همایش پژوهش های نوین در علوم و فناوری
Conference on Recent Research in Science and Technology

# بررسی چالش‌های امنیتی در رایانش ابری

**عزیزه زینالی خسروشاهی [۱]، شهرام بابائی[۲]، احسان قاسمی [۳]**

*[۱و۲] گروه مهندسی کامپیوتر، دانشگاه آزاد اسلامی واحد تبریز، تبریز، ایران*

*Stu.azeinaly@iaut.ac.com*

*[۳] گروه مهندسی برق، دانشگاه غیر انتفائی پیام گلپایگان، گلپایگان، ایران*

**چکیده**

*به لطف شبکه‌های کامپیوتری و پیشرفت در علوم الکترونیک، شبکه‌های رایانش ابری با قابلیت دسترس پذیری خارج از زمان و مکان، امکان ارتباط کاربران با یکدیگر را فراهم نموده اند. محاسبات ابری در رابطه با نرم افزار خود، هنوز در مراحل ابتدایی است. هنگامی که منابع در حال استفاده نیستند، هزینه کل از رفتن به سمت ابر تقریبا صفر است. بنابراین جای تعجب نیست که تحقیقات علمی و صنعت به سمت محاسبات ابری در حال حرکت است. زمانی که از سیستم‌هایی توزیع شده و چند عامله در شبکه‌های رایانش ابری استفاده شود، مسئله امنیت دارای ضرورتی خاص می‌گردد. به منظور جلوگیری از این نگرانی‌ها، سیستم‌های تشخیص نفوذ و همچنین یک سری چارچوب‌های امنیتی، معرفی شده اند. در این تحقیق سعی بر آن است تا با مطالعه روش‌های ارائه شده به صورت هوشمند، سیستم‌های تشخیص نفوذ و چارچوب‌های پیشنهادی در شبکه رایانش ابری، مورد مطالعه و تحقیق واقع شود.*

**کلمات کلیدی:** رایانش ابری، امنیت، سیستم تشخیص نفوذ، یادگیری ماشین، سیستم‌های هوشمند.

## ۱. مقدمه

امروزه شبکه‌های کامپیوتری به عنوان یکی از اصلی‌ترین بخش‌ها در ارتباطات و همچنین سایر صنایع، به کار گرفته می‌شود. مرتبط با هر صنعتی، می‌توان از ساختارهای مختلف شبکه‌ای استفاده و بهره جست. یکی از شبکه‌هایی که امروزه بیشتر از سایرین مورد توجه قرار گرفته است و دلیل آن به خاطر نگهداری داده‌ها در خود است و مانند یک هارد دیسک عمل می‌کند، 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 می‌تواند عضویت داشته باشد. هر کاربری می‌تواند فایل‌های خود شامل فایل متنی، چند رسانه‌ای 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 می‌باشد، زیرا کاربران فایل‌های خود را به شبکه انتقال می‌دهند و ممکن است این فایل‌ها، از طریق سازمان‌ها ارسال شده باشد که دارای اهمیت خاصی می‌باشند و دسترسی هر شخصی به آن نباید مقدور باشد. لذا حفظ حریم خصوصی کاربران شبکه رایانش ابری، دارای ضرورت است.

[1] Cloud Computing

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 سیستم‌هایی ارائه شده اند که به صورت خودکار، می‌توانند هرگونه عملیات مشکوکی را در طول شبکه رایانش ابری، شناسایی نمایند، اعم از ورودهای غیرمجاز، عبور از دیوار آتش[۲]، جلوگیری از ارسال داده‌های ویروسی و دارای انواع حملات و غیره است. این سیستم که به نام سیستم تشخیص نفوذ[۳] و همچنین جلوگیری از نفوذ[۴] شناخته می‌شود، به عنوان یک نرم افزار جداگانه بر روی ساختار شبکه‌های رایانش ابری و حتی سایر شبکه‌های کامپیوتری، قابل نصب است. این سیستم توانایی محافظت از هرگونه نفوذ یا حمله‌ای در شبکه را بر عهده دارد. در واقع سیستم تشخیص نفوذ، مانند یک آنتی ویروس[۵] با دیوار آتشین اما از نوع پیشرفته، عمل می‌کند.

## ۲. شبکه رایانش ابری

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 سیستم‌هایی ارائه شده اند که به صورت خودکار، می‌توانند هرگونه عملیات مشکوکی را در طول شبکه رایانش ابری، شناسایی نمایند، اعم از ورودهای غیرمجاز، عبور از دیوار آتش[۶]، جلوگیری از ارسال داده‌های ویروسی و دارای انواع حملات و غیره است. این سیستم که به نام سیستم تشخیص نفوذ[۷] و همچنین جلوگیری از نفوذ[۸] شناخته می‌شود، به عنوان یک نرم افزار جداگانه بر روی ساختار شبکه‌های رایانش ابری و حتی سایر شبکه‌های کامپیوتری، قابل نصب است. این سیستم توانایی محافظت از هرگونه نفوذ یا حمله‌ای در شبکه را بر عهده دارد. در واقع سیستم تشخیص نفوذ، مانند یک آنتی ویروس[۹] با دیوار آتشین اما از نوع پیشرفته، عمل می‌کند.

یک سیستم رایانش ابری را می‌توان این گونه بیان نمود: ارائه خدمات نرم افزاری و سخت افزاری از طریق اینترنت به کاربران و سازمان‌ها در تمام سطوح. نرم افزار، قدرت پردازشی، ظرفیت ذخیره سازی داده و پایگاه داده، از جمله خدماتی هستند که یک سیستم رایانش ابری از طریق شرکت‌های فراهم کننده منابع زیر ساخت، در اختیار کاربران قرار می‌گیرد. کاربر به ازای خدماتی که استفاده می‌کند، هزینه پرداخت می‌کند. در سیستم‌های رایانش ابری، فضای کار بر روی داده‌ها و اطلاعات از روی یک سیستم شخصی به یک واحد ابر در اینترنت، منتقل می‌شود. لذا کاربران در هر زمان و در هر مکانی از دنیا به راحتی می‌توانند به داده‌ها و اطلاعات خود دسترسی داشته باشند.

رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه ای از منابع رایانشی قابل‌تغییر و پیکربندی (مانند شبکه ها، سرورها، فضای ذخیره سازی، برنامه‌های کاربردی و خدمات) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم فراهم کننده سرویس به سرعت فراهم شده یا آزاد گردد. بر اساس این تعریف، پنج ویژگی ضروری شامل اشتراک منبع رایانش مجازی، دستیابی به شبکه گسترده، قابلیت انعطاف سریع، سلف سرویس درخواستی (بنا بر سفارش و تقاضا)، خدمات اندازه‌گیری شده را برای ابر در نظر گرفته است. همچنین گره‌ها در شبکه رایانش ابری به دو دسته ثابت و متحرک تقسیم می‌شوند. گره‌های ثابت گره‌هایی هستند که در یک مکان استقرار یافته و شبکه را به صورت ایستا تبدیل می‌کنند. در چنین حالتی فقط چند گره سینک وجود دارد که با تحرک پذیری، اطلاعات را از گره‌ای به گره دیگر با سرعت بالا ارسال و به پایگاه مرکزی می‌فرستد. در مقابل، گره‌های متحرک، در ابعاد شبکه حرکت می‌کنند و می‌توانند در هر مکانی خارج از بُعد، به ارسال داده‌ها بپردازند. از مشکلات آن دسترس پذیری پایین و مصرف انرژی بالا می‌باشد.

[۲] Firewall
[۳] Intrusion Detection System (IDS)
[۴] Intrusion Prevention Systems (IPS)
[۵] Anti-Virus
[۶] Firewall
[۷] Intrusion Detection System (IDS)
[۸] Intrusion Prevention Systems (IPS)
[۹] Anti-Virus

### ۳. سیستم تشخیص نفوذ

یکی از مهمترین مسائل موجود در شبکه‌های کامپیوتری امروزی، مبحث امنیت است که به یک چالش پیچیده تبدیل شده است. جهت ایمن سازی شبکه‌ها، ابزارهایی به وجود آمده اند که یکی از آن‌ها سیستم تشخیص نفوذ است. سیستم‌های تشخیص نفوذ ابزارهای امنیتی هستند که مانند سایر اندازه گیرهای امنیتی مانند نرم افزارهای آنتی ویروس[۱۰]، دیوار آتش و نمودارهای کنترل دسترسی، امنیت اطلاعات در سامانه‌های ارتباطی را تقویت می‌نمایند. سیستم‌های تشخیص نفوذ یکی از راهکارهای موجود برای نظارت بر وضعیت امنیتی شبکه‌ها و تحلیل آن‌ها می‌باشند. در تشخیص نفوذ، هم از ترافیک معمول و هم از ترافیک حمله استفاده می‌شود[۲]. یک سیستم تشخیص نفوذ مجموعه‌ای از فعالیت‌ها است که با هدف محافظت و برقراری امکان دسترسی امن به منابع توسعه یافته است[۲]. سیستم‌های تشخیص نفوذ با وضع کردن قوانین خاصی عملکرد کاربران را محدود و بر روی آن نظارت می‌کنند[۲].

سیستم تشخیص نفوذ، سیستمی است که به نظارت رویدادهای سیستم کامپیوتری به منظور کشف فعالیت های مشکوک و ایجاد هشدار می پردازد [۳]. یک سیستم تشخیص نفوذ نرم‌افزاری است که فرایند کشف تخلف را خودکار می‌کند. سیستم تشخیص نفوذ نرم افزاری است که دارای همه قابلیت های سیستم کشف تخلف است و می تواند تلاش کند و رویدادهای ممکن را متوقف سازد. این بخش مروری بر فناوری‌های سیستم تشخیص نفوذ و سیستم‌های جلوگیری از نفوذ[۱۱] خواهد داشت. عموما استفاده از یک دیوار آتش برای محافظت در برابر حملات جهت امن سازی سیستم مورد استفاده واقع می‌شود. جهت ایمن سازی سیستم‌ها، به مکانیزم‌های امنیتی بالاتری مانند سیستم تشخیص نفوذ نیاز است، زیرا دیوارهای آتشین توانایی تشخیص حملات در شبکه را ندارند. اما ممکن است که درصد بالایی از نفوذها از شبکه باشد و سیسم تشخیص نفوذ می‌تواند عملیات نظارت و تجزیه و تحلیل رویدادهای گوناگون را در شبکه انجام بدهد و اگر اشکالی در یک بخش باشد، آن را سریعا به مدیر شبکه گزارش می‌کند.

طبق منابع اطلاعاتی، سیستم تشخیص نفوذ به دو دسته کلی تقسیم می‌شود که یکی برپایه میزبان[۱۲] است و دیگری برپایه شبکه[۱۳] [۴]. سیستم تشخیص نفوذ مبتنی بر میزبان به شناسایی حملات در مقابل یک میزبان منفرد می‌پردازد. این روش بر روی سیستم‌هایی که آسیب پذیری بیشتری برای حمله به وب سرور دارند، مورد استفاده واقع می‌شود. این سیستم به گرداوری اطلاعات از تماس‌های سیستم، مسیر ردپای سیستم عامل، ورودهای برنامه‌های کاربردی، و غیره می‌پردازد[۴]. دو نمونه از سیستم تشخیص نفوذ برپایه میزبان OSSSEC و Tripwire هستند. سیستم تشخیص نفوذ مبتنی بر شبکه به شناسایی و تشخیص حملات در سیستم‌های گوناگون در شبکه می‌پردازد. این سیستم از ترافیک شبکه جهت تشخیص فعالیت‌های مشکوک استفاده می‌کند که هدف آن جلوگیری از دسترسی‌های غیرقانونی به منابع شبکه است[۵]. چند نمونه از سیستم‌های تشخیص نفوذ برپایه شبکه شامل Cisco Secure IDS، BRO، SNORT، Dragon و غیره است.

### ۴.مطالعه‌ای بر روش‌های پیشین

مبحث امنیت در سیستم‌های رایانش ابری، بحثی بزرگ است که سعی این پژوهش، مطالعه و تحقیقی مختصر از آخرین روش‌های بهینه در این زمینه می‌باشد. یکی از مباحث امنیتی در بستر ابر، سیستم‌های تشخیص نفوذ هستند، همچنین ارائه یک سری چارچوب‌ها در این بین نیز وجود دارد که به صورت دوگانه در این تحقیق به آن‌ها پرداخته می‌شود. در [۶] به امنیت سیستم‌های ابری[۱۴] در مقابل حملات HTTP-DOS و XML-DOS پرداخته اند. یکی از تهدیدات بسیار جدی در محیط ابر، HTTP-DSO و XML-DOS است. اگر یکی از این حملات ابر رخ دهد، آن را به طور بالقوه می‌تواند فلج سازد. HDOS حمله ایست که به طور بالقوه برای محاسبات ابری کشنده است، زیرا دقیقا روی HTTP است که متکی به برقراری ارتباط با خود و دیگر سیستم ابر است. جهت پیدا کردن منبع از این حملات، یک دنبال کننده ردپا در هر مرحله از طریق دنبال کننده عملیات

[10] Anti-Virus
[11] Intrusion Prevention System (IPS)
[12] Host IDS (HIDS)
[13] Network IDS (NIDS)
[14] Cloud Computing System

در ابر ارائه شده است. نتایج نشان می‌دهد که سیستم ساخته شده قادر به شناسایی منبع حمله و فیلتر کردن بسیاری از پیام‌های حمله در یک دوره کوتاه است. همچنین حمله مهم دیگری که مورد بحث واقع شده است، XDOS نام دارد که حمله مرگباری است که با هدف خرابی خدمات ابر، ایجاد می‌شود. برای دفاع در برابر این حملات ، مدلی به نام CBT را معرفی شده است. CBT نشان داد که می‌توان آن را در یک حمله XDOS واقعی استفاده کرد. نتایج نشان داد که CBT، قادر به پیدا کردن منبع یک حمله در هر ثانیه است.

در [۷] به ارائه یک سیستم تشخیص نفوذ در سیستم رایانش ابری پرداخته شده است. ایده بدین صورت است که بسته ارسالی از طریق یکی از پروتکل‌های IP، UDP، TCP و یا ICMP در صف قرار می‌گیرد. سپس با قوانینی که در سیستم تشخیص نفوذ از قبل تعبیه شده است، بسته ارسالی چک می‌شود. در صورتی که دارای مورد مشکوکی باشد، ورود را منقضی اعلام می‌کند، در غیر این صورت، دسترسی انجام می‌گیرد و به کاربر یک گزارش داده می‌شود. در [۸] امنیت رایانش ابری با استفاده از چهار روش سیستم تشخیص نفوذ AM-Clust، Honeyd، Honeywall و Honeycomb مورد مطالعه و بررسی واقع شده است. این مقاله یک رهیافت جدید در معماری زیر ساخت ابر را ارائه می‌دهد که به ترکیب سیستم تشخیص نفوذ برپایه ریز عامل‌های متحرک با استفاده از سه نوع هانی پات[15] می‌پردازد.

در [۹] به ایجاد یک سیستم تشخیص نفوذ در رایانش ابری پرداخته شده است که مبتنی بر یادگیری تقویتی[16] است. روش یادگیری تقویتی Q است که باعث توسعه کنترل کننده تطبیقی بلادرنگ[17] برای یک منبع پویا در سیستم رایانش ابری شده است. نتایج نشان می‌دهد که روش ارائه شده در ۹۰ روز، حمله ای را شناسایی نکرد و مشکلی در سیستم به وجود نیامد. رویکرد دیگر این پژوهش این است که کنترل کننده تطبیقی سیستم تشخیص نفوذ یاد می‌گیرد که ظرفیت ورودهای مانده را کاهش بدهد که در ۹۹ روز، ۱۱,۹٪ بهینه سازی در حافظه و سرعت شده است. در [۱۰] به مطالعه یک سیستم تشخیص نفوذ مبتنی بر روش‌های هوش مصنوعی در مرکز داده‌های ابر پرداخته شده است. مقاله به سیستم تشخیص نفوذی اشاره می‌کند که به صورت خودکار عملیات به روز رسانی فعالیت‌های کاربران مشکوک در ابر را انجام می‌دهد و زمانی که کاربر جدیدی قصد دسترسی به فایل‌های دیگر در ابر را دارد و یا حتی استفاده از ابر را می‌خواهد، ابتدا با پایگاه داده‌های موجود در سیستم تشخیص نفوذ عملیات مقایسه انجام می‌شود که از طریق یک مدیر این کار انجام می‌شود. با یک دید منطقی و منتقدانه می‌توان گفت که این روش به منظور این که نظارتی بر روی مدیر نیست، زیاد روش جالبت توجهی نمی‌باشد. نکته دیگر انتقادانه از این کار، این است که اگر حجم کاربران ابر زیاد شود، مدیریت سیستم تشخیص نفوذ امری پیچیده و سخت می‌شود. لذا برای سیستم‌های ابری کوچک، این روش می‌تواند با صرف نظر از مدیریت بر روی مدیر سیستم، جالب باشد.

در [۱۱] به ارائه یک سیستم تشخیص نفوذ سریع و امن با همکاری شبکه‌های چند موضوعی[18] (نخی) به صورت سیستم تشخیص نفوذ شبکه‌ای و سیستم تشخیص نفوذ مبتنی بر میزبان پرداخته شده است. در این سیستم تشخیص نفوذ در ابر، بسته‌ها از شبکه دریافت می‌شوند، سپس مورد تجزیه و تحلیل قرار می‌گیرند و سپس گزارشی به مدیر ابر به منظور تحلیل بیشتر ارسال می‌شود. این مدیر، در واقع مدیر صاحب همان ابری است، یعنی کاربر ابر و در نبود ابر، سیستم به طور خودکار کار می‌کند. که به عنوان مزیت اصلی کار شناخته می‌شود. روش تحلیل برپایه مدل ترکیبی الگوریتم نزدیک‌ترین همسایه K [19] و شبکه عصبی[20]، طبقه بندی و تحلیل می شود. به منظور آموزش و تست داده ها، از مجموعه داده‌های NSL-KDD استفاده شده است. بعد از دریافت گزارشی از سیستم تشخیص نفوذ ابر، فراهم کننده خدمات ابر، یک هشدار برای کاربر به منظور حفظ و نگهداری فایل‌های کاربر در زمان نبود وی جهت جلوگیری از بدافزارها و مالویرها تولید می‌کند و سپس به تشخیص و جلوگیری از حملات احتمالی می‌پردازد.

[15] Honeypot
[16] Reinforcement Learning
[17] Real-time Adaptive Controller
[18] Multi-threaded
[19] K-Nearest Neighbor (KNN)
[20] Neural Network

در [۱۲] به استفاده از الگوریتم ژنتیک اَبَر گراف[۲۱] برای بهینه سازی پارامترها و انتخاب بهترین ویژگی‌ها در تشخیص نفوذ و همچنین به کارگیری ماشین بردار پشتیبان[۲۲] جهت این تشخیص ها، پرداخته شده است. شناسایی و تشخیص بر اساس بهترین نرخ دقت و کمترین خطا، مدنظر این کار می‌باشد. در [۱۳] به ترکیب سیستم‌های فازی ژنتیکی[۲۳] و یادگیری جفتی[۲۴] جهت ارتقای نرخ تشخیص انوع حملات در یک سیستم تشخیص نفوذ پرداخته شده است. از جمله مزایای این روش آن است که منطق فازی به دلیل عدم قطعیتی که در تشخیص نفوذها دارد، امر را اسده تر کرده که با استفاده از توابع عضویت[۲۵]، متغیرهای زبانی، برچسب ها، قوانین و سطح فازی[۲۶]، می‌توان آن را تولید نمود. همچنین طرح یادگیری تفسیر و تسخیر می‌تواند به عنوان یک رویکرد جالب توجه با در نظر گرفتن یک فضای حالت و جستجو با رویکرد تکاملی، مدنظر واقع شود تا بتوان حملات را تشخیص داد.

در [۱۴] به استفاده از الگوریتم بهینه سازی کلونی مورچگان[۲۷] جهت تشخیص نفوذ پرداخته شده است. ارائه یک سیستم تشخیص فازی با استفاده از منطق فازی[۲۸] و ترکیب آن با آنتروپی[۲۹] به منظور انتخاب ویژگی‌ها و سپس ایجاد یک محیط بلادرنگ برای طبقه بندی و تشخیص این نفوذها، با استفاده از الگوریتم کلونی مورچگان انجام گرفته است. در [۱۵] به ارائه یک سیستم ترکیبی طبقه بندی مبتنی بر روش‌های هوش ازدحامی[۳۰] در سیستم‌های تشخیص نفوذ پرداخته شده است. روش ترکیبی استفاده استفاده از روش‌های ماشین بردار پشتیبان همراه با نزدیک ترین همسایه K به همراه الگوریتم ازدحام ذرات بهینه[۳۱] می‌باشد. دو روش ماشین بردار پشتیبان و نزدیک ترین همسایه K برای طبقه بندی بر اساس فواصل و داده‌های ورودی می‌باشند و الگوریتم ازدحام ذرات بهینه جهت ایجاد وزن‌ها به منظور ایجاد یک محیط طبقه بند با بهترین دقت می‌باشد. داده استفاده شده نیز KDDCUP99 است. در تحقیق دیگری که در [۱۶] ارائه شده است، به استفاده از الگویتم ازدحام ذرات بهینه به منظور بهبود سیستم تشخیص نفوذ موجود پرداخته شده است. این ساختار از برنامه نویسی خطی استفاده می‌کند و به منظور بهبود طبقه بندی روش MCLP به کار گرفته شده است. داده استفاده شده نیز KDDCUP99 می‌باشد.

تا به این جا، روش‌های توضیح داده شده به عنوان سیستم تشخیص و جلوگیری از نفوذ بودند. در ادامه به بررسی چند راهکار جدید که مبتنی بر ارائه رهیافت و چارچوب جهت حفظ امنیت در محیط‌های ابری ارائه شده اند، پرداخته می‌شود. در [۱۷] مطالعه و تحقیق راجع به استفاده از دستگاه‌های امنیتی و نرم افزارهای موجود در آن در محیط ابر پرداخته شده است. در این رویکرد، جایابی استفاده از دستگاه‌ها به عنوان یک مسئله مهم برشمرده می‌شود و مسئله مهم دیگر، نرم افزارهای موجود در آن به منظور حفظ امنیت است. هدف کلی، بهبود امنیت، کاهش هزینه ها و دارای کارایی بالا است. نرم افزارهای امنیتی شامل دیوار آتشین، سیستم تشخیص و جلوگیری از نفوذ، سیستم شناسایی منبع پنهان[۳۲] که اصطلاحا NAT نیز نامیده می‌شود و رمزنگاری IPSec می‌باشد. در تحقیق دیگری که در [۱۸] ارائه شده است، یک چارچوب امنیتی در سطح پلتفرم به عنوان خدمات[۳۳] در محیط‌های چند ابری ارائه شده است. این امر منجر می‌شود که کاربران بتوانند از سطح امنیت حساب‌های کاربری خود مطلع گردند و بتوان میزان حافظه مصرف شده بر اساس فعالیت‌های پیشین خود را مشاهده کنند. ارتقای دو DSL در چارچوبی به نام CAMEL که پیش‌تر در [۱۹] شده بود، منجر به پوشش دهی امنیت در بستر ابر گردیده است. به صورت کلی، مدیر ابر می‌تواند فعالیت‌های داخلی و خارجی کاربران را مشاهده و نظارت نماید. همچنین یک مطالعه موردی و بسیار کامل در زمینه سیستم‌های تشخیص نفوذ به همراه چارچوب‌های ارائه شده در مسئله امنیت در محیط ابری در [۲۰]

[21] Hyper Graph Genetic Algorithm (HGGA)
[22] Support Vector Machine (SVM)
[23] Fuzzy Genetic Algorithm (FGA)
[24] Pairwise Learning
[25] Membership Functions (MFs)
[26] Fuzzy Surface
[27] Ant Colony Optimization (ACO)
[28] Fuzzy Logic
[29] Entropy
[30] Swarm Intelligence
[31] Particle Swarm Optimization (PSO)
[32] Source Identity Hiding (SIH) / NAT
[33] Platform as a Service (PaaS)

ارائه و تدوین شـــده اســـت. این تحقیق با در نظر گرفتن اهداف گوناگونی هم چون دســـترس پذیری، مقیاس پذیری، انعطاف پذیری، زمان استفاده از منابع و ارائه محیطی کاربر پسند، مسئله امنیت در روش‌های پیشین را مورد مطالعه قرار داده است.

### ۵.داده‌ها و ابزارها

در زمینه سیستم‌های تشخیص نفوذ در محیط ابری، یک مجموعه داده معتبر وجود دارد که CIDD [۳۴] می‌باشد که دارای حملاتی چون شامل DoS، U2R، R2P، SP و AUB می‌باشد. این مجموعه داده دارای یک سری ورود[۳۵]های مختلف در شبکه ابری است که همراه با یک سری حمله بوده است. همچنین شامل روش‌های تزریق شده به آن به صورت ماتریسی نیز می‌باشد. اکثر حملات این داده در پروتکل‌های مبتنی بر اینترنت و TCP رخ می‌دهد. همچنین داده دیگری به نام KDD CUP [۳۶] نیز وجود دارد که نسخه‌های متنوعی از سال ۱۹۹۸ الی ۲۰۱۶ دارد که شامل حملات مختلف در بین سال‌های نام برده می‌باشد که به آن اضافه شده است.

اصولا سیستم‌های تشخیص نفوذ در ابر در محیط‌های توسعه یافته ایجاد می‌شوند. از جمله ابزارهایی که می‌توان از آن جهت پیاده سازی رویکردهای مختلف بهره جست، شبیه سازهایی چون NS-3، NS-2، OPNet، OMNet++، JSIM، QualNET، GloMoSIM، CloudSIM، GNS3 و MATLAB است. با توجه به این که اکثر شبیه سازهای شبکه‌های کامپیوتری دارای پیچیدگی‌های بالایی هستند و دارای یک سری روش‌ها و ابزارها نیستند و باید به زبان‌های برنامه نویسی JAVA و یا C++ به آن‌ها فایل سرآیند[۳۷] و کتابخانه‌ای[۳۸]، الحاق نمود، زیرا استفاده از آن‌ها سخت و مرسوم نمی‌باشد. لذا استفاده از یک محیط توسعه یافته به نام MATLAB می‌تواند جهت ارزیابی، امری ساده تر تلقی گردد. مشکل استفاده از هرکدام از این شبیه سازها به صورت جداگانه بیان شده است (گرچه هرکدام مزایایی نیز دارند که از آن‌ها چشم پوشی می‌گردد):

- ✓ CloudSim: قابلیت استفاده از روش‌های تکاملی و هوش ازدحامی در آن سخت می‌باشد و می‌بایست به زبان C++ کد شده و به عنوان یک کتابخانه در این شبیه ساز، فراخوانی و اجرا شود. همچنین نیزاب به یک سری توابع به صورت فایل‌های سرآیند با پسوند h. نیز می‌باشد.
- ✓ NS-2 یا NS-3: نصب این دو شبیه ساز بسیار پیچیده و سخت است و به کارکیری یک سیستم تشخیص نفوذ، نیاز به نصب یک سری بسته‌های جداگانه به عنوان افزونه را طلب می‌کند. همچنین کدها باید به زبان tcl نوشته شوند و بخش‌های اصلی الگوریتم پیشنهادی به زبان C++ نوشته و الحاق گردد.
- ✓ OPNet: این شبیه ساز نسخه‌های رایگان جالبی در ایران ندارد و استفاده از آن ریسک بالایی در به خطر افتادن روش‌های پیشنهادی به عنوان ایده در انواع شبکه ها محسوب می‌شود.
- ✓ OMNet++: یک شبیه ساز قدرتمند است، اما نصب آن پیچیده و نیاز به ابزارهایی برای به راه انداختن دارد و باید کدهای روش پیشنهادی نیز با زبان C++ نوشته و الحاق گردد.

سـایر شـبیه سـازها شـامل JSIM، QualNET و GNS3: فاقد کتابخانه‌های لازم برای شبیه سازی این رویکرد و به کارگیری شـبکه رایانش ابری و سیستم‌های تشخیص نفوذ می‌باشند و بایستی تمام بخش‌ها به زبان C++ و Java کد شده و الحاق گردد که امری پیچیده و زمان بر است.

### ۶.نتیجه‌گیری

شبکه‌های رایانش ابری با هدف در دسترس بودن داده‌ها در هر محیطی خارج از زمان و مکان برای کاربران، تعبیه شده اند. این شبکه به دلیل میزان دسترس پذیری کاربران بالا و اشتراک گذاری فایل‌ها، می‌تواند دچار مسائل امنیتی بالایی شود. لذا مطالعه و تحقیق راجع به روش‌های امنیتی در این حوزه، به شدت امری ضروری است. در این تحقیق، سعی بر آن شده است که

[34] http://www.di.unipi.it/~hkholidy/projects/cidd
[35] Log
[36] http://www.kdd.org/kdd-cup
[37] Header File
[38] Library File

یک سری از آخرین دستاوردهای حوزه امنیت در شبکه‌های رایانش ابری، مورد بررسی واقع گردد. از جمله مهمترین عملیات امنیتی که در محیط ابر صورت می‌گیرد، می‌توان به سیستم‌های تشخیص و جلوگری از نفوذ اشاره نمود. همچنین یک سری رهیافت و چارچوب دیگر خارج از مبحث سیستم‌های تشخیص و جلوگیری نفوذ ارائه می‌گردد تا بتوان حفظ امنیت را در وهله دوم، اثبات نمود. نفوذ و حملات، می‌تواند پایه و اساس بستر ابر را به شدت زیر سوال ببرد، لذا ارائه روش و مدل‌هایی برای ایجاد و برقراری امنیت در ابر، یکی از چالش‌های اصلی در زمینه رایانش ابری به شمار می‌رود.

## ۷.پیشنهادات آتی

به عنوان مطالعه و پیشنهادات آتی، می‌توان به ارائه یک روش یا مدل جدید در بستر ابر با استفاده از روش‌های یادگیری ماشین را ارائه داد. زیرا بر اساس مطالعات صورت گرفته، واضح و مبرهن است که روش‌های این دسته، دارای دقت و کاربرد بیشتر در حوزه مسائل مختلف می‌باشند و می‌توان امنیت را در ابر، تضمین داد.


## تشکر و قدردانی

نویسـندگان این مقاله از هم‌فکری تمام اعضای کمیته علمی همایش پژوهش‌های نوین علوم و فناوری کمال سپاسگزاری را دارند.


## مراجع


[1] Roschke, Sebastian, Cheng, Feng, and Meinel, Christoph. (2009). Intrusion Detection in the Cloud. Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[2] Raghunath, Bane Raman, and Mahadeo, Shivsharan Nitin. (2011). Network Intrusion Detection System (NIDS). First International Conference on Emerging Trends in Engineering and Technology, pp. 1272-1277.

[3] Huang, Weijian, An, Yan, and Du, Wei. (2010). A Multi-Agent-Based Distributed Intrusion Detection System. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol. 3, pp. 141-143.

[4] Peng, Jian, Choo, Kim-Kwang Raymond, and Ashman, Helen. (2016). User profiling in intrusion detection: A review. Journal of Network and Computer Applications, In Press, Accepted Manuscript, 2016.

[5] Gautam, Sunil Kumar, and Om, Hari. (2016). Computational neural network regression model for Host based Intrusion Detection System. Perspectives in Science, In Press, Corrected Proof.

[6] Chonka, Ashley, Xiang, Yang, Zhou, Wanlei, and Bonti, Alessio. (2011). Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, Vol. 34, pp. 1097–1107.

[7] Shelke, Parag K., Sontakke, Sneha, and Gawande, A. D. (2012). Intrusion Detection System for Cloud Computing. International Journal of Scientific & Technology Research, Vol. 1, Issue 4.

[8] Saadi, Chaimae, and Chaoui, Habiba. (2016). Cloud Computing Security Using IDS-AM-Clust, Honeyd, Honeywall and Honeycomb. International Conference on Computational Modelling and Security (CMS 2016), Procedia Computer Science, Vol. 85, pp. 433-442.

[9] Bahrpeyma, Fouad, Zakerolhoseini, Ali, and Haghighi, Hassan. (2016). Using IDS fitted *Q* to develop a real-time adaptive controller for dynamic resource provisioning in Cloud's virtualized environment. Applied Soft Computing, Vol. 26, pp. 285-298.

[10] Kene, Snehal G., and Theng, Deepti P. (2015). Implementation of Artificial Intelligence for IDS in Cloud Data Centers. International Journal of Innovative Research in Computer and communication Engineering, Vol. 3, Issue 4.

[11] Gosh, Partha, Mandal, Abhay Kumar, and Kumar, Rupesh. (2015). An Efficient Cloud Network Intrusion Detection System. Advances in Intelligent Systems and computing, Vol. 339, pp. 91-99.
[12] Raman, M. R. Gauthama, Somu, Nivethitha, Kirthivasan, Kannan, Liscano, Ramiro, and Sriram, V. S. Shankar. (2017). An Efficient Intrusion Detection System based on Hypergraph - Genetic Algorithm for Parameter Optimization and Feature Selection in Support Vector Machine. Knowledge-Based Systems, Available online 6 July 2017, In Press, Accepted Manuscript — Note to users.
[13] Elhag, Salma, Fernández, Alberto, Bawakid, Abdullah, Alshomrani, Saleh, and Herrera, Francisco. (2015). On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems. Expert Systems with Applications, Vol. 42, Issue 1, pp. 193-202.
[14] Varma, P. Ravi Kiran, Kumari, V. Valli, and Kumar, S. Srinivas. (2016). Feature Selection Using Relative Fuzzy Entropy and Ant Colony Optimization Applied to Real-time Intrusion Detection System. Procedia Computer Science, Vol. 85, pp. 503-510.
[15] Aburommanm, Abdulla Amin, and Reaz, Mamun BinIbne. (2016). A novel SVM-kNN-PSO ensemble method for intrusion detection system. Applied Soft Computing, Vol. 38, pp. 360-372.
[16] Hosseini, Bamakan, Seyed Mojtaba, Amiri, Behnam, Mirzabagheri, Mahboubeh, and Shi, Yong. (2015). A New Intrusion Detection Approach Using PSO based Multiple Criteria Linear Programming. Procedia Computer Science, Vol. 55, pp. 231-237.
[17] Kumar Majhi, Santosh, and Kumar Dhal, Sunil. (2016). Placement of Security Devices in Cloud Data Centre Network: Analysis and Implementation. International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA, Procedia Computer Science, Vol. 78, pp. 33–39
[18] Kritikos, Kyriakos, Kirkham, Tom, Kryza, Bartosz, and Massonet, Philippe. (2018). Reprint of "Towards a security-enhanced PaaS platform for multi-cloud applications. Future Generation Computer Systems, Vol. 78, Part 1, pp. 155-175.
[19] Rossini, A., Kritikos, K., Nikolov, N., Domaschka, J., Griesinger, F., Seybold, D., and Romero, D. (2015). CloudML Implementation Documentation (Final version), PaaSage project deliverable.
[20] Singh, Ashish, and Chatterjee, Kakali. (2016). Cloud security issues and challenges: a survey. Journal of Network and Computer Applications, Vol. 79, pp. 88-115.

# Checking security challenges in cloud computing

Azizeh Zeinali Khosroshahi
Department of Computer Engineering, Faculty of Engineering, Islamic Azad university ,Tabriz, Iran, E-mail: stu.azeinaly@iaut.ac.ir

Shahram Babaie
Department of Computer Engineering, Faculty of Engineering, Islamic Azad university ,Tabriz, Iran

Ehsan Ghasemi
Department of Electrical Engineering, University of Paiam, Golpaigan, Iran

**Abstract**. Thanks to computer networks and advancements in electronic science, cloud computing networks with off-site accessibility make it possible for users to communicate with one another. Cloud computing in relation to your software is still in its infancy. When resources are not in use, the total cost of going to the cloud is almost zero. So it's no surprise that scientific and industry research is moving toward cloud computing. When it comes to distributed systems and multi-agent applications in cloud computing networks, security issues are a must-have requirement. In order to avoid these concerns, intrusion detection systems as well as a series of security frameworks have been introduced. In this research, we try to study the methods presented intelligently, intrusion detection systems and proposed frameworks in the cloud computing network.

**Keywords:** Cloud computing, Security, Intrusion detection system, Machine learning, Intelligent system