تخمینی دقیقاً متناسب با داده‌های اصلی مالک داده می‌باشد.

$$\bar{y} = \frac{1}{n}\sum_i y_i = \frac{1}{2}(19+22) = 20/5$$

[1] Homomorphic

[2] Availability

[3] False Hits