استفاده از سیستم تشخیص نفوذ در شبکه های رایانش ابری

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

امروزه رایانش ابری به عنوان یک محیط ذخیره سازی با کاربردهای فراوان دیگر برای کاربران شبکه، شناخته شده است. این فناوری که پیشرفت شگرفی در ذخیره سازی داده ها و فناوری های زیر مجموعه آن ایجاد نموده است، با رشد فراوان سیستم های دیگر، دچار مشکلاتی شده است. از جمله این مشکلات، دسترسی افراد در هر زمان و هر کجا از هر سیستمی به محیط ابر است. لذا ممکن است سیستم مبدا آلوده باشد. لذا ممکن است سودجویان، با ارسال یک بسته آلوده، شبکه را به تباهی بکشانند. لذا در نظر گرفتن یک سیستم که بتواند آلودگی بسته ها را تشخیص بدهد دارای ضرورت است. این نفوذها که به صورت بسته در می آیند می توانند شبکه را مختل و سرعت پاسخ به درخواست کاربران آن را تا حد بالایی، کاهش دهند. از این رو، سیستم های تشخیص نفوذ ایجاد شدند که با هدف شناسایی، تشخیص و جلوگیری از بروز هرگونه بسته ای که خارج از مجوز باشد، را انجام می دهد. ضرورت وجود سیستم تشخیص نفوذ در شبکه های رایانش ابری مانند سایر شبکه های کامپیوتری، دارای اهمیت بالایی است تا بتوان از بروز هرگونه مشکلی از جمله داده های آلوده به نفوذ در شبکه، جلوگیری نمود. در این تحقیق مقدمات اصلی استفاده از سیستم تشخیص نفوذ و مبدا ایجاد آن در شبکه ارائه و سپس به بررسی چند روش پیشین در همین حوزه پرداخته می شود.

کلمات کلیدی

رایانش ابری، امنیت، سیستم تشخیص نفوذ، تشخیص حملات

مقدمه

یکی از جالب ترین ساختارهای شبکه، شبکه رایانش ابری[۱] است که امروزه دارای محبوبیت فراوانی است. فناوری های مختلفی در شبکه رایانش ابری وجود دارد. دسترسی بیسیم برای محیط های بیسیم جهت مدیریت منابع از پروتکل تغییر یافته ای به نام 802.11a برای لایه MAC و از CSMA/CA به عنوان برنامه دسترسی رسانه انتقال استفاده می شود. در حقیقت، پروتکل 802.11p با استفاده از مدولاسیون FDM و حداکثر محدوده پوشش دهی امواج رادیویی را مشخص کرده و یک دامنه چند کیلومتری را سیگنال دهی می کنند. یکی از مباحث مهم در چنین شبکه ای، دسترسی های مجاز و غیرمجاز به داده های موجود است.

امنیت[۲] در ابر نیز چالشی بزرگ به حساب می آید، به طوری که در حال حاضر بزرگ ترین مانع در اتخاذ یک ابر توسط سازمان ها و شرکت ها، مسئله امنیت است. به دلیل طبیعت توزیع پذیری این سیستم ها، محیط ابر می بایست دارای امنیت بالایی باشد. امروزه سازمان های تجاری بزرگ اقدام به قرار دادن داده های خود در یک ابر می کند و بدون داشتن نگرانی به عنوان یک فراهم کننده خدمات ابر اقدام به ذخیره سازی، نگهداری داده و اجرای نرم افزار بر روی سیستم می کنند. واگذاری کنترل در داده و برنامه های کاربردی به عنوان یک چالش امنیتی به شمار می رود که شامل جامعیت، محرمانگی و در دسترس پذیری است. به دلیل ایجاد یک محیط امن، از سامانه هایی به نام سیستم تشخیص نفوذ[۳] جهت کشف حملات و هرگونه حرکت مشکوکی در طول شبکه استفاده می گردد. در واقع این سامانه به صورت نرم افزاری است و بر روی یک سرور، نصب می شود و می تواند تمامی فعالیت های شبکه را کنترل نماید.

شبکه رایانش ابری

شبکه رایانش ابری، شبکه ای است که با قرار دادن تعدادی سرور، امکان ارسال و دریافت فایل کاربران در آن وجود دارد که از طریق اینترنت خارج از محدوده زمانی و مکانی، این امر را میسر می

[۱] Cloud Computing

[۲] Security
[۳] Intrusion Detection System (IDS)