مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال پنجم، شماره ۲، تابستان ۱۳۹۶، ص ۱۸ -۱

روشی برای اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری 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 به‌عنوان 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 پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده از چالش‌های موجود در این زمینه بوده است. تاکنون تلاش‌های فراوانی برای حصول اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده به‌عمل آمده‌اند و راه‌حل‌های مختلفی ارائه گردیده‌اند امّا آنچه در همه آن‌ها مشترک است، ارائه راه‌کار با حفظ انگیزه‌های شدید مادی و معنوی عوامل دخیل در محیط تجاری برون‌سپاری پایگاه داده است. در این مقاله، برون‌سپاری پایگاه داده به‌صورت بازی تجاری که در آن چهار عامل سرور خارجی، مالک داده، کاربر و دشمن با انگیزه‌های مختلف مادی و معنوی حضور دارند، درنظر گرفته شده و براساس تئوری بازی روشی برای اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده پیشنهاد می‌گردد. در روش ارائه‌شده، وجود انگیزه‌های مادی و معنوی متفاوت در بازیکنان به‌عنوان عامل تهدید جامعیت نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری شده معرفی گردیده است و راه‌حلی برای از بین‌بردن آن ارائه گردیده است. پندار ما این است که مطالعه این مقاله می‌تواند راه‌گشای هر یک از افراد شرکت‌کننده در برون‌سپاری پایگاه داده -ارائه‌دهنده خدمت پایگاه داده، مالک داده و مشتری- در انعقاد قراردادهای تجاری در این زمینه خواهد بود.

واژه‌های کلیدی: پایگاه داده برون‌سپاری شده، تئوری بازی، جامعیت نتایج پرس‌وجوها.

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 به‌کمک خدمت‌های فراهم‌شده توسط سرورهای خارجی شده‌اند [۱].

برون‌سپاری[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 که‌از آن پس مسؤولیت ذخیره‌سازی، مدیریت و ارائه داده را بر عهده خواهند گرفت [۲].

برون‌سپاری پایگاه داده معمولاً به‌نام پایگاه داده به‌عنوان خدمت[۲] شناخته می‌شود. اگرچه برون‌سپاری داده مزایای فراوانی به‌ویژه برای آن دسته از کاربرانی که منابع محدودی برای مدیریت داده درحال افزایش خویش دارند ولی نگرانی‌های امنیتی جدیدی را به وجود می‌آورد.

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

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

1 -Outsourcing

2 -Database as service (DAS)

3- Data integrity

Archive of SID

www.SID.ir

۱- راه‌حل‌های مبتنی بر ساختار تصدیقی[1]: در این‌جا ساختمان داده مناسبی تعریف می‌شود مانند زنجیره امضاء[2]، درخت درهم‌ساز مرکل[3] و لیست پرش[4]. این راه‌حل‌ها؛ تمامیت نتایج پرس‌وجوهایی که روی صفتی صورت می‌پذیرد، تضمین می‌نماید.

۲- راه‌حل‌های مبتنی بر ساختار احتمالاتی[5]: مبتنی بر درج دیده‌بان‌هایی در داده برون‌سپاری‌شده 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 واگذارشده 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[6] 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 برون‌سپاری‌شده 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 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 هرجا 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 برون‌سپاری‌شده 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 [۹-۸] روش‌هایی برای بررسی جامعیت به منظور اجرای پرس‌وجوهای پیچیده توسط

1- Authenticated data structures approaches
2- Signature chaining
3- Mercle Hash tree
4- Skip list
5- Probabilistic approaches
6- Service

Archive of SID

www.SID.ir

مشتری و برقراری تعادل بین پیچیدگی محاسباتی و ارتباطی پیشنهاد شده است. در[۱۰] نیز روشی برای اطمینان از صحت، تازگی و جامعیت داده‌های برون‌سپاری شده در ابر پیشنهاد شده که از رمزنگاری برای شناسایی و اثبات رفتار نامناسب خدمت‌دهنده ابر استفاده می‌کند. در [۱۱] یک روشی برای اثبات برآورده‌کردن 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 [۱۴-۱۳] نیز روش‌هایی پیشنهاد شده است که مالک داده یک سری ابرداده از داده‌های خود به‌منظور اعتبارسنجی نتایج پرس و جوها استفاده می‌کند. اما در سال‌های اخیر، استفاده از نظریه بازی‌ها به‌منظور تحلیل تعاملات بین بازیگران محیط ابر بسیار مورد توجه قرار گرفته است و مسائل مختلفی ازقبیل اختصاص و مدیریت منابع [۱۵]، مذاکره خدمت ابر[۱۶] پیشنهاد شده است. ناگفته نماند نظریه بازی‌ها در حوزه‌هایی ازقبیل 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 برآورده‌شدن نیازمندی‌های پشتیبان‌گیری داده توسط خدمت‌دهنده ابر: یک تحلیل نظریه بازی" که بهبودیافته کار خودشان در سال ۲۰۱۴ بوده است [۲۴]، ارائه کردند. در این مقاله، مشتری N مجموعه داده را روی یک ابر برون‌سپاری می‌کند و فرآیند اعتبارسنجی دسترس‌پذیری داده‌ها را به شخص سوم (TPA) می‌سپارد. سپس، مسئله را به‌عنوان یک بازی ایستا غیرمشارکتی با دو بازیگر خدمت‌دهنده ابر و TPA مدل کرده‌اند. آن‌ها مسئله را با حضور دو بازیگر مدل کرده‌اند و از دخیل‌کردن دشمن و صاحب داده‌ها و منافع آن‌ها خودداری کرده‌اند در حالی‌که ما با دخیل‌کردن این بازیگران، بازی را به‌صورتی مدل کرده‌ایم که بسیار به شرایط دنیای واقعی نزدیک و درنتیجه کاربردی‌تر است.

در سال ۲۰۱۲، روبرت نیکس و همکارش، مقاله‌ای را با عنوان " کنترل و بررسی کارآمد پرس‌وجو روی داده برون‌سپاری‌شده با استفاده از تئوری بازی " ارائه داده‌اند [۲]. آن‌ها در مقاله خود، بحث را با لزوم عمل بررسی نتایج پرس‌وجو روی پایگاه داده برون‌سپاری‌شده آغاز کرده‌اند. سپس، به چالش جامعیت داده برون‌سپاری‌شده از منظر تئوری بازی پرداخته‌اند. به اعتقاد آن‌ها، هیچ‌کدام از روش‌های موجود برای اطمینان از جامعیت نتیجه پرس‌وجو روی پایگاه داده برون‌سپاری‌شده مانند امضای رکوردها کانون مشکلات یعنی منفعت‌طلبی عوامل شریک در برون‌سپاری 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 درنظر گرفته‌اند که وظیفه کنترل و بررسی روی نتایج پرس‌وجوها را نیز خود مالک داده برعهده دارد. با استفاده از تئوری بازی و حل بازی بالا، الگویی برای انعقاد قراردادهای برون‌سپاری داده -بین مالک داده و ارائه‌دهنده خدمت پایگاه داده- به‌دست آمده است. درحالی‌که در این مقاله بازی برون‌سپاری پایگاه داده با حضور چهار بازیکن مالک داده، ارائه‌دهنده خدمت پایگاه داده، مشتری و دشمن با انگیزه‌ها و اهداف تجاری متفاوت درنظر گرفته می‌شوند. در واقع، برون‌سپاری پایگاه داده با یک نگاه امنیتی (با درنظر گرفتن دشمن) به‌صورت 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 به‌خطرافتادن جامعیت داده؛ سه بازیکن دیگر چگونه باید بازی را ادامه دهند تا منافع آنان محفوظ بماند. در این مقاله، براساس 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 پرس‌وجو روی پایگاه داده برون‌سپاری‌شده را به‌دست خواهد داد. در [۲]، مشتری را به بازی وارد نکرده است درحالی‌که 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. به‌همین دلیل، این عملیات و هم‌چنین عملیات امضا قرارداد را به مالک داده می‌سپارند، پس حضور مشتری در بازی برون‌سپاری 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 دست‌کاری اطلاعات توسط او را مدل نکرده‌اند. مدل ما به‌نحوی طراحی شده است که جلو تقلب سرور را با حضور دشمن می‌گیرد. این‌که چرا آن‌ها این دو بازیکن را به بازی وارد نکرده‌اند، به‌دلیل فرضیات آن‌ها از مسئله بوده است و تغییراتی که اثر واردکردن این دو بازیکن به سناریو مقاله [۲] ایجاد می‌شود به دیدگاه نویسنده

Archive of SID

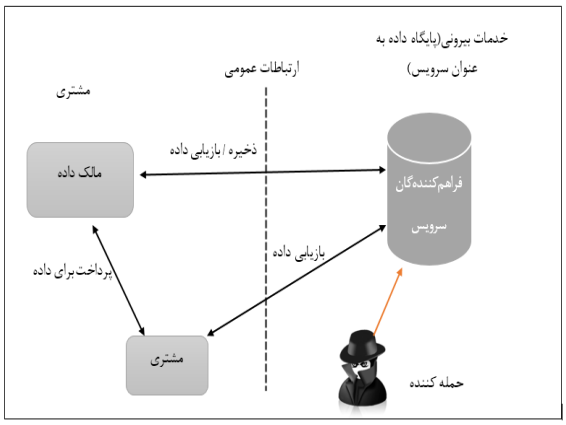
www.SID.ir

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 جریمه‌کردن و جایزه‌دادن به فراهم‌کننده داده و مشخص‌کردن 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 درحالی‌که 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 جریمه‌کردن آن‌ها درصورت تقلب سعی در تحریک آن‌ها برای انجام محاسبات درست را دارد. این مدل نیز از مدل‌کردن 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، درحالی‌که 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 درحالی 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 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 به‌خطرافتادن 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 به‌وجودآمدن آسیب‌پذیری سرور خارجی گردد. انگیزه ارائه‌دهنده خدمت پایگاه داده می‌تواند مادی باشد و برای صرفه‌جویی اقتصادی و اختصاص امکانات جهت پردازش‌های دیگر (برای به‌دست‌آوردن پول بیش‌تر) امنیت کافی را برای سرور خارجی فراهم ننماید. از آن‌جایی‌که 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 بین‌بردن انگیزه ارائه‌دهنده خدمت پایگاه داده در سهل‌انگاری و کوتاهی در انجام تعهداتش است. از آن‌جایی‌که در بازی برون‌سپاری پایگاه داده با چهار بازیکن مالک داده، کاربر، سرورخارجی و دشمن برخورد انگیزه‌ها موجب بروز مشکل است با استفاده از تئوری بازی و برمبنای 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

Archive of SID

www.SID.ir

جلوگیری از نفوذ دشمن تقویت می‌نماید. بدین منظور، یک‌سری مفروضات اولیه به‌شرح ذیل درنظر گرفته می‌شوند:

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 می‌باشد، به یک ارائه‌دهنده خدمت پایگاه داده می‌سپارد و نسبت به معرفی مشتریانش به این شرکت اقدام می‌نماید.

۲- ارائه‌دهنده خدمت پایگاه داده: با انعقاد قرارداد رسمی که قابل طرح در مراجع قانونی خواهد بود، با دریافت پول، عهده‌دار مدیریت و نگه‌داری پایگاه داده مالک داده شده و وظیفه تامین امنیت پایگاه داده در شبکه عمومی و ارائه پاسخ‌های جامع (صحیح، تمام و تازه) به پرس‌وجوهای مشتریان را برعهده می‌گیرد. هم‌چنین این شرکت متعهد می‌گردد که خدمتی پایدار ارائه دهد به‌طوری‌که 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- حمله‌کننده (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، ارائه‌دهنده خدمت پایگاه داده را در ارائه پاسخ جامع به پرس‌وجوهای مشتریان و خدمتی پایدار ناتوان نماید.

۵- ارائه‌دهنده خدمت پایگاه داده: از جهت حفظ امانت داده و ارائه خدمت پایدار به مشتریان، قابل اعتماد بوده و خود درصدد تغییر محتوای پایگاه داده برنمی‌آید ولی ممکن است بنابه دلایل اقتصادی سهل‌انگاری نماید و تمهیدات امنیتی لازم را برای جلوگیری نفوذ دشمن به‌کار نگیرد. درنتیجه دشمن با سوءاستفاده از رخنه ایجادشده سعی می‌نماید سرور خارجی را از کار انداخته یا با سرقت اطلاعات روی آن و جایگزینی با اطلاعات جعلی، ارائه‌دهنده خدمت پایگاه داده را در ارائه خدمت پایدار و پاسخ‌های جامع به پرس‌وجوهای مشتریان ناتوان سازد.

۶- نحوه اجرای پرس‌وجوها: توسط سرور و روشی که مالک داده، سرور خارجی و کاربر برای احراز هویت و جامعیت پاسخ به پرس‌وجوها به‌کار می‌گیرند، خارج از موضوع این مقاله می‌باشد.

۷- تعداد کاربران (مشتریان): تاثیری در روش پیشنهادی نخواهند داشت و همان‌گونه‌که بعداً خواهید دید هرچه تعداد مشتریان بیشتر باشد اطمینان از نتایج پرس‌وجوها بیش‌تر خواهد گردید.

برای سادگی بحث، فقط یک سرور خارجی و فقط یک مالک داده وجود دارند درحالی‌که روش ارائه‌شده قابل تعمیم به چند سرور و چند مالک داده نیز می باشد.

۴- روش پیشنهادی

روشی‌که در ادامه ارائه می‌گردد فارغ از نوع پرس‌وجوهای مشتریان می‌باشد و به روشی‌که مالک داده، سرور خارجی و مشتریان جهت حفظ جامعیت پاسخ پرس‌وجوها به‌کار می‌برند، وابسته نمی‌باشد. بلکه در این‌جا روشی پیشنهاد می‌گردد که انگیزه ارائه‌دهنده خدمت پایگاه داده را در عدم انجام تعهداتش مبنی بر ارائه خدمتی پایدار و پاسخ‌های جامع به پرس‌وجوهای مشتریان از بین می‌برد. شرکت ارائه‌دهنده خدمت پایگاه داده موجودی قابل اعتماد اما خردمند می‌باشد که برای کسب سود بیشتر، امکان دارد از تمام منابع سخت‌افزاری و نرم‌افزاری 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 هرکدام از معیارهای جامعیت[1] پاسخ‌ها به پرس‌وجوهای مشتریان (صحت[2]، تمامیت[3] و تازگی[4]) را به‌خطر اندازد و یا با از کار انداختن سرور خارجی مانع از پیوستگی خدمات سرور خارجی به مشتریان شود.

در این روش با درنظر گرفتن حمله احتمالی دشمن، سود و زیان هریک از بازیکنان محاسبه می‌گردد و می‌توان با توجه به این محاسبات، قرارداد برون‌سپاری پایگاه داده را طوری تنظیم نمود که انگیزه سرور خارجی را در عدم انجام تعهداتش و هرگونه سهل‌انگاری در برقراری امنیت سایت خویش از بین ببرد. این روش می‌تواند برای هرگونه حمله دشمن با توجه به میزان احتمال وقوع آن به‌کار گرفته شود.

۴-۱- مدل بازی

بازی برون‌سپاری پایگاه داده به‌صورت زیر تعریف می‌شود:

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

Archive of SID

www.SID.ir

۴-۱-۱- بازیکنان

چهار بازیکن به نام‌های مالک داده[1] (DO)، سرور خارجی[2] (S)، مشتری[3] (C) و حمله‌کننده[4] (A).

۴-۱-۲- فعالیت‌ها

مشتری پرس‌وجوی (Q) خود را به سمت سرور می‌فرستد و پاسخ Q (D) را دریافت می‌نماید. البته ممکن است مشتری در برابر پرس‌وجوی خویش پاسخ Q´ (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 Q´ (D) و یا عدم دریافت پاسخ موضوع را به اطلاع مالک داده می‌رساند و مطالبه خسارت می‌کند. مالک داده نیز با انجام بررسی و مشخص‌شدن قصور سرور خارجی در تامین امنیت کافی، طلب خسارت می‌نماید. بدیهی است میزان خسارت در قراردادهای منعقده 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 منعقده 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 آن‌جایی‌که دو حالت "نفوذ دشمن" و "عدم نفوذ دشمن" درنظر گرفته خواهند شد، بنابراین می‌توان راهبردهای بازیکنان را به دو صورت زیر درنظر گرفت:

(a، d، v و q): این بدین معنی است که (به ترتیب از چپ به راست) بازیکن مشتری درحال پرس‌وجو[5](q) است. بازیکن مالک داده درحال کنترل و بررسی[6] نتایج پرس‌وجوهاست (v). بازیکن سرور خارجی درحال دفاع در برابر حملات[7] دشمن است (d) و بازیکن دشمن درحال حمله به سرور خارجی[8] می‌باشد ولی موفق به نفوذ به آن نمی‌گردد (a).

(i، f، r و r): این بدین معنی است که (به ترتیب از چپ به راست) بازیکن مشتری به‌دنبال کسب جریمه[9] از مالک داده بوده (r) و پیرو آن بازیکن مالک داده نیز به‌دنبال کسب جریمه از ارائه‌دهنده خدمت پایگاه داده می‌باشد (r). بازیکن سرور خارجی نتوانسته است امنیت کافی را برقرار نماید و دچار شکست[10] شده است (f) و درنتیجه دشمن توانسته به‌راحتی به سرور خارجی نفوذ[11] نماید (i).

۴-۱-۵- سودها[12]

از آن‌جایی‌که 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 درنظر گرفتن مدل احتمالی حمله دشمن مجدداً سود بازیکنان محاسبه می‌شود و براساس نتیجه به‌دست‌آمده چگونگی انعقاد قرارداد میان بازیکنان توضیح داده خواهد شد به‌گونه‌ای‌که 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 به‌دلیل تامین امنیت مناسب از سوی ارائه‌دهنده

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

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

Archive of SID

www.SID.ir

خدمت پایگاه داده، نمی‌تواند به سرور خارجی نفوذ نماید. بنابراین، جامعیت داده روی آن حفظ می‌گردد و حتی خدمت پایگاه داده به‌طور پایدار ادامه خواهد یافت. با این توضیح سود بازیکنان به شرح زیر به‌دست خواهد آمد:

مشتری (کاربر) ارزش اطلاعاتی نتایج حاصل از پرس‌وجوها روی پایگاه داده را منهای هزینه‌ای که در این رابطه به مالک داده می‌پردازد، به‌دست می‌آورد. می‌توان 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 می‌دارد و در مقابل هزینه‌ای را بابت پردازش پرس‌وجو توسط سرور خارجی به او می‌پردازد. می‌توان سود این بازیکن را به شکل زیر نمایش داد:

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

ارائه‌دهنده خدمت پایگاه داده مبلغ پرداختی توسط مالک داده را دریافت داشته و با صرف هزینه سخت‌افزاری و نرم‌افزاری جهت پردازش پرس‌وجوی کاربر و حفظ امنیت سایت پاسخ لازم را به او خواهد داد. با این توضیح می‌توان سود سرور خارجی را به‌صورت 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 آن‌چه بازیکنان دریافت می‌دارند بیش‌تر از ارزش آن چیزی است که هزینه می‌کنند در غیر این صورت، بازی دیگر بین افراد خردمند برقرار نیست و سود برخی از بازیکنان از صفر کم‌تر خواهد شد و در صورت ادامه بازی به همین منوال دیگر اسم بازی را نمی توان روی آن گذاشت مگر آن‌که بازیکن با سود صفر (با دریافت یارانه) سعی می‌کند بازی را برای اهداف دیگر ادامه دهد.

در مدلی‌که در بالا توضیح داده شد سرور به‌درستی به تعهدات خود برای تامین امنیت سایت خویش اقدام نموده است و جلوی نفوذ حمله‌کننده را گرفته و در واقع پاسخ‌هایی که کاربر در برابر پرس‌وجوهایش دریافت می‌دارد همگی صحیح می‌باشند بنابراین سود حمله‌کننده به شکل زیر محاسبه می‌گردد:

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

این رابطه نشان می‌دهد موقعی که سرور خارجی بتواند با به‌کارگیری تمهیدات مناسب نسبت به تامین امنیت کافی اقدام نماید، حمله‌کننده نه تنها سودی به‌دست نمی‌آورد بلکه فقط بابت منابعی که جهت حمله و نفوذ به سرور خارجی صرف می‌کند هزینه‌ای می‌پردازد و این منطقی به‌نظر می‌رسد.

۴-۱-۵-۲- نفوذ دشمن

اما در دنیای واقعی وضع بدین گونه نیست، یعنی حمله‌کننده می‌تواند 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 پرس‌وجوهای کاربران داده‌های نادرست ارائه دهند. در این صورت، بازی به شکلی دیگر رقم خواهد خورد و لازم است سودهای بازیکنان مجدداً محاسبه گردد.

درصورت موفقیت‌آمیز بودن حمله دشمن و نفوذ او به سرور، سود حمله‌کننده به‌صورت زیر در می‌آید:

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

این رابطه بیان می‌دارد سودی که حمله‌کننده از نفوذ به سرور خارجی و از کار انداختن آن یا سرقت اطلاعات روی آن و درج اطلاعات نادرست روی آن به‌دست می‌آورد 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 می‌دهیم. اما دشمن جهت موفقیت خویش هزینه‌ای را بابت به‌کارگیری 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 خراب‌کاری به‌جامانده از آن مواجه می‌شود. از طرفی، بابت پاسخ‌های نادرستی که در برابر پرس‌وجوهای کاربران داده است می‌بایست جریمه‌ای را به مالک داده بپردازد. این جریمه در قرارداد منعقده بین مالک داده و ارائه‌دهنده خدمت پایگاه داده به‌طور شفاف بیان می‌گردد. با این توضیحات، سود ارائه‌دهنده پایگاه داده به‌شکل زیر محاسبه می‌شود:

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

این رابطه نشان می‌دهد که سود شرکت ارائه‌دهنده خدمت پایگاه داده درصورت موفق‌بودن حمله دشمن برابر است با مقدار پولی که مالک داده بابت مدیریت و نگه‌داری پایگاه داده و پاسخ به پرس‌وجوها به او می‌پردازد (Pdo(Q)) منهای هزینه‌ای که سرور در این زمینه برای پاسخ به پرس‌وجوی کاربر مصروف می‌دارد (– Costs(Q)) منهای هزینه‌ای که سرور مجبور است جهت بازیابی اطلاعات از دست‌رفته یا راه‌اندازی مجدد خرج نماید تا بتواند دوباره به‌نحو مطلوب در مقابل پرس‌وجوهای مشتریان پاسخ‌های مناسب دهد (– Costrec (Q)) منهای جریمه‌ای (-FS)

Archive of SID

www.SID.ir

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

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

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

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) –) به‌علاوه 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 (F_S) باید به اندازه‌ای باشد که علاوه‌بر 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 (F_{do}).

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 منعقده با مالک داده به‌طور کامل بیان شده است. رابطه زیر بیانگر سود مشتری درصورت موفقیت دشمن در حمله سرور خارجی می‌باشد:

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

رابطه بالا نشان می‌دهد که مشتری نه تنها از اطلاعات مالک داده سودی نبرده است بلکه هزینه‌ای بابت پرس‌وجو روی پایگاه 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 به‌قدری باشد که حاصل‌جمع جبری عبارت فوق مثبت گردد. واضح است که جریمه دریافتی از مالک داده این انگیزه را در او تقویت می‌نماید به‌دنبال جبران ضرر وارده به مشتری خود باشد (مشتری‌مداری) و بنابراین پس از بررسی تخلف شرکت ارائه‌دهنده خدمت پایگاه داده، مطابق قرارداد منعقده 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 به‌دنبال آن است تا بتواند تجارت سودآوری داشته باشد و مشتریان خود را راضی نگه دارد.

همان‌گونه‌که 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 درصورت 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 درصورت تخلف سرور بیشتر می‌شود. بنابراین در روش پیشنهادی محاسبه جریمه‌ها درصورت حمله احتمالی دشمن موضوعی است که به آن پرداخته خواهد شد.

۴-۱-۵-۳- نفوذ احتمالی دشمن

دشمن همیشه درحال 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 ذخیره‌شده 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 به‌طوری‌که ارائه‌دهنده خدمت پایگاه داده دارای دو راهبرد دفاع و شکست است. راهبرد دفاع یعنی آن‌که 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 آن‌که 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 به‌طوری‌که اگر

Archive of SID

www.SID.ir

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 درنتیجه 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 به‌دست‌آوردن 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 درنظر گرفته شود احتمال دفاع ارائه‌دهنده خدمت پایگاه داده در برابر نفوذ دشمن معادل مقدار β خواهد بود به‌طوری‌که:

$$\beta = 1-\alpha \qquad (۱۰)$$

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

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

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

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

$$Ua(q,v,\beta,a) = (1-\beta)\, Iv(Q) - Costa(Q) \qquad (۱۱)$$

این رابطه نشان می‌دهد که دشمن در برابر راهبرد دفاع سرور خارجی (با احتمال β) سودی معادل (1-β) Iv(Q) - Costa(Q) خواهد داشت. این نتیجه آن است که دشمن با انجام هزینه Costa(Q) و با احتمال 1-β 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:

$$Us(q, v, d, \alpha) = \alpha\, Us(r,r,f,i) + (1-\alpha)\, Us(q,v,d,a) \qquad (۱۲)$$

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

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

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

این رابطه بیانگر این واقعیت است که سرور خارجی در برابر راهبرد حمله دشمن (با احتمال نفوذ α) سودی معادل Pdo(Q) – Costs(Q) – αCostrec(Q′) – αFS به‌دست 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 αCostrec(Q′) – αFS – بیانگر آن است که درصورت موفقیت دشمن و نفوذ او به سرور خارجی او باید با احتمال α هزینه‌ای معادل جریمه پرداختی به مالک داده به‌علاوه 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:

$$Udo(q,v,\beta,a) = \beta\, Udo(q,v,d,a) + (1-\beta)\, Udo(r,r,f,i) \qquad (۱۳)$$

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

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

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

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-β) تاثیر خود را در آن گذاشته است.

از آن‌جایی‌که 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:

$$Uc(q,v,\beta,a) = \beta\, Uc(q,v,d,a) + (1-\beta)\, Uc(r,r,f,i) \qquad (۱۴)$$

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

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

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

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

Archive of SID

www.SID.ir

می‌داند و با احتمال انتخاب راهبرد شکست از سوی سرور خارجی و نفوذ دشمن (β-1) 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 مشتریانش و نیز پیگیری خواسته‌های کاربران برای رفع از کارافتادگی سرور خارجی، جریمه‌ای است که باید به مشتریان پرداخت نماید (Fdo).

از آن‌جایی‌که 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 درصورت نیاز در محاکم قانونی قابل طرح باشند، می‌بایست فرمولی برای محاسبه آن‌ها به‌دست 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 زیانی که از بابت عدم دریافت اطلاعات جامع به او رسیده است، تکافوی مبلغی که بابت پرس‌وجوی Q به او پرداخته است نیز باشد یعنی:

$$Fdo \geq (1-\beta)\, Iv(Q) + Pc(Q) \qquad (۱۵)$$

که در آن، (1-β) Iv (Q) زیانی 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:

$$Fdo \leq Pc(Q) \qquad (۱۶)$$

با توجه به فرض $Iv(Q) \geq Pc(Q)$ و این موضوع که هرگونه ادعایی که مشتری بابت مقدار Iv(Q) نماید، مورد پذیرش مالک داده نخواهد بود پس در محاسبات آینده به‌ناچار به‌جای Iv(Q) از حداقل مقدار آن یعنی Pc(Q) استفاده خواهیم کرد تا مقدار جریمه مورد توافق طرفین (مالک داده و مشتری) به‌دست آید. پس از رابطه ۱۵ داریم:

$$Fdo \geq (1-\beta)\, Pc(Q) + Pc(Q) \qquad (۱۷)$$

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

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

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

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

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

$$1 \geq \beta \geq \frac{2\, Pc(Q) - Fdo\,(Q')}{Pc(Q)} \geq 0 \qquad (۱۸)$$

از نامساوی بالا می‌توان نتیجه گرفت:

$$\frac{2\, Pc(Q) - Fdo}{Pc(Q)} \geq 0 \qquad (۱۹)$$

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

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

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

$$1 \geq \frac{2\, Pc(Q) - Fdo}{Pc(Q)} \qquad (۲۰)$$

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

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

$$Fdo \geq Pc(Q)$$

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

$$Pc(Q) \leq Fdo \leq 2\, Pc(Q) \qquad (۲۱)$$

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 (β).

Archive of SID

www.SID.ir

۴-۳- جریمه سرور خارجی (FS)

از رابطه (۱۳) چنین برداشت می‌شود که مالک داده به دنبال آن است تا جریمه‌ای که از سرور خارجی دریافت می‌نماید علاوه بر جبران جریمه‌ای که از بابت نقض جامعیت پاسخ‌های او به پرس‌وجوهای مشتریانش باید به آن‌ها بدهد، تکافوی مبلغی که بابت پرس‌وجوی q به او پرداخته است نیز باشد یعنی:

$$Fs \geq Pdo(Q) + (1-\beta)\, Fdo \qquad (۲۲)$$

که در آن، Pdo (Q) پولی است که مالک داده بابت پرس‌وجوی q به سرور خارجی پرداخته است و مقدار (1-β) Fdo معادل جریمه‌ای است که از بابت سهل‌انگاری ارائه‌دهنده خدمت پایگاه داده در تأمین امنیت سرور خارجی باید به مشتری بپردازد. از سوی دیگر، ارائه‌دهنده خدمت پایگاه داده به دنبال آن است که جریمه‌ای بیش‌تر از استرداد پولی که از مالک داده بابت پرس‌وجوی q دریافت داشته بپردازد یعنی:

$$Fs \leq Pdo(Q) \qquad (۲۳)$$

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

$$Fs \geq Pdo(Q) + (1-\beta)\, 2\, Pc(Q) \qquad (۲۴)$$

این عبارت با این‌که راهی برای محاسبه جریمه سرور خارجی پیش‌روی مالک داده است ولی مورد توافق ارائه‌دهنده خدمت پایگاه داده نیست زیرا مقدار Pc(Q) سودی است که مالک داده از فروش اطلاعاتش به‌دست آورده و برای ارائه‌دهنده خدمت پایگاه داده قابل پذیرش نمی‌باشد. بنابراین، طرفین باید به توافقی برای محاسبه جریمه سرور خارجی دست یابند، پس با توجه به فرض Pc(Q) ≥ Pdo(Q)؛ به‌جای عبارت Pc(Q) از مقدار حداقلی آن یعنی از مقدار Pdo(Q) بهره گرفته می‌شود. واضح است که این مقدار مورد توافق طرفین بوده و در متن قرارداد منعقده نیز آمده است. با این توضیحات خواهیم داشت:

$$Fs \geq Pdo\,(Q) + (1-\beta)\, 2\, Pdo\,(Q) \qquad (۲۵)$$

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

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

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

از آن‌جایی‌که مقدار احتمال β بین مقادیر ۰ و ۱ است خواهیم داشت:

$$1 \geq \beta \geq \frac{3\, Pdo(Q) - Fs}{2\, Pdo(Q)} \geq 0 \qquad (۲۶)$$

از نامساوی بالا می‌توانیم مقدار جریمه سرور خارجی را به‌صورت تقریبی به‌دست آوریم:

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

$$3\, Pdo\,(Q) - Fs \geq 0 \qquad (۲۷)$$

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

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

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

$$3\, Pdo\,(Q) - Fs \leq 2\, Pdo\,(Q) \qquad (۲۸)$$

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

$$Pdo(Q) \leq Fs$$

این عبارت نیز حداقل جریمه سرور خارجی را نشان می‌دهد. می‌توان نتایج فوق را به شکل زیر نمایش داد:

$$Pdo(Q) \leq Fs \leq 3\, Pdo(Q) \qquad (۲۹)$$

با توجه به نامساوی بالا واضح است که ارائه‌دهنده خدمت پایگاه داده به دنبال چانه‌زنی برای تعیین مقدار حداقلی جریمه یعنی Pdo(Q). این مقدار پولی است که از مالک داده بابت انجام پردازش روی داده دریافت می‌دارد. درحالی‌که مالک داده به دنبال تعیین مقدار حداکثری جریمه سرور خارجی یعنی 3 Pdo(Q). درواقع ارائه‌دهنده خدمت پایگاه داده باید مراقب باشد که مقدار جریمه از 3 Pdo(Q) بیش‌تر نگردد و مالک داده نیز باید مواظبت نماید که مقدار جریمه از Pdo(Q) کم‌تر نشود. دلیل آن‌که جریمه سرور خارجی به‌صورت بازه‌ای محاسبه می‌شود وجود احتمال حمله دشمن (α) و متقابلاً دفاع احتمالی سرور خارجی در برابر آن است (β).

همان‌طور که بیان شد درصورتی‌که سرور تقلب کند هزینه‌ای معادل با FS +Costrec(Q´) بپردازد.

قضیه: این بازی با استفاده از قرارداد بالا یک تعادل در راهبرد خالص دارد. مالک داده β را به نحوی انتخاب می‌کند که برای سرور، تقلب‌کردن از پاسخ صحیح برگرداندن بسیار کم‌ارزش‌تر باشد و درنتیجه سرور تقلب نمی‌کند. بنابراین β را به‌نحوی تعیین می‌کنیم 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 برمی‌گرداند از حالتی که تقلب می‌کند بیش‌تر باشد. هم‌چنین می‌دانیم که:

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

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

Archive of SID

www.SID.ir

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

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

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

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 Costrec(Q´) و FS به اندازه کافی بزرگ باشند. بنابراین تا زمانی که نامساوی بالا برقرار باشد سرور هیچ انگیزه‌ای برای تقلب‌کردن ندارد.

وقتی‌که Costrec(Q´) یک عدد ثابت است ما می‌توانیم FS را در قرارداد تنظیم کرد و هرچه مقدار آن بیش‌تر باشد می‌توانیم β را کاهش دهیم. ما قبل از این محدوده FS را تعیین کرده‌ایم و همان‌طورکه بیان شد تا زمانی‌که نامساوی بالا برقرار باشد سرور هیچ انگیزه‌ای برای تقلب‌کردن ندارد.

هم‌چنین باید نشان دهیم که β با مالک داده سازگار است. در نظر بگیرید وقتی‌که 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 درمجموع 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 درنظر 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 برون‌سپاری پایگاه داده ارائه گردید.

در این روش جریمه‌های بازیکنان متخلف به‌عنوان عامل اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده درنظر 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 ازکارافتادگی 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 درنظرگرفتن حمله احتمالی دشمن و هم‌چنین دفاع احتمالی ارائه‌دهنده پایگاه داده در برابر او عاملی برای اطمینان از نتایج پرس‌وجوهای کاربران روی پایگاه داده برون‌سپاری‌شده 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 انجام‌وظیفه خود برای برقراری امنیت سرور خارجی کوتاهی ورزد به‌طوری‌که دشمن بتواند جامعیت داده برون‌سپاری‌شده را به خطر اندازد باید جریمه‌ای معادل:

$$Fs\,(Q')\geq 3Pdo(Q)-2\beta Pdo(Q) \qquad (۳۱)$$

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:

$$2Pc(Q)-\beta Pc(Q)\leq Fdo\,(Q') \qquad (۳۲)$$

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

Archive of SID

www.SID.ir

نیست، اما به‌منظور 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 فرمول‌های به‌دست‌آمده، جریمه سرور و مالک داده را محاسبه می‌کنیم. هدف ما از پیاده‌سازی بررسی اثر مقادیر مختلف گفته‌شده در بالا در میزان جریمه سرور و مالک داده و استفاده از این تفاسیر هنگام انعقاد قرارداد برون‌سپاری است، بنابراین، نوع حملات دشمن و میزان از دست رفتن نتایج پرس‌وجو در این پیاده‌سازی مدنظر نیست. مطابق جدول (۱) و بر اساس مقادیر داده‌شده به احتمال β جریمه مالک داده (F_{do}) و جریمه سرور خارجی (F_s) را به‌دست می‌آید. لازم به یادآوری است که شرط بازی عبارت بود از $P_c(Q) \geq P_{do}(Q)$. یعنی لازمه آن‌که بازی تجاری بین مشتری، مالک داده و ارائه‌دهنده خدمت پایگاه داده در جریان باشد، می‌بایست پولی که مشتری بابت پرس‌وجو روی داده مالک داده به او می‌پردازد حداقل با مقدار پولی که مالک داده بابت انجام پردازش روی داده‌اش به سرور خارجی می‌پردازد 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) به‌دست می‌آید.

اکنون با فرض این‌که Pc(Q)=1 و Pdo(Q)=۰/۸ باشند. جریمه مالک داده (F_{do}) و جریمه سرور خارجی(F_s) در احتمالات مختلف دفاع سرور خارجی (β) مطابق جدول (۲) به‌دست می‌آیند.

جدول (۱): محاسبه جریمه‌های مالک داده و سرور خارجی

β	۰	۰/۱	۰/۲	۰/۳	۰/۴	۰/۵
Fdo≥	۲ Pc(Q)	۱/۹ Pc(Q)	۱/۸ Pc(Q)	۱/۷ Pc(Q)	۱/۶ Pc(Q)	۱/۵ Pc(Q)
Fs ≥	۳ Pdo(Q)	۲/۸ Pdo(Q)	۲/۶ Pdo(Q)	۲/۴ Pdo(Q)	۲/۲ Pdo(Q)	۲ Pdo(Q)
β	۰/۶	۰/۷	۰/۸	۰/۹	۱	-
Fdo≥	۱/۴ Pc(Q)	۱/۳ Pc(Q)	۱/۲ Pc(Q)	۱/۱ Pc(Q)	Pc(Q)	-
Fs ≥	۱/۸ Pdo(Q)	۱/۶ Pdo(Q)	۱/۴ Pdo(Q)	۱/۲ Pdo(Q)	Pdo(Q)	-

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

β	۰	۰/۱	۰/۲	۰/۳	۰/۴	۰/۵
F_{do} ≥	۲	۱/۹	۱/۸	۱/۷	۱/۶	۱/۵
F_s ≥	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} ≥	۱/۴	۱/۳	۱/۲	۱/۱	۱	-
F_s ≥	۱/۴۴	۱/۲۸	۱/۱۲	۰/۹۶	۰/۸	-

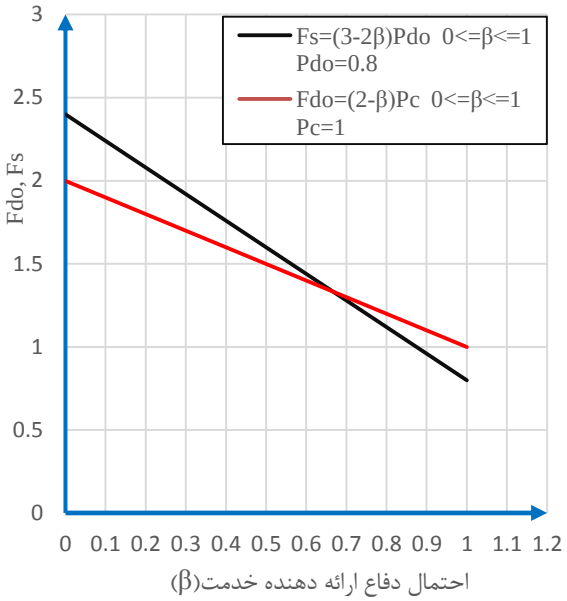
همان‌گونه که از جداول فوق قابل‌مشاهده است؛ با افزایش احتمال دفاع سرور خارجی در برابر حملات دشمن، مقادیر جریمه مالک داده و سرور خارجی روبه کاهش است تا جایی که اگر احتمال دفاع سرور خارجی (β) برابر با مقدار ۱ شود مقدار جریمه مالک داده برابر با مقدار ۱ ($P_c(Q)$) می‌گردد. یعنی پولی که مشتری بابت استفاده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

هم‌چنین می‌توان دید که اگر احتمال دفاع سرور خارجی (β) برابر با مقدار ۱ شود مقدار جریمه سرور خارجی برابر با مقدار ($P_{do}(Q)$)=۰/۸ می‌شود. یعنی پولی که مالک داده بابت پردازش داده توسط سرور خارجی به ارائه‌دهنده خدمت پایگاه داده پرداخت می‌نماید.

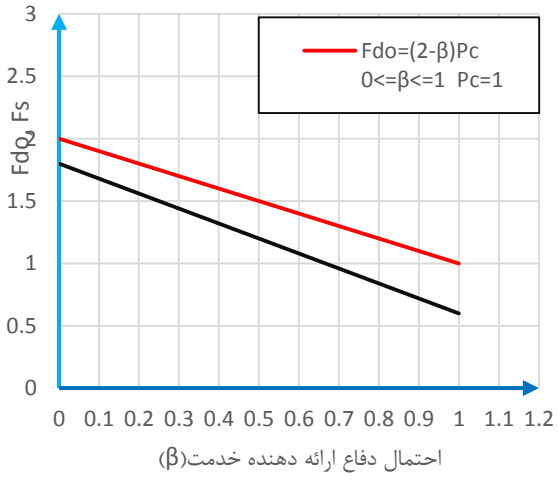
Archive of SID

www.SID.ir

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 درصورتی‌که درواقع 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 $P_c(Q)$=۱ و مقادیر مختلف $P_{do}(Q)$ (به‌طور نمونه مقادیر ۰/۸ و ۰/۶ و ۰/۲) به‌صورت زیر دست‌یافت.

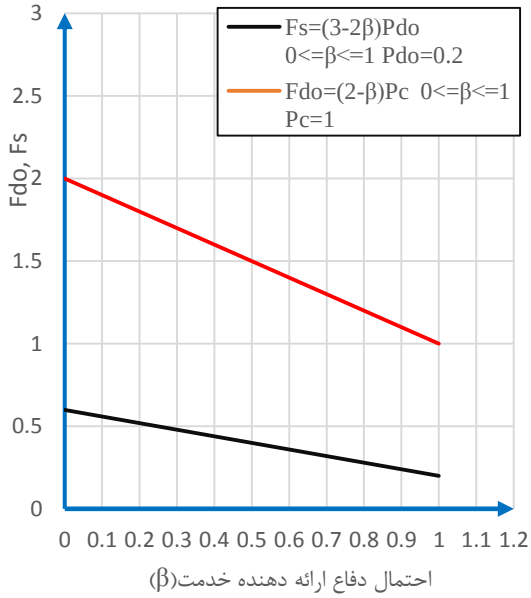


نمودار (۱): توابع جریمه مالک داده و سرور خارجی با توجه Pdo (Q) = 0.8 و Pc(Q) = 1



نمودار (۲): توابع جریمه مالک داده و سرور خارجی با توجه Pdo (Q) = 0.6 و Pc(Q) = 1

نمودارهای بالا مقدار جریمه سرور خارجی و جریمه مالک 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 (Fdo) و سرور خارجی (Fs) می‌باشند. خط قرمزرنگ بیانگر نمودار تابع جریمه مالک داده برحسب مقدار احتمال دفاع ارائه‌دهنده خدمت پایگاه داده در برابر حملات دشمن و خط سیاه‌رنگ 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 Pdo(Q) = 0.2 و Pc(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. به‌عبارت‌دیگر، 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 به‌دست‌آمده برای جریمه‌های مالک داده و سرور خارجی حاکی از زیاده‌خواهی به ترتیب مشتری و مالک داده است که واضح است هیچ‌یک از

Archive
www.SID.ir

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 درحالی‌که جریمه سرور خارجی بر اساس مقدار Pdo(Q) به‌دست می‌آید و همان‌گونه که می‌دانیم رابطه Pc(Q) ≥ 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. درهرحال، 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 پرس‌وجو روی پایگاه داده برون‌سپاری‌شده 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 نه‌تنها تکافوی سود ازدست‌رفته 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 واردکردن دشمن در بازی به‌عنوان یک بازیگر پرهیزکرده‌اند 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 درنظر نگرفتن حضور دشمن و تأثیر آن بر شرایط بازی، غیرمنطقی و غیرواقعی است. بنابراین، ما با واردکردن 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 را به جریمه سرور افزوده‌ایم و با اعمال تأثیر آن را بر رفتار سرور به عملیاتی‌ترشدن 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 برون‌سپاری 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 برون‌سپاری ارائه می‌کند و تنظیم قرارداد بر اساس این مدل کاملاً منطقی است.

۵-۲- بحث

ازآنچه در بالا بیان شد می‌توان نتیجه گرفت که با زیادشدن اختلاف Pdo(Q) از Pc(Q) (مثلاً وقتی‌که Pdo(Q) برابر ۰/۲ و Pc(Q) برابر با ۱ باشد) مقدار جریمه سرور خارجی (Fs) از جریمه مالک داده (Fdo) بسیار کم‌تر می‌گردد. این موضوع انگیزه مالک داده را در کنترل و بررسی پرس‌وجوها روی سرور خارجی افزایش می‌دهد و اطمینان از نتایج پرس‌وجوهای کاربران را بالا می‌برد زیرا جریمه‌ای که مالک داده دریافت می‌کند نه‌تنها تکافوی سود ازدست‌رفته او را نخواهد داد بلکه جبران جریمه‌ای که باید به مشتری‌اش بپردازد نیز نخواهد بود، اما مالک داده به دلیل آن‌که موجودی سودجوست دوست دارد جریمه‌ای که از سرور خارجی دریافت می‌نماید حداقل مساوی جریمه‌ای باشد که به مشتری می‌پردازد (یعنی Fs ≥ Fdo). بنابراین، خواهیم داشت:

$$Fs \geq Fdo \qquad (۳۳)$$

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

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

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

رابطه بالا نشان می‌دهد که برای آن‌که 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 منعقده با ارائه‌دهنده خدمت پایگاه داده رابطه (۳۳) را مدنظر قرار دهد. به‌عبارت‌دیگر، 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 پرس‌وجوهای 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 به‌دست می‌آید:

$$Fs(Q') \geq \frac{2\beta^2-7\beta+6}{3-2\beta}\ Pc(Q) \qquad (۳۴)$$

Archive of SID

www.SID.ir

درصورتی‌که 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 منعقده با ارائه‌دهنده خدمت پایگاه داده حداقل برابر با رابطه (۳۴) محاسبه نماید. البته این موضوع شاید موردپذیرش ارائه‌دهنده خدمت پایگاه داده نباشد زیرا جریمه سرور خارجی مطابق رابطه بالا بر اساس مقدار Pc(Q) محاسبه شده است. درحالی‌که ارائه‌دهنده خدمت پایگاه تمایل دارد جریمه خود را بر اساس مقدار Pdo(Q) محاسبه نماید. موفقیت مالک داده در این زمینه بستگی به قدرت چانه‌زنی او خواهد داشت.

در این بخش، روشی که برای اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده در بخش گذشته به‌طور کامل بیان گردید، مورد ارزیابی قرار گرفت. در این بخش نشان داده شد که جریمه‌های پیش‌بینی‌شده برای ارائه‌دهنده خدمت پایگاه داده و مالک داده به درستی انگیزه تخلف را از انجام وظیفه آنان از بین می‌برد. در خاتمه نیز اشاره گردید برای آن‌که مالک داده در هنگام کوتاهی ارائه‌دهنده خدمت پایگاه داده بابت اختلاف جریمه دریافتی از او و هم‌چنین جریمه پرداختی به مشتری متضرر نگردد می‌بایست در قرار منعقده با ارائه‌دهنده خدمت پایگاه داده، جریمه سرور خارجی را از رابطه (۳۳) محاسبه نماید اما این موضوع انگیزه مالک داده را در کنترل و بررسی پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده کاهش می‌دهد.

۶- نتیجه‌گیری

در این مقاله، برون‌سپاری پایگاه داده و چالش‌های مربوط به آن مورد بررسی قرار گرفت و سپس با معرفی تئوری بازی به‌عنوان دانش مطالعه رقابت‌ها تلاش گردید برای چالش "اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده" بر اساس تئوری بازی راه‌حلی ارائه گردد. در روش ارائه‌شده برون‌سپاری پایگاه داده با یک نگاه امنیتی به شکل یک بازی با حضور چهار بازیکن (دشمن، ارائه‌دهنده خدمت پایگاه داده، مالک داده و کاربر) تعریف گردید. درواقع نگاه ما به چالش "اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده" در بازی برون‌سپاری پایگاه داده به انگیزه‌های منفعت‌طلبانه هریک از بازیکنان بوده است. در این مقاله با درنظر گرفتن انگیزه‌های منفت‌طلبانه بازیکنان سعی گردید روشی ارائه گردد که با از بین‌بردن انگیزه هریک از بازیکنان در کوتاهی از انجام وظایف خود، اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده را به‌دست دهد.

در روش ارائه‌شده با درنظر گرفتن مدل احتمالی برای حمله دشمن و متقابلاً مدل احتمالی برای دفاع ارائه‌دهنده خدمت پایگاه داده بازی برون‌سپاری پایگاه داده برون‌سپاری‌شده به‌صورت یک بازی ایستای مختلط تعریف گردید. در این بازی با محاسبه سود هر یک از بازیکنان درنهایت جریمه‌هایی برای هر یک از بازیکنان ارائه‌دهنده خدمت پایگاه داده و مالک داده به‌دست آمدند. این جریمه‌ها عامل اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده می‌باشند. مقدار این جریمه‌ها در حدی است که افراد سودجویی مانند ارائه‌دهنده خدمت پایگاه داده و مالک داده به‌دنبال فرار از پرداخت آن می‌باشند و درنتیجه ارائه‌دهنده 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 پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده نهایت تلاش و کوشش خود را به کار گیرد. این همان نتیجه مطلوبی است که به دنبال آن هستیم.

۷- کارهای آینده

ازجمله کارهای آینده می‌توانند بررسی اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده به چند سرور خارجی و هم‌چنین تحت مالکیت چند مالک داده باشد. به‌طوری‌که هرکدام از سرورهای خارجی انگیزه‌های متفاوتی برای برقراری امنیت پایگاه داده دارند. چه‌بسا هرکدام از مالکان داده نیز انگیزه متفاوتی برای کوتاهی در کنترل و بررسی نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری‌شده دارند. هم‌چنین می‌توان انواع حملات مختلف که جامعیت پایگاه داده برون‌سپاری‌شده را تهدید می‌کنند را با احتمالات وقوع متفاوت در نظر گرفت.

همه این موارد می‌توانند بر اساس تئوری بازی، مورد بررسی قرارگیرند، به‌طوری‌که با محاسبه سود و زیان بازیکنان راه‌حل‌هایی برای اطمینان از نتایج پرس‌وجوها روی پایگاه داده برون‌سپاری شده به‌دست آیند. این موضوعات گوشه‌ای از کارهایی است که می‌توانند مبتنی بر نظریه بازی به حل چالش‌های برون‌سپاری پایگاه داده پرداخت.

۸- تشکر و قدردانی

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

Archive of SID

www.SID.ir

۹- مراجع

[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.

[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.

Archive of SID

www.SID.ir

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.customer.

Keywords: Outsourced Database, Game tTheory, Query Results Integrity

Archive of SID

*Corresponding Author Email: ghayoori@ihu.ac.ir

www.SID.ir