رویکرد ارزیابی خطر مقیاس پذیر برای رایانش ابری با استفاده از نظریه بازی(CCRAM)

رایانش ابری یکی از رایج ترین مفاهیم پردازش اطلاعات در جهان فناوری اطلاعات امروز محسوب می شود.امنیت رایانش ابر پیشرفته وپیچیده تر شده است زیرا هر مدل خدمات یا سرویس از مولفه ها وعناصر زیر ساختی متفاوتی بهره می برد.مدل های ارزیابی ریسک و خطر امنیتیجاری به طور کلی قابل تعمیم بهسیستم های رایانش ابری نیست که وضعیت آن ها را سریع تغییر می دهد. در این مطالعه،مدل ارزیابی خطرامنیت مقیاس پذیر برایرایانش ابری به عنوان راه حل مسئله با نظریه بازیپیشنهاد شده است. با این رویکرد ما ارزیابی می کنیم که آیا ریسک در سیستم بایستی توسط عرضه کنندهابر یا سیستم تثبیت شود یا خیر.

کلمات کلیدی: امنیت رایانش ابری، امنیت مقیاس پذیر با استفاده از مدل های خدمات ابر، مدل سازی امنیت نظریه ی بازی

مقدمه

رایانش ابر در سال های اخیر توسط سازمان ها برای ارائه خدمات جدید، ورود به بازارهای جدید، نزدیک شدن به مشتریان و کاهش هزینه های عملیات IT، به طور فزاینده ای مورد استفاده قرار گرفته است. به طور کلی، رایانش ابری به عنوان استفاده از منابع کامپیوتر دیگر به عنوان یک سرویس که با استفاده از یک شبکه تحویل داده می شود، تعریف می شود. پیشرفت های تکنولوژیکی در ارتباطات پهنای باند امکان استفاده از رایانه های ابری برای کاربران عادی اینترنت را فراهم می آورد.

از آنجایی که بیش از یک نهاد از این منابع کامپیوتری استفاده می کند، امنیت آن مهم تر از منابع طبیعی IT است که توسط یک نهاد استفاده می شود. با تعریف موسسه ملی استاندارد و فناوری (NIST)، معمولا سه مدل خدمات مختلف ارائه شده برای رایانش ابر ارائه شده است [1]

• نرم افزار به عنوان یک سرویس (SaaS): مدل تحویل نرم افزار با استفاده از زیرساخت ابر. از آنجا که هیچ چیز اضافی برای نصب وجود ندارد، کاربران می توانند از این سرویس در هر جایی که اینترنت دارند دسترسی داشته

باشند. بعضی مثالها خدمات پستی، برنامه های کاربردی اداری، مدیریت ارتباط با مشتری (CRM) و همکاری و غیره است.

• پلت فرم به عنوان یک سرویس (PaaS): در این مدل خدمات، مستاجر می شود یک پلت فرم که در آن او می تواند برنامه خود را توسعه و اجرا کند. ارائه دهندگان ابر ارائه خدمات مکمل و زیرساخت های فن آوری مورد نیاز برای توسعه و اجرای برنامه. گوگل AppEngine، Force.com و مایکروسافت لاورو معروف هستند که ارائه دهندگان PaaS هستند.

• زیرساخت به عنوان یک سرویس (IaaS): در IaaS، فروشندگان ابر ارائه زیرساخت به مستاجر را در قالب قدرت رایانش یا ذخیره سازی. زیرساخت از مراکز داده ای می آید که مجازی سازی برای تقسیم و توزیع منابع آن استفاده می شود. Rackspace Cloud، Google Computing Engine و EC2 آمازون نمونه ای از مدل سرویس IaaS هستند.

• ذخیره سازی به عنوان یک سرویس (STaaS یا SaaS): در این مدل، ارائه دهنده خدمات فضا را در زیرساخت های آن به شخص یا شخص دیگری ارایه می دهد.

• دسکتاپ به عنوان سرویس (DaaS): دسکتاپ "مجازی شده" را به کاربر ارائه می کند؛ بنابراین تمام برنامه ها، برنامه ها، پردازش ها و داده ها بر روی سرور مرکزی نگهداری می شود.

• شبکه به عنوان یک سرویس (NaaS): این مدل شامل شتاب دهنده برنامه، اقدامات امنیتی یا مدیریت دستگاه تلفن همراه و غیره است.

• داده های یک سرویس (DaaS): ارائه اطلاعات در مورد تقاضای مستاجر بدون توجه به جدایی جغرافیایی یا سازمانی ارائه دهنده یا مستاجر

اقدامات امنیتی برای این مدل خدمات متفاوت است به دلیل الزامات منابع مختلف. به عنوان مثال، نیاز به دسترسی به NaaS مهم تر از سایر الزامات است. از آنجا که، نیاز ابتدایی برای این سرویس برای ارائه پهنای باند و شبکه است. ارائه دهنده ابر مسئولیت اطمینان از محرمانه بودن و یکپارچگی داده های عبور را ندارد. اما، چون تمام رایانش توسط

ارائه دهنده در مدل SaaS انجام می شود، تمام ویژگی های امنیتی ارائه شده در جدول 1 باید توسط ارائه کننده SaaS اجرا شود.

مهاجمان شبکه عموما به عنوان انسان هوشمند و عقلایی شناخته می شوند. آنها هزینه و سود حملات خود را در نظر می گیرند. مدافعان هنگامی که یک حمله مضر توسط سیستم های امنیتی آنها مسدود می شوند سود می برند. اما، اگر چنین اتفاقی رخ ندهد، می توانند به دلیل اقدامات امنیتی غیر ضروری، پول را از دست بدهند. این خواص این امکان را برای مدل سازی این رفتار در نظریه بازی [14،15] فراهم می کند. مانند امنیت شبکه، اتصال بازی مهم بین مهاجمان و مدافعان در رایانش ابری وجود دارد. استراتژی دفاعی ایده آل و استراتژی توهینآمیز ایده آل ممکن است بسته به یکدیگر تغییر کند.

تکنیک های تئوری بازی در اقتصاد، زیست شناسی، ریاضیات، روانشناسی و دیگر علوم اجتماعی و رفتاری استفاده می شود. در علوم کامپیوتر، بسیاری از آثار از نظریه بازی استفاده شده است بر روی سیستم های تشخیص نفوذ (IDS) [2]، برنامه ریزی امنیتی [3] و امنیت شبکه / سایبری [4، 15-20]. در سال های اخیر، مطالعات بین تئوری بازی، نظریه اقتصادی و علوم رایانه، راه را برای یک زمینه جدید، نظریه بازی الگوریتمی [5]هموار کرده است. در این کار، یک مدل برای تعیین استراتژی های دفاعی دفاعی و تهاجمی با استفاده از خواص مدافعان و مهاجمانی که در بالا ذکر شده است، مورد توجه قرار گرفته و اقدامات امنیتی انجام گرفته است. استراتژی های افزایش یا کاهش آسیب به بازیکنان مربوطه با استفاده از این مدل ارائه می شود. در نتیجه، کارمندان امنیتی ابر رایانه می توانند تعیین کنند که کدام اقدامات امنیتی باید بسته به میزان سود یا ضرر آنها انجام شود. مدل پیشنهادی راه حل جدیدی است برای امنیت رایانش ابری. ریسک های امنیتی ارزیابی شده با استفاده از روش پیشنهادی در سیستم رایانش ابری باید توسط یک ارائه دهنده ابر یا مستاجر سیستم کاهش یابد.

بقیه مقاله به شرح زیر است: بخش 2 شامل آثار مرتبط است. بخش 3 مدل پیشنهادی را معرفی می کند. بخش 4 مثال مفصلی عملی و بحث را ارائه می دهد. بخش 5 نتایج و کارهای آینده را ارائه می دهد.

2-کارهای مرتبط

از آنجا که ارزیابی خطر در رایانش ابری یک موضوع داغ است، بیشتر تحقیقات در این موضوع بر روی زیرساخت های رایانشی شبکه ساخته شده است. تحقیقاتی که براساس رایانش شبکه انجام می شود عموما ذخیره سازی داده ها را پوشش نمی دهد که جنبه مهمی از رایانش ابری است زیرا اکثر شبکه ها برای حل یک کار تنها مورد استفاده قرار می گیرند و ذخیره داده ها را پوشش نمی دهند و همچنین بیشتر این تحقیق بر روی ارزیابی خطر استاتیک. درمنبع 6 مدل FPVA عمدتا به شبکه میان افزار متصل می شود که برای جدا کردن بار کار یک برنامه به ماشین های فیزیکی بیشتر استفاده می شود.

اگر چه به نظر می رسد مشابه یک ابر است، زیرا کاربران ایجاد پلت فرم و یا تغییر پلت فرم در مدل های خدمات IaaS و PaaS، مدل FPVA برای چنین اهدافی بی تاثیر است. اساسا، این مدل ابتدا یک درخت ایجاد می کند که متشکل از تعاملات بین برنامه ها و دارایی ها است. پس از آن، هر گره در این درخت برای ارتباط با یکدیگر و برای آسیب پذیری های امنیتی مورد بررسی قرار می گیرد. سپس، کد برنامه نویسی هر گره توسط کارشناسان با در نظر گرفتن آسیب پذیری های احتمالی امنیتی که این رابطه درخت ارائه شده است، دستی بررسی می شود. یکی از بزرگترین مشکلات این مدل این است که دستی بررسی API های ابر زمان زیادی را با توجه به میزان API های IaaS و PaaS می گیرد. یکی دیگر از مشکلات این است که حتی اگر تکنولوژی های ابر و شبکه به نظر شبیه باشند، خطرات مرتبط با آنها با یکدیگر متفاوت است.

• سطح اول: مشکل را در ساختار سلسله مراتبی تشکیل می دهد. هدف کلی در بالای سطح قرار می گیرد. در این مدل، آن را به ارزیابی کلی پلت فرم سیستم رایانش ابری مربوط می شود.

• سطح دوم: شامل هشت ویژگی است که شامل عوامل اصلی شناسایی شده برای ارزیابی سطح اول است.

• سطح سوم: آخرین سطح برای عوامل ارزیابی بنیادی در چارچوب تصمیم گیری است. سی و نه عامل با توجه به سطوح بالاتری و شرایط خاص محلی شناسایی شدند.

پیاده سازی AHP نیاز به سه اصل دارد: تجزیه، مقایسات جبری و ترکیب وزن. برخی مزایای استفاده از پردازش AHP در رایانش ابری عبارتند از:

• توانایی شکستن مشکل به قطعات ارثی

• قادر به محاسبه قضاوت های آزمایشی تصمیم گیرنده، به ویژه هنگامی که اهداف داده های قابل اندازه گیری فاقد اطلاعات باشند.

تصمیم گیرندگان ارزیابی را با توجه به عوامل تعیین شده در سطح سوم ارزیابی می کنند و هر کدام یک وزن می دهند و در یک ماتریس قرار می گیرند تا عامل وزن را بدست آورند. مشکل در اینجا، تصمیم گیرندگان مجبور به تغییر دستی بردارها تا زمانی که ارزیابی ها تایید صحت را تایید کنند.

جویرود یک رویکرد نیمه کمی برای ارزیابی ریسک برای رایانش ابری ارائه دادند. تصمیم گیری با توجه به اشیاء سطح کسب و کار مانند؛ به حداکثر رساندن سود و رضایت کاربر. در این رویکرد نیمه کمی، برخی از خطرات حتی برای کسب و کار سود می کنند. تاثیر خطرات بین دو عامل تغییر می کند: سود و تهدید. قبل از مقایسه، خطرات با توجه به عوامل زیر گروه بندی می شوند:

• احتمال رخداد یک رویداد خطر: مقادیر بین 1 و 5 را بیان می کند. بیان شده بوسیله بسیار نامطلوب (1، به عنوان مثال یک بار در 20 سال)، بعید است (2، به عنوان مثال سالانه)، ممکن (3، مانند ماهانه یا هفتگی) ، به احتمال زیاد (4، به عنوان مثال روزانه) و مکرر (5، به عنوان مثال در هر لحظه).

• تأثیر آن رویداد: یا یک تهدید، یک مزیت، و یا هر دو، نیمه تعریف شده بین بسیار بالا (-5 یا 5، به ترتیب منفی و مثبت)، بالا (-4/4)، متوسط (-3/3)، کم (-2/2) و بسیار کم (-1/1).

• برآورد سطح خطر: این متناسب با احتمال یک رویداد داده شده و شیء کسب و کار مورد نظر است

در این روش، احتمال ریسک با تأثیر ریسک برای بدست آوردن سطح ریسک که بین مقادیر 25 و 25 می باشد، افزایش می یابد [8]. با توجه به تاثیر خطرات (مزایا و تهدید)، این یک فاصله محدود است. در روش ما، با توجه به مدل سرویس ارائه دهنده و ارزش سیستم، اندازه فاصله ما بزرگتر است. همچنین، مدل پیشنهادی به هیچ وجه به عنوان یک مزیت برای رفع هر مشکلی که ممکن است در آینده اتفاق بیفتد، خطر نداشته باشد. م. کیران و همکاران.

[9] در مقاله خود توضیح داد که اکثر ارزیابی های پیشنهادی ریسک در رایانش ابری به شدت بر روی کاربر در نظر گرفته می شود

م. کیران و همکاران. [9] در مقاله خود توضیح داد که اکثر ارزیابی های پیشنهادی خطر در رایانش ابر به شدت به سمت کاربر در نظر گرفته می شود. هر دو در مدل و روش ارائه شده در اینجا سعی در نگاه کردن به ابعاد ارائه دهنده ابر دارند. حتی اگر مدلهای ما به همان شکل نگاه کنند، مقاله آنها سرویس دهنده های ابر را به دو دسته تقسیم می کند: ارائه دهنده سرویس و ارائه دهنده زیرساخت. ارائه دهندگان خدمات به عنوان موسسه بین المللی تعریف می شوند که زیرساخت را از ارائه دهندگان خدمات زیرساخت ایفا می کند و از این پایه برای ایجاد یک سرویس که کاربران می توانند کار کنند استفاده می شود. به این ترتیب، ارائه دهندگان خدمات و ارائه دهندگان زیرساخت ها می توانند ارزیابی خطر را با دادن وزن های مختلف به عوامل خاص انجام دهند. این ارزیابی با جداسازی خطرات به دسته های مختلف ادامه می یابد.

3-روش ارزیابی ریسک رایانش ابری با تئوری بازی

در امنیت اطلاعات، حمله به عنوان تعامل بین مهاجم و سیستم دفاع که برای محافظت از هدف استفاده می شود تعریف می شود. در این وضعیت، سیستم دفاع و مهاجم، بازیکنان فعال هستند که نتایج آنها بسته به درگیری آنها با یکدیگر تغییر می کند. تئوری بازی یک رویکرد بین رشته ای است برای بازرسی رفتار بین دو بازیکن یا یک گروه با استفاده از ویژگی های خاص خود. تئوری بازی به دنبال یافتن راهبردهای مطلوب است که نتیجه را افزایش می دهد یا آسیب را در پاسخ به رفتار گروهی یا نهادی دیگر کاهش می دهد. برای انتخاب استراتژی مطلوب، برخی از مفروضات به شرح زیر ارائه می شود.

- هر بازیکن قادر به انجام دو یا چند اقدام مشخص و یا مجموعه ای از اقدامات است.
- هر اقدامی که بازیکنان به یک حالت پایان به خوبی تعریف می کنند، حتی اگر بازی به نظر می رسد مداوم باشد.
- هر بازیکن با یک امتیاز مشخص در هر حالت انتهای همراه است.
- هر بازیکنی که تصمیم گیری می کند، قواعد بازی را می داند و از مزایای دیگر بازیکنان برخوردار است.

• با توجه به دو اقدام، فرض می شود که بازیکنان در تلاش برای به حداکثر رساندن بازده خود هستند (فرض عقلانیت و حداکثر سازی).

دلیل مدل سازی نظریه ی بازی این است که توضیح دهید که چرا انسان ها به نحوی خاص رفتار می کنند و حدس می زنند که کدام اقدامات با توجه به رفتار آنها انجام می شود.

در زمینه امنیت، تئوری بازی می تواند برای کمک به انتخاب راهکارهای بهینه برای دفاع و حمله با توجه به احتمال اقداماتی که مدافع یا مهاجم انجام می دهد، استفاده شود [14،15]. با توجه به معیارهای بازی، تابع ابزار برای هر بازیکن با نظریه بازی تعریف می شود. این توابع ابزار برای نشان دادن نتایج اقداماتی که توسط بازیکنان انجام شده است استفاده می شود. اگر یک بازیکن استراتژی A را انتخاب می کند که نتیجه آن را با توجه به استراتژی B فرد یا گروه دیگر به حداکثر می رساند، استراتژی A بهترین پاسخ نامیده می شود. اگر این برای همه بازیکنان قابل اجرا باشد، به عبارت دیگر، اگر هیچ بازیکن انگیزه ای برای کنار گذاشتن تصمیم خود پس از انتخاب طرف مقابل نداشته باشد، این پروفایل های استراتژی نامزهای تعادل نامیده می شود.

یکی از بخش های مهم مدل امنیتی، محاسبه عوامل خطر در ارزیابی ریسک است. بنابراین، به دنبال فرضهای لازم است:

• مهاجم و مدافع بازیکن بازی هستند. اگر بیش از یک مهاجم وجود داشته باشد، فرض می شود که آنها با یکدیگر همکاری می کنند. اگر بیش از یک مدافع وجود داشته باشد، آنها همگی با یکدیگر همکاری می کنند.

• مهارت های هر یک از مهاجمین به عنوان برابر است. بنابراین، حتی در حملات معمول، مهاجمان فکر می کنند که امکان حمله مشابهی را داشته باشند و هر تهدیدی یک خطر مهم برای ارائه دهنده است.

• هر حمله به عنوان موفقیت آمیز محسوب می شود، مگر اینکه یک اقدام امنیتی برای آن وجود داشته باشد.

• اگر مدافع یک اقدام امنیتی برای این نوع حمله انجام دهد، هر حملهی در آن نوع تشخیص داده می شود و می تواند متوقف شود.

CCRAM یک مدل بازی ناتمام است که با استفاده از اطلاعات غیرواقعی است. مطمئنا مهاجم و مدافع یک هدف مشترک ندارند، بنابراین بازی غیر تعاونی است. جنبش مهاجم و مدافع هزینه دارد. بنابراین، فقط استفاده از دستاوردها در توابع ابزار نتیجه مناسب را نمی دهد. بنابراین، از دست دادن یکی از طرفین همیشه به نفع طرف دیگر نیست. بنابراین بازی غیر صفر است. هدف اصلی این مدل این است که مدافع را در انتخاب یک استراتژی دفاعی در صورت حمله، که بر روی سیستم خود یا سیستم خریداری شده از یک ارائه دهنده ابر دیگر تأثیر می گذارد، انتخاب کنید.

تعریف 1:G:(P,S,S)

1) P = (1،a2، ...، n) نشان دهنده بازیکنان به نام مهاجم و مدافعان بازی است. اگر بیش از یک مهاجم یا مدافع وجود داشته باشد، در نظر گرفته می شود که به ترتیب با دیگر مهاجمان یا مدافعان همکاری کند.

S = (s1 ،s2 ، ...، sn) فضای استراتژی بازیکنان و ∀x∈ را نشان می دهد

P، Sx ≠ ∅، Sx = (S1 x ،S2 x ، ...، Sm x) مجموعه ای از استراتژی بازیکن x است.

U = (U1 ،c2 ، ...، Un) عملکرد تابع از بازیکنان در بازی است

تعریف 2:CCRAM یک مدل ناتمام اطلاعات غیر سازشی غیر عادی استاتیک است که به عنوان تعریف شده است:

$$CCRAM = \{(a,d),(S_a,S_d),(U_a,U_d)\}$$

که A نشان دهنده مهاجم و د نماینده مدافع است. مجموعه سوS1d) = ، S2d، ...، Sm a) فضای استراتژی مهاجم است و sj a استراتژی است که می تواند توسط مهاجم مورد استفاده قرار گیردS1 d) = Sd .. S2 d، ...، Sm d) فضای استراتژی مدافع است و sj d یک استراتژی است که می تواند توسط مدافع مورد استفاده قرار گیرد Ua .و Ud توابع ابزار مهاجم و مدافع هستند.

3-1مدل سازی حمله و دفاع

در مطالعه MIT آزمایشگاه لینکلن، تاثیر بر میزبان ناشی از حمله نمی تواند با یک پارامتر بیان شود. در پاسخ به این، روش ما از اصول اساسی اوراق بهادار اطلاعات، یعنی محرمانه بودن، یکپارچگی و در دسترس بودن برای اندازه گیری تاثیر بر روی سیستم هدف استفاده خواهد کرد.

محرمانگی، یکپارچگی و قابلیت دسترسی (CIA) می تواند برای محاسبه تاثیر حمله به یک سیستم استفاده شود. پایگاه اطلاعات آسیب پذیری [10] از CIA به عنوان ضریب تاثیر در CVSS v2 Definitions استفاده می کند. طبقه بندی حمله با در نظر گرفتن آنچه مهاجم می خواهد با نوع حمله انجام دهد انجام می شود. با توجه به اهداف استراتژیک این حمله، هر نقطه ای در CIA بین 0 و 1 به منظور تمایز با انواع دیگر حملات (وزن 2) ارائه می شود. روش های دفاعی به ترتیب در جدول 3 مطابق با زمان مورد نیاز برای اعمال اندازه گیری امنیتی و تاثیر آن بر اندازه گیری امنیت در عملکرد عادی سیستم، به سه دسته تقسیم می شوند.

3-2محاسبه ارزش سیستم

پایه رایانش ابری مجازی سازی است. مجازیسازی یک نسخه مجازی سختافزار (CPU، RAM و غیره)، منابع شبکه (روترها، سوئیچها و غیره)، سیستمهای عامل یا دستگاههای ذخیرهسازی را ایجاد میکند. تبادلگرایی اساسا با تقسیم دارایی به ابعاد مختلف دارایی برای استفاده بهتر از آن انجام میشود . به عنوان مثال، به طور سنتی CPU سرور به طور کلی بیش از 20٪ استفاده نمی کند، اگر آن را انجام یک کار واحد. بنابراین، 80٪ از آن در واقع به هدر میرود. با این حال، اگر CPU به پنج تقسیم شود و هر قطعه یک شغل داده می شود، استفاده از پردازنده به 100٪ نزدیک می شود

جدول 2: نمونه هایی از حمله

مقوله	تعری	C I A
DOS کاربر داده اسکن	انکار سرویس کسب مزیت کاربر دسترسی غیرمجاز به داده دست یابی به مزیت کاربر	0 0 1 0.5 0.1 0.05 1 1 0.2 1 0.1 0.05 0.3 0 0.2

جدول 3:برخی مثال های مربوط به کلاس های دفاع

مقوله	تعریف	ویژگی
پایه	تغییر پیکر بندی	زمان مورد نیاز برای تغییر پیکر بندی
میانی	شروع ماشین	زمان مورد نیاز برای اعمال تغییرات
پیشرفته	عملیات سنگین	زمان مورد نیازنسبت به سه مورد دیگر

اگر ما یک سیستم را بررسی می کنیم که به عنوان یک ماشین مجازی در حال اجرا بر روی hypervisor در نظر گرفته شده است، چند چیز است که باید قبل از تعریف ارزش آن سیستم مورد توجه قرار گیرد. یکی از این موارد مهاجرت زنده سیستم است. مهاجرت زنده انتقال یک منبع از یک مکان فیزیکی به مکان فیزیکی دیگر بدون وقفه سرویس است. این کار برای دو دلیل انجام می شود: متعادل سازی بار، برخی از دارایی های مجازی دیگر در سیستم مورد حمله قرار می گیرند یا سیستم فیزیکی که میزبان مجازی یک مشکل است، و غیره.

مدل پیشنهادی نیاز به ارزش سیستم در قالب سیا دارد. ما می بینیم که اگر سیستم مورد نظر زندگی می کند به مکان جغرافیایی دیگری منتقل می شود، ارزش CIA آن نمی تواند یکسان باقی بماند. هر مهاجرت زنده هر دو ارزش CIA سیستم فیزیکی و مجازی را تغییر می دهد. برای حل این مشکل، محرمانه بودن هر یک از میزبان، یکپارچگی و

مقادیر در دسترس در یک پایگاه داده ذخیره می شود. هنگامی که یک ماشین مجازی جدید ایجاد می شود، ارزش CIA به آن بسته به سطح خدماتی که مستاجر نیاز دارد و همچنین سیاست هایی که ارائه دهنده ابر ارائه می دهد، داده می شود. بنابراین، هنگامی که در زیربنای ابری داده می شود، بر اساس اهمیت CIA ارزش CIA را ارائه می دهد. وقتی سیستم مهاجرت می کند، ارزش CIA آن بسته به نوع دیگر تغییر می کند

سیستم های مجازی در مکان فیزیکی. با ذخیره این مقادیر در پایگاه داده، اهمیت رایانه که در طول زمان تغییر می کند، می تواند تعیین شود. با توجه به مقیاس رایانش ابری، می توان گفت که اندازه پایگاه داده به سرعت افزایش می

یابد. ابزار بانک اطلاعاتی Round Robin (ابزار RRD) می تواند برای حل این مشکل استفاده شود. چه ابزار RRD آن را به عنوان داده ها می شود بزرگتر؟ میانگین یک مجموعه ای از امتیازات را می گیرد و این میانگین را به یک نقطه واحد کاهش می دهد. هنگامی که داده یک ساله است، به عنوان مثال فقط میانگین هفتگی به جای میانگین روزانه از داده های قدیمی مورد نیاز است.

اساسا، هفت امتیاز به یک نقطه کاهش می یابد. بنابراین، از آنجا که داده ها بزرگتر و مسن تر می شوند، ممکن است کمتر دقیق باشند، اما هنوز هم می توانیم اطلاعات کافی از آن بازیابی کنیم. و قطعا بهتر از هیچ داده ای نیست.

3-3مقایسه ریسک

مدل ما تاثیر خطرات را به عنوان مقدار کمی محاسبه می کند، به همین دلیل، بر خلاف سایر مدل ها، می توان از آن برای مقایسه خطرات استفاده کرد. این می تواند برای تعیین ریسک مهم تر از دیگران باشد. این کار با استفاده از: ارزش سیستم در دست ارائه دهنده همانطور که در فرم (VC CIA، VI، VA) نشان داده شده توسط ضریب تاثیر ریسک بر روی میزبان در شکل (LC CIA، LI، LA) . کل محصولات با زیر نمره بهره وری (Efac) که می توان از پایگاه اطلاعات آسیب پذیری کسبکرد

$$E_{fac} * ((L_C * V_C) + (L_I * V_I) + (L_A * V_A)) \quad (1)$$

با استفاده از این مقادیر کمی، حملات به سیستم هدف می تواند با یکدیگر مقایسه شود. علاوه بر این، ما می توانیم اهمیت خطرات مشابه بین مدل سرویس ابر (SaaS، PaaS و غیره) را با یکدیگر مقایسه کنیم، به عنوان مثال اگر خطرات به عنوان v، w، x، y، z تعریف می شوند، بر اساس مقدار خطرات SaaS می تواند از x، y، z و PaaS آسیب بیشتری وارد کند، می تواند از v، z، w بیشتر آسیب برساند.

3-4محاسبه ماتریس مزایا

برای محاسبه بازده بازیکن، هزینه و سود باید در نظر گرفته شود. اگر Ukl a فرض شود که تابع ویژگی مهاجم را نشان دهد، Bkl a به نفع مهاجم است. هزینه حمله توسط Ckl a نشان داده شده است. نمادهای k و l نشان می

دهد که مهاجم استراتژی kth را در فضای استراتژی مهاجم انتخاب می کند؛ به همین ترتیب، مدافع استراتژی lth در فضای استراتژی مدافعان را انتخاب می کند. به همین ترتیب، Ukl d نشان دهنده تابع مفید مدافع است، Bkl d نشان دهنده سود مهاجم است و Ckl d نشان دهنده هزینه اقدامات امنیتی است. و دوباره نمادها k و l نشان می دهند که مهاجم استراتژی kth را در فضای استراتژی مهاجم انتخاب می کند؛ به همین ترتیب، مدافع استراتژی lth در فضای استراتژی مدافعان را انتخاب می کند.

تعریف 3:توابع مطلوبیت:

$$U = B - C \qquad (2)$$

$$U_{kl}^{a} = B_{kl}^{a} - C_{kl}^{a} \qquad (3)$$

$$U_{kl}^{d} = B_{kl}^{d} - C_{kl}^{d} \qquad (4)$$

3-5 مزیت مدافع

در طبقه بندی حمله، ما پیشنهاد می کنیم که یک حمله می تواند به خواص CIA دارایی آسیب برساند. اگر سطح آسیب به دارایی توسط LC، LI، LA و ارزش دارایی در نظر ارائه دهنده ابر ارائه شده توسط VC، VI، VA نشان داده شده است، پس از آن ضرب آنها نشان می دهد چقدر ارزش دارایی در وقوع یک حمله از دست می رود. اگر دارایی با استفاده از یک معیار امنیتی بهبود یابد، R به عنوان مقدار بهبودی از حمله با استفاده از یک معیار امنیتی تعریف می شود

$$(R_C * V_C) + (R_I * V_I) + (R_A * V_A)) \qquad (5)$$

در جدول 4، SLD یک استراتژی دفاعی موفق در برابر استراتژی حمله sk است. - SLI نشان دهنده یک اقدام امنیتی ناموفق و یا هیچ اقدام امنیتی برای استراتژی حمله اس اس نیست. هیچ وضعیت حمله ای توسط - sk a نشان داده نمی شود.

جدول 4:مزیت مدافع

Strategy	Benefit
s_k^a, s_l^d	$B_{kl}^d = (R_c - L_c) * V_c + (R_I - L_I) * V_I + (R_A - L_A) * V_A$
$s_k^a, -s_l^d$	$B_{kl}^d = -((L_C * V_C) + (L_I * V_I) + (L_A * V_A))$
$-s_k^a, s_l^d$	$B_{kl}^d = 0$
$-s_k^a, -s_l^d$	$B_{kl}^d = 0$

جدول 5: هزینه مدافع

Strategy	Cost
s_k^a, s_l^d	$C_{kl}^d = C_P + C_M + C_C$
$s_k^a, -s_l^d$	$C_{kl}^d = 0$
$-s_k^a, s_l^d$	$C_{kl}^d = C_P + C_M + C_C$
$-s_k^a, -s_l^d$	$C_{kl}^d = 0$

3-6هزینه مدافع

اقدامات امنیتی که توسط مدافع انجام می شود بر سیستم اثر می گذارد. این هزینه ها بسته به نوع دفاع در جدول 5 تغییر می کند. این هزینه ها عبارتند از:

• هزینه های فرآیند (Cp): شامل زمان صرف شده و منابع رایانشی مورد نیاز برای انجام اقدامات احتیاطی امنیتی.

• هزینه مواد (CM): شامل هزینه مستقیم مواد مورد نیاز برای اندازه گیری امنیت و یا پول است.

• هزینه تداوم سیستم (CC): این هزینه ها آسیب پذیری را در بر می گیرد که اتفاق می افتد زمانی که سیستم مورد نیاز برای تطبیق اقدامات امنیتی بسته شود.

3-7 مزیت مهاجم

مزیت مهاجم از دست دادن سیستم مدافعان است. به عبارت دیگر، از دست دادن ارزش CIA دارایی مدافعان است. اما، همه از دست دادن مدافع می تواند توسط مهاجم به دست آید. برای بیان این، یک کافاکر [0 ∈k،1] تعریف شده است تا نشان دهد که چقدر از دست دادن به نفع مهاجم تبدیل شده است. فرمول سود به عنوان Ba = - k * BD برای مهاجم تبدیل می شود (جدول 6).

3-8 هزینه مهاجم

برای اجرای حمله، مهاجم باید نوع خاصی از تجهیزات (CE) یا زمان (CT) را داشته باشد. در شرایط عادی، مجموع این هزینه های مهاجم است. با این حال، اگر یک اقدام امنیتی انجام شده توسط مدافع حمله را شناسایی کند، مهاجم بسته به نوع حمله قرار می گیرد. مجازات قرار گرفتن در معرض توسط CPE نشان داده شده است (جدول 7).

4-نتایج ازمایشی و مقایسه

برای نشان دادن روش پیشنهادی، یک مطالعه موردی در مورد دو ارائه دهندگان مختلف ابر که از انواع مختلف خدماتی استفاده می کنند، ساخته شده است. این مورد استفاده نهایی از منابع اجاره شده از ارائه دهندگان برای استفاده در کار مربوط به پایگاه داده مورد توجه قرار می گیرد.

تامین کننده SaaS مسئول تقریبا تمام نیازهای امنیتی است، زیرا در مدل SaaS هر دو داده و رایانش در طرف ارائه دهنده انجام می شود. با این حال، ارائه دهنده IaaS عموما مسئولیت دسترسی منابع را نه به سمت امنیت آن انجام می دهد. هنگامی که نقض امنیتی در مدل IaaS اتفاق می افتد، اگر آن را به سایر دارایی های مستاجر گسترش ندهد، این مشکل مستاجر است که دارایی های آن مورد بهره برداری قرار می گیرند. با توجه به این حقایق، مقادیر CIA برای منابع (یا فقط ماشین های مجازی) که در این آزمایش استفاده می شود در جدول 8 آمده است.

جدول 6: مزیتمهاجم

Strategy	Benefit
s_k^a, s_l^d	$B_{kl}^a = k((R_c - L_c) * V_c + (R_l - L_l) * V_l + (R_A - L_A) * V_A)$
$s_k^a, -s_l^d$	$B_{kl}^a = k((L_C * V_C) + (L_l * V_l) + (L_A * V_A))$
$-s_k^a, s_l^d$	$B_{kl}^a = 0$
$-s_k^a, -s_l^d$	$B_{kl}^a = 0$

جدول 7: هزینه مهاجم

Strategy	Benefit
s_k^a, s_l^d	$C_{kl}^a = C_E + C_T + C_{PE}$
$s_k^a, -s_l^d$	$C_{kl}^a = C_E + C_T$
$-s_k^a, s_l^d$	$C_{kl}^a = 0$
$-s_k^a, -s_l^d$	$C_{kl}^a = 0$

4-1 مقایسه ریسک

برای دیدن سطح اهمیت در مدل های سرویس های مختلف، پنج خطرات با یکدیگر در مدل های متفاوت خدمات ابر مقایسه می شوند. این خطرات واقعا آسیب پذیری های واقعی هستند که می توانند یک میزبان در ابر را تحت تاثیر قرار دهند. به خاطر این آزمایش، سطح آسیب های سیا از نمونه ای است که در جدول 2 نشان داده شده است. آسیب پذیری های واقعی در زندگی روزمره برای هر نوع داده می شود. DoS (CVE-2012-1820)، کاربر (CVE-2012-2752)، داده ها (CVE-2012-4579)، مدیر (CVE-2011-4005) و اسکن (CVE-2010- 1638). نمره بهره برداری برای هر ریسک از صفحات مورد نظر به دست می آید. نتایج در جدول 9 نشان داده شده است.

منظور از اهمیت خطراتی که در جدول 9 برای مدل SaaS دیده می شود، متفاوت از مدل IaaS است. برای مدل SaaS، داده ها و نوع مدیریت حملات جدی تر از دیگران است. منظور مهم برای SaaS داده ها، مدیر، اسکن، DoS و کاربر است. با این حال، منظور اهمیت خطرات برای IaaS، DoS، data، admin، user و scan است.

4-2 بازی ریسک

برای این مورد، فرض شده است که هر دو ارائه دهنده CVE-2012-0116 آسیب پذیری در سیستم های خود. به عنوان یک اساس، این آسیب پذیری به عنوان حمله داده شده در جدول 2 درنظر گرفته می شود. بنابراین سطح آسیب آن در شکل CIA برابر با LC = 1، LI = 1، LA = 0، 2. بعضی پارامتر ها به سبب تجربه RC = 1، RI = 1، و Ra = 0، 4.

ما اندازه گیری امنیتی را که می تواند این حمله را متوقف کند هزینه های CP = 60، CM = 70 و CC = 50 را در نظر بگیریم. هزینه های مهاجم CE = 25، CT = 5 برای این نوع حمله. اگر مهاجم به علت اقدامات امنیتی در معرض خطر قرار گیرد، او به عنوان هزینه CPE = 50 هزینه پرداخت خواهد کرد. پس از محاسبه توابع ابزار برای هر دو مهاجم و مدافع، ماتریس های نتیجه در جداول 10 و 11 ارائه شده است.

بر اساس تعادل نش، هر بازی محدود دارای حداقل یک نقطه تعادل است. ماتریس راه حل IaaS نشان داده شده در جدول 10 را می توان با استفاده از بهترین پاسخ حل کرد. اگر مهاجم تصمیم به انجام حمله بگیرد، مدافع هیچ گونه اقداماتی را انتخاب نخواهد کرد، زیرا بیشتر از آن سود می برد. اگر مدافع تصمیم به انجام اقدامات امنیتی نداشته باشد، اجرای حمله بیشتر به مهاجم خواهد بود. (از آنجا که "بدون اندازه" استراتژی غالب برای مدافع است.) از آنجا که این استراتژی اشاره یک سلول (A، NM) در ماتریس، می توان گفت که این یک استراتژی خالص نقطه ناس است.

در این نوع بازی ها، تعادل خالص نها یا تعادل ناس ترکیبی وجود دارد. با نگاهی دقیق به جدول 11 می توان گفت که ماتریس محلول SaaS حاوی استراتژی خالص تعادل نها (NA، NM) است. اما، در این مورد، مهاجم و مدافع هیچ کاری نمی کنند. بنابراین، ما از تعادل ناس استراتژی مخلوط [12] برای تعیین نتیجه بازی استفاده خواهیم کرد. با استفاده از استراتژی مخلوط تعادل نها، معادله. (6) و (7) را می توان تعریف کرد.

$$(-168) * \mathbf{p_A} + (-180) * (1-\mathbf{p_A}) = (-224) * \mathbf{p_A} + (0) * (1-\mathbf{p_A}) \quad (6)$$

جدول 8:ارزش دارایی سرور ها در مدل هایسرویس

	Confidentiality	Integrity	Availability
SaaS system	100	100	60
IaaS system	20	80	100

جدول 9:اثر محاسبه شده ریسک

نوع حمله	امتیاز کل SaaS	امتیاز کل IaaS
DoS	330	550
User	245.7	89.7
Data	1441.6	326.4
Admin	971.8	283.8
Scan	420	80

جدول10: ماتریسحل مدل

		Defender	
		Take measures (TM)	No measures (NM)
Attacker	Attack (A)	−100, −160	110, −140
	No action (NA)	0, −180	0, 0

$$(-92) * \mathbf{p_D} + (194) * (1-\mathbf{p_D}) = (0) * \mathbf{p_D} + (0) * (1-\mathbf{p_D}) \qquad (7)$$

پس از حل معادلات (6) و (7) ما 0 = pA،76 و 0 = pD،68 را بدست آوریم. بنابراین ما می توانیم بگوییم که اگر مدافع حرکت را "اقدامات" را با احتمال 0.68 انتخاب کند، نتیجه مهاجم بین حمله و اعمال هیچ گونه تفاوتی نمی کند. بنابراین، از لحاظ دیدگاه مهاجم، حمله و اقدام بدون نتیجه همان نتایج را دارد. به همین ترتیب، اگر مهاجم تصمیم به اجرای حمله با احتمالی 0.76 را انتخاب کند، نتیجه مدافع تغییر نخواهد کرد و اگر اقدامات انجام شود یا نه.

به عبارت دیگر، اگر مدافع در 68٪ از کل سیستم اندازه گیری کند، مهاجم از حمله استفاده می کند. به همین ترتیب، از دیدگاه مدافع، اگر بگوئیم بیش از 76٪ از کل سیستم ها مورد حمله قرار گرفته اند، اقدامات امنیتی هزینه بیشتری نسبت به انجام هیچ عملیاتی ندارد.

4-3انتظارزیان سالانه

یکی از رایج ترین روش ها برای ارزیابی خطر، انتظارات از دست دادن سالانه (ALE) است. ALE نشان دهنده از دست دادن ارزش سهام مورد انتظار به دلیل خطر بیش از یک سال است.

$$ALE = SLExARO \qquad (8)$$

ALE ضرب از انتظارات تنها ضرر و زیان (SLE) و نرخ سالانه نرخ (ARO) است. سیستم ارائه شده در جدول 11 نشان می دهد که انجام اقدامات امنیتی در 68٪ از سیستم، نتیجه مهاجم تغییر نمی کند که آیا او حمله کرده یا نه. ما می توانیم از ALE استفاده کنیم تا از دست رفتن 32٪ از سیستم محافظت نشده. اگر سیستم از دست رفته محافظت نشده بزرگتر از هزینه های اقدامات امنیتی برای این سیستم باشد، بقیه سیستم نیز تحت حفاظت قرار می گیرد.

4-4 مقایسه با روش های دیگر

ما می توانیم هر نوع خدمات داده شده را در روش ما جدا کنیم. بنابراین، خدمات ابری را می توان فراتر از دو نوع که توسط M. Kiran و همکاران تعریف شده است. در [7 ref]. همانطور که قبلا ذکر شد، مدل های بیشتری از NIST تعریف شده مانند؛ SaaS که برای پشتیبان گیری از داده ها استفاده می شود، NaaS است که برای اجاره دارایی های شبکه و DaaS استفاده می شود که رایانش و داده های مشتری را در ابر قرار می دهد و داده ها را به مشتری هنگامی که مشتری نیاز دارد. اگر ارائه دهنده خدمات در [7 ref] تعریف شده به عنوان یک ارائه کننده SaaS دیده شود، بقیه خدمات به عنوان یک تهیه کننده زیرساخت در نظر گرفته می شود که اختلاف اختیاری بین IaaS و STaaS را نادیده می گیرد. در روش ما، ما هر مدل خدماتی را که می توان از چنین خطری آسیب دید، مقایسه می کنیم، با یکدیگر به شیوه مقیاس پذیر.

به طور کلی، روش های ارزیابی ریسک به مدت طولانی طول می کشد و به آرامی پردازش می شود. بر خلاف روش های دیگر، روش ما یک بازی را از اثرات خطراتی که ما می توانیم با استفاده از نظریه ی بازی حل کنیم، ایجاد می کنیم. همچنین با استفاده از تاریخ ارائه دهنده، روش ما می تواند تعیین کند که چه دارایی مورد حمله قرار می گیرد. مدل ما سرعت و ارائه رایانش خاص را تضمین می کنیم

5-نتیجه گیری و کار های اینده

تطبیق سریع رایانه ابری همچنین مشکلات امنیتی را با آن به ارمغان می آورد [13]. روشهای ارزیابی ریسک امروز برای رایانش ابری هزینه و مزایای مهاجمان و مدافعان را مطرح نمیکنند. کار ما تلاش می کند مشکل حل تصمیم گیری یک استراتژی ایده آل را برای اقدامات امنیتی هنگام استفاده از رایانه های ابری حل کند. روش پیشنهادی از تئوری بازی استفاده می کند تا نتیجه مدافع و مهاجم را مدل کند. ما استراتژی ایده آل مدافع را با استفاده از ارزش دارایی در چشم ارائه دهنده ابر و خطراتی که می تواند به دارایی رخ دهد، محاسبه کنیم. مدل ما را می توان با محاسبه خطرات مختلف در یک زمان گسترش داده و قرار دادن این اعداد در یک ماتریس راه حل. با استفاده از این روش می توانیم اقدامات مختلف امنیتی را محاسبه کنیم که می تواند نوع خطرات را کاهش دهد. همچنین این راه،

اگر هزینه های امنیتی دیگری کاهش یابد، می توانیم آن را انتخاب کنیم. پارامترهایی که عملکردهای ابزار را تشکیل می دهند، نیاز به برخی کارها برای ارائه پاسخ بهتر دارند. به ویژه، تاریخ ارزش CIA که توسط ابر ارائه شده است بسیار مهم است، زیرا به طور مستقیم بر اثربخشی مدل ما تاثیر می گذارد.

References

[1] P. Mell, T. Grance, The NIST definition of cloud computing, National Institute of Standards and Technology Special Publication 800–145, 2011.
[2] B. Wang, J. Cai, S. Zhang, J. Li, A network security assessment model based on attack-defense game theory, International Conference on Computer Application and System Modeling (ICCASM), 2010, (Taiyuan Shanxi, China).
[3] J. Pita, M. Jain, J. Marecki, Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport, 2008. (Estoril, Portugal).
[4] S. Shiva, S. Roy, D. Dasgupta, Game theory for cyber security, Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '10), ACM, 2010, (New York, NY, USA).
[5] R.J. Lipton, V.V. Vazirani, M. Mihail, C. Tovey, E. Vigoda, Algorithmic game theory, 2007.
[6] J.A. Kupsch, B.P. Miller, E. Heyman, E. César, First principles vulnerability assessment, Proceedings of the 2010 ACM workshop on Cloud computing security workshop CCSW '10, 2010, (New York, NY, USA).
[7] L. Peiyu, L. Dong, The new risk assessment model for information system in cloud computing environment, Procedia Eng. 15 (2011) 3200–3204.
[8] J.O. Fitó, J. Guitart, Business-driven management of infrastructure-level risks in Cloud providers, Futur. Gener. Comput. Syst. 32 (2014) 41–53.
[9] M. Kiran, M. Jiang, D.J. Armstrong, K. Djemame, Towards a service lifecycle based methodology for risk assessment in cloud computing, Dependable, Autonomic and Secure Computing (DASC), Dec 2011, pp. 449–456.
[10] CVSS v2 vector definitions, http://nvd.nist.gov/cvss.cfm?vectorinfo&version=2.
[11] National vulnerability database version 2.2, http://nvd.nist.gov/.
[12] M.J. Osborne, An introduction to game theory, Oxford University Press, USA, 2003.
[13] Cloud Security Alliance, Security guidance for critical areas of focus in cloud computing 3.0, https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.
[14] T. Alpcan, T. Başar, Network security: a decision and game theoretic approach, Cambridge University Press, Jan. 2011.
[15] M. Tambe, Security and game theory: algorithms, deployed systems, lessons learned, Cambridge University Press, Dec. 2011.
[16] T. Spyridopoulos, G. Karanikas, T. Tryfonas, G. Oikonomou, A game theoretic defense framework against DoS/DDoS cyber attacks, Comput. Secur. 38 (2013) 39–50.
[17] M.H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, J.-P. Hubaux, Game theory meets network security and privacy, ACM Comput. Surv. 45 (3) (2013) 25:1–25:39.
[18] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Futur. Gener. Comput. Syst. 28 (2012) 583–592.
[19] C.Y.T. Ma, N.S.V. Rao, D.K.Y. Yau, A game theoretic study of attack and defense in cyber-physical systems, Infocom Workshops, 2011.
[20] G. Fan, H. Yu, L. Chen, D. Liu, A game theoretic method to model and evaluate attack-defense strategy in cloud computing, IEEE 10. Int. Conference on Services Computing (SCC), 2013, pp. 659–666.