فصلنامه علمی-ترویجی پدافند غیرعامل
سال پنجم، شماره ۱، بهار ۱۳۹۳، (پیاپی ۱۷): صص ۱-۱۰

ارائه یک طبقه‌بندی جدید از تهدیدات برون‌سپاری پایگاه داده با رویکرد پدافند غیرعامل

محمد محمدی[۱]، مجید غیوری ثالث[۲]

تاریخ دریافت: ۹۲/۰۴/۰۵
تاریخ پذیرش: ۹۲/۱۰/۱۶

چکیده

رعایت «اصل پراکندگی»، یکی از اصول پدافند غیرعامل می‌باشد. این اصل را می‌توان به خدمات فناوری اطلاعات نیز تعمیم داد. برون‌سپاری پایگاه داده در یک سازمان، می‌تواند به «اصل پراکندگی» در ذخیره‌سازی اطلاعات برای آن سازمان کمک کند. ارائه یک طبقه‌بندی مناسب از چالش‌های برون‌سپاری پایگاه داده و دسته‌بندی آن‌ها، به شناخت راهکارهای مناسب برای کاهش آسیب‌پذیری در برابر تهدیدات و اقدامات خصمانه دشمن کمک می‌کند. در این مقاله با بررسی معماری پایگاه داده برون‌سپاری‌شده، یک طبقه‌بندی جدید از چالش‌های امنیتی فراروی برون‌سپاری داده‌ها ارائه شده است که نقایص طبقه‌بندی‌های قبلی را برطرف می‌کند. این طبقه‌بندی جدید می‌تواند در جهت‌دهی دقیق‌تر تحقیقات آینده بسیار راهگشا باشد.

کلیدواژه‌ها: برون‌سپاری خدمات، پایگاه داده، خدمات پایگاه داده‌ای، طبقه‌بندی چالش‌های امنیتی.

۱- دانشجوی کارشناسی ارشد دانشگاه جامع امام حسین(ع) ihu.mohammadi@gmail.com - نویسنده مسئول
۲- استادیار و عضو هیئت علمی دانشگاه جامع امام حسین(ع) ghayoori@ihu.ac.ir

۱- مقدمه

رشد سریع فناوری اطلاعات و ارتباطات، منجر به رشد ۵۲ درصدی هزینه‌های مدیریت ذخیره‌سازی[1] اطلاعات شده است [۲]. این هزینه‌ها شامل سخت‌افزار، نرم‌افزار و نیروی متخصص می‌باشد و ممکن است خیلی از سازمان‌ها و ادارات از عهده هزینه آن برنیایند. این مسئله به گسترش ایده برون‌سپاری داده‌ها دامن زده است. برون‌سپاری یعنی واگذاری تمام یا بخشی از وظایف یک سازمان به یک کارگزار ثالث که آن وظایف را به صورت خدمات ارائه می‌نماید. با برون‌سپاری، سازمان‌ها می‌توانند به جای تحمل هزینه‌های قابل توجه، از جمله خرید سخت‌افزار، نرم‌افزار و هزینه‌های متخصصان، بر روی وظایف اصلی خود متمرکز شوند و برنامه‌های کاربردی کسب‌وکار را از طریق اینترنت (شبکه) عملی کنند. امروزه سازمان‌ها و نهادهای دولتی برای برنامه‌ریزی بهتر در جهت رسیدن به اهداف خود، به تبادل اطلاعات با یکدیگر نیازمند هستند. برون‌سپاری داده، برای سازمان‌های نظامی و امنیتی که دارای اطلاعات حیاتی هستند راه حلی مناسب برای رعایت پدافند غیرعامل، - حداقل در برابر تهاجم فیزیکی دشمن - است. به عنوان مثال، یک یگان نظامی مستقر در مرز را در نظر بگیرید که مرکز نگهداری اطلاعات آن، در محل خود یگان مرزی باشد، در این صورت با اولین تهاجم فیزیکی و یا حتی با یک حمله چریکی محدود، ممکن است امنیت اطلاعات و اسناد آن به خطر بیفتد. در حالی که اگر همین یگان مرزی اطلاعات خود را در مراکز داده‌ایِ مستقر در مکانی دیگر نگهداری کرده باشد اصل »پراکندگی «در پدافند غیرعامل را رعایت نموده است. لازم به یادآوری است که منظور از برون‌سپاری داده‌ها در سازمان‌های نظامی، سپردن داده‌ها به سازمان‌های غیر نظامی نیست؛ بلکه این خدمات برون سپاری توسط خود سازمان‌های نظامی انجام می‌شود. همچنین یکی از نیازمندی‌های اصلی سیستم‌های فرماندهی و کنترل یکپارچه (C4I) برای مواجهه با بحران، ایجاد بانک اطلاعاتی است. بانک اطلاعاتی مذکور در این سیستم، از داده‌های سازمان‌های ذی‌ربط تشکیل می‌شود که در یک یا چند مرکز داده‌ای نگهداری می‌شود. این مثال‌ها نمونه کوچکی از اهمیت امنیت و پدافند غیرعامل در برون‌سپاری پایگاه داده را نشان می‌دهد. از طرفی دیگر، عدم توانایی یا رغبت سازمان‌ها و نهادهای نظامی و غیرنظامی برای درگیر شدن با مسائل تخصصی و فنی مانند ایجاد، ذخیره‌سازی، پشتیبان‌گیری و به‌روزرسانی پایگاه داده‌های مورد نیاز خود، سبب می‌شود که آن‌ها این خدمات را به طرف ثالثی به عنوان شرکت ارائه دهنده خدمات پایگاه داده[2] (DAS) واگذار نمایند [۲,۳]. برون‌سپاری پایگاه داده‌ها و یا در کل، برون‌سپاری فناوری اطلاعات، می‌تواند مخاطرات متنوعی داشته باشد. «میشل اِرل» برای برون‌سپاری فناوری اطلاعات، هفت تهدید[3] را به صورتی که در ادامه آمده است ذکر می‌کند [۴]:

۱- ***امکان مدیریت ضعیف:*** چنانچه برون‌سپاری به‌خوبی مدیریت نشود مشکل‌آفرین است. اگر سرور ارائه دهنده خدمات و یا سازمان برون‌سپار به‌خوبی عملیات را مدیریت نکنند می‌تواند مخاطره‌آمیز باشد.

۲- ***نیروهای بی‌تجربه:*** با حضور فناوری‌های جدید، کارمندان سازمان‌ها نسبت به آن بی‌تجربه بوده و نیازمند آموزش هستند.

۳- ***کسب‌وکار نامطمئن:*** در طی سالیان گذشته، تجربه به‌خوبی نشان داده است که خیلی از سرویس‌ها، سخت افزارها و نرم‌افزارها، به‌طور کامل غیرقابل استفاده شده و یا متقاضی آن بسیار کم شده است. به این دلیل خیلی از شرکت‌ها رغبت به برون‌سپاری ندارند؛ چون به موفقیت آن در آینده تردید دارند.

۴- ***منسوخ شدن مهارت‌های فنی:*** با ظهور فنون جدید، مهارت‌های قبلی باید به‌روزرسانی شوند. برون‌سپاری پایگاه‌داده، فنّ جدیدی است و باید چالش‌های آن را شناخت و طریقه استفاده کارا و مؤثر آن را فرا گرفت.

۵- ***تردیدهای ذاتی:*** پذیرش فنون جدید همیشه با احتیاط صورت می‌گیرد.

۶- ***هزینه‌های پنهان:*** **هزینه‌ها به دو صورت:** ۱) هزینه‌های نصب و راه‌اندازی سرویس برون‌سپاری، و ۲) هزینه مدیریت و نگهداری آن تقسیم می‌شوند. چون شرکت‌ها برآورد دقیقی از هزینه‌های بعدی نگهداری و مدیریت آن ندارند بعد از شروع کار، با مشکل مواجه می‌شوند.

۷- ***فقدان آموزش سازماندهی شده:*** اکثر آموزش‌ها در خصوص قابلیت‌های فناوری اطلاعات تجربی هستند و معمولاً استاندارد مشخصی برای آموزش وجود ندارد.

با وجود این مشکلات، سازمان‌ها در آینده به‌منظور بهره‌مندی از مزایای برون‌سپاری، ناچار به استفاده از این سرویس‌ها هستند.

1- Storage Management Cost

2- Database As Server

3– risk

برون‌سپاری پایگاه داده، قطعاً دارای مزایایی نیز می‌باشد. «راسلو» و همکارانش در یک تحقیق با بررسی ۱۰۰۰ سازمان که اقدام به برون‌سپاری کرده بودند نشان دادند که این امر باعث کاهش ۲۰ درصدی هزینه مدیریت ذخیره‌سازی داده‌های آن‌ها شده است [۲]. بنابراین، کاهش هزینه‌ها می‌تواند محرک مهمی برای گرایش به استفاده از خدمات DAS باشد. اگر برون‌سپاری به شکل صحیح مدیریت گردد قطعاً مزایای زیادی دربر خواهد داشت که به تعدادی از آن‌ها در ادامه اشاره می‌شود. «احمدالنیابت» و همکارانش مزایایی مانند کاهش هزینه ۵ تا ۱۰ برابری حالت اولیه، افزایش دسترس‌پذیری پایگاه داده، ارائه تعدادی سرویس ارزان و ارائه مهارت پایدار را برای برون‌سپاری بیان می‌کنند [۵]. افزایش تقاضای اطلاعات، رشد ارائه خدمات برخط[1] را به‌دنبال داشته است؛ با برون‌سپاری هزینه داخلی سازمان برای تجهیزات خدمات برخط کاهش می‌یابد [۶].

به‌عنوان جمع‌بندی، با توجه به مطالب بیان‌شده، سه دلیل زیر انگیزه اصلی برای برون‌سپاری پایگاه داده محسوب می‌شوند:

- افزایش هزینه‌های برپاسازی سیستم‌های مدیریت پایگاه داده؛
- رشد هزینه‌های مدیریت ذخیره‌سازی اطلاعات؛
- نیاز به سخت‌افزار، نرم‌افزار و نیروی انسانی متخصص؛

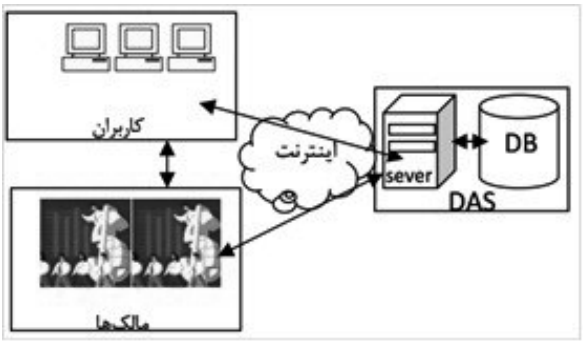
در این مقاله سعی بر این است تا پاسخ سؤالات زیر برای خواننده روشن شود:

چه چالش‌هایی برون‌سپاری را تهدید می‌کند؟ روش‌های رفع هر چالش کدام است؟

ساختار مقاله به صورت زیر است: در بخش ۲ مقاله، معماری پایگاه داده برون‌سپاری معرفی شده و در بخش ۳ چالش‌های برون‌سپاری بیان شده است. در بخش ۴ به کارهای مرتبط پرداخته شده و در بخش ۵، طبقه‌بندی جدید و کامل‌تر نگارندگان مقاله از چالش‌های برون‌سپاری پایگاه داده ارائه شده است. در بخش ۶ مروری گذرا بر راه‌کارهای موجود برای غلبه بر هر یک از چالش‌ها بیان شده و در نهایت، نتیجه‌گیری و مراجع ذکر شده است.

۲- معماری برون‌سپاری پایگاه داده

در مدل پایگاه داده برون‌سپاری شده[2] (ODB)، خدمات پایگاه داده‌ای (DAS) در جایی غیر از سازمان مربوط به مالک داده ارائه می‌شود. مایکلتون و همکارانش یک معماری عمومی از نحوه برون‌سپاری پایگاه داده را مطابق شکل (۱) ارائه کرده‌اند.



شکل ۱- روابط و موجودیت‌های مدل DAS [۷]

در شکل (۱) موجودیت‌های معماری برون‌سپاری پایگاه داده و روابط بین آن‌ها آمده است. مطابق با سناریوی برون‌سپاری داده، سه نقش (موجودیت) اصلی در این معماری وجود دارد [۱]:

۱. مالک داده: که داده را تولید می‌کند و صاحب داده به شمار می‌آید.

۲. ارائه‌کننده سرویس پایگاه داده (DAS): از مالک، داده‌ها را دریافت می‌کند و آن‌ها را در شبکه در دسترس قرار می‌دهد.

۳. کاربر: استفاده کننده از داده‌ها.

در این مدل برای دسترسی کاربران به داده‌ها، چون داده در جایی دیگر - غیر از محل درخواست‌کننده اطلاعات - نگهداری می‌شود، تراکنش زیادی بین درخواست‌کننده و ارائه‌دهنده سرویس انجام می‌شود. «مایکلتون» و همکارانش پنج عامل سربار به شرح ذیل را برای این مدل بیان می‌کنند که باید تلاش شود تا به حداقل رسانده شود[۷]:

۱. **کاهش محاسبات پرس‌وجو کننده:** شناسایی یکپارچگی/ احراز هویت یک مجموعه از رکوردها در پاسخ به پرس‌وجو با حداقل پردازش مورد نیاز توسط کاربر.

۲. **پهنای باند پرس‌وجو کننده:** به حداقل رساندن رد و بدل کردن اطلاعات در هنگام پرس‌وجو.

۳. **محاسبات سمت سرور:** نتیجه پرس‌وجو در عین اینکه باید جامعیت و صحت داشته باشد، باید سریع نیز انجام شود.

1- Online
2- Outsourced database

۴. **محاسبات مالک داده:** کاهش محاسبات حفظ یکپارچگی اطلاعات برای داده‌های برون‌سپاری‌شده.

۵. **کاهش حجم ذخیره‌سازی:** عدم ایجاد افزونگی بیش از حد به علت رمزنگاری داده‌ها.

ارائه‌دهنده خدمات را می‌توان از لحاظ اجازه خواندن، نوشتن یا تغییر در اطلاعات سازمان به دو دسته تقسیم کرد: سرور مطمئن[1] (قابل اعتماد) و سرور نامطمئن (غیرقابل اعتماد). اگر ارائه دهنده سرویس از نظر کاربر یا مالک داده، مجاز به خواندن، نوشتن و یا تغییر داده‌های ذخیره‌شده در سمت خود باشد به این چنین خدمات دهنده‌ای، مطمئن (قابل اعتماد) و در غیر این صورت، سرور نامطمئن (غیرقابل اعتماد) گفته می‌شود [۸ و ۵]. به عنوان فرضیات مسئله، اغلب در برون‌سپاری، پایگاه داده خدمت، مورد اعتماد نیست؛ او ممکن است با استفاده از حق دسترسی که به داده‌ها دارد، آن‌ها را تغییر دهد. در بیشتر روش‌های ارائه‌شده در حالت سرور غیرقابل اعتماد، سرور از نظر نگهداری از داده‌ها و عدم ارسال عمدی پاسخ اشتباه، قابل اعتماد فرض می‌شود. او در دسترس بودن داده‌ها را تضمین کرده و کاربر در هر زمان که مایل باشد می‌تواند به داده‌ها دسترسی داشته باشد. یک سرور کنجکاو مانند یک مهاجم[2] فرض می‌شود؛ و یک سرور درستکار ولی کنجکاو، از نظر مشاهده داده‌ها نامطمئن می‌باشد.

۳- چالش‌های برون‌سپاری پایگاه داده

از آنجا که در برون‌سپاری، اطلاعات در جایی غیر از محل مالکِ داده نگهداری می‌شود، چالش‌های فراوانی ایجاد خواهد شد. مطابق بررسی‌های ما، تمام چالش‌های موجود بر سر راه برون‌سپاری را می‌توان در پنج گروه زیر دسته‌بندی کرد:

۱. سوء استفاده سرویس‌دهنده؛
۲. سرقت رسانه ذخیره‌ساز؛
۳. تهدیدات فضای سایبر؛
۴. بلایای طبیعی؛
۵. سربارهای ارتباطی و محاسباتی؛

حفظ امنیت اطلاعات ذخیره‌شده در سرورهای ارائه دهنده خدمات پایگاه داده، نیاز اساسی مالکان داده می‌باشد. آسیب‌رسانی یا سوءاستفاده از این داده‌ها نه‌تنها یک کاربر یا برنامه را تحت تأثیر خود قرار می‌دهد، بلکه ممکن است اثرات غیرقابل جبرانی بر روی تمام سازمان داشته باشد [۹]. عوامل مختلفی امنیت داده‌های برون‌سپاری‌شده را تهدید می‌کند. پشتیبان گیری و کنترل دسترسی، یکی از سازوکارهای حفاظت از سیستم پایگاه داده‌ها است. اما پشتیبان گیری برای حفاظت در مقابل آسیب‌های طبیعی مثل سیل، زلزله، آتش‌سوزی و خرابی دیسک به کار می‌رود در حالی که سازوکارهای کنترل دسترسی، پایگاه داده‌ها را در مقابل دسترسی افراد غیرمجاز مصون نگاه می‌دارد. تاکنون مدل‌های مختلفی برای کنترل دسترسی به پایگاه داده‌ها ارائه شده است [۱۰]. با این حال، کنترل دسترسی تنها در صورتی مفید است که مهاجم از طریق واسط اصلی پایگاه داده وارد شود؛ اما کنترل دسترسی، به صورت تضمینی مانع دستیابی غیرمجاز به داده‌ها نیست. مثلاً اگر رسانه حاوی داده‌ها به سرقت رود، یا مدیر پایگاه داده‌ها بخواهد به داده‌های حساس دسترسی داشته باشد یا اگر اطلاعات حین انتقال از بستر شبکه، شنود یا سرقت شود، کنترل دسترسی نمی‌تواند مانع افشاء داده‌های حیاتی شود.

ارائه‌دهنده خدمات برون‌سپاری مسئول ارائه منابع و مکانیزم‌های لازم برای مدیریت کارآمد و دسترسی به اطلاعات برون سپاری توسط مالکین داده و مشتری‌ها به طور جداگانه است. ارائه‌دهندگان خدمات همیشه نمی‌توانند مورد اعتماد باشند (خود آن‌ها ممکن است نیت سوء داشته باشند)، یا ممکن است امنیت آن‌ها توسط طرف‌های دیگر با قصد تخریب به مخاطره بیفتد (مهاجم) یا با اجرای نرم‌افزارهای معیوب (خطاهای غیر عمدی) در روی سرور باعث خرابی در داده‌ها شوند [۸].

۴- کارهای مرتبط

«دانگ» در سال ۲۰۰۸ چالش‌های امنیتی در برون سپاری پایگاه داده را دسته‌بندی کرده که در شکل (۲) نشان داده شده است [۱۱].

در مدل «دانگ» چالش‌ها در چهار گروه اصلی به صورت زیر دسته‌بندی شده‌اند:

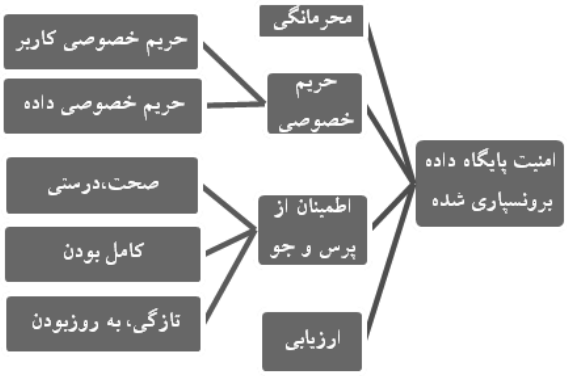
۴-۱- محرمانگی[3]

ارائه‌دهنده خدمات و حتی بیگانگان قادر نباشند که داده‌های برون‌سپاری‌شده را ببینند. این مسئله شامل دو بخش است:

۴-۱-۱- حریم خصوصی کاربر[4]

ارائه‌دهنده خدمات نتواند درباره پرس‌وجوهای کاربر و نتایج بازگشتی آن‌ها چیزی بداند.

1- Trust server
2- Attacker
3- Confidentiality
4- User privacy



شکل ۲- مباحث امنیت در برون‌سپاری داده‌ها [۱۱]

۴-۲- حریم خصوصی داده[1]

کاربران نتوانند اطلاعاتی بیش از آنچه از سرور درخواست نموده‌اند دریافت نمایند.

۴-۳- اطمینان از پرس‌وجو[2]

توانایی کاربر یا مشتری برای وارسی صحت[3]، تمامیت (کامل بودن[4]) و تازگی[5] نتایج پرس‌وجو.

۴-۳-۱- صحت پرس‌وجو

اطمینان از اینکه نتایج پرس‌وجو همه شرایط را پوشش داده و همچنین داده‌های بازگشتی، همان داده‌های مالک باشد و مورد ناخنک‌زنی[6] قرار نگرفته باشد.

۴-۳-۲- کامل بودن پرس‌وجو

اطمینان از اینکه نتایج بازگشتی، تمام چندتایی‌های[7] مورد درخواست مشتری در پرس‌وجو را شامل شود؛ نه شامل اطلاعات اضافی بوده و نه نقصان داشته باشد.

۴-۳-۳- تازگی پرس‌وجو

نتایج پرس‌وجو باید شامل تازه‌ترین تغییرات داده‌های ثبت‌شده در پایگاه داده باشد.

۴-۴- ارزیابی

وارسی فرایندهای انجام شده، برای حصول اطمینان از صحت انجام فرایندها.

بنابراین، در برون‌سپاری داده‌ها ممکن است هر کدم از مباحث بالا به خطر بیفتد.

در مقاله‌ای دیگر، خانم «فِراری» پس‌زمینه امنیت و حریم خصوصی داده‌ها را در سه بحث معرفی می‌کند [۱۲]:

محرمانگی داده: یعنی جلوگیری از افشاء نابجای اطلاعات به کاربران غیرمجاز.

جامعیت داده: یعنی حفاظت از تغییرات و حذف نابجا یا غیرمجاز داده.

دسترس‌پذیری: جلوگیری و ترمیم خطاهای سخت‌افزاری و نرم‌افزاری و یا داده‌های بدافزار که دسترسی به بخشی یا همه پایگاه داده را مختل می‌کند.

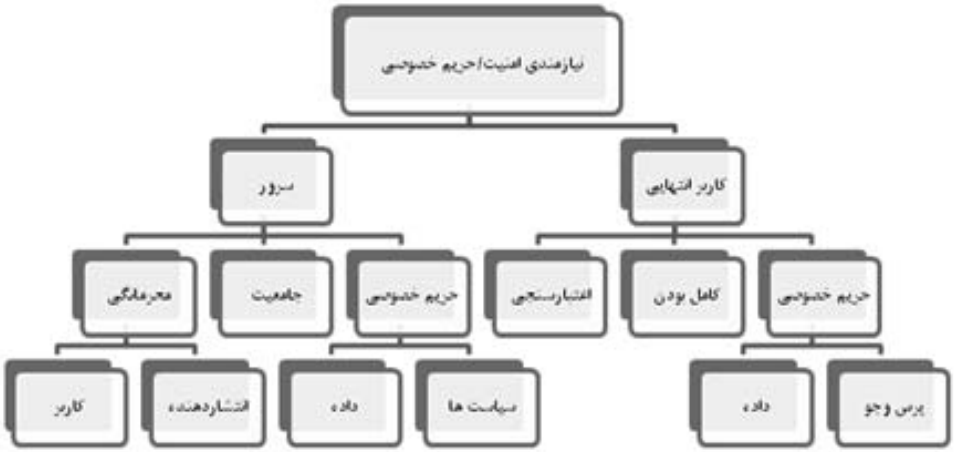
ایشان در ادامه، طبقه‌بندی[8] چالش‌های امنیتی پایگاه داده برون‌سپاری‌شده را در قالب یک ساختار درختی که در شکل (۳) آمده است معرفی می‌کند. در درخت طبقه‌بندی شکل (۳)، محرمانگی در دو بخش کاربران و انتشاردهنده[9] دسته‌بندی شده است. محرمانگی در سطح کاربر یعنی حفاظت از عملیات غیرمجاز خواندن داده‌ها توسط کاربران انتهایی.

انتشاردهنده یا سرور میزبان (DBMS) ممکن است مورد اعتماد نباشد، لذا در اینجا سطح دوم محرمانگی مطرح می‌شود که مربوط به انتشاردهنده یا سرور می‌باشد. محرمانگی در سطح انتشاردهنده یعنی اینکه سرور ارائه‌دهنده خدمات پایگاه داده مجاز به خواندن داده‌های ذخیره شده در سمت خود نیست و از خواندن داده‌ها توسط سرور جلوگیری می‌شود.

اطمینان از جامعیت، تحقق دو هدف را در پی دارد:

اول، اینکه دریک تعارض، جایی که سرور مورد اعتماد نیست ایجاب می‌کند که داده‌ها وارسی شوند تا اطمینان حاصل شود که سرور، داده‌ها را به سود خود جایگزین نکرده باشد و دوم، اینکه با وارسی اطمینان حاصل شود که داده‌ها توسط کاربرانی که از مالک داده‌ها مجوز گرفته‌اند تغییر یافته باشند.

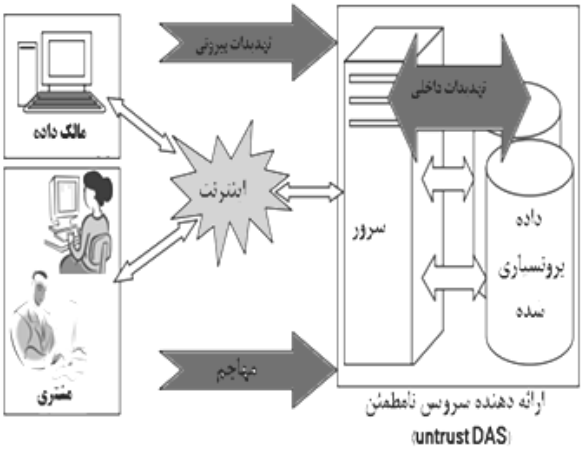
1- Data privacy
2- Query assurance
3- Correctness
4- Completeness
5- Freshness
6- Data tampering
7- Tuple
8- Taxonomy
9- Publisher



شکل ۳-درخت طبقه‌بندی چالش‌های برون‌سپاری [۱۲]

در شکل‌های (۲) و (۳)، طبقه‌بندی[1] چالش‌های پایگاه داده توسط «دانگ» و «فِراری» ارائه گردید. هر کدام از این طبقه‌بندی‌ها نقایصی دارند؛ به عنوان مثال، در طبقه‌بندی ارائه شده توسط «دانگ»، محرمانگی یا دسترس‌پذیری داده لحاظ نشده است. در مدل «فِراری» نیز چالش‌ها در دو سمت کاربر و سرور لحاظ شده، و چالش‌های سمت مالک داده، مانند احراز اصالت و حفظ حریم خصوصی مالک لحاظ نشده است.

«دانگ» در [۱۱]، «برنت سیمپسون» و همکارش در [۱۳] و «آندرو کلارک» و همکارش در [۱۴] یک معماری برای نشان دادن ارتباط بین موجودیت‌های مدل پایگاه داده برون‌سپاری‌شده همراه با مخاطرات آن ارائه کرده‌اند که شکل (۴) خلاصه‌ای از این مدل‌ها را نشان می‌دهد.



شکل ۴- مخاطرات برون‌سپاری پایگاه داده [۱۴،۱۳،۱۱]

مطابق شکل (۴)، چالش‌های برون‌سپاری در سه حوزه تهدیدات داخلی، تهدیدات بیرونی و تهدیدات خصمانه (از جانب یک مهاجم) اتفاق می‌افتد. تهدیدات داخلی به سوء استفاده احتمالی از اطلاعات، افشاء و خرابکاری عمدی یا سهوی توسط سرور اشاره می‌کند. تهدیدات بیرونی و مهاجم عمدتاً شامل دسترسی غیر مجاز، سرقت، افشاء و دست‌کاری اطلاعات است. تاکنون مطالعات فراوانی برای رفع یا بهبود هرکدام از چالش‌های ذکرشده در این بخش صورت گرفته که در بخش ۶ به آن پرداخته شده است.

۵- ارائه طبقه‌بندی جدید چالش‌های برون‌سپاری

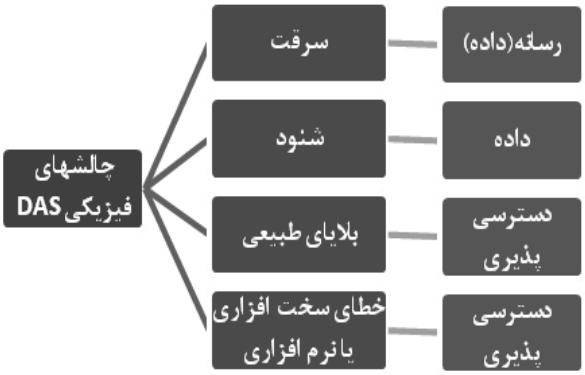
در این بخش ما قصد داریم تا یک طبقه‌بندی کامل‌تر معرفی کنیم که نقایص هرکدام از دو درخت قبلی را برطرف کرده و همه موارد محتمل را در خود پوشش دهد.

در این درخت طبقه‌بندی، ما چالش‌ها و تهدیدات[2] را به دو دسته کلی تقسیم کرده‌ایم؛ چالش‌های منطقی و چالش‌های فیزیکی. چالش‌های فیزیکی شامل بلایای طبیعی، آتش‌سوزی، سرقت فیزیکی، شنود، خطای سخت‌افزاری و نرم‌افزاری می‌باشد؛ چالش‌های منطقی شامل احراز هویت[3]، محرمانگی[4]، حریم خصوصی[5]، جامعیت[6]، دسترس‌پذیری[7]، صحت[8]، تمامیت[9] و

1- Taxonomy
2- Threats
3- Authentication
4- Confidentiality
5- Privacy
6- Integrity
7- Availability
8- Correctness
9- Completeness

تازگی[1] می‌باشد. هرکدام از این چالش‌ها روی یکی از اشیاء موجود در مدل DAS متمرکز است. در این مدل سعی شده که راه حل‌های عمومی هر چالش در گره برگ شاخه مربوطه آورده شود. درخت طبقه‌بندی ما چالش‌ها را به دو دسته کلی تقسیم می‌کند. یک دسته از چالش‌ها را که به عنوان چالش‌های فیزیکی مطرح می‌کنیم بیشتر در سمت سرور موضوعیت دارد؛ دسته‌ای دیگر با عنوان کلی چالش‌های منطقی، بیشتر در سمت مالک داده یا کاربر موضوعیت دارند، هرچند ممکن است که در سمت سرور نیز مطرح باشند.

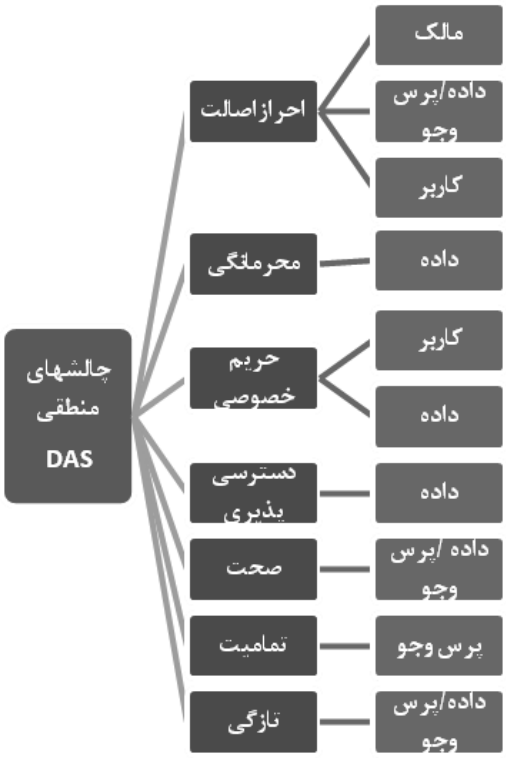
در قسمت الف شکل (۵)، چالش‌های فیزیکی برون سپاری نمایش داده شده است. در این دسته‌بندی بخش عمده‌ای از چالش‌ها که توسط محققین قبلی مورد غفلت واقع شده، ارائه شده است؛ لذا یک مزیت درخت پیشنهادی ما نسبت به طبقه‌بندی‌های مذکور در این مقاله، توجه به تمام چالش‌ها به طور جامع است.



شکل ۵-الف)طرح پیشنهادی درخت طبقه‌بندی چالش‌های فیزیکی DAS

در شکل (۵-ب) چالش‌های منطقی برون‌سپاری که غالباً در سمت کاربر و مالکِ داده وجود دارند بیان شده است. مزیت این طبقه‌بندی نسبت به طبقه‌بندی‌های ذکر شده قبلی در این است که چالش‌های مربوط به موجودیت‌های کاربر، داده و مالک و حتی پرس‌وجو روی داده‌ها را پوشش می‌دهد. در شکل (۵)، ستون وسط، چالش‌ها را نشان می‌دهد، ستون سمت راست، اشیاء متأثر از چالش‌های امنیتی را معرفی می‌کند. احراز اصالت شامل فنون اعتبارسنجی برای هر کدام از اشیاء متأثر از آن می‌باشد. به عنوان مثال، احراز اصالت مالک یا کاربر، یعنی بررسی و تأیید هویت شخص مدعی مالکیت یا کاربری؛ این امر در مورد داده و پرس‌وجوهای انجام‌شده بر روی آن نیز نیاز است.

1- Freshness



شکل ۵-ب) طرح پیشنهادی درخت طبقه‌بندی چالش‌های منطقی DAS

۶- راه حل‌های رفع چالش‌ها

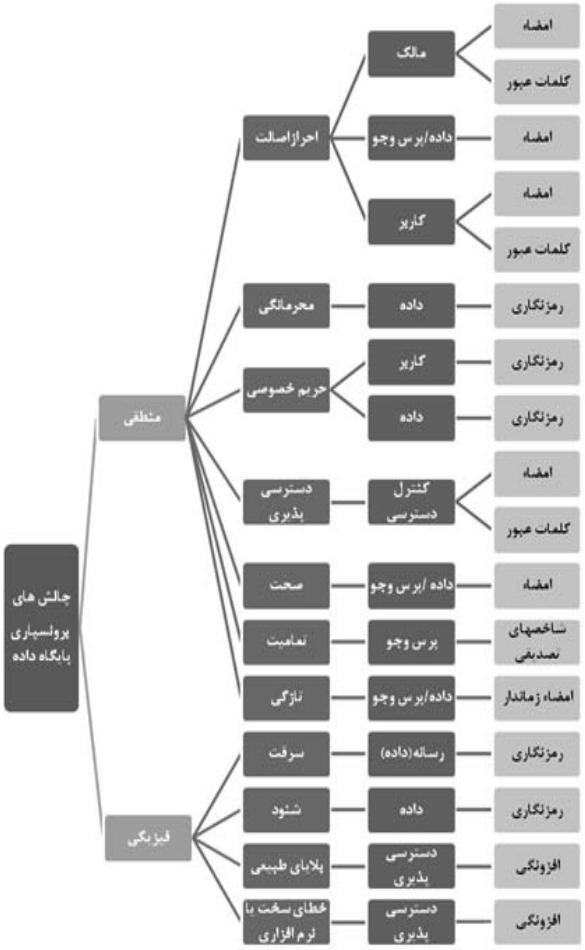
«دانگ» در [۱۱] راه‌کارهای حصول اطمینان از صحت، تمامیت و تازگی را با استفاده از داده سه شاخصه مورد مطالعه قرار داده است. «کلارک» در [۱۴] راه‌کارهای بهبود اطمینان از پرس‌وجو را مورد مطالعه قرار می‌دهد. در محدوده محرمانگی تعدادی از مقالات نظراتی را در مورد داده‌های امن در سرورهای نامطمئن با استفاده از رمزنگاری پیشنهاد کرده اند. «دونگ» و همکارانش یک طرح رمزنگاری ارائه کرده‌اند که اجازه می‌دهد متن‌های رمز شده با یک کلید، به متن‌های رمز شده با کلیدهای دیگر تبدیل شود [۱۵]. «کارمیناتی» و همکارانش یک مدل برای اطمینان از محرمانگی داده‌ها که با استفاده از کنترل دسترسی و رمزنگاری همزمان با هم انجام می‌شود، پیشنهاد کردند [۱۶]. در طرف دیگر، حریم خصوصی عموماً با کنترل دسترسی به‌دست می‌آید. یکی از کنترل دسترسی‌های ابتدایی روی دید امنیتی xml، توسط «استویکا» و همکارانش در سال ۲۰۰۲ ارائه شد [۱۷]. «مِهراترا» و همکارانش نیز به بررسی مسائل حریم خصوصی پرداخته‌اند [۱۸]. تضمین اجرای پرس‌وجو در [۱۹] توسط «رادو سی‌او»، و امنیت در ارتباطات با کنترل دسترسی مورد نیاز در

[۲۰] توسط «میکلائو» و همکارانش، و در [۲۱] توسط «پانگ» و همکارانش مورد مطالعه قرار گرفته است. پشتیبان‌گیری برای حفاظت در مقابل آسیب‌های طبیعی مثل سیل، زلزله، آتش‌سوزی و خرابی دیسک به کار می‌رود؛ در حالی که سازوکارهای کنترل دسترسی، پایگاه داده‌ها را در مقابل دسترسی افراد غیرمجاز مصون نگاه می‌دارد. راهکارهای عمومی احراز اصالت پرس‌وجو استفاده از امضاء است؛ کاربر و مالک داده‌ها عموماً با استفاده از امضاء و کلمات عبور، احراز اصالت می‌شوند. راه‌کار چالش محرمانگی و حریم خصوصی نیز عموماً استفاده از رمزنگاری و یا کنترل دسترسی است. در استفاده از رمزنگاری باید دو موضوع را مد نظر قرار داد: اول افزونگی، که غیر قابل اجتناب بوده اما باید سعی شود که به حداقل ممکن برسد؛ دوم، تازگی پاسخ پرس‌وجوهاست که با استفاده از فنون امضای زمانی (مهر زمانی) قابل حصول است. یکی دیگر از چالش‌ها، دسترس‌پذیری است که در حقیقت، مجوز دسترسی یا عدم دسترسی به داده‌ها را با استفاده از راه‌کارهایی مانند امضاء یا کلمات عبور به مالک یا کاربر مدعی می‌دهد. صحت داده یا پرس‌وجو را می‌توان با استفاده از امضاء مورد تأیید قرار داد. تمامیت یا کامل بودن پرس‌وجو را با استفاده از شاخص‌های تصدیقی می‌توان تأیید کرد. چالش تازگی داده یا پرس‌وجو را می‌توان با یک طرح امضاء زمان‌دار پوشش داد. چالش‌هایی که در گروه فیزیکی قرار گرفته‌اند بیشتر چالش‌های سمت سرور محسوب می‌شوند؛ به عنوان مثال، سرقت و شنود داده‌ها با استفاده از رمزنگاری قابل حل است؛ بلایای طبیعی و خرابی سخت‌افزاری و نرم‌افزاری که دسترس‌پذیری به سرویس‌ها را مختل می‌کنند با انواع فنون مختلف افزونگی قابل حل هستند.

با توجه به مطالعات انجام شده، راه حل‌های عمومی‌تر برای رفع چالش‌های ذکر شده در طبقه‌بندی پیشنهادی بخش ۵، در شکل (۶) به تصویر کشیده شده است. همان‌طور که در شکل پیداست ستون اول از سمت راست، راه حل هر چالش برای شیء متأثر از آن چالش را بیان می‌کند. برای مثال، چالش احراز اصالت برای مالک داده با استفاده از امضاء یا کلمات عبور و یا ترکیبی از آن دو حل می‌شود. همچنین تأثیر چالش بلایای طبیعی با استفاده از افزونگی، رفع شده و یا کاهش می‌یابد.

۷- نتیجه‌گیری

رشد ذخیره‌سازی داده‌ها با افزایش حجم اطلاعات و نیاز به کاهش هزینه‌های مدیریت آن در کنار مزایایی مانند عدم نیاز به



شکل ۶- راه‌حل‌های رفع چالش‌های برون‌سپاری

افراد متخصص و تجهیزات پیچیده، افزایش دسترس‌پذیری پایگاه داده و ارائه سرویس‌های ارزان و پایدار، برون سپاری داده‌ها را افزایش داده است. اما چالش‌های برون‌سپاری، مانع استفاده سازمان‌ها و بخصوص سازمان‌های نظامی از آن است. در این مقاله با بررسی معماری پایگاه‌داده برون‌سپاری‌شده، سعی در شناسایی چالش‌های آن نمودیم. همچنین طبقه‌بندی جدیدی از چالش‌های برون‌سپاری ارائه شد که نقایص دو طبقه‌بندی بررسی شده در این مقاله را پوشش می‌دهد. با مطالعه این مقاله، سازمان‌های مشتاق به برون‌سپاری، قادرند چالش‌های موجود بر سر راه برون‌سپاری را شناخته و با راه حل‌های آن آگاه شده و تمهیدات لازم به منظور ارتقاء قابلیت اطمینان و اتکاپذیری خدمات برون‌سپاری را ایجاد کنند. برون‌سپاری با توجه به کاربرد »اصل پراکندگی «در پدافند غیرعامل، برای تمام سازمان‌ها بخصوص سازمان‌های نظامی، ضروری‌تر به نظر می‌آید.

مراجع

۱. امیدی، سجاد؛ شهریاری، حمیدرضا؛ اِعمال کنترل دسترسی نوشتن در سناریوی برون‌سپاری داده‌ها با استفاده از مدیریت کلید رمزنگاری، هشتمین کنفرانس بین‌المللی انجمن رمز ایران، شهریور (۱۳۹۰).

2. G.Russello,N.Dulay C.Dong, "Shared and Searchable Encrypted Data From Untrusted Servers," Annual IFIP WG 11.3 Working Conference on Data and Applications Security, vol. 5094, pp. 127 -143, July**(2008)**.

3. Laks V.S.Lakshmanan, Hui Wang, "Efficient Secure Query Evaluation over Encrypted XML," ACM.VLDB, vol. 1-59593-385, June **(2006)**.

4. Michael J.Earl, "The Risk Of Outsourcing IT," Principal of London Business School, **(1996).**

5. Bahaa Eldin M. Hasan , Abd El Fatah.A. Hegazy Ahmed M.A. Al thneibat, "Secure Outsourced Database Architecture," International Journal of Computer Science and Network Security (IJCSNS), vol. 10, no. 5, pp. 246-255, May **(2010).**

6. H., Iyer, B.R., Mehrotra Hacigumus, "Providing database as a service," International Conference on Data Engineering (ICDE), **(2002).**

7. M.Narasimha, G. Tsudik E. Mykletun, "Authentication and Integrity in Outsourced Databases," School of Information and Computer Science University of California, Irvine, (2006).

8. Marios Hadjieftheriou, George Kollios, and Leonid Reyzin Feifei Li, "Authenticated Index Structures for Outsourced Databases," *Computer Science Department*, **(2008).**

9. M.Wang J.He, "Cryptography and Relational Database Management System," IDEAS, pp. 273-284, **(2001).**

10. R. Sandhu, E. Bertino, "Database Security Consepts, Approaches, and Challenges," IEEE Transactions on Dependable and Secure Computing, pp. 2-19, Jan **(2005).**

11. Tran khanh Dang, "Ensuring Correctness,completeness, and Freshness for Outsourced tree-Indexed Data," Information Resource Management Journal, vol. 29, pp. 59-76, , January-March **(2008).**

12. Elena Ferrari, "Database as a Service: Challenges and Solutions for Privacy and Security," IEEE Asia-Pacific Services Computing Conference, pp. 46-51, **(2009).**

13. Eric Pardede Brent Kimpton, "Securing Queries to Outsourced XML Databases," IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, pp. 419-424, **(2010).**

14. Eric Pardede Andrew Clarke, "Outsourced XML Database: Query Assurance," IEEE 24th International Conference on Advanced Information Networking and Applications, pp. 1181-1188, **(2010).**

15. Giovanni Russello, and Naranker Dulay Changyu Dong, "Shared and searchable encrypted data for untrusted servers," In DAS LNCS, vol. 5094, pp. 127–143, **(2008).**

16. Barbara Carminati and Elena Ferrari, "Confidentiality enforcement fo xml outsourced data," In EDBT Workshops, LNCS 4254, pp. 234–249, **(2006).**

17. Csilla Farkas Andrei Stoica, "Secure xml views," DBSec, pp. 133–146, **(2002).**

18. Mehrotra, S., Tsudik, G. Hore B., "A privacy-preserving index for range queries," Proc. of Very Large Data Bases (VLDB), pp. 720-731, **(2004).**

19. Radu Sion, "Query Execution Assurance for Outsourced Databases," Proceedings of the 31st VLDB Conference, pp. 601-612, **(2005).**

20. G., Suciu, D Miklau, "Controlling access to published data using cryptography," In: Proc. of Very Large Data Bases (VLDB), p. 898

21. H., Jain, A., Ramamritham, K., Tan, K.L Pang, "Verifying completeness of relational query results in data publishingtional query results in data publishing," In: Proc. of ACM Management of Data (SIGMOD), pp. 407-418, **(2005).**

Presenting a new taxonomy of database outsourcing threats with the passive defense approach

M.mohammadi [1]

M.ghayoori [2]

Abstract

Observing the "principle of dispersion" is one of the principles of passive defense. This principle can also be applied to IT services. Database outsourcing in an organization can contribute to "the principle of dispersion" in data storage for that organization. Presenting a suitable classification of the challenges of outsourcing will contribute to the identification of appropriate strategies to mitigate vulnerability against hostile threats and actions. In this paper, through investigating the architecture of database outsourcing, a new category of security challenges facing data outsourcing is presented that will eliminate shortcomings of previous category. This new classification can be helpful in better directing the future research.

Key Words: *outsourcing, database, database services, security challenges taxonomy.*

1- MS in Software Engineering, Imam Hossein Comprehensive University (ihu.mohammadi@gmail.com) - Writer in Charge
2- Assistant Professor and Academic Member of Imam Hossein Comprehensive University (ghayoori@ihu.ac.ir)