مجله محاسبات نرم، جلد ۱۰، شماره ۱ (بهار و تابستان ۱۴۰۰)، صفحه ۲ـ۱۵
https://dx.doi.org/10.22052/scj.2021.242842.0

مجله محاسبات نرم
SOFT COMPUTING JOURNAL
تارنمای مجله: scj.kashanu.ac.ir

دانشگاه کاشان
University of Kashan

مدل‌سازی امنیت ماشین‌های مجازی در ابر با استفاده از تئوری بازی تکرار شونده✧

امیرحسین یداللهی[۱]، دانشجوی کارشناسی ارشد، جواد سلیمی سرتختی[۱]، استادیار، سلمان گلی بیدگلی[۱*]، استادیار
[۱] گروه مهندسی کامپیوتر، دانشکده برق و کامپیوتر، دانشگاه کاشان، کاشان، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت ۰۱ خرداد ماه ۱۴۰۰
پذیرش ۲۰ آذر ماه ۱۴۰۰

کلمات کلیدی:
رایانش ابری
امنیت
نظریه بازی
تعادل نش
بازی تکرارشونده

چکیده

امروزه مزایای زیاد رایانش ابری باعث شده بسیاری از نهادهای کوچک و بزرگ، از خدمات ابری برای کاهش هزینه‌های خود استفاده کنند. در این میان برخی از موانع بازدارنده برای استفاده از سرویس‌های ابری وجود دارد که یکی از بزرگ‌ترین آن‌ها حملات امنیتی متاثر از فوق‌ناظر است. هنگامی که یک حمله مستقیم به یک کاربر روی یک فوق‌ناظر انجام می‌شود، ممکن است به طور غیرمستقیم ماشین مجازی سایر کاربران را نیز مورد حمله قرار دهد. در این بین، اهداف و منافع متضاد کاربران سرویس‌های ابری و مهاجمین، تصمیم‌گیری فراهم‌کنندگان سرویس‌های ابری در خصوص سرمایه‌گذاری روی ماژول‌های امنیتی سرورهای ابری را دشوار می‌سازد. لذا در این مقاله، با استفاده از تئوری بازی راه‌حل مناسبی برای تصمیم‌گیری در خصوص سرمایه‌گذاری روی یکی از ماژول‌های امنیتی برای هر یک از بازیگران ارائه می‌شود. همچنین با استفاده از مدل بازی تکرار شونده، کلیه تعادل‌های نش نیز استخراج و تحلیل شده است. نتایج نشان می‌دهد که تئوری بازی می‌تواند به خوبی در اتخاذ تصمیم مناسب و یافتن تعادل مناسب برای تصمیم‌گیری در مورد سرمایه‌گذاری در حوزه امنیت کاربردی باشد. بر اساس نتایج شبیه‌سازی، می‌توان گفت که در بازی‌های تکرار شونده با احتمال تکرار بازی بین ۰/۲ تا ۰/۸، استراتژی‌های از پیش تعیین شده سرمایه‌گذاری یا عدم سرمایه‌گذاری می‌تواند منجر به یک تعادل نش مناسب شده و حداکثر منافع برای کاربران سرویس‌های ابری را در پی داشته باشد.

© ۱۴۰۰ ـ مجلهٔ محاسبات نرم، کلیه حقوق محفوظ است.

۱. مقدمه

رایانش ابری در واقع ارائه خدمات رایانه‌ای از جمله محاسبات، ذخیره‌سازی، اجرای نرم‌افزار، تجزیه و تحلیل داده‌ها و موارد مشابه از طریق اینترنت است. با رایانش ابری محیط‌های نرم‌افزاری و خدماتی بر مبنای منابع اشتراکی ارائه می‌شوند. کاربران به جای این‌که یک مجوز نرم‌افزاری مشخص را خریداری کنند، ماهانه هزینه‌ای را به عنوان حق سرویس می‌پردازند. نرم‌افزارها و پلتفرم‌ها توسط ارائه‌دهندگان سرویس مدیریت می‌شوند و به صورت مداوم به‌روزرسانی می‌شوند تا عملکرد و امنیت آن‌ها بیشینه شود [۱]. رایانش ابری به سرعت در حال تبدیل شدن به یک منبع استاندارد در زمینه فناوری اطلاعات است [۲]. با توجه به چنین رشد حیرت انگیزی، در نظر گرفتن چالش‌های امنیتی بسیار مهم و هزینه‌بر بوده و نیازمند تصمیم‌گیری در مورد

✧ نوع مقاله: پژوهشی
* نویسنده مسئول
پست(های) الکترونیک: amirhosein972012@yahoo.com (یداللهی)
salimi@kashanu.ac.ir (سلیمی سرتختی)
salmangoli@kashanu.ac.ir (گلی بیدگلی)

نحوه ارجاع به مقاله: یداللهی، امیرحسین، سلیمی سرتختی، جواد، گلی بیدگلی، سلمان، «مدل‌سازی امنیت ماشین‌های مجازی در ابر با استفاده از تئوری بازی تکرار شونده»، مجله محاسبات نرم، جلد ۱۰، شماره ۱، ص۲ـ۱۵، بهار و تابستان ۱۴۰۰.

وسعت پیاده سازی و سرمایه‌گذاری است. این مساله در شرایطی است که ملاحظات امنیتی، اغلب به دلیل عملکرد و قابلیت اطمینان نسبی سرویس‌های ابری، توسط مشتریان نادیده گرفته می‌شود [۳]. از طرفی کمی‌سازی و ارزیابی امنیت دشوار بوده و نسبت به سایر اقدامات کاهش هزینه، مزایای آشکار کمتری را به همراه دارد. شرکت‌های حساس امنیتی از سرقت احتمالی اطلاعات محرمانه یا اطلاعات حساس دیگر، هراس فراوان دارند و این ترس "مانع قابل توجهی در برابر پذیرش سرویس‌های ابری" توسط آن‌ها است.

این استدلال که مکانیزم‌های امنیتی کنونی در رایانش ابری ناکافی است، مسئله قابل توجهی است. بسیاری از ارائه-دهندگان سرویس‌های ابری از میزان آسیب پذیری‌های امنیتی خود اطلاع ندارند. بسیاری از کاربران، به جای استفاده از ماشین‌های مجازی از همان سخت افزار فیزیکی استفاده می-کنند و این موضوع می‌تواند به یک مهاجم اجازه دهد حمله خود را به فوق‌ناظر[1] و روی تمام ماشین‌های مجازی که روی آن فوق‌ناظر اجرا می‌شوند گسترش دهد. در این شرایط، هنگامی که یک حمله مستقیم به یک ماشین بر روی یک فوق-ناظر انجام می‌شود، ممکن است به طور غیر مستقیم به ماشین مجازی کاربر دیگر نیز سرایت کند. این پدیده در شبکه‌های سنتی معمولی وجود ندارد، بلکه در آن یک مهاجم باید از یک روش چند_تک مرحله‌ای[2] برای حمله غیرمستقیم به چندکاربر استفاده کند. بنابراین، وابستگی امنیتی متقابل بین کاربران یک فوق‌ناظر، ارائه دهندگان سرویس‌های ابری را با یک چالش جدی مواجه کرده است [۴].

مجازی‌سازی در محاسبات ابری به دو صورت کامل و ناقص شکل می‌گیرد. در مجازی‌سازی کامل از یک نوع نرم افزار خاص با نام فوق‌ناظر استفاده می‌شود. فوق‌ناظر به طور مستقیم با فضای دیسک و CPU سرور فیزیکی ارتباط دارد. این نرم-افزار مانند یک سکو برای سیستم عامل سرور مجازی عمل می‌کند. فوق‌ناظر، هر سرور مجازی را به طور کامل مستقل و جدا از سرورهای مجازی دیگری که بر روی همان ماشین فیزیکی اجرا می‌شوند، نگهداری می‌کند. برخلاف تکنیک مجازی‌سازی کامل، سرورهای مهمان در یک مجازی‌سازی ناقص از وجود یکدیگر اطلاع دارند. یک نرم افزار فوق‌ناظر در ساختار مجازی‌سازی ناقص به قدرت پردازش زیادی برای مدیریت سیستم‌های عامل مجازی احتیاج ندارد، زیرا هر سیستم عامل از مطالبات سایر سیستم‌های عامل از سرور فیزیکی آگاه است. کل این سیستم با یکدیگر به صورت یک واحد به هم پیوسته کار می‌کنند. در این تحقیق بررسی و مدلسازی امنیت ماشین‌های مجازی در حالت مجازی‌سازی کامل مورد بررسی قرار خواهد گرفت. برقراری سطح خاصی از امنیت در سرویس‌های ابری، نیاز به تصمیم‌گیری و سرمایه-گذاری بهینه دارد. روش‌های مختلفی برای برقراری امنیت وجود دارد که از جمله آن‌ها می‌توان به استفاده از سیستم شناسایی ورود غیر مجاز[3]، سیستم جلوگیری از نفوذ[4] و دیواره آتش[5] اشاره کرد. البته باید به این نکته توجه شود که برقراری امنیت توسط هر یک از این روش‌ها نیازمند صرف هزینه و یا به عبارتی سرمایه‌گذاری در حوزه خرید، نصب، راه اندازی و نگهداری ماژول‌های سخت‌افزاری و نرم‌افزاری آن‌ها است. در این تحقیق با مدلسازی رفتار کاربران و مهاجمین یک فوق‌ناظر و تحلیل استراتژی و سود دهی هر کدام، استراتژی مناسب سرمایه‌گذاری یا عدم سرمایه‌گذاری روی ماژول‌های امنیتی یک ماشین مجازی مورد بررسی قرار گرفته است.

از میان روش‌های موجود برای مدل‌سازی سیاست‌های سرمایه‌گذاری امنیتی در رایانش ابری، مدل‌سازی و تحلیل این سیستم با نظریه بازی با در نظر گرفتن چندین بازیکن هوشمند همواره مورد توجه بوده است [۵]. نحوه تخصیص ماشین‌های مجازی به کاربران توسط ارائه دهندگان سرویس‌های ابری تاثیر مستقیمی روی امنیت خود کاربر و سایر کاربرن یک فوق‌ناظر دارد. هدف ما در این نوشتار استفاده از دانش به دست آمده از این مدل‌سازی برای کمک به تصمیم‌سازی ارائه-

[1] Hypervisor
[2] Multi-single stage
[3] Intrusion Detection System (IDS)
[4] Intrusion prevention System (IPS)
[5] Firewall

دهندگان رایانش ابری در خصوص هزینه کرد روی ماژول‌های امنیتی ماشین مجازی است.

عمده مطالعات صورت گرفته در زمینه تامین امنیت سرویس-های ابری متکی بر رویکردهای سخت افزاری است که گران هستند. در برخی از مطالعات این حوزه [۶]، مدل‌های پیشنهادی هوشمندانه، مناسب‌ترین ماژول را از بین همه ماژول‌های ممکن برای تشخیص حمله انتخاب می‌کند. انتخاب یک ماژول تشخیص خاص به جای استفاده از همه به صورت موازی، نه تنها منجر به کاهش مصرف انرژی می‌شود، بلکه کارایی کلی سیستم مدافع را نیز افزایش می‌دهد. در دسته دیگری از روش‌ها [۷]، بر اساس مقادیر تعادل نش بدست آمده در نظریه بازی، حمله را از درخواست‌های عادی متمایز کرده و شدت حمله و مبدأ آن را تعیین می‌کنند و این نتایج می‌تواند در انتخاب ماژول مناسب برای ایجاد امنیت کمک کننده باشند.

در این مطالعه، با فرض وجود مجازی‌سازی کامل، با استفاده از تئوری بازی راه حل مناسبی برای تصمیم‌گیری در مورد سرمایه‌گذاری روی ماژول‌های امنیتی ارائه می‌شود. لذا از جمله تفاوت‌های اصلی این تحقیق نسبت به سایر مطالعات می‌توان به موارد زیر اشاره کرد:

۱. استفاده از مدل بازی تکرار شونده جهت تحلیل.
۲. استخراج کلیه تعادل‌های نش در زمینه سرمایه‌گذاری یا عدم سرمایه‌گذاری در ماژول‌های امنیتی در شرایط مختلف.
۳. اتخاذ تصمیم مناسب برای سرمایه‌گذاری در امنیت.

بنابراین در بخش ۲ مروری بر کارهای مرتبط بیان شده و در بخش۳ این مقاله مدل سیستم در رایانش ابری و شرح جزئیات معماری ابری که در مدل بازی استفاده می‌شود ارائه می‌شود. در بخش ۴ مدل بازی، تجزیه و تحلیل و نتیجه بازی برای ساده‌ترین حالت و در نهایت در بخش ۵ به نتیجه‌گیری و بررسی تاثیر بازی تکرارشونده در بحث ماشین‌های مجازی پرداخته شده است.

۲. مروری بر کارهای مرتبط

رایانش ابری شامل مجموعه متنوعی از فن‌آوری‌ها از جمله شبکه‌سازی و مجازی‌سازی است. بنابراین، نسبت به طیف وسیعی از تهدیدهای امنیتی آسیب‌پذیر است. برخی از مهم‌ترین مسائل امنیتی که سیستم‌های رایانش ابری را تهدید می‌کنند ناشی از تکنیک‌های مجازی‌سازی هستند. لذا برای برقراری این امنیت در رایانش ابری می‌بایست در خصوص نحوه و تعداد ماژول‌های امنیتی تصمیم‌گیری و سرمایه‌گذاری کرد تا ایمنی سیستم در برابر حملات احتمالی تامین شود.

لذا یک مسئله مهم در رایانش ابری چگونگی ایجاد و ارتباط نمونه‌های ماشین‌مجازی با ماژول‌های امنیتی بالقوه (دیواره آتش، سیستم‌های تشخیص نفوذ، آنتی ویروس) است. در مطالعات پیشین، روش‌های زیادی برای حل مساله بررسی امنیت در رایانش ابری، بررسی شده است. بسیاری از راه‌حل‌های ارائه شده مربوط به تخصیص ماشین‌های مجازی بر اساس تکنیک‌های تعادل بار، مصرف انرژی و یا هر دو بوده است [۸ و ۹]. نظریه بازی تاکنون در برخی جنبه‌های خاص رایانش ابری، از جمله انعطاف‌پذیری در قیمت‌گذاری سرویس‌های رایانش ابری [۱۰] و تخصیص ماشین‌مجازی و تشخیص حملات استفاده شده است [۱۱-۱۶].

جلاپارتی و همکاران [۱۷]، سعی در حل مسئله تخصیص منابع رایانش ابری با نظریه بازی داشته و در تحقیقی مشابه، وی[1] و همکاران از تئوری بازی برای تخصیص منابع ابری به دستگاه‌های با ظرفیت محدود اینترنت اشیاء استفاده کردند [۱۸]. بنابراین، آن‌ها به طور همزمان مشکل ارائه دهنده ابری را با بهینه‌سازی تخصیص منابع رایانش ابری حل کردند و به ارائه دهنده خدمات اجازه دادند ضمن ایجاد امنیت در ماشین مجازی قیمت‌های تقریباً بهینه برای استفاده از ابر را بپردازد.

با تخصیص منابع و راه‌اندازی یک ماشین مجازی در هر سرور، یک مهاجم می‌تواند اطلاعات حساس را از جمله ترافیک وب و حتی کلیدهای رمزگذاری را مورد حمله قرار دهد. بدین

[1] Wei

منظور هان و همکارانش از تئوری بازی برای یافتن بهترین روش برای کاهش چنین حملاتی استفاده کرده‌اند [۱۹].

در مطالعه Halabi و همکاران در سال ۲۰۱۸، حالت خاصی از ابرهای فدرال با استفاده از یک نظریه بازی بر اساس سطح امنیت و شهرت ارائه‌دهندگان خدمات، مدل شده است. این مدل، ارائه‌دهندگان خدمات را تشویق به سرمایه‌گذاری برای پیوستن به ابرهای فدرال کرده در حالی که امنیت آن‌ها تضمین می‌شود. نتایج نشان می‌دهد که مدل توسعه داده شده باعث حفظ سطح بالاتر امنیت در شبکه می‌شود [۲۰].

در مطالعه‌ای توسط Agarwal و همکاران در سال ۲۰۱۹، الگوریتمی برای جایابی امن ماشین مجازی توسعه داده شده که در آن یک ارائه دهنده ابر می‌تواند از مکانیزم‌های جایابی برای برقراری امنیت هوشمند آن استفاده کند. نتایج شبیه‌سازی، نشان می‌دهد که الگوریتم پیشنهادی با استفاده از نظریه بازی در مقایسه با رویکردهای موجود، افزایش قابل توجهی در امنیت سرویس‌های ابری را فراهم کرده است [۲۱].

در مطالعه‌ای توسط Liang و همکاران در سال ۲۰۱۹، به طور گسترده روش‌های نظریه بازی در شبکه‌های انسان و ماشین[1] مورد بررسی قرار گرفته و برای بررسی و تجزیه و تحلیل هر سیستم، اهداف برنامه، بازیکنان، استراتژی‌ها، مدل‌های بازی و تعادل نش بر اساس نیازهای پیشنهادی تعیین شده است [۲۲].

Ousmane و همکاران در سال ۲۰۱۹، یک روش جدید برای به حداقل رساندن حمله مهاجم به ماشین مجازی را پیشنهاد می‌کنند. در این روش سیاست‌های مختلف تخصیص ماشین مجازی با استفاده از یک رویکرد نظریه بازی برای تجزیه و تحلیل کمی مدل استفاده شده است. نتایج نشان می‌دهد که به منظور به حداقل رساندن بهره‌وری مهاجم، ارائه دهنده ابر باید از سیاست تخصیص احتمالی ماشین مجازی استفاده کند [۲۳].

اختصاص چندین ماشین مجازی بر روی یک سرور به افزایش استفاده از منابع رایانش ابری و کاهش هزینه عملکرد آن کمک می‌کند. با این حال، ماشین‌های مجازی با سطوح مختلف امنیتی در یک سرور باعث ایجاد خطرات عمده وابسته به امنیت سایبری ماشین مجازی-به- ماشین مجازی می‌شوند که Homsi و همکاران در سال ۲۰۱۹، با مدل‌سازی آن به عنوان یک بازی به مشکل تخصیص استاتیک ماشین مجازی با آگاهی از دست دادن امنیت می‌پردازد [۲۴]. Prabhakar و همکاران در سال ۲۰۱۹، در تحقیقی، سعی داشتند مجموعه‌ای از استراتژی‌ها را پیشنهاد کنند تا قوانینی را برای امنیت بر اساس نظریه بازی تنظیم کنند تا فوق‌ناظر را از تهدیدات احتمالی مصون کند [۲۵].

Wang و همکاران در سال ۲۰۲۰ الگوریتمی ارائه داده‌اند که در آن حملات مبتنی بر آسیب پذیری‌های مختلف سیستم عامل به عنوان استراتژی‌های مختلف "حمله" در نظر گرفته شده و توزیع‌های مختلف سیستم عامل در یک شبکه ماشین مجازی، به عنوان استراتژی‌های مختلف "دفاعی" در نظر گرفته می‌شوند. نتایج نشان می‌دهد که در مقایسه با الگوریتم‌های دیگر، الگوریتم پیشنهادی توزیع سیستم‌های عامل می‌تواند تمایل مهاجم در انتخاب استراتژی حمله را در حدود ۲۳/۱۵ درصد کاهش دهد [۲۶].

وقتی امنیت در مساله تخصیص منابع در نظر گرفته شود به دلیل نیاز به محافظت از سایر ماشین‌های مجازی، این طرح حتی بیش‌تر چالش برانگیز می‌شود. در مطالعه‌ای توسط Carvalho و همکاران در سال ۲۰۲۰، مکانیزم بهینه امنیت مبتنی بر چارچوب فرآیند تصمیم‌گیری نیمه مارکوف[2] مدل شده که به صورت بهینه و پویا، شرایط ماشین‌های مجازی را بر اساس نوع خدمات و ویژگی‌های تصادفی آن‌ها، هزینه خدمات امنیتی، هزینه مسدود کردن و هزینه مکان تعیین می‌کند [۲۷]. در مطالعه‌ای توسط Kandoussi و همکاران در سال ۲۰۲۰، یک سیستم دفاعی یکپارچه با ترکیب ماشین‌های مجازی در رایانش ابری پیشنهاد شده و اثربخشی سیستم پیشنهادی از نظر سیاست‌های امنیتی مورد بحث قرار گرفته است. علاوه بر این، در مدل پیشنهادی مسیرهای حمله بالقوه به صورت کمی تعیین شده تا برای مدل‌سازی تعامل مهاجم-مدافع، از تئوری بازی تصادفی استفاده شود. سیستم دفاعی

[1] Human–Machine Networks

[2] Semi-Markov decision process (SMDP)

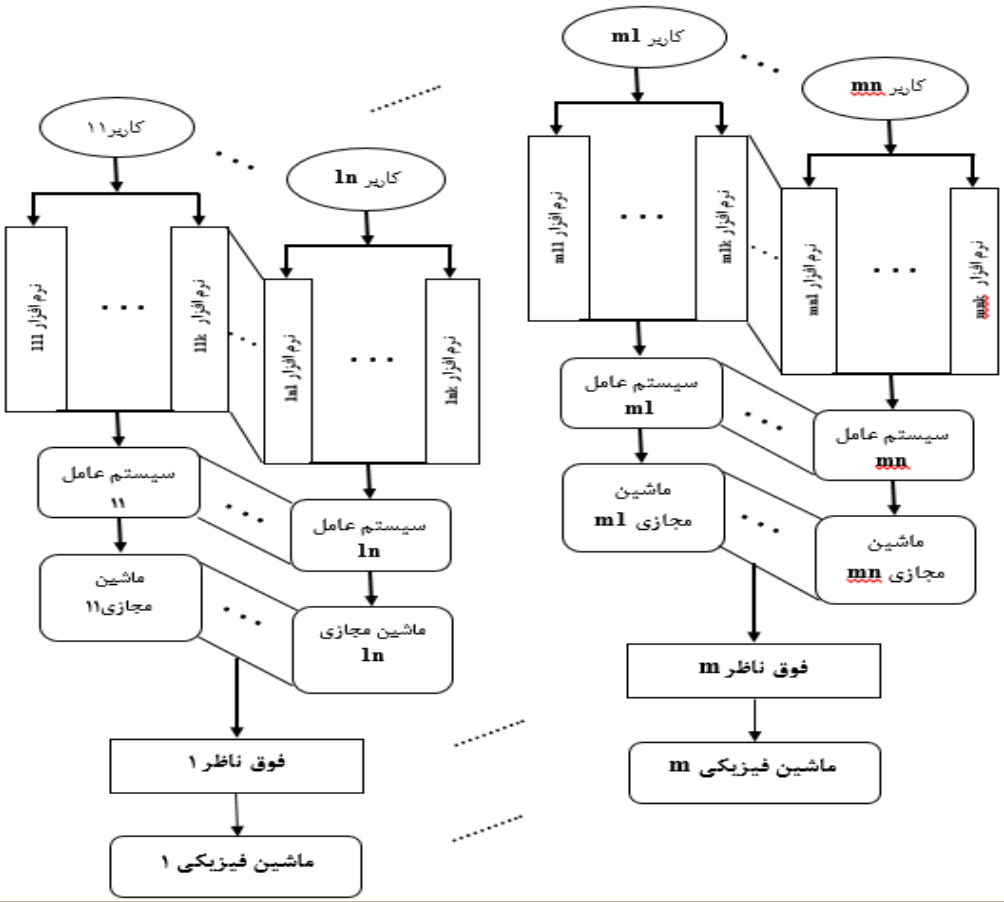
پویا پیشنهاد شده به شبکه کمک می‌کند تا بداند اقدامات امنیتی جدید در کدام مکان از شبکه باید بـه کـار گرفتـه شـود [۲۸]. جدول (۱) خلاصه‌ای از مطالعات مرتبط اخیر را نشان می‌دهد.

جدول (۱): مقایسه مهم‌ترین روش‌های تحلیلی نظریه بازی در حوزه امنیت رایانش ابری

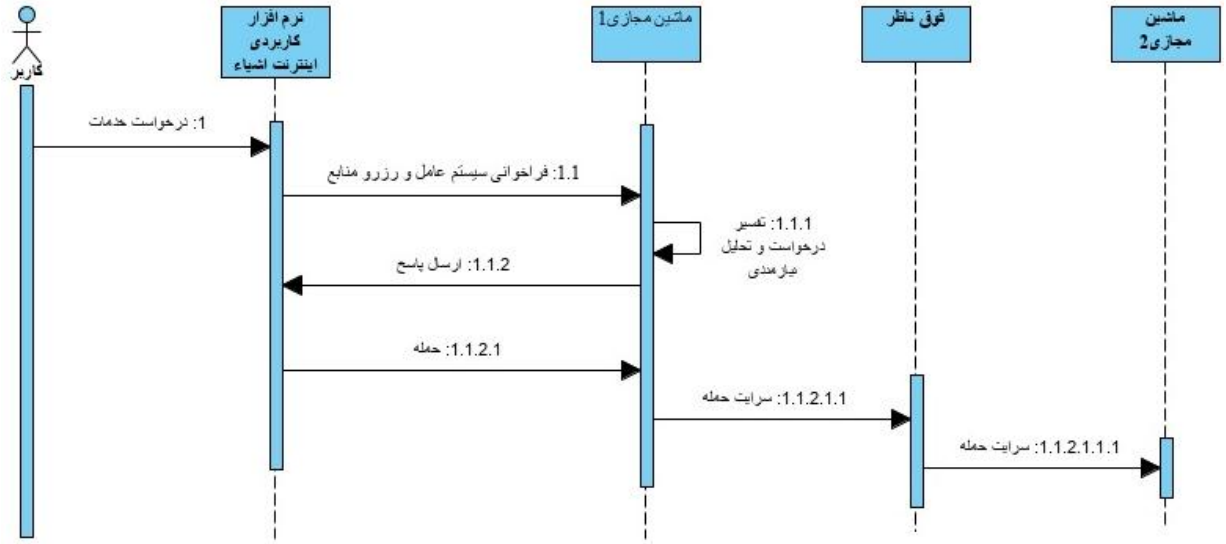
سال	مرجع	هدف	رویکرد	معیارهای کارایی	مزایا	معایب
۲۰۱۷	[۶]	مشخص کردن شدت و مبدا حمله	بازی غیرمشارکتی	سرعت و کارآیی تشخیص حملات	کاهش مصرف انرژی و افزایش کارایی سیستم	احتمال خطای ۱۵ درصدی در تشخیص حمله
۲۰۱۹	[۲۱]	ایمن‌سازی ماشین مجازی در مراکز داده ابری	الگوریتم Previously Co Located Users First	اعمال خودکار امنیت در برابر حملات	کاهش احتمال هم مکان شدن حمله‌ها به ماشین‌های مجازی	معیارهای محدود برای ارزیابی و اندازه‌گیری امنیت در محل استقرار ابرها
۲۰۱۹	[۲۳]	به حداقل رساندن حمله به ماشین‌های مجازی	نظریه بازی	تعدلد حمله، هزینه، مصرف انرژی	نیاز به هیچ گونه تغییری در زیرساخت اصلی ندارد	عدم بررسی سیاست‌های مختلف تخصیص VM
۲۰۱۹	[۲۴]	تخصیص ماشین مجازی ایستا با آگاهی از دست دادن امنیت سایبری	نظریه بازی two-player zero-sum	امنیت سایبری	عملکرد بهتر نسبت به روش‌های پر کاربرد مانند VBP	عدم بررسی استراتژی-های تخصیص پویا
۲۰۱۹	[۲۵]	ایجاد امنیت در برابر تهدیدات احتمالی به فوق ناظر	نظریه بازی tower defence	برقراری امنیت در برابر نفوذها و حملات	شناسایی حملات احتمالی و طراحی قوانین امنیتی مناسب	نیاز به هوشنمدی کامل سیستم در مورد اطلاعات شبکه و استراتژی مهاجم
۲۰۲۰	[۷]	انتخاب یک ماژول مناسب برای تشخیص حمله	تئوری بازی GTM-CSec	انتخاب ماژول با بهترین تعادل نش	کاهش مصرف انرژی و افزایش کارایی سیستم مدافع	انتخاب ماژول از بین تعداد محدودی ماژول موردنظر
۲۰۲۰	[۲۸]	افزایش امنیت در محیط محاسبات ابری با ترکیب استراتژی بهینه برای مهاجرت VM و استقرار honeypot	نظریه بازی تصادفی	افزایش امنیت سیستم با انتخاب اقدام امنیتی مناسب	ایجاد سیستم پویای یکپارچه برای تشخیص حملات استراتژیک در شبکه‌های ابری	استفاده از یک بازی تصادفی استاتیک و عدم توانایی در کاهش تعداد مهاجرت‌های ناکارآمد
۲۰۲۱	[۲۶]	ایجاد امنیت یک سیستم عامل با وجود ماشین مجازی	مدل بازی attack-defensE (CLOSURE)	کاهش انگیزه مهاجم برای حمله به یک سیستم عامل	به طور پویا استراتژی-های دفاعی در انتخاب ماشین مجازی تغییر می‌کند.	در نظر گرفتن تنها یک مهاجم و عدم کارایی مدل در افزایش تعداد مهاجمان
۲۰۲۱	[۲۰]	ارئه یک مدل تشکیل فدراسیون ابر که سطح امنیت CSP ها را در نظر می‌گیرد.	روش Goal-Question-Metric (GQM)	سطح امنیت در قبال شهرت CSP ها	افزایش دقت مدل با توجه به رضایت امنیتی مشتریان ابر و شهرت CSP ها در طول فرایند ارزیابی	عدم ایجاد یک Security-SLA کارآمد و قابل اندازه‌گیری و عدم تاثیر هزینه

۳. مدل سیستم

برای مدل‌سازی سیستم فرض می‌شود در یک زیرساخت رایانش ابری عمومی، یک فوق‌ناظر با نام H1 در حال اجرا بوده و n کاربر وجود دارد که با علامت U11، U12 تا U1n مشخص می‌شوند. در این سیستم هر یک از آن‌ها یک ماشین مجازی را اجرا می‌کنند که با VM12،VM11 تا VM1n مشخص می‌شوند. در شکل (۱) این مدل نشان داده شده است. در این سیستم، کاربر، ماشین‌های مجازی را که به عنوان یک رابط در سیستم قرار دارند، مدیریت می‌کند. همچنین فرض می‌شود که کاربر ابری با حسن نیت عمل خواهد کرد (یعنی کاری را انجام می‌دهد که بیش‌ترین امنیت را برای کاربر هدف داشته باشد). بنابراین، در این مقاله فقط کاربر هدف مورد بررسی قرار داده می‌شود. یک سیستم عامل منفرد ممکن است چندین برنامه را اجرا کند که از آن‌ها با عنوان Application111 تا Applicationmnk یاد می‌شود. هر برنامه برای نشان دادن به سه شاخص نیاز دارد. شاخص سوم برنامه‌های اجرا شده توسط سیستم عامل را از یکدیگر متمایز می‌کند. شاخص دوم نمایانگر سیستم عامل یا ماشین مجازی بوده و شاخص اول فوق‌ناظر را نشان می‌دهد که برنامه در آن قرار دارد. هر کاربر ممکن است چندین نمونه ماشین مجازی (و چندین سیستم عامل) را اجرا کند، اما بدون از دست دادن کلیت مساله و برای ساده سازی فرض می‌شود که هر کاربر یک ماشین مجازی را اجرا می‌کند. بنابراین، طراحی شکل (۱) در واقع یک ساده‌سازی دقیق و یک ساختار مشترک برای یک رایانش ابری عمومی بوده که دیاگرام توالی آن برای یک حالت خاص با درنظر گرفتن یک کاربر و یک نرم‌افزار در شکل (۲) نشان داده شده است.



شکل (۱): مدل سیستم



شکل (۲): دیاگرام توالی یک مدل ساده شده سیستم با یک کاربر و یک نرم‌افزار

۴. مدل بازی

مدل بازی پیشنهادی در اینجا شبیه مدل ارائه شده در [۱] است. در این مدل چهار بازیکن وجود دارد که شامل یک مهاجم و سه کاربر می‌باشد. این چهار بازیکن از طریق دو فوق‌ناظر در حال بازی هستند. شرایط بازی به گونه‌ای است که هر بازیکن می‌تواند در هر انتخاب، سود خود را حساب کرده و بهترین موقعیت را برای خود انتخاب کند. در طی این انتخاب‌های پی در پی سرانجام هر بازیکن به تعادلی می‌رسد که در آن حالت بیش‌ترین سود خود را کسب کرده است.

در این بازی، مهاجم سه استراتژی برای حمله دارد. استراتژی اول حمله به کاربر۱ (A1)، استراتژی دوم حمله به کاربر۲ (A2) و استراتژی سوم حمله به کاربر۳ (A3) است. یکی از قوانین بازی این است که مهاجم در یک لحظه فقط به یک کاربر می‌تواند حمله کند. انتخاب‌های ممکن برای هر کاربر سرمایه‌گذاری یا عدم سرمایه‌گذاری (استفاده از یکی از ماژول‌های امنیتی پیش‌فرض با پرداخت هزینه آن) روی امنیت می‌باشد. برای سهولت در بررسی روابط و نتایج ارائه شده در این بخش، نمادها و پارامترهای مورد استفاده در این تحقیق در جدول (۲) ارئه شده است.

جدول (۲): معرفی پارامترهای مورد استفاده در این تحقیق

نماد	توضیحات
A_i	استراتژی iام (حمله به کاربر iام)
$I(H_2)$	سرمایه‌گذاری روی امنیت
$N(H_1)$	عدم سرمایه‌گذاری روی امنیت
L_i	هزینه کاربر iام در اتخاذ تصمیم موردنظر
q_I	احتمال موفقیت یک حمله روی کاربری که در امنیت سرمایه‌گذاری کرده
q_N	احتمال موفقیت یک حمله روی کاربری که در امنیت سرمایه‌گذاری نکرده
π	احتمال حمله موفق روی یک فوق ناظر
e	هزینه سرمایه‌گذاری روی امنیت
R	سود کلی یک سرویس ابر
(A_i, N)	حمله به کاربر i (استراتژی A_i) و عدم سرمایه گذاری کاربر موردنظر در امنیت
(A_i, I)	حمله به کاربر i (استراتژی A_i) و سرمایه گذاری کاربر موردنظر در امنیت

فرض کنید که کاربر۲ به دنبال آن است که نتیجه بگیرد آیا در امنیت سرمایه‌گذاری کند یا خیر؟ این تصمیم در شرایطی اتخاذ می‌شود که کاربر۱ تصمیم به عدم سرمایه‌گذاری (عدم پرداخت هزینه و استفاده از ماژول‌های امنیتی) و کاربر۳ تصمیم به سرمایه‌گذاری روی امنیت دارد. در این شرایط

مهاجم سه استراتژی A1، A2 و A3 را پیش رو دارد. جدول (۳) سود و زیان هر بازیکن و مهاجم در تصمیم‌گیری‌های مختلف را نشان می‌دهد. در این روابط فرض می‌شود که هزینه هر کاربر برای انتخاب هر تصمیم با L نشان داده شده رابطه زیر برقرار است [۱].

$$L_1 < L_2 < L_3 \qquad (۱)$$

از طرفی با تعریف احتمالات تعریف شده qI و qN می‌توان نوشت [۱]:

$$0 < q_I < q_N < 1 \qquad (۲)$$

جدول۳: مدل بازی در حالت نرمال [۱]

		User 2	
		N(H1)	**I(H2)**
Attacker	A_1	$q_N L_1 + q_N \pi L_2$ $R - q_N \pi L_2$	$q_N L_1$ $R - e$
	A_2	$q_N L_2 + q_N \pi L_1$ $R - q_N L_2$	$q_I L_2 + q_I \pi L_3$ $R - e - q_I L_2$
	A_3	$q_I L_3$ R	$q_I L_3 + q_I \pi L_2$ $R - e - q_I \pi L_2$

در این روابط احتمال حمله موفق روی یک فوق‌ناظر نیز همواره بین ۰ و ۱ است ($0 < \pi < 1$). اگر سود کلی یک سرویس ابری برابر R باشد، سود هر کاربر بعد از انتخاب تصمیم مناسب از محاسبه تفاضل R از هزینه ناشی از آن انتخاب محاسبه می‌شود.

با توجه به نتایج مطالعه [۱] مشخص شده است که همواره (A3,N) یک تعادل نش ممکن برای این بازی می‌باشد. در مطالعه مذکور با مقایسه سایر حالت‌های ممکن با تعادل (A3,N) در نهایت چهار حالت برای شناسایی تعادل نش معرفی شده که در موارد زیر بیان شده است.

-اگر $L3 > \frac{q_N}{q_I}(L2 + \pi L1)$ صحیح باشد، استراتژی (A3,N) یک تعادل نش مناسب است.

-اگر $L3 < \frac{q_N}{q_I}(L2 + \pi L1)$ و $e > (q_N - q_I)L2$ برقرار باشند، استراتژی (A2,N) یک تعادل نش مناسب است.

-اگر $L1 > \frac{q_I}{q_N}(L3 + \pi L2)$ و $e < q_N \pi L2$ برقرار باشد، استراتژی (A1,I) یک تعادل نش مناسب است.

-اگر سه شرط زیر برقرار باشد:

$$\begin{aligned} &L3 < \frac{q_N}{q_I}(L2 + \pi L1) \\ &e < (q_N -)L2 \\ &L1 < \frac{q_I}{q_N}(L3 + \pi L2) \end{aligned} \qquad (۳)$$

یک تعادل نش مخلوط به صورت زیر نیز ارائه می‌شود:

$$u_a(A_2) = \alpha(q_N L_2 + q_N \pi L_1) + (1-\alpha)(q_I L_2 + q_I \pi L_3 \qquad (۴)$$

$$u_a(A_3) = \alpha(q_I L_3) + (1-\alpha)(q_I L_3 + q_I \pi L_2) \qquad (۵)$$

که در این روابط

$$\alpha = \frac{q_I[(L_3 + \pi L_2) - (L_2 + \pi L_3)]}{q_N(L_2 + \pi L_1) - q_I(L_2 + \pi L_3) + q_I \pi L_2} \qquad (۶)$$

۴،۱. بازی تکرار شونده

در تئوری بازی، یک بازی تکراری، بازی فرم گسترده است که شامل تعدادی تکرار برخی از بازی‌های پایه است. بازی‌های تکرار شونده این ایده را به ذهن متبادر می‌کنند که بازیکن باید تأثیر فعلی خود را بر عملکردهای دیگر بازیکنان در نظر بگیرد. بازی‌های تکراری بسته به مدت زمان انجام بازی، ممکن است به طور کلی به دو دسته محدود و نامحدود تقسیم شوند. بازی‌های محدود به بازی‌هایی گفته می‌شود که در آن هر دو بازیکن بدانند که بازی در دوره‌ای مشخصی (و محدود) انجام می‌شود و بعد از آن به طور قطعی پایان می‌یابد. بازی-های نامحدود به بازی‌هایی گفته می‌شود که در آن‌ها بازی به تعداد بی‌نهایت انجام شده و بازیکنان بازی نمی‌دانند که چند دور بازی انجام می‌شود. حتی اگر بازی در هر دور یکسان باشد، تکرار آن بازی به تعداد محدود یا نامحدود، می‌تواند به طور کلی منجر به نتایج و همچنین استراتژی‌های بهینه بسیار متفاوت شود.

کاربر ممکن است یک سرویس ابری را برای مدت طولانی انتخاب کرده و مورد استفاده قرار دهد. لذا این سرویس ممکن است بارها و از طریق‌های مختلف مورد حمله قرار گیرد. این

موضع نشان می‌دهد که کاربر می‌بایست برای بهینه بودن هزینه انجام شده روی امنیت مرتبا استراتژی خود را تغییر دهد. این مهم لزوم بررسی بازی تکرار شونده در سرمایه‌گذاری روی امنیت را نشان می‌دهد. در ادامه حالت‌های مختلفی برای طراحی بازی بررسی شده که طی آن هر کدام از استراتژی‌ها بتوانند تعادل نش باشند.

الف: فرض کنید برای تعادل نش بودن (A3,I)، طراح بازی استراتژی زیر را برای بازی تکراری در نظر گرفته است:

در مرحله اول، مهاجم به کاربر۳ حمله کرده تا زمانی که کاربر۲ از یکی از مکانیزم های امنیتی استفاده نکرده به آن حمله نمی کند. اما اگر کاربر۲ تخطی کرد و بنا به دلایل مختلف (از جمله مالی) تصمیم به عدم استفاده از یکی از مکانیزم‌های امنیتی تعبیه شده را در دوره فعلی داشته باشد مهاجم به خود او (کاربر۲) حمله می‌کند، در نتیجه کاربر تصمیم می‌گیرد در امنیت سرمایه گذاری کند.

سناریو: مهاجم به کاربر۳ حمله می‌کند تا زمانی که کاربر۲ در امنیت سرمایه گذاری کند. در این حالت با توجه به مقادیر نوشته شده در جدول (۳) می‌توان نوشت:

$$(A_3, I) = (q_I L_3 + q_I \pi L_2 , R\text{-}e\text{-}q_I \pi L_2) \text{ forever} \quad (۷)$$

جریمه: در صورت بازی کردن N توسط کاربر۲، در هر مرحله‌ای، مهاجم به خود کاربر۲ حمله کند تا پایان بازی

$$(A_2, I) = (q_I L_2 + q_I \pi L_3 , R - e - q_I L_2) \text{ forever} \quad (۸)$$

در این حالت میزان وسوسه کاربر۲ برای تخطی در بازی از (A3,I) به (A3,N) مقدار زیر می‌باشد:

$$R - (R - e - q_I \pi L_2) = e + q_I \pi L_2 \quad (۹)$$

لذا اگر دلتا مقدار احتمال تکرار در بازی تکرار شونده را نشان دهد، برای محاسبه مقدار احتمال تکرار می‌توان نوشت:

$$e + q_I \pi L_2 < \delta(u(A_3, I) \text{ forever} - u(A_2, I) \text{ forever}) \quad (۱۰)$$

در ادامه با جایگذاری مقادیر u از جدول (۳)، رابطه (۱۱) حاصل شده و در ادامه با ساده‌سازی این معادله، رابطه (۱۲) حاصل می‌شود.

$$\begin{aligned} e + q_I \pi L_2 < \delta[&((R - e - q_I \pi L_2) \\ &+ (R - e - q_I \pi L_2)\delta \\ &+ (R - e - q_I \pi L_2)\delta^2 + \cdots) \\ &- ((R - e - q_I L_2) \\ &+ (R - e - q_I L_2)\delta \\ &+ (R - e - q_I L_2)\delta^2 + \cdots)] \end{aligned} \quad (۱۱)$$

$$\begin{aligned} e + q_I \pi L_2 < \delta[&(q_I L_2(1 - \pi)) \\ &+ (q_I L_2(1 - \pi))\delta \\ &+ (q_I L_2(1 - \pi))\delta^2 + \cdots] \\ &< \delta\left(\frac{(q_I L_2(1 - \pi))}{1 - \delta}\right) \end{aligned} \quad (۱۲)$$

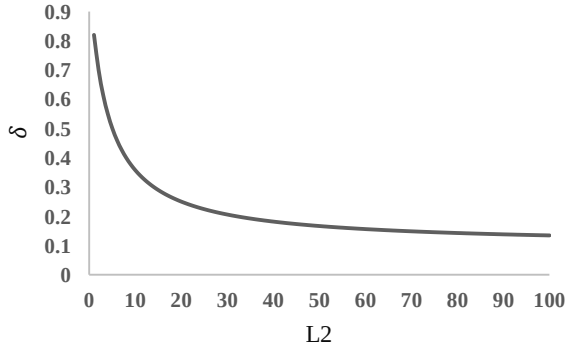
در نتیجه داریم:

$$e + q_I \pi L_2 < \delta\left(\frac{(q_I L_2(1 - \pi))}{1 - \delta}\right) \quad (۱۳)$$

با حل معادله فوق:

$$\delta > \frac{e + q_I \pi L_2}{e + q_I L_2} \quad (۱۴)$$

نمودار دلتا (احتمال تکرار بازی) برای مقادیر مختلف L2 (1<L2<100) برای بازی تکراری در این حالت در شکل (۳) نشان داده شده است. همانطور که مشاهده می‌شود، می‌توان گفت که با احتمال تکرار بازی بین ۰/۲ تا ۰/۸، استراتژی‌های از پیش تعیین شده سرمایه‌گذاری یا عدم‌سرمایه‌گذاری می‌تواند منجر به یک تعادل نش مناسب شده و هرچه مقدار هزینه (L2) افزایش می‌یابد احتمال تکرار بازی کمتر شده و کاربر با همان سیاست‌های قبلی به بازی خود ادامه می‌دهد. در هزینه-های پایین، احتمال تکرار بازی افزایش می‌یابد و کاربر تمایل دارد مرتبا استراتژی خود را تغییر داده و شرایط مطلوب امنیتی خود را تامین کند.



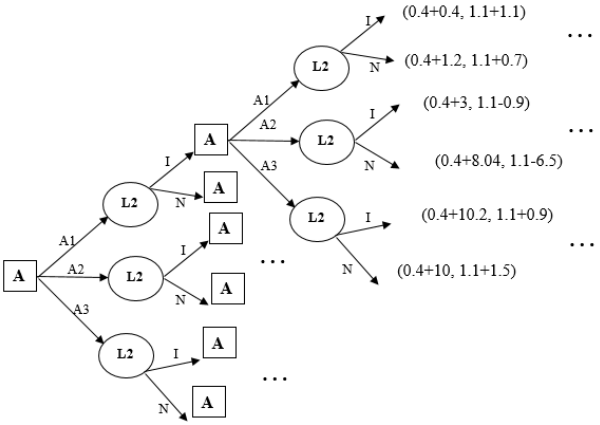
شکل (۳): تغییرات احتمال δ با توجه به بازه پتانسیل جریمه کاربر۲

لذا با مقدار $\alpha = \frac{e+q_I \pi L_2}{e+q_I L_2}$ می‌توان گفت که بازی (A3,I) تعادل نش می‌باشد.

مثال: برای بررسی بازی تکرار شونده مسئله را با فرض $L_2 = 20$ مورد بررسی قرار می‌دهیم. با توجه به پارامترهای این مثال جدول سود و زیان مربوط به این بازی در جدول (۴) خلاصه خواهد شد. با توجه به این بازی تک مرحله‌ای چون شرط ۱ گفته شده در این حالت صدق می‌کند، لذا تعادل نش در این حالت (A3,N) می‌باشد. نمودار درختی این بازی در تکرارهای بیشتر، اگر شروع کننده مهاجم باشد، در شکل (۴) نشان داده شده است.

جدول (۴): جدول سود و زیان به ازای $L_2 = 20$

		User 2	
		N(H)	I(H)
Attacker	A_1	(۰/۷ و ۱/۲)	(۱/۱ و ۰/۴)
	A_2	(۸/۰۴ و ۶/۵-)	(۰/۹- و ۳)
	A_3	(۱/۵ و ۱۰)	(۰/۹ و ۱۰/۲)



شکل (۴): نمودار درختی در بازی تکرارشونده با شروع بازی توسط مهاجم

سناریو: مهاجم به کاربر۳ حمله می‌کند تا زمانی که کاربر۲ در امنیت سرمایه‌گذاری کند:

$$(A_3, I) = (10.2\,, 0.9) \text{ forever} \qquad (۱۵)$$

جریمه: در صورت بازی کردن N توسط کاربر۲، در هر مرحله‌ای، مهاجم به خود کاربر۲ حمله کند تا پایان بازی

$$(A_2, I) = (3\,, -0.9) \text{ forever} \qquad (۱۶)$$

در این حالت میزان وسوسه کاربر۲ برای تخطی در بازی از $(A_3, I) = (10.2\,, 0.9)$ به $(A_3, N) = (10\,, 1.5)$ مقدار 1.5-0.9 است.

$$1.5 - 0.9 < \delta(\mathrm{u}(A_3, \mathrm{I}) \text{ forever} - \mathrm{u}(A_2, \mathrm{I}) \text{ forever}) \qquad (۱۷)$$

در ادامه مقدار احتمال تکرار بازی برای بررسی این تعادل نش با کمک رابطه (۱۸) محاسبه می‌شود.

$$\begin{aligned} 1.5 - 0.9 < \ & \delta[(0.9 + 0.9\delta + 0.9\delta^2 + 0.9\delta^3 + \cdots) \\ & - (-0.9 - 0.9\delta - 0.9\delta^2 - 0.9\delta^3 - \cdots)] \\ < \ & \delta(1.8 + 1.8\delta + 1.8\delta^2 + 1.8\delta^3 + \cdots) < \delta\left(\frac{1.8}{1-\delta}\right) \\ & \rightarrow 0.6 < \frac{1.8\,\delta}{1-\delta} \rightarrow 0.6 - 0.6\delta < 1.8\delta \rightarrow 0.6 < 2.4\delta \rightarrow \delta > \frac{1}{4} \end{aligned} \qquad (۱۸)$$

لذا با مقدار $\alpha = \frac{1}{4}$ می‌توان گفت که بازی (A3,I) با فرض $L_2 = 20$ تعادل نش می‌باشد.

ب: فرض کنید برای تعادل نش بودن (A3,N) طراح بازی استراتژی زیر را برای بازی تکراری در نظر گرفته است:

در تکرار اول کاربر۲ در عدم امنیت سرمایه‌گذاری می‌کند و مهاجم تا زمانی که به کاربر۳ حمله کند کاربر۲ استراتژی خود را تغییر ندهد. اما اگر مهاجم تخطی کرد، کاربر۲ در امنیت سرمایه‌گذاری می‌کند.

سناریو: کاربر۲ در عدم امنیت سرمایه‌گذاری می‌کند تا زمانی که مهاجم به کاربر۳ حمله کند:

$$(A_3, \mathrm{N}) = (q_I L_3\,, \mathrm{R}) \text{ forever} \qquad (۱۹)$$

جریمه: در صورت حمله مهاجم به کاربر۲، در هر مرحله‌ای، کاربر۲ در امنیت سرمایه‌گذاری می‌کند.

$$(A_2, \mathrm{I}) = (q_I L_2 + q_I \pi L_3\,, \mathrm{R} - \mathrm{e} - q_I L_2) \text{ forever} \qquad (۲۰)$$

در این حالت میزان وسوسه مهاجم برای تخطی در بازی از (A3,N) به (A2,N) مقدار زیر می‌باشد:

$$q_N L_2 + q_N \pi L_1 - q_I L_3 \qquad (۲۱)$$

لذا برای محاسبه مقدار احتمال تکرار می‌توان نوشت:

$$\begin{aligned} q_N L_2 + q_N \pi L_1 - q_I L_3 \\ < \delta(u(A_3, N) \text{ forever} \\ - u(A_2, I) \text{ forever}) \end{aligned} \qquad (۲۲)$$

در ادامه مشابه فرآیند اجرا شده برای معادله (۱۲) می‌توان با جایگذاری مقادیر u از جدول (۳) به معادله (۲۳) و با ساده‌سازی آن به معادله (۲۴) دست یافت:

$$\begin{aligned} q_N L_2 + q_N \pi L_1 - q_I L_3 \\ < \delta \left[\left((q_I L_3) + (q_I L_3)\delta \right. \right. \\ + (q_I L_3)\delta^2 + \cdots \big) \\ - \big((q_I L_2 + q_I \pi L_3) \\ + (q_I L_2 + q_I \pi L_3)\delta \\ \left. \left. + (q_I L_2 + q_I \pi L_3)\delta^2 + \cdots \right) \right] \end{aligned} \qquad (۲۳)$$

$$\begin{aligned} q_N L_2 + q_N \pi L_1 - q_I L_3 \\ < \delta[(q_I L_3(1-\pi) - q_I L_2) \\ + (q_I L_3(1-\pi) - q_I L_2)\delta \\ + (q_I L_3(1-\pi) - q_I L_2)\delta^2 \\ + \cdots] \\ < \delta\left(\frac{(q_I L_3(1-\pi) - q_I L_2)}{1-\delta}\right) \end{aligned} \qquad (۲۴)$$

در نتیجه داریم:

$$q_N L_2 + q_N \pi L_1 - q_I L_3 < \delta\left(\frac{(q_I L_3(1-\pi) - q_I L_2)}{1-\delta}\right) \qquad (۲۵)$$

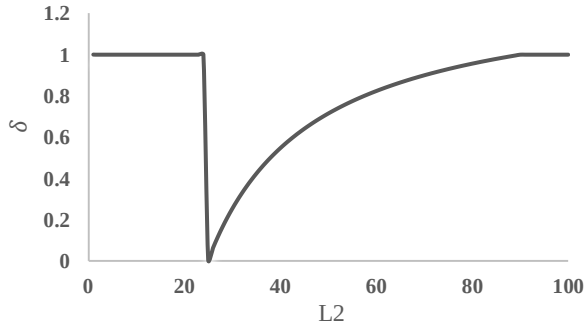
با حل معادله فوق:

$$\delta > \frac{q_N L_2 + q_N \pi L_1 - q_I L_3}{q_N L_2 + q_N \pi L_1 - q_I \pi L_3 - q_I L_2} \qquad (۲۶)$$

نمودار دلتا برای مقادیر مختلف L2 (با توجه به اینکه L1<L2<L3 لذا 1<L2<100) برای بازی تکراری در این حالت در شکل (۳) نشان داده شده است.

در توضیح نمودار ارائه شده در شکل (۵) می‌توان گفت، با توجه به روابط ارائه شده در بخش تعادل نش مختلط، به ازای L بین ۱ تا ۲۴، (A3,N) خود تعادل نش بوده و لذا هیچ وسوسه‌ای در جریان بازی تکراری حاکم نیست ولی با افزایش مقدار L با شروع تعادل نش مختلط حاکم بر بازی می‌توان انتظار داشت که وسوسه بازیکن برای سرپیچی از قانون حاکم بر بازی با افزایش مقدار هزینه، افزایش می‌یابد.

لذا با مقدار $\alpha = \frac{q_N L_2 + q_N \pi L_1 - q_I L_3}{q_N L_2 + q_N \pi L_1 - q_I \pi L_3 - q_I L_2}$ می‌توان گفت که بازی (A3,N) تعادل نش می‌باشد. با روش نشان داده شده در شرایط مختلف و با طراحی استراتژی مناسب می‌توان هر یک از شش حالت موجود در بازی را در یک بازی تکرارشونده به عنوان تعادل نش معرفی کرد.



شکل (۵): تغییرات احتمال δ با توجه به بازه پتانسیل جریمه کاربر۲

۵. نتیجه‌گیری

ویژگی‌های منحصر به فرد یک ساختار رایانش ابری و مجازی‌سازی کامل می‌تواند زمینه‌های جدید حمله را فراهم کند. همانطور که پیش از این گفته شد، ساختار ابر فرصت‌های جدیدی برای اتخاذ تصمیم مناسب توسط کاربران در خصوص سرمایه‌گذاری روی یکی از ماژول‌های امنیتی (و پرداخت هزینه) در نتیجه اقدام مهاجمان را می‌دهد. ارائه دهندگان خدمات ابری ممکن است با صرف هزینه بابت ماژول‌های نرم‌افزاری یا سخت‌افزاری آسیب‌پذیری‌های خود را کاهش دهند و از اثرات حمله و نشر آن به سایر ماشین‌های مجازی جلوگیری کنند، اما این جنگ ادامه داشته و بستگی به استراتژی‌های متقابل کاربران سرویس‌های ابری، حمله کنندگان و هزینه‌های متحمل شده توسط هر یک از آن‌ها است. بسیاری از ارائه دهندگان ابری ممکن است به میزان قابل توجهی ایمن‌تر از آنچه تصور می‌کنند نباشند و بسیاری از مشتریان از نقاط ضعف بالقوه موجود در ابری ابراز بی‌اطلاعی کنند. یکی از موضوعاتی که در این مقاله به آن پرداخته شد، مسئله ورود کاربر جدید بوده که در صورت اتخاذ تصمیم عدم سرمایه‌گذاری در امنیت (عدم پرداخت هزینه و استفاده از یکی

از ماژول‌های امنیتی) توسط یک کاربر ممکن است تهدیدهای امنیتی بر کاربر دیگر نیز تأثیر بگذارد. همان‌طور که نشان داده شد استراتژی تعادل نش نسبت به عوامل خارجی و تصمیمات سایر کاربران حساسیت بیشتری نسبت به شرایط اولیه مانند ضرر احتمالی کاربران یا هزینه سرمایه‌گذاری دارد. بدیهی است که مقدار "هزینه سرمایه‌گذاری روی امنیت (e)" در تعیین تعادل نش نقش مهمی دارد. بنابراین برای کاربران، آگاهی از مقادیر e و π (احتمال حمله موفق روی یک فوق ناظر) می‌تواند در تصمیم‌گیری در مورد این‌که آیا ماژول‌های امنیتی پیشنهادی رایانش ابری ابزاری مفید بوده تا با صرف هزینه کم، امنیت مناسب را در پی داشته باشد می‌تواند بسیار مهم باشد. نتایج حاصل از تحلیل وپیاده‌سازی به کاربر تازه وارد سرویس ابری کمک می‌کند تا با در نظر گرفتن هزینه سرویس‌های امنیتی، احتمالات حمله و هزینه ناشی از آن، مناسب‌ترین استراتژی (تکرار بازی و بازبینی سیاست‌های امنیتی موجود و یا ادامه روند قبلی) را اتخاذ کرده و به بهترین نتیجه از لحاظ هزینه و امنیت دست پیدا کند. به عنوان کار آینده می‌توان هزینه مختلف حملات و تاثیرات آن‌ها را متفاوت در نظر گرفته و استراتژی‌های کاربر در خصوص انتخاب یکی از ماژول‌های امنیتی را نیز به صورت فازی مدل کرد تا نتایج جزئی‌تری از تاثیر متقابل سیاست‌های امنیتی و هزینه‌های پرداختی به دست آید.

تعارض منافع: نویسندگان اعلام می‌کنند که هیچ تعارض منافعی ندارند.

مراجع

[1] Kwiat L., Kamhoua C.A., Kwiat K.A., and Tang J., "Risks and Benefits: Game-Theoretical Analysis and Algorithm for Virtual Machine Security Management in the Cloud," Assur. Cloud Comput., pp. 49–80, 2018, doi: 10.1002/9781119428497.ch3.

[2] Shabeera T.P., Madhu Kumar S.D., Salam S.M., and Murali Krishnan K., "Optimizing VM allocation and data placement for data-intensive applications in cloud using ACO metaheuristic algorithm," Eng. Sci. Technol. an Int. J., 20(2): 616–628, 2017, doi: 10.1016/j.jestch.2016.11.006.

[3] Tavluoğlu C. and Korkmaz A., "Use of Cloud Computing Applications in Reference Services," Bilgi Dünyasi, 15(2), 2015, doi: 10.15612/bd.2014.420.

[4] Lee C.S., "Multi-objective game-theory models for conflict analysis in reservoir watershed management," Chemosphere, 87(6): 608–613, 2012, doi: 10.1016/j.chemosphere.2012.01.014.

[5] Kamhoua C.A., Kwiat L., Kwiat K.A., Park J.S., Zhao M., and Rodriguez M., "Game theoretic modeling of security and interdependency in a public cloud," IEEE Int. Conf. Cloud Comput. CLOUD, pp. 514–521, 2014, doi: 10.1109/CLOUD.2014.75.

[6] Gill K.S., Saxena S., and Sharma A., "GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot," Comput. Secur., vol. 92, 2020, doi: 10.1016/j.cose.2020.101732.

[7] Nezarat A., "A Game Theoretic Method for VM-To-Hypervisor Attacks Detection in Cloud Environment," Proc. - 2017 17th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGRID 2017, pp. 1127–1135, 2017, doi: 10.1109/CCGRID.2017.138.

[8] Moseley M., "The Nation's Guardians: America's 21st Century Air Force," pp. 1–10, 2007, Accessed: Feb. 16, 2021. [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a477488.pdf.

[9] Ristenpart T., Tromer E., Shacham H., and Savage S., "Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds," in Proceedings of the ACM Conference on Computer and Communications Security, 2009, pp. 199–212, doi: 10.1145/1653662.1653687.

[10] Kwiat K., "Can reliability and security be joined

reliably and securely?," Proc. IEEE Symp. Reliab. Distrib. Syst., pp. 72–73, 2001, doi: 10.1109/reldis.2001.969750.

[11] Mosweu T., Luthuli L., and Mosweu O., "Implications of cloud-computing services in records management in Africa: Achilles heels of the digital era?," SA J. Inf. Manag., 21(1), 2019, doi: 10.4102/sajim.v21i1.1069.

[12] Kamhoua C.A., Kwiat L., Kwiat K.A., Park J.S., Zhao M., and Rodriguez M., "Game theoretic modeling of security and interdependency in a public cloud," IEEE Int. Conf. Cloud Comput. CLOUD, pp. 514–521, 2014, doi: 10.1109/CLOUD.2014.75.

[13] Shiri H., Park J., and Bennis M., "Communication-Efficient Massive UAV Online Path Control: Federated Learning Meets Mean-Field Game Theory," 2020. doi: 10.1109/TCOMM.2020.3017281.

[14] Higham R. and Carter E.F., "Railways in Wartime.," Mil. Aff., 29(4):208, 1965, doi: 10.2307/1984412.

[15] Kim H., Park J., Bennis M., and Kim S.L., "Massive UAV-to-Ground Communication and its Stable Movement Control: A Mean-Field Approach," 2018. doi: 10.1109/SPAWC.2018.8445906.

[16] Rao N.S.V., Poole S.W., He F., Zhuang J., Ma C.Y.T., and Yau D.K.Y., "Cloud computing infrastructure robustness: A game theory approach," 2012. doi: 10.1109/ICCNC.2012.6167441.

[17] Jalaparti V., Nguyen G., Gupta I., and Caesar M., "Cloud Resource Allocation Games," Sort, 2010, Accessed: Sep. 13, 2021. [Online]. Available: http://hdl.handle.net/2142/17427.

[18] Wei G., Vasilakos A.V., Zheng Y., and Xiong N., "A game-theoretic method of fair resource allocation for cloud computing services," J. Supercomput., 54(2): 252–269, 2010, doi: 10.1007/s11227-009-0318-1.

[19] Han Y., Alpcan T., Chan J., and Leckie C., "Security games for virtual machine allocation in cloud computing," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2013, vol. 8252 LNCS, pp. 99–118, doi: 10.1007/978-3-319-02786-9_7.

[20] Halabi T. and Bellaiche M., "Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach," IEEE Trans. Cloud Comput., 8(3): 928–942, 2020, doi: 10.1109/TCC.2018.2820715.

[21] Agarwal A. and Duong T.N.B., "Secure virtual machine placement in cloud data centers," Futur. Gener. Comput. Syst., 100: 210–222, 2019, doi: 10.1016/j.future.2019.05.005.

[22] Liang X. and Yan Z., "A survey on game theoretical methods in Human–Machine Networks," Futur. Gener. Comput. Syst., 92:674–693, 2019, doi: 10.1016/j.future.2017.10.051.

[23] Ousmane S.B., Mbacke B.C.S., and Ibrahima N., "A game theoretic approach for virtual machine allocation security in cloud computing," in ACM International Conference Proceeding Series, 2019, vol. Part F1481, doi: 10.1145/3320326.3320379.

[24] Homsi S., Quan G., Wen W., Chapparo-Baquero G.A., and Njilla L., "Game theoretic-based approaches for cybersecurity-aware virtual machine placement in public cloud clusters," Proc. - 19th IEEE/ACM Int. Symp. Clust. Cloud Grid Comput. CCGrid 2019, pp. 272–281, 2019, doi: 10.1109/CCGRID.2019.00041.

[25] Prabhakar K., Dutta K., Jain R., Sharma M., and Khatri S.K., "Securing Virtual Machines on Cloud through Game Theory Approach," Proc. - 2019 Amity Int. Conf. Artif. Intell. AICAI 2019, pp. 859–863, 2019, doi: 10.1109/AICAI.2019.8701229.

[26] Wang Y., Guo Y., Guo Z., Baker T., and Liu W., "CLOSURE: A cloud scientific workflow scheduling algorithm based on attack–defense game model," Futur. Gener. Comput. Syst., 111:460–474, 2020, doi: 10.1016/j.future.2019.11.003.

[27] Carvalho G.H.S., Woungang I., Anpalagan A., and Traore I., "Security- and Location-Aware Optimal Virtual Machine Management for 5G-Driven MEC Systems," in Lecture Notes on Data Engineering and Communications Technologies, vol. 51, Springer, 2020, pp. 123–134.

[28] Kandoussi E.M., Hanini M., El Mir I., and Haqiq A., “Toward an integrated dynamic defense system for strategic detecting attacks in cloud networks using stochastic game,” Telecommun. Syst., 73(3): 397–417, Mar. 2020, doi: 10.1007/s11235-019-00616-1.