هفتمین همایش سالانه
بانکداری الکترونیک
و نظام‌های پرداخت
نوآوری، بازیگران جدید و کارآیی در کسب وکار مالی
تهران، مرکز همایش‌های بین‌المللی برج میلاد - ۲و۳ بهمن ۱۳۹۶
7th Annual Conference
on Electronic Banking
and Payment Systems

ارزیابی امنیت در محیط رایانش ابری و شبیه سازی حملات سایبری

Provide a Method for Simulation of Cyber Attack, Intrusion Detection and Assessment of Security in Cloud Computing Environments

اردوان رجایی، کارشناس و شرکت خدمات انفورماتیک ،A_Rajaei@ISC.CO.IR

چکیده

امروزه با توجه به پیشرفت های فناوری اطلاعات نیاز به محاسبات سنگین و حجیم رو به افزایش است .از این رو افراد مایل هستند که محاسبات خود را با هزینه کمتری در بخش سخت افزاری و نرم افزاری انجام دهند .رایانش ابری بر مبنای شبکه های بزرگ همچون اینترنت است و امکان دسترسی به منابع را بصورت انعطاف پذیر و مقیاس پذیر بر مبنای تقاضا کاربر و به صورت بلادرنگ از طریق اینترنت ارایه می نماید .رایانش ابری مزیت های فراوانی را به همراه دارد در کنار مزیت های فراوان فناوری رایانش ابری، چالش های مختلفی به وجود آمده است .از مهمترین چالش ها موجود در رایانش ابری بحث امنیت است .امنیت خود در رایانش ابری به قسمت های مختلفی مانند امنیت داده های کاربران، امنیت مجوزهای دسترسی و غیره تقسیم بندی میشود .با توجه به گسترش روز افزون استفاده از رایانش ابری، حملات سایبری مختلفی با مقاصد گوناگون در ابرانجام می شود .از مهمترین حملات به ابرها، حمله انکار سرویس است .حمله انکار سرویس به منظور از دسترس خارج کردن منابع ابر و عدم توانایی ابر در پاسخگویی به درخواست های معتبر است .در این مقاله یک روش جهت شبیه سازی حملات انکار سرویس در محیط رایانش ابری ارائه شده است .که با استفاده از ترکیب روش های مبتنی بر امضاء و الگوریتم نزدیکترین همسایه، یک سیستم تشخیص نفوذ به ابر و شبیه سازی های انجام شده در قالب کاری زبان برنامه نویسی کلودسیم[۱] و به زبان برنامه نویسی جاوا[۲] انجام شده .نتایج حاصل از شبیه سازی نشان می دهد که در طول مدت اجرای برنامه و در هنگام حمله انکار سرویس، مراکز داده تعریف شده به طور معمول 20 الی 30 درصد از دسترس خارج میشوند .در بخش سیستم تشخیص نفوذ نیز استفاده همزمان از دو روش به صورت ترکیبی، توانایی تشخیص بیش از 80 درصد حملات امکان پذیر است.

کلمات کلیدی : رایانش ابری ، امنیت ، حملات سایبری ، اینترنت ، حمله انکار سرویس ، سیستم تشخیص نفوذ

Abstract

Today, due to advances in information technology requires massive computing is on the rise. For this reason, people tend to do their computing with lower cost in hardware and software. Cloud computing based on large networks such as the internet, and flexible and scalable access to resources based on user demand in real time via the internet. Cloud computing brings with many advantages; Along with the vast benefits of cloud computing technology, there have been several challenges. The main challenge in cloud computing is security. Security in the cloud divided into different parts such as users data, access permissions and etc. Due to the increasing use of cloud computing, cyber attacks with different purposes is done in cloud. The most important attacks on clouds, denial of service attacks. DoS attack in order to paper out cloud resources and cloud inability to respond to valid requests. In this study, a method for simulating DoS attacks in cloud computing environment is provided. Then using a combination of signature-based method and k-nearest neighbor, and intrusion detection system was submitted to the cloud. Simulations was done in CloudSim framework and Java programming language. The result of the simulation shows that, during the simulation running and when DoS attack, data centers typically 20 to 30 percent are out of reach. In intrusion detection system using combination

Keywords: Cloud Computing, Security, Cyber Attacks, Internet , Denail of Service

مقدمه

در چند سال اخیر تلاش ها حول این مفهوم جدید(رایانش ابری)آغاز شده است؛ رایانش ابری به عنوان یک نمونه موفق از پردازش مطرح شده است .به کمک این مفهوم پردازش از محدوده کامپیوترهای شخصی و یا چند سرویس دهنده برنامه کاربردی به سمت ابری از کامپیوترها منتقل شده است .کاربران ابر کافی است تنها درگیر خدمات پردازشی که آن را درخواست کرده اند باشند و جزئیات چگونگی فراهم شدن این سرویس ها از آن ها پنهان شده است.

رایانش ابری راهی برای توسعه برنامه های کاربردی در یک محیط مجازی فراهم می کند .در این حالت کاربران که نگران کمبود فضا، پهنای باند، امنیت و یا قابلیت اطمینان نیستند .نیاز به نصب نرم افزاری نبوده و در یک محیط پردازش مجازی تنها دغدغه کاربران توسعه و گسترش برنامه و مدیریت آن است .از لحاظ هزینه ها ، نیز تنها برای مدت زمان استفاده و فضای اشغال کرده هزینه پرداخته می شود.

بررسی حملات از نوع انکار سرویس و تمیز دادن آن با درخواست های کاربران قانونی از چالش های اصلی در محیط رایانش ابری است .حملات انکار سرویس باعث تحت تأثیر قرار گرفتن تمام بخش های محیط رایانش ابری و مدل های سرویس دهی آن می شود .اینگونه از حملات می توان از بیرون و یا داخل محیط رایانش ابری صورت پذیرد .روش های مقابله با حملات خارجی به ابر با ایجاد پروتکل های امنیتی و شناسایی کاربران تا حدودی مؤثر و کارا است .یکی از مهمترین نوع حملات انکار سرویس، حملات از نوع حمله سیل آسا در داخل و یا خارج محیط ابر است.

با توجه به تأثیر بسیار زیاد ابر در هنگام حملات انکار سرویس و ایجاد مخاطرات از نظر قابلیت اطمینان کاربران به ابر و هزینه، تشخیص و مقابله با حملات انکار سرویس از چالش های مهم در امنیت رایانش ابری و انگیزه اصلی این مقاله است.

اهداف مقاله

در این مقاله هدف اصلی ارائه یک روش برای شبیه سازی حملات انکار سرویس از نوع سیل آسا، سپس تشخیص حملات انکار سرویس و مقابله با آن در محیط رایانش ابری شبیه سازی شده است .طبقه بندی رایانش ابری، سرویس های مختلف ارائه شده در ابر، بررسی چالش های امنیتی رایانش ابری از دیگر اهداف این مقاله است.

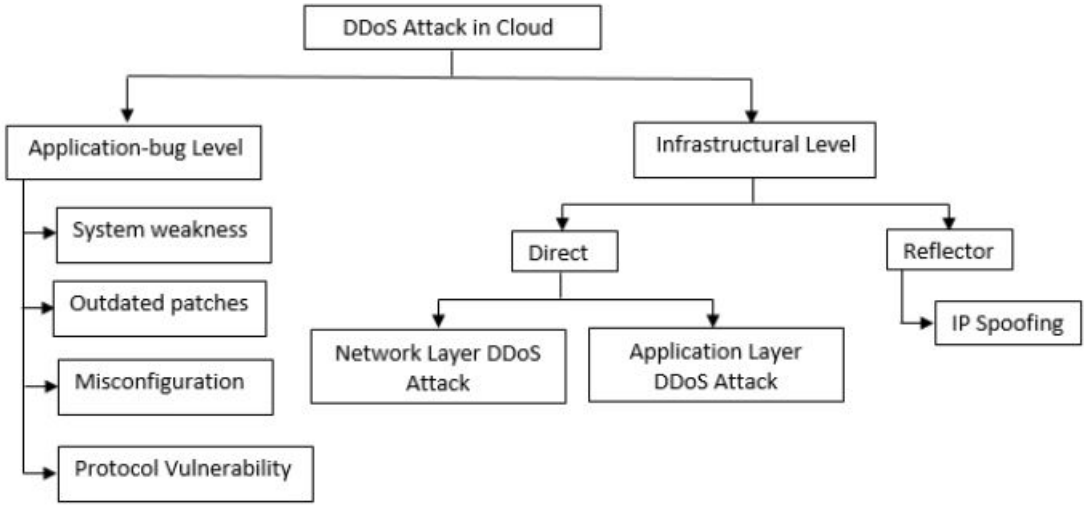
ساختار مقاله

ساختارمقاله بدین شرح است کلیات تحقیق، تعاریف و مفاهیم مبنای در مورد رایانش ابری ارائه شده است .سپس تعریف دقیق و استاندارد از رایانش ابری، سرویس های خدمات دهی رایانش ابری، معماری و انواع مدل های پیاده سازی ابر، همچنین مزیت ها و ریسک های بالقوه موجود در محیط رایانش ابری ارائه شده است .همچنین مروری بر مهمترین کارهای انجام شده تاکنون در زمینه حملات انکار سرویس به منابع پردازشی موجود در ابر و تجزیه و تحلیل آنها مورد بررسی قرار گرفته است . روش پیشنهادی پیاده سازی شده و شرح چگونگی کارکرد آن نمایش داده شده و نتایج روش پیشنهادی و ارزیابی نتایج مورد بررسی قرار گرفته است .در نهایت، نتیجه گیری و کارهای آتی که می توان در این حوزه انجام گیرد و مورد بررسی قرار گیرد ارائه شده است.

ادبیات موضوع

طبقه بندی جامع و استانداری برای حملات انکار سرویس در ابر وجود ندارد .برای مثال در [42] دشموخ و همکاران حملات DDoS را به گروه های اخلال در پهنای باند و تخلیه منابع طبقه بندی کرده اند .در [43] حملات DDoS بر روی وب سرویس های ابر بررسی شده و به دسته های بسته های اطلاعاتی بزرگ و حملات سیل آسا تقسیم بندی شده است . همچنین در [44] این نوع حملات را منحصرا مربوط به حملات زیرساخت سطح زیرساخت، لایه های 3 و 4 مدل OSI و حملات برنامه کاربردی(سطح برنامه، لایه 7 مدل OSI) معرفی کرده است.

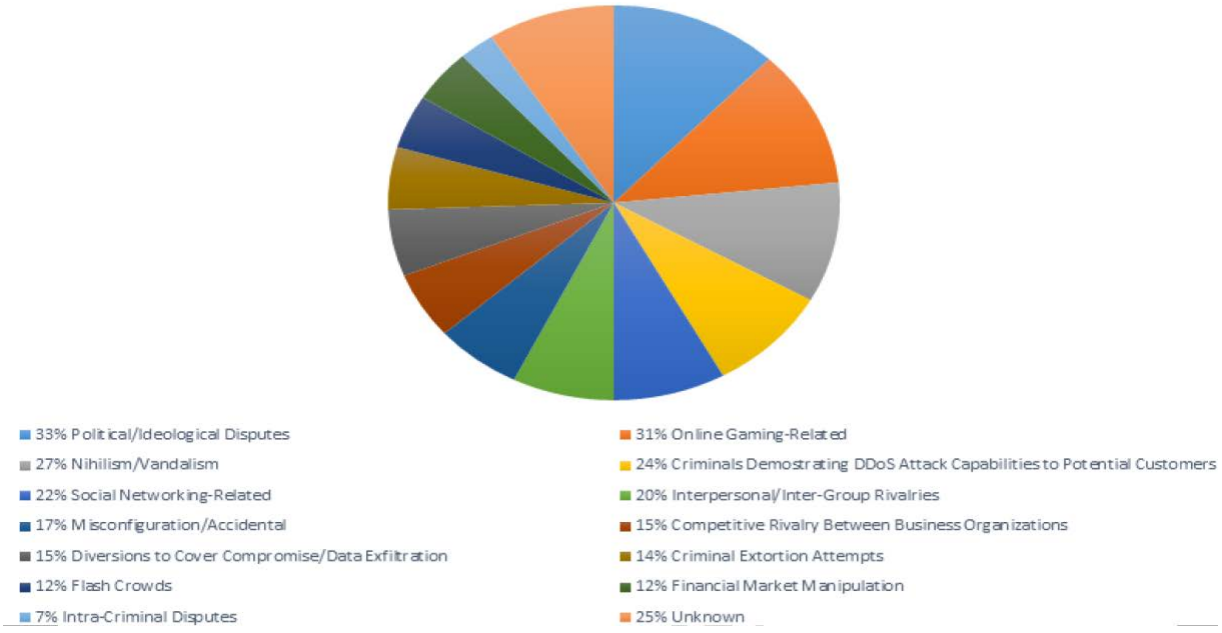
به طور کلی حملات DDoS را میتوان به دو گروه اصلی سطح برنامه و سطح زیرساخت تقسیم بندی کرد .این دوسطح نیز به نوبه خود دارای انواع حملات با توجه به گروه خود هستند. دسته بندی مورد توافق اکثر محققین ارائه شده است.در شکل زیر مشخص است.



شکل ۱- انواع حملات DDoS در ابر [ ]

حملات DDoS توسط یک یا چند سیستم که توسط هکر(ها)کنترل میشود برای انجام حملات از پیش تعیین شده با استفاده از بسته های ناقص یا مخرب برای ایجاد اختلال در منابع هدف انجام می شود .عواقب اصلی یک حمله موفق از نوع DDoSخارج شدن توانایی سرویس دهی سیستم و در رایانش ابری سرویس ابر است.[27]

بررسی های اخیر نشان می دهد که انتقام، اخاذی، مسائل سیاسی، آزمون حملات سایبری و رقابت انگیزه های اصلی حملات DDoS به سرویس های ابر است [28]و[29]



شکل ۲- انگیزه های مختلف برای حملات انجام DDoS [28]

حملات DDoS در رایانش ابری

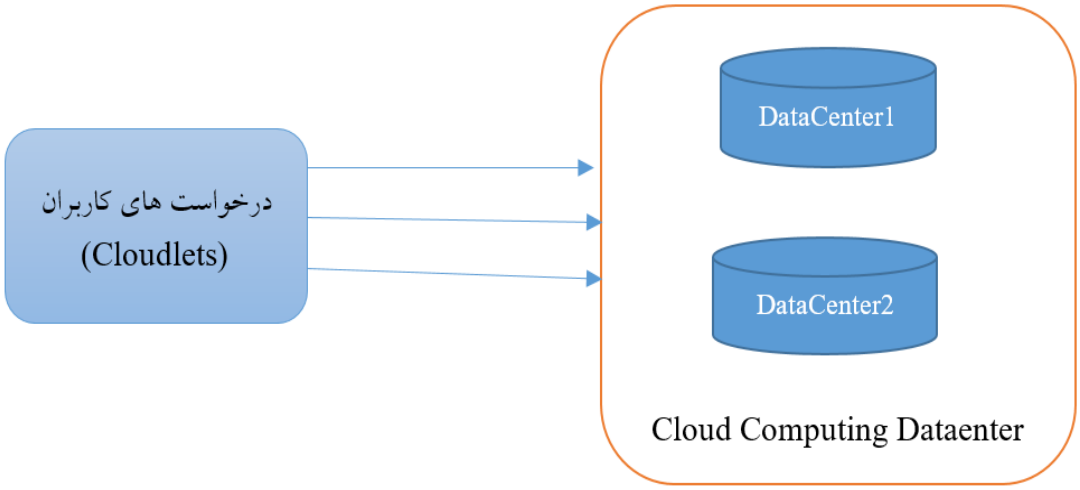
سیاست استقرار امنیت در ابر توسط سه اصل محرمانگی [۳] ، یکپارچگی [۴] و در دسترس بودن [۵] هدایت میشود و به اختصار تحت عنوان CIA نمایش داده میشود .در ساده ترین شکل حمله DDoS در ابر، میتواند با استفاده از گره های(سیستم) آسیب پذیر در اینترنت انجام شود .اهداف مورد حمله پس از دریافت بسته های مهاجم نمی دانند چگونه با آنها برخورد کنند و در نهایت منابع با راه اندازی مجدد و یا خارج شده از دسترس روبرو می شوند .هنگامی که این اتفاق میافتد، دسترسی کاربران قانونی ابر به منابع و خدمات ابر دچار اختلال میشود.[34

چندین نوع حمله DDoS در بازه های زمانی مختلف با استفاده از سیستم های واسط به شکل های مختلف و برای حمله به اجزاء مختلف ابر گزارش شده است . [35] مرلو و همکاران در [36] نشان دادند که چگونه حملات DDoS میتوان بر روی یک شبکه سلولی از دستگاه های بیسیم انجام شود .این حملات میتواند باعث تخریب خدمات در ارتباطات تلفنی جهانی و اخلال در پوشش شبکه تلفن همراه شود.

روش های تشخیص حملات به دو گروه اصلی مبتنی بر امضاء و مبتنی بر ناهنجاری تقسیم میشوند .عمده مزیت تشخیص بر اساس امضاء سرعت عملکرد آن و عیب اصلی آن نیز عدم توانایی یافتن الگوهای جدید است .در تشخیص مبتنی بر ناهنجاری از انواع تکنیک ها و الگوریتم ها در زمینه های مختلف مانند محاسبات نرم، داده کاوی، یادگیری ماشین، آمار و غیره برای تشخیص حملات استفاده میشود.

روش تحقیق

یک روش برای شبیه سازی حملات انکار سرویس در محیط رایانش ابری با استفاده از ابزار شبیه سازی کلودسیم ارائه شده است .برای شبیه سازی یک حمله انکار سرویس در ابتدا دو سناریوی حمله و حالت عادی در مرکز داده ابر ایجاد می شود .در ادامه مکانیزم ترکیبی با استفاده از دو روش تشخیص مبتنی بر امضاء و داده کاوی برای تشخیص نفوذ به ابر ارائه می شود.
برای شبیه سازی حملات انکار سرویس و ارائه روش پیشنهادی، در ابتدا معماری مرکز داده محیط رایانش ابری و مشخصات آن در محیط کلودسیم مشخص می شود .در این مقاله برای تعریف معماری محیط رایانش ابر در کلودسیم، دو مرکز داده برای پاسخگویی به درخواست کاربران ایجاد شده است .پس از آن برای هر کدام از مراکز داده میزبان و ماشین های مجازی مختص به آنها ایجاد میشود .شکل(۳) معماری مرکز داده ابر را نشان میدهد.



شکل۳- معماری مرکز داده ابر

در ادامه شکل (۳) نمونه کد مربوط به تولید مرکز داده ارائه شده است .همانطور که مشاهده می شود تعداد مرکز داده در نظر گرفته شده برای پیاده سازی محیط ابر دو عدد بوده که برای ایجاد هر کدام از مراکز داده یک بار فراخوانی می شود.
در هنگام ایجاد مراکز داده، در هر کدام از مراکز داده نیز اطلاعات میزبان های مربوط به هر کدام از آنها ایجاد میشود .این میزبان ها در واقع منابع فیزیکی مشخص در هر مرکز داده محیط شبیه سازی شده است. شکل (۴) کد مربوط به مشخصات میزبان های فیزیکی هر مرکز داده را نشان میدهد.
در هنگام ایجاد مرکز داده ابر یکی از موارد مهم تعریف کارگزار مرکز داده ابر است .یک کارگزار وظیفه پنهان سازی مدیریت ماشین های مجازی در هنگام ایجاد، از بین بردن و همچنین تخصیص کلودلت ها به ماشین های مجازی است .شکل (۵) کد تعریف کارگزار مرکز داده ابر را نشان می دهد.

شکل ۴- نمونه کد مربوط به مشخصات میزبان های فیزیکی

```
private static DatacenterBroker createBroker(){

        DatacenterBroker broker = null;
        try {
                broker = new DatacenterBroker("Broker");
        } catch (Exception e) {
                e.printStackTrace();
                return null;
        }
        return broker;
}
```

شکل ۵- تعریف کارگزار مرکز داده ابر

برای هر دو مرکز داده میتوان یک کارگزار و یا به صورت جداگانه تعریف کرد .در شبیه سازی های انجام شده از یک کارگزار برای بخش مدیریت و اجرای کلودلت ها توسط مراکز داده استفاده شده است. در ادامه به منظور ایجاد فضای مجازی بر روی منابع فیزیکی مراکز داده ابر، ماشین های مجازی در برنامه تعریف میشود .شکل (۶) تابع تعریف ماشین های مجازی را نشان می دهد.

```
private static List<Vm> createVM(int userId, int vms) {

        //Creates a container to store VMs. This list is passed to the broker later
        LinkedList<Vm> list = new LinkedList<Vm>();

        //VM Parameters
        long size = 10000; //image size (MB)
        int ram = 512; //vm memory (MB)
        int mips = 1000;
        long bw = 1000;
        int pesNumber =1; //number of cpus
        String vmm = "Xen"; //VMM name

        //create VMs
        Vm[] vm = new Vm[vms];
```

شکل ۶- تابع تعریف ماشینهای مجازی

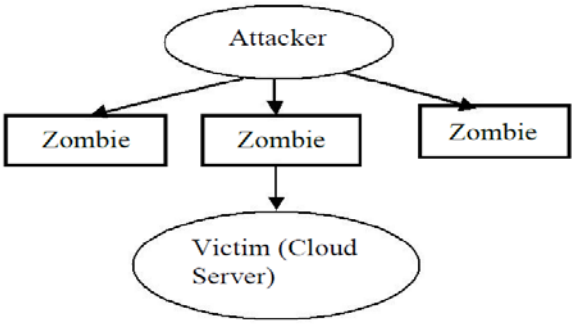
پس از ایجاد مراکز داده، کارهای ارسالی به منابع پردازشی ابر جهت انجام و تکمیل باید ایجاد شود .در ابتدا ترافیک موجود در دیتاست از فایلهای مربوطه به سیستم وارد میشود .اینکار توسط کلاسReadingData صورت میگیرد .
داده های ترافیک مربوط به هر کدام از نمونه های دو بردار ویژگی آموزش و آزمایش توسط کلاس ReadingData از فایلهای بیرونی(متنی)خوانده میشوند .در این کلاس در هنگام خواندن اطلاعات، داده ها جهت استفاده نوع داده ها به عدد تبدیل شده و کلاس مربوط به هر کدام نیز مشخص می شود .پس از تبدیل اطلاعات و ایجاد بردارهای ویژگی داده های آموزش و آزمایش در ادامه دو مجموعه کلودلت متناظر با داده های آموزشی و آزمایشی ایجاد می شود .

در تولید هر کلودلت طول کار، اندازه فایل خروجی و حتی آدرس آی پی به صورت کاملاً تصادفی انجام میشود .این امر به دلیل ایجاد یک شبیه سازی نزدیک به دنیای واقعی است .

پس از تولید کلودلت ها و ایجاد سناریوهای مختلف، پس از اجرای کلودلت ها، نتایج خروجی دریافتی از مراکز داده توسط تابع printCloudletList در خروجی نمایش داده میشود.

شبیه سازی حمله

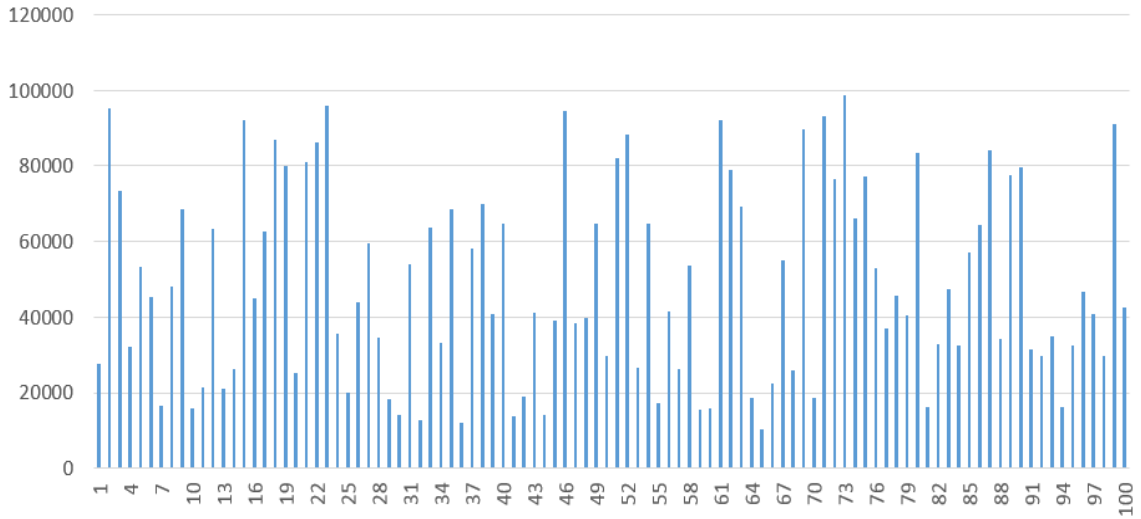
به منظور شبیه سازی یک حمله انکار سرویس در کلودسیم روش کار بدین شرح است .دو سناریوی حمله و حالت عادی توسط کلودلت تعریف میشود .شکل (۷)معماری کلی یک حمله انکار سرویس توزیع شده در ابر را نشان می دهد.[71]



شکل۷_معماری یک حمله انکار سرویس توزیع شده[۷۱]

سناریوی حمله

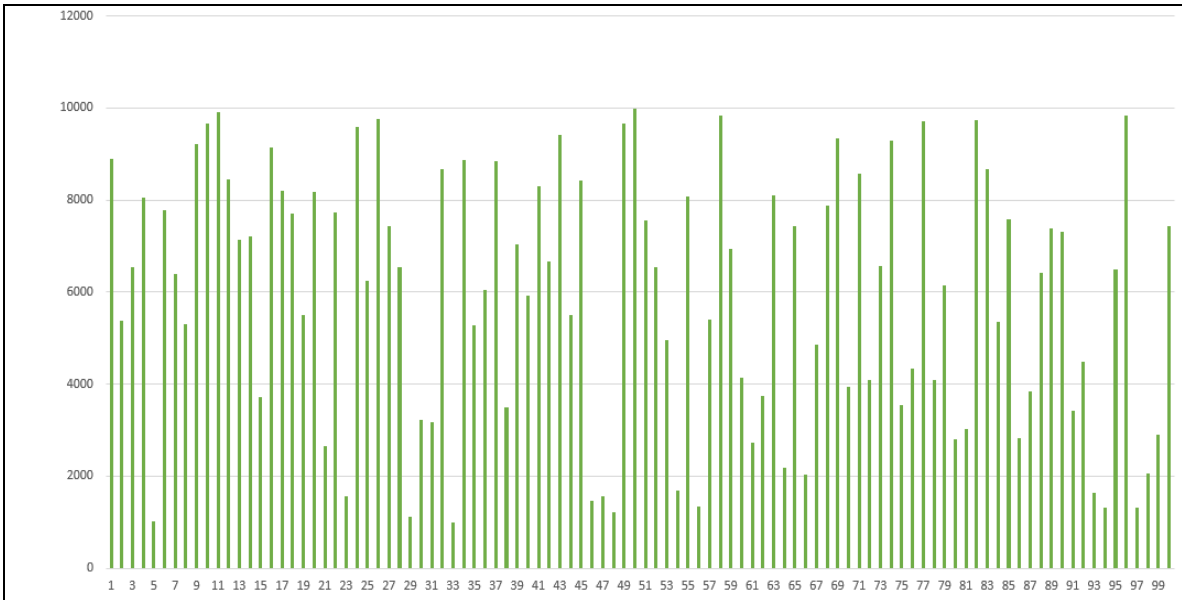
در هنگام حمله انکار سرویس با توجه به اینکه هدف از دسترس خارج کردن منابع ابر(در کلودسیم مرکزداده)است؛ معمولاً طول کارهای ارسالی به ابر بسیار زیاد است .در اینجا نیز به منظور ایجاد شبیه سازی به طور تصادفی، طول کارهای ارسالی با تقریبی بیشتر از توان مرکز داده باید در نظر گرفته شود .برای مثال طول کلودلت دارای حمله بین000 ، 10الی000 ، 100 در نظر گرفته می شود .در کلودسیم طول یک کار تنها آیتمی است که می توان از آن برای انجام شبیه سازی بهره برد .در ادامه علاوه بر طول کار به هر کلودلت مشخصات دیگری مانند آدرس آی پی، اندازه فایل خروجی، تعداد پردازنده مورد نیاز برای اجرا و یک نمونه ترافیک شبکه اضافه می شود .از آدرس آی پی و ترافیک نمونه در قسمت تشخیص نفوذ استفاده می شود .شکل (۸) نمونه کلودلت های ایجاد شده برای سناریوی حمله را نشان می دهد .طول هر کلودلت به صورت تصادفی و در برنامه ایجاد می شود.



شکل۸-نمونه کلودلت های ایجاد شده با طول های مختلف

سناریوی حالت عادی

در این حالت طول کارهای ارسالی به ابر به صورت غیر عادی افزایش نیافته و باید تقریبی کمتر از توان مرکز داده باشد .در این حالت طول هر کلودلت به صورت تصادفی بین 1000و 10,000 است .دلیل این انتخاب ایجاد امکان شبیه سازی حمله در کلودسیم است .در این حالت نیز علاوه بر طول کار، مشخصات دیگر کلودلت به آن اضافه میشود .شکل (۸) کلودلت های ایجاد شده برای سناریوی حالت عادی سرورهای کلود را نشان می دهد .در اینجا نیز طول هر کدام به صورت تصادفی در بازه در نظر گرفته شده ایجاد می شود.



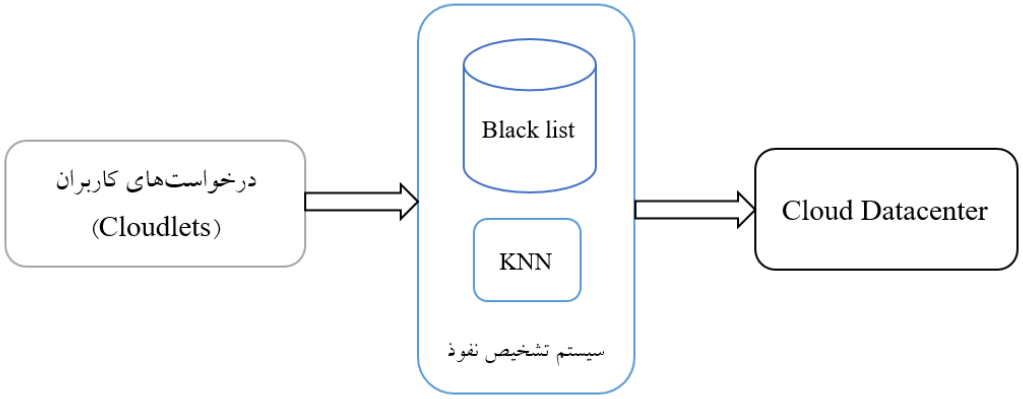
شکل ۹ -نمونه کلودلت های ایجاد شده با طولهای مختلف

شکل ۱۰ -کد کلودلت ها برای ایجاد سناریو عادی کلود

سناریوی تشخیص نفوذ

پس از ایجاد یک بستر شبیه سازی حمله به ابر، در این سناریو به دنبال یافتن تشخیص نفوذ توسط کلودلت ها هستیم .در قسمت تشخیص نفوذ دو روش مبتنی بر امضاء و الگوریتم نزدیکترین همسایه به صورت ترکیبی برای تشخیص نفوذ استفاده می شود .در روش مبتنی بر امضاء اطلاعات کلودلت های مشکوک ویا کلودلت هایی که قبلاً به عنوان حمله انکار سرویس تشخیص داده شده است در داخل لیست سیاه ذخیره می شود، در شبیه سازی انجام شده این کار به صورت آدرس آی پی در سیستم ذخیره می شود .مزیت استفاده از روش مبتنی بر امضاء افزایش سرعت برای تشخیص حملات بعدی و مشکوک است . در کنار روش مبتنی بر امضاء، همزمان از یک الگوریتم داده کاوی به نام نزدیکترین همسایه نیز برای تشخیص خودکار استفاده میشود.

نمونه ترافیک انتخاب شده برای هر کلودلت در این قسمت استفاده می شود .شکل (۱۱) معماری سیستم تشخیص نفوذ ترکیبی را نشان می دهد.



شکل ۱۱- معماری سیستم تشخیص نفوذ پیشنهادی

محدودیت های تحقیق

در این مقاله هدف ارائه یک مکانیزم شبیه سازی حمله و سپس تشخیص نفوذ به ابر جهت جلوگیری از حمله انکار سرویس است .مهمترین مشکل در شبیه سازی عدم وجود یک دیتاست استاندارد برای شبیه سازی و تشخیص نفوذ به شبکه ابر است . به همین دلیل در هنگام تعریف یک کلودلت ترافیک نمونه انتخاب شده برای آن به صورت تصادفی از یک مجموعه داده استاندارد شبکه به نام KddCUP استفاده شده است.[72 مزیت استفاده از دیتاست KddCUP وجود ترافیک حالت عادی و حالت حملات انکار سرویس در آن است.

نرم افزارهای مورد استفاده

در این مقاله به منظور شبیه سازی حمله انکار سرویس و تشخیص نفوذ به ابر، از نرم افزارها و ابزارهایی به شرح زیر استفاده شده است.

Eclipse IDE: به منظور اجرای شبیه سازی و استفاده از قالب کاری کلودسیم از نرم افزار توسعه ایکلیپس و زبان برنامه نویسی جاوا استفاده شده است.

CloudSim: قالب کاری مورد نظر برای شبیه سازی و ایجاد بستر رایانش ابری است .در این مقاله از نسخه 3.0.3 آن استفاده شده است.

Excel : از نرم افزار اکسل نسخه 2016 نیز برای تولید برخی از نمودارها نتایج حاصل از شبیه سازی استفاده شده است.

Matlab:از نرم افزار متلب نسخه 2016 نیز برای ایجاد نمودارهای ROC و ماتریس درهم ریختگی حاصل از نتایج شبیه سازی استفاده شده است.

اجرای شبیه سازی

در این مقاله شبیه سازی های انجام شده در نرم افزار ایکلیپس و به زبان برنامه نویسی جاوا صورت گرفته و از کتابخانه های موجود در کلودسیم برای تعریف محیط رایانش ابری استفاده شده است .اجرای برنامه شبیه سازی شده به دفعات متعدد و به صورت تصادفی انجام شده است .شکل (۱۲) و شکل (۱۳) قسمت هایی از نتایج خروجی برنامه شبیه سازی انجام شده را نشان می دهد.

```
0.2: Broker: Sending cloudlet 7 to VM #0
0.2: Broker: Sending cloudlet 25 to VM #1
0.2: Broker: Sending cloudlet 26 to VM #2
0.2: Broker: Sending cloudlet 32 to VM #3
0.2: Broker: Sending cloudlet 35 to VM #4
0.2: Broker: Sending cloudlet 36 to VM #5
0.2: Broker: Sending cloudlet 53 to VM #6
0.2: Broker: Sending cloudlet 65 to VM #7
0.2: Broker: Sending cloudlet 73 to VM #8
0.2: Broker: Sending cloudlet 75 to VM #9
0.2: Broker: Sending cloudlet 77 to VM #10
0.2: Broker: Sending cloudlet 80 to VM #11
0.2: Broker: Sending cloudlet 94 to VM #0
0.2: Broker: Sending cloudlet 99 to VM #1
37.654: Broker: Cloudlet 94 received
42.626000000000005: Broker: Cloudlet 73 received
43.028000000000006: Broker: Cloudlet 53 received
45.61: Broker: Cloudlet 26 received
50.006: Broker: Cloudlet 32 received
61.851: Broker: Cloudlet 36 received
71.143: Broker: Cloudlet 80 received
81.315: Broker: Cloudlet 65 received
91.227: Broker: Cloudlet 77 received
95.342: Broker: Cloudlet 75 received
97.658: Broker: Cloudlet 35 received
102.125: Broker: Cloudlet 99 received
116.69800000000001: Broker: Cloudlet 7 received
118.85000000000001: Broker: Cloudlet 25 received
118.85000000000001: Broker: All Cloudlets executed. Finishing...
118.85000000000001: Broker: Destroying VM #0
118.85000000000001: Broker: Destroying VM #1
118.85000000000001: Broker: Destroying VM #2
118.85000000000001: Broker: Destroying VM #3
118.85000000000001: Broker: Destroying VM #4
118.85000000000001: Broker: Destroying VM #5
118.85000000000001: Broker: Destroying VM #6
118.85000000000001: Broker: Destroying VM #7
118.85000000000001: Broker: Destroying VM #8
118.85000000000001: Broker: Destroying VM #9
118.85000000000001: Broker: Destroying VM #10
118.85000000000001: Broker: Destroying VM #11
```

شکل ۱۲- بخشی از خروجی شبیه سازی

```
Broker is shutting down...
Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.
Datacenter_0 is shutting down...
Datacenter_1 is shutting down...
Broker is shutting down...
Simulation completed.
Simulation completed.

========== OUTPUT ==========
Cloudlet ID     STATUS     Data center ID     VM ID        Time     Start Time     Finish Time
     94         SUCCESS         Datacenter_0     0       37.45         0.2           37.65
     73         SUCCESS         Datacenter_1     8       42.43         0.2           42.63
     53         SUCCESS         Datacenter_1     6       42.83         0.2           43.03
     26         SUCCESS         Datacenter_0     2       45.41         0.2           45.61
     32         SUCCESS         Datacenter_0     3       49.81         0.2           50.01
     36         SUCCESS         Datacenter_0     5       61.65         0.2           61.85
     80         SUCCESS         Datacenter_1    11       70.94         0.2           71.14
     65         SUCCESS         Datacenter_1     7       81.11         0.2           81.31
     77         SUCCESS         Datacenter_1    10       91.03         0.2           91.23
     75         SUCCESS         Datacenter_1     9       95.14         0.2           95.34
     35         SUCCESS         Datacenter_0     4       97.46         0.2           97.66
     99         SUCCESS         Datacenter_0     1      101.92         0.2          102.12
      7         SUCCESS         Datacenter_0     0       116.5         0.2           116.7
     25         SUCCESS         Datacenter_0     1      118.65         0.2          118.85
CloudSimExample6 finished!
simulation ended....
```

شکل ۱۳- بخشی از خروجی شبیه سازی

پیکربندی و مشخصات مرکز داده ابر، میزبان و ماشین مجازی

جدول ۱- مشخصات مرکز داده ابر

تعداد مراکز داده	۲
تعداد میزبان در هر مرکز	۲
تعداد ماشین مجازی	۲۰
تعداد کلودلت	۱۰۰

جدول ۲- مشخصات پیکربندی مرکز داده

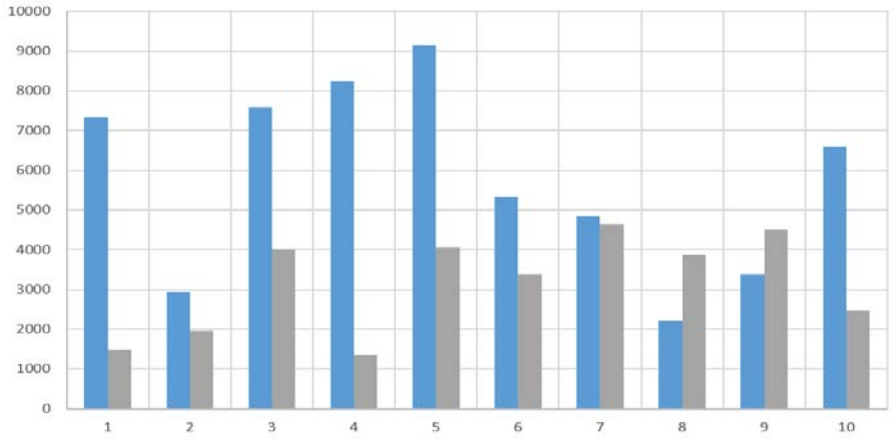
RAM	2048

معیارهای فراخوانی، دقت و صحت استفاده کرد.

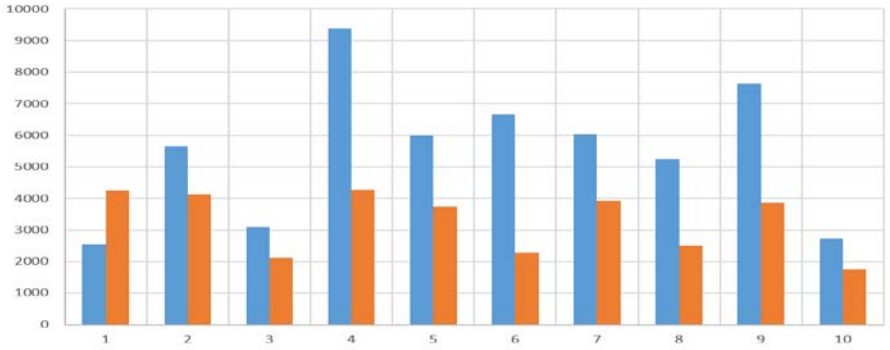
معیار فراخوانی [۶] به معنی نسبت نمونه های(کلودلت های)شناسایی شده به عنوان حمله به تعداد کل نمونه های حمله در آزمایش است .عبارت (۱) این رابطه را نشان میدهد.

عبارت (۱)

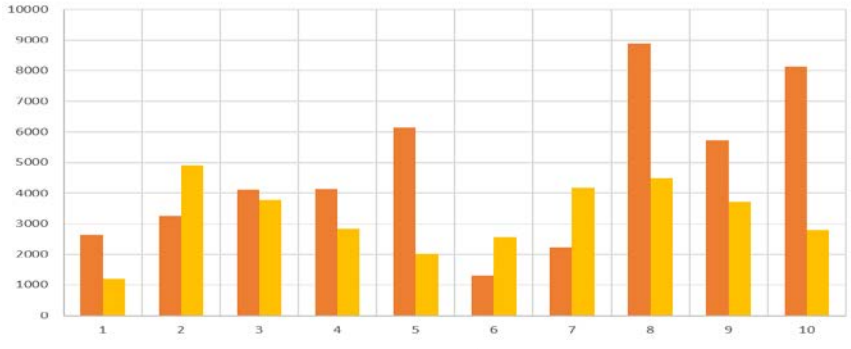
در آن tp تعداد نمونه های حمله صحیح تشخیص داده شده و fp تعداد نمونه های حمله اشتباه(ترافیک عادی معیار دقت به معنی نسبت تعداد نمونه هایی است که به درستی دسته بندی شده و از نوع حمله بوده به تعداد کل نمونه هایی که به عنوان حمله شناسایی شده است که عبارت (۲) رابطه آن را نشان میدهد .



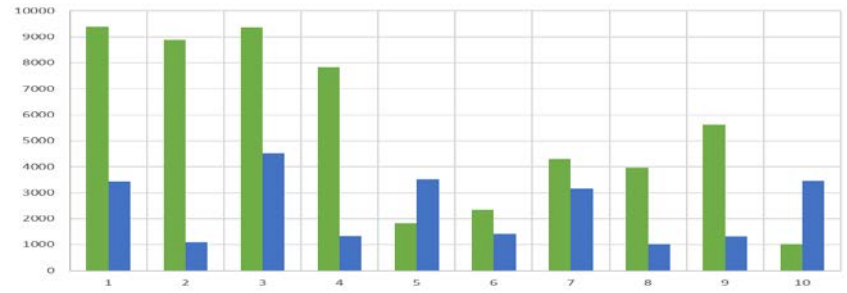
شکل۱۵- مقایسه کلودلت های نمونه در اجرای اول



شکل۱۶- مقایسه کلودلت های نمونه در اجرای دوم

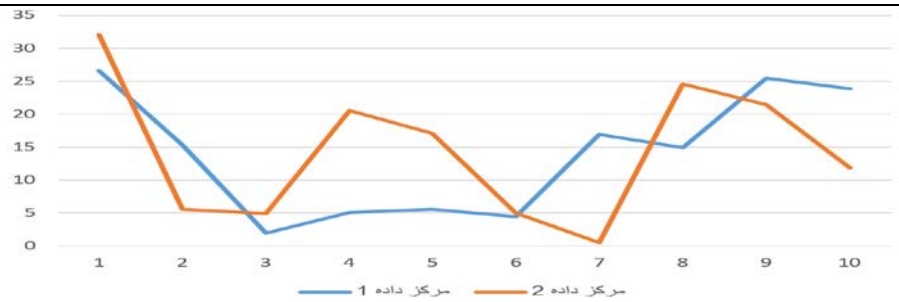


شکل ۱۷- مقایسه کلودلت های نمونه در اجرای سوم



شکل۱۸- مقایسه کلودلت های نمونه در اجرای چهارم

نمودار شکل (۱۹) میزان درصد از دسترس خارج شدن مراکز داده را در هنگام اجراهای مختلف و شبیه سازی حمله نشان می دهد.



شکل۱۹- میزان از دسترس خارج شدن مراکز داده ابر

همانطور که بیان شد روش دیگر برای بررسی حمله انکار سرویس میزان اجرای برنامه است. که جدول(۴) این مورد را نشان می دهد.

جدول ۴- زمان اجرای برنامه

شماره اجرا	سناریوی حالت عادی(میلی ثانیه)	سناریوی حمله انکار سرویس(میلی ثانیه)
۱	۱۵۰	۴۰۰
۲	۱۳۰	۳۸۰
۳	۸۹	۴۰۲
۴	۸۰	۳۶۰
۵	۷۱	۳۳۱

نتایج ارزیابی سیستم تشخیص نفوذ به ابر

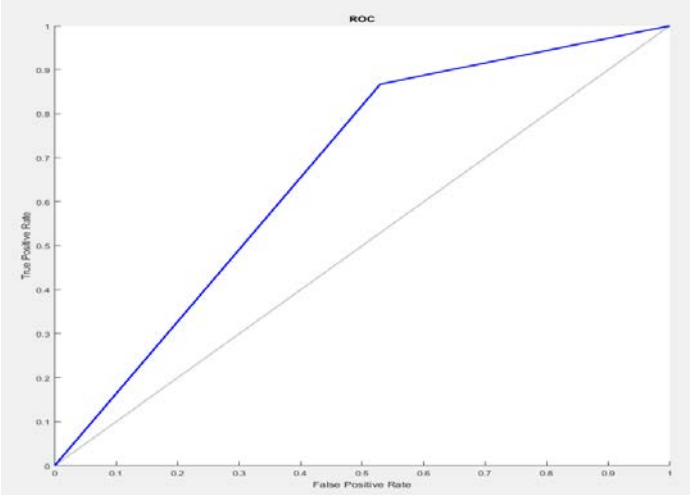
برای آزمایش الگوریتم نزدیکترین همسایگی در هر دور اجرا 100 عدد کلودلت به عنوان آزمون ایجاد شده و ترافیک مربوط به هر کدام نیز به صورت تصادفی و بدون جایگذاری از مجموعه داده KddCup استفاده شده است .همچنین برای مقایسه و اندازه گیری نزدیکترین همسایگان، تعداد 1000 نمونه نیز از مجموعه داده به صورت تصادفی انتخاب شده است .در ادامه نتایج حاصل از یک دور اجرای شبیه سازی ارائه شده است .جدول (۵)تعداد نمونه ها و دقت تشخیص را نشان میدهد.

جدول ۵- دقت تشخیص حاصل از یک دور اجرای برنامه

تعداد کل نمونه ها	تعداد نمونه های آموزش	تعداد نمونه های آزمایش	دقت تشخیص صحیح
12000	1000	100	٪80

شکل۲۰- ماتریس درهمریختگی

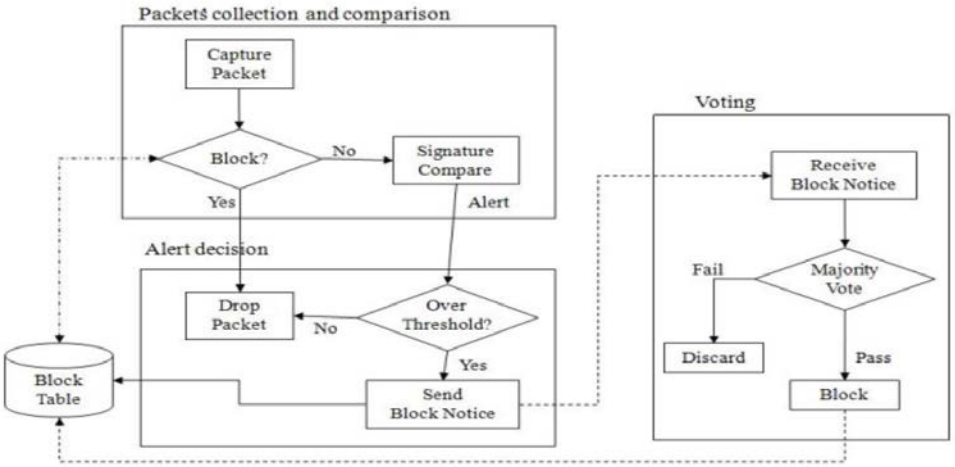
همچنین در شکل(۲۱) نمودار ROC مربوط به اجرای الگوریتم نزدیکترین همسایه نمایش داده شده است .نمودار ROC به منظور نمایش کارایی تشخیص یک طبقه بندی مورد استفاده قرار می گیرد.



شکل۲۱- نمودارROC

مقایسه روش پیشنهادی با کارهای دیگران

در [67] چیچون و همکاران یک قالب کاری برای تشخیص نفوذ به ابر ارائه کردند .روش ارائه شده در [67] از یک روش مشارکتی برای تشخیص نفوذ و موارد مشکوک استفاده می کند .روش ارائه شده بر مبنای لیست سیاه و بلوکه کردن آی پی های مشکوک و یا قربانی حملات است .شکل(۲۲) نمای بلوک دیاگرام روش پیشنهادی در [67] را نشان می دهد.



شکل ۲۲- نمای بلوک دیاگرام ارائه شده در[67]

روش ارائه شده [67] در مقایسه با روش پیشنهادی در این مقاله دقت کمتری نسبت به تشخیص برای حملات جدید در ابر را دارد.

نتیجه گیری

در این مقاله یک روش جهت شبیه سازی حملات انکار سرویس در محیط رایانش ابری ارائه شده است. در ادامه با استفاده از ترکیب روشهای مبتنی بر امضاء و الگوریتم نزدیکترین همسایه، یک سیستم تشخیص نفوذ به ابر نیز ارائه شد .

شبیه سازی های انجام شده در قالب کاری کلودسیم و به زبان برنامه نویسی جاوا انجام شده است .نتایج حاصل از شبیه سازی نشان میدهد که در طول مدت اجرای برنامه و در هنگام حمله انکار سرویس، مراکز داده تعریف شده به طور معمول 20 الی 30 درصد از دسترس خارج میشوند .در بخش سیستم تشخیص نفوذ نیز استفاده همزمان از دو روش به صورت ترکیبی، توانایی تشخیص بیش از 80 درصد حملات امکانپذیر است

کارهای آینده

باتوجه به وجود چالش های مختلف امنیتی برای محیط رایانش ابری، پتانسیل بالایی برای ارتقاء امنیت در ابر وجود دارد . امنیت را میتوان به عنوان یک عامل تمایز در بین رقیبان ارائه کرد و با توجه به محیط ابر امنیت مقیاس پذیر است .به عنوان کارهای آینده و عمومی میتوان به موارد زیر اشاره کرد:

استانداردسازی مسائل امنیتی برای محیط رایانش ابری و همچنین واسطها

تمرکز بر منابع و توسعه سیستمهای مانیتورینگ

توافقنامه های سطح سرویس

تشخیص ریسکهای امنیتی و ایجاد سناریوهای مختلف برای آنها

بررسی نقاط آسیبپذیری سیستم و تأثیر آنها بر ابر

ایجاد یک مجموعه داده استاندارد از کلودلتها مختص حملات انکار سرویس به منظور آزمایش روشهای مختلف امنیتی

ارائه یک مکانیزم هوشمند برای حذف اطلاعات تکراری در داخل لیست سیاه

استفاده از دیگر الگوریتمهای هوشمند همچون شبکههای عصبی مصنوعی، درخت تصمیم و غیره در بخش تشخیص نفوذ در ابر

مراجع

[1] A. Saurabh Singh, Young-Sik Jeong, Jong Hyuk Park, A survey on cloud computing security: Issues, threats, and solutions, Journal of Network and Computer Applications, Volume 75, November 2016, Pages 200-222, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.09.002.

[2] Minhaj Ahmad Khan, A survey of security issues for cloud computing, Journal of Network and Computer Applications, Volume 71, August 2016, Pages 11-29, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.05.010.

[3] Choudhury, A. J., Kumar, P., Sain, M., Lim, H., & Jae-Lee, H. (2011). A Strong User Authentication Framework for Cloud Computing. In IEEE Asia-Pacific Services Computing Conference (pp. 110ت115). IEEE. http://doi.org/10.1109/APSCC.2011.14

[4] C. C. Lo, C. C. Huang and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," Parallel Processing Workshops (ICPPW), 2010 39th International Conference on, San Diego, CA, 2010, pp. 280-284. doi: 10.1109/ICPPW.2010.46.

[5] Qiao Yan and F. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing," in IEEE Communications Magazine, vol. 53, no. 4, pp. 52-59, April 2015. doi: 10.1109/MCOM.2015.7081075.

[6] R. Aishwarya and S. Malliga, "Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment,"
, Chennai, 2014, pp. 1-6. doi: 10.1109/ICRTIT.2014.6996163

[7] Bhagat, S., & Pasupuleti, S. K. (2015, September). Simulated Raindrop Algorithm to Mitigate DDoS Attacks in Cloud Computing. In Proceedings of the Sixth International Conference on Computer and Communication Technology,India, 2015 (pp. 412-418). ACM.

[8] U. Tariq, M. Hong, K. Lhee, A comprehensive categorization of ddos attack and ddos defense techniques, in: X. Li, O. Zaane, Z.-h. Li (Eds.), Advanced Data Mining and Applications, Vol. 4093 of Lecture Notes in Computer Science, Springer Berlin /Heidelberg, 2006, pp. 1025-1036

[9] Corero, "DDoS Trends and Analysis Quarterly Report Q4 2014", Corero, Available:http://www.corero.com/resources/files/Reports, 2015-03-35

[10] A. Albugmi, M. O. Alassafi, R. Walters and G. Wills, "Data security in cloud computing,"
, London, United Kingdom, 2016, pp. 55-59. doi: 10.1109/FGCT.2016.7605062

[11] Buyya, Rajkumar and Pathan, Mukaddim and Vakali, Athena, "A Taxonomy of CDNs", 2008, Springer Berlin Heidelberg, Berlin, Heidelberg , 33-77, 978-3-540-77887-5,

doi="10.1007/978-3-540-77887-5_2"
[12] W. Alosaimi, M. Alshamrani and K. Al-Begain, "Simulation-Based Study of Distributed Denial of Service Attacks Prevention in the Cloud," 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, 2015, pp. 60-65.doi: 10.1109/NGMAST.2015.50
[13] B. Khadka, C. Withana, A. Alsadoon and A. Elchouemi, "Distributed Denial of Service attack on cloud: Detection and prevention," 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, BC, 2015, pp. 1-6.doi: 10.1109/IEMCON.2015.7344496
[14] V. Geetha, N. Laavanya, S. Priyadharshiny and C. Sofeiyakalaimathy, "Survey on security mechanisms for public cloud data," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), Pudukkottai, 2016, pp. 1-8.
[15] Mell P, Grance T. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145, January 2011
[16] Naidila Sadashiv, S. M Dilip Kumar,پCluster, Grid and Cloud Computing: A Detailed Comparisonپ The 6th International Conference on Computer Science & Education,Singapore, IEEE 2011.
[17] Qi Zhang □Lu Cheng □Raouf Boutaba,پCloud computing: state-of-the-art and research challengesپ J Internet Serv Appl, Springer 2010.
[18] T. Grandison, E. M. Maximilien, S. Thorpe and A. Alba, "Towards a Formal Definition of a Computing Cloud," , Miami, FL, 2010, pp. 191-192. doi: 10.1109/SERVICES.2010.111
[19] Maricela-Georgiana Avram (Olaru),پ Advantages and challenges of adopting cloud computing from an Enterprise perspectiveپ The 7th International Conference Interdisciplinarity in Engineering, Romania, Elsevier, 2013.
[20] M. Kim et al., "Building scalable, secure, multi-tenant cloud services on IBM Bluemix," in IBM Journal of Research and Development, vol. 60, no. 2-3, pp. 8:1-8:12, March-May 2016. doi: 10.1147/JRD.2016.2516942
[21] K.Stanoevska-Slabeva, T. Wozniak, S.Ristol, بGrid and CloudComputing Abusiness Perspective on Technology and Applications, Springer, ISBN: 978-3-642-05192-0, 2010.
[22] Juan Li, Frederique Biennier, and Youssef Amghar, Business as a Service Governance in a Cloud Organisation, INSA-Lyon. LIRIS. UMR5205, F-69621, France.
[23] Peeyush Mathur, Nikhil Nishchal, "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing, India (PDGC - 2010).
[24] W. Yang and C. Fung, "A survey on security in network functions virtualization," 2016 IEEE NetSoft Conference and Workshops (NetSoft), Seoul, 2016, pp. 15-19.doi: 10.1109/NETSOFT.2016.7502434
[25] Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi, Muzammil Hussain, Suleman Khan, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, On cloud security attacks: A taxonomy and intrusion detection and prevention as a service, Journal of Network and Computer Applications, Volume 74, October 2016, Pages 98-120, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2016.08.016.

[26] B. Wang, Y. Zheng, W. Lou, Y. Hou, DDoS attack protection in the era of cloud computing and Software-Defined Networking, Computer Networks 81 (2015) P 308-319
[27] J. Choi, C. Choi, B. Ko, D. Choi, P. Kim, P, Detecting web based DDoS attack using MapReduce operations in cloud computing environment, Journal of internet services and information security 3(3/4), (2013) 28-37.
[28] S.T. Zargar, J. Joshi, T. David, A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks, IEEE Communications Surveys & Tutorials 15(4) (2013) 2046-2069.
[29] T. Mahboob, S. Ghaffar and Z. B. Akhtar, "A survey Cloud computing a global perspective," 2015 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), Melaka, 2015, pp. 190-195.doi: 10.1109/IC3e.2015.7403511
[30] Nelson L. S. da Fonseca; Raouf Boutaba, "Performance Management and Monitoring," in Cloud Services, Networking, and Management, 1, Wiley-IEEE Press, 2015, pp.432- doi: 10.1002/9781119042655.ch9
[31] Rania El-Gazzar, Eli Hustad, Dag H. Olsen, Understanding cloud computing adoption issues: A Delphi study approach, Journal of Systems and Software, Volume 118, August 2016, Pages 64-84, ISSN 0164-1212, http://dx.doi.org/10.1016/j.jss.2016.04.061.
[32] A. Girma, M. Garuba, J. Li and C. Liu, "Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment," 2015 12th International Conference on Information Technology - New Generations, Las Vegas, NV, 2015, pp. 212 - 217. doi: 10.1109/ITNG.2015.40
[33] J. Chen, X. Wu, S. Zhang, W. Zhang and Y. Niu, "A Decentralized Approach for Implementing Identity Management in Cloud Computing," 2012 Second International Conference on Cloud and Green Computing, Xiangtan, 2012, pp. 770-776. doi: 10.1109/CGC.2012.118
[34] A. Mishra, B. B. Gupta, R.C Joshi, A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques, in: proceedings of IEEE European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 2011, pp. 286-289.
[35] A. Khadke, M. Madankar and M. Motghare, "Review on mitigation of distributed Denial of Service (DDoS) attacks in cloud computing," 2016 10th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, 2016, pp. 1-5. doi: 10.1109/ISCO.2016.7726917
[36] A. Merlo, M. Migliardi, N. Gobbo, F. Palmieri, A. Castiglione, A denial of service attack to UMTS networks using SIM-less devices, IEEE Transactions on Dependable and Secure Computing, 11(3) (2014) 280-91.
[37] M. Ficco, and M. Rak, Stealthy denial of service strategy in cloud computing, IEEE Transactions on Cloud Computing, 3(1) (2015) 80-94.
[38] J. Idziorek, T. Mark, Tannian, D. Jacobson, The Insecurity of Cloud Utility Models, IEEE IT Professional, 15(2) (2013) 22-27.
[39] F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, A. Castiglione, Energy-oriented denial of service attacks: an emerging menace for large cloud infrastructures, Journal of Supercomputing, 71(5) (2013) 1620-1641.
[40] F. Palmieri, M. Ficco, A. Castiglione, Adaptive Stealth Energy-related DoS Attacks Against Cloud Data Centers, in: Proceedings of 8th IEEE International Conference on

Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Birmingham, England, 2014, pp. 265-272.
[41] A. Chonka, J. Abawajy, Detecting and mitigating HX-DoS attacks against cloud web services, in: Proceedings of 15th IEEE International Conference on Network-Based Information Systems (NBiS), Melbourne, Australia, 2012, pp. 429-434.
[42] R.V Deshmukh, K. K. Devadkar, Understanding DDoS Attack & its Effect in Cloud Environment, Procedia Computer Science 49 (2015) 202-210.
[43] B. Cha, J. Kim, Study of multistage anomaly detection for secured cloud computing resources in future internet, In: IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC),Sydney, Australia, 2011, pp. 1046-1050
[44] M.H Bhuyan, D.K. Bhattacharyya, J.K Kalita, An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection, Pattern Recognition Letters
[45] Y.G. Dantas, V. Nigam, I.E. Fonseca, A Selective Defense for Application Layer DdoS Attacks. In: Proceedings of IEEE Joint Intelligence and Security Informatics Conference (JISIC), Hague, Netherlands, 2014, pp. 75-82.
[46] H. Beitollahi, G. Deconinck, Analyzing well-known countermeasures against distributed denial of service attacks. Computer Communications 35(11) (2012) 1312-1332.
[47] F. Wong, C.X. Tan, A survey of trends in massive DDoS attacks and cloud-based mitigations, International Journal of Network Security & Its Applications (IJNSA) 6(3) (2014) 57-71.
[48] B. Cha, J. Kim, Study of multistage anomaly detection for secured cloud computing resources in future internet. In: Proceedings of IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), Sydney, Australia, 2011, pp. 1046-1050.
[49] X. Rui, M. Wen-Li, Z. Wen-Ling, Defending against UDP flooding by negative selection algorithm based on eigenvalue sets, in: Proceedings of IEEE fifth International Conference on Information Assurance and Security (IAS'09), Xi an, China, 2009, Vol. 2, pp. 342-345.
[50] T. Karnwal, T. Sivakumar, G. Aghila, A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack. In: Proceedings of IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2012, pp. 1-5.
[51] N. Gruschka, L.L Iacono, Vulnerable cloud: Soap message security validation revisited. In: Proceedings of IEEE International Conference on Web Services (ICWS 2009), Los Angeles, USA, 2009, pp. 625-631.
[52] M. Darwish, A. Ouda, L.F Capretz, Cloud-based DDoS attacks and defenses, In: IEEE International Conference on Information Society (i-Society), Toronto, Canada, 2013, pp. 67-71
[53] S. Arukonda, S. Sinha, The Innocent Perpetrators: Reflectors and Reflection Attacks,ACSIJ Advances in Computer Science: an International Journal, 4(1) (2015) 94-98.
[54] A. Bakshi, B. Yogesh, Securing cloud from ddos attacks using intrusion detection system in virtual machine, in: Proceedings of Second IEEE International Conference on Communication Software and Networks (ICCSN'10), Singapore, 2010, pp. 260-264
[55] A. M. Lonea, D. E. Popescu, O. Prostean, H. Tianfield, Soft Computing Applications , Evaluation of Experiments on Detecting Distributed Denial of Service (DDoS) Attacks in Eucalyptus Private Cloud (2013) 367-379.

[56] T. Karnwal, S. Thandapanii, A. Gnanasekaran, A filter tree approach to protect cloud computing against xml ddos and http ddos attack, In Intelligent Informatics (2013) 459-469.
[57] V. Chandola, B. Arindam, K. Vipin, Anomaly detection: A survey, ACM computing surveys (CSUR) 41(3) (2009)15:1-58.
[58] Victor Prokhorenko, Kim-Kwang Raymond Choo, Helen Ashman, Web application protection techniques: A taxonomy, Journal of Network and Computer Applications, Volume 60, January 2016, Pages 95-112, ISSN 1084-8045, http://dx.doi.org/10.1016/j.jnca.2015.11.017.
[59] T. Vissers, T.S Somasundaram, L. Pieters, K. Govindarajan, P. Hellinckx, DdoS defense system for web services in a cloud environment, Future Generation Computer Systems 37 (2014) 37-45.
[60] P. Shamsolmoali, M. Zareapoor, Statistical-based filtering system against DDOS attacks in cloud computing, in: Proceedings of International Conference on Advances in Computing, Communications and Informatics (ICACCI), New Delhi, India, 2014, pp. 1234-1239.
[61] J. Choi, C. Choi, B. Ko, P. Kim, A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment, Soft Computing, 18(9), (2014) 1697-1703.
[62] B. Joshi, B.K Joshi, Securing cloud computing environment against DDoS attacks, in: Proceedings of IEEE International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2012, pp. 1-5,
[63] N. Jeyanthi, N. C. Iyengar, P. M. Kumar, A. Kannammal, An enhanced entropy approach to detect and prevent DDoS in cloud environment, International Journal of Communication Networks and Information Security (IJCNIS) 5(2) (2013) 119-140.
[64] N. Jeyanthi, U. Barde, M. Sravani, V. Tiwari, N. C. Iyengar, Detection of distributed denial of service attacks in cloud computing by identifying spoofed IP, International Journal of Communication Networks and Distributed Systems 11(3) (2013) 262-279.
[65] S. Gupta, P. Kumar, A. Abraham, A profile based network intrusion detection and prevention system for securing cloud environment, International Journal of Distributed Sensor Networks (2013) 1-12
[66] D. Krishnan, M. Chatterjee, An adaptive distributed intrusion detection system for cloud computing framework, in: Proceedings of International Conference of Recent Trends in Computer Networks and Distributed Systems Security (SNDS), Trivandrum, India, 2012, pp. 466-473.
[67] C. C. Lo, C. C. Huang and J. Ku, "A Cooperative Intrusion Detection System Framework for Cloud Computing Networks," 2010 39th International Conference on Parallel Processing Workshops, San Diego, CA, 2010, pp. 280-284. doi: 10.1109/ICPPW.2010.46
[68] W. Long, L. Yuqing and X. Qingxin, "Using CloudSim to Model and Simulate Cloud Computing Environment," 2013 Ninth International Conference on Computational Intelligence and Security, Leshan, 2013, pp. 323-328. doi: 10.1109/CIS.2013.75
[69] P. Lv, P. Yang, Y. Dong and L. Gu, "BALLKNN: An efficient and scalable KNN based on Euclidean similarity," 2016 International Joint Conference on Neural Networks (IJCNN), Vancouver, BC, 2016, pp. 5141-5148. doi: 10.1109/IJCNN.2016.7727878
[70] Ashalatha R., J. Agarkhed and S. Patil, "Analysis of simulation tools in cloud computing," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 748-751. doi:

10.1109/WiSPNET.2016.7566233
[71] R. Aishwarya and S. Malliga, "Intrusion detection system- An efficient way to thwart against Dos/DDos attack in the cloud environment," 2014 International Conference on Recent Trends in Information Technology, Chennai, 2014, pp. 1-6. doi: 10.1109/ICRTIT.2014.6996163
[72] L. Ya-Dong, "Study on Detection Algorithm of DDoS Attack for Cloud Computing," 2014 Fifth International Conference on Intelligent Systems Design and Engineering Applications, Hunan, 2014, pp. 950-953. doi: 10.1109/ISDEA.2014.210