فصلنامه علمی-ترویجی پدافند غیرعامل
سال ششم، شماره ۲، تابستان ۱۳۹۴، (پیاپی ۲۲): صص ۷۴-۶۳

تهدیدات و تمهیدات پایگاه داده به‌عنوان سرویس در رایانش ابری از دیدگاه پدافند غیرعامل

مجتبی رفیعی کرکوندی[1*]، سید کامیار ایزدی[2]، ابوالفضل خوش‌صفت[3]

تاریخ دریافت: ۹۳/۰۴/۰۹
تاریخ پذیرش: ۹۳/۰۴/۰۱

چکیده

رشد روز افزون حجم اطلاعات و نداشتن امکانات کافی محاسباتی و ذخیره‌سازی، سازمان‌ها را با چالش‌های مدیریتی متنوعی رو به رو کرده است. وجود این چالش‌ها از یک سو و گسترش روز افزون سرویس‌های ذخیره‌سازی از سوی دیگر، سازمان‌ها را بر آن داشته تا نگهداری و مدیریت داده‌ها و پرس‌وجوهای خود را به ارائه‌دهنده‌گان خدمات فضای ذخیره‌سازی ابری واگذار نمایند. از آن‌جا که داده‌های سازمان درصورت استفاده از چنین سرویس‌هایی، در قالب برون‌سپاری خارج از محیط سازمان نگهداری می‌شود و داده‌ها تحت نظارت و کنترل مستقیم مالک داده نمی‌باشد، نگرانی‌های امنیتی به‌وجود می‌آید. برای مقابله با این نگرانی‌های امنیتی راه‌حل‌های بسیاری ارائه گردیده است اما بیشتر این راه‌حل‌ها بر روی جنبه خاصی از چرخه حیات داده مانند فازهای ذخیره‌سازی و استفاده، تاکید داشته‌اند. آشنایی با چرخه حیات داده و چالش‌ها و فرصت‌های فراروی سازمان‌ها می‌تواند کمک شایانی در ارائه راه‌کارهای مناسب برای بهبود این تکنولوژی جدید به‌همراه داشته باشد. در این مقاله ابتدا به بررسی چالش‌ها و فرصت‌های فراروی سازمان‌ها می‌پردازیم و در ادامه معماری جدیدی برای برون‌سپاری پایگاه داده با توجه به چرخه حیات داده ارائه می‌دهیم.

کلیدواژه‌ها: رایانش ابری، برون‌سپاری، چرخه حیات داده، امنیت برون‌سپاری، طبقه‌بندی اطلاعات، معماری برون‌سپاری

۱- کارشناس ارشد، دانشگاه شهید بهشتی تهران student.rafiee@gmail.com- نویسنده مسئول
۲- استادیار، دانشگاه شهید بهشتی تهران
۳-کارشناس ارشد، دانشگاه شهید بهشتی تهران

۱- مقدمه

با پیشرفت تکنولوژی‌های نو ظهور، حجم اطلاعات سازمان‌ها روز به روز در حال افزایش است. رشد روز افزون اطلاعات، کنترل و مدیریت داده‌ها را بیش از پیش پیچیده‌تر ساخته و هزینه‌های مربوط به آن را افزایش داده است. سازمان‌ها برای رویارویی با این مسئله می‌توانند تمهیداتی چون افزودن منابع ذخیره‌سازی و به‌کارگیری افراد اجرایی بیشتر و یا واگذاری مدیریت داده‌های خود به یک کارگزار خارجی[1] را در پیش گیرند. راه‌حل اول تا حدودی کنترل و مدیریت داده‌ها را آسان می‌سازد اما به سبب به‌کارگیری منابع ذخیره‌سازی و نیروی انسانی بیشتر، سبب افزایش هزینه‌های سازمان می‌گردد. از این‌رو سازمان‌های تمایل بیشتری به برون‌سپاری اطلاعات داشته و چنین سرویس‌هایی روز به روز در حال فراگیر شدن است.

برای اولین بار شرکت EDS[2] در دهه ۱۹۶۰ به اجرای خدمات گوناگون پردازش داده پرداخت. مبلغ قرارداد بین EDS و مشتریانش به مقدار چشم‌گیری پایین بود. در دهه ۱۹۸۰ برون‌سپاری فناوری اطلاعات به یک کسب و کار سودمند تبدیل شد و تعداد عرضه کننده‌گان و سطح تخصص آن‌ها افزایش قابل توجهی یافت. در این زمان، عرضه کننده‌گان، سرویس‌های خدماتی با کیفیت بالا و قیمت پایین تامین می‌کردند و این امر راه را برای برون‌سپاری کامل در سال ۱۹۹۰ هموار کرد. در آن زمان با تصمیم شرکت کوداک مبنی بر برون‌سپاری تمام فعالیت‌های فناوری اطلاعات خود به شرکت IBM[3]، دیگر سازمان‌ها اعم از دولتی و خصوصی به استفاده از این فن‌آوری ترغیب شدند. امروزه شرکت مایکروسافت تقریبا همه بخش‌های خود، از تولید نرم افزارهای کامپیوتری گرفته تا توزیع محصولات را برون‌سپاری می‌کند و خود تنها بر روی پردرآمدترین بخش یعنی نوشتن کد نرم‌افزار متمرکز شده است [۱].

با ظهور میزبانی محاسبات ابری و سرویس‌های ذخیره سازی، سرویس‌های برون‌سپاری داده در بستر رایانش ابری شکل تازه‌ای به خود گرفت. با پیشرفت فنآوری به‌عنوان سرویس، کاربران فقط به منابعی که برای انجام کارشان نیاز دارند دسترسی پیدا می‌کنند. بنابراین نیازی به پرداخت هزینه برای منابع مصرف نشده شبیه به روش سنتی ندارند. رایانش ابری علاوه بر این‌که باعث صرفه‌جویی در هزینه‌های سازمان می‌گردد به کاربران نیز امکان دسترسی به آخرین نرم‌افزارها و زیرساخت‌ها به‌منظور نوآوری در کسب و کار را ارائه می‌دهد.

با وجود این مزایا، به‌علت مدیریت داده توسط یک سازمان خارجی و عدم کنترل مستقیم مالک داده بر آن، چالش‌های امنیتی جدیدی در این زمینه مطرح می‌گردد. برای رویارویی با این چالش‌ها، راه‌حل‌های امنیتی زیادی ارائه گردیده است اما بیشتر این راه‌حل‌ها تنها بر جنبه خاصی از چرخه حیات داده مثل ذخیره‌سازی و استفاده متمرکز شده‌اند. در این مقاله سعی داریم چرخه امنیتی برون‌سپاری داده در بستر رایانش ابری را بررسی کرده و بر طبق آن سناریوی برون‌سپاری جدیدی را ارائه نماییم.

ساختار این مقاله به این صورت است که در بخش دوم مباحثی را پیرامون مفهوم پدافند غیرعامل و ضرورت توجه به آن مورد بحث و بررسی قرار می‌دهیم. سپس از آن‌جا که ویژگی‌ها و خصایص محیط برون‌سپاری پایگاه داده یکی از مهم‌ترین پارامترهای تاثیرگذار بر کمیت چالش‌های امنیتی بوده و مدل های تهدید متنوعی را معرفی می‌نماید، در بخش سوم به مباحث پیرامون رایانش ابری می‌پردازیم. در بخش چهارم، سناریو پایه برون‌سپاری پایگاه داده و مولفه‌های موجود در آن را مورد بحث و بررسی قرار می‌دهیم. در بخش پنجم مزایای برون‌سپاری داده در بستر رایانش ابری و چالش‌های موجود در آن را معرفی خواهیم کرد. در بخش ششم، چرخه حیات داده را معرفی می‌کنیم. در بخش هفتم، معماری‌های موجود برای برون‌سپاری را مطرح می کنیم. در بخش هشتم، نتایج تحلیل معماری های مطرح شده را مورد بحث و بررسی قرار می دهیم و در بخش آخر، نتایج حاصل از این پژوهش آورده شده است.

۲- پدافند غیرعامل

هر کشوری دارای نگرانی‌های امنیتی از ناحیهٔ سایر کشورها می‌باشد و تمایل دارد تا همه چیز را در مورد وضعیت آن‌ها بداند و از اطلاعات خودش در مقابل آن‌ها کمال حفاظت را بنماید. در این قرن که عصر اطلاعات نام‌گذاری شده است، تجربهٔ جنگ‌های اخیر در دو دهه قبل از عملیات توفان صحرا در جنگ خلیج فارس در سال ۱۹۹۱، جنگ کوزوو در سال ۱۹۹۹ و جنگ سلطه (اشغال عراق) در سال ۲۰۰۳ نشان می‌دهد که این جنگ‌ها عمدتا از ماهیت جنگ اطلاعاتی برخوردار بودند و جنگ‌های مدرن آتی نیز بر پایهٔ اطلاعات و تکنولوژی هدایت خواهند شد، زیرا قوای نظامی از سیستم‌های شناسایی با توانایی رویت، شنود، هدایت و همچنین

1– Service Provider
2– Electronic Data Systems
3– International Business Machines

نمود و با بهره‌گیری از تکنولوژی سنجش از راه دور ماهواره‌ای و غیر ماهواره‌ای خواهند توانست با قابلیت‌های دقیق تصویر برداری، شنود، و موقعیت‌یابی کرده و جنگ افزارها را هدایت نمایند. برای کشور ما که در معرض تهدیدات می‌باشد، این موضوع از حساسیت ویژه‌ای برخوردار است و طبیعی است که دشمن با صرف هزینه‌های گزاف به‌طور پیوسته مشغول جمع‌آوری، پردازش و تجزیه و تحلیل اطلاعاتی کشور به‌خصوص در بعد توانمندی‌های نظامی و استراتژیک می‌باشد. شناسایی و پایش مراکز، تجهیزات، سایت‌های حساس و فعّالیت‌های نظامی، اقتصادی و حیاتی کشور از اقدامات بدیهی دشمن برای استفاده در مقاصد فعلی و آینده‌اش می‌باشد. بنابراین با توجه به تلاش دشمنان کشور جمهوری اسلامی ایران در کسب این اطلاعات و نقش ماهواره‌ها در جنگ‌های احتمالی آینده، لازم و ضروری است تا با آشنایی و شناخت این توانایی‌ها و قابلیت‌های وسیع آن‌ها، راه‌کارهای مناسب مقابله با آن را پیش‌بینی نماییم. چنانچه این اقدامات انجام نگیرد با توجه به روند توسعه و پیشرفت تکنولوژی‌های جدیدتر روز به روز تهدیدات ناشی از کسب اطلاعات نظامی از کشور افزایش یافته و به عبارتی دیگر توان دفاعی کشور در معرض آسیب‌پذیری شدید قرار می‌گیرد .

فضای سایبر، حوزه‌ای بسیار وسیع و گسترده است که در حال ظهور در همه عرصه‌های زندگی بشری نقش ایفا می‌کند به‌طوری که امروزه تقریباً زندگی بشر در همه زمینه‌ها وابسته به دنیای مجازی است و دیگر نمی‌توان عرصه مجازی را از دنیای واقعی تفکیک نمود. جهان شمول بودن اینترنت و فضای سایبری موجب ظهور دنیای مجازی در کنار دنیای حقیقی شده است که معادلات سنتی حاکم بر زندگی بشر را دگرگون ساخته است. این دنیای جدید دارای ویژگی های جدیدی چون عدم وابستگی به زمان ومکان، عدم محدودیت (یا محدودیت کم) به قوانین حکومتی، تغییر هویت، جنسیت و غیر دارد. این مشخصات دنیای جدید، همان‌گونه که دستاوردهایی را همراه با خود دارد، تهدیدهای نیز علیه زندگی جوامع انسانی داشته و موجب آسیب‌هایی شده است. شناخت این آسیبپذیری‌ها و تهدیدات فضای مجازی جهت محافظت از انقلاب اسلامی می‌تواند یکی از کارکردهای پدافند غیرعامل باشد.

۳- رایانش ابری

نتایج مطالعات اخیر شرکت‌ها نشان می‌دهد به‌طور متوسط ۱۸٪ کاهش در بودجه فن‌آوری اطلاعات و ۱۶٪ کاهش در هزینه‌های منابع را از طریق بهره‌مندی از رایانش ابری به‌دست آورده‌اند [۲]. بسیاری از متخصصان تجاری و دانشگاهی سعی بر ارائه تعریف دقیقی از رایانش ابری و خصیصه‌های منحصر به فرد آن داشته‌اند. موسسه ملی فنآوری و استاندارد آمریکا[1] رایانش ابری را مدلی برای فراهم کردن دسترسی آسان، بر اساس تقاضای کاربر از طریق شبکه به مجموعه‌ای از منابع رایانشی قابل پیکره‌بندی (مثل شبکه، سرور، فضاهای ذخیره‌سازی، برنامه‌های کاربردی و ...) می‌داند و از جمله ویژگی‌های بارز آن را دسترسی سریع با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم کارگزار بر می‌شمارد [۳]. بی شک آنچه که رایانش ابری را به این درجه از محبوبیت رسانده، وجود خصیصه‌ها و ویژگی‌هایی چون مقیاس‌پذیری و قابلیت ارتجاعی، دسترس پذیری و قابلیت اعتماد، قابلیت اداره و برهم‌کنش‌پذیری، قابلیت دسترسی و جابه‌جایی، کارایی و بهینه‌سازی می‌باشد [۴].

۳-۱- مزایا و چالش‌های رایانش ابری

منافع رایانش ابری را می‌توان از دو دیدگاه سازمان و کاربران نهایی دسته‌بندی نمود [۵]. از دید سازمان، رایانش‌ابری سبب کاهش سرمایه‌گذاری اولیه، کاهش هزینه‌های سرمایه‌ای، بهبود تخصص صنعتی و بهبود بهره‌برداری از منابع در سازمان می‌گردد و از دید کاربران نهایی نیز منافعی چون کاهش قدرت محاسباتی محلی، کاهش قدرت ذخیره‌سازی محلی و تنوع Thin Client[2] در زندگی روزمره را به‌همراه دارد.

با توجه به این‌که رایانش ابری، انبوه متمرکزی از منابع را برای ما مهیا می‌سازد این نکته قابل تامل است که انبوهی متمرکز از خطرات و ریسک‌ها را نیز در بر می‌گیرد چرا که اگر روزنه‌ای از نقص و خطا در بخشی از ابر پدیدار گردد، آسیب بسیار بزرگ و غیرقابل جبرانی را برجای خواهد گذاشت. ابر مانند یک جعبه سیاه بزرگ عمل می‌کند و درون خود را از دید کاربران پنهان می‌سازد، بنابراین مالکان داده[3] هیچ‌گونه کنترل یا اریه ایده‌ای از خود برای درون ابر نخواهند داشت. با این وجود هر چند ارایه دهنده‌گان ابر صادق باشند، اما این خطر وجود دارد که مدیران مخرب سیستم به محرمانگی و جامعیت داده‌ها آسیب‌هایی را وارد نمایند.

۳-۲- مدل‌های استقرار رایانش ابری

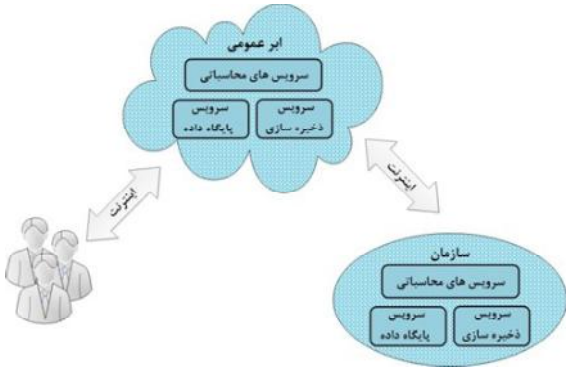
موسسه ملی فنآوری و استاندارد آمریکا مدل‌های استقرار

1- National Institute of Standards and Technology

۲- به کامپیوتر یا برنامه کامپیوتری اطلاق می‌شود که برای تحقق وظایف محاسباتی خود به کامپیوترهای دیگر وابسته است.

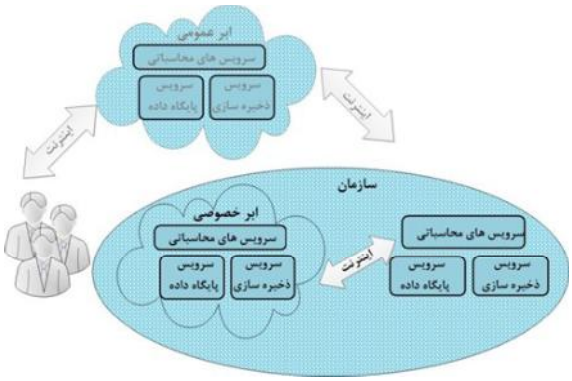
ریانش ابری را در چهار رده تقسیم‌بندی کرده است [۳]. تفاوت اصلی مدل‌های استقرا رایانش ابری در دامنه پوششی آن‌ها و همچنین دست‌یابی سرویس‌های ارائه‌شده در ابر می‌باشد.

ابر عمومی: در این مدل زیرساخت ابر برای استفاده عموم فراهم گردیده است و ممکن است توسط یک سازمان دولتی، دانشگاهی و یا تجاری مالکیت و مدیریت گردد. این نوع ابر توصیف‌کننده رایانش ابری در معنای اصلی و سنتی‌اش می‌باشد و بیشترین سطح چالش‌های امنیتی نیز در این مدل مطرح می‌گردد.



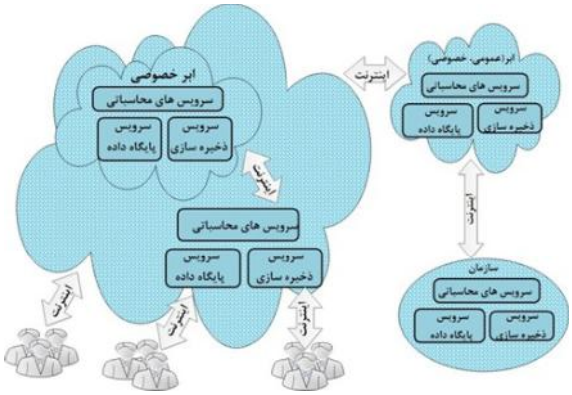
شکل ۱- ابر عمومی

ابر خصوصی: در این مدل زیرساخت ابر برای استفاده یک سازمان تکی که شامل چندین مشتری است، تهیه می‌گردد و ممکن است توسط خود سازمان، سازمان خارجی و یا ترکیبی از آن‌ها مدیریت و مالکیت گردد. مزیت اصلی ابر خصوصی امنیت بیشتر آن به‌دلیل استقرار تجهیزات در درون سازمان و عدم برقراری ارتباط با دنیای خارج می‌باشد.



شکل ۲- ابر خصوصی

ابر گروهی: در این مدل زیرساخت ابر برای استفاده انحصاری چندین سازمان که مشابهت‌های یکسانی از لحاظ ماموریت، سیاست‌های کاری و نیازمندی‌های امنیتی دارند فراهم می‌گردد و ممکن است توسط یک یا چند سازمان بهره‌گیرنده از این مدل، سازمان خارجی و یا ترکیبی از آن‌ها مدیریت و مالکیت گردد.

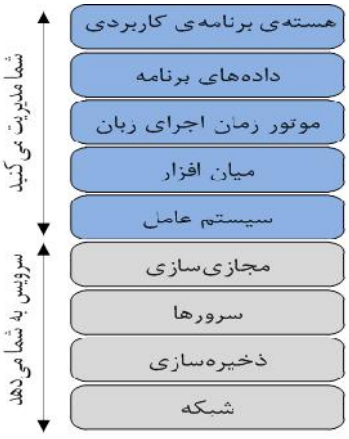


شکل ۳- ابر گروهی

ابر آمیخته: در این مدل زیرساخت ابر ترکیبی از دو یا چند ابر متمایز عمومی، خصوصی و یا گروهی می‌باشد. این نوع ابر گزینه مناسبی برای بیشتر موسسات تجاری به‌حساب می‌آید.

۳-۳. مدل‌های سرویس رایانش ابری

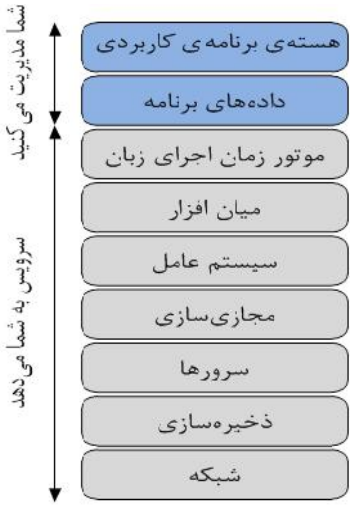
زیرساخت به‌عنوان سرویس: قابلیت ارائه‌شده برای مشتریان به‌منظور تامین منابع پردازشی، ذخیره‌سازی، شبکه و سایر منابع محاسباتی اساسی می‌باشد. در این سرویس مشتریان قادر به استقرار و اجرای نرم‌افزارهای دلخواه شبیه سیستم‌عامل یا دیگر برنامه‌های کاربردی می‌باشند. مشتریان کنترل و مدیریتی بر روی



شکل ۴- ابر خصوصی

زیرساخت ابر نداشته و آنچه می‌توانند مدیریت نمایند فضای ذخیره‌سازی، سیستم‌عامل، برنامه‌های کاربردی مستقر در ابر و تا حدودی کنترل بر اجزای شبکه است. نمونه‌هایی از این سرویس عبارتند از : Amazon EC2, Eucalyputs, OpenNebula [6].

بستر به‌عنوان سرویس: قابلیت ارائه‌شده برای مشتریان است که بر روی زیرساخت‌های ابر استقرار یافته و برنامه‌های کاربردی ابر را تغذیه می‌نماید. مشتریان، زیرساخت‌های ابر چون شبکه، سرور، سیستم‌عامل و منابع ذخیره‌سازی را کنترل و مدیریت نمی‌کنند بلکه آنچه مدیریت و کنترل می‌کنند برنامه‌های کاربردی مستقر بر روی زیرساخت ابر و پیکره‌بندی محیط میزبانی برنامه است. نمونه‌هایی از این سرویس عبارتند از : Microsoft Windows Azure, Google App Engine, Hadoop [۶].



شکل ۵- مدیریت و سرویس در بستر به عنوان سرویس

نرم‌افزار به‌عنوان سرویس: قابلیت تامین‌شده برای مشتریان است که اجرای برنامه‌های کاربردی بر روی زیرساخت ابر را ممکن می‌سازد. برنامه‌های کاربردی از طریق یک رابط Thin Client در دسترس مشتریان قرار می‌گیرند. مشتری زیرساخت‌های ابر چون شبکه، سرور، منبع ذخیره‌سازی و سیستم عامل را مدیریت و کنترل نمی‌کند و حتی در مورد تنظیمات برنامه‌های کاربردی نیز تنها تعداد محدودی از کاربران مجاز به پیکره‌بندی آن‌ها می‌باشند و کاربر تنها یک استفاده‌کننده محض از سرویس است. نمونه‌هایی از این سرویس عبارتند از: Gmail, Google Docs, Google sites [۶]

شکل ۶- مدیریت و سرویس در بستر به عنوان سرویس

۴- سناریوی پایه برون‌سپاری پایگاه داده

سناریوی برون‌سپاری داده برای اولین بار توسط هاسیگموس و همکارانش در سال ۲۰۰۲ با عنوان پایگاه‌داده به‌عنوان خدمت معرفی گردید. در واقع این سناریو، پدیده جدیدی در حوزه مدیریت و نگهداری داده ایجاد کرده است که در آن یک سازمان خارجی مسئولیت نگهداری پایگاه‌داده را برعهده می‌گیرد. از جمله مزایای این سناریو می‌توان به کاهش هزینه‌های مدیریتی، دسترس پذیری بالا و کار آمدی بیشتر اشاره‌کرد. مولفه‌ها و اجزای درگیر در سناریوی برون‌سپاری پایگاه‌داده عبارتند از:

مالک داده: به سازمانی اطلاق می‌شود که مالک حقیقی داده بوده و به‌دلایل مختلفی از جمله کاهش هزینه‌های مدیریتی و نگهداری، افزایش کارایی و دسترس‌پذیری، پایگاه‌داده را در فضای ذخیره‌سازی یک سازمان خارجی تحت یک آزادسازی کنترل شده برون‌سپاری می‌کند.

کاربر: کاربر یا پرسش‌گر موجودیتی است که با ابزاری نه چندان قوی از نظر محاسباتی و ذخیره‌سازی، پرس و جوها را به کارفرما ارسال و نتایج حاصل را دریافت می‌کند.

کارفرما: پرس‌وجوهای داده‌شده از طرف کاربر را به یک پرس و جو معادل برای اجرا شدن روی داده رمز شده سمت کارگزار تبدیل می‌کند. همچنین نتایج بازگشتی از سمت کارگزار را دریافت، رمزگشایی و پایش نموده و نتایج اصلی را برای کاربر ارسال می‌نماید.

کارگزار: سازمانی است که مسئولیت نگهداری و مدیریت پایگاه‌های داده برون‌سپاری شده را بر عهده دارد. این سازمان با فراهم آوردن زیر ساخت‌های سخت‌افزاری و نرم افزاری قوی، پایگاه‌داده سازمان‌های مختلف را میزبانی کرده و به پرس‌وجوهای کاربران پاسخ می‌دهد. کارگزار را می‌توان از لحاظ اجازه خواندن، نوشتن و تغییر در اطلاعات سازمان، به دو دسته قابل اعتماد و غیر قابل اعتماد تقسیم نمود. اگر کارگزار از نظر مالک داده یا کاربر، مجاز به خواندن، نوشتن و یا تغییر داده ذخیره شده در سمت خود باشد، کارگزار قابل اعتماد و در غیر این صورت غیرقابل اعتماد تلقی می‌گردد.

پایگاه داده: سطوح ریزدانگی در رمزنگاری پایگاه داده می‌تواند بر اساس تعدد دست‌یابی و نوع داده ، متفاوت باشد. برخی از این سطوح به قرار زیر است:

رابطه[1]: هر رابطه در یک پایگاه داده پس از اعمال تابع رمزنگاری به‌عنوان یک مقدار داده‌ای واحد در پایگاه داده رمزشده در نظر گرفته می‌شود . بنابراین تاپل‌ها و خصیصه‌ها در داده برون سپاری شده غیرقابل تمیزاند و نمی‌توانند در یک پرس و جو روی پایگاه داده، لحاظ گردند.

خصیصه[2]: هر ستون(خصیصه) در پایگاه داده به‌عنوان یک ارزش تکی در رابطه رمز شده تبدیل می‌شود.

تاپل[3] : هر سطر از پایگاه داده به‌عنوان یک ارزش تکی در رابطه رمز شده تبدیل می‌شود.

عنصر[4]: هر سلول در پایگاه داده به‌عنوان یک ارزش واحد در رابطه رمز شده تبدیل می‌شود.

با توجه به تعاریف بالا، رمزنگاری در سطح رابطه و خصیصه بر این موضوع دلالت دارند که برای یک پرس‌وجو بایستی کل رابطه شامل شده در پرس‌وجو به‌سمت کارخواه بازگردانده شود و بنابراین استخراج زیر مجموعه‌ای از تاپل‌ها در این نوع از ریزدانگی غیرممکن است. از طرف دیگر ریزدانگی در سطح عنصر نیز به کار اضافی برای مالک داده و کارخواه جهت رمزگذاری و رمزگشایی منجر می‌شود. برای ایجاد یک تعادل بین بارکاری کارفرما و کارایی اجرای پرس‌وجوها، بیشتر ارائه‌ها فرض می‌کنند که پایگاه داده در سطح تاپل رمزنگاری می‌شوند.

1– Relation
2– Attribute
3– Tuple
4– Element

رمزنگاری پایگاه داده یک سطح امنیتی نسبتا خوبی برای محافظت از داده‌ها تامین می‌نماید، اما این کار اجرای مستقیم پرس‌و جو بر روی داده‌های رمز شده را غیرممکن می‌سازد. در اصل کارفرما به‌محض دریافت یک پرس و جو، تنها می‌تواند رابطه رمزنگاری شده درگیر در پرس‌وجو را به درخواست کننده بفرستد و کارخواه مجبور است که کل رابطه برگشت داده‌شده را رمزگشایی نموده و پرس و جو را بر روی آن اجرا نماید. یک روش کاراتر برای اجرای پرس‌وجوها، استفاده از ترکیبی از روش‌های شاخص‌گذاری و رمزنگاری است. در این صورت کارفرما ، یک رابطه رمزگذاری‌شده را به‌همراه یک شاخص برای هر خصیصه ذخیره می‌نماید و به هنگام اجرای پرس و جو نیز از این شاخص‌ها استفاده کرده و تنها تاپل‌هایی را که شاخص نسبت داده به آن‌ها شرط مورد پرس‌وجو را ارضا می‌کند، به کارخواه باز می‌گرداند.

فرا داده

کارخواه و کارفرما به‌منظور مدیریت و دست‌یابی بهتر داده‌های برون‌سپاری شده، مبادرت به ذخیره‌سازی برخی اطلاعات اضافی به نام فرا داده می‌کنند. فرا داده‌ها در قالب جداول رابطه‌ای ذخیره شده و می‌توانند همانند داده‌های اصلی مورد پرس‌وجو قرار گیرند. به‌طور اساسی سه نوع فراداده اختیارات، توصیفی و مدیریت کلید وجود دارد [۱۹].

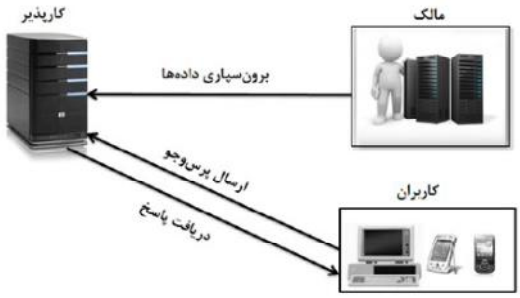
فراداده اختیارات: شامل اطلاعات مربوط به سیاست‌های کنترل دسترسی تعریف شده توسط مالک داده می‌باشد و به‌طور اساسی شامل دو رابطه است. یکی رابطه Tabuser که اطلاعات پیرامون کاربران سیستم را نگهداری می‌کند. و دیگری رابطه Access Matrix که اطلاعاتی پیرامون این‌که چه کسی، اجازه دسترسی به چه رابطه‌ای را دارد ، در بر می‌گیرد. از آنجایی که این جداول خیلی حساس هستند، توصیه می‌شود که در سمت کارخواه نگهداری شوند.

فراداده‌های توصیفی: توصیف‌کننده اطلاعات بوده و شبیه به کاتالوگ‌های سیستمی عمل می‌کند و شامل چهار رابطه است. رابطه Tabrelation که بیانگر تطابق بین نام رابطه اصلی و نام رابطه رمزشده می‌باشد. رابطه Tabindex نیز بیانگر تطابق بین نام یک خصیصه و نام شاخص متناظر با آن با توجه به‌روش شاخص‌گذاری استفاده شده می‌باشد. رابطه Tabmethod، اطلاعات مربوط به تابع درهم ساز استفاده‌شده برای یک روش

شاخص‌گذاری به‌همراه مقادیر متناظر با پارامترهای آن می‌باشد. رابطه EncrypAlgo اطلاعاتی پیرامون الگوریتم رمزنگاری به‌همراه مقادیر متناظر با پارامترهای آن را در بر می‌گیرد. فاش شدن این جداول امکان دسترسی به پایگاه داده‌های رمزشده را برای کاربران متخاصم مهیا می‌سازد، بنابراین نباید فراداده‌های توصیفی را در سمت کارفرما ذخیره‌سازی نمود.

فرا داده مدیریت کلید: شامل اطلاعاتی پیرامون روش اشتقاق کلید و مقادیر کلید تبادل شده بین مالکان داده و کاربران می‌باشد. استراتژی های متفاوتی برای ذخیره سازی این نوع فراداده وجود دارد، به‌عنوان مثال می‌توان آن‌ها را به‌طور کامل در سمت کارخواه و یا کارفرما و یا به‌طور ترکیبی بخشی از آن را در سمت کارخواه و بخش دیگر را در بخش کارفرما ذخیره نمود. استراتژی ذخیره‌سازی فراداده مدیریت کلید در سمت کارفرما سبب کاهش میزان حافظه مصرفی سمت کارخواه می‌شود اما پهنای باند بیشتری را مصرف می‌کند. با توجه به‌دلایل ذکرشده در بالا معمولا از حالت ترکیبی برای ذخیره‌سازی این نوع فراداده استفاده می‌شود.

در اغلب سناریوها فرض بر این است که کارفرما و مالک داده امن بوده و کارگزار نیز از نظر نگهداری داده و ارسال عمدی پاسخ اشتباه، قابل اعتماد است.



شکل ۷- سناریوی پایه برون‌سپاری پایگاه‌داده

۵. مزایا و چالش‌های برون‌سپاری پایگاه داده

رشد سریع فناوری اطلاعات و ارتباطات منجر به رشد ۵۲ درصدی هزینه‌های مدیریت و ذخیره‌سازی اطلاعات شده است. این هزینه‌ها شامل سخت‌افزار، نرم‌افزار و نیروی انسانی متخصص بوده و بسیاری از سازمان‌ها و ادارات از عهده پرداخت آن برنمی‌آیند. لذا این مسایل منجر به گسترش ایده برون‌سپاری داده گردید.

برون‌سپاری مزایای قابل توجهی چون کاهش هزینه‌های مدیریتی، دسترس‌پذیری بالا و کارآمدی بیشتر را به‌همراه دارد. از مهم‌ترین انگیزه‌های سازمان به‌منظور برون‌سپاری و مدیریت داده‌ها می‌توان به کمبود زیرساخت‌های سخت‌افزاری و نرم‌افزاری مناسب، کمبود نیروی انسانی متخصص، پیچیده شدن ماموریت‌ها و تمایل سازمان‌ها برای تمرکز روی اهداف اصلی اشاره کرد. اما با این وجود چالش‌ها و تهدیدهایی نیز در این زمینه وجود دارد. پیرامون طبقه‌بندی چالش‌ها و تهدیدهای موجود در برون‌سپاری پایگاه‌داده، تحقیقات بسیاری صورت پذیرفته است. بر طبق این تحقیقات، به‌طور کلی چالش‌ها و موانع برون‌سپاری داده در دو رده چالش‌های فیزیکی و چالش‌های منطقی تقسیم‌بندی می‌شود [۱۱]. چالش‌های فیزیکی بواسطه مسائلی چون خطاهای سخت‌افزاری و نرم‌افزاری، سرقت رسانه داده و بلایای طبیعی پدید می آیند و دسترس‌پذیری و محرمانگی داده را تحت تاثیر قرار می‌دهند. چالش‌های منطقی که در این زمینه مطرح‌اند نیز عبارتند از:

احراز اصالت: این چالش در دو سطح احراز اصالت کابر و داده مطرح می‌گردد. در سطح احراز اصالت کاربران، ارائه دهنده سرویس در واقع می‌خواهد اطمینان پیدا کند که داده یا پرس وجوی دریافتی، از سمت کابران مجاز صورت گرفته است یا خیر. در سطح احراز اصالت داده، ارائه دهنده سرویس می‌خواهد از منشا تولید داده و زمان تولید آن اطمینان حاصل نماید. برای رویارویی با این دسته از چالش‌ها می‌توان از روش‌های موجود برای امضای دیجیتال بهرمند گردید.

محرمانگی داده: در این سطح باید داده‌های برون‌سپاری‌شده برای ارائه دهندگان خدمات و کاربران غیرمجاز نامفهوم باشد. برای رویارویی با این سطح از چالش‌ها می‌توان از الگوریتم‌های رمزنگاری بهره‌مند گردید.

حریم خصوصی: این چالش نیز در دو سطح حریم خصوصی کاربر و داده مطرح می‌گردد. در سطح حریم خصوصی کاربر، ارائه دهنده خدمات نباید درباره پرس‌جوهای کاربر و نتایج بازگشتی حاصل از آن اطلاعی پیدا کند و در سطح حفظ حریم خصوصی داده نیز کاربران نباید اطلاعاتی بیش از آنچه که از کارفرما درخواست نموده‌اند دریافت نمایند. برای رویارویی با این چالش می‌توان از رمزنگاری و اعمال کنترل دسترسی بهره‌مند گردید.

1– Token

اطمینان از پرس‌وجو: این سطح، توانایی کاربر برای بررسی صحت، تمامیت و تازه‌گی پرس‌وجو را شامل می‌شود. صحت پرس‌وجو در واقع بیانگر این است که نتایج پرس‌وجو همه شرایط پرس‌وجو را پوشش داده و همچنین داده‌های بازگشتی همان داده‌های مالک بدون هیچ‌گونه دست‌کاری در آن باشند. تمامیت پرس‌وجو نیز بیانگر اطمینان از آن است که نتایج بازگشتی تمام مجموعه داده‌های درخواستی مشتری را در برگرفته و حاوی اطلاعات اضافه‌تر یا کمتر نباشد. همچنین تازه‌گی پرس‌وجو نیز بیانگر این مفهوم است که نتایج پرس‌وجو باید حاوی آخرین تغییرات اعمال شده در پایگاه داده باشد. اغلب روش‌های ارائه‌شده برای رفع این چالش، از مفاهیم امضای رقمی و ساختار احراز اصالت استفاده می‌کنند تا کاربر با استفاده از داده وارسی، اجرای صحیح پرس وجو ها توسط کارفرما را ارزیابی کند.

۶- چرخه حیات داده

امروزه امنیت داده به یکی از مسائل مهم رایانش ابری تبدیل شده است. در این باره تعداد زیادی راه‌حل‌های امنیتی ارائه گردیده است اما بیشتر آنها تنها بر بخشی از چرخه حیات داده متمرکز بوده‌اند و از آنجا که آسیب‌پذیری امنیتی در هر بخش از چرخه حیات داده می‌تواند سبب اختلال درکل امنیت داده گردد، می‌بایست به کلیه مراحل این چرخه توجه ویژه شود. در یک دسته‌بندی کلی می‌توان کل چرخه حیات داده را در سه وضعیت فعال، نیمه فعال و بایگانی خلاصه کرد. اتحادیه امنیت رایانش ابری[1]

شکل ۸- چرخه حیات

مفهوم چرخه حیات داده را در شش فرآیند تولید، ذخیره سازی، استفاده، اشتراک، آرشیو و انهدام ارائه داده است [۹].

ایجاد: این مرحله بیانگر رویه ایجاد داده می‌باشد. داده ممکن است سمت کارخواه[2] و یا حتی سمت کارفرما[3] تولید گردد.

ذخیره‌سازی: این مرحله بیان‌گر بارگیری و ذخیره‌سازی داده در محیط ابر می‌باشد و برای حصول اطمینان در ابر ممکن است داده در چندین گره[2] ذخیره شود.

استفاده و اشتراک: این مرحله بیان‌گر استخراج داده‌ها از ابر می‌باشد. داده‌ها می‌توانند توسط مالک داده مورد استفاده قرار گیرند و یا بین چندین شخص به اشتراک گذاشته شوند.

بایگانی: داده‌هایی که به‌طور موقت مورد استفاده قرار نمی‌گیرد، توسط کارفرما به مکان دیگری در ابر انتقال داده می‌شود.

انهدام: در این مرحله داده‌ها مطابق نظر مالک داده حذف می‌شوند و در این شرایط برای اطمینان از عدم فاش شدن اطلاعات، کارفرما می‌بایست داده‌های حذفی را در سمت خود نامعتبر و غیرقابل بازیافت نماید.

۷. بررسی برخی از سناریوهای موجود

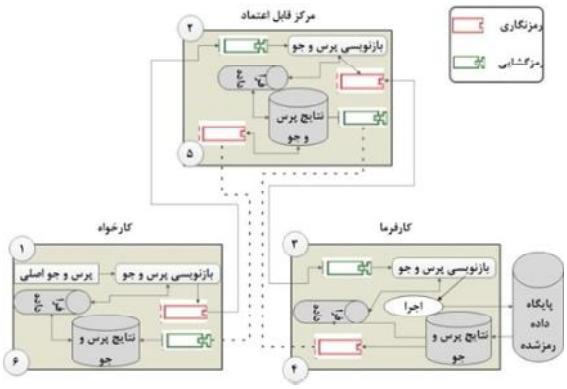
کادهم و همکاران [۱۲] یک معماری جدید برون‌سپاری پایگاه داده بر پایه حفظ محرمانگی پایگاه ارائه داده‌اند. نقش‌های موجود در این معماری عبارتند از: کارخواه، کارفرما و شخص سوم قابل اعتماد. در این معماری پرس‌وجوهای درخواستی کارخواه با توجه به فرا داده‌های موجود در این بخش به پرس‌وجوی جدیدی برای اجرا در سمت کارفرما بازنویسی می‌شود، سپس این پرس‌وجو به شخص سوم قابل اعتماد ارسال گردیده و در این بخش نیز با توجه به سیاست‌ها و کنترل‌های موجود، بازنویسی دیگری بر روی پرس‌وجو صورت می‌پذیرد و نهایتا پرس‌وجو تولیدی به کارفرما ارسال می‌گردد. در سمت کارفرما نیز بر روی پرس‌وجو دریافتی با توجه به فرا داده، تمهیدات لازم اتخاذ شده و پرس‌وجو نهایی بر روی پایگاه داده رمزشده اجرا می‌گردد. دادهای حاصل از اجرای پرس‌وجو به شخص سوم قابل اعتماد و سپس به کارخواه بازگردانده شده و فرآیند پرس‌وجو به اتمام می‌رسد.

هور و همکاران [۱۳] معماری برون‌سپاری جدیدی را بر پایه کنترل دسترسی ارائه دادند. این معماری شامل مولفه‌هایی چون

1- Cloud Security Alliance

2- Node

تامین‌کننده خدمات، مالک داده، کاربر و شخص قابل اعتماد صادر کننده اختیارات (TA[1]) می‌باشد. TA یک عنصر کلیدی در این معماری محسوب‌شده و پارامترهای عمومی و خصوصی مورد نیاز در سیستم را تولید می‌نماید. TA مسئول صدور، لغو و به‌روز رسانی کلیدهای کاربران بوده و با توجه به ویژگی‌های کاربران حقوق دسترسی متفاوتی را به آن‌ها ارائه می‌نماید. مالک داده مسئولیت تعریف سیاست‌های دسترسی، کنترل‌ها و تمهیدات امنیتی مورد نیاز قبل از برون‌سپاری پایگاه داده را برعهده دارد. کاربر در واقع عاملی است که می‌خواهد داده برون‌سپاری‌شده را مورد دست‌یابی قرار دهد. اگر کاربری مجموعه تمامی خصیصه‌های مورد نیاز برای ارضا کردن سیاست‌های دسترسی داده مورد نظر را داشته باشد، قادر خواهد بود تا به آنها دسترسی داشته و داده مورد نظر را رمزگشایی نماید. تامین کننده خدمات در واقع سرویس های برون‌سپاری را در اختیار کارخواهان قرار می‌دهد و مسئول مدیریت و کنترل داده‌های برون‌سپاری شده را برعهده دارد. در اغلب سناریوها فرض می‌شود که کارفرما از لحاظ نگهداری اطلاعات و پاسخ به پرس‌وجوها صادق بوده و نسبت به کسب اطلاعات در مورد داده‌های اصلی کنجکاو است [۱۶-۱۴].

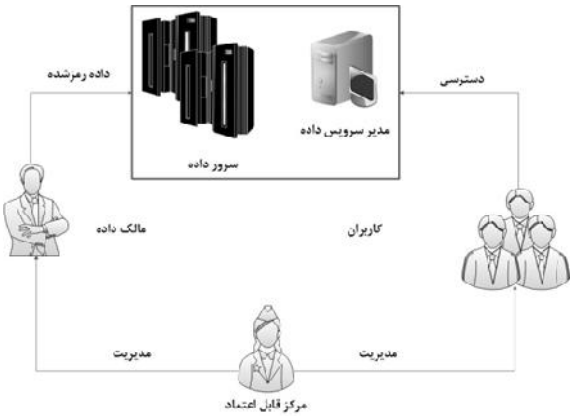


شکل ۹- معماری برون‌سپاری کادهم و همکاران

وایرمکاتی و همکاران [۱۷] معماری دیگری بر پایه حفظ محرمانگی و کنترل دسترسی ارائه کرده‌اند. در معماری ارائه شده دو نوع پایگاه داده به قرار زیر وجود دارد .

- پایگاه داده رمزشده حاوی داده‌های برون‌سپاری شده مشتریان.
- پایگاه داده محتوی سیاست‌های کنترل دسترسی به منظور مدیریت دستیابی اطلاعات سمت کارفرما.

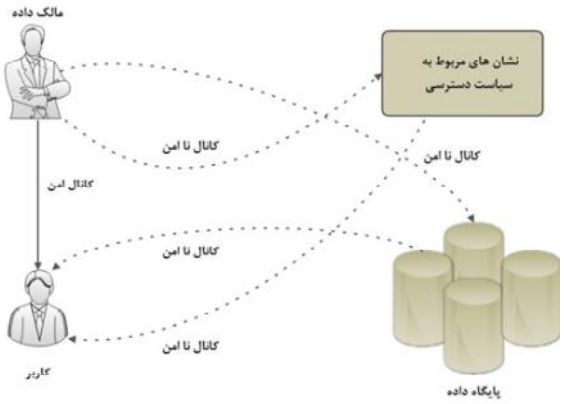
1– Metadata



شکل ۱۰- معماری برون‌سپاری هور و همکاران

پایگاه داده دوم در واقع به‌منظور تضمین دسترسی کاربران مجاز به پایگاه داده رمزشده مورد استفاده قرار می‌گیرد. ایده پایه لحاظ‌شده در این معماری آن است که ابتدا یک کلید محرمانه توسط مالک برای کاربر تولید شده و سپس کاربر با استفاده از این کلید و مجموعه‌ای از نشان‌ها[1] می‌تواند کلیدهای دیگری را نیز به‌دست آورد. فهرست نشان‌ها تنها برای کاربرانی که از قبل به کلید محرمانه دسترسی دارند، قابل دست‌یابی می‌باشد. مسئولیت فهرست نشان‌ها بر عهده مالک داده بوده و می‌بایست ارایه صحیحی از سیاست‌های دسترسی که مالک داده می‌خواهد بر روی داده‌های خود پیاده‌سازی کند، داشته باشد. کاربران مجاز، به‌منظور دسترسی به منابع داده مورد نظرخود می‌بایست از فهرست نشان‌ها، تمامی نشان‌های مورد نیاز را بازیابی نمایند.

فورستی [۱۸] یک معماری کلی با توجه به معماری‌های موجود برای برون سپاری پایگاه داده ارائه داده است که شامل چهار مولفه زیر می‌باشد.



شکل ۱۱- معماری برون‌سپاری وایرمکاتی و همکاران

مالک داده: مالک وظیفه تولید و برون‌سپاری داده به‌منظور قابل دسترس نمودن داده‌ها تحت یک آزادسازی کنترل شده برای کاربران را برعهده دارد.

کاربر: درخواست‌های خود را در قالب پرس‌وجو به سیستم تحویل می‌دهد.

کارخواه: پرس‌وجوی ارائه شده توسط کاربر را به یک پرس‌وجوی معادل، برای اجرا شدن روی داده رمزنگاری شده سمت کارفرما، تبدیل می‌کند.

کارفرما: داده‌های رمز شده توسط یک یا چند مالک را دریافت، ذخیره سازی و برای کاربران مجاز قابل دسترس می‌نماید.

به‌طور خلاصه مهم‌ترین گام‌های مورد نیاز برای اجرای یک پرس‌وجوی مطرح شده از طرف کاربر در این معماری نیز به قرار زیر است:

گام اول، تحویل پرس‌وجوی کاربر(Q) به کارخواه می‌باشد. در این گام کاربر نیازی به آگاهی از برون‌سپاری داده‌ها ندارد.

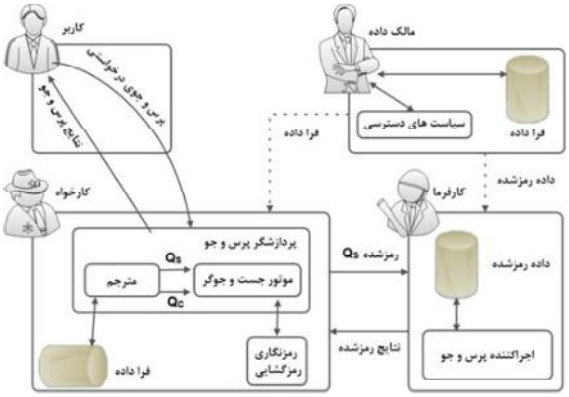
گام دوم، کارخواه پرس‌وجوی کاربر را به دو پرس‌وجوی Q_S و Q_C نگاشت می‌کند و سپس پرس‌وجوی Q_S را به کارفرما می‌فرستد.

پرس‌وجوی Q_S روی داده رمزشده عمل می‌کند و پرس و جوی اضافی Q_C روی نتایج حاصل از Q_S اعمال شده و نتایج برگشتی را پالایش نموده و جواب خالص را تولید می‌نماید.

گام سوم، کارفرما، پرس‌وجوی Q_S دریافتی را بر روی داده رمز شده اجرا نموده و نتایج حاصل از آن را که مجموعه‌ای از داده‌های رمز شده است به سمت کارخواه ارسال می‌نماید.

گام چهارم، کارخواه نتایج برگشتی از کارفرما را رمزگشایی نموده و در نهایت با اجرای Q_C بر روی آن، داده‌های خالص (داده‌های هدف) را به‌دست آورده و به کاربر می‌فرستد.

کلیه معماری‌های بیان شده در بالا تنها بر بخشی از چرخه حیات داده متمرکز هستند و از آنجا که آسیب‌پذیری امنیتی در هر بخش از چرخه حیات داده می‌تواند سبب اختلال در امنیت داده گردد می‌بایست به کلیه مراحل این چرخه توجه ویژه شود. طراحی یک معماری خوب برای سازمان‌ها این امکان را فراهم خواهد کرد تا خط مشی‌های مدیریتی، نیازهای کاربران و استراتژی‌های درونی سازمان با کمترین نیاز به تغییرات اعمال گردد.



شکل ۱۲- معماری برون‌سپاری هور و همکاران

۸- تحلیل و بررسی

تهدیدات مختلفی از آغاز تولید داده تا انهدام آن، امنیت داده را تحت تاثیر قرار می‌دهد. بنابراین می‌بایست در هر مرحله از چرخه حیات داده، تهدیدات را شناسایی و تمهیدات لازم را برای آنها اتخاذ نمود. در این بخش سعی داریم تا برخی سناریوهای ارایه‌شده دراین مقاله را از نظر چالش‌های امنیتی برون‌سپاری پایگاه‌داده مورد بحث و بررسی قرار دهیم. معیار مقایسه هر سناریو را بر پایه هشت چالش امنیتی مطرح در بخش پنجم و شش وضعیت چرخه حیات داده قرار داده‌ایم (شکل ۱۳). شکل (۱۴) معماری‌های موجود را براساس معیارهای شکل (۱۳) مورد مقایسه قرار داده است.

سناریوی کادهم و همکاران بر پایه حفظ محرمانگی طراحی گردیده‌است و تمهیدات امنیتی را برای رفع چالش‌های حفظ حریم خصوصی در دو سطح داده و کاربر، حفظ محرمانگی و همچنین احراز اصالت در سطح کاربر در دو فاز ذخیره‌سازی و اشتراک در نظر گرفته است. عیب این سناریو آن است که در هیچ یک از مراحل چرخه حیات داده، تمهیداتی را برای چالش‌های اطمینان از پرس‌وجو و احراز اصالت لحاظ نکرده است.

سناریوی فورستی بر پایه حفظ محرمانگی طراحی گردیده است و شامل تمهیدات امنیتی برای احراز اصالت در دو سطح کاربر و داده، محرمانگی و حفظ حریم خصوصی در سطح داده برای فازهای ایجاد، استفاده، اشتراک و ذخیره‌سازی می‌باشد. عیب این سناریو آن است که برای چالش حفظ حریم خصوصی در سطح کاربر و همچنین چالش اطمینان از پرس‌وجو، تمهیدات مورد نیاز لحاظ نشده است.

سناریوی هور و همکاران بر پایه کنترل دسترسی ارائه گردیده است و شامل تمهیدات امنیتی برای رفع چالش‌های احراز اصالت در دو سطح داده و کاربر، حفظ محرمانگی و حفظ حریم خصوصی در دو سطح داده و کاربر برای فازهای ایجاد، استفاده، اشتراک و ذخیره‌سازی در نظر گرفته شده است. با این وجود در این سناریو نیز چالش اطمینان از پرس‌وجو هنوز نیز وجود دارد.

سناریوی وایمرکاتی و همکاران بر پایه ترکیبی از کنترل دسترسی و حفظ محرمانگی بنا نهاده شده است و از لحاظ پوشش تمهیدات شبیه به روش هور و همکاران است با این تفاوت که در فاز استفاده از چرخه حیات داده، برای چالش‌های احراز اصالت، حفظ محرمانگی و همچنین حفظ حریم خصوصی تمهیدات امنیتی جامع‌تری در نظر گرفته شده است.

توجه به پیوستگی مراحل چرخه حیات داده به هنگام اتخاذ تمهیدات امنینی امری ضروری است، چرا که اگر نقص امنیتی تنها در یک مرحله از چرخه حیات داده صورت پذیرد در حالی‌که مراحل دیگر بهترین تدابیر امنیتی را لحاظ کرده باشند، می تواند امنیت کل چرخه حیات داده را تحت تاثیر قرار دهد. لذا در مقایسه‌های فوق پرواضح است که تمام قسمت‌های چرخه حیات داده در نظر گرفته نشده و تنها به بخشی از آنها اتکا شده است. لذا سناریوهای امن سناریوهایی هستند که برکلیه چرخه حیات داده توجه ویژه داشته باشد. لازم به‌ذکر است کارایی استفاده از هر معماری منوط به الگوریتم‌ها و پروتکل‌های استفاده‌شده در اجزا معماری برون‌سپاری دارد. ما در مقاله تمرکزمان بر روی معماری امن برون‌سپاری فارغ از الگوریتم‌ها و پروتکل‌های موجود برای اجزا است و در واقع هدف بررسی و امکان سنجی بستری مناسب و فراگیر برای توسعه امن برون‌سپاری می‌باشد.

که برکلیه چرخه حیات داده متمرکز باشد. لازم به‌ذکر است کارایی استفاده از هر معماری منوط به الگوریتم‌ها و پروتکل‌های استفاده‌شده در اجزا معماری برون‌سپاری آن دارد. ما در مقاله تمرکزمان بر روی معماری امن برون‌سپاری فارغ از الگوریتم‌ها و پروتکل‌های موجود برای اجزا است و در واقع هدف ایجاد بستری مناسب و فراگیر برای توسعه امن برون‌سپاری می‌باشد.

۹- نتیجه‌گیری

رشد روز افزون اطلاعات سازمان‌ها و نیاز به کاهش هزینه‌های ذخیره‌سازی و مدیریت داده‌ها سبب شده تا تمایل به برون‌سپاری داده‌ها روز به روز در حال افزایش باشد. هر چند برون‌سپاری سبب کاهش هزینه‌های مدیریت داده‌ها می‌گردد اما مشکلات و چالش‌های جدید امنیتی برای داده‌های برون‌سپاری شده ایجاد می‌نماید. طراحی یک معماری خوب برای سازمان‌ها این امکان را فراهم خواهد کرد تا خط مشی‌های مدیریتی، نیازهای کاربران و استراتژی‌های درونی سازمان با کمترین نیاز به تغییرات در کل سیستم اعمال گردد. از این‌رو ما در این مقاله به ارائه یک معماری جدید برون سپاری مطابق با چرخه حیات داده پرداخته‌ایم که این معماری با توجه به ویژگی‌های لحاظ‌شده در مقایسه با معماری‌های قبلی به لحاظ در نظر گرفتن چرخه حیات داده، امن‌تر است. همچنین با مطالعه این مقاله سازمان‌های مشتاق به برون سپاری پایگاه داده در بستر رایانش ابری قادر خواهند بود با محیط برون‌سپاری، ابعاد داده از لحاظ حساسیت و چرخه حیات، چالش‌ها و تهدیدهای پیش‌روی و راه‌حل‌ها و کنترل‌های امنیتی برون‌سپاری پایگاه داده در بستر رایانش ابری آشنا و تمهیدات لازم برای ارتقاء قابلیت اعتماد و اتکاپذیری بر خدمات برون‌سپاری را اتخاذ نماید.

شکل ۱۳- تهدیدات مطرح در هر یک از گام های چرخه حیات داده

چرخه حیات داده / چالش امنیتی		ایجاد	ذخیره‌سازی	استفاده	اشتراک	بایگانی	انهدام	تمهیدات امنیتی مورد نیاز
احراز اصالت	کاربر	✓	✓	✓	✓	✓	✓	روش‌های مبتنی بر امضای دیجیتال
	داده	✓	✓					
حفظ محرمانگی			✓	✓	✓	✓	✓	روش‌های مبتنی بر رمزنگاری
حفظ حریم خصوصی	کاربر	✓	✓	✓	✓	✓	✓	روش‌های مبتنی بر رمزنگاری و کنترل دسترسی
	داده		✓	✓				
حفظ جامعیت	صحت		✓	✓	✓			روش‌های مبتنی بر مفاهیم امضای دیجیتال و ساختار احراز اصالت
	تمامیت		✓	✓	✓			
	تازگی		✓	✓	✓			

شکل ۱۳- تهدیدات مطرح در هر یک از گام های چرخه حیات داده

چالش امنیتی	احراز اصالت		حفظ محرمانگی	حفظ حریم خصوصی		حفظ جامعیت		
سناریو	کاربر	داده		کاربر	داده	صحت	تمامیت	تازگی
کادهم و همکاران	۲و۴	-	۲و۴	۲و۴	۲و۴	-	-	-
هور و همکاران	۲و۳و۴	۱و۳	۲و۳و۴	۱و۲و۳و۴	۲و۴	-	-	-
وایرمکاتی و همکاران	۲و۳و۴	۱و۳	۲و۳و۴	۱و۲و۳و۴	۲و۴	-	-	-
فورستی	۲و۳و۴	۱و۳	۲و۳و۴	-	۲و۴	-	-	-

۱۰- مراجع

1. J. N. Lee, M. Q. Huynh, R. C. W. Kwok, and S. M. Pi, "IT outsourcing evolution: past, present, and future," Communications of the ACM, pp. 84-89, **(2003).**
2. P. Mcfredries, "Technically speaking: The cloud is the computer," Spectrum, IEEE 2008, pp. 20-20, **(2008).**
3. P. Mell and T. Grance, "The NIST definition of cloud computing (draft)," NIST special publication, pp. 1-8, **(2011).**
4. J. Q. Anderson and H. Rainie, "The future of cloud computing," Washington, DC, Pew Internet & American Life Project, **(2010).**
5. M. Miller, "Cloud computing: Web-based applications that change the way you work and collaborate online," Que publishing, **(2008).**
6. R. Buyya, J. Broberg, and Goscinski, "Cloud computing: Principles and paradigms," John Wiley & Sons, **(2010).**
7. R. Saint-Germain, "Information security management best practice based on ISO/IEC 17799," Information Management Journal, pp. 60-66, **(2005).**
8. L. Bouganim and P. Pucheral, "Chip-secured data access: Confidential data on untrusted servers," In Proceedings of the 28th international conference on Very Large Data Bases, **(2002).**
9. G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing v2. 1," Cloud Security Alliance, pp. 1-76, **(2009).**
10. C. Dong, R. Giovanni, and D. Naranker, "Shared and searchable encrypted data for untrusted servers," Journal of Computer Security, pp. 367-397, **(2011).**
11. E. Ferrari, "Database as a Service: Challenges and solutions for privacy and security," Services Computing Conference, **(2009).**
12. H. Kadhem, T. Amagasa, and H. Kitagawa, "A novel framework for database security based on mixed cryptography," In Internet and Web Applications and Services, Fourth International Conference IEEE, pp. 163-170, **(2009).**
13. J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," Parallel and Distributed Systems, IEEE Transactions on, pp. 1214-1221, **(2011).**
14. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security pp. 261-270, **(2010).**
15. S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," In Proceedings of the 33rd international conference on Very large data bases, pp. 123 -134, **(2007).**
16. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," In Information Security Applications, pp. 309-323, **(2009).**
17. S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "A data outsourcing architecture combining cryptography and access control," In Proceedings of the ACM workshop on Computer security architecture, pp. 63-69, **(2007).**
18. S. Foresti, "Preserving privacy in data outsourcing," Springer **(2010).**
19. E. Damiani, S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Metadata management in outsourced encrypted databases," In Secure Data Management, pp. 16-32, **(2005).**
20. E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM, **(2006).**

A novel architecture for database outsourcing in cloud computing with regard to data life cycle

M. Rafiee karkavandi[1]
S. K. Izadi[2]
A. Khoshsefat[3]

Abstract

The increasing amount of information as well as lack of existence of sufficient computational facilities and storage in organizations have caused various management problems. These problems on the one hand and the rapid expansion of storage services on the other hand have made different organizations to use cloud storage service providers in order to store and manage their organizational information. Using such services, causes organizational information to be stored outside of the organization environment and therefore the owner have less control over its information. Therefore, security concerns will be raised. Many security solutions are proposed to deal with these security concerns, but most of these solutions have focused on a particular aspect of data life cycle such as storage phases. Understanding and considering the data life cycle as well as the challenges and the opportunities facing organizations leads to provide appropriate solutions to overcome security concerns. This paper aims at discussing and analyzing the challenges and opportunities facing organizations using data outsourcing services, and then a new architecture for the database outsourcing with regards to the data life cycle will be presented.

Key Words: *Cloud Computing, Outsourcing, Data Life Cycle, Outsourcing Security, Data Classification, Outsourcing Architecture*

1- M.S Candidate of Shahid Beheshti University (student.rafiee@gmail.com) - Writer-in-Charge
2- Assistant Professor of Shahid Beheshti University
3- M.S Candidate of Shahid Beheshti University