مجله علمی ـ پژوهشی «پدافند الکترونیکی و سایبری»
سال اول، شماره ۳، پاییز ۱۳۹۲، ص ۷۱-۶۳

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

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

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

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

(دریافت: ۹۱/۰۷/۲۹، پذیرش: ۹۱/۱۲/۲۰)

چکیده

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

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

۱. مقدمه

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

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

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

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

[1] Cloud Computing
[2] Data Center
[3] Hosting
[4] Data Management
[5] Log
[6] Database As A Service
[7] Database Service Provider (Dbsp)