

ارزیابی روش های برقراری امنیت در محاسبات ابری و ارایه یک چارچوب مدیریت کلید و رمزگشایی سریع

در محیط ابری موبایل

پرستو شهابی^۱، مهدی فرخ بخت فومنی^۲

^۱ دانشجوی کارشناسی ارشد مهندسی نرم افزار کامپیوتر دانشگاه آزاد فومن و شفت Email: Shahabi_parastoo@yahoo.com

^۲ گروه کامپیوتر، واحد فومن و شفت، دانشگاه آزاد اسلامی، فومن، ایران Email: Farrokhbakht@gmail.com

که این نتیجه یعنی راین پژوهش می تواند از لحاظ کاربرد در ابرهای موبایلی بسیار مناسب باشد.

واژگان کلیدی: رایانش ابر، رایانش ابری موبایل، امنیت و طرح های CP-ABE گمنام.

۱- مقدمه

محاسبات ابری ایده ای است که به وسیله آن داده ها و برنامه ها می توانند به صورت متمرکز در ابر ذخیره شوند و در هر زمان و در هر نقطه قابل دسترسی باشند. تعاریف رسمی مختلفی برای محاسبات ابری وجود دارد موسسه استاندارد و فناوری ملی آمریکا محاسبات ابری را چنین تعریف می کند: «مدلی برای ایجاد سهولت در درخواست دسترسی به شبکه به منظور به اشتراک گذاردن مجموعه ای از منابع محاسباتی با قابلیت پیکربندی شدن (مانند شبکه ها، سرورها، سیستم های ذخیره سازی و سرویس ها) که سریعاً و با صرف کمترین عملیات مدیریتی و تعامل با فراهم کننده خدمات، قابل دسترس است» [۱]. سازمان ها به منظور بکارگیری خدمات ابری نیاز به تضمین امنیت کافی دارند تا دارایی های اطلاعاتی سازمان هایشان به مخاطره نیفتد. پیش از این امنیت را با استفاده از طرز کارها و سیاست های امنیتی مختلف برای سازمان خود فراهم می آوردیم و دارایی های سازمان خود را در پشت دیوارهای آتش، VPN و غیره پنهان می کردیم. حال با ظهور محاسبات ابری، نه تنها داده های شخصی و خصوصاً سازمانی در توده ابری قرار دارد که حتی محل آن معلوم نیست، بلکه برنامه های کاربردی و ابزارهای مختلفی که از آن ها استفاده می شوند نیز در چنین وضعیتی قرار دارند که مشخص نیست دقیقاً چه کدی را بر روی داده ها اجرا می کنند [۲]. اولین وظیفه ی امنیت، حفاظت از سرمایه های یک سازمان است که ممکن است شامل آیتم های ملموسی نظیر یک صفحه وب و یا بانک اطلاعاتی مشتریان و یا آیتم های غیرملموسی نظیر شهرت و اعتبار یک سازمان باشد.

چکیده: محاسبات ابری روشی نوین برای ذخیره داده ها و برنامه ها به صورت متمرکز در ابر می باشد و در هر زمان و هر نقطه قابل دسترسی است. یکی از چالش های کنونی این تکنولوژی تضمین امنیت کافی است تا دارایی های اطلاعاتی سازمان هایشان به مخاطره نیفتد. در روش های قبل امنیت را با استفاده از طرز کارها و سیاست های امنیتی مختلف برای سازمان فراهم می کردند و دارایی های سازمان خود را در پشت دیوارهای آتش، VPN و غیره پنهان می کردند. از دید سرویس دهندگان ابر، امنیت یک ضرورت مهم برای حفظ منابع و ایجاد اعتماد در کاربران است. در این پایان نامه از یک روش که در آن از یک تکنیک جدید ابتدا تطبیق سپس رمزگشایی استفاده شده است و نتیجه مطلوب این است که با در نظر داشتن افزایش زمان پاسخگویی تعداد جفت سازی لازم برای تطبیق و رمزگشایی به حداقل رسیده است. همچنین در این پژوهش روشی برای افزایش امنیت فایل های اشتراکی پیشنهاد شد که براساس آن از لینک های اشتراکی منحصر به فرد در بهره برداری از اطلاعات مشترک کاربران استفاده شد که باعث امنیت بالاتری گردید. در این پژوهش قالب امنیتی با نظارت بر روی تنظیمات، مدیریت و امنیت اطلاعات کار می کند و باعث شده فرایند کسب و کار و سرویس ها با حداقل ریسک ارائه شده و سطح خطاها کاهش یابد. این روش پیشنهادی می تواند در ابرهای موبایلی بخاطر زمان پاسخگویی مناسب استفاده گردد. در واقع سازمانی که محاسبات ابری را پذیرفته با استفاده از روش پیشنهادی، می تواند سرویس هایی مانند اطلاعات سلامت سرویس ها، هوش مصنوعی سرویس ساز نظر از نظر نوع مدل و سائز کلیدها و تعداد جفت سازی ها و اطلاعات بیومتریک آن ها در کسب و کار خود ارائه دهد. برای بخش شبیه سازی روش پیشنهادی با روش های یکسان (از نظر نوع مدل و سائز کلیدها و تعداد جفت سازی ها) مورد مقایسه قرار گرفت و یکی از نتایج مهم تعداد ثابت جفت سازی بوده که زمان پاسخگویی را نسبت به روش های دیگر بسیار کاهش می دهد. روش پیشنهادی در مقایسه با روش بدون استفاده از تطبیق زمان اتمام کلیه رمزنگاری و رمزگشایی پیام های مطلوب تری از خود نشان داده