

روشی برای اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده مبتنی بر نظریه بازی

محمد گورانی^۱، مجید غیوری ثالث^{۲*}

۱- کارشناسی ارشد، ۲- استادیار، دانشگاه جامع امام حسین (ع)

(دریافت: ۹۴/۰۵/۱۲، پذیرش: ۹۵/۱۰/۱۴)

چکیده

با گسترش وب و پیشرفت فناوری اطلاعات و ارتباطات، تجارتی نوین با نام "پایگاه داده به عنوان خدمت" پا به عرصه وجود نهاد. در این محیط رقابتی، افراد و سازمان‌هایی که مدیریت و نگهداری پایگاه‌های اطلاعاتی‌شان چیزی جز زحمت و دردسر و دغدغه نمی‌باشد (با پرداخت پول) این امر مهم را به شرکت‌هایی می‌سپارند که توانایی ارائه خدمت فراگیر در زمینه پایگاه داده را دارند. موضوع اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده از چالش‌های موجود در این زمینه بوده است. تاکنون تلاش‌های فراوانی برای حصول اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده به عمل آمده‌اند و راه‌حل‌های مختلفی ارائه گردیده‌اند اما آنچه در همه آن‌ها مشترک است، ارائه راه‌کار با حفظ انگیزه‌های شدید مادی و معنوی عوامل دخیل در محیط تجاری برون سپاری پایگاه داده است. در این مقاله، برون سپاری پایگاه داده به صورت بازی تجاری که در آن چهار عامل سرور خارجی، مالک داده، کاربر و دشمن با انگیزه‌های مختلف مادی و معنوی حضور دارند، در نظر گرفته شده و بر اساس تئوری بازی روشی برای اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده پیشنهاد می‌گردد. در روش ارائه شده، وجود انگیزه‌های مادی و معنوی متفاوت در بازیکنان به عنوان عامل تهدید جامعیت نتایج پرس و جوها روی پایگاه داده برون سپاری شده معرفی گردیده است و راه‌حلی برای از بین بردن آن ارائه گردیده است. پندار ما این است که مطالعه این مقاله می‌تواند راه‌گشای هر یک از افراد شرکت کننده در برون سپاری پایگاه داده - ارائه دهنده خدمت پایگاه داده، مالک داده و مشتری - در انعقاد قراردادهای تجاری در این زمینه خواهد بود.

واژه‌های کلیدی: پایگاه داده برون سپاری شده، تئوری بازی، جامعیت نتایج پرس و جوها.

۱- مقدمه

در سال‌های اخیر، انقلاب سریع در فناوری‌های ارتباطی، پردازش و حافظه؛ روش‌های قدیمی در مدیریت، ذخیره‌سازی و ارائه داده را تغییر داده است. کاربران هرچه بیشتر علاقه‌مند به اشتراک‌گذاری و ارائه اطلاعات خودشان به کمک خدمات‌های فراهم‌شده توسط سرورهای خارجی شده‌اند [۱].

برون سپاری^۱ داده، پدیده‌ای است که به کاربران و شرکت‌ها اجازه می‌دهد تا برای صرفه‌جویی در زمان و هزینه، داده خود را به سرورهای خارجی بسپارند که از آن پس مسئولیت ذخیره‌سازی، مدیریت و ارائه داده را بر عهده خواهند گرفت [۲].

برون سپاری پایگاه داده معمولاً به نام پایگاه داده به عنوان

خدمت^۲ شناخته می‌شود. اگرچه برون سپاری داده مزایای فراوانی به‌ویژه برای آن دسته از کاربرانی که منابع محدودی برای مدیریت داده در حال افزایش خویش دارند ولی نگرانی‌های امنیتی جدیدی را به وجود می‌آورد.

یکی از چالش‌های امنیتی برون سپاری پایگاه داده اطمینان از جامعیت داده^۳ است. یعنی اطمینان از این‌که پاسخ‌هایی که در قبال پرس و جوها از سرور خارجی دریافت می‌گردد صحیح، تمام و تازه باشد [۳-۴]. تضمین جامعیت نتایج پرس و جو اهمیت فراوانی دارد. بررسی جامعیت نتایج پردازش داده جهت پیاده‌سازی در بسترهای با وسعت زیاد مانند پردازش ابری خیلی مشکل است. راه‌حلی‌هایی که در این زمینه ارائه شده‌اند را می‌توان به دو گروه تقسیم کرد [۴-۵]:

2- Database as service (DAS)

3- Data integrity

* رایانامه نویسنده مسئول: ghayoori@ihu.ac.ir

1- Outsourcing

برون‌سپاری پایگاه داده (کاربر، مالک داده، ارائه‌دهنده خدمت پایگاه داده و دشمن) بازی تجاری - اطلاعاتی به‌وجود می‌آید. این بازی موقعی شرایط برد را به خود می‌گیرد که انگیزه کوتاهی و سهل‌انگاری ارائه‌دهنده خدمت پایگاه داده در تامین امنیت سرور خارجی از بین برود. بدین ترتیب، تمامی بازیکنان (مالک داده، ارائه‌دهنده خدمت پایگاه داده و کاربر) سود مورد نظر را خواهند برد و تعادل بر بازی حکمفرما می‌باشد. در غیر این صورت، بازی به نفع دشمن رقم خواهد خورد.

بهترین روش برای تعریف این بازی و قواعد حاکم بر آن، استفاده از تئوری بازی است. در واقع هر جا انسان‌ها، گروه‌ها و جوامع باهم در تعامل هستند و درصدد تلاش برای حل تعارض‌ها و یا ضربه‌زدن به یکدیگر هستند، مجبور به فراگیری نظریه بازی نیز هستند [۶]. در این مقاله، برخلاف راه‌حل‌های گذشته روشی برای اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری شده ارائه خواهد گردید. به‌طوری‌که اساس این روش از بین‌بردن انگیزه ارائه‌دهنده خدمت پایگاه داده برای سهل‌انگاری و کوتاهی در انجام تعهدات امنیتی سرور خارجی است. بدین ترتیب، ارائه‌دهنده خدمت پایگاه داده تمام تلاش خود را به‌کار خواهد بست تا تمهیدات امنیتی مناسب را برای تامین امنیت سرور خارجی استفاده نماید و بدین‌گونه، اطمینان مورد نظر از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری شده حاصل خواهد شد.

ساختار این مقاله به این صورت است که در قسمت بعد کار مرتبطی که در زمینه برون‌سپاری پایگاه داده با استفاده تئوری بازی صورت گرفته است، بیان خواهد شد. در قسمت سوم، مسائل اصلی و فرضیات اولیه مرور خواهد شد. در بخش‌های چهارم و پنجم روش پیشنهادی ما و ارزیابی آن ارائه می‌گردد. بالاخره پس از جمع‌بندی و نتیجه‌گیری در قسمت ششم، در بخش هفتم کارهای آینده‌ای که در این خصوص می‌توان انجام داد، اشاره خواهد شد.

۲- کارهای مرتبط

در حوزه تکنولوژی ابر اعتبارسنجی توافق خدمت‌دهنده ابر با توجه به نیازمندی‌های امنیتی یک مسئله بسیار مهم است. یکی از مهمترین شاخص‌های اعتبارسنجی داده‌های برون‌سپاری شده بحث جامعیت داده‌ها است. منظور از اعتبارسنجی جامعیت داده‌ها بررسی صحت، دقت و تازگی داده‌های ذخیره شده در ابر در تمام لحظات می‌باشد که در [۷] روش‌های ارائه شده برای بررسی جامعیت و دیگر شاخص‌های امنیتی داده‌های برون‌سپاری شده در ابر ارائه شده است. برای مثال، در [۸-۹] روش‌هایی برای بررسی جامعیت به منظور اجرای پرس‌وجوهای پیچیده توسط

۱- راه‌حل‌های مبتنی بر ساختار تصدیقی^۱: در این جا ساختمان داده مناسبی تعریف می‌شود مانند زنجیره امضاء^۲، درخت درهم‌ساز مرکب^۳ و لیست پرش^۴. این راه‌حل‌ها؛ تمامیت نتایج پرس‌وجوهای که روی صفتی صورت می‌پذیرد، تضمین می‌نمایند. ۲- راه‌حل‌های مبتنی بر ساختار احتمالاتی^۵: مبتنی بر درج دیده‌بان‌هایی در داده برون‌سپاری شده است که این دیده‌بان‌ها باید در نتیجه پرس‌وجو نیز باشند. این راه‌حل‌ها یک اعتماد و اطمینان احتمالی (نسبی) از تمامیت نتایج پرس‌وجو ارائه می‌دهند.

آنچه در همه راه‌حل‌های بالا مشترک است، حفظ انگیزه‌های شدید مادی و معنوی عوامل دخیل در محیط تجاری برون‌سپاری پایگاه داده است.

برون‌سپاری داده از نگاه دیگری نیز قابل بررسی می‌باشد. از آنجایی‌که در برون‌سپاری داده، شرکت‌هایی که خدمت پایگاه داده را ارائه می‌دهند به‌دنبال کسب پول می‌باشند و از طرفی بابت پردازش اطلاعات و آگندار شده منابع سخت‌افزاری و نرم‌افزاری مصرف می‌کنند، پس انگیزه قوی در به‌دست‌آوردن پول بیشتر و صرف منابع کم‌تری دارند. درحالی‌که مالکان داده برعکس به دنبال پرداخت پول کم‌تر و خدمات پردازشی بهتری می‌باشند. از طرف دیگر، کاربران نیز انتظار دارند در برابر پولی که به مالکان داده می‌پردازند از اطلاعاتی که جامعیت آن‌ها تضمین شده است استفاده نمایند ضمن آن‌که دریافت خدمت پایدار از مالک داده نیز مورد درخواست آن‌ها است.

ارائه‌دهنده خدمت پایگاه داده (سرور خارجی) صرفاً برای مدیریت و نگه‌داری پایگاه داده قابل اعتماد است. این موضوع طبیعی است زیرا او دارای انگیزه قوی برای کسب درآمد بیشتر است و به‌همین خاطر، ممکن است جهت صرفه‌جویی اقتصادی یا استفاده از منابع خود برای سایر پردازش‌های مشتریان دیگر -برای کسب درآمد بیشتر- از تعهد کاری خود یعنی حفظ جامعیت داده (صحت، تمامیت و تازگی) و ارائه خدمت پایدار و همیشگی غفلت ورزد. همین امر، زمینه‌ای را برای عامل چهارمی که معمولاً در ساختار برون‌سپاری داده نادیده گرفته می‌شود به‌وجود می‌آورد. این شخصیت؛ موجود بدخواهی است که موفقیت ارائه‌دهنده خدمت پایگاه داده، مالک داده و کاربر را تحمل نمی‌نماید. دشمن با سوء استفاده از رخنه به‌وجودآمده سعی می‌نماید با حمله به سرور خارجی و دست‌کاری داده برون‌سپاری شده و حتی از کارانداختن آن، جامعیت داده و پایداری و همیشگی خدمت پایگاه داده را خدشه‌دار می‌کند.

با این نگاه، برخورد انگیزه‌ها میان عوامل شرکت‌کننده در

1- Authenticated data structures approaches

2- Signature chaining

3- Merkle Hash tree

4- Skip list

5- Probabilistic approaches

6- Service

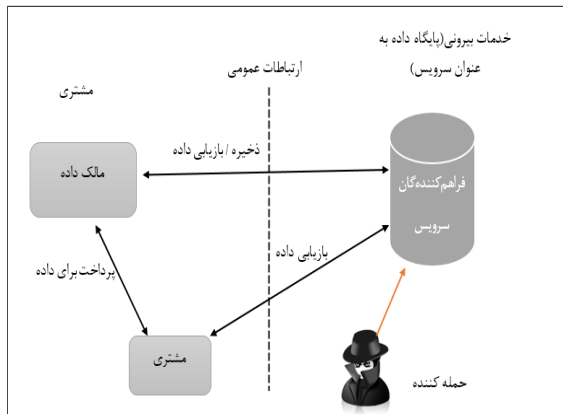
کانون مشکلات یعنی منفعت طلبی عوامل شریک در برون سپاری داده را نشانه نگرفته‌اند. طبیعی است که این انگیزه‌ها می‌توانند با یکدیگر تعارض داشته باشد و راه منطقی تحلیل رقابت انگیزه‌ها استفاده از تئوری بازی است. آن‌ها بازی را با دو بازیکن ارائه‌دهنده خدمت پایگاه داده و مالک داده در نظر گرفته‌اند که وظیفه کنترل و بررسی روی نتایج پرس و جوها را نیز خود مالک داده برعهده دارد. با استفاده از تئوری بازی و حل بازی بالا، الگویی برای انعقاد قراردادهای برون سپاری داده - بین مالک داده و ارائه‌دهنده خدمت پایگاه داده - به دست آمده است. در حالی که در این مقاله بازی برون سپاری پایگاه داده با حضور چهار بازیکن مالک داده، ارائه‌دهنده خدمت پایگاه داده، مشتری و دشمن با انگیزه‌ها و اهداف تجاری متفاوت در نظر گرفته می‌شوند. در واقع، برون سپاری پایگاه داده با یک نگاه امنیتی (با در نظر گرفتن دشمن) به صورت یک بازی تعریف خواهد شد و طی آن، این موضوع بررسی خواهد گردید که با حضور دشمن و امکان حمله او به سرور خارجی و به خطر افتادن جامعیت داده؛ سه بازیکن دیگر چگونه باید بازی را ادامه دهند تا منافع آنان محفوظ بماند. در این مقاله، بر اساس تئوری بازی، روشی ارائه خواهد شد که انگیزه ارائه‌دهنده خدمت پایگاه داده را در محافظت سرور خارجی در برابر حملات دشمن دوچندان خواهد کرد و بدین ترتیب منافع مالک داده و مشتری حفظ می‌شود و این موضوع، اطمینانی از نتایج پرس و جو روی پایگاه داده برون سپاری شده را به دست خواهد داد. در [۲]، مشتری را به بازی وارد نکرده است در حالی که یکی از دلایل اصلی مهاجرت به سمت ابر، استفاده از اطلاعات (پایگاه داده) شرکت‌ها و سازمان‌ها توسط مشتریان از مکان‌های مختلف می‌باشد. بنابراین، حضور مشتری در این بازی ضروری است. همچنین بعضی از مشتریان زیرساخت و دانش کافی برای ارزیابی نتایج سرور را ندارند. به همین دلیل، این عملیات و همچنین عملیات امضا قرارداد را به مالک داده می‌سپارند، پس حضور مشتری در بازی برون سپاری داده ضروری است اما در [۲] فقط مالک داده را وارد کرده و بازی را محدود کرده است. همچنین در آن مقاله، خطر تقلب سرور در استفاده از زیرساخت‌ها مدل کرده و بنابراین حضور دشمن و امکان خرابی و دست کاری اطلاعات توسط او را مدل نکرده‌اند. مدل ما به نحوی طراحی شده است که جلوگیری از تقلب سرور را با حضور دشمن می‌گیرد. این که چرا آن‌ها این دو بازیکن را به بازی وارد نکرده‌اند، به دلیل فرضیات آن‌ها از مسئله بوده است و تغییراتی که اثر وارد کردن این دو بازیکن به سناریو مقاله [۲] ایجاد می‌شود به دیدگاه نویسنده

مشتری و برقراری تعادل بین پیچیدگی محاسباتی و ارتباطی پیشنهاد شده است. در [۱۰] نیز روشی برای اطمینان از صحت، تازگی و جامعیت داده‌های برون سپاری شده در ابر پیشنهاد شده که از رمزنگاری برای شناسایی و اثبات رفتار نامناسب خدمت‌دهنده ابر استفاده می‌کند. در [۱۱] یک روشی برای اثبات برآورده کردن تضمین‌های امنیتی توسط خدمت‌دهنده ابر پیشنهاد کرده‌اند. همچنین در [۱۲] یک روش بسیار مفید پیشنهاد شده است که مشتری می‌تواند عملیات اعتبارسنجی را به شخص سوم واگذار کند. در [۱۳-۱۴] نیز روش‌هایی پیشنهاد شده است که مالک داده یک سری ابر داده از داده‌های خود به منظور اعتبارسنجی نتایج پرس و جوها استفاده می‌کند. اما در سال‌های اخیر، استفاده از نظریه بازی‌ها به منظور تحلیل تعاملات بین بازیگران محیط ابر بسیار مورد توجه قرار گرفته است و مسائل مختلفی از قبیل اختصاص و مدیریت منابع [۱۵]، مذاکره خدمت ابر [۱۶] پیشنهاد شده است. ناگفته نماند نظریه بازی‌ها در حوزه‌هایی از قبیل امنیت شبکه [۲۰-۱۷]، شبکه‌های بی‌سیم [۲۱] و تشخیص نفوذ [۲۲] کاربرد دارد. در ادامه، مقالات مرتبط با موضوع این مقاله را بررسی می‌کنیم.

در سال ۲۰۱۶، Z. Ismail و همکارانش [۲۳]، مقاله‌ای تحت عنوان "حسابرسی برآورده شدن نیازمندی‌های پشتیبان‌گیری داده توسط خدمت‌دهنده ابر: یک تحلیل نظریه بازی" که بهبود یافته کار خودشان در سال ۲۰۱۴ بوده است [۲۴]، ارائه کردند. در این مقاله، مشتری N مجموعه داده را روی یک ابر برون سپاری می‌کند و فرآیند اعتبارسنجی دسترس‌پذیری داده‌ها را به شخص سوم (TPA) می‌سپارد. سپس، مسئله را به عنوان یک بازی ایستا غیرمشارکتی با دو بازیگر خدمت‌دهنده ابر و TPA مدل کرده‌اند. آن‌ها مسئله را با حضور دو بازیگر مدل کرده‌اند و از دخیل کردن دشمن و صاحب داده‌ها و منافع آن‌ها خودداری کرده‌اند در حالی که ما با دخیل کردن این بازیگران، بازی را به صورتی مدل کرده‌ایم که بسیار به شرایط دنیای واقعی نزدیک و در نتیجه کاربردی‌تر است.

در سال ۲۰۱۲، روبرت نیکس و همکارش، مقاله‌ای را با عنوان "کنترل و بررسی کارآمد پرس و جو روی داده برون سپاری شده با استفاده از تئوری بازی" ارائه داده‌اند [۲]. آن‌ها در مقاله خود، بحث را با لزوم عمل بررسی نتایج پرس و جو روی پایگاه داده برون سپاری شده آغاز کرده‌اند. سپس، به چالش جامعیت داده برون سپاری شده از منظر تئوری بازی پرداخته‌اند. به اعتقاد آن‌ها، هیچ‌کدام از روش‌های موجود برای اطمینان از جامعیت نتیجه پرس و جو روی پایگاه داده برون سپاری شده مانند امضای رکوردها

گذارد. بنابراین، کسب حفاظت موثر و عملی از داده در این قبیل موارد پیچیده است. این مطلب در شکل (۱) به تصویر کشیده شده است.



شکل (۱): مدل سامانه پایگاه داده برون‌سپاری‌شده در یک شبکه عمومی

آنچه که موجب به‌خطراتادن جامعیت داده می‌شود انگیزه عوامل شرکت‌کننده در بازی تجاری برون‌سپاری پایگاه داده است. یعنی ارائه‌دهنده خدمت پایگاه داده دارای انگیزه قوی برای کم‌کاری و سهل‌انگاری در انجام تعهدات خویش است و به همین خاطر، ممکن است در به‌کارگیری تمام توان خویش برای تامین امنیت سایت کوتاهی ورزد و این موضوع، موجب به‌وجود آمدن آسیب‌پذیری سرور خارجی گردد. انگیزه ارائه‌دهنده خدمت پایگاه داده می‌تواند مادی باشد و برای صرفه‌جویی اقتصادی و اختصاص امکانات جهت پردازش‌های دیگر (برای به‌دست آوردن پول بیشتر) امنیت کافی را برای سرور خارجی فراهم ننماید. از آنجایی که ارائه خدمت به مشتریان معمولاً از طریق یک شبکه عمومی مانند اینترنت صورت می‌پذیرد، کوتاهی ارائه‌دهنده خدمت پایگاه داده موجب سوءاستفاده موجود بدخواهی به نام دشمن خواهد شد که دارای انگیزه قوی برای عدم موفقیت هر یک از بازیکنان حاضر در صحنه است یعنی مالک داده، مشتری و سرور خارجی.

مسئله اصلی در این مقاله، برون‌رفت از این مشکل با از بین بردن انگیزه ارائه‌دهنده خدمت پایگاه داده در سهل‌انگاری و کوتاهی در انجام تعهداتش است. از آنجایی که در بازی برون‌سپاری پایگاه داده با چهار بازیکن مالک داده، کاربر، سرور خارجی و دشمن برخورد انگیزه‌ها موجب بروز مشکل است با استفاده از تئوری بازی و بر مبنای فرضیاتی که در ادامه ارائه شده‌اند فضای تعامل میان بازیکنان مدل‌سازی می‌شود و با محاسبه سود و زیان بازیکنان -بنابه انگیزه‌ای که دارند- روشی ارائه می‌گردد که انگیزه ارائه‌دهنده خدمت پایگاه داده را در تامین امنیت سرور خارجی و

مقاله نسبت به راهبردهای این دو بازیکن و سودهای آنها بستگی دارد. در [۲۵] نیز یک مدل بازی ارائه شده است که سعی در ایجاد قرارداد بهینه بین فراهم‌کننده خدمات و مشتری دارد. این مدل بازی به‌گونه‌ای است که مشتری با استفاده جریمه کردن و جایزه‌دادن به فراهم‌کننده داده و مشخص کردن میزان آنها در هنگام انعقاد قرارداد، فراهم‌کننده داده را تحریک می‌کند که محاسبات درست و کاملی را روی داده‌های مشتری انجام دهد و اعتبار محاسبات نیز توسط مشتری بررسی می‌شود. این مدل، از جایزه‌دادن نیز برای تحریک فراهم‌کننده داده استفاده می‌کند در حالی که ما فقط از جریمه استفاده می‌کنیم. هم‌چنین این مدل سعی در تحریک فراهم‌کننده خدمات به انجام محاسبات صحیح دارد اما ما سعی در تحریک فراهم‌کننده خدمات به انجام بهترین دفاع با حضور دشمن داریم.

در [۲۶] نیز چند مدل بازی برای ارزیابی جامعیت و دسترس‌پذیری داده‌های برون‌سپاری‌شده در ابر پیشنهاد شده است که هیچ یک حضور دشمن را در بازی مدل نکرده‌اند و بازی را این‌گونه سازمان‌دهی کرده‌اند که از حضور دشمن جلوگیری می‌کند. در [۲۷] نیز یک مدل بازی ارائه شده است که در آن مالک داده، داده‌ها را روی دو سرور جدا ذخیره می‌کند سپس با احتمال یکسان پرس و جوها را به سرورها می‌فرستد و با مقایسه نتایج به‌دست‌آمده و جریمه کردن آنها در صورت تقلب سعی در تحریک آنها برای انجام محاسبات درست را دارد. این مدل نیز از مدل کردن دشمن پرهیز کرده است و دو سرور برای ردیابی نتایج استفاده کرده است که هزینه بیشتری را به مالک داده تحمیل می‌کند.

۳- بیان مساله و مفروضات اولیه

در برون‌سپاری پایگاه داده، خیلی از مزایای خلاصی از دردسرهای مدیریت و نگهداری آن و نیز دسترس‌پذیری همگانی اطلاعات فراهم می‌شوند، در حالی که نگرانی‌های امنیتی جدیدی نیز به وجود می‌آیند. ارائه‌دهنده خدمت پایگاه داده از طریق یک شبکه عمومی یا وب، متعهد به ارائه پاسخ جامع به پرس‌وجوهای کاربران و خدمتی پایدار است و این در حالی است که حضور موجود بدخواهی به نام دشمن در فضای شبکه عمومی یا وب می‌تواند پس از نفوذ به سرور خارجی و بدون اطلاع از محتویات داده، قسمتی از داده پاسخ را حذف و یا اطلاعات جعلی وارد آنها نموده و حتی از ارسال آنها به کاربر جلوگیری کند یا با انجام انواع حمله به سرور خارجی، او را در ارائه خدمت مورد تعهد ناکام

۷- **تعداد کاربران (مشتریان):** تاثیری در روش پیشنهادی نخواهند داشت و همان گونه که بعداً خواهیم دید هر چه تعداد مشتریان بیشتر باشد اطمینان از نتایج پرس و جوها بیش تر خواهد گردید.

برای سادگی بحث، فقط یک سرور خارجی و فقط یک مالک داده وجود دارند درحالی که روش ارائه شده قابل تعمیم به چند سرور و چند مالک داده نیز می باشد.

۴- روش پیشنهادی

روشی که در ادامه ارائه می گردد فارغ از نوع پرس و جوهای مشتریان می باشد و به روشی که مالک داده، سرور خارجی و مشتریان جهت حفظ جامعیت پاسخ پرس و جوها به کار می برند، وابسته نمی باشد. بلکه در این جا روشی پیشنهاد می گردد که انگیزه ارائه دهنده خدمت پایگاه داده را در عدم انجام تعهداتش مبنی بر ارائه خدمتی پایدار و پاسخ های جامع به پرس و جوهای مشتریان از بین می برد. شرکت ارائه دهنده خدمت پایگاه داده موجودی قابل اعتماد اما خردمند می باشد که برای کسب سود بیشتر، امکان دارد از تمام منابع سخت افزاری و نرم افزاری خویش جهت انجام تعهداتش بهره نگیرد و با عدم تامین امنیت مناسب در سایت خویش زمینه را برای نفوذ دشمن فراهم نماید. بنابراین احتمال دارد دشمن با نفوذ به سرور خارجی با سرقت اطلاعات و جایگزینی آن با اطلاعات جعلی هر کدام از معیارهای جامعیت^۱ پاسخ ها به پرس و جوهای مشتریان (صحت^۲، تمامیت^۳ و تازگی^۴) را به خطر اندازد و یا با از کار انداختن سرور خارجی مانع از پیوستگی خدمات سرور خارجی به مشتریان شود.

در این روش با در نظر گرفتن حمله احتمالی دشمن، سود و زیان هریک از بازیکنان محاسبه می گردد و می توان با توجه به این محاسبات، قرارداد برون سپاری پایگاه داده را طوری تنظیم نمود که انگیزه سرور خارجی را در عدم انجام تعهداتش و هرگونه سهل انگاری در برقراری امنیت سایت خویش از بین ببرد. این روش می تواند برای هرگونه حمله دشمن با توجه به میزان احتمال وقوع آن به کار گرفته شود.

۴-۱- مدل بازی

بازی برون سپاری پایگاه داده به صورت زیر تعریف می شود:

جلوگیری از نفوذ دشمن تقویت می نماید. بدین منظور، یک سری مفروضات اولیه به شرح ذیل در نظر گرفته می شوند:

۱- **مالک داده:** در واقع با پرداخت پول، مدیریت و نگهداری پایگاه داده خویش را با انعقاد قرارداد رسمی که قابل طرح در مراجع قانونی می باشد، به یک ارائه دهنده خدمت پایگاه داده می سپارد و نسبت به معرفی مشتریان به این شرکت اقدام می نماید.

۲- **ارائه دهنده خدمت پایگاه داده:** با انعقاد قرارداد رسمی که قابل طرح در مراجع قانونی خواهد بود، با دریافت پول، عهده دار مدیریت و نگهداری پایگاه داده مالک داده شده و وظیفه تامین امنیت پایگاه داده در شبکه عمومی و ارائه پاسخ های جامع (صحیح، تمام و تازه) به پرس و جوهای مشتریان را برعهده می گیرد. هم چنین این شرکت متعهد می گردد که خدمتی پایدار ارائه دهد به طوری که مشتری در هر زمانی و در هر مکانی بتواند داده مورد نیاز خود را بدست آورد.

۳- **مشتری:** با انعقاد قرارداد رسمی که قابل طرح در مراجع قانونی خواهد بود، با پرداخت پول به مالک داده انتظار دریافت داده مورد نیاز خویش را خواهد داشت.

۴- **حمله کننده (دشمن):** موجودی بدخواه بوده که ممکن است با انجام انواع حمله مانند از کار انداختن سرور، سرقت اطلاعات روی سرور، برخی از رکودهای داده را حذف و با رکوردهای جعلی جایگزین نماید، و بدین ترتیب، ارائه دهنده خدمت پایگاه داده را در ارائه پاسخ جامع به پرس و جوهای مشتریان و خدمتی پایدار ناتوان نماید.

۵- **ارائه دهنده خدمت پایگاه داده:** از جهت حفظ امانت داده و ارائه خدمت پایدار به مشتریان، قابل اعتماد بوده و خود درصدد تغییر محتوای پایگاه داده بر نمی آید ولی ممکن است بنابه دلایل اقتصادی سهل انگاری نماید و تمهیدات امنیتی لازم را برای جلوگیری نفوذ دشمن به کار نگیرد. در نتیجه دشمن با سوء استفاده از رخنه ایجاد شده سعی می نماید سرور خارجی را از کار انداخته یا با سرقت اطلاعات روی آن و جایگزینی با اطلاعات جعلی، ارائه دهنده خدمت پایگاه داده را در ارائه خدمت پایدار و پاسخ های جامع به پرس و جوهای مشتریان ناتوان سازد.

۶- **نحوه اجرای پرس و جوها:** توسط سرور و روشی که مالک داده، سرور خارجی و کاربر برای احراز هویت و جامعیت پاسخ به پرس و جوها به کار می گیرند، خارج از موضوع این مقاله می باشد.

1- Integrity
2- Correctness
3- Completeness
4- Freshness

۴-۱-۱- بازیکنان

چهار بازیکن به نام‌های مالک داده^۱ (DO)، سرور خارجی^۲ (S)، مشتری^۳ (C) و حمله‌کننده^۴ (A).

۴-۱-۲- فعالیت‌ها

مشتری پرس‌وجوی (Q) خود را به سمت سرور می‌فرستد و پاسخ (D) را دریافت می‌نماید. البته ممکن است مشتری در برابر پرس‌وجوی خویش پاسخ (D) را دریافت نماید که نشان از نقض جامعیت داده توسط حمله‌کننده می‌باشد. ضمناً ممکن است سرور از دسترس مشتری خارج باشد و او نتواند پرس‌وجوی خویش را انجام دهد و این حاکی از آن است که سرور توسط حمله‌کننده از کار افتاده است.

مشتری با دریافت پاسخ نادرست (D) و یا عدم دریافت پاسخ موضوع را به اطلاع مالک داده می‌رساند و مطالبه خسارت می‌کند. مالک داده نیز با انجام بررسی و مشخص شدن قصور سرور خارجی در تامین امنیت کافی، طلب خسارت می‌نماید. بدیهی است میزان خسارت در قراردادهای منعقد فی‌مابین مشتری و مالک داده و هم‌چنین مالک داده و سرور خارجی به‌طور کامل مشخص و به تایید طرفین رسیده است. واضح است که جریمه‌ها و خسارت‌ها عامل بازدارنده بازیکنان از عدم انجام تعهداتشان است.

حمله‌کننده (دشمن) سعی دارد با انجام حملات پی در پی و نفوذ به سرور خارجی، منافع مشتری و سرور خارجی را تهدید نماید. از آن‌جا که در این روش فرض بر این است که سرور خارجی مسئول پایداری خدمت و جامعیت پاسخ‌ها به مشتریان می‌باشد هرگونه کوتاهی سرور خارجی در زمینه مقابله با حمله‌کننده‌ها موجب خسران مالی او خواهد شد. بدیهی است این موضوع به‌طور شفاف در انعقاد قرارداد بین مالک داده و سرور خارجی بیان گردیده است.

۴-۱-۳- اطلاعات

مالک داده (DO) پایگاه داده خودش (D) را به سرور خارجی (S) می‌سپارد. البته مالک داده طی این برون‌سپاری سعی می‌کند جامعیت رکوردهای اطلاعاتی را با اتخاذ روشی مناسب مثلاً با اضافه‌نمودن امضاء روی هر رکورد داده حفظ نماید. با این کار، سرور خارجی نمی‌تواند تغییری در محتوای رکوردهای داده دهد. از طرفی، کاربر با آگاهی از امضای مالک داده نسبت به اعتبارسنجی پاسخ پرس‌وجوها اقدام می‌نماید. مالک داده، سرور

خارجی و مشتری (کاربر) قبلاً در این مورد به توافق رسیده‌اند و این موضوع طی قرارداد منعقد فی‌مابین به اطلاع بازیکنان رسیده است. بدیهی است مغایرت امضای پاسخ‌ها به معنی تغییر اطلاعات در سرور می‌باشد که حاکی از نفوذ حمله‌کننده به سرور خواهد بود.

۴-۱-۴- راهبردها

از آن‌جایی که دو حالت "نفوذ دشمن" و "عدم نفوذ دشمن" در نظر گرفته خواهند شد، بنابراین می‌توان راهبردهای بازیکنان را به دو صورت زیر در نظر گرفت:

(a, d, v و q): این بدین معنی است که (به ترتیب از چپ به راست) بازیکن مشتری در حال پرس‌وجو^۵ (q) است. بازیکن مالک داده در حال کنترل و بررسی^۶ نتایج پرس‌وجوهاست (v). بازیکن سرور خارجی در حال دفاع در برابر حملات^۷ دشمن است (d) و بازیکن دشمن در حال حمله به سرور خارجی^۸ می‌باشد ولی موفق به نفوذ به آن نمی‌گردد (a).

(e, f, r و t): این بدین معنی است که (به ترتیب از چپ به راست) بازیکن مشتری به‌دنبال کسب جریمه^۹ از مالک داده بوده (r) و پیرو آن بازیکن مالک داده نیز به‌دنبال کسب جریمه از ارائه‌دهنده خدمت پایگاه داده می‌باشد (t). بازیکن سرور خارجی نتوانسته است امنیت کافی را برقرار نماید و دچار شکست^{۱۰} شده است (f) و در نتیجه دشمن توانسته به راحتی به سرور خارجی نفوذ^{۱۱} نماید (i).

۴-۱-۵- سودها

از آن‌جایی که روش پیشنهادی مبتنی بر مدل احتمالی حمله دشمن است ابتدا سود بازیکنان در دو حالت "عدم نفوذ دشمن" و "نفوذ دشمن" محاسبه می‌گردد سپس با در نظر گرفتن مدل احتمالی حمله دشمن مجدداً سود بازیکنان محاسبه می‌شود و براساس نتیجه به‌دست‌آمده چگونگی انعقاد قرارداد میان بازیکنان توضیح داده خواهد شد به‌گونه‌ای که انگیزه تخلف از بازیکنان در انجام تعهداتشان از بین برود.

۴-۱-۵-۱- عدم نفوذ دشمن

در این حالت، دشمن علی‌رغم حملات پی‌درپی که به سرور خارجی دارد به دلیل تامین امنیت مناسب از سوی ارائه‌دهنده

5- Query
6- Verify
7- Defend
8- Attack
9- Refund
10- Fail
11- Intrusion
12- Utilities

1- Data Owner
2- Server
3- Client
4- Attacker

به کارگیری تمهیدات مناسب نسبت به تامین امنیت کافی اقدام نماید، حمله کننده نه تنها سودی به دست نمی آورد بلکه فقط بابت منابعی که جهت حمله و نفوذ به سرور خارجی صرف می کند هزینه ای می پردازد و این منطقی به نظر می رسد.

۴-۱-۵-۲- نفوذ دشمن

اما در دنیای واقعی وضع بدین گونه نیست، یعنی حمله کننده می تواند با نفوذ به سرور خارجی و از کار انداختن آن یا سرقت اطلاعات روی آن و جایگزینی با اطلاعات ناصحیح موجب گردد که سرور در پاسخ به پرس و جویهای کاربران داده های نادرست ارائه دهند. در این صورت، بازی به شکلی دیگر رقم خواهد خورد و لازم است سودهای بازیکنان مجدداً محاسبه گردد. در صورت موفقیت آمیز بودن حمله دشمن و نفوذ او به سرور، سود حمله کننده به صورت زیر در می آید:

$$Ua(r,r,f,i) = Iv(Q) - Costa(Q) \quad (۶)$$

این رابطه بیان می دارد سودی که حمله کننده از نفوذ به سرور خارجی و از کار انداختن آن یا سرقت اطلاعات روی آن و درج اطلاعات نادرست روی آن به دست می آورد در واقع متناسب با نیت بدخواهانهای بوده است که از قبل در ذهن داشته است یعنی "سود نبردن مشتری از اطلاعات دریافتی". ما این موضوع را به صورت $Iv(Q)$ نشان می دهیم. اما دشمن جهت موفقیت خویش هزینه ای را بابت به کارگیری منابع مصرف نموده است که این مورد به شکل $Cost_a(Q)$ در رابطه بالا ظاهر شده است.

در این حالت سرور با نفوذ دشمن و خراب کاری به جامانده از آن مواجه می شود. از طرفی، بابت پاسخ های نادرستی که در برابر پرس و جویهای کاربران داده است می بایست جریمه ای را به مالک داده بپردازد. این جریمه در قرارداد منعقد شده بین مالک داده و ارائه دهنده خدمت پایگاه داده به طور شفاف بیان می گردد. با این توضیحات، سود ارائه دهنده پایگاه داده به شکل زیر محاسبه می شود:

$$Us(r,r,f,i) = Pdo(Q) - Costs(Q) - Costrec(Q') - FS \quad (۷)$$

این رابطه نشان می دهد که سود شرکت ارائه دهنده خدمت پایگاه داده در صورت موفق بودن حمله دشمن برابر است با مقدار پولی که مالک داده بابت مدیریت و نگهداری پایگاه داده و پاسخ به پرس و جویها به او می پردازد ($Pdo(Q)$) منهای هزینه ای که سرور در این زمینه برای پاسخ به پرس و جوی کاربر مصرف می دارد ($Costs(Q)$) منهای هزینه ای که سرور مجبور است جهت بازیابی اطلاعات از دست رفته یا راه اندازی مجدد خرج نماید تا بتواند دوباره به نحو مطلوب در مقابل پرس و جویهای مشتریان پاسخ های مناسب دهد ($Costrec(Q)$) منهای جریمه ای (FS)

خدمت پایگاه داده، نمی تواند به سرور خارجی نفوذ نماید. بنابراین، جامعیت داده روی آن حفظ می گردد و حتی خدمت پایگاه داده به طور پایدار ادامه خواهد یافت. با این توضیح سود بازیکنان به شرح زیر به دست خواهد آمد:

مشتری (کاربر) ارزش اطلاعاتی نتایج حاصل از پرس و جویها روی پایگاه داده را منهای هزینه ای که در این رابطه به مالک داده می پردازد، به دست می آورد. می توان سود مشتری را به شکل زیر نمایش داد:

$$Uc(q,v,d, a) = Iv(Q) - Pc(Q) \quad (۱)$$

مالک داده مبلغ پرداختی از سوی کاربر را دریافت می دارد و در مقابل هزینه ای را بابت پردازش پرس و جو توسط سرور خارجی به او می پردازد. می توان سود این بازیکن را به شکل زیر نمایش داد:

$$Udo(q, v, d, a) = Pc(Q) - Pdo(Q) \quad (۲)$$

ارائه دهنده خدمت پایگاه داده مبلغ پرداختی توسط مالک داده را دریافت داشته و با صرف هزینه سخت افزاری و نرم افزاری جهت پردازش پرس و جوی کاربر و حفظ امنیت سایت پاسخ لازم را به او خواهد داد. با این توضیح می توان سود سرور خارجی را به صورت زیر نشان داد:

$$Us(q,v,d, a) = Pdo(Q) - Costs(Q) \quad (۳)$$

بدیهی است که:

$$Iv(Q) \geq Pc(Q) \geq Pdo(Q) \geq Costs(Q) \quad (۴)$$

زیرا ارزش آن چه بازیکنان دریافت می دارند بیش تر از ارزش آن چیزی است که هزینه می کنند در غیر این صورت، بازی دیگر بین افراد خردمند برقرار نیست و سود برخی از بازیکنان از صفر کم تر خواهد شد و در صورت ادامه بازی به همین منوال دیگر اسم بازی را نمی توان روی آن گذاشت مگر آن که بازیکن با سود صفر (با دریافت یارانه) سعی می کند بازی را برای اهداف دیگر ادامه دهد.

در مدلی که در بالا توضیح داده شد سرور به درستی به تعهدات خود برای تامین امنیت سایت خویش اقدام نموده است و جلوی نفوذ حمله کننده را گرفته و در واقع پاسخی که کاربر در برابر پرس و جویهایش دریافت می دارد همگی صحیح می باشند بنابراین سود حمله کننده به شکل زیر محاسبه می گردد:

$$Ua(q,v,d, a) = -Costa(Q) \quad (۵)$$

این رابطه نشان می دهد موقعی که سرور خارجی بتواند با

داده مالک داده به او پرداخته است ($Pc(Q)$). بنابراین، مشتری باید جریمه‌ای که از مالک داده دریافت می‌کند به اندازه‌ای باشد که جبران ضرر وارده به او باشد ($+ Fdo$). این بدین معنی است که مقدار جریمه باید به قدری باشد که حاصل جمع جبری عبارت فوق مثبت گردد. واضح است که جریمه دریافتی از مالک داده این انگیزه را در او تقویت می‌نماید به دنبال جبران ضرر وارده به مشتری خود باشد (مشتری‌مداری) و بنابراین پس از بررسی تخلف شرکت ارائه‌دهنده خدمت پایگاه داده، مطابق قرارداد منعقد شده طلب خسارت می‌نماید و بدین ترتیب شرکت ارائه‌دهنده خدمت پایگاه داده جهت فرار از پرداخت جریمه سعی می‌کند نسبت به تامین امنیت مناسب برای سرور خود و جلوگیری از نفوذ دشمن به آن تمهیدات لازم را بگمارد. این موضوع همان انتظار مطلوبی است که مالک داده به دنبال آن است تا بتواند تجارت سودآوری داشته باشد و مشتریان خود را راضی نگه دارد.

همان‌گونه که ملاحظه می‌شود آنچه انگیزه ارائه‌دهنده خدمت پایگاه داده را در انجام تعهدات خویش مبنی بر تامین امنیت سرور خارجی برای حفظ جامعیت داده و ارائه خدمتی پایدار دوچندان می‌کند جریمه‌ای است که باید در صورت موفقیت دشمن به مالک داده بپردازد. همچنین انگیزه مالک داده برای کنترل و بررسی جامعیت داده روی سرور و پیگیری شکایت مشتری از نحوه ارائه خدمت سرور خارجی با الزام پرداخت جریمه به کاربر در صورت تخلف سرور بیشتر می‌شود. بنابراین در روش پیشنهادی محاسبه جریمه‌ها در صورت حمله احتمالی دشمن موضوعی است که به آن پرداخته خواهد شد.

۴-۱-۵-۳- نفوذ احتمالی دشمن

دشمن همیشه در حال حمله به سرور خارجی است اما قسمتی از این حملات موفق به نفوذ می‌شوند که می‌توانند منجر به از کار انداختن سرور خارجی و نقض جامعیت داده ذخیره شده روی آن شوند. این موضوع بیانگر آن است که نفوذ دشمن به سرور خارجی یک مدل احتمالی است.

این مساله را می‌توان از زاویه دیگر نیز نگاه کرد به طوری که ارائه‌دهنده خدمت پایگاه داده دارای دو راهبرد دفاع و شکست است. راهبرد دفاع یعنی آن که سرور خارجی در امنیت است و دشمن نمی‌تواند به آن نفوذ نماید و جامعیت داده حفظ می‌شود و حتی پایداری و همیشگی خدمت پایگاه داده پابرجاست. راهبرد شکست یعنی آن که سرور خارجی در خطر است و دشمن می‌تواند به آن نفوذ نماید و در نتیجه جامعیت داده به خطر می‌افتد و حتی ممکن است پایداری و همیشگی خدمت پایگاه داده از دست رود. ارائه‌دهنده خدمت پایگاه داده راهبردهای فوق را بنا به انگیزه خود براساس یک مدل احتمالی بر می‌گزیند به طوری که اگر

که بابت سهل‌انگاری در تامین امنیت کافی سرور باید به مالک داده بدهد. بدیهی است مقدار جریمه‌ای که ارائه‌دهنده خدمت پایگاه داده می‌پردازد باید به گونه‌ای باشد که انگیزه او را بابت قصور در انجام وظایف مورد تعهد (برقراری امنیت لازم جهت جلوگیری از نفوذ دشمن) به حداقل برساند.

در صورت موفقیت دشمن و نفوذ او به سرور خارجی و شکست لایه‌های امنیتی جامعیت پایگاه داده برون‌سپاری شده به خطر می‌افتد و ممکن است سرور خارجی از کار بیفتد و این موضوع منافع کاربران (مشتریان) را - سودی که از اطلاعات می‌برند - به خطر می‌اندازد. واضح است در صورت به خطر افتادن منافع کاربران (مشتریان) مطابق قرارداد فی‌مابین آن‌ها و مالک داده امکان طلب خسارت از مالک داده به وجود می‌آید و این بیانگر تهدید منافع مالک داده می‌باشد. در رابطه زیر میزان بهره‌ای که مالک داده در صورت موفقیت دشمن به دست می‌آورد، محاسبه می‌گردد:

$$Udo(r,r,f,i) = Pc(Q) - Pdo(Q) + FS - Fdo \quad (۸)$$

این رابطه نشان می‌دهد سود مالک داده برابر است با پولی که از مشتری بابت پرس‌وجو روی داده متعلق به او دریافت می‌کند ($Pc(Q)$) منهای هزینه‌ای که بابت پاسخ سرور خارجی به پرس‌وجوی کاربر به او می‌پردازد ($- Pdo(Q)$) به علاوه جریمه‌ای است که از شرکت ارائه‌دهنده خدمت پایگاه داده بابت سهل‌انگاری در تامین امنیت دریافت می‌نماید ($+ FS$) منهای جریمه‌ای که بابت نقض جامعیت پاسخ سرور خارجی و قطع خدمت‌رسانی او باید به کاربر بپردازد ($- Fdo$).

بدیهی است که مقدار جریمه دریافتی از ارائه‌دهنده خدمت پایگاه داده (FS) باید به اندازه‌ای باشد که علاوه بر جبران هزینه‌ای که مالک داده بابت پاسخ سرور خارجی به پرس‌وجوی کاربر به او می‌پردازد، تکافوی جریمه‌ای باشد که می‌بایست بابت خسارت به مشتری بدهد (Fdo).

از سویی دیگر، کاربر (مشتری) نیز بابت ضرری که از سهل‌انگاری شرکت ارائه‌دهنده خدمت پایگاه داده نموده است می‌تواند از مالک داده طلب خسارت نماید. این موضوع کاملاً قانونی بوده زیرا قبلاً طی قرارداد منعقد شده با مالک داده به طور کامل بیان شده است. رابطه زیر بیانگر سود مشتری در صورت موفقیت دشمن در حمله سرور خارجی می‌باشد:

$$Uc(r,r,f,i) = -Pc(Q) + Fdo \quad (۹)$$

رابطه بالا نشان می‌دهد که مشتری نه تنها از اطلاعات مالک داده سودی نبرده است بلکه هزینه‌ای بابت پرس‌وجو روی پایگاه

$$Us(q,v,d,\alpha) = \alpha Pdo(Q) - \alpha Costs(Q) - \alpha Costrec(Q') - \alpha FS + Pdo(Q) - Costs(Q) - \alpha Pdo(Q) + \alpha Costs(Q)$$

$$Us(q, v, d, \alpha) = Pdo(Q) - Costs(Q) - \alpha Costrec(Q') - \alpha FS$$

این رابطه بیانگر این واقعیت است که سرور خارجی در برابر راهبرد حمله دشمن (با احتمال نفوذ α) سودی معادل $\alpha FS - \alpha Pdo(Q) - \alpha Costs(Q) - \alpha Costrec(Q')$ خواهد آورد. عبارت $Pdo(Q) - Costs(Q)$ سود منطقی و طبیعی سرور خارجی از بازی تجاری است که بین او و مالک داده در جریان است که قبلاً توضیح داده شده است. عبارت $\alpha FS - \alpha Costrec(Q')$ بیانگر آن است که در صورت موفقیت دشمن و نفوذ او به سرور خارجی او باید با احتمال α هزینه‌ای معادل جریمه پرداختی به مالک داده به علاوه هزینه بازیابی مجدد داده را بپردازد تا بتواند مجدداً اعتماد مالک داده را جلب نماید و بازی تجاری را ادامه دهد.

با آگاهی از این که ارائه‌دهنده خدمت پایگاه داده با احتمال β راهبرد دفاع را برمی‌گزیند و امنیت سرور خارجی را تامین می‌کند می‌توان سود مالک داده را به شکل زیر محاسبه نمود:

$$Udo(q,v,\beta,a) = \beta Udo(q,v,d, a) + (1-\beta) Udo(r,r,f,i) \quad (13)$$

$$Udo(q, v, \beta, a) = \beta (Pc(Q) - Pdo(Q)) + (1-\beta) (Pc(Q) - Pdo(Q) + FS - Fdo(Q'))$$

$$Udo(q,v,\beta,a) = \beta Pc(Q) - \beta Pdo(Q) + Pc(Q) - Pdo(Q) + FS - Fdo(Q') - \beta Pc(Q) + \beta Pdo(Q) - \beta FS + \beta Fdo(Q')$$

$$Udo(q,v,\beta,a) = Pc(Q) - Pdo(Q) + (1-\beta)FS - (1-\beta)Fdo(Q')$$

این عبارت بیانگر سود مالک داده در حالت نفوذ دشمن به سرور خارجی است با این تفاوت که احتمال انتخاب راهبرد شکست از سوی سرور خارجی $(1-\beta)$ تاثیر خود را در آن گذاشته است.

از آنجایی که سود مشتری وابسته به عملکرد صحیح مالک داده است و از طرفی انجام تعهدات از سوی مالک داده وابسته به عملکرد صحیح سرور خارجی می‌باشد، می‌توان سود مشتری را به‌طور غیرمستقیم وابسته به عملکرد صحیح سرور خارجی دانست. بنابراین می‌توان سود مشتری (کاربر) را به‌شکل زیر محاسبه نمود:

$$Uc(q,v,\beta,a) = \beta Uc(q,v,d, a) + (1-\beta) Uc(r,r,f,i) \quad (14)$$

$$Uc(q, v, \beta, a) = \beta (Iv(Q) - Pc(Q)) + (1-\beta) (-Pc(Q) + Fdo)$$

$$Uc(q, v, \beta, a) = \beta Iv(Q) - \beta Pc(Q) - Pc(Q) + Fdo + \beta Pc$$

$$Uc(q,v,\beta,a) = \beta Iv(Q) - Pc(Q) + (1-\beta) Fdo$$

این عبارت به‌طور واضح وابستگی سود مشتری را به اتخاذ راهبرد مختلط از سوی سرور خارجی نشان می‌دهد به‌طوری که سود مشتری (کاربر) را با احتمال انتخاب راهبرد دفاع از سوی سرور خارجی (β) معادل ارزش تجاری داده پرس‌وجو شده

تصمیم به درست‌کاری داشته باشد و تمام توان خود را برای امنیت سرور خارجی به‌کار بندد با احتمال بالایی راهبرد دفاع را به‌کار خواهد بست و در نتیجه امنیت سرور خارجی به‌دست خواهد آمد و اگر تصمیم به‌کارگیری تمام توان خود برای امنیت سرور خارجی نداشته باشد و منابع سخت‌افزاری و نرم‌افزاری خود را برای به‌دست آوردن سود بیشتر به سایر پردازش‌ها اختصاص دهد با احتمالی دیگر راهبرد شکست را برخواهد گزید. با این توضیح می‌توان میان ارائه‌دهنده خدمت پایگاه داده، مالک داده، مشتری و دشمن یک بازی ایستا با راهبرد مختلط تعریف نمود به‌گونه‌ای که در آن دشمن همیشه در حالت حمله است و بنا به نوع حمله با یک احتمال مشخص می‌تواند موفق باشد که این احتمال متقابلاً احتمال انتخاب راهبرد توسط ارائه‌دهنده خدمت پایگاه داده است. اگر احتمال نفوذ دشمن (موفقیت حمله دشمن) برابر با مقدار α در نظر گرفته شود احتمال دفاع ارائه‌دهنده خدمت پایگاه داده در برابر نفوذ دشمن معادل مقدار β خواهد بود به‌طوری که:

$$\beta = 1 - \alpha \quad (10)$$

بنابراین سود بازیکنان به‌صورت زیر به‌دست خواهند آمد. می‌توان گفت که سرور خارجی با احتمال β در برابر نفوذ دشمن دفاع خواهد نمود (راهبرد دفاع) و با احتمال $1-\beta$ در برابر نفوذ دشمن شکست خواهد خورد (راهبرد شکست). بنابراین با وجود این احتمال سود بازیکن دشمن به‌شکل زیر خواهد بود:

$$Ua(q,v,\beta,a) = \beta Ua(q,v,d, a) + (1-\beta) Ua(r,r,f,i)$$

$$Ua(q, v, \beta, a) = \beta (-Cost_a(Q)) + (1-\beta) (I_v(Q) - Cost_a(Q))$$

$$Ua(q, v, \beta, a) = -\beta Cost_a(Q) + Iv(Q) - Cost_a(Q) - \beta Iv(Q) + \beta Cost_a(Q)$$

$$Ua(q,v,\beta,a) = (1-\beta) Iv(Q) - Cost_a(Q) \quad (11)$$

این رابطه نشان می‌دهد که دشمن در برابر راهبرد دفاع سرور خارجی (با احتمال β) سودی معادل $(1-\beta) Iv(Q) - Cost_a(Q)$ خواهد داشت. این نتیجه آن است که دشمن با انجام هزینه $Cost_a(Q)$ و با احتمال $1-\beta$ پاداش تلاشش را خواهد گرفت که معادل با ارزش اطلاعاتی است که مشتری از سرور خارجی به‌دست خواهد آورد. در واقع، این نتیجه‌گیری متناسب با نیت بدخواهانه دشمن است که به‌دنبال سودنبردن مشتری (کاربر) می‌باشد.

اگر دشمن با احتمال α موفق به نفوذ به سرور خارجی شود و بتواند جامعیت داده روی آن را نقض نماید و حتی او را از کار اندازد آن‌گاه سودی که سرور از تجارتش خواهد برد به شکل زیر محاسبه می‌شود:

$$Us(q, v, d, \alpha) = \alpha Us(r,r,f,i) + (1-\alpha) Us(q,v,d, a) \quad (12)$$

$$Us(q,v,d,\alpha) = \alpha (Pdo(Q) - Costs(Q) - Costrec(Q') - FS) + (1-\alpha) (Pdo(Q) - Costs(Q))$$

ادعایی که مشتری بابت مقدار $Iv(Q)$ نماید، مورد پذیرش مالک داده نخواهد بود پس در محاسبات آینده به‌ناچار به جای $Iv(Q)$ از حداقل مقدار آن یعنی $Pc(Q)$ استفاده خواهیم کرد تا مقدار جریمه مورد توافق طرفین (مالک داده و مشتری) به دست آید. پس از رابطه ۱۵ داریم:

$$Fdo \geq (1-\beta) Pc(Q) + Pc(Q) \quad (17)$$

$$Fdo \geq Pc(Q) - \beta Pc(Q) + Pc(Q)$$

$$Fdo \geq 2 Pc(Q) - \beta Pc(Q)$$

$$\beta Pc(Q) \geq 2 Pc(Q) - Fdo$$

$$\beta \geq \frac{2 Pc(Q) - Fdo(Q)}{Pc(Q)}$$

با توجه به این که احتمال β قطعاً عددی بین ۰ و ۱ است خواهیم داشت:

$$1 \geq \beta \geq \frac{2 Pc(Q) - Fdo(Q)}{Pc(Q)} \geq 0 \quad (18)$$

از نامساوی بالا می‌توان نتیجه گرفت:

$$\frac{2 Pc(Q) - Fdo}{Pc(Q)} \geq 0 \quad (19)$$

$$2 Pc(Q) - Fdo(Q) \geq 0$$

$$2 Pc(Q) \geq Fdo$$

این عبارت بدین معنی است که جریمه مالک داده حداکثر مقدار $2Pc(Q)$ خواهد بود. مجدداً از رابطه (۱۸) می‌توان نتیجه گرفت که:

$$1 \geq \frac{2 Pc(Q) - Fdo}{Pc(Q)} \quad (20)$$

$$Pc(Q) \geq 2 Pc(Q) - Fdo$$

$$Fdo \geq 2 Pc(Q) - Pc(Q)$$

$$Fdo \geq Pc(Q)$$

این نتیجه بدین معنی است که حداقل جریمه مالک داده مقدار $Pc(Q)$ می‌باشد. می‌توان نتایج بالا را به شکل زیر نمایش داد:

$$Pc(Q) \leq Fdo \leq 2 Pc(Q) \quad (21)$$

با توجه به نامساوی بالا واضح است که مالک داده به دنبال چانه‌زنی برای تعیین مقدار جریمه معادل $Pc(Q)$ یعنی معادل پولی که از مشتری بابت پرس‌وجو دریافت داشته است، می‌باشد. درحالی‌که مشتری در پی افزایش جریمه به حداقل مقدار $2Pc(Q)$ است. درواقع مالک داده باید مراقب باشد که مقدار جریمه از $2Pc(Q)$ بیش‌تر نگردد و مشتری نیز باید مواظبت نماید که مقدار جریمه از $Pc(Q)$ کم‌تر نشود. این‌که جریمه مالک داده به‌صورت بازه‌ای محاسبه می‌شود به دلیل وجود احتمال حمله دشمن (α) و متقابلاً احتمال دفاع سرور خارجی در برابر آن است (ب).

می‌داند و با احتمال انتخاب راهبرد شکست از سوی سرور خارجی و نفوذ دشمن $(1-\beta)$ معادل جریمه‌ای که از سوی مالک داده دریافت می‌دارد، می‌داند. بازی برون‌سپاری پایگاه داده با چهار بازیکن مشتری، مالک داده، سرور خارجی و دشمن، یک بازی کاملاً رقابتی می‌باشد. سرور خارجی سعی می‌کند احتمال انتخاب راهبرد دفاع یا شکست را از سایر بازیکنان یعنی مالک داده و مشتری مخفی دارد.

عامل بازدارنده ارائه‌دهنده خدمت پایگاه داده از هرگونه سهل‌انگاری و کوتاهی در تامین امنیت سرور خارجی، جریمه‌ای است که باید از این بابت به مالک داده بپردازد (FS). هم‌چنین عامل محرک مالک داده برای کنترل و بررسی سرور خارجی جهت ارائه پاسخ‌های دارای شرایط جامعیت (صحت، تازگی و تمامیت) به مشتریان و نیز پیگیری خواسته‌های کاربران برای رفع از کارافتادگی سرور خارجی، جریمه‌ای است که باید به مشتریان پرداخت نماید (Fdo).

از آن‌جایی که در قراردادهای تجاری میان مشتری و مالک داده و هم‌چنین قراردادهای تجاری میان مالک داده و ارائه‌دهنده خدمت پایگاه داده می‌بایست جریمه‌های فوق به‌طور صریح مشخص شوند تا در صورت نیاز در محاکم قانونی قابل طرح باشند، می‌بایست فرمولی برای محاسبه آن‌ها به دست آورد.

۴-۲- جریمه مالک داده (Fdo)

از رابطه (۱۴) چنین برداشت می‌شود که مشتری به‌دنبال آن است تا جریمه‌ای که از مالک داده دریافت می‌نماید علاوه‌بر جبران زبانی که از بابت عدم دریافت اطلاعات جامع به او رسیده است، تکافوی مبلغی که بابت پرس‌وجوی Q به او پرداخته است نیز باشد یعنی:

$$Fdo \geq (1-\beta) Iv(Q) + Pc(Q) \quad (15)$$

که در آن، $Iv(Q)$ زبانی است که مشتری از بابت شکست سرور خارجی در برابر تهاجمات دشمن و دریافت پاسخ‌های فاقد اطلاعات جامع از او متحمل شده است. $Pc(Q)$ نیز پولی است که مشتری بابت پرس‌وجوی Q به مالک داده می‌پردازد.

از سوی دیگر، مالک داده به دنبال آن است در صورت تخلف ارائه‌دهنده خدمت پایگاه داده از تعهدات خویش مبنی بر برقراری امنیت سرور خارجی و عدم نفوذ دشمن به آن، جریمه‌ای بیش‌تر از استرداد پولی که از مشتری بابت پرس‌وجوی وی دریافت داشته است، مبلغ دیگری نپردازد. بنابراین خواهیم داشت:

$$Fdo \leq Pc(Q) \quad (16)$$

با توجه به فرض $Iv(Q) \geq Pc(Q)$ و این موضوع که هرگونه

به صورت تقریبی به دست آوریم:

$$\frac{3 Pdo(Q) - Fs}{2 Pdo(Q)} \geq 0$$

$$3 Pdo(Q) - Fs \geq 0 \quad (27)$$

$$3 Pdo(Q) \geq Fs$$

این عبارت حداکثر جریمه سرور خارجی را نشان می دهد. مجدداً از رابطه (۲۶-۶) خواهیم داشت:

$$\frac{3 Pdo(Q) - Fs}{2 Pdo(Q)} \leq 1$$

$$3 Pdo(Q) - Fs \leq 2 Pdo(Q) \quad (28)$$

$$3 Pdo(Q) - 2 Pdo(Q) \leq Fs$$

$$Pdo(Q) \leq Fs$$

این عبارت نیز حداقل جریمه سرور خارجی را نشان می دهد. می توان نتایج فوق را به شکل زیر نمایش داد:

$$Pdo(Q) \leq Fs \leq 3 Pdo(Q) \quad (29)$$

با توجه به نامساوی بالا واضح است که ارائه دهنده خدمت پایگاه داده به دنبال چانه زنی برای تعیین مقدار حداقلی جریمه یعنی $Pdo(Q)$. این مقدار پولی است که از مالک داده بابت انجام پردازش روی داده دریافت می دارد. در حالی که مالک داده به دنبال تعیین مقدار حداکثری جریمه سرور خارجی یعنی $3 Pdo(Q)$. در واقع ارائه دهنده خدمت پایگاه داده باید مراقب باشد که مقدار جریمه از $3 Pdo(Q)$ بیش تر نگردد و مالک داده نیز باید مواظبت نماید که مقدار جریمه از $Pdo(Q)$ کم تر نشود. دلیل آن که جریمه سرور خارجی به صورت بازه ای محاسبه می شود وجود احتمال حمله دشمن (α) و متقابلاً دفاع احتمالی سرور خارجی در برابر آن است (β).

همان طور که بیان شد در صورتی که سرور تقلب کند هزینه ای معادل با $(FS + Costrec(Q))$ پردازد.

قضیه: این بازی با استفاده از قرارداد بالا یک تعادل در راهبرد خالص دارد. مالک داده β را به نحوی انتخاب می کند که برای سرور، تقلب کردن از پاسخ صحیح برگرداندن بسیار کم ارزش تر باشد و در نتیجه سرور تقلب نمی کند. بنابراین β را به نحوی تعیین می کنیم که رابطه زیر برقرار باشد:

$$U_s(q, v, \beta, a) \geq U_s(r, r, f, i)$$

یعنی سود سرور وقتی که پاسخ صحیح را برمی گرداند از حالتی که تقلب می کند بیش تر باشد. هم چنین می دانیم که:

$$U_s(q, v, \beta, a) = \beta U_s(q, v, d, a) + (1 - \beta) U_s(r, r, f, i)$$

$$U_s(q, v, \beta, a) = \beta (P_{do}(Q) - Cost_s(Q)) +$$

۳-۴- جریمه سرور خارجی (FS)

از رابطه (۱۳) چنین برداشت می شود که مالک داده به دنبال آن است تا جریمه ای که از سرور خارجی دریافت می نماید علاوه بر جبران جریمه ای که از بابت نقض جامعیت پاسخ های او به پرس و جویهای مشتریان باید به آن ها بدهد، تکافوی مبلغی که بابت پرس و جوی q به او پرداخته است نیز باشد یعنی:

$$Fs \geq Pdo(Q) + (1 - \beta) Fdo \quad (22)$$

که در آن، $Pdo(Q)$ پولی است که مالک داده بابت پرس و جوی q به سرور خارجی پرداخته است و مقدار $(1 - \beta) Fdo$ معادل جریمه ای است که از بابت سهل انگاری ارائه دهنده خدمت پایگاه داده در تأمین امنیت سرور خارجی باید به مشتری بپردازد. از سوی دیگر، ارائه دهنده خدمت پایگاه داده به دنبال آن است که جریمه ای بیش تر از استرداد پولی که از مالک داده بابت پرس و جوی q دریافت داشته بپردازد یعنی:

$$Fs \leq Pdo(Q) \quad (23)$$

مالک داده برای محاسبه جریمه سرور خارجی از رابطه (۲۲) استفاده کرده و با جایگزینی Fdo با حداکثر مقداری که از رابطه ۲۱ به دست آورده فرمول زیر را به دست می آورد زیرا مالک داده موجودی سودجو است و به دنبال منفعت بیش تری است:

$$Fs \geq Pdo(Q) + (1 - \beta) 2 Pc(Q) \quad (24)$$

این عبارت با این که راهی برای محاسبه جریمه سرور خارجی پیش روی مالک داده است ولی مورد توافق ارائه دهنده خدمت پایگاه داده نیست زیرا مقدار $Pc(Q)$ سودی است که مالک داده از فروش اطلاعاتش به دست آورده و برای ارائه دهنده خدمت پایگاه داده قابل پذیرش نمی باشد. بنابراین، طرفین باید به توافقی برای محاسبه جریمه سرور خارجی دست یابند، پس با توجه به فرض $Pc(Q) \geq Pdo(Q)$ ؛ به جای عبارت $Pc(Q)$ از مقدار حداقلی آن یعنی از مقدار $Pdo(Q)$ بهره گرفته می شود. واضح است که این مقدار مورد توافق طرفین بوده و در متن قرارداد منعقد نیز آمده است. با این توضیحات خواهیم داشت:

$$Fs \geq Pdo(Q) + (1 - \beta) 2 Pdo(Q) \quad (25)$$

$$Fs \geq Pdo(Q) + 2 Pdo(Q) - \beta 2 Pdo(Q)$$

$$\beta 2 Pdo(Q) \geq 3 Pdo(Q) - Fs$$

$$\beta \geq \frac{3 Pdo(Q) - Fs}{2 Pdo(Q)}$$

از آن جایی که مقدار احتمال β بین مقادیر ۰ و ۱ است خواهیم داشت:

$$1 \geq \beta \geq \frac{3 Pdo(Q) - Fs}{2 Pdo(Q)} \geq 0 \quad (26)$$

از نامساوی بالا می توانیم مقدار جریمه سرور خارجی را

برون سپاری پایگاه داده ارائه گردید.

در این روش جریمه‌های بازیکنان متخلف به‌عنوان عامل اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری شده در نظر گرفته شد زیرا موجب بازدارندگی ارائه‌دهنده خدمت پایگاه داده از عدم تأمین امنیت کافی سرور خارجی و همچنین بازدارندگی مالک داده از عدم کنترل و بررسی سرور خارجی از ارائه پاسخ‌های جامع به پرس‌وجوهای مشتریان و از کارافتادگی سرور خارجی می‌باشند. این جریمه‌ها به‌صورت تقریبی به‌دست آمدند به‌طوری‌که الگویی برای چانه‌زنی هریک از بازیکنان مالک داده، مشتری و ارائه‌دهنده خدمت پایگاه داده در هنگام انعقاد قراردادهای تجاری به‌دست می‌دهد. در بخش بعدی نسبت به ارزیابی روش پیشنهادی و تفسیر نتایج حاصله از آن خواهیم پرداخت.

۵- ارزیابی و تفسیر نتایج

روشی که در بخش قبل ارائه گردید با در نظر گرفتن حمله احتمالی دشمن و همچنین دفاع احتمالی ارائه‌دهنده پایگاه داده در برابر او عاملی برای اطمینان از نتایج پرس‌وجوهای کاربران روی پایگاه داده برون‌سپاری شده به‌نام جریمه معرفی گردید که می‌توانست انگیزه تخلف بازیکنان در انجام تعهداتشان به‌منظور ارائه خدمتی پایدار و نیز پاسخ‌های جامع به پرس‌وجوها روی پایگاه داده را کاهش دهد بدین شکل که:

اگر ارائه‌دهنده خدمت پایگاه داده در انجام وظیفه خود برای برقراری امنیت سرور خارجی کوتاهی ورزد به‌طوری‌که دشمن بتواند جامعیت داده برون‌سپاری شده را به خطر اندازد باید جریمه‌های معادل:

$$F_s(Q') \geq 3P_{do}(Q) - 2\beta P_{do}(Q) \quad (31)$$

را به مالک داده بپردازد. این در حالی است که مالک داده نیز در اثر سهل‌انگاری و خطای ارائه‌دهنده خدمت پایگاه داده که در پی عدم کنترل و بررسی همیشگی و به‌موقع او به وقوع پیوسته است، می‌بایست جریمه‌ای معادل:

$$2P_c(Q) - \beta P_c(Q) \leq F_{do}(Q') \quad (32)$$

را به کاربر بپردازد. در ادامه با استفاده از روش مقداردهی نتایج به‌دست‌آمده را بیش‌تر مورد ارزیابی قرار می‌گیرد.

۵-۱- ارزیابی عددی

روش ارائه‌شده در این مقاله چون از نظر ریاضیات ثابت شده است نیاز به پیاده‌سازی به‌منظور بررسی صحت و درستی آن

$$(1 - \beta) (P_{do}(Q) - Cost_s(Q) - Cost_{rec}(Q') - F_s)$$

$$U_s(q, v, \beta, a) = \beta P_{do}(Q) - \beta Cost_s(Q) + P_{do}(Q) - Cost_s(Q) - Cost_{rec}(Q') - F_s - \beta P_{do}(Q) + \beta Cost_{rec}(Q') + \beta Cost_s(Q) + \beta F_s$$

$$U_s(q, v, \beta, a) = P_{do}(Q) - Cost_s(Q) - Cost_{rec}(Q') - F_s + \beta Cost_{rec}(Q') + \beta F_s$$

با توجه به مطالب بالا و رابطه (۷) داریم:

$$U_s(q, v, \beta, a) \geq U_s(r, r, f, i)$$

$$P_{do}(Q) - Cost_s(Q) - Cost_{rec}(Q') - F_s + \beta Cost_{rec}(Q') + \beta F_s \geq P_{do}(Q) - Cost_s(Q) - Cost_{rec}(Q') - F_s$$

از ساده‌کردن رابطه بالا به رابطه زیر می‌رسیم: (۳۰)

$$\beta \geq \frac{1}{Cost_{rec}(Q') + F_s}$$

وقتی β زیاد شود سود حاصل از تقلب‌کردن کاهش پیدا می‌کند به شرط آن‌که $Cost_{rec}(Q')$ و F_s به اندازه کافی بزرگ باشند. بنابراین تا زمانی که نامساوی بالا برقرار باشد سرور هیچ انگیزه‌ای برای تقلب‌کردن ندارد.

وقتی که $Cost_{rec}(Q')$ یک عدد ثابت است ما می‌توانیم F_s را در قرارداد تنظیم کرد و هرچه مقدار آن بیش‌تر باشد می‌توانیم β را کاهش دهیم. ما قبل از این محدودده F_s را تعیین کرده‌ایم و همان‌طور که بیان شد تا زمانی که نامساوی بالا برقرار باشد سرور هیچ انگیزه‌ای برای تقلب‌کردن ندارد.

هم‌چنین باید نشان دهیم که β با مالک داده سازگار است. در نظر بگیرید وقتی که β زیاد شود چه اتفاقی می‌افتد. اگر β از مقدار بالا بزرگ‌تر باشد مالک داده عملیات اعتبارسنجی داده‌ها را انجام نمی‌دهد زیرا سرور پاسخ صحیح برمی‌گرداند. بنابراین، مالک داده ارزش خود را از دست می‌دهد. لذا مالک داده β بزرگ‌تر از مقدار بالا انتخاب نمی‌کند. حال اگر مقدار β از این مقدار کم‌تر باشد سرور شروع به تقلب‌کردن می‌کند و در مجموع سود مالک داده کاهش پیدا می‌کند. به همین خاطر مالک داده β کم‌تر از این مقدار انتخاب نمی‌کند. پس با توجه به توضیحات بالا مالک داده مایل به تغییر مقدار β به‌دست‌آمده در بالا را ندارد پس این مقدار β یک تعادل است.

در این بخش با استفاده از تئوری بازی و با در نظر گرفتن مدل احتمالی حمله دشمن به سرور خارجی و مدل دفاع احتمالی ارائه‌دهنده خدمت پایگاه داده در برابر حملات دشمن (احتمال سهل‌انگاری و کوتاهی ارائه‌دهنده خدمت پایگاه داده در تأمین امنیت سرور خارجی به‌صورت دفاع احتمالی لحاظ گردیده است)، روشی برای محاسبه بهره بازیکنان شرکت‌کننده در بازی

بازی تجاری بین مشتری، مالک داده و ارائه دهنده خدمت پایگاه داده در جریان باشد، می بایست پولی که مشتری بابت پرس و جو روی داده مالک داده به او می پردازد حداقل با مقدار پولی که مالک داده بابت انجام پردازش روی داده اش به سرور خارجی می پردازد برابر باشد و بلکه بسیار بزرگتر باشد ($P_c(Q) >> P_{do}(Q)$). با آگاهی از این موضوع که مقدار احتمال β قطعاً بین مقادیر ۰ و ۱ خواهد بود جدول (۱) به دست می آید.

اکنون با فرض این که $P_c(Q)=1$ و $P_{do}(Q)=0/8$ باشند. جریمه مالک داده (F_{do}) و جریمه سرور خارجی (F_s) در احتمالات مختلف دفاع سرور خارجی (β) مطابق جدول (۲) به دست می آید.

جدول (۱): محاسبه جریمه های مالک داده و سرور خارجی

β	۰	۰/۱	۰/۲	۰/۳	۰/۴	۰/۵
$F_{do} \geq$	$2 P_c(Q)$	$1/9 P_c(Q)$	$1/8 P_c(Q)$	$1/7 P_c(Q)$	$1/6 P_c(Q)$	$1/5 P_c(Q)$
$F_s \geq$	$3 P_{do}(Q)$	$2/8 P_{do}(Q)$	$2/6 P_{do}(Q)$	$2/4 P_{do}(Q)$	$2/2 P_{do}(Q)$	$2 P_{do}(Q)$
β	۰/۶	۰/۷	۰/۸	۰/۹	۱	-
$F_{do} \geq$	$1/4 P_c(Q)$	$1/3 P_c(Q)$	$1/2 P_c(Q)$	$1/1 P_c(Q)$	$P_c(Q)$	-
$F_s \geq$	$1/8 P_{do}(Q)$	$1/6 P_{do}(Q)$	$1/4 P_{do}(Q)$	$1/2 P_{do}(Q)$	$P_{do}(Q)$	-

جدول (۲): جریمه های مالک داده و سرور خارجی با مقادیر نمونه

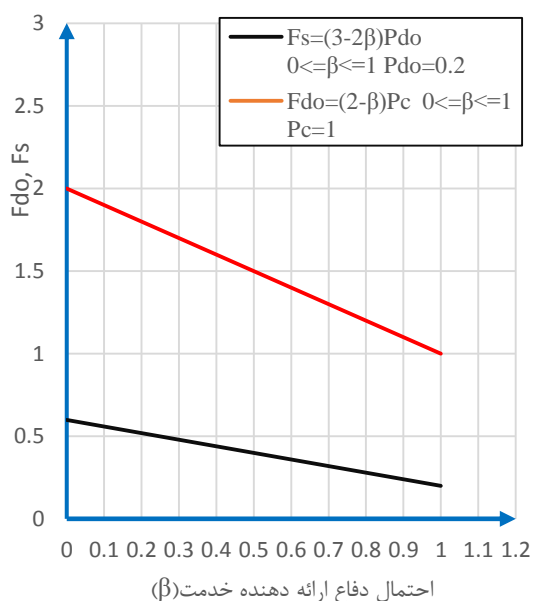
β	۰	۰/۱	۰/۲	۰/۳	۰/۴	۰/۵
$F_{do} \geq$	۲	۱/۹	۱/۸	۱/۷	۱/۶	۱/۵
$F_s \geq$	۲/۴	۲/۲۴	۲/۰۸	۱/۹۲	۱/۷۶	۱/۶
β	۰/۵	۰/۶	۰/۷	۰/۸	۰/۹	-
$F_{do} \geq$	۱/۴	۱/۳	۱/۲	۱/۱	۱	-
$F_s \geq$	۱/۴۴	۱/۲۸	۱/۱۲	۰/۹۶	۰/۸	-

همچنین می توان دید که اگر احتمال دفاع سرور خارجی (β) برابر با مقدار ۱ شود مقدار جریمه سرور خارجی برابر با مقدار $(P_{do}(Q))=0/8$ می شود. یعنی پولی که مالک داده بابت پردازش داده توسط سرور خارجی به ارائه دهنده خدمت پایگاه داده پرداخت می نماید.

نیست، اما به منظور تفسیر و درک بهتر، ما این روش را بر اساس مقادیر مختلف احتمال دفاع سرور (β)، $P_c(Q)$ و $P_{do}(Q)$ سپس جایگذاری این مقادیر در فرمول های به دست آمده، جریمه سرور و مالک داده را محاسبه می کنیم. هدف ما از پیاده سازی بررسی اثر مقادیر مختلف گفته شده در بالا در میزان جریمه سرور و مالک داده و استفاده از این تفاسیر هنگام انعقاد قرارداد برون سپاری است، بنابراین، نوع حملات دشمن و میزان از دست رفتن نتایج پرس و جو در این پیاده سازی مدنظر نیست. مطابق جدول (۱) و بر اساس مقادیر داده شده به احتمال β جریمه مالک داده (F_{do}) و جریمه سرور خارجی (F_s) را به دست می آید. لازم به یادآوری است که شرط بازی عبارت بود از $P_c(Q) \geq P_{do}(Q)$. یعنی لازمه آن که

همان گونه که از جداول فوق قابل مشاهده است؛ با افزایش احتمال دفاع سرور خارجی در برابر حملات دشمن، مقادیر جریمه مالک داده و سرور خارجی روبه کاهش است تا جایی که اگر احتمال دفاع سرور خارجی (β) برابر با مقدار ۱ شود مقدار جریمه مالک داده برابر با مقدار ۱ ($P_c(Q)$) می گردد. یعنی پولی که مشتری بابت استفاده از داده وی به او پرداخت می نماید.

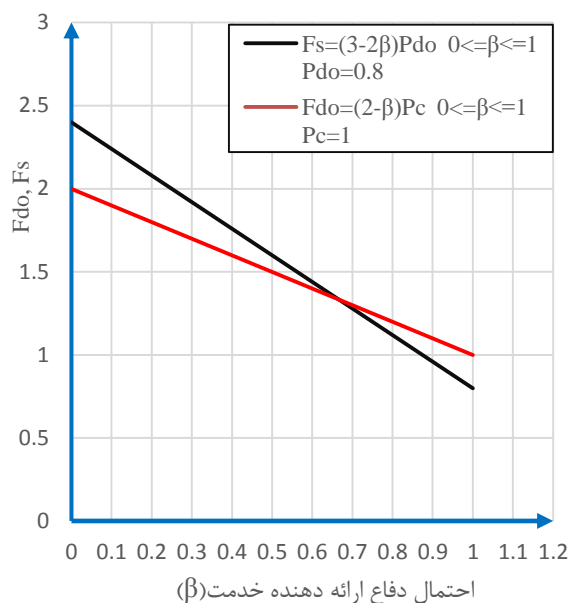
داده را برحسب مقدار احتمال دفاع ارائه‌دهنده خدمت پایگاه داده نشان می‌دهند. محور افقی نشان‌دهنده مقدار احتمال دفاع ارائه‌دهنده خدمت پایگاه داده از سرور خارجی (β) در برابر حملات دشمن و محور عمودی مقدار جریمه‌های مالک داده (F_s) و سرور خارجی (F_d) می‌باشند. خط قرمز رنگ بیانگر نمودار تابع جریمه مالک داده برحسب مقدار احتمال دفاع ارائه‌دهنده خدمت پایگاه داده در برابر حملات دشمن و خط سیاه رنگ نمودار تابع جریمه سرور خارجی برحسب مقدار احتمال دفاع ارائه‌دهنده خدمت پایگاه داده از او در برابر حملات دشمن می‌باشد.



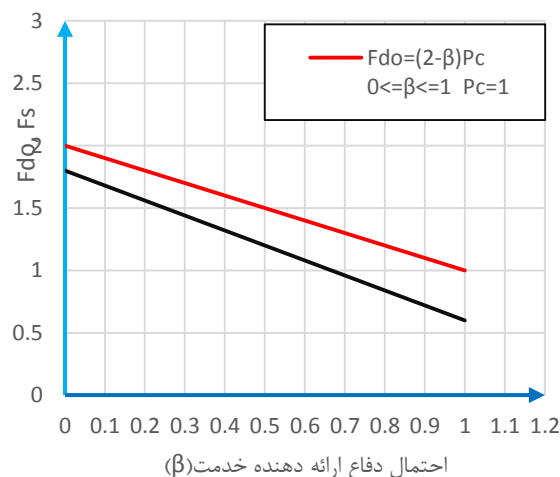
نمودار (۳): توابع جریمه مالک داده و سرور خارجی با توجه $P_{do}(Q) = 0.2$ و $P_c(Q) = 1$

با دقت در نمودارهای بالا می‌توان دریافت با افزایش مقدار احتمال دفاع سرور خارجی در برابر حملات دشمن مقادیر جریمه‌های مالک داده و سرور خارجی در حال کاهش است. به عبارت دیگر، هرچه قدر ارائه‌دهنده خدمت پایگاه داده در برقراری امنیت سرور خارجی دقت نماید، جریمه کم‌تری را خواهد پرداخت تا جایی که اگر احتمال دفاع سرور خارجی برابر ۱ گردد، آنگاه ارائه‌دهنده خدمت پایگاه داده جریمه‌ای را نخواهد پرداخت. البته نمودارهای بالا نشان می‌دهند که اگر احتمال دفاع سرور خارجی در برابر حملات دشمن برابر ۱ شود مقدار جریمه‌ها صفر نمی‌شوند، این موضوع با توجه به فرمول به دست آمده برای جریمه‌های مالک داده و سرور خارجی حاکی از زیاده‌خواهی به ترتیب مشتری و مالک داده است که واضح است هیچ‌یک از

این در حالی است که در حالت دفاع کامل سرور خارجی در برابر حملات دشمن باید مقادیر جریمه‌ها برابر صفر می‌گردیدند. این تناقض نتایج به خاطر منفعت‌طلبی مالک داده و مشتری است در صورتی که در واقع در این حالت جریمه‌ای پرداخت نخواهد شد. حال سعی می‌گردد به تحلیلی بر پایه نمودار توابع جریمه‌ها بر اساس تغییر احتمال دفاع سرور خارجی (β) با توجه به مقدار $P_c(Q)=1$ و مقادیر مختلف $P_{do}(Q)$ (به‌طور نمونه مقادیر 0.8 و 0.6 و 0.2) به صورت زیر دست‌یافت.



نمودار (۱): توابع جریمه مالک داده و سرور خارجی با توجه $P_{do}(Q) = 0.8$ و $P_c(Q) = 1$



نمودار (۲): توابع جریمه مالک داده و سرور خارجی با توجه $P_{do}(Q) = 0.6$ و $P_c(Q) = 1$
نمودارهای بالا مقدار جریمه سرور خارجی و جریمه مالک

را به جریمه سرور افزوده‌ایم و با اعمال تأثیر آن را بر رفتار سرور به عملیاتی‌تر شدن مدل کمک کنیم. هم‌چنین ما با مشخص کردن محدوده جریمه‌ها که یک موضوع اساسی در تنظیم قرارداد با سرور است کمک شایانی به کسانی قصد استفاده از این مدل برای برون سپاری را دارند، کرده‌ایم. با پیاده‌سازی این روش و تحلیل محدوده جریمه‌ها درستی این مطلب نیز بررسی شد. با توجه به مطالب گفته‌شده در بالا این مدل بازی یک مدل کاملاً عملیاتی از شرایط برون سپاری ارائه می‌کند و تنظیم قرارداد بر اساس این مدل کاملاً منطقی است.

۵-۲- بحث

از آنچه در بالا بیان شد می‌توان نتیجه گرفت که با زیاد شدن اختلاف $Pdo(Q)$ از $Pc(Q)$ (مثلاً وقتی که $Pdo(Q)$ برابر 0.7 و $Pc(Q)$ برابر با 1 باشد) مقدار جریمه سرور خارجی (F_s) از جریمه مالک داده (F_d) بسیار کم‌تر می‌گردد. این موضوع انگیزه مالک داده را در کنترل و بررسی پرس و جوها روی سرور خارجی افزایش می‌دهد و اطمینان از نتایج پرس و جوها را کاربران را بالا می‌برد زیرا جریمه‌ای که مالک داده دریافت می‌کند نه تنها تکافوی سود از دست‌رفته او را نخواهد داد بلکه جبران جریمه‌ای که باید به مشتری‌اش بپردازد نیز نخواهد بود، اما مالک داده به دلیل آن که موجودی سودجوست دوست دارد جریمه‌ای که از سرور خارجی دریافت می‌نماید حداقل مساوی جریمه‌ای باشد که به مشتری می‌پردازد (یعنی $F_s \geq F_d$). بنابراین، خواهیم داشت:

$$F_s \geq F_d \quad (33)$$

$$3Pdo(Q) - 2\beta Pdo(Q) \geq 2Pc(Q) - \beta Pc(Q)$$

$$(3-2\beta) Pdo(Q) \geq (2-\beta) Pc(Q)$$

$$Pc(Q) Pdo(Q) \geq \frac{2-\beta}{3-2\beta}$$

رابطه بالا نشان می‌دهد که برای آن که جریمه سرور خارجی در همه مقادیر احتمال β از مقدار جریمه مالک داده بیشتر باشد، مالک داده باید در محاسبه جریمه سرور خارجی در متن قرارداد منعقد با ارائه‌دهنده خدمت پایگاه داده رابطه (۳۳) را مدنظر قرار دهد. به عبارت دیگر، در زمان محاسبه جریمه سرور خارجی، مالک داده باید با چانه‌زنی برای جبران خسارت پرداختی به مشتری، مقدار پولی که به ارائه‌دهنده پایگاه داده بابت پردازش پرس و جوها مشتری می‌پردازد را حداقل برابر با $\frac{2-\beta}{3-2\beta} Pc(Q)$ در نظر بگیرد. با جایگزینی رابطه بالا در فرمول جریمه ارائه‌دهنده خدمت پایگاه داده (رابطه ۳۱)، جریمه سرور خارجی به شکل زیر به دست می‌آید:

$$F_s(Q) \geq \frac{2\beta^2 - 7\beta + 6}{3-2\beta} Pc(Q) \quad (34)$$

بازیکنان مالک داده و ارائه‌دهنده خدمت پایگاه داده زیر بار چنین جریمه‌ای در صورت برقراری امنیت سرور خارجی نخواهند رفت. موضوع دیگری که با توجه به نمودارهای بالا می‌توان نتیجه گرفت این است که معمولاً مقدار جریمه مالک داده، جریمه‌ای که مالک داده باید در برابر سهل‌انگاری و کوتاهی ارائه‌دهنده خدمت پایگاه داده در تأمین امنیت سرور خارجی به مشتری بپردازد، از مقدار جریمه سرور خارجی، جریمه‌ای که ارائه‌دهنده خدمت پایگاه داده باید در قبال عدم انجام تعهداتش به مالک داده بپردازد، بیش‌تر است. این امر طبیعی است زیرا جریمه مالک داده بر اساس مقدار $Pc(Q)$ محاسبه می‌گردد در حالی که جریمه سرور خارجی بر اساس مقدار $Pdo(Q)$ به دست می‌آید و همان‌گونه که می‌دانیم رابطه $Pc(Q) \geq Pdo(Q)$ از قبل جزو شروط بازی بوده است. البته همان‌طور که از نمودارهای (۳-۱) می‌توان مشاهده نمود برای بعضی از مقادیر β که $Pdo(Q)$ نزدیک به مقدار $Pc(Q)$ باشد مقدار جریمه مالک داده کوچک‌تر از مقدار جریمه سرور خارجی خواهد بود. در هر حال، موضوع بیشتر بودن مقدار جریمه مالک داده از مقدار جریمه سرور خارجی، موجب خواهد شد مالک داده همیشه به وظیفه خود یعنی سپردن داده به ارائه‌دهنده خدمت پایگاه داده‌ای که امنیت بیش‌تری برای سرور خارجی فراهم می‌نماید و هم‌چنین کنترل و بررسی همیشگی نتایج پرس و جو روی پایگاه داده برون سپاری شده جهت اطمینان از جامعیت پاسخ‌ها بپردازد و عاملی که او را در این مسیر جلو می‌برد ترس از پرداخت جریمه‌ای است که باید در صورت خطای ارائه‌دهنده خدمت پایگاه داده در تأمین امنیت سرور خارجی به مشتری‌اش بپردازد. جریمه‌ای که نه تنها تکافوی سود از دست‌رفته او را نخواهد داد، بلکه جبران جریمه‌ای که باید به مشتری‌اش بپردازد نیز نخواهد بود.

یک تفاوت اساسی بین روش پیشنهادی با سایر مقالات که در کارهای مرتبط این است که آن‌ها از وارد کردن دشمن در بازی به عنوان یک بازیگر پرهیز کرده‌اند و بازی را به نحوی مدل کرده‌اند که جلوی تقلب سرور در استفاده از زیرساخت‌ها را بدون حضور دشمن می‌گیرند. بنابراین، امکان حضور دشمن و خرابی و دست‌کاری اطلاعات توسط او را در نظر نگرفته‌اند. از نظر ما در نظر نگرفتن حضور دشمن و تأثیر آن بر شرایط بازی، غیرمنطقی و غیرواقعی است. بنابراین، ما با وارد کردن دشمن در بازی و حضور احتمالاتی آن، یک مدل واقعی و عملیاتی ارائه کردیم.

تفاوت دیگر این روش با سایر روش‌ها این است که آن‌ها هزینه بازیابی اطلاعات مشتری در صورت نفوذ دشمن در سرور، که به سرور تحمیل می‌شود را در نظر نگرفته‌اند اما ما این هزینه

در روش ارائه شده با در نظر گرفتن مدل احتمالی برای حمله دشمن و متقابلاً مدل احتمالی برای دفاع ارائه دهنده خدمت پایگاه داده بازی برون سپاری پایگاه داده برون سپاری شده به صورت یک بازی ایستای مختلط تعریف گردید. در این بازی با محاسبه سود هر یک از بازیکنان در نهایت جریمه‌هایی برای هر یک از بازیکنان ارائه دهنده خدمت پایگاه داده و مالک داده به دست آمدند. این جریمه‌ها عامل اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده می‌باشند. مقدار این جریمه‌ها در حدی است که افراد سودجویی مانند ارائه دهنده خدمت پایگاه داده و مالک داده به دنبال فرار از پرداخت آن می‌باشند و در نتیجه ارائه دهنده خدمت پایگاه داده سعی می‌کند در برقراری امنیت سرور خارجی نهایت تلاش و کوشش خود را به کار گمارد و مالک داده نیز سعی می‌کند در کنترل و بررسی نتایج پرس و جوها روی پایگاه داده برون سپاری شده نهایت تلاش و کوشش خود را به کار گیرد. این همان نتیجه مطلوبی است که به دنبال آن هستیم.

۷- کارهای آینده

از جمله کارهای آینده می‌تواند بررسی اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده به چند سرور خارجی و همچنین تحت مالکیت چند مالک داده باشد. به طوری که هر کدام از سرورهای خارجی انگیزه‌های متفاوتی برای برقراری امنیت پایگاه داده دارند. چه بسا هر کدام از مالکان داده نیز انگیزه متفاوتی برای کوتاهی در کنترل و بررسی نتایج پرس و جوها روی پایگاه داده برون سپاری شده دارند. همچنین می‌توان انواع حملات مختلف که جامعیت پایگاه داده برون سپاری شده را تهدید می‌کنند را با احتمالات وقوع متفاوت در نظر گرفت.

همه این موارد می‌توانند بر اساس تئوری بازی، مورد بررسی قرار گیرند، به طوری که با محاسبه سود و زیان بازیکنان راه‌حلی برای اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده به دست آیند. این موضوعات گوشه‌ای از کارهایی است که می‌توانند مبتنی بر نظریه بازی به حل چالش‌های برون سپاری پایگاه داده پرداخت.

۸- تشکر و قدردانی

در تهیه و تنظیم این مقاله جناب آقای یحیی لرمحمدحسینی دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین (ع) زحماتی را متقبل شدند که بدین وسیله از ایشان تشکر و قدردانی می‌شود.

در صورتی که مالک داده بخواهد جریمه دریافتی از سرور خارجی تکافوی جریمه پرداختی به مشتری را بدهد، مالک داده می‌بایست جریمه سرور خارجی را در متن قرارداد منعقد شده با ارائه دهنده خدمت پایگاه داده حداقل برابر با رابطه (۳۴) محاسبه نماید. البته این موضوع شاید مورد پذیرش ارائه دهنده خدمت پایگاه داده نباشد زیرا جریمه سرور خارجی مطابق رابطه بالا بر اساس مقدار $Pc(Q)$ محاسبه شده است. در حالی که ارائه دهنده خدمت پایگاه تمایل دارد جریمه خود را بر اساس مقدار $Pdo(Q)$ محاسبه نماید. موفقیت مالک داده در این زمینه بستگی به قدرت چانه زنی او خواهد داشت.

در این بخش، روشی که برای اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده در بخش گذشته به طور کامل بیان گردید، مورد ارزیابی قرار گرفت. در این بخش نشان داده شد که جریمه‌های پیش‌بینی شده برای ارائه دهنده خدمت پایگاه داده و مالک داده به درستی انگیزه تخلف را از انجام وظیفه آنان از بین می‌برد. در خاتمه نیز اشاره گردید برای آن که مالک داده در هنگام کوتاهی ارائه دهنده خدمت پایگاه داده بابت اختلاف جریمه دریافتی از او و همچنین جریمه پرداختی به مشتری متضرر نگردد می‌بایست در قرار منعقد شده با ارائه دهنده خدمت پایگاه داده، جریمه سرور خارجی را از رابطه (۳۳) محاسبه نماید اما این موضوع انگیزه مالک داده را در کنترل و بررسی پرس و جوها روی پایگاه داده برون سپاری شده کاهش می‌دهد.

۶- نتیجه گیری

در این مقاله، برون سپاری پایگاه داده و چالش‌های مربوط به آن مورد بررسی قرار گرفت و سپس با معرفی تئوری بازی به عنوان دانش مطالعه رقابت‌ها تلاش گردید برای چالش "اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده" بر اساس تئوری بازی راه‌حلی ارائه گردد. در روش ارائه شده برون سپاری پایگاه داده با یک نگاه امنیتی به شکل یک بازی با حضور چهار بازیکن (دشمن، ارائه دهنده خدمت پایگاه داده، مالک داده و کاربر) تعریف گردید. در واقع نگاه ما به چالش "اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده" در بازی برون سپاری پایگاه داده به انگیزه‌های منفعت طلبانه هریک از بازیکنان بوده است. در این مقاله با در نظر گرفتن انگیزه‌های منفعت طلبانه بازیکنان سعی گردید روشی ارائه گردد که با از بین بردن انگیزه هریک از بازیکنان در کوتاهی از انجام وظایف خود، اطمینان از نتایج پرس و جوها روی پایگاه داده برون سپاری شده را به دست دهد.

۹- مراجع

- [15] M. Hassan, B. Song, and E.-N. Huh, "Distributed resource allocation games in horizontal dynamic cloud federation platform," in Proceedings of the 13th International Conference on High Performance Computing and Communications (HPCC), pp. 822–827, 2011.
- [16] X. Zheng, P. Martin, W. Powley, and K. Brohman, "Applying bargaining game theory to web services negotiation," in 2010 IEEE International Conference on Services Computing (SCC), pp. 218–225, 2010.
- [17] A. Gueye and V. Marbukh, "A game-theoretic framework for network security vulnerability assessment and mitigation," in Decision and Game Theory for Security, pp. 186–200, 2012.
- [18] T. Alpcan and T. Basar, "Network Security: A Decision and Game-Theoretic Approach," Cambridge University Press, 2010.
- [19] M. H. Manshai, Q. Zhu, T. Alpcan, T. Basar, and J. Hubaux, "Game theory meets network security and privacy," ACM Trans. Comput. Logic, vol. 5, pp. 1–35, 2010.
- [20] K.-w. Lye and J. M. Wing, "Game strategies in network security," Int. J. Inf. Sec., vol. 4, pp. 71–86, 2005.
- [21] M. Felegyhazi and J. P. Hubaux, "Game Theory in Wireless Networks: A Tutorial," In EPFL technical report, LCA-REPORT-2006.
- [22] L. Chen and J. Leneutre, "A game theoretical framework on intrusion detection in heterogeneous networks," IEEE Transactions on Information Forensics and Security, vol. 4, no. 2, pp. 165–178, 2009.
- [23] Z. Ismail, C. Kiennert, J. Leneutre, and L. Chen, "Auditing a Cloud Provider's Compliance with Data Backup Requirements: A Game Theoretical Analysis," IEEE Transactions on Information Forensics and Security, pp. 155–170, 2016.
- [24] B. Djebaili, C. Kiennert, J. Leneutre, and L. Chen, "Data integrity and availability verification game in untrusted cloud storage," in Proceedings of the 5th International Conference on Decision and Game Theory for Security (GameSec), pp. 287–306, 2014.
- [25] V. Pham, MHR. Khouzani, and C. Cid, "Optimal Contracts for Outsourced Computation," pp. 1–20, 2014.
- [26] B. Djebaili, C. Kiennert, J. Leneutre, and L. Chen, "Data Integrity and Availability Verification Game in Untrusted Cloud Storage," GameSec, pp. 287–306, 2014.
- [27] R. Nix and M. Kantarcioglu, "Contractual Agreement Design for Enforcing Honesty in Cloud Outsourcing," GameSec, pp. 296–308, 2012.
- [1] P. Samarati and S. De Capitani di Vimercati, "Data protection in outsourcing scenarios: Issues and directions," in Proc. of ASIACCS 2010, Beijing, China, April, 2010.
- [2] R. Nix and M. Kantarcioglu, "Efficient Query Verification on Outsourced Data: A Game-Theoretic Approach," CoRR abs/1202.1567, 2012.
- [3] "Handbook on Securing Cyber-Physical Critical Infrastructure," DOI: 10.1016/B978-0-12-415815-3.00027-3 677- 2012, Elsevier Inc, 2012.
- [4] M. Ghayoori Sales, M. Haghjoo, K. Salmani, "Completeness Auditing of Continuous Query Results", Journal of Passive Defence Science and Technology, vol.2, pp. 217_230, 2011. In persian
- [5] M. Ghayoori Sales, M. Haghjoo, K. Salmani, "Detecting Integrity Attacks to a Data Stream Management System", Journal of Passive Defence Science and Technology, vol.2, pp. 70-75, 2011. In persian
- [6] GH.Abdoli, "Game Theory and its Applications", SID Publications, Tehran, vol.2, 2009. In persian
- [7] B. Padmavathi and A. R. Pathak, "Survey of Confidentiality and Integrity in Outsourced Databases," International Journal of Scientific Engineering and Technology, Volume 2 Issue 3, pp. 122-128, 2013.
- [8] Q. Zheng, S. Xu, and G. Ateniese, "Efficient query integrity for outsourced dynamic databases," CCSW, pp. 71-82, 2012.
- [9] D. T. Khanh, "Security Protocols for Outsourcing Database Services," Information & Security: An International Journal, ProCon Ltd., Sofia, ISSN 1311-1493, vol. 18, 2005.
- [10] S. Papadopoulos, D. Papadias, W. Cheng, and K.-L. Tan, "Separating Authentication from Query Execution in Outsourced Databases," Proc. IEEE 25th Int'l Conf. Data Eng. (ICDE), 2009.
- [11] R. Popa, J. Lorch, D. Molnar, H. Wang, and L. Zhuang, "Enabling Security in cloud storage SLAs with Cloud Proof," in Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference, Ser. USENIXATC'11, pp. 31–31, 2011.
- [12] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, pp. 1–9, 2010.
- [13] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. Yau, "Efficient provable data possession for hybrid clouds," in Proceedings of the 17th ACM Conference on Computer and Communications Security, ser. CCS 10, pp. 756–758, 2010.
- [14] J. Yang, H. Wang, J. Wang, C. Tan, and D. Yu, "Provable data possession of resource-constrained mobile devices in cloud computing," JNW, vol. 6, no. 7, pp. 1033–1040, 2011.

A Method to Ensure the Results of Queries on the Outstanding Database Based on the Game Theory

M. Goorani , M. Ghayoori Sales*

*Imam Hossein University

(Received: 03/08/2015, Accepted: 03/01/2017)

ABSTRACT

The widespread use of the web and development of ICT led to the emergence of a new trade called "database as a service." In this competitive environment, individuals and organizations who find it difficult to manage and maintain their database hire companies that can provide extensive services in the field. Great effort has been made to ensure the integrity of the results of queries on outsourced databases, and a variety of methods have been proposed. However, what is shared between all these methods is that all solutions are offered with high financial considerations by those in the outsourced database business environment. This paper introduces database outsourcing as a business game with four major players: external server, data owner, user and enemy with financial and non-financial interests. It then proceeds to present a way, using the Game Theory, to ensure the integrity of the results of the queries on outsourced databases. This method considers the financial and non-financial interests of the players to be a threat to the integrity of the results of queries, and provides a solution to eliminate this threat. It is believed that this paper can provide useful guidelines for each of the participating parties in business contracts related to database outsourcing, from the service provider to the data owner and the customer.

Keywords: Outsourced Database, Game Theory, Query Results Integrity