بررسی تأثیرات چالش‌های امنیتی رایانش‌ابری بر زیرساخت‌های NFV و راه‌حل‌های کاهش مخاطرات

امیرحسین پورشمس*[1]، محمد رضا حسنی آهنگر[2] و محمود صالح اصفهانی[3]

[1]دانشجوی کارشناسی ارشد، گروه کامپیوتر، دانشگاه جامع امام حسین (ع)، تهران، ایران
ahpourshams@ihu.ac.ir

[2] استاد، گروه کامپیوتر، دانشگاه جامع امام حسین(ع)، تهران، ایران
mr.hasani@ihu.ac.ir

[3] استادیار، گروه کامپیوتر، دانشگاه جامع امام حسین(ع)، تهران، ایران
masaleh@ihu.ac.ir

چکیده

افزایش سرعت انتقال داده‌های پهن‌باند به گیگابیت برای مشتریان و هزینه‌های تأمین منابع آن همچنین ضرورت تأمین سطح سرویس کیفی قابل توافق، استفاده از مجازی‌سازهای المان‌های مجازی‌شده شبکه را اجتناب‌ناپذیر کرده است؛ از این‌رو شناسایی و بررسی چالش‌های امنیتی این نوع مجازی‌سازها به‌همراه راه‌حل‌های ممکن برای رفع چالش‌ها به‌منظور پوشش نگرانی‌های امنیتی هم‌زمان با توسعه آن ضروری است. نسل بعدی شبکه‌های مخابراتی (5G) مبتنی بر دو فناوری کلیدی مجازی‌سازکاربردهای‌شبکه و شبکه‌نرم‌افزارمحور خواهد بود و به‌کارگیری هر کدام از این فناوری‌ها، فرصت‌ها و تهدیداتی را به‌دنبال خواهد داشت. در این میان توجه به چالش‌های امنیتی رایانش ابری در کنار چالش‌های موجود زیرساخت‌های NFV به‌منظور استخراج وابستگی‌ها و ارائه راه‌حل‌های رفع آن ضروری است. در این مقاله پس از معرفی متدولوژی محاسبات ابری و فناوری مجازی‌سازی و مجازی‌ساز کاربردهای شبکه، چالش‌های امنیتی شناخته‌شده برای آنها با یک نگاه تطبیقی-مقایسه‌ای، با توجه به تهدیدات زیرساخت‌های رایانش ابری مورد مطالعه و بررسی قرار خواهد گرفت؛ همچنین در ادامه ضمن ارائه راه‌حل‌های طرح‌شده برای آن، مقایسه کاربردی هر یک از راه‌حل‌ها بیان خواهد شد.

واژگان کلیدی: مجازی سازکاربردشبکه، پشته باز، چالش های امنیتی، راه حل های امنیتی، چالش‌های امنیتی رایانش ابری

۱- مقدمه

در شبکه‌های سنتی مخابرات، افزودن یک مؤلفه شبکه جدید در معماری نیازمند تأمین سخت‌افزاری و نصب فیزیکی در محل‌های تعبیه‌شده بود؛ علاوه‌بر آن توسعه پیوسته نسل‌های مخابراتی و تأمین ظرفیت مورد نیاز سرویس‌دهی، افزایش هر روزه تجهیزات، تأمین هزینه‌های نصب و راه‌اندازی و پیچیده‌شدن معماری شبکه را به‌دنبال داشت [۱ و ۲]. امروزه شبکه‌های مخابراتی به‌سرعت در حال توسعه بوده و ضروری است زیرساخت‌های سخت‌افزاری و نرم‌افزاری آن نیز هم‌زمان توسعه یابند [۲]. در این میان زیرساخت‌های مجازی‌سازی مخابراتی به‌دلیل فراهم‌آوری ساختاری انعطاف‌پذیر، پویا و کم‌هزینه در طراحی، مورد توجه بسیاری از تأمین‌کنندگان زیرساخت‌های ارتباطی قرار گرفته است.

مجازی‌سازهای‌کاربردهای‌شبکه[1] (NFV) با ایجاد مؤلفه‌های شبکه به‌صورت نرم‌افزاری بر روی بستر مجازی‌سازی زیرساخت‌های مخابراتی توانسته‌اند بسیاری از مشکلات شبکه‌های قدیمی از جمله وابستگی توسعه و ارتقای به خرید سخت‌افزار، هزینه بالای توسعه و عدم پویایی توزیع منابع را برطرف کند [۳]. مجازی‌سازی که یکی از اصلی‌ترین کارکردهای رایانش ابری به‌منظور توزیع ابر منابع برای مؤلفه‌ها است، توانسته است با فراهم‌آوری شرایط پویا اختصاص و توزیع منابع به‌همراه سادگی در اختصاص آنها، توسعه کارکردهای شبکه را آسان کند. در این میان تهدیدات امنیتی لایه‌های مختلف که این بستر را فراهم می‌کنند بر اساس تأثیرگذاری آنها ضروری است، مورد بررسی قرار گیرند.

[1] Network Function Virtualization

*نویسندهٔ مسؤول

۱-۱- رایانش ابری

رایانش ابری یک راه حل کارآمد برای ایجاد سرویس اشتراکی منابع با هزینه پایین‌تر، به‌محض‌درخواست[1] و اختصاص منابع به‌صورت پویا را نسبت به ساختارها و منابع فیزیکیِ محلی فراهم می‌آورد. این منابع در کمینه زمان و به‌سرعت مدیریت می‌شود و در سه سطح مدل سرویس زیرساخت، بستر و نرم‌افزار ارائه می‌شوند [۴]. به‌عبارت دیگر ساختارهای رایانش ابری یک بستر مبتنی بر شبکه از نگاه کاربر را ایجاد می‌کند که مسیری به‌منظور اشتراک منابع رایانشی، ذخیره‌سازی و شبکه‌ای را فارغ از محل قرارگیری فراهم می‌آورد.

مؤسسه ملی فناوری و استانداردها[2] ساختار رایانش ابری را این‌گونه تعریف می‌کند"یک قالب برای فراهم‌کردن دسترسی مناسب و درصورت نیاز، اینترنتی به مجموعه از منابع شبکه‌ای[3] قابل برنامه‌ریزی، منابع ذخیره‌سازی، سرویس‌دهنده که به‌صورت پویا و با کمترین مدیریت و نظارت از طرف فراهم‌کننده قابل تغییر باشد. این استاندارد یک مدل هماهنگ‌سازی سرویس سه‌سطحی را پیشنهاد می‌دهد [۵].

- لایه سخت‌افزاری شامل همه منابع رایانشی (CPU، Memory)، منابع شبکه‌ای (Firewall، Router، Switches)، منابع ذخیره سازی (Hard Disk) و ...
- لایه کنترل و انتزاع منابع شامل همهٔ اجزای سیستم، که فراهم‌کننده ابری به‌منظور اختصاص و مدیریت دسترسی به منابع سخت‌افزاری و رایانشی توسط لایه مجازی‌سازی مورد استفاده قرار می‌دهد.
- لایه سرویس شامل همه واسط‌هایی است که ارائه‌دهنده سرویس‌های ابری به‌منظور فراهم‌آوری دسترسی بهره‌برداران به سرویس‌های رایانشی و منابع فراهم می‌آورند.

رایانش ابری دارای چهار مدل توسعه‌ای از جمله ترکیبی[4]، ارتباطی[5]، خصوصی و عمومی همچنین سه مدل سرویس PAAS[6]، به‌عنوان سرویس‌دهنده بستر، IAAS[7] به‌عنوان سرویس‌دهنده زیرساخت و SAAS[8] به‌عنوان سرویس‌دهنده خدمات برای این زیرساخت قابل ارائه است. آنچه NIST عنوان کرده در شکل (۱) قابل مشاهده است.

(شکل-۱): چارچوب ساختارهای ابری تعریف‌شده توسط NIST

۲-۱- مجازی‌سازی

مجازی‌سازی[9] فناوری کلیدی در رایانش ابری است. این فناوری توسط تسهیم، تجمیع و شبیه‌سازی منابع فیزیکی، مجازی‌سازی آن‌ها را با ایجاد واسط‌های مربوطه انجام می‌دهد [۴]. مؤلفه‌های اصلی مجازی‌سازی عبارت از ماشین‌مجازی، هایپروایزر[10] و شبکه مجازی است که در زیر شرح داده شده است [۷].

- ماشین مجازی: یک سامانهٔ نرم‌افزاری شبیه سیستم سخت‌افزاری که محیطی را به‌منظور به‌کارگیری سیستم‌های عامل و نرم افزار فراهم می‌آورد.
- هایپروایزر: تجریدی[11] از منابع فیزیکی مانند پردازنده، حافظه موقت، ذخیره‌ساز و شبکه که امکان به‌کارگیری چندین سیستم‌عامل به‌صورت هم‌زمان را بر روی یک مجموعه سخت‌افزاری فراهم می‌آورد. این مؤلفه به‌صورت مستقیم بر روی سخت‌افزار و یا بخشی از Host به‌کار گرفته می‌شود.
- شبکه مجازی: این مؤلفه امکان ارتباط مجازی میان مؤلفه‌های مجازی ایجادشده را توسط سوئیچ‌های مجازی فراهم می‌آورد.

۳-۱- تفاوت رایانش ابری و مجازی‌سازی

مجازی‌سازی یک فناوری جداکننده نقش‌ها از سخت‌افزار است؛ درحالی که رایانش ابری متکی بر این جداسازی است و هر دوی آنها به ایجاد یک محیط مناسب تجرید منابع می‌پردازند. به‌عبارت دیگر رایانش ابری یک متدولوژی و

[1] On-Demand
[2] National Institute of Standards and Technology (NIST)
[3] Grids
[4] Hybrid
[5] Community
[6] Platform as a Service
[7] Infrastructure as a Service
[8] Software as a Service
[9] Virtualization
[10] Hypervisor
[11] Abstraction

مجازی‌سازی یک فناوری است. هدف اولی ارائه روش فراهم‌کردن منابع برای استفاده در زمان نیاز و هدف دومی ارائه فناوری بهره‌برداری از منابع ایجاد شده است [۸]. جدول (۱) تفاوت‌های اساسی رایانش ابری و مجازی‌سازی را ارائه می‌کند.

(جدول-۱): مقایسه رایانش ابری و مجازی‌سازی

	مجازی‌سازی	رایانش ابری
تعریف	فناوری	متدولوژی
هدف	ایجاد چندین محیط شبیه‌سازی‌شده از یک محیط مجازی	مجتمع و خودکارسازی منابع مجازی برای درخواست در زمان نیاز
استفاده	ارائه منابع بسته‌ای به کاربران خاص برای اهداف خاص	ارائه منابع متغیر مختلف به گروهی از کاربران برای اهداف متفاوت
پیکربندی	مبتنی بر تصویر	مبتنی بر قالب
مقیاس‌پذیری	Scale up	Scale out
حجم‌کاری	Stateful	Stateless

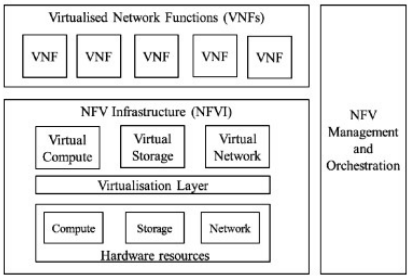
۴-۱- مجازی‌ساز کارکرد شبکه

مجازی‌ساز کارکرد شبکه پیاده‌سازی نرم‌افزاری یک کارکرد اجرایی شبکه[1] است که بر بستر رایانشی، ذخیره‌سازی و شبکه‌ای مجازی‌شده پیاده‌سازی می‌شود. در این ساختار تعداد کارکرد مجازی‌سازی‌شده[2] بدون وابستگی به سخت‌افزار و بر اساس معماری‌ها و نیازمندی‌های تعریف‌شده در استاندارد ETSI پیاده‌سازی شده و برای توسعه آنها نیازی به افزودن سخت‌افزارهای جدید نیست. مزیت اصلی NFV جداسازی زیرساخت نرم‌افزاری از کارکرد نرم‌افزاری است. این جداسازی عدم وابستگی تغییر نسل کارکردهای شبکه، اشتراک و استفاده توزیعی را از منابع و پویایی در اختصاص منابع به سخت‌افزار به‌دنبال دارد. براساس چارچوب تدوین‌شده توسط ETSI، این ساختار در سه سطح مطابق شکل (۲) تعریف شده است [۶]:

- کاکرد مجازی‌سازی‌شده که شامل فعالیت اجرایی سرویس شبکه است و به‌صورت نرم‌افزاری تعریف شده است.
- زیرساخت مجازی‌ساز کارکردشبکه[3] که شامل همه سخت‌افزارهایی است که به یک مجازی‌ساز اختصاص یافته تا نقش خود را ایفا کند.

[1] Network Function
[2] Virtualized Network Function (VNF)
[3] NFV infrastructure (NFVI)

- مدیریت و هماهنگ‌کننده مجازی‌ساز عملکرد شبکه[4] از جمله ایجاد یک VNF جدید و مدیریت چرخه حیات آن را بر عهده دارد.



(شکل-۲): چارچوب ساختارهای ابری تعریف شده توسط NIST

از آنجا که کارکردهای‌شبکه از ساختارهای فیزیکی و متکی‌به‌خود به ساختارهای مجازی متکی به زیرساخت اشتراکی تبدیل می‌شوند، تهدیدات امنیتی جدید نیز برای آنها ممکن خواهد بود و تحت تأثیر قرارگرفتن یک مؤلفه می‌تواند دیگر مؤلفه‌ها و زیرساخت را تحت تأثیر قرار دهد. مطابق مؤسسه ملی فناوری و استانداردها، پنج سطح بهره‌برداری برای NFV تعریف شده است [۱۴].

- ارائه زیرساخت NFV به‌عنوان سرویس: قابلیت ارائه منابع ذخیره‌سازی اولیه، منابع شبکه‌ای، توانایی‌های محاسباتی و دیگر منابع پایه رایانشی است که برای ارائه سرویس دلخواه شبکه‌ای به مشتریان بدون نیاز به کنترل لایه پایینی زیرساخت فراهم شده است. در این مدل یک نیازمند سرویس شبکه‌ای می‌تواند نمونه‌های[5] VNF را بر روی یک ارائه‌کننده زیرساخت توسعه دهد.
- ارائه پلتفرم NFV به‌عنوان سرویس: ارائه یک پلتفرم و مجموعه‌ای از زیرساخت‌ها و برنامه‌های کاربردی که بهره‌بردار می‌تواند کارکردهای شبکه خود را بر اساس نیاز در آن ایجاد و توسعه دهد. پلتفرم، امکان مدیریت، کنترل و اعمال پیکربندی بر اساس نیاز را فراهم می‌آورد؛ بنابر این معماری شبکه بر اساس برنامه‌ها و سرویس‌های موجود در پلتفرم توسط بهره‌بردار توسعه و طراحی می‌گردد.
- ارائه NVF به‌عنوان سرویس: در این مدل بهره بردار به‌عنوان گیرنده کارکردهای سرویس مخابراتی ایجاد و فعال‌شده بر روی پلتفرم تلقی می‌شود. در این مدل بهره‌بردار تنها قادر به پیکربندی سطح کارکرد بدون امکان دسترسی به سطح زیرساخت و یا تغییرات پلتفرم است.

[4] NFV management and orchestration (MANO)
[5] Instances

- مجازی‌سازی هسته شبکه موبایل[1] و ایستگاه پایه[2]: در این نوع ارائه خدمت، سرویس‌های موبایل مانند IMS[3]، ایستگاه پایه موبایل، EPC[4]، HSS[5] و دیگر سرویس‌های مورد نیاز به‌همراه بخش‌هایی از سرویس ارائه زیرساخت رادیویی بر اساس معماری مورد نیاز بهره‌بردار ارائه می‌شود.
- مجازی‌ساز مؤلفه دسترسی شبکه ثابت[6]: در این مدل سرویس‌دهندگان مختلف شبکه ثابت می‌توانند منابع خود را برای کاهش هزینه‌ها با یکدیگر به اشتراک بگذارند؛ بنابراین، شبکه‌های ترکیبی DSL[7] با ایده جداسازی سطح کنترل از سطح داده شکل گرفته است که به‌وسیلهٔ NFV کنترل می‌شود.

در بخش نخست این مقاله، چالش‌های امنیتی عنوان‌شده برای رایانش ابری، مجازی‌سازها و NFV به‌همراه برخی از حملات از جمله منع‌سرویس، حملات نقض جامعیت و محیط اعتماد شبکه، استفاده ناپسند از منابع، تغییر در کارکرد، تغییر سطح اختیارات، نقض محرمانگی از طریق‌منابع اشتراکی و حملات داخلی به‌همراه دیگر حملات ممکن‌الاجرا مورد بررسی قرار خواهد گرفت؛ همچنین در بخش دیگری ضمن مقایسه و تطبیق چالش‌های مختلف امنیتی رایانش ابری و حملات ممکن مجازی‌سازی در یک نمایش، تلاش می‌شود تأثیرات چالش‌های امنیتی رایانش ابری بر مجازی‌سازی، حملات ممکن ناشی از آن بر اساس بردارهای‌حمله و سپس در بخش پایانی ضمن طرح راه‌حل‌های ارائه‌شده توسط پژوهش‌گران این حوزه و مقایسه کاربردی آن، نتیجه‌گیری بررسی انجام شده ارائه شود.

تمایز این بررسی نسبت به دیگر بررسی‌های صورت‌گرفته این است که علاوه‌بر طرح چالش‌های مرتبط با زیرساخت‌های NFV، چالش‌های مربوط به رایانش ابری که بر زیرساخت‌های NFV تأثیرگذار هستند نیز ارائه شده است.

۲- چالش‌های امنیتی

چالش امنیتی عبارت است از هر آنچه در هر یک از دارایی‌ها منجر به حمله سایبری شود که از جمله آن می‌توان به نقض در پیکربندی، خطا در روال‌ها و فرآیندها، ضعف در سازوکارهای امنیتی و ضعف در پیاده‌سازی صحیح کاربردها اشاره کرد. هدف از طرح چالش‌های امنیتی در این بخش استخراج و ارائه چالش‌هایی است که بر اساس مشخصه‌های رایانش ابری و مجازی‌سازی اختصاصی شده‌اند.

۱-۲- چالش‌های امنیتی رایانش ابری

آنچه مفاهیم تهدیدات و چالش‌های امنیتی در رایانش ابری همچنین پایش و تشخیص حملات را از مفاهیم ساختارهای سنتی متمایز و دشوارتر می‌کند، اشتراک و توزیع‌شدگی منابع و روش‌های اختصاص آن است [۲۸]. به‌طور کلی چالش‌های امنیتی ساختارهای رایانش ابری به هفت دسته کلی ذخیره‌سازی و رایانش داده، مجازی‌سازی، واسط‌های ارتباطی، شبکه، نرم‌افزار، مدیریت اعتماد همچنین تابعیت و حاکمیت قابل تقسیم است [۸،۹،۱۰]. در کنار سطوح ارائه‌شده، مؤسسه ملی فناوری و استانداردها نیز در سندی به‌عنوان راهنمای امنیت و حریم خصوصی در رایانش ابری عمومی، نه محور امنیتی را عنوان کرده که عبارتند از حاکمیت، تابعیت، اعتماد، معماری، مدیریت دسترسی و اصالت‌سنجی، ایزوله‌کردن نرم‌افزار، محافظت داده، دسترسی‌پذیری و پاسخ‌گویی به رخدادهای امنیتی [۳،۱۱]. آنچه در بخش‌های بعدی مورد بررسی قرار خواهد گرفت، عبارت است از تهدیداتی که در ساختارهای مجازی‌ساز کارکرد شبکه تأثیرگذار خواهد بود.

۱-۱-۲- چالش‌های ذخیره‌سازی و رایانش داده‌ها

داده‌ها یکی از بخش‌های حیاتی رایانش ابری هستند. آنها ممکن است در محسبات به‌کار گرفته‌شده و یا برای کاربردهای مختلف به‌صورت ایزوله‌شده و نفوذناپذیر ذخیره شوند. نشت داده‌ها اغلب در زمان تغییر و یا رایانش به وقوع می‌پیوندد؛ لذا داده‌ها باید در طول هر مرحله از رایانش محرمانه باقی بمانند [۸،۱۰]. بخشی از مهم‌ترین چالش‌های امنیتی داده‌ها عبارتند از:

- ذخیره داده: از آنجا که ذخیره‌ساز رایانش ابری یک منبع اشتراکی از محل‌های مختلف داده‌ها را ارائه می‌کند و محل فیزیکی ذخیره داده‌ها ممکن است توزیع شود، ساختارهای رایانش ابری برای کنترل کامل و پایش دسترسی به داده با چالش مواجه بوده و نقض کنترل دسترسی به داده چالش منجر به نشت داده در این بخش است. مهم‌تر آنکه برای حفظ داده‌ها، پشتیبان آنها نیز در نقاط مختلف با سیاست‌ها و رویه‌های متفاوت ذخیره و احتمال نقض سیاست و به‌دنبال آن نشت داده‌ها وجود دارد [۳،۸،۱۰].

[1] Mobile Core Network
[2] Mobile Base Station
[3] IP Multimedia Subsystem
[4] Evolved Pocket Core
[5] Home Subscriber Server
[6] Fixed Access Network
[7] Digital Subscriber Line

- محاسبات غیرقابل اعتماد: یکی از چالش‌های رایانش ابری، دشواری در یافتن سرویس‌دهنده‌های رایانشی قابل اعتماد، دقیق و امین[1] است که نتایج درست و قابل اعتماد را در پاسخ به درخواست‌های ارسال‌کننده ارائه می‌کند. درصورتی‌که محیط اجرایی جامعیت[2] داده‌ها را نتواند تضمین کرده و در زمان اجرا محرمانگی و یا جامعیت آن دچار نقض شود، اعتماد رایانشی وجود نخواهد داشت. این جامعیت در سطح سخت‌افزار، سطح مشتری-میزبان، سطح شبکه و یا در زمان استفاده از تجهیزات امنیتی طرح می‌شود [۸،۹،۱۱].
- دسترسی‌پذیری داده و سرویس: ایجاد اختلال در منابع سخت‌افزاری با توجه به امکان ایجاد زنجیره اختلال در سطح سرویس‌دهنده‌ها یکی از مهم‌ترین اهداف مهاجمان است. همچنین در سطح سرویس نیز زمانی که نقاط و سطح دسترسی‌پذیری افزایش می‌یابد، حملات به‌کارگیری و مصرف منابع به‌منظور اختلال سرویس نیز افزایش می‌یابد [۸،۱۰].
- محرمانگی: سازوکارهای رمزنگاری به‌منظور حفظ اطلاعات در سطوح مختلف رایانش ابری به کار می‌روند. محرمانگی در محاسبات ابری به دو عنصر الگوریتم و نحوه پیاده‌سازی آن همچنین کلید و نگهداری آن وابسته است. ضعف در هرکدام از الگوریتم و انتشار کلید می‌تواند داده‌ها را به مخاطره اندازد [۱۰،۱۵].
- بازیابی داده‌ها: از آنجا که فضای ابری در بازه‌های مختلف در اختیار منابع مختلف قرار می‌گیرد و داده‌ها را در فضاهای توزیع‌شده ذخیره‌سازی می‌کند، باید اطمینان حاصل شود که داده‌های سابق یک مؤلفه در زمان اختصاص به مؤلفه دیگر به‌خوبی حذف و تمام یا بخشی از آن نیز قابل بازیابی نباشد [۳،۸،۱۰].
- پشتیبان داده‌ها: یکی از فرآیندهای مهم در رایانش ابری، پشتیبان‌گیری از داده‌ها به‌منظور حفظ دسترسی‌پذیری آن است؛ لذا چگونگی حفظ پشتیبان داده‌ها، دسترسی‌پذیری آنها و محافظت از حملاتی که منجر به حذف پشتیبان می‌شود، مورد اهمیت است.

۲-۱-۲- چالش‌های مجازی‌سازی

چالش‌های ذخیره‌ساز در چهار سطح ماشین‌مجازی، مجازی‌ساز، زیرساخت فیزیکی، مدیریت و پایش قابل بررسی است[۸،۱۰]. به‌طور کلی یک مفهوم مهم در امنیت مجازی‌سازی این است که تفکیک و ایزوله‌سازی به‌طور کامل میان نمونه‌های مختلف انجام پذیرفته باشد.

۱-۲-۱-۲- ماشین مجازی

چرخهٔ حیات[3] یک نمونه ماشین‌مجازی می‌تواند در وضعیت‌های متفاوتی از جمله ایجاد، انتظار، درحال اجرا، تعلیق، ازسرگیری، خاموش، متوقف و یا حذف شده باشد. [۳]. چالش‌های امنیتی که در طول این چرخه صورت می‌پذیرد، عبارت از موارد زیر است:

- رونوشت ماشین‌مجازی: فرآیند رونوشت یا انتقال یک ماشین مجازی موجود با شناسه، نام، نشانی پروتکل IP[4]، نشانی MAC[5] و نشانی‌های تخصیصی یکسان به بستر دیگر یا همان بستر موجود است. در زمان رونوشت اطلاعات، کلیدها و داده‌های متعلق به بهره‌بردار ممکن است، به سرقت برود. همچنین از آنجا که دیگر ماشین‌های مجازی به این ماشین و وضعیت اولیه آن اعتماد کرده‌اند، ممکن است از آن سوء استفاده صورت پذیرد [۱۶ و ۱۷].
- ایزوله‌کردن ماشین‌مجازی: منابع سخت‌افزاری توسط هایپروایزر که تسهیم‌کننده منابع است، باید تنها به یک ماشین مجازی اختصاص و توسط دیگر منابع در طول بهره‌برداری یک منبع قابل دسترسی نباشد. دسترسی ماشین‌های مختلف به هایپروایزر بر اساس سطح دسترسی تعیین‌شده برای آنها مشخص می‌شود و افزایش این سطح دسترسی امکان دورزدن سازوکارهای ایزوله‌سازی را فراهم می‌آورد [۲۰].
- مهاجرت ماشین مجازی: این امکان را فراهم می‌آورد که یک ماشین مجازی به‌صورت خودکار یا دستی و برخط یا انفعالی به‌منظور استفاده بهینه، بر روی منابع فیزیکی گسترش و انتقال یابد. با توجه به اینکه وضعیت حافظه، پردازنده و ذخیره‌ساز در طول انتقال حفظ می‌شود، ضروری است، سازوکار لازم به‌منظور حفظ جامعیت داده‌ها و جلوگیری از دست‌کاری آنها به‌کار گرفته شود؛ همچنین با توجه به وجود سیاست‌های متفاوت در سطح مجازی‌ساز، سیاست‌های تداخلی ضروری است، مرتفع شود. [۸،۱۱،۲۱،۲۲]
- عقب‌گرد ماشین مجازی: این قابلیت که امکان بازگشت به وضعیت اولیه شروع به فعالیت را فراهم می‌کند، زمانی

[1] Honest
[2] Integrity
[3] Life-cycles
[4] Internet Protocol
[5] Media Access Control

یک چالش امنیتی را ایجاد می‌کند که در وضعیت قبلی، یک آسیب‌پذیری وصله‌نشده موجود بوده و یا بدافزاری سیستم را تحت تأثیر قرار داده باشد [۸ و۲۳].

در ادامه گفتنی است از آنجا که ایجاد ماشین مجازی و اختصاص منابع به آن به‌سادگی اما بهره‌برداری و حذف آن با دقت طی فرآیند مشخص مدیریت منابع انجام نمی‌شود، وجود ماشین‌های بدون استفاده که پشتیبانی کامل امنیتی در آنها صورت نمی‌پذیرد، نقطه ورود مهاجمان در نظر گرفته می‌شود. همچنین یک کاربر متخاصم داخلی می‌تواند با توسعه ماشین‌های مجازی بی‌شمار، رفتار ناهنجار خود را پنهان نگاه دارد [۸،۲۰،۲۴]. همچنین از آنجا که اختصاص سیاست‌ها و رویه‌های مستقل برای هر ماشین ایجاد می‌شود، ممکن است با سیاست‌های جدید نیز تداخل داشته باشد.

۲-۲-۱-۲- مجازی‌ساز

دورزدن سازوکارهای امنیتی در نظر گرفته‌شده در مجازی‌ساز می‌تواند امکان دسترسی به همه منابع در صورت دسترسی اولیه را فراهم آورد. عدم مدیریت و انعطاف‌پذیری زیاد مجازی‌ساز یکی از دلایل ایجاد این چالش است. مواردی که در این سطح می‌تواند چالش امنیتی ایجاد کند در ادامه آورده شده است:

- شبکه مجازی: طراحی شبکه مجازی باید این اطمینان را ایجاد کند که داده تنها میان موجودیت‌های تعیین‌شده انتقال/قابل‌دسترس باشد و با تضمین جامعیت، دسترسی‌پذیری و محرمانگی انتقال یابد [۸،۱۳،۲۵].
- تجرید منابع فیزیکی[1]: تجریدساز منابع فیزیکی به‌عنوان یک لایه افزون امنیتی در مجازی‌ساز به‌حساب می‌آید. به‌وسیله این عامل، دسترسی مستقیم به منابع فیزیکی و جزئیات سخت‌افزار محدود و سبب می‌شود سیستم‌های عامل یکسان با پیکربندی‌های متفاوت بتوانند اجرا شوند. نقض امنیتی در این عامل دسترسی غیر مجاز به منابع سخت‌افزاری را فراهم می‌کند [۸ و ۲۶].
- ایزوله‌ساز: اصلی‌ترین وظیفه مجازی‌ساز، ایجاد محدوده‌هایی از منابع فیزیکی است و به‌صورت تفکیک‌شده این امکان را فراهم می‌کند که هر ماشین مجازی تنها به منابع اختصاص‌داده خود دسترسی داشته باشد. نقض مدیریت این محدوده‌ها می‌تواند امکان دسترسی به دیگر محدوده‌های غیر مجاز را فراهم کند [۲۶].
- محاسبات مجازی قابل اعتماد: پیش از اجرا، یک ماشین مجازی باید مطمئن باشد که محیطی که در آن قرار گرفته به‌منظور بهره‌برداری از حافظه، زیرساخت‌های پردازشی و ذخیره‌سازی قابل اعتماد است [۲۳]. در سیستم‌های قدیمی، یک سیستم‌عامل به‌صورت قابل اعتماد بر روی زیرساخت فیزیکی نصب و اجرا می‌شود؛ اما در ساختار مجازی، با توجه به اینکه منابع به‌صورت مجازی در اختیار ماشین‌های مجازی قرار می‌گیرد، مجازی‌ساز باید ارزیابی‌های لازم را به‌منظور ایجاد محیط قابل اعتماد پردازشی فراهم کند [۲۷].

۳-۲-۱-۲- زیرساخت فیزیکی

زیرساخت فیزیکی شامل منابع پردازشی، حافظه، شبکه، ذخیره‌ساز، ورودی و خروجی همچنین دیگر اجزا فیزیکی است که به‌صورت یک مخزن در اختیار مجازی‌ساز جهت توزیع میان ماشین‌های مجازی قرار می‌گیرد. از آنجا که بستر رایانش ابری، منابع مختلف در محل‌های فیزیکی مختلف را به‌منظور استفاده مجازی‌ساز یک‌پارچه می‌کند، لذا ضروری است، اقدامات لازم به‌منظور اختصاص و توزیع صحیح منابع جهت جلوگیری از فعالیت‌های اتلاف منابع صورت پذیرد. همچنین با توجه به اینکه تجهیزات امنیتی نیز باید به‌صورت توزیع‌شده سیاست‌گذاری شوند، طراحی سیاست‌ها و پیکربندی خود تجهیزات فیزیکی باید به‌گونه‌ای باشد که در ساختار یک‌پارچه‌شده نیز قابل استفاده باشد.

همچنین با توجه به اقدامات پیوسته پشتیبان‌گیری از منابع ذخیره‌ساز و نگهدارنده داده، این اقدام باید به‌گونه‌ای باشد که ضمن حفظ جامعیت داده‌ها، محرمانگی آن را نیز حفظ کند.

۳-۱-۲- چالش‌های واسطهای ارتباطی

زیرساخت‌های ابری، بخش مهمی از نیازمندی‌های کاربران و تعاملات کاربردی[2] را در سطوح مختلف توسط واسطهای کاربری فراهم می‌کنند. واسطهای ارتباطی یک زیرساخت رایانش ابری به چهار دسته واسطهای API[3]، واسطهای مدیریتی، واسطهای پایش و واسطهای کاربری قابل تقسیم‌بندی هستند [۱۴،۲۸،۲۹]. اصلی‌ترین چالش‌های امنیتی واسطهای ارتباطی رایانش ابری عبارت از ضعف

[1] Physical Resource Abstraction

[2] Functional Interactions

[3] Application Programming Interface

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

اعتبارنامه، بررسی اصالت‌سنجی ناکافی، اعتبارسنجی ورودی نامناسب و آسیب‌پذیری‌های سطح کاربرد است [۱۶،۲۸،۲۹].

مهم‌ترین چالش امنیتی واسطهای ارتباطی از ضعف در احراز اصالت ناشی می‌شود. این احراز اصالت تنها متعلق به انسان نبوده و در ارتباطات ماشین-ماشین نیز مورد استفاده قرار می‌گیرد. با توجه به اینکه سازوکارهای احراز اصالت پیچیده در ارتباطات ماشین-ماشین قابل استفاده نیست، لذا امکان سوء استفاده آن توسط مهاجمان وجود خواهد داشت. در کنار ضعف‌های موجود در احراز اصالت، ضعف در طراحی و پیاده‌سازی برنامه کاربردی که منجر به ایجاد آسیب‌پذیری می‌شود، همچنین عدم اعتبارسنجی مناسب ورودی، سبب می‌شود تا مهاجمان بتوانند با استفاده از حملاتی مانند تزریق SQL و یا XSS دسترسی جدید ایجاد کرده و با ارتقای سطح دسترسی، به منابع، پیکربندی‌ها و یا دیگر منابع سیستم دست یابند. از طرف دیگر، مجتمع‌سازی داده‌ها بر روی یک واسط به‌منظور پایش باید به‌گونه‌ای باشد که کلیه درخواست‌ها را تنها از یک نقطه منطقی پاسخ دهد [۱۴].

۲-۱-۴- چالش‌های شبکه

شبکه‌ها به انواع مختلف اشتراکی یا غیر اشتراکی، عمومی یا خصوصی، بیرونی یا داخلی همچنین وسیع یا کوچک قابل تقسیم‌بندی بوده و در زیرساخت‌های ابری در دو گروه شبکه مجازی منطقی ایجاد شده به‌وسیلهٔ مجازی‌ساز و پل[1] ارتباط شبکه مجازی و شبکه منطقی پیاده‌سازی می‌شوند. چالش‌های امنیتی در این ساختارها به‌دلیل اشتراک‌گذاری منابع و زیرساخت‌ها ایجاد می‌شود [۲۷].

مهم‌ترین دغدغه امنیتی در میان چالش‌های شبکه، حفظ محرمانگی و جامعیت پیام است. با توجه به اینکه یک داده ممکن است در شبکه‌ای با هر یک از ویژگی‌های عنوان‌شده منتقل شود، ضروری است بر اساس تهدیدات موجود در هر یک از ساختارها، تدابیر لازم به‌منظور حفظ محرمانگی پیام صورت پذیرد [۸].

از آنجا که داده‌های کنترلی یک زیرساخت پردازش ابری از طریق بستر شبکه انتقال و تمامی سرویس‌ها از طریق آن تأمین می‌شود، لذا حفظ دسترسی‌پذیری به‌عنوان یکی از مهم‌ترین چالش‌های موجود در بستر شبکه است.

علاوه‌بر تمامی حملات شبکه‌های سنتی مانند آلوده‌کردن ARP، شنود داده‌ها و یا جعل نشانی شبکه که در شبکه‌های رایانش ابری نیز موجود هستند، از طرف دیگر، با توجه به اینکه همه کاربران موجود دسترسی اولیه به شبکه مجازی اختصاص‌یافته به خود را داشته و انتقال داده‌ها به‌صورت منطقی تفکیک شده‌اند، لذا وجود هرگونه ضعف پیکربندی و یا کاربردی در سطوح دیگر که ضعف در تفکیک خطوط انتقال داده‌ها را ایجاد کند، می‌تواند منجر به افزایش دسترسی، نشت داده و یا تغییر در آنها را برای مهاجم فراهم کند.

۲-۱-۵- چالش‌های نرم‌افزار

با توجه به ماهیت شبکه‌ای رایانش ابری، برنامه‌های کاربردی در این ساختار اغلب از طریق رابط‌های کاربری وب ارائه می‌شوند. با توجه به معماری چندلایه و منابع اشتراکی، وجود یک آسیب‌پذیری در سطح برنامه کاربردی این امکان را به مهاجم می‌دهد که با عبور از لایه‌های مختلف، دسترسی‌های خود را تا منابع مجازی‌سازی‌شده ارتقا بدهد. از آنجا که واسط‌های کاربری وب به‌طورعمومی یک دسترسی اولیه کاربری عمومی را فراهم می‌آورد، این دسترسی عمومی ضروری است در مقابل حملات که مهم‌ترین آنها در ده اولویت OWASP به‌عنوان مرجع ارائه‌کنندهٔ حملات این حوزه عنوان شده است، امن شوند [۲۳].

۲-۱-۶- چالش‌های مدیریت اعتماد

اعتماد عبارت از تشخیص[2] یک عنصر، شناسایی و اعتماد به رفتارهای در حال اجرا توسط آن است. اعتماد توسط مجموعه‌ای از ارزش‌ها و درجه آنها تعریف می‌شود که بر اساس زمان و یا محتوا متغیر هستند [۳۰].

اعتماد در رایانش ابری به‌عنوان یک پارامتر غیرقابل اندازه‌گیری بوده که در ابعاد مختلف از جمله میان مشتری و سرویس، بسترهای ارائه سرویس، سرویس‌های مختلف همچنین لایه‌های سرویس قابل تعریف است.

۲-۱-۷- چالش‌های تابعیت و حاکمیت

کاربران سرویس‌های ابری تنها امنیت برنامه کاربردی در SaaS، بستر توسعه‌یافته در PaaS و یا زیرساخت ایجادی در IaaS را مدیریت کرده و از آنچه در لایه‌های پایین‌تر در حال وقوع است، بی‌اطلاع هستند. ممکن است، وجود یک آسیب‌پذیری در سطح مجازی‌ساز یا چالش در پیکربندی سخت‌افزاری امکان دسترسی به حافظه موقت یک مشتری را

[1] Bridge

[2] Recognition

فراهم آورد. چالش‌های حاکمیتی به ازدست‌رفتن مدیریت، عملیات و کنترل‌های امنیتی بر روی یک زیرساخت ابری اشاره می‌کنند. ازدست‌دادن کنترل بر روی افزونگی داده، محل ذخیره‌سازی، سیستم‌های فایل و پیکربندی همچنین عدم تعیین و دخالت در اعمال سیاست‌ها و رفع آسیب‌پذیری‌ها از جمله این موارد هستند. همچنین موارد مرتبط با چالش‌های وابستگی به تأمین‌کننده[1] نیز در این دسته قرار می‌گیرد. عدم تبعیت از واسطهای استاندارد و قوانین حاکمیتی این وابستگی را ایجاد و در رفع آسیب‌پذیری‌ها و چالش‌های امنیتی نیز در صورت عدم پشتیبانی تأثیرگذار خواهد بود [۲۸،۲۹].

وابسته به نوع سرویس ابری در حال استفاده و یا سطح دریافت خدمت، و یا نیز بر اساس زیرساخت فراهم‌کنندگان سرویس‌های ابری به‌طور معمول یک توافق سطح‌سرویس[2] معیار قرار می‌گیرد. این توافق به‌طورمعمول به‌دلیل عدم واضح‌بودن نیازهای امنیتی نمی‌تواند کلیه ابعاد امنیت را پوشش دهد.

۲-۲- چالش‌های مجازی‌ساز عملکرد شبکه

از آنجا که مؤلفه‌های فیزیکی شبکه در ساختار مجازی ارائه سرویس می‌کنند، شامل سطحی از انتزاع در محیط پویا شامل منابع فیزیکی یا مجازی، پروتکل‌ها و کنترل‌ها می‌شوند که در شبکه‌های سنتی مشاهده نمی‌شود. این فضا باعث می‌شود مرز دقیقی میان دامنه مجازی و حقیقی کارکرد شبکه وجود نداشته باشد [۳۱].

همان‌طور که در بخش ۱-۰۴ بر اساس نهاد استانداردهای مخابراتی اروپا نیز عنوان شد، مجازی‌ساز کارکرد شبکه دارای سه بخش است که تهدیدات امنیتی در هریک از آنها در ادامه مورد بررسی قرار خواهد گرفت. همچنین چالش‌های به‌کارگیری تجهیزات امنیتی در این نوع زیرساخت‌ها نیز مورد بررسی قرار خواهد گرفت.

۱-۲-۲- کارکرد مجازی‌سازی‌شده

علاوه بر چالش‌های امنیتی شبکه‌های سنتی مانند تغییر و جعل نشانی کنترل دسترسی سخت‌افزار[3] که مؤلفه‌های شبکه با آن مواجه هستند، موارد زیر نیز قابل بیان است:

۱-۱-۲-۲- چرخهٔ حیات

فعالیت‌های ممکن بر روی کارکرد مجازی‌سازی‌شده شامل یکی از حالت‌های ایجاد یا حذف، پیکربندی و مدیریت بسته، مهاجرت، تغییر وضعیت عملیاتی، تغییر توپولوژی، توسعه / کاهش طولی[4] و یا عرضی[5] است [۳۴].

- ایجاد یا حذف: ایجاد یا حذف یک عملکرد مجازی‌سازی‌شده، نیازمند به‌روزرسانی در سطح شبکه، اعتبارنامه‌ها، رمزنگاری‌ها، پیکربندی‌ها و دیگر تنظیمات بر اساس نیازمندی آن مؤلفه و کاربر ایجادکننده است که می‌تواند به‌صورت پیش‌پیکربندی تعریف‌شده و جدید ایجاد یا حذف شود. عدم رعایت و تطبیق سیاست‌ها در ایجاد یک مولفه جدید ممکن است به‌دلیل تناقض با دیگر سیاست‌ها منجر به بروز چالش امنیتی شود. همچنین ضروری است اعتبارنامه‌ها در زمان ایجاد و یا حذف اختصاصی شده و رمزنگاری‌های مستقل نیز در نظر گرفته شده و همه رویدادها به‌صورت مناسب و قابل پی‌جویی ثبت و گزارش شود.
- پیکربندی و مدیریت بسته: به‌روزرسانی سیستم‌عامل شامل نصب وصله‌های امنیتی یا کاربردی، نصب بسته‌ها و کتابخانه‌های جدید، اضافه یا حذف بسته‌های نرم‌افزاری و تغییر در پیکربندی سیستم عامل از جمله واسطها و کاربردهای شبکه‌ای ممکن است منجر به تداخل سیاست‌ها و درنهایت بروز یک حفره امنیتی شود.
- مهاجرت: با توجه به ضرورت فعالیت بلادرنگ در زیرساخت‌های NFV، شرایطی فراهم شده است که در صورت بروز خطا، بدون وقفه یک کارکرد مجازی‌سازی‌شده شبکه بتواند در زیرساخت‌های مختلف بدون دریافت زمان توقف سرویس منتقل شود. استفاده مجدد از حافظه، حفظ پارامترهای خصیصه‌ها، سازگاری پیکربندی و پارامترهای دسترسی‌پذیری، مهمترین مواردی هستند که در طول انتقال ضروری است، مورد بررسی و به‌منظور رفع چالش‌های امنیتی در نظر گرفته شوند.
- تغییر وضعیت عملیاتی: وضعیت‌های عملیاتی می‌تواند شامل هر یک حالت‌های خاموش، روشن، بازگشت، هایبرنیت[6]، توقف موقت و دیگر موارد باشد که اقدامات

[1] Vendor lock-in issue
[2] Service Level Agreements
[3] Media Access Control
[4] Scale-up
[5] Scale-Out
[6] Hibernation

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

سهوی یا عمدی همچنین اقدامات نگهداری و مدیریت می‌تواند در طول اجرای آنها منجر به نقض جامعیت در آنها بشود.

- تغییر توپولوژی: زمانی که توپولوژی در سطح زیرساخت تغییر یا به‌روزرسانی می‌شود، لازم است به‌روزرسانی و بررسی تغییرات در تمامی عملکردهای‌مجازی‌سازی‌شده موجود در دامنه نیز صورت پذیرد تا سیاست‌های قدیمی، مسیرهای ترافیک‌های ناخواسته و دیگر موارد ممکن منجر به بروز حفره امنیتی نشود.
- توسعه-کاهش طولی و یا عرضی: هرنوع توسعه و یا کاهش طولی یک کارکرد مجازی‌سازی‌شده تأثیر مستقیم بر روی اندازه حافظه موقت، ذخیره‌ساز، نیازمندی‌های پردازشی، آستانه‌های پایش و دامنه پشتیبان‌گیری خواهد گذاشت که ضروری است بر اساس تغییرات به‌روزرسانی‌های مربوطه صورت پذیرد. عدم انجام به‌روزرسانی‌ها می‌تواند منجر به بازشدن فضای حمله برای مهاجمان شود.

۲-۲-۲- زیرساخت مجازی‌ساز کارکردشبکه

از آنجا که در ساختارهای مجازی‌ساز عملکرد شبکه، بستر زیرساختی، مؤلفه‌های شبکه را به‌صورت متمرکز مدیریت می‌کند، دسترسی‌پذری برای توسعه حمله افزایش یافته و مهاجم با بدافزار می‌تواند به‌سرعت سطح حمله خود را توسعه دهد؛ ازاین‌روز ضعف امنیت در این لایه، کلیه لایه‌های مرتبط را که با مؤلفه‌های آن در ارتباط هستند، از جمله نمونه‌های VNF را با توجه به سرویسی که برای آن فراهم می‌آورند، تحت تأثیر قرار خواهند داد [۳۲،۳۶]. این حملات می‌تواند در سطح منابع محاسباتی، منابع شبکه، ذخیره‌سازها و دیگر منابع که نمونه‌های مجازی را برای کارکردهای شبکه فراهم می‌آورند گسترش یابد. برخلاف تمامی مزیت‌های زیرساخت مجازی‌ساز کارکرد شبکه در کاهش هزینه‌ها و پویایی توسعه، دو حوزه چالش‌برانگیز امنیتی زیر می‌تواند زیرساخت‌های یک سازمان را مورد مخاطره قرار دهد [۳۳].

۱-۲-۲-۲- مشاهده‌پذیری و اعتبارسنجی پلتفرم

این توانمندی به‌منظور اعتبارسنجی فرآیندهای درحال اجرا که توسط محیط عملیاتی مشاهده‌پذیر هستند، مورد استفاده قرار می‌گیرد؛ ازاین‌رو کلیه فرآیندهای در حال اجرا باید اعتبارسنجی شده و در صورت عدم به‌کارگیری، فرآیندهای دارای رفتار سوء مانند بدافزارها می‌تواند توسط مهاجمان اجرا شود [۳۳،۳۴].

۲-۲-۲-۲- چالش‌های برنامه کاربردی NFV

یکی از برترین مزیت‌های NFV، قابلیت استفاده از ساختار کاربرد متن‌باز[1] و توسعه آن در سطح مجازی‌سازی است که نسخه رایج در حال استفاده در این راستا OpenStack است؛ در این میان هر یک از فروشندگان محصول، نسخه‌ای اختصاصی‌شده از آن را بر اساس کارکردهای خود ارائه داده و وابستگی به او در طول بهره‌برداری با وجود انتشار نسخه‌های بعدی وجود دارد. این ضرورت وجود دارد که در صورت انتشار هرنوع آسیب‌پذیری و یا ارتقا، سیاست‌ها و سازوکار لازم به‌منظور ارتقا در نظر گرفته شود.

۳-۲-۲-۲- چالش‌های داخلی

عملکردهای مجازی‌سازی‌شده که به‌صورت مستقیم با یکدیگر در ارتباط هستند، دارای نیازمندی‌های امنیتی ویژه‌ای در سطح الزامات شبکه هستند و از آنجا که ترافیک آنها اغلب از تجهیزات امنیتی عبور نمی‌کنند، نیازمند تعیین معیارهای اندازه‌گیری امنیتی به‌صورت پیوسته هستند [۳۳]. همچنین گزارش‌ها [۳۵،۳۷] نشان می‌دهد که هفتاد درصد حملات به داده‌های حساس سازمان‌ها و هشت درصد از نشت اطلاعات در سال ۲۰۱۴ میلادی نتیجه حملات صورت‌گرفته و پایش‌نشده متخاصمان داخلی بوده است.

۴-۲-۲-۲- چالش‌های بیرونی

زیرساخت مجازی‌ساز کارکردشبکه می‌تواند از بیرون محدوده و توسط یک شبکه ثانویه مدیریت و کنترل شود [۳۹]. هر یک از حملات عنوان‌شده در بخش‌های قبل به واسطه ایجاد این ارتباط قابل انجام است؛ ازاین‌رو ضروری است، بستر اعتماد میان دو مؤلفه کنترل‌کننده و کنترل‌شونده فراهم شود. این اعتماد در سه حوزه زیر مورد نیاز است [۴۰].

- ایجاد اعتماد در داده‌هایی که میان دو مؤلفه مبادله می‌شوند.
- ایجاد اعتماد میان دو موجودیت نرم‌افزاری که عملیات صحیح را انجام می‌دهند.
- ایجاد اعتماد بر روی عملیات‌هایی که تأثیر مستقیم و یا غیر مستقیم بر روی داده‌ها دارند.

[1] Open Source

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

۳-۲-۲- مدیریت و هماهنگ‌کننده مجازی‌ساز عملکرد شبکه

این لایه به مدیریت و هماهنگ‌سازی لایه‌های دیگر و نمونه‌های مجازی‌سازی‌شده همچنین چرخه حیات کارکردهای مجازی‌سازی‌شده می‌پردازد [۴۱]. مهمترین چالش‌های امنیتی در مؤلفه‌های این لایه عبارتند از:

- مدیریت، هماهنگی و خودکارسازی امن: این مؤلفه موظف به مدیریت چرخه حیات نمونه‌های مؤلفه‌های مجازی‌سازی‌شده، نگهداری منابع توزیع‌شده و اندازه‌گیری کیفیت انتها-انتهای سرویس است. از آنجا که کلیه این نیازمندی‌ها بلافاصله پس از درخواست و توسط فرمان‌دهنده امن و قابل اعتماد باید انجام پذیرد، لذا هرگونه چالش امنیتی در این مؤلفه که اختلال سرویس ایجاد کند، می‌تواند سرویس در لایه‌های بالایی را نیز دچار اختلال کند [۳۸]. همچنین از طرف دیگر اجرای دستورهای مدیریتی باید به‌گونه‌ای باشد که سیاست‌های امنیتی را نقض نکند.
- تضمین کنترل امن: مدیریت و هماهنگ‌کننده مجازی‌ساز عملکرد شبکه به‌عنوان نقطه مرکزی تصمیم‌گیری درخصوص وضعیت عملکردهای مجازی‌سازی‌شده است؛ لذا از آنجا که دسترسی به این مؤلفه می‌تواند مسیر گسترده‌ای از حملات را برای مهاجم فراهم کند، کلیه مسیرهای آن باید به‌صورت دقیق پایش و بررسی شود؛ همچنین هویت‌سنجی[1]جهت جلوگیری از عدم دست‌یابی غیر مجاز، کسب‌اجازه[2] به‌منظور حفظ سیاست کمینه دسترسی و واگذاری اختیارات مجاز به دسترسی هویت‌سنجی‌شده و حسابرسی[3] به‌منظور گزارش‌گیری دنباله رفتارها و پذیرش مسئولیت رفتار دسترسی‌ها در سطح اختیار واگذارشده ضروری است به‌کارگیری و پایش شود.
- الزامات تضمین سرویس و سیاست‌ها: با توجه به این‌که پیش از ارائه سرویس، کلیه سیاست‌ها، رویه‌ها و سطح ارائه سرویس مورد نیاز مشتری تدوین و بر اساس آن خدمات مدیریت و هماهنگ‌سازی شبکه صورت می‌پذیرد، لذا ضروری است، سیاست‌ها و رویه‌های امنیتی نیز هم‌زمان منطبق بر سطح سرویس مورد نیاز تدوین و ارائه شود. از جمله این موارد می‌توان به زمان‌بندی ارائه وصله امنیتی و به‌روزرسانی اشاره کرد [۴۳].

[1] Authentication
[2] Authorization
[3] Accounting

۳- حملات امنیتی

هر رفتار ناهنجار تعمدی که با بهره‌گیری از آسیب‌پذیری‌های سیستم یکی از پارامترهای امنیتی محرمانگی، دسترسی‌پذیری و جامعیت را نقض کند یک حمله شناخته می‌شود [۴۶]. بر اساس مدل سنجش تهدید که توسط مایکروسافت ارائه شده است، حملات قابل تقسیم‌بندی به جعل نشانی، مداخله، انکار، نشت اطلاعات، ممانعت از سرویس و حملات دسترسی هستند [۶۱]. بر اساس دسته‌بندی ارائه‌شده و تطبیق آن با حملات عنوان‌شده در سطح رایانش ابری و مجازی‌سازی، بر اساس مقالات مرورشده در یکی از دسته‌های زیر قابل تفکیک هستند:

۳-۱- حملات ممانعت از سرویس

یکی از مهمترین و پراستفاده‌ترین دسته حملات در حوزه زیرساخت‌های ابری و مجازی‌سازی، حملات ممانعت از سرویس است. کاربر مهاجم با دارا بودن دسترسی مجاز یا فراهم‌کردن آن، اقدام به ارسال داده‌هایی می‌کند که در عملکرد سیستم اختلال ایجاد می‌کند. این حملات در لایه‌های زیر می‌توانند مجموعه زیرساخت‌های ابری و یا سرویس‌های آن را تحت تأثیر قرار دهند [۴۷،۴۸،۴۹]:

- ممانعت از سرویس سطح کنترل: این حمله با ارسال تعداد زیادی درخواست مهاجرت توسط مهاجم به ماشین هدف به‌منظور جلوگیری از اجرای فرامین در صف انجام می‌پذیرد.
- ممانعت از سرویس سطح انتقال داده: در این حمله مهاجم با ارسال داده‌های پیوسته و به‌کارگیری ظرفیت انتقال داده، در دسترسی دیگر کاربران به منابع، اختلال ظرفیتی ایجاد می‌کند.
- ممانعت از سرویس در سطح کاربرد: مهاجم با ارسال درخواست‌های مشخص و بهره‌برداری از آسیب‌پذیری‌های موجود در سطح کاربرد از جمله امکان دریافت ورودی‌های نامعتبر و با استفاده از واسط‌های کاربری اقدام به ایجاد ممانعت در سرویس می‌کند [۵۱].

۳-۱-۱- حملات ساختار داده

حملات ساختار داده، با سوء بهره‌برداری[4] از آسیب‌پذیری‌های فرآیندها و مدیریت ساختار داده سیستم، کاربردها و حفاظت‌های رایج سیستم را مورد حمله قرار داده و می‌تواند به داده‌های سیستم به‌صورت مستقیم دسترسی

[4] Exploit

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

یابد. تغییر ارجاعات مؤلفه‌های کاربری و یا حمله و دست‌کاری حافظه موقت اشتراکی از جمله فعالیت‌هایی است که در این دسته حملات و با ایجاد فعالیت‌هایی مانند سرریزپشته[1] انجام می‌پذیرد. مهاجم با این دسته از حملات می‌تواند از سطح مجازی‌ساز عبور کرده، سپس کد مخرب و فرامین خود را در سطح میزبان فیزیکی اجرا کند [۱۶،۴۵].

۳-۱-۲- کد مخرب تعبیه‌شده

لایه‌های مختلف مجازی‌ساز و زیرساخت ممکن است شامل کدهای مخرب پیش‌تعبیه‌شده‌ای باشد که به‌صورت بمب‌زمانی[2]، دروازه ورودی[3] و یا تروجان عمل کند. به‌کارگیری و ارائه دستور به این کد ممکن است، توسط ورود یک فایل حاوی ناهنجاری، فایل صوتی دارای نهان‌نگاری، مرور یک نشانی دسترسی به وب و یا تفسیر یک فایل در حال اجرا توسط نمونه فعال در مجازی‌ساز باشد [۴۵].

۳-۱-۳- حملات شنود

مهاجمان بخشی از داده‌های حساس را به‌وسیلهٔ شنود بستر شبکه جمع‌آوری می‌کنند. شنود داده‌ها به‌صورت انفعالی و یا فعال انجام می‌پذیرد. در حالت نخست، با ایجاد یک حمله مرد میانه[4] در بستر دسترسی، مهاجم در میان دو مؤلفه قرار گرفته و داده‌های آن‌ها را جمع‌آوری می‌کند. همچنین مهاجم با دورزدن محدودیت‌های اعمالی در تفکیک منطقی شبکه ممکن است، داده‌های مورد نیاز خود را جمع‌آوری کند. در حالت فعال، مهاجم با استفاده از ابزارهای مختلف، اطلاعات پیکربندی و داده‌های سیستم را که می‌تواند منجر به کشف آسیب‌پذیری‌های سیستم و یا نقوض در پیکربندی باشد، استخراج می‌کند [۱۶،۲۰]. یکی از مهمترین حملات شنود در لایه واسطهای ارتباطی انجام می‌پذیرد. مهاجم با شنود واسطهای ارتباطی می‌تواند اطلاعات مهمی از جمله نام‌های کاربری و پارامترهای پیکربندی را استخراج کند [۵۲].

۳-۱-۴- حملات تزریق

یکی از حملات رایج در زیرساخت‌های رایانش ابری، حمله تزریق کد است. در این حمله، مهاجم کدهای تغییریافتهٔ سوء را به برنامه کاربردی به‌منظور دریافت دسترسی غیرمجاز به منابع سیستم یا ارتقای آن با بهره‌گیری از آسیب‌پذیری‌های موجود ارسال می‌کند [۵۳]. همچنین یکی دیگر از حملات، تزریق بدافزار است. در این حمله مهاجم با بارگذاری یک نمونه مجازی دست‌کاری‌شده از سرویس‌های مورد نیاز هدف حمله، درخواست‌ها را در زمان ارائه سرویس آلوده می‌کند [۵۴].

از آنجا که بخش مهمی از سرویس‌های رایانش ابری توسط وب سرویس ارائه می‌شود، حملات تزریق شامل حملات تزریق کد SQL و تزریق دستورهای سیستم نیز ممکن است آن‌ها را تحت تأثیر قرار دهند. در این حمله، مهاجم با دست‌کاری محتوای پیام‌ها و جای‌گذاری دستورها و یا محتوای درخواستی خود در میان محتوای اولیه، به پایگاه سیستم دسترسی ایجاد می‌کند [۵۵].

۳-۱-۵- حملات انحصار منابع

حملات انحصار منابع، شامل اقداماتی است که مهاجم به‌منظور کاهش بازدهی دیگر ماشین‌های مجازی‌شده به‌کار می‌گیرد تا منابع اختصاص‌یافتهٔ خود را افزایش دهد. در این دسته حملات، مهاجم با بهره‌برداری از ضعف‌های الگوریتم‌های تخصیص منابع، پیش از زمان اختصاص منبع به دیگر ماشین‌ها، آن را اشغال کرده و خود استفاده می‌کند. یکی دیگر از روش‌های انحصار منابع، ایجاد سربار دست‌کاری‌شده بر روی ورودی/خروجی[5] و سپس دست‌کاری صف اشتراک ورودی/خروجی است.

۳-۱-۶- حملات بدافزاری

ممکن است، یک نمونهٔ آلودهٔ جدید در زیرساخت رایانش ابری بارگذاری و یا نمونهٔ موجود به‌دلیل ضعف امنیتی آلوده شود. تزریق یک بدافزار می‌تواند مبتنی بر شبکه و یا به‌طورمستقیم توسط توزیع‌کننده منابع انجام پذیرد [۵۴،۵۷]. از آنجا که بدافزار می‌تواند در انواع ساختارهای فایل قرار گرفته و سپس خود را منتشر کند، مهاجم توسط بهره‌برداری از فایل‌های مرسوم، محدودیت‌های بارگذاری را پشت سر می‌گذارد. حملات بدافزاری با اهداف مختلف طراحی می‌شوند. این حملات ممکن است، برای ایجاد یک درب پشتی به‌منظور حملات بعدی، سرقت اطلاعات پیکربندی و یا کاربردی، ایجاد واسط حمله به شخص ثالث و یا تخریب منابع به‌کار گرفته شوند [۵۴،۵۵].

[1] Buffer Overflow
[2] Timebomb
[3] Trapdoor
[4] Man-In-The-Middle

5 Input/Output

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

۷-۱-۳- حملات نقض جامعیت

حملات نقض جامعیت به فعالیت‌هایی ناهنجاری گفته می‌شود که به‌وسیلهٔ آن، داده‌های ذخیره‌شده و یا در حال انتقال بدون اطلاع ایجادکننده و یا ارسال‌کننده/دریافت‌کننده آن تغییر می‌یابد [۵۸]. حملات نقض جامعیت داده در زیرساخت‌های رایانش ابری عبارتند از:

- حمله دست‌کاری داده‌های محاسباتی: مدلی از حمله که به‌وسیلهٔ تغییر دادهٔ ذخیره‌شده در منابع محاسباتی مانند پردازش‌گر یا حافظه موقت، انجام پذیرفته و مهاجم توسط آن اقدام به افزودن کد مخرب و یا تغییر پارامترهای موجود می‌کند.
- دست‌کاری داده‌های ذخیره‌شده: این دسته از حمله شامل تغییر در داده‌های ذخیره‌شده به‌صورت محلی و یا راه دور است. این داده‌ها ممکن است، داده‌های کاربران، پشتیبان‌ها و یا پیکربندی باشد.
- نقض جامعیت در طول مهاجرت: در این حمله مهاجم تلاش می‌کند که داده‌های پیکربندی و یا موجود در حافظه آخرین وضعیت ذخیره‌شده در نمونه در حال انتقال را تغییر داده و یا داده‌های مخربی در آن وارد کند.

۸-۱-۳- حملات کانال جانبی

در حمله کانال جانبی، مهاجم از راه‌های غیر مستقیم مانند اندازه‌گیری فرکانس استفاده‌شده به‌وسیلهٔ هر ماشین پردازش‌گر و ارسال داده‌های مختلف به آن، تلاش می‌کند رفتار یک ماشین مجازی را پیش‌بینی کند. یکی از مهم‌ترین حملات کانال جانبی، حمله زمان‌بندی است که در آن میزان موفقیت و زمان در درخواست‌های محاسباتی مختلف اندازه‌گیری می‌شود. با تکرار این حمله که به‌سختی قابل تشخیص است، مهاجم می‌تواند داده‌های حساس در حال محاسبه مانند کلیدهای رمزنگاری را استخراج کند [۵۹]؛ همچنین دیگر حمله مرتبط در این حوزه به‌کارگیری ماشین موازی مجازی نزدیک به هدف حمله به‌منظور استخراج داده‌ها است.

۹-۱-۳- حملات مردی در ابر

هدف این حمله سوء استفاده از فعالیت‌های هم‌زمان‌سازی است که به‌منظور پشتیبانی و یا سرویس‌های فعال/آماده[1] استفاده می‌شود، می‌باشد. با توجه به این‌که انتقال و هم‌زمان‌سازی به‌وسیلهٔ یک نشانه[2] انجام می‌پذیرد، مهاجم با مهندسی اجتماعی و ارسال یک داده مخرب به کاربر، نشانه او را به سرقت برده و سپس توسط آن پس از قرار گیری میان مبدأ و مقصد هم‌زمان‌سازی، به داده‌های هم‌زمان‌شده دسترسی می‌یابد [۶۰].

۱۰-۱-۳- حملات ارتقای دسترسی

یکی از مهم‌ترین حملات در زیرساخت‌های ابری که اغلب پیش‌زمینه دیگر حملات هستند، ارتقای دسترسی است. این حمله که بیشتر توسط متخاصمان داخلی اتفاق می‌افتد مهاجم با توسط به دسترسی مجاز اولیه‌ای که دارد و به‌وسیلهٔ بهره‌برداری از آسیب‌پذیری در لایه‌های مختلف، سطح اولیه دسترسی خود را به سطوح مدیریتی و یا دیگر کاربران افزایش داده و به منابع اختصاص‌یافته و یا داده‌ها دسترسی می‌یابد.

۴- بررسی تطبیقی چالش‌ها و حملات

در زیرساخت‌های رایانش ابری، تمامی تعاملات میان دو مؤلفه از سه مؤلفهٔ کاربران سرویس، نمونه‌های سرویس و فراهم‌کننده ابررایانشی است. در وضعیت مشابه، بردار حمله نیز از یکی از مؤلفه‌های یادشده به دیگر مؤلفه یادشده شکل می‌گیرد. حمله ممکن است در یکی از حالات زیر انجام پذیرد که در شکل (۳) ارائه شده است [۶۱]:

- حمله از سرویس‌دهنده به کاربر
- حمله از کاربر به سرویس‌دهنده
- حمله از ابررایانشی به سرویس
- حمله از سرویس به ابررایانشی
- حمله از کاربر به ابررایانشی
- حمله از ابررایانشی به کاربر

هر یک از مؤلفه‌های یادشده، برای ارتباط با دیگر مؤلفه‌ها یک یا چند واسط ارتباطی را فراهم می‌آورند که براساس استانداردها، فرامین و داده‌ها میان آن‌ها انتقال می‌یابد.

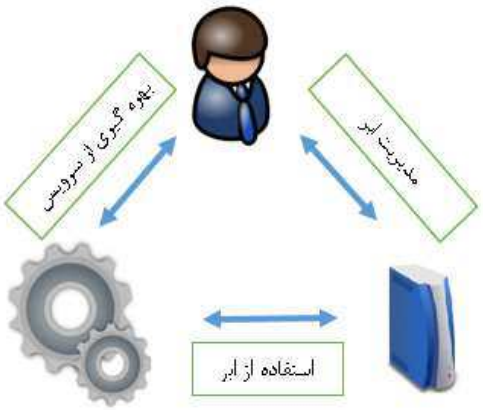
از آنجا که ساختارهای مختلف سرویس مجازی‌ساز عملکرد شبکه با بهره‌برداری از رایانش ابری و منطبق بر استاندارد، در سطح سرویس ساختار منطقی و مؤلفه‌های افزونه‌ای را ارائه می‌کنند [۶۱،۶۲]، ضعف‌ها و دغدغه‌های عنوان‌شده در هر یک از مؤلفه‌ها که در بخش ۲ عنوان شد،

[1] Active\standby

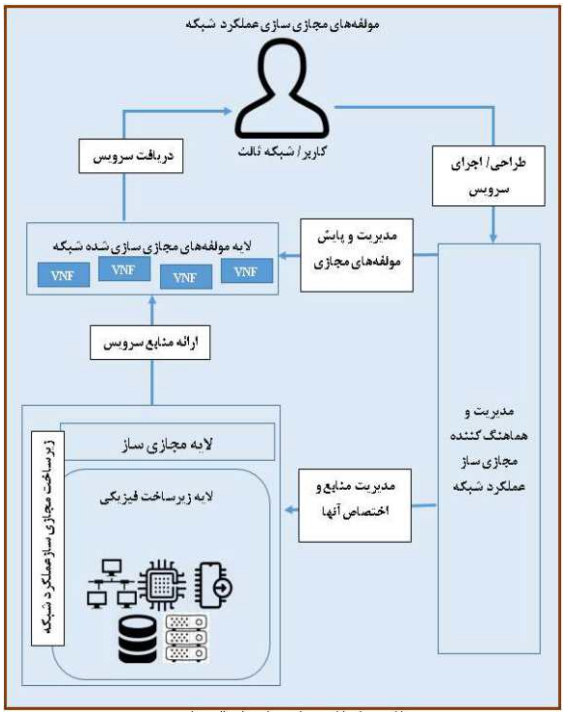
[2] Token

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

می‌توانند به‌منظور بهره‌برداری در یک یا چند دسته از حملات عنوان‌شده در بخش ۳ به‌کار گرفته شود و بر زیرساخت مجازی‌ساز عملکرد شبکه نیز تأثیر گذارد.



(شکل-۳): بردار حملات زیرساخت‌های ابری



(شکل-۴): بردار تعاملات زیرساخت مجازی‌ساز عملکرد شبکه

بردار تعاملات مؤلفه‌ها در مجازی‌ساز کارکرد شبکه به‌صورت آنچه در شکل (۴) ارائه شده است، قابل بیان خواهد بود. همانند زیرساخت‌های رایانش ابری، هر یک از مؤلفه‌های عنوان‌شده به‌وسیلهٔ واسط‌های استاندارد، نقش خود را ایفا می‌کنند.

بر اساس نقش‌های عنوان‌شده، مهاجم می‌تواند در نقش هر یک مؤلفه‌ها قرار گرفته و حملات خود را اجرا کند. تطبیق حملات بر اساس چالش‌های امنیتی موجود در رایانش ابری که تعاملات مؤلفه‌های مختلف را تحت تأثیر قرار می‌دهد در پنج دسته قابل تفکیک خواهد بود.

۴-۱- کاربر / شبکه ثالث

نقش کاربر/شبکه ثالث به دو صورت دریافت‌کننده سرویس و طراحی/اجرای سرویس قابل تعریف است. جدول (۲) نگاشت چالش‌های امنیتی به حملات را برای این نقش به‌همراه نمونه تأثیر ناشی از حمله نشان می‌دهد. مطابق بخش (الف) جدول(۲)، ممکن است یک کاربر که به‌دلیل ضعف در مدیریت بسته آخرین وصله امنیتی را نصب نکرده و آسیب‌پذیر است، پس از آلودگی به بدافزار توسط شبکه دیگر، امکان دریافت فرمان از مهاجم را فراهم و اطلاعات دسترسی خود را به‌همراه معماری مورد نیاز در اختیار وی قرار داهد. همچنین مهاجم می‌تواند با تأثیر بر این لایه، به لایه‌های بعدی نیز به‌وسیلهٔ این لایه نفوذ کند.

۴-۲- مدیریت و هماهنگ‌کننده مجازی‌ساز عملکرد شبکه

این مؤلفه در دو نقش مدیریت منابع و اختصاص آنها به ماشین‌های مجازی و همچنین مدیریت عملکردهای مجازی‌سازی‌شده براساس چرخه حیات آنها عمل می‌کند. همچنین این مؤلفه به‌عنوان فراهم‌کننده زیرساخت برای پیکربندی و اجرای سرویس درخواستی کاربر/شبکه ثالث، واسطی را برای ارائه درخواست‌ها و پایش آن‌ها فراهم می‌آورد[۳۸،۶۲]. در هر یک از نقش‌های مرتبط، این مؤلفه می‌تواند در نقش مبدأ حمله و یا هدف حمله قرار گیرد. جدول (۲) نگاشت چالش‌های امنیتی به حملات را برای این نقش نشان می‌دهد.

۴-۳- زیرساخت مجازی‌ساز عملکرد شبکه

این لایه که در دو سطح زیرساخت فیزیکی و لایه مجازی‌ساز عمل می‌کند، اصلی‌ترین نقطه اهداف مهاجمان را تشکیل داده و در معرض سطح وسیعی از حملات است [۵۷]. دسترسی مهاجم به این لایه همچنین می‌تواند کلیه لایه‌های دیگر را نیز تحت تأثیر قرار دهد. مهاجم با تحت تأثیر قراردادن لایه کنترل و به‌کارگیری حملات، می‌تواند منابع مختلف را تسخیر و یا رویه‌های تعریف‌شده را در سطح شبکه و یا محاسبات تغییر دهد [۴۴].

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

۴-۴- کارکرد مجازی‌سازی‌شدهٔ شبکه

از آنجا که وظیفه این سطح، فراهم‌آوری سرویس‌های شبکه مبتنی بر مجازی‌سازی است، ترکیب حملات سطح شبکه با حملات سطح مجازی‌سازی صورت می‌پذیرد. به‌عنوان نمونه مهاجم با استفاده از حملات تزریق کد و وجود ضعف در واسط ارائه سرویس مؤلفه مجازی‌سازی‌شده، اطلاعات ماشین مجازی را استخراج و پس از استخراج داده‌ها، در مسیر دیگر مؤلفه‌های شبکه قرار گرفته و با حمله مردی‌درمیان، اقدام به تغییر اطلاعات در دیگر مسیرهای شبکه‌ای می‌کند [۶۰].

(جدول-۲): بررسی تطبیقی چالش‌ها و حملات به همراه نمونه تأثیر

مؤلفه	چالش‌های پیش‌رو	نوع حمله	نمونه تأثیر حمله	عامل
(الف): کاربر/شبکه ثالث	ضعف در مدیریت وصله ضعف در واسط امن ضعف در مدیریت اعتماد ضعف در مدیریت پشتیبانی	جعل اعتبار	ارسال فرمان از طرف کاربر دیگر	الف
		تزریق	تزریق فرمان به کاربر جهت دریافت دسترسی	الف/ت
		بدافزار	سرقت اطلاعات موجود کاربر و یا بازکردن درب پشتی	الف/ب
		نقض جامعیت	تغییر فرامین و دستورات کاربر/ شبکه ثالث	الف
		ارتقاء دسترسی	نشت اطلاعات و ارسال دستورات سطح بالا	الف/ت
(ب): مدیریت و هماهنگ‌کننده مجازی‌ساز عملکرد شبکه	ضعف در مدیریت وصله ضعف در واسط امن ضعف در مدیریت اعتماد ضعف در اعتبارسنجی ورودی ضعف در سنجش اعتماد ضعف در ذخیره داده‌ها ضعف در شبکه امن ضعف در تطبیق سیاست‌ها ضعف در کنترل امن	ممانعت از سرویس	عدم ایجاد یا تغییر پیکربندی، کشف عیب و مدیریت بستر	الف
		تزریق	تغییر پیکربندی، ایجاد مؤلفه و یا دسترسی اطلاعات بهره برداران و نشت اطلاعات	الف
		بدافزار	ایجاد درب پشتی، اختلال در عملکرد، سرقت اطلاعات کاربران و یا اطلاعات پیکربندی	الف/ت
		نقض جامعیت	تغییر و دستکاری داده‌ها و فرامین ارسالی به مجازی ساز و مؤلفه‌های مجازی سازی شده	الف/ت
		شنود	دسترسی مؤلفه‌ها به اطلاعات در حال مبادله، سرقت اطلاعات پیکربندی و تغیر آن	الف/ت
		ارتقا دسترسی	با توجه به دسترسی اولیه کاربران برای پکیرندی، دسترسی بالاتر اخذ و پیکربندی تغییر یابد.	الف
(پ): زیرساخت مجازی ساز	ضعف در مشاهده‌پذیری ضعف در اعتبار سنجی ضعف در سنجش اعتماد ضعف در ایزوله‌سازی ضعف در مهاجرت ضعف در ذخیره‌سازی داده ضعف در عقبگرد ضعف در تجرید منابع فیزیکی ضعف در واسط‌های	ممانعت از سرویس	عدم ارائه سرویس به دیگر ماشین های مجازی	ب/ت
		تزریق	دسترسی به حافظه و پردازش‌گر و سرقت اطلاعات و یا تزریق کد به دیگر نمونه ها	ت
		بدافزار	ایجاد درب پشتی و سرقت اطلاعات	ت
		نقض جامعیت	انحصار منابع، ارسال فرامین غیر مجاز، سرقت اطلاعات	ب/ت
		شنود	استخراج اطلاعات کاربری و داده‌های نمونه‌ها	ت
		ساختار داده	دسترسی به دیگر بخش‌های حافظه، پردازشگر و شبکه. دسترسی به کنترل میزبان	ت
		کد مخرب	اعمال فرمان و تغییر پیکربندی دیگر مؤلفه‌های دریافت‌کننده منابع. تغییر نمونه در حال مهاجرت و ایجاد درب پشتی درآن	ت
		مردی در ابر	سرقت اطلاعات پشتیبان‌های در حال ذخیره‌سازی که می تواند شامل اطلاعات کاربری و پیکربندی باشد	ب/ت

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

	ارتباطی ضعف مدیریت چرخه حیات ضعف در مدیریت بسته ضعف در توسعه طولی/عرضی	انحصار منابع	دریافت منابع دیگر نمونه ها به منظور استفاده در تولید رمز ارزها و یا شکستن الگو های رمز شده	ت
		کانال جانبی	استخراج کلیدهای رمزنگاری به‌منظور خواندن فایل‌های رمزشده در حال انتقال و یا پشتیبان	ب/ت
(ت): مؤلفه‌های مجازی‌سازی شده شبکه	ضعف در اعتبارسنجی ضعف در ذخیره‌سازی داده ضعف در عقبگرد ضعف در واسط‌های ارتباطی ضعف در مدیریت بسته تغییر توپولوژی ضعف در نرم‌افزار شبکه ضعف در مهاجرت ضعف در جامعیت	ممانعت از سرویس	اختلال در ارائه سرویس شبکه	الف
		شنود	شنود اطلاعات میان نمونه مجازی‌سازی‌شده یا کاربر یا زیرساخت مجازی ساز	الف
		کد مخرب	تغییر پیکربندی نرم‌افزار شبکه‌ای بدون اعتبار سنجی	الف
		بدافزار	ایجاد درب پشتی و یا سرقت اطلاعات	الف/پ
		ارتقا دسترسی	ارتقا دسترسی بهره‌برداری به کاربر و یا مدیر جهت اعمال پیکربندی و یا سرقت اطلاعات	الف
		ساختار داده	عبور از سطح ماشین و دریافت دسترسی از مجازی ساز	الف
		تزریق	SQLدسترسی به حافظه ماشین توسط تزریق درخواست	الف
		نقض جامعیت	تغییر در فرامین دریافتی و یا حافظه ماشین متوقف	الف

۵- راه‌حل‌های موجود تأمین امنیت

بر اساس مطالعات و نتایج حاصله از بررسی‌های این مقاله، ۲۲ چالش امنیتی در زیرساخت‌های مجازی‌سازی عملکرد شبکه، چهارده چالش امنیتی در سطح رایانش ابری و چهارده چالش امنیتی در سطح مجازی ساز کارکرد شبکه قابل استخراج است که می‌تواند توسط ده حمله مختلف تحت تأثیر سوء قرار گیرد. ازاین‌رو بخشی از راه‌کارهای قابل بررسی برای مقابله با هر یک از این حملات که می‌تواند مؤلفه‌های مختلف این زیرساخت را تحت تأثیر قرار دهد در این بخش ارائه می‌شود.

۵-۱- به‌کارگیری شناساگر و مدیریت دسترسی

هدف شناساگر و مدیریت دسترسی[1] ارائه یک بستر به‌منظور دسترسی یک فرد مجاز به یک منبع مجاز در زمان مجاز و از طریق مجاز است. این ابزار به‌منظور ایجاد دسترسی، برداشت، ضبط و مدیریت کاربر شناسایی‌شده به‌همراه دسترسی‌های وی و همچنین داده‌هایی که کاربر در طول فعالیت خود به‌کار می‌گیرد، استفاده می‌شود؛ بنابراین مجوز دسترسی به کاربر توسط توالی بررسی مجوزها و ممیزی دقیق و بر اساس تفسیر دقیق قوانین و سیاست‌ها محقق می‌شود. از آنجا که زیرساخت‌های ابری یک بستر چندمتولی و چندزیرساختی را فراهم می‌کند، فراهم‌کردن این ابزار با پیچیدگی فراوانی مواجه است. راه حل ارائه‌شده شامل یک کاربرد احراز اصالت انعطاف‌پذیر به‌منظور جلوگیری از ارتقای دسترسی و جلوگیری از نشت داده است. مؤلفه‌های اصلی این راه حل فراهم‌کننده منابع ابری، مدیریت شناسایی، مدیریت سیاست، منابع هسته و تصمیم‌گیری سیاست است [۶۲]. همچنین در زیرساخت‌های مجازی‌ساز کارکرد شبکه راه حل AC-VNF به‌منظور کنترل تعداد زیادی کارکرد مجازی‌سازی‌شده همراه احراز اصالت کاربر قابل بهره‌برداری است. سیاست‌ها در این بستر بر اساس اینکه چه کسی به کدام منابع دسترسی داشته باشد و همچنین چگونگی اشتراک منابع، قابل تعریف است [۶۳].

۵-۲- مقابله با ممانعت از سرویس

حملات ممانعت از سرویس، ناشی از افزایش ترافیک بسته‌های ترافیکی دست‌کاری‌شده و یا ارسال یک داده ناهنجار به سطح کاربرد است که اختلال و به‌کارگیری حجم

[1] Identity and Access Management (IAM)

زیادی از منابع در پردازش و حافظه است. همچنین این حملات می‌تواند به‌صورت ممانعت از سرویس توزیع‌شده[1] یا از منابع محدود مشخص، سیستم را تحت تأثیر قرار دهد [۷]. با توجه به این‌که تعاملات لایه کاربرد اغلب توسط واسطهای کاربردی انجام می‌پذیرد، مهم‌ترین راه‌حل جلوگیری از حملات ممانعت از سرویس این لایه، کنترل و تصفیه‌کردن ورودی‌ها، تفکیک و تشخیص داده‌ها بر اساس رفتار و امضا، همچنین احراز اصالت کاربران به‌منظور جلوگیری از دسترسی کاربران غیر مجاز به واسط کاربری است [۶۴]. روش‌های مقابله با حملات ممانعت از سرویس بسته به قرارگیری نزدیک هدف حمله و یا نزدیک به مبدأ حمله یا در میانه مبدأ و مقصد متفاوت است. در ابزارهای نزدیک مبدأ، میزان ترافیک ورودی و خروجی از نزدیک‌ترین مسیریاب به مبدأ یا مبادی حمله سنجیده و در صورت مشاهده رفتار ناهنجار یا به‌کارگیری نشانی‌های شناسه جعلی شبکه به‌منظور ارسال ترافیک، مبدأ مسدود می‌شود. در موارد نزدیک مقصد، ابزار با شناسایی الگوی ترافیکی و وابستگی بسته‌ها، آماری از مبادی استخراج و در صورت ناهنجاری آن را مسدود می‌کند. در روش میانی هر دو دسته قبلی یادشده به‌همراه وابستگی به یکدیگر تحلیل و مبادی حمله شناسایی می‌شود. از طرف دیگر دسته‌بندی ممکن برای این حملات راه‌حل‌های قبل از حمله، در زمان حمله و بعد از آن قابل تقسیم‌بندی است. در طول حمله ممانعت از سرویس، محتوا و یا رفتار ترافیکی توسط تحلیل خبرگی شناسایی و مبادی جهت کنترل آن بررسی و محدودیت‌های لازم از ریشه تا مؤلفه تحت حمله صورت می‌پذیرد [۶۵].

۳-۵- ایزوله‌سازی

ایزوله‌سازی یکی از مهم‌ترین بخش‌ها در حفاظت از زیرساخت‌های رایانش ابری است. مهم‌ترین بخش‌هایی که ضروری است، ایزوله‌سازی در آن‌ها انجام پذیرد، عبارت است از:

- ایزوله‌سازی داده: باید تفکیک و تعریف کامل میان داده‌های دارای حساسیت بالا و داده‌های معمول صورت پذیرد. داده‌ها در زیرساخت رایانش ابری و زیرساخت‌های مجازی‌ساز کارکرد شبکه قالب‌های متفاوتی دارند. داده‌های کاربردی، پیکربندی زیرساخت، برنامه‌های کاربردی عمل‌گر شبکه، داده‌های توسعه‌ای و یا اسکریپت‌ها انواع مختلف داده‌ها هستند. نخستین قدم در محافظت از داده‌ها، تعریف کنترل دسترسی و رمزنگاری داده‌ها است. با توجه به ذخیره‌شدن بخشی از داده‌ها در پایگاه‌داده، روش‌های مختلفی به‌منظور ایزوله‌سازی داده‌ها وجود دارند که براساس کنترل منابع و درجه‌بندی اولویت داده‌ها رمزنگاری و کنترل دسترسی را ارائه می‌کنند. راه‌حل‌هایی همچون ایجاد پایگاه‌های داده مختلف و یا نما[2] برای بهره‌برداران مختلف و یا اختصاص منابع تفکیک‌شده برای کاربران مختلف پیشنهاد شده است. همچنین داده‌ها در سه سمت کاربر، سمت مجازی‌ساز و زیرساخت فیزیکی باید رمزنگاری و تفکیک بر اساس اولویت آن‌ها صورت پذیرد تا مقابله لازم با حملات نشت داده یا نقض جامعیت آن صورت پذیرد [۶۶،۶۷،۶۹].
- ایزوله‌سازی شبکه: ایزوله‌سازی شبکه دارای دو بعد ایزوله‌سازی شبکه، تفکیک منطقی و یا فیزیکی شبکه و ایجاد یک بستر امن انتقال بر روی آن و نیز تضمین و مدیریت کیفیت سرویس است که به‌منظور جلوگیری از حملات حوزه شبکه انجام می‌پذیرد. ایجاد تونل کلیدی‌ترین کاربرد عامل در تفکیک شبکه‌های منطقی و یا فیزیکی است. راه‌حل دیگر ایزوله‌سازی شبکه، تفکیک ترافیک در هسته است که بر اساس فرمان به هر سوئیچ در مسیر، شبکه را اجبار به تبعیت از فرامین مرکزی می‌کند. بسترهای مختلف تجاری نیز بر اساس معماری خود، شرایط ایزوله‌سازی را نیز فراهم آورده‌اند. به‌عنوان نمونه، Cisco، OpenFlow و OpenStack به‌وسیلهٔ ابزارهای توسعه یافته‌خود تفکیک ترافیک را سامان‌دهی می‌کنند [۶۹].
- ایزوله‌سازی هایپروایزر: هدف اصلی ایزوله‌سازی هایپروایزر این است که در صورت حمله به نمونه ماشین مجازی یا کارکرد مجازی‌سازی‌شدهٔ شبکه، دیگر ماشین‌های مجازی یا مؤلفه‌ها تحت تأثیر قرار نگیرند.

۴-۵- محافظت از داده

محافظت از داده‌ها در دو حوزه فناوری اطلاعات و مخابرات دارای راه‌حل‌های متفاوتی است. در حوزه فناوری اطلاعات، راه‌حل‌هایی کنترل‌کننده‌ای مانند POSTER پیشنهادشده که شبکه دسترسی محلی را توسط یک شبکه تفکیک‌شده برای مؤلفه‌های مختلف فراهم می‌آورد [۶۸]. یکی از دغدغه‌های امنیت داده، مدیریت کلید در نگهداری داده‌های رمزشده است. یک مدل مناسب این است که علاوه بر درنظرگرفتن نیازمندی‌های رمزنگاری بر اساس طول کلید و

[1] Distributed Denial of Service

[2] Schema

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

مدل رمزنگاری در تولید کلید و ذخیره‌سازی آن، فرآیندهای انجام آن خارج از فضای رایانش ابری و به‌وسیلهٔ پیمانه سخت‌افزاری امن[1] تولید و نگهداری کلید انجام پذیرد. از دیگر راه‌حل‌های محافظت از داده در زیرساخت‌های رایانش ابری، به‌کارگیری تصفیه داده[2] است. هدف این راه‌حل حذف داده‌های حساس از تجهیز ذخیره‌سازی در موقعیت‌های مختلف همانند انتقال یک ذخیره‌ساز از موقعیتی به موقعیت دیگر و یا حذف داده‌ها و غیرقابل بازآوری‌کردن از تجهیزات سخت‌افزاری در زمان تغییر وضعیت نمونه مجازی‌سازی‌شده است [۶۷].

با توجه به اینکه یکی از مهمترین اقدامات در ساختارهای ابری، پشتیبان‌گیری داده‌ها است، ضروری است سیاست‌ها ذخیره‌سازی و پشتیبان‌گیری داده‌ها به‌صورت رمزشده تدوین و محل ذخیره‌سازی آن همچنین دسترسی به آن به‌صورت امن صورت پذیرد [۷۰].

۶-۵- امنیت هایپروایزر

همان‌گونه که در بخش قبلی عنوان شد، هایپروایزر بالاترین سطح حمله را دارد. با توجه به این‌که فرض شده واسطهای کاربری هایپروایزر قابل اعتماد هستند، برای توسعه راه‌حل‌های امنیتی نیز مناسب هستند. برخی راه‌حل‌های تأمین امنیت هایپروایزر به‌طور کلی شامل موارد زیر است [۱۸]:

- مقابله نفوذ روتکیت با کنترل جامعیت توسط راه‌حل‌هایی مانند HyperGuard، Hypercheck، HyperSentry، HyperSafe و MGUARD؛
- امنیت واسط مدیریت هایپروایزر از متخاصم داخلی با تجزیه‌کردن واسطهای کاربری اختصاصی برای هر ماشین مجازی هم‌زمان با محیط اجرای یکسان همچنین رویدادنگاری و ممیزی؛
- جلوگیری از دسترسی به حافظه و سخت‌افزار در صورت عبور از ماشین مجازی با استفاده از راه‌حل‌هایی از جمله sHype، NoHype، TrustOSV، Min-V و DeHype؛
- به‌کارگیری روش‌ها و پروتکل‌های اعتبارسنجی مقصد مانند IVRS[3] در رویدادهای مهاجریت یک ماشین مجازی از یک هایپروایزر به هایپروایزر دیگر.

۷-۵- امنیت شبکه مجازی

برای امنیت شبکه مجازی‌شده، راه‌حل‌های امنیتی متفاوتی مانند دیوار آتش، سامانه‌های تشخیص‌تفوذ مبتنی بر ترافیک یا میزبان، سامانه‌های محافظت از ناهنجاری و موارد دیگر وجود دارد. نکته قابل بیان این است که کلیه موارد یادشده، در مواجهه با چالش پیکربندی پویا و مداوم شبکه‌های مجازی‌شده نیازمند ویژگی دریافت سیاست‌ها به‌صورت پیوسته و متمرکز هستند. یکی از راه‌حل‌ها استفاده از زبان‌های چندسطحی سیاست‌گذاری است. این زبان‌ها سیاست‌ها را در سه سطح بالا، میانی و پایین در سطح شبکه توزیع می‌کنند [۷۱].

۸-۵- مدیریت وصله

به‌منظور جلوگیری از تأثیر حملات ناشی از آسیب‌پذیری‌های شناخته‌شده، روش‌های مختلفی جهت مدیریت وصله در زیرساخت‌های ابری پیشنهاد شده است. Shavlik یکی از این دسته ابزارها است که پس از توزیع وصله‌ها میان ماشین‌های مجازی به‌وسیلهٔ سرویس‌دهندهٔ توزیع‌شده، سطح وصله اعمال‌شده را پایش و داده‌های وصله‌های اعمال شده را به همراه وابستگی‌های آن‌ها گردآوری می‌کند. همچنین می‌تواند به‌کارگیری ماشین‌های مجازی و راه‌اندازی آن‌ها را محدود و پس از اعمال کلیه وصله‌ها کرد [۷۲].

۹-۵- مقابله با حملات کانال جانبی

راه‌حل‌های مختلفی به‌منظور جلوگیری از حملات کانال جانبی ارائه شده؛ با این حال هنوز تضمینی برای استخراج داده‌های مهم مانند کلیدهای امنیتی ارائه نشده است. استفاده از Cache partitioning یکی از متداول‌ترین راه‌حل‌ها در این حوزه است. همچنین به‌کارگیری رنگ‌گذاری صفحات به‌صورت پویا، تقسیم‌بندی زمانی بوت و جلوگیری از ورود ماشین‌های غیر اعتماد از جمله رایج‌ترین روش‌های قابل به‌کارگیری در این حوزه است.

۶- نتیجه‌گیری

به‌کارگیری زیرساخت‌های رایانش ابری هر روز در حال گسترش است. یکی از مهم‌ترین فناوری‌هایی که با استفاده از این بستر در حال گسترش است، مجازی‌ساز کارکرد شبکه است. با توجه به این‌که تهدیدات مرتبط با زیرساخت‌های رایانش ابری به‌صورت مستقیم بر این فناوری تأثیرگذار است،

[1] Hardware Secure Module
[2] Sanitization
[3] Integrity Verification and Report Service

ضروری است، ابعاد مختلف این روش مورد بررسی قرار گیرد. یکی از مهم‌ترین ابعاد، تهدیدات حوزه امنیت سایبری است. در این مقاله تلاش شد پس از تشریح ویژگی‌های فنی، چالش‌های امنیتی زیرساخت‌های رایانش ابری و مجازی‌ساز کارکرد شبکه براساس مقالات مروری دارای بیشترین ارجاع علمی نسبت به دیگر مقالات موجود بررسی و سپس حملات مرتبط با هر یک بیان شود. دانتها پس از مقایسه تطبیقی حملات و گردش آن‌ها، رایج‌ترین راه‌حل‌های قابل به‌کارگیری تشریح شد.

۷- مراجع

[1] T. Tarik & A. Ksentini, & B. Sericola, "On Service Resilience in Cloud-Native 5G Mobile Systems," *IEEE Journal on Selected Areas in Communications*, 2016.

[2] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0, April 2009, https://cloudsecurityalliance.org/working-groups/virtualization/.

[3] Zh. Shao Ying & Scott-Hayward, S & J. Ludovic & H. Richard, Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications, 2017.

[4] P. Mell, T. Grance, "Definition of cloud computing", Technical report SP 800–145, *National Institute of Standard and* Technology (NIST), Gaithersburg, MD, 2007.

[5] ETSI. Network Functions Virtualisation (NFV); NFV Security; Architectural Framework. Technical report, ETSI GS NFV 002 V1.1.1, 2013-10.

[6] P. Bhat, & K. Dutta, "A Survey on Various Threats and Current State of Security in Android Platform", *ACM Computing Surveys*, Vol.52(1), pp.1–35, 2015.

[7] M. A. Khan, "A survey of security issues for cloud computing", *Journal of Network and Computer Applications*, Vol.71, pp.11–29, 2016.

[8] A. Singh, & K. Chatterjee, "Cloud security issues and challenges", *Journal of Network and Computer Applications*, vol.79, pp. 88–115, 2017.

[9] NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing

[10] ETSI GR NFV 001, "Network Functions Virtualization (NFV); Use Cases," May 2017, accessed: 2018-06-03. [Online].Available:https://docbox:etsi:org/ISG/NFV/Open/Publications pdf/SpecsReports/NFV%20001v1:2:1%20-%20GR%20-%20NFV%20Use%20Cases%20revision:pdf

[11] S. K. Majhi, & S. K. Dhal, "A Study on Security Vulnerability on Cloud Platforms", *Procedia Computer Science*, vol.78, pp.55–60, 2016.

[12] T. Bhatia, & A. K. Verma, "Data security in mobile cloud computing paradigm: a survey, taxonomy and open research issues", *The Journal of Supercomputing*, vol.73 (6), pp.2558–2631. 2017.

[13] A. N.Rukavitsyn, K.A.Borisenko, I.I. Holod, A. V. Shorov, "The method of ensuring confidentiality and integrity data in cloud computing", 2017 XX IEEE International Conference on Soft Computing and Measurements (SCM), 2017.

[14] J. Hong, K. Armstrong, H. Dan, F. Alaa, Kh.Noora, Khaled, "Systematic Identification of Threats in the Cloud: A Survey", *Computer Networks*, pp.150. 2018.

[15] B. Yi, X. Wang, K. Li , S. k. Das, & M. Huang, "A comprehensive survey of Network Function Virtualization", *Computer Networks*, vol.133, pp. 212–262, 2018.

[16] A. M. Alwakeel, A. K. Alnaim, & E. B. Fernandez, "A Survey of Network Function Virtualization Security", *SoutheastCon 2018*, 2018.

[17] D. Firoozjaei, M. Jeong, J. Paul, H. Ko, H. Kim, "Security challenges with network functions virtualization", *Future Generation Computer Systems*, vol.67, pp.315–324, 2017.

[18] R. Patil, & C. Modi, "An Exhaustive Survey on Security Concerns and Solutions at Different Components of Virtualization", *ACM Computing Surveys*, vol. 52(1), pp.1–38, 2019.

[19] R.Soni, S. Ambalkar, &P. Bansal, "Security and privacy in cloud computing", *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016.

[20] M. R. Anala, J.Shetty & G.Shobha, "A framework for secure live migration of virtual machines", *2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2013.

[21] K.Hashizume, D. G. Rosado, E. Fernández-Medina, & E. B. Fernandez, " An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, vol.4(1),pp. 5, 2013.

[22] D. A. B.Fernandes, L. F. B.Soares, J. V.Gomes, M. M. Freire &, P. R. M. Inácio, "Security issues in cloud environments: a survey",

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

[23] S.Singh, Y. S. Jeong, & J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions", *Journal of Network and Computer Applications*, vol.75, pp.200–222, 2016.

[24] G. Obasuyi, and A. Sari, "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment", *International Journal of Communications: Network and System Sciences*, vol.8, pp.260-273, 2015.

[25] M.Pearce, S. Zeadally, & R. Hunt, "Virtualization", *ACM Computing Surveys*, vol.45(2), pp.1–39, 2013.

[26] C.Modi, D.Patel, B. Borisaniya, A. Patel, M. Rajarajan, " A survey on security issues and solutions at different layers of Cloud computing", *The Journal of Supercomputing*, vol.63(2), pp.561–592, 2012.

[27] M. Gonzalez, N. Miers, Ch. Redígolo, F.Carvalho, T. Simplicio, M. Naslund, M. Pourzandi, " A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing", *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 1, pp. 231-238, 2011.

[28] W. Li, L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", *Cloud Computing*, pp.69–79, 2009.

[29] H. Farahmandian, "Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies", 10.1007/978-3-319-64653-4_, 2017.

[30] W. Li, L. Ping, "Trust Model to Enhance Security and Interoperability of Cloud Environment", *Cloud Computing. CloudCom 2009, Lecture Notes in Computer Scienc*e, vol 5931, 2009.

[31] A. Aljuhani, & T. Alharbi, "Virtualized Network Functions security attacks and vulnerabilities", *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC*), 2017.

[32] ETSI. Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance, ETSI GS NFV-SEC 003 V1.1.1, 2014-12.

[33] C. Wueest, M. B. Barcena, and L. O'Brien, "Mistakes in the IaaS Cloud Could Put Your Data At Risk," May 2015, accessed:2017-07-21 . [Online]. Available: http://www:symantec:com/content/en/us/enterprise/media/security response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk:pdf

[34] G. Pék, L. Butty´an, B. Bencsáth, "A survey of security issues in hardware virtualization", *ACM Computing Surveys*, vol.45 (3), pp.1–34, 2013.

[35] E. Markatos, "Large Scale Attacks on the Internet Lessons learned from the LOBSTER Project," Jun 2008, accessed: 2017-07-16. [Online]. Available: https://www:ist-lobster:org/publications/presentations/markatos-attacks:pdf

[36] M. Pattaranantakul, R. He, A. Meddahi, Z. Zhang,"SecMANO: Towards Network Functions Virtualization (NFV) Based Security MANagement and Orchestration", *2016 IEEE Trustcom/BigDataSE/ISPA,* 2016.

[37] Alcatel-Lucent, Providing security innfv-challenges and opportunities, Alcatel-Lucent White Paper. Technical Report, Alcatel-Lucent, 2014.

[38] "ETSI group specification: network functions virtualization (nfv) nfv security; security and trust guidance," Dec. 2014.

[39] ETSI GS NFV-MAN 001,"Network Functions Virtualization (NFV); Management and Orchestration", Dec 2014. Available: http://www.etsi.org/deliver/etsigs/NFV-MAN/001099/001/01.01.0160/gs nfv-man001v010101p.pdf

[40] FCC TAC Cybersecurity Working Group, "White Paper: Considerations for Securing SDN/NFV", Jan 2016. Available: https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2016/Securing%20-SDN-NFV%20-SWG-WP-Final.pdf

[41] S. Duflos, V. C. Gay, B. Kervella, and E. Horlait, "Improving the SLA-Based Management of QoS for Secure Multimedia Services", *Manage-ment of Multimedia Networks and Services*, Springer Berlin Heidelberg, Vol. 3754, Series. Lecture Notes in Computer Science, 2005, pp. 204-215, 2005.

[42] F. Sabahi, "Virtualization-level security in cloud computing", *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011.

[43] F. Reynaud, F. Aguessy, O. Bettan, M. Bouet, V. Conan, "Attacks against Network Functions Virtualization and Software-Defined Networking: State-of-the-art", *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, 2019.

[44] Ch. Simmons, E. Charles & S. Dasgupta, W., Chase, "AVOIDIT: A Cyber Attack Taxonomy",2009.

[45] T. Grance, W.Jansen, "Guide lines on security and privacy in public cloud computing", *NIST,* 2009.

[DOR: 20.1001.1.24763047.1398.8.2.3.1]

environment and the solutions", *2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT)*, 2013.

[57] A. Amittai , H. Sen & F. Bryan , G. Ramakrishna," Determinating Timing Channels in Compute Clouds", 2010.

[58] IMPERVA – Man in the Cloud (MITC) attacks, hacker intelligence initiative. July 2015 https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

[59] N. Gruschka, M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services", 2010 *IEEE 3rd International Conference on Cloud Computing*, 2010.

[60] M.Pattaranantakul, R. He, Q. Song, Z.Zhang, A. Meddahi, "NFV Security Survey: From Use Case Driven Threat Analysis to State-of-the-Art Countermeasures", *IEEE Communications Surveys & Tutorials,* vol.1, 2018.

[61] Microsoft, The stride threat model. [Online]. Available: http://msdn.microsoft.com

[62] Y. Yang, X. Chen, G. Wang, L. Cao, " An Identity and Access Management Architecture in Cloud", *2014 Seventh International Symposium on Computational Intelligence and Design,* 2014.

[63] J. Eduardo, J. Matías, M. Alaitz , V. Garay, J. Pinedo, " Deploying a Virtual Network Function over a Software Defined Network infrastructure: Experiences deploying an Access Control VNF", in the University of the Basque Country's OpenFlow Enabled Facility, 2014.

[64] M. Jensen, N. Gruschka, R. Herkenhöner, "A survey of attacks on web services", *Computer Science - Research and Development*, vol. 24(4), pp.185–197, 2009.

[65] B.B. Gupta, O.P. Badve, "Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment", *Neural Computing and Applications*, vol. 28(12), pp.3655–3682, 2016.

[66] Q. Shen, X. Yang, X. Yu, P. Sun, Y. Yang, Z.Wu, "Towards Data Isolation & Collaboration in Storage Cloud", *2011 IEEE Asia-Pacific Services Computing Conference*, 2011.

[67] W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", *2011 44th Hawaii International Conference on System Sciences*, 2011.

[68] Y. Juba, H.-H.Huang, K. Kawagoe, POSTER, *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, 2014.

[69] V. Del Piccolo, A. Amamou, K. Haddadou, G. Pujolle, " A Survey of Network Isolation

[46] H. Badis, D. Guillaume, G. Rida, "Understanding bot clouds from a system perspective: A principal component analysis", *IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World*, pp.1-9, 2014.

[47] Y. Jarraya, A. Eghtesadi, M. Debbabi, Y. Zhang, M. Pourzandi, " Cloud calculus: Security verification in elastic cloud computing platform", *2012 International Conference on Collaboration Technologies and Systems (CTS),* 2012.

[48] T.K, Subramaniam & B, Deepa," Security Attack Issues and Mitigation Techniques in Cloud Computing Environments", *International Journal of UbiComp*, Vol.7, pp. 1-11, 2016.

[49] D. Bhattacharyya, K. Dhruba & K. Kumar, "DDoS Attacks: Tools, Mitigation Approaches, and Probable Impact on Private Cloud Environment", 2014.

[50] N. Gonzalez, C. Miers, F. Redigolo, T. Carvalho, M. Simplicio, M. Naslund, & M. Pourzandi, "A Quantitative Analysis of Current Security Concerns and Solutions for Cloud Computing", *2011 IEEE Third International Conference on Cloud Computing Technology and Science*, 2011.

[51] M. Jensen, J.Schwenk, I. GruschkaN,"Ontechnical securityissues in cloud computing", *Proceedings of the 2009 IEEE international conference on cloud computing (CLOUD '09*), Washington, DC, USA: IEEE Comput Soc, pp.109–16, 2014.

[52] M. Swathy Akshaya, G. Padmavathi, "Taxonomy of Security Attacks and Risk Assessment of Cloud Computing", *Advances in Big Data and Cloud Computing*, pp.37–59, 2018.

[53] M. Xiao, D. Xiao, " Alert Verification Based on Attack Classification in Collaborative Intrusion Detection", *Eighth ACIS International Conference on Software Engineering*, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007), 2007.

[54] A. R.Riddle, S.M. Chung, " A Survey on the Security of Hypervisors in Cloud Computing", *2015 IEEE 35th International Conference on Distributed Computing Systems Workshops*, 2015.

[55] A. Pandey, S. Srivastava, " An approach for virtual machine image security", *2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014),* 2014.

[56] S. Meena, F. Daniel, N.A. Vasanthi, "Survey on various data integrity attacks in cloud

Solutions for Multi-Tenant Data Centers", *IEEE Communications Surveys & Tutorials*, vol.18(4), pp.2787–2821, 2016.

[70] N. Zhu, T. Chiueh, T, "Portable and Efficient Continuous Data Protection for Network File Servers", *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*, 2007.

[71] C. Basile, A. Lioy, C. Pitscheider, F. Valenza, M. Vallini, "A novel approach for integrating security policy enforcement with dynamic network virtualization", *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*, 2015.

[72] O.AbdElRahem, A.M. Bahaa-Eldin, A. Taha, "Virtualization security: A survey", *2016 11th International Conference on Computer Engineering & Systems (ICCES)*, 2016.

امیرحسین پورشمس تحصیلات مقطع کارشناسی را در رشته مهندسی کامپیوتر گرایش نرم‌افزار دانشگاه صنعتی اصفهان گذرانده و دانشجوی رشته رایانش امن در مقطع کارشناسی ارشد دانشگاه امام حسین (ع) است. وی هم‌اکنون به‌عنوان کارشناس امنیت شبکه‌های مخابراتی در شرکت ارتباطات سیار ایران در حال فعالیت است. علایق پژوهشی ایشان امنیت و اعتماد در نسل‌های مختلف شبکه‌های مخابراتی، زیرساخت‌های NFV -SDN و قراردادهای هوشمند می باشد.

محمدرضا حسنی آهنگر تحصیلات مقطع کارشناسی و کارشناسی ارشد خود را در رشته کامپیوتر دانشگاه جامع امام حسین(ع) گذرانده و دارای دکترای مهندسی کامپیوتر، هوش مصنوعی و رباتیک از دانشگاه علم و صنعت است. ایشان هم‌اکنون دارای رتبه استادی و ریاست دانشگاه جامع امام حسین (ع) را بر عهده دارد. ایشان همچنین به‌عنوان محقق برتر نهمین جشنواره سلمان فارسی و پژوهشگر برتر وزارت علوم، و دانشگاه امام حسین(ع) معرفی شده است.

محمود صالح اصفهانی تحصیلات مقطع کارشناسی را در رشته مهندسی کامپیوتر گرایش سخت‌افزار دانشگاه صنعتی اصفهان گذرانده و دارای مدرک کارشناسی ارشد و دکترا از دانشگاه‌های Wollongong و Latrobe استرالیا در رشته‌های سخت‌افزار و شبکه‌های کامپیوتری است. ایشان استادیار گروه کامپیوتر دانشگاه جامع امام حسین (ع) بوده و مشاور ایمنی شبکه شرکت ارتباطات سیار ایران می باشد.

[DOR: 20.1001.1.24763047.1398.8.2.3.1]