

عنوان تحقیق :

مبارزه با حملات سایبری در شبکه های ابری با استفاده از یادگیری ماشین

استاد راهنما : دکتر محسن چگین و استاد مشاور : دکتر حمید

براتی ، گروه مهندسی کامپیوتر ، معماری ، دانشگاه آزاد اسلامی ، واحد دزفول ، ایران ،

دانشجو افسانه بساطی

گروه مهندسی کامپیوتر ، دانشگاه آزاد اسلامی ، واحد دزفول ، دزفول ، ایران

afsaneh.besati.93@gmail.com

چکیده:

امروزه رایانش ابری مکانیزم در حال ظهور برای محاسبات سطح بالاست. ابرها بر حسب میزان هزینه و تقاضای کاربران اطلاعات را دریافت و ارسال می کنند. در این مقاله برای برقراری امنیت در شبکه های ابری و جلوگیری از حمله های انکار از سرویس (DOS) روشی را به کار می بریم که با استفاده از الگوریتم یادگیری ماشین و با استفاده از تکنیک عامل متحرک تشخیص نفوذ را بسیار سریعتر انجام خواهد داد. در این رویکرد به کمک عامل های متحرک، اطلاعات مربوط به تشخیص نفوذ در کل شبکه پخش نشده بلکه در همسایگی عاملها منتشر خواهد شد. در این روش، توپولوژی شبکه را به صورت خوشه بندی و با انتخاب سر خوشه ایجاد می کنیم که در واقع هدف ما از اینکار بهینه کردن دو پارامتر انرژی مصرفی و کاهش فاصله است. روش پیشنهادی پس از شبیه سازی با الگوریتم EVDF مقایسه شده است در این شبیه سازی پس از 2000 امین بار اجرا، تمام گره های روش پیشنهادی هنوز هم انرژی دارند در صورتی که در روش EVDF انرژی هر گره به زیر 0/1 رسیده است. در بخش های دیگر ارزیابی و مقایسه مشاهده شد که روش EVDF در 5000 بسته ی ردو بدل شده می تواند تنها 30 درصد از حمله را تشخیص دهد. در حالیکه در روش پیشنهادی 35 درصد از حملات تشخیص داده می شود. به همین دلیل است که روش پیشنهادی باعث بهبود پارامترهای فاصله و انرژی و نیز باعث افزایش طول عمر شبکه می شوند.

1- مقدمه

توجه به تکامل در عرصه رایانش ابری روش های بسیاری جهت توزیع منابع و پیشرفت استفاده از داده ها از قبیل خوشه بندی داده ها، رایانش توری و سیستم مدیریت پایگاه داده های توزیع شده معرفی شده اند. امروزه رایانش ابری مکانیزم در حال ظهور برای محاسبات سطح بالا به عنوان یک سیستم ذخیره سازی تلقی می شود که در آن ابرها به کاربران خود بر مبنای میزان استفاده از منابع هزینه دریافت کرده و سرویس های خود را در اختیار آن ها قرار می دهند. از این رو می توان سرویس های ابری را در ایجاد انگیزه برای شروع یک کسب و کار با هزینه های مالی پایین تر سهیم دانست. رایانش ابری بسته به نوع توزیع منابع از سه لایه زیرساخت به عنوان سرویس، پلتفرم به عنوان سرویس و نرم افزار کاربردی به عنوان سرویس تشکیل شده است. [1]. در پایین ترین سطح، که لایه زیرساخت به عنوان سرویس (IaaS) نامیده می شود، پردازنده، حافظه و اجزای سخت افزاری توسط فراهم کننده سرویس ابری ارائه می گردد. لایه میانی یا پلتفرم به عنوان سرویس (Paas) میزبان محیط های مختلف برای ارائه خدمات می باشد. در آخر، بالاترین لایه نرم افزار کاربردی به عنوان سرویس (SaaS) است که دسترسی به این خدمات از طریق وب سرویس ها و مرورگرهای وب صورت می گیرد. Google, Amazon Ec2, App و Salesforce به ترتیب نمونه های لایه های ارائه شده رایانش ابری می باشند. واضح است که رایانش ابری گام بعدی تکامل سرویس های فناوری اطلاعات بر حسب تقاضا می باشد. با این حال مسئله امنیت در رایانش ابری یکی از مسائل پیچیده به شمار رفته که تمامی سه لایه ابر، مسئولیت هایی که بین کاربران و ارائه دهندگان تقسیم می شود و حتی شخص ثالث را درگیر می کند. مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم های رایانش ابری قلمداد می شود. براساس بررسی های انجام شده در سال 2010 میلادی همانگونه که در شکل 1 نشان داده شده است، امنیت به عنوان مهم ترین چالش شبکه های ابری از میان 8 چالش موجود شناخته شده است. تازه ترین بررسی ها در سال 2012 حاکی از کاهش 33.5 درصدی چالش امنیت و رسیدن این درصد به عدد 55 می باشد. [2]