سیستم های تشخیص نفوذ در شبکه های رایانش ابری: مطالعه و بررسی روش ها

زهرا مصطفی[۱]، مجید حق پرست[۲]، مهرداد مایین[۳]

[۱]گروه کامپیوتر، واحد یادگار امام خمینی (ره)شهرری، دانشگاه آزاد اسلامی، تهران، ایران ، zahramostafa7070@gmail.com
[۲] گروه کامپیوتر، واحد یادگار امام خمینی (ره)شهرری، دانشگاه آزاد اسلامی، تهران، ایران، haghparast@iausr.ac.ir
[۳] گروه کامپیوتر، واحد یادگار امام خمینی (ره)شهرری، دانشگاه آزاد اسلامی، تهران، ایران،mehrdad.maeen@gmail.com

چکیده

در عصری که پیچیدگی محاسبات در حال رشد و پیشرفت است و دسترسی به نتایج مورد نیاز بستگی به پردازش داده ها و اطلاعات بزرگ دارد، جهان محاسبات چاره ای جز به رسمیت شناختن استفاده از رایانش ابری ندارد. انتخاب هر یک از مدل های پیشرفته رایانش ابری (ابرهای ترکیبی، خصوصی، اجتماعی، عمومی) مدل های خدماتی مورد نظر را با سیاست های امنیتی مختلف فراهم می کند. یکی از مباحث مهم در شبکه های رایانش ابری، مسئله امنیت در این شبکه ها است که برای مدیران سازمان، نگرانی هایی از لحاظ دسترسی های بدون مجوز را فراهم نموده است. زمانی که از سیستم هایی توزیع شده و چند عامله در شبکه های رایانش ابری استفاده شود، مسئله امنیت دارای ضرورتی خاص می گردد. به منظور جلوگیری از این نگرانی ها، سیستم های تشخیص نفوذ معرفی شده اند. در این تحقیق سعی بر آن است تا با مطالعه روش های ارائه شده به صورت هوشمند، سیستم های تشخیص نفوذ در شبکه رایانش ابری، مورد مطالعه و تحقیق واقع شود.

کلمات کلیدی

رایانش ابری، سیستم تشخیص نفوذ، یادگیری ماشین، سیستم های هوشمند

مقدمه

امروزه شبکه های کامپیوتری به عنوان یکی از اصلی ترین بخش ها در ارتباطات و همچنین سایر صنایع، به کار گرفته می شود. مرتبط با هر صنعتی، می توان از ساختارهای مختلف شبکه ای استفاده و بهره جست. یکی از شبکه هایی که امروزه بیشتر از سایرین مورد توجه قرار گرفته است و دلیل آن به خاطر نگهداری داده ها در خود است و مانند یک هارد دیسک عمل می کند، شبکه رایانش ابری[۱] است. این شبکه متشکل از کامپیوترهایی است که در نقاط مختلف پراکنده هستند و هر کاربر با ثبت نام در آن می تواند عضویت داشته باشد. هر کاربری می تواند فایل های خود شامل فایل متنی، چند رسانه ای و غیره را در این محیط ذخیره سازی نماید و در هر زمان و مکانی با استفاده از رمز عبور و نام کاربری که دارد، وارد شده و به آن دسترسی داشته باشد. یکی از مباحثی که در همین قسمت حائز اهمیت است، امنیت در حریم خصوصی افراد می باشد، زیرا کاربران فایل های خود را به شبکه انتقال می دهند و ممکن است این فایل ها، از طریق سازمان ها ارسال شده باشد که دارای اهمیت خاصی می باشند و دسترسی هر شخصی به آن نباید مقدور باشد. لذا حفظ حریم خصوصی کاربران شبکه رایانش ابری، دارای ضرورت است.

با توجه به مسائل امنیتی که در شبکه رایانش ابری وجود دارد، باید بتوان از داده های کاربران در مقابل هرگونه نفوذی، ایستادگی و مقابله نمود. لذا سیستم هایی ارائه شده اند که به صورت خودکار، می توانند هرگونه عملیات مشکوکی را در طول شبکه رایانش ابری، شناسایی نمایند، اعم از ورودهای غیرمجاز، عبور از دیوار آتش[۲]، جلوگیری از ارسال داده های ویروسی و دارای انواع حملات و غیره است. این سیستم که به نام سیستم تشخیص نفوذ[۳] شناخته می شود، به عنوان یک نرم افزار جداگانه بر روی ساختار شبکه های رایانش ابری و حتی سایر شبکه های کامپیوتری، قابل نصب است. این سیستم توانایی محافظت از هرگونه نفوذ یا حمله ای در شبکه را بر عهده دارد. در واقع سیستم تشخیص نفوذ، مانند یک آنتی ویروس[۴] با دیوار آتشین اما از نوع پیشرفته، عمل می کند.

شبکه رایانش ابری

رایانش ابری منجر به تغییر دنیای فناوری اطلاعات[۵] شده است. این فناوری جدید با خدماتی چون تامین زیرساخت، هزینه نگهداری پایین، تضمین موجود بودن خدمات و داده ها، دسترسی سریع و مقیاس پذیری، توانسته است در سالیان اخیر، کاربردهای فراوانی در حوزه های مختلف داشته باشد. رایانش ابری دارای سه لایه انتزاعی است که شامل لایه سیستمی، لایه پلتفرم[۶] و لایه کاربردی است [۱]. لایه سیستمی، لایه انتزاع ماشین مجازی یک

[۱] Cloud Computing

[۲] Firewall
[۳] Intrusion Detection System (IDS)
[۴] Anti-Virus
[۵] Information Technology (IT)
[۶] Platform