ICWR2020

کنفرانس بین المللی وب پژوهی
ایران، تهران ۲۲ خرداد ۱۳۹۹

A Security-aware Virtual Machine Placement in the Cloud

Sattar Feizollahibarough [1], Mehrdad Ashtiani [*2]

[1] M.Sc. Student, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran
s_feizollahibarough@cmps2.iust.ac.ir

[2] Assistant Professor, School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran
m_ashtiani@iust.ac.ir

Abstract

With the rapid growth and development of cloud computing, many startups or even large enterprises have decided to employ cloud services due to its dynamic provisioning and also reducing costs through the reduction of seasoned human resources needed to maintain the infrastructure. On the other hand, the risks of using shared resources and virtual machines are among the biggest threats that have always challenged the advantages of using cloud services. It is now possible for an attacker to attack a virtual machine and through that target the virtual machine manager or hypervisor. This approach will allow the attacker to completely control other virtual machines existing in the domain. Therefore, using a mechanism to decrease the co-location degree of vulnerable virtual machines on the same physical machine can be effective in reducing such security risks. To address these issues, we have proposed a security-aware virtual machine placement scheme to reduce the risk of vulnerable virtual machines co-placement. To manage the precision of security evaluation, it is vital to consider some hesitancy factors regarding security evaluations. Thus, to consider hesitancy in our proposed method, hesitant fuzzy sets are applied and several experimental evaluations have demonstrated the benefits of the proposed approach.

Keywords: Cloud Computing, Virtual Machine Placement, Hesitant Fuzzy Sets, Cybersecurity.

JCWR2020

کنفرانس بین المللی وب پژوهی
ایران، تهران ۲۲ خرداد ۱۳۹۹

یک روش جانمایی آگاه از مخاطرات امنیتی ماشین‌های‌مجازی در محیط‌های رایانش ابری

ستار فیض‌اللهی باروق[۱]، مهرداد آشتیانی*[۲]

[۱] دانشگاه علم و صنعت ایران، دانشکده مهندسی کامپیوتر
s_feizollahibarough@cmps2.iust.ac.ir

[۲] دانشگاه علم و صنعت ایران، دانشکده مهندسی کامپیوتر
m_ashtiani@iust.ac.ir

چکیده

با رشد و گسترش سریع محاسبات ابری، بسیاری از شرکت‌های نوپا و یا حتی کسب‌وکارهای بزرگ تصمیم دارند با توجه به قابلیت مقایس‌پذیری پویا و همچنین عدم نیاز به نیروی‌انسانی متخصص برای نگهداری از زیرساخت و به منظور صرفه‌جویی در هزینه‌های خود از خدمات ابری استفاده کنند. از سوی دیگر مخاطرات ناشی از استفاده از منابع و چارچوب‌های اشتراکی مانند ناظر ماشین‌مجازی، جز تهدیداتی محسوب می‌شوند که مزیت‌های خدمات ابری را همواره به چالش کشیده‌اند. در حال حاضر این امکان وجود دارد تا فرد مهاجمی، یک ماشین‌مجازی را مورد حمله قرار دهد تا در ادامه بتواند ناظر ماشین‌مجازی را مورد هدف قرار دهد که در صورت وقوع این اتفاق، مهاجم به صورت کامل سایر ماشین‌های مجازی که ناظر ماشین‌مجازی آنها را کنترل می‌کند را نیز به کنترل خود در آورد یا از کار بیاندازد. در این پژوهش، روشی بر اساس مجموعه فازی مردد ارائه شده است که با ایجاد آگاهی نسبت به مخاطرات امنیتی موجود در مرکز داده ابری، ماشین‌های‌مجازی را بر اساس این مخاطرات به صورت آگاه از حملات امنیتی بر روی ماشین‌های فیزیکی جانمایی می‌کند تا در صورت حمله به یک ماشین‌مجازی، مهاجم امکان کمتری برای گسترش حملات به سایر ماشین‌های‌مجازی و یا ناظر ماشین‌مجازی را داشته باشد. در انتها، به منظور بررسی عملکرد راه‌کار پیشنهادی، سه سناریو مطرح شده است و به ارزیابی راه‌کار پیشنهادی پرداخته شده است که در آخرین سناریو، این راه‌کار با دو مطالعه مرتبط دیگر مقایسه شده است.

کلمات کلیدی

محاسبات ابری، جانمایی ماشین‌مجازی، مجموعه فازی مردد، امنیت سایبری

۱- مقدمه

با بلوغ هر چه بیشتر خدمات ابری از یک سو و تمایل بیشتر شرکت‌ها و افراد برای استفاده از این خدمات، بررسی، کاوش و تلاش برای نفوذ به این خدمات توسط مهاجمین و افراد سودجو نیز افزایش چشم‌گیری پیدا کرده است. یکی از چالش‌های امنیتی که به صورت عمده این خدمات را مورد تهدید قرار می‌دهد، لایه‌ی مجازی‌سازی است[1]. در این لایه، مهاجم تلاش می‌کند با رسوخ به یک ماشین‌مجازی بتواند به سایر ماشین‌های مجازی دیگر که در همان ماشین فیزیکی جانمایی شده‌اند دست یابد و یا با رسوخ به ناظر ماشین‌مجازی کنترل تمامی ماشین‌های‌مجازی را به دست گیرد. از این روی طی چند سال گذشته تحقیقات صنعتی و دانشگاهی در حال سوق پیدا کردن به سویی است که علاوه بر برطرف کردن نیازهای گذشته هم‌چون استفاده بهینه از منابع و پایبندی فراهم‌کننده‌ی زیرساخت ابری[۱] به توافق‌نامه سطح خدمت[۲]، بتوانند چالش‌های امنیتی ناشی از استفاده از منابع اشتراکی را نیز مرتفع کنند.

در همین راستا، این پژوهش نیز برای پاسخگویی به این چالش شکل گرفته است و سعی دارد با ارائه یک مدل برای جانمایی ماشین‌های‌مجازی در یک محیط محاسباتی ابری به صورت خودکار به این مشکل بپردازد. در این مدل، عمل جانمایی ماشین‌های‌مجازی بر روی ماشین‌های‌فیزیکی به صورت خودکار با توجه به آسیب‌پذیری‌های موجود در ماشین‌های‌مجازی، انجام

می‌پذیرد. در مدل ارائه شده، هدف، کمینه‌سازی مخاطرات امنیتی در لایه‌ی ناظر ماشین‌های‌مجازی خواهد بود و برای نیل به این مقصود، امر جانمایی ماشین‌های‌مجازی به صورتی انجام خواهد شد که ماشین‌های‌مجازی با آسیب‌پذیری‌های پر مخاطره بر روی یک ماشین‌فیزیکی جانمایی نشوند تا در ادامه مهاجم نتواند از این آسیب‌پذیری‌ها برای رسوخ به سایر ماشین‌های‌مجازی و یا ناظر ماشین‌مجازی استفاده کند.

برای جانمایی ماشین‌های‌مجازی با رویکرد امنیتی نیاز است از سنجه‌های امنیتی استفاده کرد تا بتوان میزان آسیب‌پذیری هر ماشین‌مجازی و همچنین کل یک ماشین‌فیزیکی را مورد ارزیابی قرار داد. در مطالعات پیشین این امر انجام شده است ولی در هیچکدام از مطالعات قبلی به موضوع عدم قطعیت در خصوص این سنجه‌ها پرداخته نشده است. با توجه به این نکته که این سنجه‌ها هر کدام با توجه به شرایط و محیط توسعه ابر می‌توانند مقادیری متفاوت را تولید کنند، لذا در نظر گرفتن عدم قطعیت برای هر کدام از این سنجه‌ها حیاتی و لازم است که در این مطالعه به صورت ویژه طرح جانمایی با این رویکرد مدل شده است. برای مدل کردن این طرح از مجموعه فازی مردد استفاده شده است که در عمل می‌تواند عدم قطعیت در تصمیم‌گیری برای مسئله جانمایی را نمایش دهد. مجموعه فازی مردد در کنار مدل کردن عدم قطعیت در تصمیم‌گیری، این قابلیت را نیز بوجود آورده است که بتوان اولویت‌های موجود را در تصمیم‌گیری لحاظ کرد. این قابلیت یکی دیگر از مزایایی است که به مدل جانمایی این امکان را می‌دهد که اولویت‌های فراهم‌کننده ابر را لحاظ کند. این مطالعه در ادامه به این صورت سازمان‌دهی شده است: در بخش دوم، پیشینه تحقیق ارائه شده است. در بخش سوم، مبانی نظری مورد بحث قرار گرفته است که در این بخش اطلاعات لازم در خصوص ارزیابی امنیت و مجموعه فازی مردد ارائه شده است. در بخش چهارم، راه‌کار پیشنهادی به همراه جزئیات مدل ارائه شده است. در بخش پنجم ارزیابی‌های انجام شده برای دقت و درستی مدل ارائه شده است و در نهایت در بخش ششم این مطالعه، نتیجه‌گیری به همراه مطالعات آتی ذکر گردیده است.

۲- پیشینه تحقیق

در این بخش سعی شده است تا با مطالعه گسترده در حوزه‌ی ادبیات موضوع، پیشینه جامعی گردآوری و همچنین کاربرد مدل‌های موجود در این حوزه مطرح گردد. در دو دهۀ گذشته و به‌خصوص با شدت گرفتن استفاده از زیرساخت‌های ابری، راه‌کارهای فراوانی جهت جانمایی ماشین‌های مجازی پیشنهاد شده است. اکثر این راه‌کارها در جهت کاهش مصرف انرژی و یا ترافیک شبکه مدل‌هایی را ارائه کرده‌اند [2][3]. اما در سال‌های گذشته و با توجه به افزایش آگاهی نسبت به مخاطرات موجود در زیرساخت‌های ابری مطالعات بیشتری در این خصوص در حال انجام است [4]. در این بخش نیز مطالعات صورت گرفته در سال‌های اخیر در مورد جانمایی ماشین‌های‌مجازی با رویکرد امنیتی مورد بحث و بررسی قرار گرفته است.

در مطالعه‌ای که توسط آگاروال و همکاران انجام شده است، الگوریتمی را ارائه کرده‌اند که از آن تحت عنوان "ماشینِ جانمایی شده قبلی کاربران اول"[۳] یاد شده است. در این راه‌کار در هنگام تخصیص جا برای یک ماشین‌مجازی جدید زمان‌بند ملزم به بررسی است که آیا کاربری که صاحب ماشین‌مجازی است کاربری جدید است و یا کاربری قدیمی است. اگر کاربر، کاربری جدید است آنگاه الگوریتم یکی از ماشین‌های فیزیکی را به صورت تصادفی انتخاب و سپس ماشین‌مجازی را در آن جانمایی می‌کند. در غیر این صورت و در صورت وجود ظرفیت در ماشین‌های فیزیکی، الگوریتم سعی می‌کند ماشین مجازی جدید را بر روی ماشین‌های فیزیکی جانمایی نماید که کاربر از قبل بر روی آنها ماشین‌مجازی داشته است. دلیل اصلی این راه‌کار، محدود کردن تعداد کاربران بدون ریسک است که کاربران مخرب می‌توانند با آنها کنار یکدیگر جانمایی شوند[5]. با توجه به مزایایی که این راه‌کار پیشنهادی دارد، اما همچنان محدودیت‌هایی نیز دیده می‌شود. مهم‌ترین محدودیت این راه‌کار آن است که ماشین‌های‌مجازی بر اساس میزان جدید بودن و قدیمی بودن صاحب ماشین‌مجازی سنجیده می‌شوند و بر اساس میزان آسیب‌پذیری‌های موجود و واقعی در هر ماشین‌مجازی سنجیده نمی‌شوند. این فرض درست است که هر چقدر کاربر قدیمی‌تر باشد و رفتار مخربی از خود نشان نداده باشد می‌توان به آن اعتماد بالاتری داشت اما این امکان وجود دارد که فرد مهاجم دیگری از آسیب‌پذیری‌های موجود بر روی ماشین‌های‌مجازی این کاربر استفاده کند و اقدام به حمله به سایر زیرساخت‌ها نماید.

همچنین در مطالعه دیگری که توسط یانگ و همکاران انجام شده است، راه‌کاری ارائه شده است که در ابتدا ماشین‌های‌مجازی بر اساس عوامل مرتبط با حملات کانال جانبی[۴]، بررسی و سپس بر اساس این آسیب‌پذیری‌های، ماشین‌های مجازی بر اساس بهینه‌سازی خطی عدد صحیح[۵] به ماشین‌های فیزیکی قرنطینه مهاجرت داده می‌شوند [6]. این راه‌کار پیشنهادی با توجه استفاده از عوامل مختلف توانسته است تا مقیاس‌پذیری بالا را برای اجرا و پیاده‌سازی در یک مرکز داده‌ای ابری بدست آورد؛ اما با وجود این رجحان در این مدل پیشنهادی، مهم‌ترین محدودیت این راه‌کار آن است که این راه‌کار تنها برای جلوگیری از وقوع حملات کانال جانبی در نظر گرفته شده است و سایر حملات از جمله مهم‌ترین این دسته یعنی گریز از ماشین مجازی[۶] را تحت پوشش قرار نمی‌دهد.

در مطالعه‌ای که هان و همکاران انجام داده‌اند مدلی آگاه نسبت به مخاطرات امنیتی ارائه شده است که در آن از راهبردی چند هدفه برای بهبود امنیت استفاده شده است. راهبردهایی که در این مطالعه برای کاهش مخاطرات در نظر گرفته شده بر اساس قیودی است که کاربر مشخص می‌نماید و به صورت عمده بر روی میزان مصرف حافظه‌ی اصلی و ترافیک شبکه تمرکز دارد [1]. سرعت تولید طرح جانمایی مبتنی بر این مدل‌ها به علت سادگی محاسبات بسیار بالا است، اما به شدت وابسته به قیودی است که توسط فراهم‌کننده‌ی خدمت و مشتری مشخص شده است. این قیود با توجه به این‌که در اکثر موارد توسط متخصصان زمینه‌ی امنیت وضع نشده‌اند نمی‌توانند به صورت کارا سیستم را ایمن سازند. محدودیت دیگری که این قیود ایجاد می‌کنند این است که ممکن است به مصرف بهینه‌ی منابع صدمه وارد کنند و بخش عمده‌ای از منابع را هدر بدهند.

برخی دیگر از مطالعات از قوانین انزوا برای جانمایی ماشین‌های‌مجازی استفاده کرده‌اند. برای مثال احمد و همکاران یک الگوریتم برای جانمایی ماشین‌های‌مجازی ارائه داده‌اند که در آن امنیت در محیط‌های محاسباتی ابری با استفاده از قوانین انزوای بین کاربران بهبود یافته است [7]. مهترین نقطه ضعف این مدل‌ها تعیین جانمایی بر اساس رویکرد کاربران است. این نقطه ضعف از دو جهت مهم خواهد بود. نخست آنکه کاربران لازم است تا از نحوه‌ی جانمایی خدمات یک‌دیگر با خبر باشند که این نکته ممکن است خود باعث ایجاد مخاطره امنیتی شود. مورد بعدی آن که کاربر ممکن است از مخاطرات امنیتی که خود را تهدید می‌کند به صورت کامل مطلع نباشد. در این صورت این مدل از جانمایی نمی‌تواند کارایی لازم را داشته باشد.

کویات و همکاران راه‌کاری ارائه کرده‌اند که در آن تمام ماشین‌های‌مجازی به صورت دوره‌ای بر اساس نظریه بازی بر روی ماشین‌های فیزیکی جانمایی می‌شوند [8]. یکی از بارزترین مزایای این مدل آزادی عمل کاربر برای انتخاب نوع راهبرد امنیتی برای هر ماشین‌مجازی است. اما مهم‌ترین محدودیت این مدل تعیین رفتار مهاجم به صورت از پیش تعریف شده و استفاده محدود از چند آسیب‌پذیری رایج است. در صورتی که در عمل، حرکات و فضای عمل مهاجم غیرقابل پیش‌بینی و متنوع خواهد بود.

۳- مبانی نظری

در این بخش سعی بر آن داریم تا مبانی نظری که برای درک مدل ارائه شده لازم است مرور شوند.

۳-۱- ارزیابی امنیت

در این پژوهش برای ارزیابی مخاطرات امنیتی که هر کدام از ماشین‌های‌مجازی را مورد تهدید قرار می‌دهند از بانک‌اطلاعاتی آسیب‌پذیری ملی آمریکا[۷] که در آن آسیب‌پذیری‌ها بر اساس سیستم امتیازدهی آسیب‌پذیری عام[۸] امتیازدهی می‌شوند، استفاده شده است. این سیستم امتیازدهی از سه سنجه[۹] تشکیل شده است که شامل: پایه[۱۰]، موقتی[۱۱] و محیطی[۱۲] می‌شود که سنجه‌ی پایه، خصوصیات ذاتی آسیب‌پذیری که با گذر زمان و در محیط‌های مختلف ثابت هستند را نمایش می‌دهد ولی دو سنجه موقتی و محیطی خصوصیات یک آسیب‌پذیری را به ترتیب در زمانی خاص و یا یک محیط خاص نمایش می‌دهد [9]. به صورت پیش فرض سنجه پایه مورد استفاده قرار می‌گیرد و یک آسیب‌پذیری را در بازه صفر تا ده امتیازدهی می‌کند. اما با توجه به نیاز، متخصصان حوزه امنیت با اضافه کردن دو سنجه دیگر این امتیاز را می‌توانند تغییر دهند. سنجه پایه خود از دو مجموعه از سنجه‌ها تشکیل شده است. اولین سنجه، سنجه قابلیت بهره‌برداری[۱۳] نام دارد که میزان سختی فنی برای استفاده از آسیب‌پذیری را مشخص می‌کند و دومین سنجه که با نام سنجه تاثیر[۱۴] شناخته می‌شود، تاثیری را که استفاده موفقیت آمیز مهاجم از آسیب‌پذیری بر روی دارایی‌های سازمان می‌گذارد مشخص می‌کند [9].

۳-۲- مجموعه فازی مردد[۱۵]

از زمانی که لطفی‌زاده [10] نظریه فازی را ارائه داده است، محققان بسیاری از این نظریه برای توضیح مسائل مربوط به فرآیند تصمیم‌گیری در شرایط عدم‌قطعیت استفاده نموده‌اند. مساله مربوط به جانمایی ماشین‌های مجازی نیز جز مسائلی است که نیازمند تصمیم‌گیری است که این تصیم‌گیری با توجه به وجود مخاطرات و شرایط مختلف که در ادامه به آنها اشاره خواهد شد همراه عدم‌قطعیت است.

یک عدد فازی که با $\tilde{A}$ نمایش داده می‌شود یک زیر مجموعه فازی از اعداد حقیقی است و تابع عضویت آن به صورت $\mu_{\tilde{A}(\chi)} = R \longrightarrow [0,1]$ نمایش داده می‌شود که در آن $\mu_{\tilde{A}(\chi)}$ نشان دهنده‌ی تابع عضویت بوده و با ویژگی‌های زیر توصیف می‌شود:

۱. $\mu_{\tilde{A}(\chi)}$ یک نگاشت پیوسته از R به نزدیک‌ترین بازه [0,1] است.
۲. $\mu_{\tilde{A}(\chi)}$ یک زیرمجموعه فازی محدب[۱۶] است.
۳. $\mu_{\tilde{A}(\chi)}$ نرمال شده یک زیرمجموعه فازی بوده به این معنا که عدد χ_0 وجود دارد به صورتی که $\mu_{\tilde{A}(\chi_0)} = ۱$ است.

در سال‌های اخیر یک بسط جدید برای مجموعه‌های فازی توسعه یافته است که از آن به عنوان مجموعه فازی مردد یاد می‌شود. همواره برای تخصیص درجه‌ی عضویت عناصر یک مجموعه‌ی فازی عدم قطعیت وجود داشته است و این بسط جدید قصد دارد که این تردید را مدل کند. مجموعه فازی مردد با استفاده از تابعی تعریف می‌شود که یک مجموعه از مقادیر عضویت را به ازای هر عنصر در دامنه برمی‌گرداند [11]. مجموعه فازی مردد را می توان از دو زاویه‌ی دید مختلف تعریف کرد:

جنبه اول آنکه اگر X یک مجموعه مرجع باشد، یک مجموعه فازی مردد بر روی X یک تابع h است که یک مجموعه از مقادیر بین [۰،۱] را برمی‌گرداند [6]:

$$h: X \rightarrow \wp([0,1)) \quad (۱)$$

مجموعه فازی مردد را می‌توان از جهت دیگری نیز مورد بررسی قرار داد و آن را به صورت زیر تعریف کرد:

اگر $M = \{\mu_1, \dots, \mu_n\}$ یک مجموعه از n تابع عضویت باشد، مجموعه فازی مردد مرتبط با M به صورت h_M نمایش داده می‌شود و به صورت فرمول (۲) تعریف خواهد شد [11]:

$$h: X \rightarrow \wp([0,1))$$
$$h_M = \bigcup_{\mu \in M} \{\mu(X)\} \quad (۲)$$

تعریف بالا نشان می‌دهد که از مجموعه فازی مردد می‌توان در مواقعی استفاده کرد که تعدادی شرط وجود داشته باشد و یک یا چند تصمیم‌گیرنده قصد تصیم‌گیری در مورد انتخاب بین چند گزینه را داشته باشند [12]. در ادامه ژیا و همکاران یک نمایش ریاضی برای مجموعه فازی مردد ارائه کرده‌اند که به صورت فرمول (۳) است [13]:

$$E = \{\langle \chi, h_E(\chi)\rangle : \chi \in X\} \quad (۳)$$

اگر $h_E(\chi)$ مجموعه‌ای از برخی از مقادیر [0,1] باشد، امکان درجه عضویت عنصر $\chi \in X$ به مجموعه E را مشخص می‌کند. در مطالعه [13]،

$h_E(\chi)$ را عنصر فازی مردد [۱۷] مجموعه E و $H = \cup h_E(x)$ را مجموعه تمام عناصر فازی مردد مجموعه E نامیده‌اند.

٤- راه‌کار پیشنهادی

در راه‌کار پیشنهادی زمان‌بند عمومی[۱۸] به گونه‌ای طراحی شده است که باید از بین چندین انتخاب $D = \{d_1, \dots, d_n\}$ یکی را به عنوان بهترین گزینه انتخاب و اجرا کند. هر d_i نشان‌دهنده یک تصمیم برای اتخاذ توسط زمان‌بند عمومی است. برای مثال d_1 به معنای آن است که عمل جابجایی صورت نگیرد و d_2 به معنای آن است که ماشین‌مجازی داده شده باید از ماشین فیزیکی جاری به ماشین فیزیکی شماره یک انتقال پیدا کند. در راه‌کار پیشنهادی چهار خصوصیت[۱۹] با توجه به شاخصه محیط ابر برای جانمایی در نظر گرفته شده است که به صورت زیر تعریف شده‌اند:

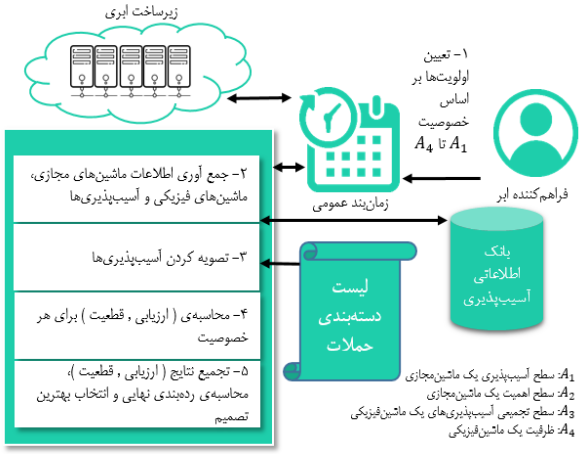
A_1: سطح آسیب‌پذیری یک ماشین‌مجازی.

A_2: سطح اهمیت یک ماشین‌مجازی.

A_3: سطح تجمیعی آسیب‌پذیری‌های یک ماشین‌فیزیکی.

A_4: ظرفیت یک ماشین‌فیزیکی.

همانطور که در شکل (۱) مشخص شده است، فراهم‌کننده ابر باید اولیت‌های خود را نسبت به این چهار خصوصیت برای زمان‌بند عمومی مشخص کند. از آنجایی که ساختار و سیاست‌های هر مرکز داده ابری با هم متفاوت است، هر فراهم‌کننده ابر با توجه به نیاز و سیاست‌های خود، اولیت را انتخاب می‌کند. در گام بعدی، زمان‌بند عمومی اقدام به پویش[۲۰] محیط ابر می‌کند تا بتواند ماشین‌های‌مجازی، ماشین‌های‌فیزیکی و آسیب‌پذیری‌های موجود بر روی هر ماشین‌مجازی را جمع‌آوری کند و این آسیب‌پذیری را بر اساس دسته‌بندی جدول (۱) تصفیه می‌کند و مابقی آسیب‌پذیری‌ها در نظر گرفته نمی‌شود. دلیل این امر آن است که مهاجم بعد از رخنه به یک ماشین‌مجازی با استفاده از یکی از انواع دسته‌بندی حملات جدول (۱) قادر خواهد بود که به ناظر ماشین‌مجازی و یا یکی از ماشین‌های‌مجازی که با آن بر روی یک ماشین فیزیکی جانمایی شده‌اند رسوخ کند و امکان رسوخ با سایر حملات نخواهد بود.



شکل (۱) : شمای عمومی راه‌کار پیشنهادی

در مرحله بعدی بر اساس داده‌های جمع‌آوری شده و با توجه به هر خصوصیت ارائه شده A_1 تا A_4، یک دوتایی به صورت (ارزیابی , قطعیت) ایجاد می‌شود که ارزیابی بیان می‌کند که برای شرط مورد نظر چه امتیازی دریافت خواهد کرد. پارامتر دوم قطعیت میزان دقیق بودن این امتیاز را بیان می‌کند. در انتها، یک مرحله تجمیعی، تمامی خصوصیات را با توجه به اولویتی که فراهم‌کننده‌ی ابر با توجه به سیاست‌ها و بافتار مشخص کرده است را تجمیع می‌کند و بر اساس نتیجه حاصل از این تجمیع زمان‌بند عمومی از میان تصمیم‌های موجود، تصمیمی با بالاترین رتبه را انتخاب می‌کند.

۴-۱- تعیین اولویت خصوصیت‌ها

اولین قدم برای این راه‌کار انتخاب اولویت خصوصیات A_1 تا A_4 بر اساس اولویت‌ها و سیاست‌های مرکز داده ابری است. این اولیت‌ها به صورت فرمول (۴) بیان می‌شوند:

$$\omega = \{\omega_1, \dots, \omega_4\} \quad (۴)$$

به صورتی که $0 \leq \omega_i \leq 1$ الویت هر خصوصیت را نمایش می‌دهد و به اصطلاح وزن خصوصیت[۲۱] خوانده می‌شود [12].

۴-۲- جمع‌آوری و تصفیه اطلاعات

در این بخش، گام دوم و سوم شمای عمومی راه‌کار پیشنهادی ارائه می‌شود. در این مرحله، ابتدا زمان‌بند عمومی اطلاعات مربوط به ماشین‌های فیزیکی، ماشین‌های‌مجازی و آسیب‌پذیری‌ها به ترتیب به صورت فرمول (۵)، (۶) و (۷)

جدول (۱) : دسته‌بندی حملات موثر در جانمایی ماشین‌های‌مجازی بر روی یک ماشین‌فیزیکی مشترک

ردیف	نوع آسیب‌پذیری	توضیح آسیب‌پذیری
۱	DOS	در این نوع از حملات، با حمله به یک ماشین مجازی و یا ناظر ماشین مجازی، دسترس‌پذیری[۲۲] ماشین‌های مجازی جانمایی شده در کنار هم تحت تاثیر قرار می‌گیرد.
۲	Hyper Jacking	در این نوع از حملات، مهاجم به ناظر ماشین مجازی حمله کرده و کدهای مخربی[۲۳] را به آن تزریق می‌کند که در ادامه، این کدها بر روی تمام ماشین‌های‌مجازی جانمایی شده بر روی آن ناظر ماشین‌مجازی قابل اجرا از راه دور خواهد بود.
۳	Memory Corruption	در این نوع از حملات، مهاجم با در اختیار گرفتن یک ماشین‌مجازی سعی در ایجاد اختلال در حافظه اشتراکی و در نتیجه آسیب به سایر ماشین‌های‌مجازی می‌کند.
۴	Virtual machine escape	در این نوع از حملات، مهاجم سعی دارد با اجرای کد مخربی به ناظر ماشین‌مجازی دست پیدا کند و آن را تحت کنترل بگیرد.
۵	Directory traversal	در این نوع از حملات، مهاجم می‌تواند به فایل‌های ماشین‌مجازی دیگر دست پیدا کند.
۶	Cross-VM cache side channel	در این نوع از حملات، مهاجم با شنود حافظه اصلی مشترک سعی بر پیدا کردن الگوهایی دارد که در ادامه منجر به افشای اطلاعات خواهد شد.

نشان می‌دهد که در آن هر ماشین فیزیکی به صورت ph_i، هر ماشین‌مجازی موجود بر روی ماشین‌فیزیکی ph_m را به صورت VM_i و هر آسیب‌پذیری موجود بر روی ماشین‌مجازی vm_n به صورت VL_i است.

$$PH = \{ph_1, \dots, ph_M\} \quad (۵)$$

$$VM_M = \{vm_1, \dots, vm_N\} \quad (۶)$$

$$VL_N = \{vl_1, \dots, vl_T\} \quad (۷)$$

در گام سوم مجموعه‌ی آسیب‌پذیری‌های موجود بر روی هر ماشین‌مجازی بر اساس جدول (۱) تصفیه می‌شود.

$$\overline{VL_N} \subseteq VL_N \quad (۸)$$

۴-۳- محاسبه‌ی خصوصیت‌ها

در این بخش، نحوه‌ی محاسبه هر کدام از خصوصیات A_1 تا A_4 بر اساس نمایش ریاضی مجموعه فازی مردد (۳) ارائه خواهد شد.

٤-۳-۱- سطح آسیب‌پذیری یک ماشین‌مجازی

این خصوصیت، همانطور که در فرمول (۹)، (۱۰) و (۱۱) نشان داده شده است، میزان آسیب‌پذیری یک ماشین‌مجازی را براساس دو سنجه تاثیر و قابلیت بهره‌برداری که از سیستم امتیازدهی آسیب‌پذیری عام استخراج شده است محاسبه خواهد کرد.

$$\overline{vl}_N = \{(\overline{imp}_1, \overline{exp}_1), \dots, (\overline{imp}_t, \overline{exp}_t)\} \quad (۹)$$

$$IMP_N = \frac{\sum_{\overline{imp}=1}^{t} imp_i}{t}$$

$$Normal(IMP_N) = \frac{IMP_N - \min(IMP_N)}{\max(IMP_N) - \min(IMP_N)} \quad (۱۰)$$

$$EXP_N = \frac{\sum_{\overline{exp}=1}^{t} exp_i}{t}$$

$$Normal(EXP_N) = \frac{exp_N - \min(exp_N)}{\max(exp_N) - \min(exp_N)} \quad (۱۱)$$

با توجه به نمایش ریاضی مجموعه فازی مردد در فرمول (۳)، فرمول (۱۲) را خواهیم داشت:

$$A_1 = \big(Normal(IMP_N), Normal(EXP_N)\big) \quad (۱۲)$$

برای مثال $A_1 = (0.59, 0.39)$ بیان می‌دارد که مجموع آسیب‌پذیری‌های ماشین‌مجازی 0.59 است ولی میزان قطعیت برای این عدد ۰.۳۹ است.

٤-۳-۲- سطح اهمیت یک ماشین‌مجازی

این خصوصیت در واقع میزان اهمیت یک ماشین‌مجازی در ساختار شبکه فراهم‌کننده زیرساخت ابری را نمایش می‌دهد. برای محاسبه ارزیابی میزان اهمیت یک ماشین‌مجازی به صورت ساده فقط از درجه‌ی مرکزیت[۲۴] که به صورت فرمول (۱۳) تعریف شده است استفاده شده است[14]:

$$C_D(vm_i) = \frac{\deg(vm_i)}{m-1}$$

$$Normal\big(C_D(vm_i)\big) = \frac{C_D(vm_i) - \min\big(C_D(vm_i)\big)}{\max\big(C_D(vm_i)\big) - \min\big(C_D(vm_i)\big)} \quad (۱۳)$$

که در معادله بالا m طول مجوعه یال‌های شبکه فراهم‌کننده زیرساخت ابری است. اما در یک شبکه، صرفاً داشتن تعداد زیادی یال به معنای مهم بودن یک ماشین‌مجازی نیست. برای مثال، ممکن است در یک محیط یک ماشین پشتیبان‌گیر دارای ارتباطات فراوان بوده اما از لحاظ اهمیت دارای کمترین اهمیت باشد. لذا برای بررسی دقیق‌تر اهمیت یک ماشین‌مجازی برای $C_D(vm_i)$ میزان عدم قطعیت در نظر گرفته شده است که این میزان به وسیله میانه‌ی مرکزی[۲۵] با فرمول‌های (۱۴) و (۱۵) محاسبه می‌گردد[14]:

$$C_{btw}(vm_i) = \sum_{s,t \in m} \frac{\sigma_{s,t}(vm_i)}{\sigma_{s,t}}$$

$$Normal\left(C_{btw}(vm_i)\right) = \frac{C_{btw}(vm_i) - \min(C_{btw})}{\max(C_{btw}) - \min(C_{btw})} \quad (۱۴)$$

$$A_2 = \big(Normal\big(C_D(vm_i)\big), Normal\left(C_{btw}(vm_i)\right)\big) \quad (۱۵)$$

٤-۳-۳- سطح تجمیعی آسیب‌پذیری‌های یک ماشین‌فیزیکی

این خصوصیت سطح تجمیعی آسیب‌پذیری‌های موجود بر روی ماشین‌های‌مجازی جانمایی شده بر روی یک ماشین فیزیکی را نمایش می‌دهد. اگر M تعداد ماشین‌های‌مجازی جانمایی شده بر روی یک ماشین‌فیزیکی باشد آنگاه فرمول (۱۶) را خواهیم داشت:

$$A_3 = \left(\frac{\sum_{i=0}^{M} Normal(IMP_M)}{M}, \frac{\sum_{i=0}^{M} Normal(EXP_M)}{M}\right) \quad (۱۶)$$

٤-۳-٤- ظرفیت یک ماشین‌فیزیکی

این خصوصیت، ظرفیت یک ماشین برای جانمایی یک ماشین‌مجازی را مورد بررسی قرار می‌دهد. برای محاسبه این خصوصیت از دو مفهوم نرخ مصرف منبع[۲۶] و نرخ تعادل منبع[۲۷] که توسط هیو و همکاران [15] معرفی گردیده استفاده شده است. اگر M تعداد ماشین‌های‌فیزیکی باشد و K تعداد ماشین‌های مجازی جانمایی شده بر روی یک ماشین فیزیکی باشد، نرخ مصرف منبع و نرخ تعادل منبع d بعدی یک ماشین فیزیکی ph_i به صورت فرمول (۱۷) تعریف خواهد شد:

$$RU_i^d = \frac{u_i^d + w_i^d}{\hat{r}_i^d} \quad (۱۷)$$

در نمایش ریاضی بالا u_i^d میزان مصرف منابع توسط ماشین‌های‌مجازی موجود با d بعد است. برای مثال ممکن است زمان‌بند عمومی قصد داشته باشد تا فقط میزان مصرف منابع توسط ماشین‌های‌مجازی را برای دو منبع پردازشگر مرکزی و حافظه‌اصلی را ارزیابی کند لذا $d = 2$ خواهد بود. پارامتر w_i^d بار[۲۸] ابتدایی برای بر روی هر منبع را نمایش می‌دهد و $\hat{r}_i^d$ مشخصات یک ماشین‌مجازی جدید بر روی یک ماشین‌فیزیکی را نمایش می‌دهد. با توجه به اینکه مقدار محاسبه شده برای نرخ مصرف منبع دقیق نیست برای تعیین این دقت از نرخ تعادل به صورت ذیل استفاده خواهد شد.

$$RB_i = \frac{u_i}{RU_i^d / max_{d\in\{1,\dots,|D|\}}} \quad (۱۸)$$

$$A_4 = (\mathrm{RU}, \mathrm{RB}) \quad (۱۹)$$

۴-۴- تجمیع نتایج

در این بخش، نتایج حاصل از چهار خاصیت A_1 تا A_4 که پیش‌تر ارائه شد برای رتبه‌بندی و انتخاب تجمیع می‌شوند تا در ادامه زمان‌بند عمومی بتواند از بین چندین انتخاب $D = \{d_1, \dots, d_n\}$ یکی را به عنوان بهترین، انتخاب نماید. به ترتیب، d_1 به معنای آن است که عمل جابجایی برای ماشین‌مجازی مورد نظر صورت نگیرد، d_2 به معنای آن است که ماشین‌مجازی به ماشین‌فیزیکی اول مهاجرت کند و d_n به معنای آن است که ماشین‌مجازی به ماشین‌فیزیکی $\mathrm{m}+1$ مهاجرت کند. همچنین، m تعداد ماشین‌های فیزیکی است. همانطور که در گام نخست معرفی شد وزن خصوصیت‌ها نیز در تصمیم زمان‌بند عمومی نقش دارد. با توجه به این موضوع نمایش ریاضی ارائه شده در [16] جهت مدل کردن مورد استفاده قرار گرفته است.

$$\mathrm{E_{d_i}} = \{\langle \mathrm{A_j}, \mathrm{h_{ij}}\rangle | \mathrm{j} = 1,2,\dots,4\}, \mathrm{i} = 1,2,\dots,\mathrm{m}+1 \quad (۲۰)$$

خروجی این مدل یک ماتریس مجموعه فازی مردد خواهد بود و برای امتیازدهی به هر $\mathrm{E_{d_i}}$ از تابع امتیازی[۲۹] استفاده شده است [10]. این تابع بیان می‌دارد که اگر $\mathrm{E_{d_1}}$ و $\mathrm{E_{d_2}}$ دو مجموعه فازی مردد باشند، $\mathrm{E_{d_1}} \geq \mathrm{E_{d_2}}$ است تنها و تنها اگر $Score(\mathrm{E_{d_1}}) \geq Score(\mathrm{E_{d_2}})$ باشد که در آن امتیاز هر کدام به صورت فرمول‌های (۲۱) و (۲۲) محاسبه خواهد شد:

$$Score(\mathrm{E_{d_1}}) = \frac{1}{\mathrm{m}+1} \sum_{\mathrm{i}=1}^{\mathrm{m}+1} \mathrm{s}\left(\mathrm{h_{E_{d1}}(d_i)}\right) \quad (۲۱)$$

$$Score(\mathrm{E_{d_2}}) = \frac{1}{\mathrm{m}+1} \sum_{\mathrm{i}=1}^{\mathrm{m}+1} \mathrm{s}\left(\mathrm{h_{E_{d2}}(d_i)}\right) \quad (۲۲)$$

۵- ارزیابی

در این قسمت، برای تشریح دقت و میزان تاثیر راه‌کار ارائه شده، سه سناریو طراحی شده است. دراولین سناریو برای تحلیل میزان تاثیر راه‌کار ارائه شده به بررسی میانگین میزان تجمعی آسیب‌پذیری‌های ماشین‌های مجازی جانمایی شده بر روی یک ماشین‌فیزیکی پرداخته شده است. همچنین برای تشریح دقت این راه‌کار، در دومین سناریو به بررسی تاثیر اولویت خصوصیت‌ها بر وضعیت جانمایی‌ماشین‌های مجازی خواهیم پرداخت. در سومین سناریو برای بررسی میزان کارایی راه‌کار پیشنهادی، این راه‌کار با دو راه‌کار دیگر که در این مطالعه، بررسی شده‌اند مقایسه خواهند شد. برای پیاده‌سازی هر کدام از این سناریوها از زبان برنامه‌نویسی پایتون استفاده شده است که در آن با استفاده از کتابخانه *NetworkX* اقدام به ایجاد گراف گردیده است و همچنین کارهای مربوط به تحلیل داده با استفاده کتابخانه *pandas* انجام شده است. در هر سناریو نیز به تفکیک نحوه شبیه‌سازی سناریو مورد بررسی قرار گرفته است.

۵-۱- سناریو۱: بررسی میانگین میزان تجمعی آسیب‌پذیری‌های ماشین‌مجازی

همانطور که در بخش یک توضیح داده شد، یکی از چالش‌های امنیتی که در خصوص جانمایی ماشین‌های‌مجازی بر روی یک ماشین‌فیزیکی وجود دارد آن است که اگر ماشین‌های‌مجازی حامل یک یا چند آسیب‌پذیری از انواعی که در جدول (۱) ذکر شده‌اند باشند و در صورتی که این ماشین‌های‌مجازی در کنار یکدیگر و بر روی یک ماشین‌فیزیکی قرار گرفته باشند، با رسوخ مهاجم به هر کدام از این ماشین‌های‌مجازی، این امکان برایش محیا خواهد بود که به سایر ماشین‌های‌مجازی جانمایی شده بر روی همان ماشین‌فیزیکی نفوذ کند و یا ناظر ماشین‌مجازی را به کنترل خود در آورد. بنابراین، با افزایش تعداد و امتیاز CVSS آسیب‌پذیری‌هایی که در تمامی ماشین‌های‌مجازی موجود بر روی یک ماشین‌فیزیکی وجود دارد، باعث افزایش احتمال خطر حمله به ماشین‌های‌مجازی یا ناظر ماشین‌مجازی خواهد شد. لذا، توزیع منطقی این آسیب‌پذیری‌ها بر روی تمام ماشین‌های فیزیکی به صورتی که میانگین میزان تجمعی آسیب‌پذیری‌های آنها به صورت یکنواخت باشد باعث بهبود کلی امنیت در مرکز داده ابری خواهد شد.

در این سناریو ابتدا مشابه ارزیابی انجام شده در مطالعه [17]، شبیه‌سازی انجام شده است که وضعیت یک مرکز داده‌ای ابری را قبل از اعمال مدل پیشنهادی ما مدل می‌کند و در آن ۱۲۰ ماشین‌فیزیکی و ۲۵۳ ماشین‌مجازی در نظر گرفته شده است. تعداد ماشین‌های‌مجازی که بر روی یک ماشین‌فیزیکی جانمایی می‌شوند به صورت تصادفی در بازه‌ی [1,10] قرار دارد و هر ماشین مجازی دارای تعدادی آسیب‌پذیری است که تعداد آن به صورت تصادفی بین بازه [1,8] انتخاب می‌شود و به صورت تصادفی به هر آسیب‌پذیری یکی از انواع مخاطرات امنیتی که در جدول (۱) ارائه شده است منصوب می‌گردد. یک ماشین‌مجازی با توجه به خدماتی که فراهم می‌کند امکان دارد همزمان چندین آسیب‌پذیری از حملاتی که در جدول (۱) ارائه شده است داشته باشد. برای مثال، اگر ماشین‌مجازی همزمان خدمات وب و بانک‌اطلاعاتی را ارائه کند، این امکان وجود دارد که در هر دوی این خدمات، آسیب‌پذیری مربوط به حملات منع سرویس وجود داشته باشد که این دو آسیب‌پذیری را باید به صورت جداگانه و تفکیک شده مورد بررسی و سنجش قرار دهیم. به همین دلیل بازه [1,8] برای تعداد آسیب‌پذیری‌های یک ماشین مجازی انتخاب شده است. سپس، میانگین تجمعی آسیب‌پذیری‌های موجود بر روی یک ماشین‌فیزیکی محاسبه می‌شود. برای شبیه‌سازی مدل پیشنهادی، خصوصیت A_1 و A_3 با استفاده از داده‌های تولید شده برای شبیه‌سازی در مرحله قبل مورد استفاده قرار گرفته است. برای محاسبه و شبیه‌سازی خصوصیت A_2، با استفاده از کتابخانه *NetworkX* زبان برنامه‌نویسی پایتون، ۱۰ گراف به صورت تصادفی تولید شده است و هر گره این گراف یک ماشین مجازی و هر یال این گراف ارتباطات بین این ماشین‌های‌مجازی فرض شده است. برای محاسبه و شبیه‌سازی خصوصیت A_4، فقط دو بعد پردازشگر مرکزی و حافظه‌اصلی لحاظ شده است و اگر ظرفیت هر ماشین مجازی برای این دو بعد را با استفاده از درصد در نظر گرفته باشیم میزان u_i^d به صورت تصادفی عددی بین [1,10] درصد خواهد بود و w_i^d با فرض اینکه هر ماشین تنها دارای یک

سیستم‌عامل به همراه یک خدمت (مانند: بانک‌اطلاعاتی، وب و غیره) خواهد بود، عدد ثابت دو در نظر گرفته شده است. در نهایت فراهم‌کننده‌ی ابری، وزن‌دهی به خصوصیت‌ها را به صورت $\omega = \{0.3,0.35,0.2,0.15\}$ مشخص کرده است.

برای بررسی میزان تاثیر مدل ارائه شده در شبیه‌سازی در هر دوره بازه تعداد کل آسیب‌پذیری‌ها در هر ماشین مجازی تا بازه‌ی $[1,30]$ افزایش پیدا کرده است. نتایج حاصل از شبیه‌سازی یک مرکز داده ابری قبل و بعد از اعمال راه‌کار پیشنهادی ما در شکل (۲) نمایش داده است. بعد از اعمال راه‌کار پیشنهادی در بهترین حالت ۴۱.۱٪ و در بدترین حالت ۲.۰۷٪ بهبود در وضعیت توزیع آسیب‌پذیری در سطح ماشین‌های‌فیزیکی بدست آمد و میانگین این بهبود ۱۸.۷٪ بوده است.

۵-۲- سناریو۲: بررسی تاثیر اولویت خصوصیت‌ها بر وضعیت جانمایی ماشین‌های مجازی

یکی از مواردی که در بخش چهار این مطالعه مطرح شد، موضوع اولویت و وزنی است که یک فراهم‌کننده زیرساخت ابری با توجه به سیاست‌ها و ساختار مرکز داده ابری خود برای خصوصیت‌های A_1 تا A_4 می‌تواند قائل شود. بنابراین، در این قسمت برای بررسی میزان دقت این اولویت‌ها و بر اساس شبیه‌سازی صورت گرفته در قسمت قبلی، تحلیلی بر اساس خصوصیت A_2 یعنی سطح اهمیت یک ماشین‌مجازی صورت گرفته است و نتایج آن در شکل (۳) نمایش داده است.

همانطور که در شکل (۳) مشهود است با افزایش میزان وزن خصوصیت A_2 زمانبند عمومی سعی بر آن دارد که ماشین‌های‌مجازی پر اهمیت‌تر را کمتر در کنار هم و بر روی یک ماشین‌فیزیکی جانمایی کند. زمانی که در شبیه‌سازی مقدار خصوصیت A_2، ۰.۱، در نظر گرفته شده است، بر روی یک ماشین فیزیکی حدود ۱.۲ ماشین‌مجازی پراهمیت قرار دارد و وقتی این مقدار به ۰.۴ تغییر می‌کند این مقدار ۰.۴۵ تغییر پیدا می‌کند. خروجی‌های این سناریو نشان می‌دهد که تصمیم‌گیری به صورت منطقی اتخاذ می‌شود. یعنی زمانی که اولویت مربوط با ماشین‌های مجازی پر اهمیت افزایش پیدا می‌کند، این ماشین‌ها بر روی ماشین‌های فیزیکی قرار می‌گیرند که ماشین‌های پر اهمیت کمتری بر روی آنها قرار دارند.

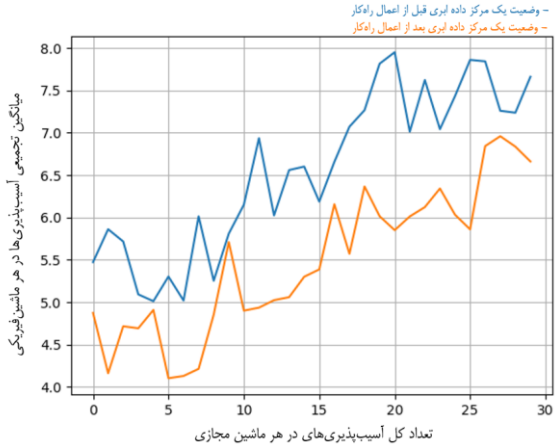
۵-۳- سناریو۳: مقایسه راه‌کار پیشنهادی با دو راه‌کار دیگر

در بخش دوم این پژوهش، مطالعاتی که تا کنون در این زمینه انجام شده است مورد بررسی قرار گرفت. از بین مطالعات صورت پذیرفته از لحاظ بافتار و نحوه‌ی نگرش به مساله مطالعه‌ی هان و همکاران [1] و مطالعه‌ی کویات و همکاران [8] بیشترین نزدیکی به راه‌کار پیشنهادی ما را دارد، لذا برای بررسی میزان کارایی این پژوهش در این قسمت به مقایسه بین راه‌کاری پیشنهادی ما و دو راه‌کار ذکر شده خواهیم پرداخت.

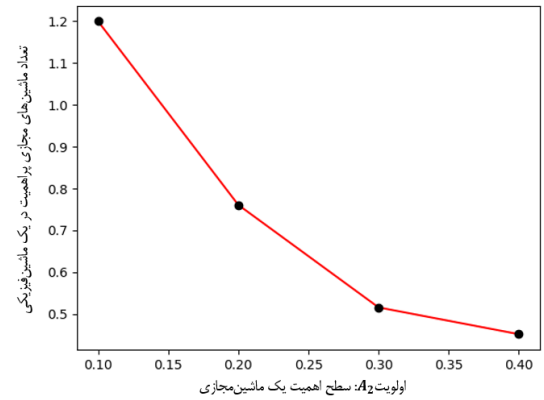
در این سناریو، شبیه سازی انجام شده است که مانند سناریو شماره یک فرض بر وجود ۱۲۰ ماشین فیزیکی است و تعداد ماشین‌های‌مجازی در ابتدا ۱۰۰ و در هر دور شبیه سازی به این تعداد ۱۰۰ عدد دیگر اضافه خواهد شد تا این عدد به ۸۰۰ برسد. در هر دور به هر برای هر سه راه‌کار درصد سطح ریسک تمامی ماشین‌های فیزیکی محاسبه می‌شود. سطح ریسک در اینجا به معنی میزان توزیع آسیب‌پذیری‌های بر روی تمامی ماشین‌های فیزیکی می‌باشد.

همانطور که در شکل (۴) نمایش داده شده است، محور عمودی نشان‌دهندهٔ درصد سطح ریسک را در ماشین های‌فیزیکی نمایش می‌دهد و محور افقی تعداد ماشین‌های مجازی در هر دوره را نمایش می‌دهند.

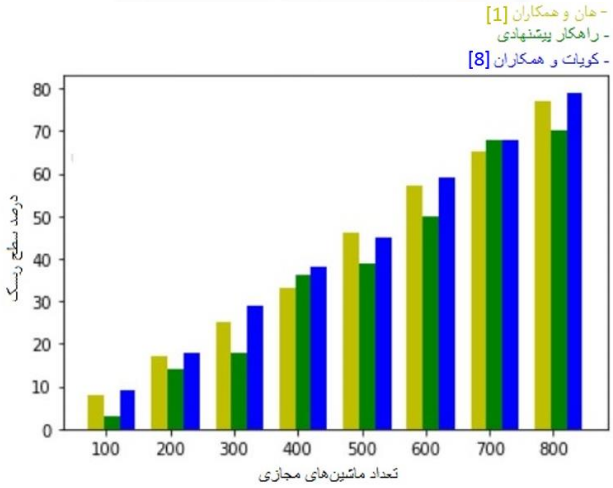
همانطور که در تصویر شماره چهار مشخص است راه‌کار بیشنهادی به جز زمانی که تعداد ماشین های مجازی ۴۰۰ است از راه‌کار بیشنهادی هان ضعیف‌تر عمل کرده و همچنان از راه‌کار کویات بهتر عمل کرده است و زمانی که تعداد ماشین های مجازی ۷۰۰ است راه‌کار بیشنهادی هم سطح با راه کار کویات بوده و از راه کار هان عملکرد کمتری دارد این در حالی است که در سایر حالات راه کار بیشنهادی درصد سطح ریسک به مراتب بهتری را نسبت به دو راه‌کار دیگر دارد. در این دو حالت نیز با بررسی دقیق‌تر خروجی شبیه‌سازی مشخص گردید که دلیل عملکرد ضعیف‌تر آن است که، برخلاف دو راه‌کار دیگر در راه‌کار پیشنهادی به صورت واقع‌بینانه ظرفیت یک



شکل (۲) : مقایسه وضعیت یک مرکز داده ابری قبل و بعد از اعمال راه‌کار پیشنهادی



شکل (۳) : مقایسه وضعیت جانمایی ماشین‌های مجازی با توجه به تغییر وزن خصوصیت A_2



شکل (٤) : مقایسه راه‌کار بیشنهادی و با کارهای مشابه

ماشین‌فیزیکی (فرمول (۱۹)) مورد بررسی قرار گرفته است. این در حالی است که دو راه‌کار دیگر این موضوع را مورد بررسی قرار نداده‌اند و در صورتی که این دو راه‌کار به صورت عملیاتی مورد استفاده قرارگیرند از این منظر با مشکل روبرو خواهند شد.

٦- نتیجه‌گیری

در این مطالعه راه‌کاری را پیشنهاد کردیم تا ماشین‌های‌مجازی را با رویکرد امنیتی و با استفاده از مجموعه فازی مردد جانمایی نماید. در این راه‌کار جانمایی ماشین‌های مجازی با در نظر گرفتن عدم قطعیت در چهار خصوصیت برای تصمیم‌گیری در خصوص این جانمایی نمایش داده شده است. همچنین، این امکان برای فراهم‌کننده ابر در نظر گرفته شده است تا اولویت‌های خود را در باره این خصوصیت‌ها بیان کند و سپس زمانبند عمومی با استفاده از این اولیت‌ها اقدام به تولید طرح جانمایی نماید. برای مثال، ممکن است برای یک فراهم‌کننده ابر، اهمیت یک ماشین‌مجازی اولیت اصلی بوده باشد و برای فراهم‌کننده دیگر میزان تجمیعی آسیب‌پذیری‌های موجود بر روی یک ماشین‌فیزیکی از درجه اهمیت بالایی برخوردار باشد.

همچنین، ما برای توسعه این مطالعه جهت بهبود و انعطاف در تصمیم‌گیری در نظر داریم تا موارد ذیل را در مطالعات آینده انجام دهیم:

۱. اضافه کردن خصوصیت‌های جدید و پویاکردن این خصوصیت، که باعث ایجاد انعطاف‌پذیری مدل برای استفاده در محیط‌های متنوع خواهد شد.
۲. استفاده از سایر مدل‌های توسعه داده شده برای مدل فازی مردد به منظور مقایسه، بررسی و پیدا کردن بهترین مدل جهت بهره‌برداری.

مراجع

[1] J. Han, W. Zang, S. Chen, M. Yu, "Reducing Security Risks of Clouds through Virtual Machine Placement," in *Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy (DBSec 2017)*, July-2017, Philadelphia, USA, pp.275-292.

[2] D. Zhao, J. Zhou and K. Li, "An Energy-Aware Algorithm for Virtual Machine Placement in Cloud Computing," *IEEE Access*, Vol. 7, pp. 55659-55668, 2019.

[3] J. Luo, W. Song and L. Yin, "Reliable Virtual Machine Placement Based on Multi-Objective Optimization with Traffic-Aware Algorithm in Industrial Cloud", *IEEE Access*, Vol. 6, pp. 23043-23052, 2018.

[4] W. Stallings, Cryptography and network security. Boston, Mass: Pearson, 2017.

[5] A. Agarwal, T, Duong, "Secure virtual machine placement in cloud data centers," *Future Generation Computer Systems*, Vol. 100, pp. 210-222, 2019.

[6] C. Yang, Y. Guo, H. Hu, W. Liu and Y. Wang, "An effective and scalable VM migration strategy to mitigate cross-VM side-channel attacks in cloud," *China Communications*, Vol. 16, No. 4, pp. 151-171, 2019.

[7] F. Ahamed, S. Shahrestani, B. Javadi, "Security Aware and Energy-Efficient Virtual Machine Consolidation in Cloud Computing Systems," in *Proceedings of the IEEE Trustcom/BigDataSE/ ISPA Conference*, August-2016, Tianjin, China, pp. 1516-1523.

[8] L. Kwiat, C. Kamhoua, K. Kwiat, J. Tang, A. Martin, "Security-Aware Virtual Machine Allocation in the Cloud: A Game Theoretic Approach," in *Proceedings of the IEEE 8th International Conference on Cloud Computing*, June-2015, New York, USA, pp. 556-563.

[9] "FIRST – Forum of Incident Response and Security Teams. CVSS Specification Document", URL : https://www.first.org/cvss/v3.1/specification-document, Access Date : 3 Octobre 2019.

[10] L. Zadeh, "Probability measures of fuzzy events," *Journal of Mathematical Analysis and Applications*, Vol. 23, No. 2, pp. 421-427, 1968.

[11] V. Torra, "Hesitant fuzzy sets," *Journal of Intelligent Systems*, Vol. 25, No.6, pp. 529-539, 2010.

[12] H. Laio, Z. Xu, "Hesitant Fuzzy Decision Making Methodologies and Applications," Springer, December 27, 2017.

[13] M. Xia, Z. Xu, "Hesitant fuzzy information aggregation in decision making, " *International Journal of Approximate Reasoning*, Vol. 52, pp. 395-407, 2011.

[14] L. Metcalf, W. Casey, "Cybersecurity and Applied Mathematics," *Elsevier Publishing*, June 7, 2016.

[15] N. Hieu, M. Francesco, A. Yl, "A virtual machine placement algorithm for balanced resource utilization in cloud data centers," in *Proceedings of the IEEE 7th International Conference on Cloud Computing*, June-2014, Anchorage, AK, USA, pp. 474-481.

[16] J. Lan, R. Jin, Z. Zheng, M. Hu, "Priority degrees for hesitant fuzzy sets: Application to multiple attribute decision making," *Journal of Operations Research Perspectives*, Vol. 4, pp. 67-73, 2017.

[17] X. Yuchi, S, Shetty, "Enabling security-aware virtual machine placement in IaaS clouds," in *Proceedings of the IEEE Military Communications Conference*, October-2015, Tampa, FL, USA, pp. 1554-1559.

زیرنویس‌ها

[1] Cloud provider

[2] Service level agreement
[3] previously co-located user's first
[4] Side-channel attack
[5] Integer linear programming
[6] Virtual machine escape
[7] US National Vulnerability Database (NVD)
[8] Common Vulnerability Scoring System (CVSS)
[9] Metric
[10] Base
[11] Temporal
[12] Environnemental
[13] Exploitability
[14] Impact
[15] Hesitant fuzzy set
[16] Convex fuzzy subsets
[17] Hesitant fuzzy element
[18] General scheduler
[19] Attribute
[20] Scan
[21] Attribute weight
[22] Availability
[23] Malicious code
[24] Degree centrality
[25] Betweenness centrality
[26] Resource utilization ratio (RU)
[27] Resource balance ration (RB)
[28] Load
[29] Score function