

امنیت داده های ذخیره شده در ابر با استفاده از بهبود الگوریتم رمزنگاری متقارن



صدف نیک فطرت، محمد ابراهیم شیری

۱- دانشجوی کارشناسی ارشد، دانشگاه آزاد واحد بروجرد

۲- استادیار، دانشگاه علم و صنعت

Sadaf.nikfetrat@gmail.com

نام ارائه دهنده: صدف نیک فطرت

خلاصه

رایانش ابری پارادایم جدیدی است که به علت توانایی در کاهش هزینه های مرتبط امروزه به داغترین منطقه پژوهش تبدیل شده است. یکی از استفاده های اصلی از رایانش ابری، ذخیره سازی داده ها می باشد که امروزه بسیاری از شرکت ها با توجه به مزایای رایانش ابری از خدمات ذخیره سازی آن استفاده می کنند. ابر رایانه به کاربران خود اجازه می دهد که مقدار زیادی از اطلاعات خود را در ابر ذخیره سازی قرار دهد و در هر زمان و نقطه از جهان به آنها دسترسی داشته باشند. داده ها در ابر در مراکز داده ای گسترده و مقیاس پذیر قرار گرفته است که در همه جا قابل دسترسی می باشد در واقع داده های ذخیره شده و منابع را در محیطی باز مثل اینترنت منتشر می کند و چون از طریق اینترنت به کاربران خود سرویس می دهد مسائل امنیتی مثل حریم خصوصی، امنیت داده ها و محرمانه بودن را شامل می شود. با رشد کاربران ابر فعالیت های مخرب نیز افزایش یافته است. با توجه به اینکه میلیون ها کاربر ابر در حال گشت و گذار در ابر برای مقاصد مختلف می باشند، بنابراین نیاز به خدمات امن و پایدار ضروری است. به منظور ایجاد مسائل امنیتی در ابر از الگوریتم های رمزنگاری استفاده می شود. ما در این مقاله پیشنهاد یک مدل حفاظت از داده ها را داریم که در آن داده ها قبل از قرار گرفتن در ابر با استفاده از الگوریتم پیشنهادی رمزگذاری شده و بنابراین می توانیم محرمانه بودن و امنیت داده ها را بهبود دهیم.

کلمات کلیدی: رایانش ابری، امنیت داده در ابر، ذخیره سازی، رمزنگاری، تکنیک های متقارن.

۱. مقدمه

دنیای فناوری اطلاعات و اینترنت که امروزه تبدیل به جزئی حیاتی از زندگی بشر شده، روز به روز در حال گسترش است و همسو با آن و نیازهای اعضای جوامع مشکلاتی مانند پردازش سریع، دسترسی پویا و آنی، قدرت تمرکز روی پروژه های سازمانی به جای اتلاف وقت برای نگهداری سرورها، صرفه جویی در هزینه ها و از همه مهمتر، امنیت داده های ذخیره شده اهمیت زیادی یافته است. راه حلی که در عرصه ی فناوری اطلاعات برای چنین مشکلاتی پیشنهاد می شود تکنولوژی است که این روزها با نام رایانش ابری به آن پرداخته می شود. مفاهیم ابتدایی رایانش ابری به دهه ی ۱۹۶۰ میلادی بر می گردد [۱]. امروزه رایانش ابری به یک موضوع داغ در صنعت فناوری اطلاعات تبدیل شده است. گارتنر پیش بینی می کند تا سال ۲۰۱۵، ۱۰٪ از کل قابلیت های شرکت های امنیتی فناوری اطلاعات در ابر تحویل داده خواهد شد. با استفاده از مفهوم رایانش ابری ما می توانیم داده و برنامه های خود را به محل ارائه دهنده ابر حرکت دهیم و با این کار باعث کاهش هزینه های سرمایه گذاری، ریسک های عملیاتی، پیچیدگی و تعمیر و نگهداری، و افزایش مقیاس پذیری شویم. رایانش ابری نوآوری است که با استفاده از قدرت محاسباتی پیشرفته و قابلیت ذخیره سازی، بهبود یافته است و یک طرح پردازش جدید است که در آن پردازش کامپیوتر در شبکه انجام می شود، به این معنی که رایانش ابری مبتنی بر اینترنت است یعنی مدیریت برنامه و منابع محاسباتی را از طریق شبکه انجام می دهد و مانند یک استخر بزرگ از منابع محاسباتی (سرور، ذخیره سازی، سیستم عامل و شبکه)،