

افزایش امنیت داده در سیستم فایل توزیعی هادوپ با درهم ریختن بلاک‌های داده

علی چاوشی^۱، مرتضی آنالویی^۲، فرزانه ابازری^۳

^۱ دانشجوی کارشناسی ارشد معماری کامپیوتر، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران
ali.chavoshi@yahoo.com

^۲ دانشیار و عضو هیئت علمی دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران
analoui@iust.ac.ir

^۳ دانشجوی دکترای تخصصی دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران
f.abazari@gmail.com

چکیده

رایانش ابر^۱ به خاطر ارائه‌ی رایانش و پردازش بر حسب نیاز و در عین حال کاهش هزینه‌ها، به عنوان فناوریِ پردازشی آینده شناخته شده است. ولی مشکل امنیت داده در این فناوری به یکی از نگرانی‌های جدی در این حوزه تبدیل شده است. امنیت داده از ابعاد مختلفی قابل بررسی است. از بُعد دسترسی غیر مجاز به داده، دو نگرانی وجود دارد. نگرانی اول ناشی از دسترسی غیر مجاز یک کاربر ابر به عنوان مهاجم، به داده‌های دیگر کاربران ابر است. نگرانی دوم از دسترسی غیرمستولانه کارمندان ابر به داده‌های محرمانه کاربران ابر بوجود می‌آید. مبحث مورد بررسی در این نوشتار، نگرانی دوم یعنی دسترسی غیرمستولانه صاحبان و کارمندان ابر به داده یک کاربر است. البته بر طرف نمودن نگرانی دوم، قطعاً منجر به بهبود نگرانی اول نیز خواهد شد. برای این منظور روش‌هایی مطرح شده است که در کنار رمزنگاری داده، منجر به افزایش محرمانگی داده خواهد شد. با استفاده از این روش‌ها، برای دسترسی به داده، نیاز به تعامل با مالک داده خواهد بود. روش‌های ارائه شده در این نوشتار، مبتنی بر زیرساخت سیستم فایل توزیعی هادوپ^۲ در ابر است. سیستم فایل توزیعی هادوپ به عنوان مهم‌ترین زیرساخت در ذخیره و بازیابی داده در رایانش ابر مطرح است. یکی از مهم‌ترین سرویس‌هایی که از ابر انتظار می‌رود ارائه کند، ذخیره داده در حجم زیاد می‌باشد. ولی این سرویس بدون ضمانت کافی در امنیت داده دچار مشکل خواهد شد. با رویکردهای ارائه شده در این مقاله می‌توان امنیت و محرمانگی داده‌ی قرار گرفته شده بر روی ابر را به شکل قابل توجهی افزایش داد.

کلمات کلیدی

رایانش ابر، سیستم فایل توزیعی هادوپ، امنیت داده، رمزنگاری، مالک داده.

۱- مقدمه

استفاده فراگیر از آن، ابهامات و نگرانی‌های امنیتی در آن است. امنیت در رایانش ابر از جهات مختلف مورد توجه قرار گرفته است و یکی از مباحث مهم در حوزه فناوری اطلاعات است [3]. در این مقاله با رویکرد حفظ محرمانگی داده به موضوع امنیت داده در رایانش ابر پرداخته شده است.

حفظ محرمانگی داده در شرایطی که محل ذخیره سازی داده دور از موقعیت کاربر است و کنترل فیزیکی و منطقی مالک داده بر روی آن کم یا ناممکن است بسیار سخت می‌شود. در این شرایط دو نگرانی مطرح است. نگرانی اول از دسترسی غیر مجاز کاربران به اطلاعات و

در سالهای اخیر فناوری رایانش ابر به یک فناوری فراگیر و رو به رشد در صنعت فناوری اطلاعات تبدیل شده است. امکان تقاضای رایانش بر حسب نیاز، فضای ذخیره‌سازی بر حسب نیاز و همچنین قابل توسعه بودن آن از مزایای اصلی فناوری رایانش ابر می‌باشد [1]. ولی از طرف دیگر استفاده از منبع خارجی برای پردازش و ذخیره‌سازی اطلاعات، به شکل ذاتی منجر به کاهش امنیت داده و اطلاعات می‌شود [2]. از این رو یکی از اصلی‌ترین مشکلات فناوری رایانش ابر برای