کنفرانس بین المللی مدیریت و مهندسی صنایع
۱۹ اسفند ۱۳۹۳
10 March 2015
International conference
ON MANAGEMENT AND INDUSTRIAL ENGINEERING
مرکز همایش های بین المللی صدا و سیما

شناسایی وتحلیل ریسک های بکارگیری رایانش ابری

روح اله تولایی ، سولماز حسین شبیری و روناک مدرسی

۱-روح الله تولایی، درجه استادیار، مقطع دکتری ، رشته مدیریت صنعتی، گروه مدیریت و حسابداری، دانشگاه شهید بهشتی
tavallaee.r@gmail.com

۲- سولماز حسین شبیری ، دانشجو ، کارشناسی ارشد ، رشته مدیریت فناوری اطلاعات ، دانشگاه شهید بهشتی
Shobeiri۶۰@gmail.com

۳- روناک مدرسی ، دانشجو ، کارشناسی ارشد ، رشته مدیریت فناوری اطلاعات ، دانشگاه شهید بهشتی
roonak.modarresi@yahoo.com

چکیده

در این تحقیق برخی از تهدیدات استفاده از رایانش ابری به همراه آسیب پذیری هایی که می تواند منجر به این تهدیدات شود ، شناسایی شده است و رابطه آسیب پذیری ها و تهدیدات تشریح گردیده است . رایانش ابری ، مدلی است که به ارائه ی دسترسی آسان ، توزیع شده وفراگیر به منابع محاسباتی تجمیعی و مشترک قابل پیکربندی ، می پردازد . در واقع رایانش ابری، یک پلتفرم ارائه انعطاف پذیر، مقرون به صرفه و اثبات شده برای فراهم آوردن خدمات فناوری اطلاعات برروی اینترنت می باشد. با این وجود، رایانش ابری نمایانگر سطح گسترده ای از ریسک می باشد چرا که خدمات ضروری ، به یک شخص ثالث سپرده می شود، که از اینرو حفظ امنیت و حریم خصوصی داده ها، پشتیبانی داده ها و پایایی خدمات را دشوار می سازد.این تحقیق ، از نظر هدف کاربردی بوده و از نظر گردآوری اطلاعات از نوع توصیفی پیمایشی است . دراین مقاله ابتدا به یک دید کلی نسبت به محاسبات ابری وسرویس‌های ارائه شده در آن پرداخته شده و سپس تهدیدها و آسیب پذیری‌هایی که در ادبیات مربوط به رایانش ابری و محیط آن وجود دارد ، شناسی گردیده است و همچنین رابطه بین آسیب پذیری ها و تهدیدات بیان گردیده است . شناسایی آسیب پذیری ها و تهدیدات به توسعه دهندگان در راستای یافتن راههای مقابله با این تهدیدات کمک خواهد نمود .

واژگان کلیدی: رایانش ابری، امنیت اطلاعات، مدل خدماتSPI، مدیریت ریسک.

کنفرانس بین المللی مدیریت و مهندسی صنایع
10 March 2015 International conference
ON MANAGEMENT AND INDUSTRIAL ENGINEERING
۱۹ اسفند ۱۳۹۳
مرکز همایش های بین المللی صدا و سیما

Identify and analyze the risks of using Cloud computing

Abstract

In this study, some of the threats in using cloud computing along with the vulnerabilities that lead to these threats are identified ,and the relationship between vulnerabilities and threats have been discussed .Cloud computing is a model to provide easy, distributed and sharing access of computational resource .In fact, cloud computing, a platform providing a flexible, cost-effective and proven to provide IT services on the Internet. However , cloud computing represents a broad level of risk because essential services are entrusted to a third party, so keep that data privacy and security, support data and service availability are too difficult . The objective of the survey is useable and the type of its collection is collect – descriptive . In this article , first we will get a general view towards cloud computing and services provided in it and then threats and vulnerabilities that exist in the literature and the environment of cloud computing have been identified , and the relationship between vulnerabilities and threats have been discussed . Identifying the threats and vulnerabilities allows the developers to find the procedures to face these threats .

Keywords: Cloud computing , Information security , SPI model , Risk management .

۱- مقدمه

اهمیت رایانش ابری رو به افزایش است، و توجه روزافزونی را در جوامع علمی و صنعتی به خود جلب کرده است. مطالعه ای توسط گارتنر (Gartner,۲۰۱۱)، رایانش ابری را به عنوان اولین تکنولوژی در میان ۱۰ تکنولوژی برتر و با چشم اندازی بهتر در سال های آتی از سوی شرکت ها و سازمان ها در نظر می گیرد.

رایانش ابری در قالب الگویی محاسباتی و مبتنی بر معماری توزیع، پدیدار گشته و از اهداف اصلی آن فراهم آوردن فضای ذخیره سازی سریع، ایمن و آسان داده ها و همچنین سرویس محاسباتی شبکه، در حالیکه تمامی منابع محاسباتی به عنوان سرویس هایی متصور می شوند که برروی اینترنت دریافت می گردند، به شمار می رود(Zhang ,۲۰۱۰, Zhao,۲۰۰۹).

رایانش ابری، تعدادی از مفاهیم و تکنولوژی ها از قبیل معماری سرویس گرا ، نسل دوم وب ، مجازی سازی و دیگر تکنولوژی ها را با تکیه بر اینترنت با هم ترکیب می نماید، و برنامه های کاربردی رایج را برروی شبکه از طریق مرورگرهای شبکه ای فراهم می آورند تا نیازهای محاسباتی کاربران را برآورده نماید ، در ضمن نرم افزار و داده هایشان برروی سرور ذخیره می گردد(Marinos,۲۰۰۹) .

اگرچه که در استفاده از رایانش ابری مزایای بسیاری وجود دارد، با این وجود تعداد موانع چشمگیر نیز در برابر استفاده رایانش ابری دیده می شود. یکی از مهم ترین موانع برای استفاده از آن امنیت می باشد (۲۰۱۰) KPMG .

از آنجایی که رایانش ابری نمایانگر الگوی محاسباتی نسبتاً جدیدی می باشد، در خصوص چگونگی اکتساب امنیت در تمامی سطوح (همانند شبکه، میزبان، برنامه های کاربردی، و سطوح داده ها) و همچنین چگونگی انتقال امنیت برنامه های کاربردی به رایانش ابری، تردید بسیاری وجود دارد (Rosado,۲۰۱۲) .

دغدغه های مربوط به امنیت به حوزه های مربوط به ریسک از جمله ذخیره سازی داده های خارجی، وابستگی به اینترنت «گروهی»، عدم کنترل، قابلیت چند مستاجری (استفاده اشتراکی توسط کاربران) و ادغام با امنیت داخلی، مرتبط می باشد. در مقایسه با تکنولوژی های رایج ، ابر ویژگی های خاص متعددی دارد، از جمله مقیاس بزرگ آن و این واقعیت که منابع متعلق به تأمین کنندگان ابری، کاملاً توزیع شده، ناهمگن و مجازی می باشند. مکانیزم های امنیتی رایج از جمله هویت، احراز هویت و صدور مجوز، برای ابرها در شکل جاری شان کافی نیستند (Li , Ping ,۲۰۰۹) .

در اینجا دسته ای از مسائل امنیتی مربوط به رایانش ابری که در مدلSPI (نرم افزار به عنوان یک سرویس ,پلتفرم به عنوان یک سرویس، زیرساخت به عنوان یک سرویس) برآن تمرکز شده است را ارائه می دهیم، و آسیب پذیری های اصلی را در این نوع از سیستم ها و همچنین مهم ترین تهدیدهای یافته شده در ادبیات موضوع در رابطه با رایانش ابری و محیط آن را شناسی خواهیم نمود.

در این تحقیق، فهرستی از آسیب پذیری ها و تهدیدها را ارائه می دهیم. همچنین، به توصیف ارتباط بین این آسیب پذیری ها و تهدیدات می پردازیم ؛ اینکه این آسیب پذیری ها چگونه برای اجرای یک حمله به کار برده می شوند را ارائه می نماییم. پس از شناسایی تهدیدات از ادبیات ، مصاحبه‌ای با

چندین خبره در حوزه رایانش ابری و مباحث مربوط به امنیت ، جهت تایید تهدیدات شناسایی شده صورت پذیرفته است که در بخش‌های آتی به آنها اشاره خواهد شد.

۲-ادبیات نظری تحقیق

مطابق با تعریف موسسه‌ملی‌فناوری‌واستانداردها(NIST)رایانش ابری مدلی است برای فراهم کردن دسترسی آسان براساس تقاضای کاربرازطریق شبکه به مجموعه ای ازمنابع رایانشی قابل تغییر و قابل پیکربندی (مثل :شبکه ها، سرورها ، فضای ذخیره سازی ، برنامه‌های کاربردی وسرویس‌ها) که این دسترسی بتواند با کمترین نیاز به مدیریت منابع ویا نیاز به دخالت مستقیم فراهم کننده سرویس به سرعت فراهم شده یا آزاد گردد . (Zhang ,۲۰۱۰)

مدلهای پیاده سازی رایانش ابری عبارتند از: ابرعمومی ، ابرخصوصی و ابرترکیبی که در زیر به توضیح مختصری از هریک از آنها خواهیم پرداخت :(صادق زاده ، ۱۳۸۶)

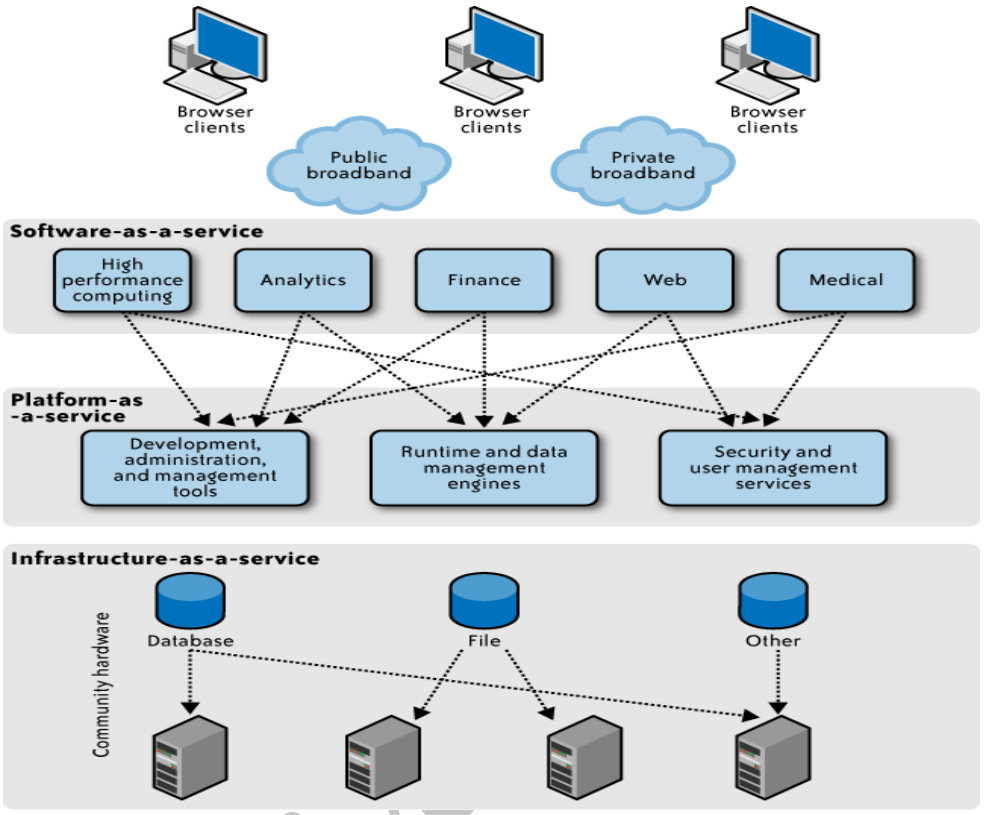
- درابرعمومی منابع محاسباتی به صورت پویا ازطریق اینترنت وبرنامه‌ها یا سرویس‌های تحت وب تهیه می شوند .ابرهای عمومی توسط شرکت‌های ارائه دهنده خدمات ابر اجرا می‌شوند وبرنامه‌های کاربران مختلف، روی سرورهای ابر ، سیستم های ذخیره‌سازی وشبکه‌ها باهم ترکیب می‌شوند.
- ابرخصوصی به رایانش ابری درشبکه های خصوصی اشاره می‌کند .ابرهای خصوصی برای استفاده انحصاری مشتریان مشخص ،کنترل کامل بر روی دادها ، امنیت وکیفیت خدمات به وجود می‌آیند .ابرهای خصوصی می‌توانند توسط خود سازمان ، شرکتها یا توسط فراهم آورندها بر ایجاد و مدیریت شوند.درواقع ابرخصوصی ، تنها از پشت فایروالها قابل دسترسی است . هرسازمانی که بخواهد زیرساخت‌های خود را روی ابر منتقل کند باید بتواند یک محیطامن جهت ارتباط با داده‌ها ایجادکند به طوریکه اطلاعات سازمان تنها در دسترس افراد مطمئن و کارمندان مشخصی قرار بگیرد .ابرخصوصی با درنظرداشتن این نیاز ، چنین فضایی را در اختیار سازمانها قرار می‌دهد .دراین حالت سازمانها به جای صرف هزینه زیاد جهت خریداری ، نصب و نگهداری

تجهیزات مرتبط با فعالیت‌های رایانشی خود ، ازخدمات ابرخصوصی بهره می‌گیرند ودرحقیقت تنها به اندازه توان رایانشی مورد نیازخود هزینه می‌کنند .

- محیط ابر ترکیبی ، مدلهای ابرهای عمومی وخصوصی را ترکیب می‌کند . ابرهای ترکیبی ، درتوزیع برنامه های کاربردی روی ابرهای عمومی و خصوصی پیچیدگی هایی دارند . به بیان دیگر ، زیرساخت ترکیبی ازچندین ابر(عمومی،خصوصی یا گروهی)تشکیل می‌شود که ممکن است هریک ازاین ابرها توسط یک ارائه کننده ایجاد شود و همه این ابرهادرکنار هم یک ابر ترکیبی را ایجادکنند.

مدل خدمات در رایانش ابری، تشریح کننده‌ی نوع خدماتی است که ارائه کننده خدمات به شما عرضه می‌کند. شناخته شده‌ترین نوع مدل خدمات، مدل‌های نرم‌افزار به عنوان سرویس ، پلتفرم به عنوان سرویس و زیرساخت به عنوان سرویس است که در اصطلاح مدل SPI(شکل ۱) نامیده می‌شود. مدل‌های خدماتی بر روی یکدیگر ساخته می‌شوند و معرف آنچه که سرویس دهنده باید مدیریت کند و آنچه که در مسئولیت مشتری است، می‌باشد.

شکل شماره (۱): مدل خدمات SPI



نرم افزار به عنوان سرویس ، پلتفرم به عنوان سرویس، زیرساخت به عنوان سرویس سه مدل اصلی و مهم محاسبات ابری هستند .هریک از این مدلها ، اثر متفاوتی بر امنیت دارا هستند .که در زیر به معرفی این سه مدل می پردازیم
(Zhang ,۲۰۱۰ , NIST, Subashini ,۲۰۱۱).

- نرم افزار به عنوان یک سرویس : توانایی فراهم آمده برای مشتری جهت استفاده از برنامه های کاربردی سرویس دهنده که در زیرساخت ابر اجرا می شوند، می باشد. دسترسی به این برنامه های کاربردی از ابزارهای مشتری های متعدد، از طریق یک رابط مشتری مانند یک مرورگر وب (همانند ایمیل وب محور) امکان پذیر می باشد.
- پلتفرم به عنوان یک سرویس : توانایی فراهم آمده برای مشتری، جهت به کارگیری برنامه های کاربردی خود مشتری در زیرساخت ابر بدون نصب هرگونه پلتفرم یا ابزاری برروی دستگاه های محلی خود می باشد. پلتفرم به عنوان یک سرویس به فراهم نمودن منابع لایه ای پلتفرم اطلاق می گردد که پشتیبانی سیستم عامل و چارچوب توسعه نرم افزار را که برای ساخت سرویس های سطح بالاتر به کار برده می شود را شامل می گردد.
- زیرساخت به عنوان یک سرویس : توانایی فراهم آمده برای مشتری ، که امکان پردازش، ذخیره سازی، و استفاده از دیگر منابع اساسی رایانشرا می دهد ، می باشد. در آن مشتری قادر به استقرار و اجرای نرم افزار دلخواه می باشد، که می تواند سیستم های عامل و برنامه های کاربردی را در برگیرد.

پیش از تحلیل چالش های امنیتی در رایانش ابری، می بایست به ارتباط و وابستگی های بین این الگوهای خدمات ابری پی ببریم (Alliance , ۲۰۱۱) .

پلتفرم به عنوان یک سرویس و نرم افزار به عنوان یک سرویس توسط زیرساخت به عنوان یک سرویس ، میزبانی می شوند؛ از اینرو، هر شکافی در زیرساخت به عنوان یک سرویس ، امنیت هر دو سرویس پلتفرم به عنوان یک سرویس و نرم افزار به عنوان یک سرویس را تحت تأثیر قرار می دهد، اما همچنین ممکن است عکس این قضیه نیز درست باشد. با این وجود، باید در نظر داشته باشیم که پلتفرم به عنوان یک سرویس، پلتفرمی برای ساخت و به خدمت گیری برنامه های کاربردی نرم افزار به عنوان یک سرویس را دراختیار می گذارد که وابستگی امنیت بین آنها را افزایش می دهد. این رابطه ها و وابستگی ها بین الگوهای ابر ممکن است همچنین منبعی از ریسک های امنیتی باشد. یک سرویس دهنده نرم افزار به عنوان یک سرویس ، ممکن است یک محیط توسعه از سرویس دهنده پلتفرم به عنوان یک سرویس کرایه نماید، همچنین ممکن است زیرساختی را نیز از سرویس دهنده زیرساخت به عنوان یک سرویس کرایه نماید. هر سرویس دهنده، مسئولیت امنیت سرویس های خود را برعهده دارد، که ممکن است به ترکیبی ناهماهنگ از الگوهای امنیتی منجر گردد. همچنین در این رابطه که کدام سرویس دهنده به هنگام رخداد یک حمله مسئول می‌باشد نیز گمراه کننده است.

امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات است که با هدف تضمین استمرار فعالیت های کاری ، به حداقل رساندن ریسک های کاری و به حداکثر رساندن میزان بازده سرمایه گذاری ها و فرصت هاصورت می پذیرد . (ISO۲۷۰۰۲)یک تهدید حمله ای بالقوه است که ممکن است به سوء استفاده از اطلاعات و منابع منجر گردد، و اصطلاح آسیب پذیری به خطاهایی در سیستم اطلاق می گردد که موفقیت یک حمله را امکان پذیر می سازد.

مسائل امنیتی نرم افزار به عنوان یک سرویس :

نرم افزار به عنوان یک سرویس ، بر حسب تقاضا سرویس هایی از برنامه های کاربردی از قبیل ایمیل، نرم افزار کنفرانس، و همچنین برنامه های کاربردی حرفه ای از قبیل برنامه ریزی منابع سازمانی، مدیریت زنجیره تامین ، و مدیریت ارتباطات با مشتری را فراهم می آورد.(Ju,۲۰۱۰)کاربران نرم افزار به عنوان یک سرویس ، از میان این سه الگوی ارائه خدمات در ابر، کنترل کمتری برروی امنیت دارند.

برنامه های کاربردی عموماً برروی اینترنت و توسط مرورگر وب ارائه می شوند . با این وجود، نقص های برنامه های کاربردی وب، ممکن است آسیب پذیری هایی را برای برنامه های کاربردی نرم افزار به عنوان یک سرویس خلق نماید. مهاجمین از وب برای به خطر انداختن رایانه کاربر و انجام فعالیت های مخرب از قبیل دزدیدن داده های حساس استفاده می نمایند .(Owens,۲۰۱۰) -چالش های امنیتی در برنامه های کاربردی نرم افزار به عنوان یک سرویس ، هیچ تفاوتی با تکنولوژی برنامه های کاربردی وب ندارند، اما راهکارهای امنیتی رایج به طور سازنده ای از آن در برابر مهاجمین محافظت نمی کنند، از اینرو رویکردهای جدید نیاز است (Subashini,۲۰۱۱).

امنیت داده ها، دغدغه ای شایع در هر نوع تکنولوژی می باشد، اما هنگامی که کاربران نرم افزار به عنوان یک سرویس ، به منظور امنیت مناسب ناچار به تکیه بر سرویس دهندگان خود باشند، امنیت داده‌ها به چالشی اساسی تبدیل می گردد (Rittinghouse,۲۰۰۹. Subashini,۲۰۱۱), . در نرم افزار به عنوان یک سرویس ، داده های سازمانی پردازش شده، و در ابر ذخیره می گردند. سرویس دهنده نرم افزار به عنوان یک سرویس ، مسئولیت امنیت داده ها به هنگام پردازش و ذخیره شدن را بر عهده دارد (Ju,۲۰۱۰) .

دسترسی به برنامه های کاربردی برروی اینترنت از طریق مرورگر وب، دسترسی به هر ابزار شبکه ای، شامل رایانه های همگانی و دستگاه های همراه، را آسان تر می سازد. با این وجود، همچنین سرویس را با ریسک های امنیتی بیشتری مواجه می سازد. اتحادیه امنیت ابر(۲۰۱۲) Alliance رساله ای

را منتشر کرده است که در آن به توصیف حالت کنونی رایانش موبایل و تهدیدهای مهم در این حوزه از قبیل نرم افزار مخرب موبایل، سرقت اطلاعات، شبکه های ناامن (بی سیم)، آسیب پذیری های یافت شده در سیستم عامل و برنامه های کاربردی رسمی، بازارهای ناامن می پردازد.

مسائل امنیتی پلتفرم به عنوان یک سرویس :

پلتفرم به عنوان یک سرویس، به کارگیری برنامه های کاربردی ابر-محور را بدون هزینه جهت خرید و حفظ لایه های نرم افزاری و سخت افزاری تسهیل می نماید (Subashini , Kavitha ,۲۰۱۱) .همانند نرم افزار به عنوان یک سرویس و زیرساخت به عنوان یک سرویس ، پلتفرم به عنوان یک سرویس نیز به شبکه ای ایمن و قابل اعتماد و یک مرورگر وب ایمن وابسته می باشد. امنیت برنامه کاربردی پلتفرم به عنوان یک سرویس از دو لایه نرم افزاری تشکیل شده است:

امنیت پلتفرم پلتفرم به عنوان یک سرویس (یعنی موتور اجرا)، و امنیت برنامه کاربردی مشتری که برروی پلتفرم پلتفرم به عنوان یک سرویس به کارگرفته شده است (Mather , Kumaraswamy , atif , ۲۰۰۹).

سرویس دهندگان پلتفرم به عنوان یک سرویس مسئولیت امنیت نرم افزار پلتفرم را برعهده دارند که موتور اجرا را شامل می شود که برنامه های کاربردی مشتری را اجرا می نماید. همانند نرم افزار به عنوان یک سرویس ، پلتفرم به عنوان یک سرویس نیز مسائل امنیتی داده ها را و دیگر چالش ها را در برداشته که در ادامه به آنها پرداخته می شود.

از نقطه نظر توسعه برنامه کاربردی، توسعه دهندگان با پیچیدگی ساخت برنامه های کاربردی ایمن که ممکن است در ابر میزبانی باشد، مواجه می‌شود . سرعت برنامه های کاربردی که در ابر تغییر می نمایند هم توسعه چرخه حیات سیستمو هم امنیت را تحت تأثیر قرار می دهد (Morsy, Grundy, Müller, ۲۰۱۰. Rittinghouse, Ransome ,۲۰۰۹) , توسعه دهندگان باید به خاطر داشته باشند که برنامه های کاربردی پلتفرم به عنوان یک سرویس باید مکرراً به روز شوند، بنابراین باید اطمینان حاصل کنند که فرآیندهای توسعه برنامه کاربردی شان برای همگام شدن با تغییرات به اندازه کافی انعطاف پذیر می باشند.(Ertaul, Singhal, Gökay,۲۰۱۰)با این وجود، توسعه دهندگان می بایست درک کنند که هر تغییری در عناصر پلتفرم به عنوان یک سرویس می تواند امنیت برنامه های کاربردی آنان را به مخاطره اندازد. علاوه بر تکنیک های توسعه ایمن، نیاز است توسعه دهندگان در مورد مسائل قانونی ذخیره‌سازی داده ها نیز آموزش ببینند، تا اینکه هیچ داده ای در مکان های نامناسب ذخیره

نشود. داده ها ممکن است در مکان های متفاوت با رژیم های قانونی مختلف ذخیره گردند که می تواند حریم خصوصی و امنیت آنان را به مخاطره اندازد.

در پلتفرم به عنوان یک سرویس ، توسعه دهندگان معمولاً به لایه های زیرین دسترسی ندارند، از اینرو سروس دهندگان مسئولیت امنیت زیرساخت های اساسی و همچنین سرویس های برنامه های کاربردی را برعهده دارند (Chandramouli, Mell,۲۰۱۰). حتی هنگامیکه توسعه دهندگان مسئول کنترل برنامه های کاربردی خود می‌باشند، از امنیت ابزارهای محیط توسعه که توسط سرویس دهندگان پلتفرم به عنوان یک سرویس فراهم آمده است، اطمینان ندارند.

در نتیجه، اطلاعات چندانی در ادبیات موضوع در خصوص مسائل امنیتی در پلتفرم به عنوان یک سرویس در دست نیست. نرم افزار به عنوان یک سرویس ارائه نرم افزار برروی وب را امکان پذیر می سازد، در حالیکه پلتفرم به عنوان یک سرویس ابزارهای توسعه ای برای ایجاد برنامه های کاربردی نرم افزار به عنوان یک سرویس در اختیار می گذارد. با این حال، ممکن است هردوی آنها از معماری با قابلیت چندمستأجری استفاده نمایند، بنابراین چند کاربر همزمان از نرم افزار مشابهی استفاده می نمایند. همچنین، برنامه های کاربردی پلتفرم به عنوان یک سرویس و داده های کاربر نیز در سرورهای ابر ذخیره شده اند که همانگونه که در بخش پیشین نیز به آن پرداخته شد، می تواند یک دغدغه امنیتی باشد. در نرم افزار به عنوان یک سرویس و پلتفرم به عنوان یک سرویس ، داده ها در ابر توسط یک برنامه کاربردی درحال اجرا مرتبط می باشند. امنیت این داده ها به هنگام پردازش ، انتقال، و ذخیره سازی به سرویس دهنده بستگی دارد.

مسائل امنیتی زیر ساخت به عنوان یک سرویس :

زیرساخت به عنوان یک سرویس مجموعه عظیمی از منابع از قبیل سرورها، محل های ذخیره سازی، شبکه ها و دیگر منابع رایانش را در قالب سیستم های مجازی شده فراهم می آورد که دست یابی به آنها از طریق اینترنت ممکن می باشد (Morsy, Grundy, Müller,۲۰۱۰).کاربران می توانند هر نرم افزاری را با کنترل و مدیریت تام، بر روی منابع اختصاص داده شده به آنها اجرا نمایند (Dahbur, Mohammad, Tarakji,۲۰۱۱). با زیرساخت به عنوان یک سرویس ، کاربران ابر در مقایسه با دیگر الگوها، مادامی که هیچ چاله امنیتی در ماشین مجازی وجود نداشته باشد، کنترل بهتری برروی امنیت دارند (Subashini, Kavitha,۲۰۱۱). آنها اجرای نرم افزار در ماشین های مجازی خود را کنترل می نمایند، و همچنین مسئولیت پیکربندی درست سیاست های امنیتی را برعهده دارند (Jaeger, Schiffman,۲۰۱۰). با این حال، زیر ساخت اساسی محاسبه، شبکه،وذخیره سازی توسط سرویسدهندگان ابر کنترل می گردد . سرویس دهندگان زیرساخت به عنوان یک سرویس ، می بایست تلاش بسیاری برای

امنیت سیستم های خود جهت به حداقل رساندن این تهدیدات به خرج دهند (Dawoud, Takouna, Meinel ,۲۰۱۰) . در اینجا، تعدادی مسائل امنیتی مرتبط با زیرساخت به عنوان یک سرویس آورده شده است.

امنیت ماشین مجازی همانند امنیت ماشین فیزیکی حائز اهمیت می باشد ، و هر گونه خطایی در هرکدام از آنها ممکن است دیگری را تحت تأثیر قرار دهد (Ertaul, Singhal, Gökay, ۲۰۱۰). محیط های مجازی شده، در برابر تمامی انواع حمله ها برای زیرساخت های نرمال آسیب پذیر می باشند؛ با این حال، امنیت چالش مهمتری است چرا که مجازی سازی امتیازاتی بیش از ورود و پیچیدگی بین ارتباط دارد(Reuben,۲۰۰۷) . برخلاف سرورهای فیزیکی ، ماشین های مجازی دارای دو مرز می باشند : فیزیکی و مجازی (Morsy, Grundy, Müller,۲۰۱۰) .

ناظر ماشین مجازی یا هایپرویژن ، مسئولیت ایزوله ماشین های مجازی را بر عهده دارد؛ از اینرو، اگر ناظر ماشین مجازی به خطر بیفتد، ماشین های مجازی آن نیز ممکن است به طور بالقوه به خطر بیفتند. ناظر ماشین مجازی یک نرم افزار سطح پایین می باشد که ماشین های مجازی اش را کنترل و مانیتور می نماید، از اینرو، همانند هر نرم افزار سنتی دیگری، نقص هایی امنیتی را به دنبال دارد (Reuben,۲۰۰۷) . هرقدر بتوان ناظر ماشین مجازی را کوچک و ساده نگه داشت ریسک آسیب‌پذیری‌های امنیتی کاهش می یابد ، چرا که یافتن و تعمیر هرگونه آسیب پذیری کار آسانی خواهد بود.

همچنین، مجازی سازی توانایی مهاجرت ماشین های مجازی بین سرورهای فیزیکی را ایجاد می نماید. این ویژگی سودمند می تواند مشکلات امنیتی را نیز به بار آورد (Dawoud, Takouna, Meinel,۲۰۱۰);
(Jasti, Shah, Nagaraj, Pendse,۲۰۱۰). یک مهاجم می تواند واحد مهاجرت در ناظر ماشین مجازی را به مخاطره انداخته و یک ماشین مجازی قربانی را به یک سرور مخرب انتقال دهد. همچنین، آشکار است که مهاجرت ماشین های مجازی محتوای ماشین های مجازی را در شبکه فاش نموده، که خود می تواند یکپارچگی و محرمانه بودن داده ها را به مخاطره اندازد. یک ماشین مجازی مخرب می تواند به میزبان دیگری مهاجرت نموده (با ناظر ماشین مجازی دیگری) و آن را به مخاطره اندازد.

ماشین های مجازی که برروی سرور مشابهی قرار دارند، می توانند پردازنده مرکزی ، حافظه، سیستم عامل ، و دیگر چیزها را با هم شریک شوند. اشتراک منابع بین ماشین های مجازی ممکن است امنیت هر ماشین مجازی را کاهش دهد. به عنوان نمونه، یک ماشین مجازی مخرب، می تواند به برخی اطلاعات در مورد دیگر ماشین های مجازی از طریق حافظه مشترک یا دیگر منابع مشترک، بدون نیاز به مخاطره انداختن هایپرویژن پی ببرد (Hashizume, Yoshioka, Fernandez,۲۰۱۳) . با استفاده از کانال های نهان، دو ماشین مجازی می توانند با نادیده گرفتن تمام قوانین تعریف شده از سوی واحد امنیت ناظر ماشین مجازی ، با هم ارتباط داشته باشند (Ranjith, Chandran, Kaleeswaran,۲۰۱۲) . از اینرو، یک ماشین مجازی مخرب، می تواند منابع مشترک را بدون اینکه ناظر ماشین مجازی متوجه شود، مانیتور نماید، لذا مهاجم می تواند به برخی اطلاعات درباره دیگر ماشین های مجازی نیز پی ببرد. در محیط های زیرساخت به عنوان یک سرویس ، تصویر ماشین مجازی ، یک قالب نرم افزار از پیش فراهم شده است که فایل های پیکربندی که برای ایجاد ماشین های مجازی استفاده می شوند را شامل می شود. از اینرو، این تصویرها برای امنیت همه جانبه ابر اساسی می باشند (Hashizume, Yoshioka, Fernandez,۲۰۱۳) ; (Wei, Zhang, Ammons, Bala, Ning,۲۰۰۹).

شخص می تواند یا تصویر ماشین مجازی خود را از ابتدا ایجاد نماید، یا اینکه می تواند از هر تصویر ذخیره شده در مخزن سرویس دهنده استفاده نماید. به عنوان مثال، آمازون مخزنی همگانی از تصویر را ارائه می دهد که دانلود یا آپلود تصویر ماشین مجازی برای کاربران را قانونی می کند. کاربران مخرب می توانند تصویرهایی شامل کد مخرب را در مخزن های همگانی ذخیره نمایند که دیگر کاربران و یا حتی سیستم ابر را به مخاطره می اندازد . به عنوان مثال، مهاجمی با اکانت معتبر می تواند تصویری را شامل کد مخرب از قبیل اسب تروژان ایجاد نماید. اگر مشتری دیگری از این تصویر استفاده نماید، ماشین مجازی ای که این مشتری ایجاد می نماید، با نرم افزار مخرب مخفی آلوده می شود. همچنین، نشت غیرعمدی داده ها،را می توان با تکثیر ماشین مجازی به وجود آورد (Grobauer, Walloschek, Stocker,۲۰۱۱). برخی اطلاعات محرمانه از جمله پسوورد یا کلیدهای رمزنگاری را می توان هنگامیکه تصویری ایجاد می گردد، ثبت نمود. اگر تصویر «پاک نشود»، این اطلاعات حساس می توانند برای دیگر کاربران فاش گردد.

علاوه براین، اگر اشتباهی رخ دهد ماشین های مجازی، اگر اشتباهی رخ دهد، می توانند به حالت پیشین خود برگردند. اما بازگشت ماشین های مجازی می تواند مجدداً آنها را با آسیب پذیری های امنیتی که پدید آمده بودند مواجه سازد یا می تواند پسوورد‌ها یا اکانت های که قبلاً از کار افتاده بودند را مجدداً فعال سازند. به منظور فراهم آوردن بازگشت، می بایست یک «کپی» از ماشین مجازی درست کنیم، که می تواند به انتشار خطاهای پیکربندی و دیگر آسیب پذیری ها منجر گردد (Garfinkel, Rosenblum,۲۰۰۵) ; (Rittinghouse, Ransome ۲۰۰۹) .

۳- پیشینه و نوآوری :

از جمله مقالاتی که در زمینه چالشهای مربوط به رایانش ابری مطرح گردیده عبارتند از (مقالات داخلی و خارجی می باشد):

- "تحلیل و بررسی چالشهای امنیتی موجود درمحاسبات ابری" که برخی از تهدیدات امنیتی در رایانش و برخی روشهای مقابله با آن را بیان نموده ولی اشاره ای به آسیب پذیری هایی که منجر به این تهدیدات می گردد ننموده است .
- "بررسی و تحلیل امنیت در فضای رایانش ابری وارائه راهکار" که صرفا به مسایل امنیتی مربوط به ماشینهای مجازی و راهکارهای مقابله با آن پرداخته است .
- "چالشهای امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن در راستای توسعه خدمات عمومی دولت الکترونیک"، که از دیدگا کلان به مسایل امنیتی مربوط به رایانش ابری پرداخته است .
- "امنیت رایانش ابری " ، در این مقاله رایانش ابری در سازمانهایی که درصدد کاهش هزینه های IT خود با واگذاری هزینه های نرم افزار خود بر روی سازمانهای شخص ثالث هستند ،مورد توجه زیادی قرار گرفته است. دو تکنولوژی چند مالکیتی، مجازی سازی وجود دارد که امنیت درباره رایانش ابری را ارائه می دهد.
- "محاسبات ابری برای سیستم های تشخیص نفوذ امنیت شبکه" که تجزیه وتحلیل ویژگی های رایانش ابری یک راه حل جامع در زمان واقعی بر اساس ارتباط بین پاد زهر سیستم ایمنی و شدت جریان حمله عامل بیماری زا پیشنهاد می‌کند . این مقاله همچنین سیستم ارزیابی دارایی و سیستم یکپارچه سازی شبکه را ترکیب می کند و همچنین بیان می کند لایه کاربردی، لایه ی است، لایه شبکه ممکن است فاکتور هایی باشند که بر خطرات شبکه تاثیر می گذارند.
- "مدلسازی و شبیه سازی رایانش ابری" که بیان می‌کند تکنولوژی مدلسازی و شبیه سازی تبدیل به ابزاری کارآمد و قدرتمند شده و رایانش ابری بهترین راه حل برای رویارویی با این موضوعات است. این مقاله، براساس بهترین شناخت ، نتایج شبیه سازی و مدلسازی رایانش ابری را نشان می دهد . از مرور مفاهیم پایه رایانش ابری و موضوعات امنیتی آن ، تا شبیه سازهای فعلی رایانش ابری را بیان می نماید.
- "تکنیک های تخصیص منبع در سرویس های رایانش ابری-چالش های پژوهشی برای برنامه های کاربردی " که بیان می کند تخصیص و زمانبندی منبع باعث شده تا سرویس های وب زیادی در کنار هم قرار گیرند. همچنین به تخمین استراتژی های تخصیص منبع در شبکه پرداخته و کاربرد آنها را در محیط محاسبات ابری بررسی می‌کند ، همچنین مختصری نیز برای تخصیص منابع در رایانش ابری، توضیح داده شده است و به بررسی و دسته بندی آخرین چالش های مرتبط با پروسه ی تخصیص منبع در رایانش ابریو بر حسب انواع تکنیک های تخصیص منبع پرداخته شده است .
- "رویکرد جدید تعادل بار در رایانش ابری" که محیط‌های رایانش ابری مقیاس پذیری را برای برنامه‌های کاربردی با ارائه مجازی‌سازی منابع پویا ارائه می‌نمایند و نشان میدهد حرکت برنامه‌های کاربردی به محیط رایانش ابری نیاز به زمان بندی دارد که آن را برای استفاده از سرویس‌های ابری برای تسهیل در اجرا قادر می‌سازد .
- " داده کاوی در رایانش ابری" که چگونگی استفاده از داده کاوی را در رایانش ابری شرح می دهد،و نشان میدهد داده کاوی برای استخراج اطلاعات مفید بالقوه از داده های خام به کار می رود و یک پارچه سازی تکنیک های داده کاوی در فعالیت های مستمر ، موقعیت رایجی پیدا کرده است.
- "مسائل امنیت رایانش ابری و چالش ها" ، که در مورد مسائل امنیتی، الزامات و چالش هایی که ارائه دهندگان سرویس های ابری با آن در رایانش ابری روبرو می شوند، بحث می کند. استانداردهای امنیتی توصیه شده و مدلهای مدیریتی برای پرداختن به مسائل تکنیکی است.

در این تحقیق علاوه بر دسته بندی تهدیدات به بررسی آسیب پذیری‌هایی که منجر به تهدیدات می گردد پرداخته شده است و با طرح مصاحبه ای در میان تعدادی از خبرگان در زمینه رایانش ابری ، به تایید تهدیدات شناسایی شده ، پرداخته شده است . علاوه بر شناسایی تهدیدات و آسیب پذیری ها ، رابطه بین آنها نیز در این تحقیق مورد بررسی قرار گرفته است .

۴- روش شناسی تحقیق

در این مقاله به مروری سیستماتیک از ادبیات موجود مربوط به امنیت در رایانش ابری، نه تنها به منظور خلاصه بندی آسیب پذیری ها و تهدیدات موجود در رابطه با این موضوع، بلکه به منظور شناسایی و تحلیل وضعیت موجود و مهمترین مسائل امنیتی در رایانش ابری، پرداخته شده است . این تحقیق با شناسایی تهدیدات و آسیب پذیری های مربوط به رایانش ابری ، به توسعه دهندگان و مجریان رایانش ابری کمک می کند تا راهکارهای مقابله با این تهدیدات را شناسایی نموده و در ایجاد ابری ایمن تلاش کنند ، لذا این تحقیق ، کاربردی است و به جهت گردآوری اطلاعات از منابع علمی و مصاحبه ، تحقیق از نوع توصیفی پیماشی می باشد.

تمرکز مساله در این تحقیق بر شناسایی مسائل مربوط به رایانش ابری می باشد که شامل آسیب پذیری ها، تهدیدات، نیازها و راهکارهای امنیت در رایانش ابری است. این مسأله می بایست با هدف تحقیق حاضر مرتبط باشد؛ یعنی شناسایی آسیب پذیری ها و تهدیدات . کلمات کلیدی و مفاهیم مرتبطی که این سوال را تشکیل می دهند، و اینکه در طول تحقیق مکررا به کار گرفته شده‌اند عبارتند از: سیستم های ابری ایمن، امنیت ابری، امنیت الگوهای ارائه (خدمات)، امنیت SPI، امنیت نرم افزار به عنوان یک سرویس ، امنیت پلتفرم به عنوان یک سرویس ، امنیت زیرساخت به عنوان یک سرویس ، تهدیدات ابری، آسیب پذیری های ابری .

انتخاب معیارهایی که به موجب آن منابع مطالعاتی را ارزیابی نمودیم، بر پایه تجربیات تحقیقاتی نویسندگان اثر حاضر استوار بود، و ضمن انتخاب این منابع محدودیت های خاصی نیز درنظر گرفته شده است: مطالعات موجود صرفا در منابع انگلیسی و فارسی نوشته شده باشند و این منابع می بایست بر روی وب در دسترس باشند. مطالعات انجام شده مسائل وموضوعاتی را شامل می شوند که امنیت در رایانش ابری را در نظر می گیرند و اینکه این مطالعات می بایست به توصیف تهدیدات، آسیب پذیری ها و ریسک ها بپردازند. علاوه بر مطالعات در ادبیات گذشته مصاحبه ای با خبرگان صورت پذیرفت و از این طریق تهدیدات شناسایی شده را تایید نموده ایم .

۵-یافته های تحقیق

تهدیدات ، آسیب پذیری ها و ارتباط آنها

در این بخش از مقاله، یافته های تحقیق در زمینه آسیب پذیری های موجود در رایانش ابری ارائه و تحلیل شده و برای هر آسیب پذیری و تهدید، مشخص شده است که چه الگو یا الگوهای سرویس دهی تحت تأثیر این مشکلات امنیتی قرار می گیرند.

جدول شماره۱، تحلیل از تهدیدات موجود در رایانش ابری را ارائه می نماید. این تحلیل، توصیفی خلاصه از مهمترین آسیب پذیری ها به دست می دهد، و مشخص می کند که چه الگوهای سرویس ابری (SPI) متأثر از آن می باشند. در این تحلیل، اساساً بر آسیب پذیری های تکنولوژی محور تمرکز می نماییم؛ با این وجود، آسیب پذیری های دیگری نیز وجود دارد که در هر سازمانی شایع می باشند، اما از آنجایی که می توانند تأثیری منفی برروی امنیت ابر و پلتفرم اساسی آن داشته باشند، می بایست آنها را مد نظر داشته باشیم. برخی از آسیب پذیری ها عبارتند از:

- عدم غربالگری کارکنان و اقدامات ضعیف مربوط به استخدام (Alliance ,۲۰۱۰) ممکن است برخی از ارائه دهندگان ابر غربالگری ای از کارکنان یا سرویس دهندگان خود به عمل نیاورند. کاربران ممتاز از جمله مدیران ابر، دسترسی نامحدودی به داده های ابر دارند.
- عدم بررسی سابقه مشتری - بسیاری از سرویس دهندگان ابر، سابقه مشتری های خود را بررسی نمی کنند، و تقریباً هر کسی می تواند با استفاده از کارت اعتباری معتبر و از طریق ایمیل یک اکانت را باز نماید. اکانت های جعلی، اجرای هر گونه اقدام مخربی را بدون شناسایی شدن برای مهاجم امکان پذیر می سازد (Alliance ,۲۰۱۰).
- عدم آموزش های امنیتی - افراد همچنان یک نقطه ضعف از حیث امنیت اطلاعات به شمار می روند (Bezemer , Zaidman ,۲۰۱۰). این قضیه در هر سازمانی صادق است؛ با این حال، در ابر، تأثیر بیشتری دارد چرا که افراد بیشتری با ابر در تعامل می باشند: سرویس دهندگان ابر، سرویس دهندگان شخص ثالث، تأمین کنندگان، مشتری های سازمانی، و کاربران نهایی.

جدول شماره (۱):توصیف آسیب پذیری های موجود در رایانش ابری

عنوان آسیب پذیری	توصیف
استفاده از رابط های کاربردی برنامه نویسی غیر ایمن	ارائه دهندگان ابر ، سرویس هایی را ارائه می دهند که می توان از طریق رابط های کاربردی برنامه نویسی به آنها دسترسی پیدا کرد (Dawoud, Takouna, Meine,۲۰۱۰). امنیت ابر به امنیت این رابط ها بستگی دارد (Alliance ,۲۰۱۰) . برخی مشکلات عبارتند از: ۱. اعتبار ضعیف ۲. بررسی ناکافی مجوز ۳. اعتبارسنجی ناکافی داده های ورودی
تخصیص نامحدود منابع	الگوسازی نادرست استفاده منابع می تواند به رزرو بیش از حد یا تامین اضافه و بلااستفاده منجر گردد (۲۰۰۹) ENISA.

آسیب پذیری های مربوط به داده ها	۱. ممکن است داده ها با داده های کاربران ناشناس (رقبا، یا متجاوزان) با جداسازی ضعیف در کنار هم چیده شوند(Viega ,۲۰۰۹) . ۲. داده ها ممکن است طبق نظام هایی که از قانون های متفاوتی دارند، پیروی می کنند کنار هم قرار بگیرند Ertaul, Singhal, Gökay ۲۰۱۰);(Carlin, Curran ,۲۰۱۱);(Bisong, Rahman ,۲۰۱۱) (. ۳. پاکسازی ناقص دادها- داده های به طور کامل برداشته نمی شوند ;(Winkler,۲۰۱۱) (Ertaul, Singhal, Gökay ,۲۰۱۰);(Grobauer, Walloschek,Stocker ,۲۰۱۱); (Jansen ,۲۰۱۱) ۴. پشتیبانی داده ها از سوی سرویس دهندگان شخص ثالث غیرقابل اعتماد صورت می گیرد (Winkler,۲۰۱۱)); (Jansen ,۲۰۱۱) . ۵. اطلاعات درمورد مکان داده ها عموماً دردسترس نبوده یابرای کاربران فاش نمی شود Jansen ,۲۰۱۱) (.
آسیب پذیری ها در ماشین های مجازی	۱.کانال های مخفی احتمالی در کنار ماشین های مجازی (Ranjith, Chandran, Kaleeswaran,۲۰۱۲); (Ristenpart,Tromer,Shacham); (Zhang, Juels, Reiter, Ristenpart,۲۰۱۲) ۲. مهاجرت کنترل نشده - ماشین های مجازیمی توانند به دلیل تحمل پذیری (تولرانس) خطا، بالانس بار، یا تعمیر و نگهداری سخت افزار، از سروری به سرور دیگر انتقال یابند (Garfinkel, Rosenblum,۲۰۰۵); (Dawoud, Takouna, Meinel,۲۰۱۰) . ۳. بازگشت کنترل نشده ممکن است به برگشت آسیب پذیری ها منجر گردد (Garfinkel, Rosenblum,۲۰۰۵) . ۴. ماشین های مجازی دارای آدرس های IP می باشند که برای هر کسی درون ابر قابل رویت می باشد- مهاجمین می توانند موقعیت هدف ماشین مجازیدرون ابر را شناسایی کنند (نقشه کشی ابر) (Garfinkel, Rosenblum,۲۰۰۵) .
آسیب پذیری ها در تصاویر ماشین مجازی	۱.جایگذاری کنترل نشده تصاویر ماشین های مجازی در مخزن های همگانی (Morsy,Grundy, Müller ,۲۰۱۰) . ۲. تصاویر ماشین مجازی را نمی توان پچ کرد(Garfinkel, Rosenblum,۲۰۰۵) .
آسیب پذیری ها در هایپرویژن ها	۱. کد هایپرویژن پیچیده (Wang, Jiang ,۲۰۱۰) . ۲. پیکربندی انعطاف پذیر ماشین های مجازی یا هایپرویژن ها برای برآورده ساختن نیازهای سازمان را می توان به کار برد
آسیب پذیری ها در شبکه های مجازی	به اشتراک گذاری پل های مجازی توسط چندین ماشین مجازی (Wu, Ding, Winer, Yao ,۲۰۱۰) .

رایانش ابری، اهرم بسیاری از تکنولوژی های موجود از قبیل سروییس های وب، مرورگرهای وب، و مجازی سازی می باشد، که در تکامل محیط ابر نقش دارند. از اینرو، هر آسیب پذیری مرتبط با این تکنولوژی ها، ابر را نیز تحت تأثیر قرار می دهد، و حتی می تواند تأثیر معناداری داشته باشد.

شکل شماره (۲):دسته بندی تهدیدات موجود در رایانش ابری

شمای کلی از تهدیدات شناسایی شده در شکل بالا نمایش داده شده است و در جدول زیر، همانند جدول ۱، به شرح و توصیف تهدیداتشناسایی شده ، پرداخته شده است . لازم به ذکر است تهدیدات شناسایی شده تنها تهدیدات مربوط به تکنولوژی به کار برده شده در محیط های ابر می باشند. ما تمرکز بیشتری برروی تهدیداتی داریم که با داده های ذخیره شده ، داده هایی که از راه دور پردازش می شوند، و همچنین داده هایی که در مجازی سازی و منابع با هم در اشتراک هستند، مرتبط می باشند.

جدول شماره (۲):توصیف تهدیدات موجود در رایانش ابری

عنوان تهدیدات	توصیف
سرقت اکانت یا سرویس	سرقت اکانت به شیوه های مختلفی صورت می گیرد، از جمله اعتبار ضعیف. اگر مهاجمی به اعتبار یک کاربر دسترسی پیدا کند، می تواند فعالیت های مخربی از جمله دسترسی به داده های حساس، دستکاری داده ها، تغییر مسیر هر گونه معامله را انجام دهد (Alliance ,۲۰۱۰).
مهار داده ها	از آنجایی که نمی توان داده ها را به طور کامل از میان برداشت، مگر اینکه دستگاه خراب شود، ممکن است مهاجمین توانایی بازیابی داده ها را داشته باشند (Mather, Kumaraswamy, Latif,۲۰۰۹);(ENISA ,۲۰۰۹);(Jansen,۲۰۱۱) .
نشت داده ها	نشت داده ها زمانی اتفاق می افتد که داده ها به هنگام ذخیره شدن، پردازش، یا انتقال به دست افراد نادرستی می افتد (Grobauer, Walloschek ,۲۰۰۹);(ENISA ,۲۰۱۰);(Alliance (Stocker ,۲۰۱۱) .
محرومیت از سرویس	این امکان وجود دارد که یک کاربر شرور تمام منابع ممکن را به دست گیرد. از اینرو، سیستم به دلیل در دسترس نبودن منبع، قادر به برآورده کردن نیازهای دیگر کاربران قانونی نمی باشد.
انحراف داده های مشتری	کاربران با دستکاری داده های ارسال شده از اجزای برنامه کاربردی سرور به برنامه های کاربردی وب حمله می کنند (OWASP ,۲۰۱۰);(Grobauer, Walloschek, Stocker,۲۰۱۱) .
کنترل هایپروژن	زمانی رخ می دهد که ماشین مجازی قادر به دستیابی به ماشین مجازی دیگری باشد (یعنی با استفاده از آسیب پذیری هایپرویژن(Jasti, Shah, Nagaraj, Pendse,۲۰۱۰);(ENISA ,۲۰۰۹) .
ایجاد ماشین مجازی مخرب	مهاجمی که یک اکانت معتبر درست می کند، می تواند یک تصویر ماشین مجازی حاوی کد مخرب مانند اسب تروژان درست کرده وآن را درمخزن سرویس دهنده ذخیره نماید (Grobauer,Walloschek, Stocker,۲۰۱۱) .
مهاجرت ناامن ماشین مجازی	مهاجرت زنده ماشین های مجازی ، محتوای فایل های ماشین مجازی را در شبکه قرار می دهد. یک مهاجم می تواند اقدامات زیر را انجام دهد: ۱. طی مهاجرت، به طور غیرقانونی به داده ها دست یابد (Dawoud , Takouna , Meinel ,۲۰۱۰). ۲. ماشین مجازی را به یک میزبان غیرقابل اعتماد انتقال دهد(Garfinkel , Rosenblum ,۲۰۰۵) . ۳. چندین ماشین مجازی را ایجاد کرده و مهاجرت نماید که خرابی ایجاد کند
Sniffing/ spoofing شبکه های مجازی	یک ماشین مجازی مخرب می تواند به شبکه مجازی گوش داده و یا حتی از ARP spoofing برای ارسال مجدد بسته ها از یک ماشین مجازی به ماشین مجازی دیگری استفاده نماید (Wu , Ding , Winer , Yao ,۲۰۱۰);(Reuben ,۲۰۰۷).

ارتباط بین تهدیدات و آسیب پذیری ها در جدول ۳ نشان داده شده است، این جدول نشان می دهد یک تهدید در اثر کدامیک از آسیب پذیری ها ممکن است رخ دهد و سیستم را به خطر بیندازد. هدف از این جدول این است که در نهایت بتوان اقدامات پیشگیرانه موجود را شناسایی نمود .

جدول شماره (۳): ارتباط بین تهدیدات و آسیب پذیری های رایانش ابری

تهدید	آسیب پذیری ها
سرقت اکانت یا سرویس	استفاده از رابط های کاربردی برنامه نویسی غیر ایمن
مهار داده ها	آسیب پذیری های مربوط به داده ها
نشت داده ها	آسیب پذیری های مربوط به داده ها آسیب پذیری ها در ماشین های مجازی آسیب پذیری ها در تصاویر ماشین مجازی آسیب پذیری در شبکه های مجازی
محرومیت از سرویس	استفاده از رابط های کاربردی برنامه نویسی غیر ایمن تخصیص نامحدود منابع
انحراف داده های مشتری	استفاده از رابط های کاربردی برنامه نویسی غیر ایمن
کنترل هایپروژن	آسیب پذیری ها در ماشین های مجازی آسیب پذیری ها در هایپروژن ها
ایجاد ماشین مجازی مخرب	آسیب پذیری ها در تصاویر ماشین مجازی
مهاجرت ناامن ماشین مجازی	آسیب پذیری ها در ماشین های مجازی
Sniffing/ spoofing شبکه های مجازی	آسیب پذیری ها در شبکه های مجازی

جمع بندی ونتیجه گیری

رایانش ابری مفهوم نسبتاً جدیدی است که تعداد مناسبی مزیت را در اختیار بهره برداران قرار می دهد ؛ با این حال، تعدادی مشکلات امنیتی را به بارمی آورد که ممکن است استفاده از آن را آهسته نمایند. دانستن این موضوع که چه آسیب پذیری هایی در رایانش ابری وجود دارد به سازمان ها در تغییر مسیر خود به سمت ابر ایمن کمک خواهد نمود. از آنجایی که رایانش ابری اهرم تکنولوژی های بسیاری است، از اینرو مسائل امنیتی آنها را نیز به ارث برده است. ما مسائل امنیتی برای الگوی SPIرا ارائه نمودیم: زیرساخت به عنوان یک
سرویس ، پلتفرم به عنوان یک سرویس ، و نرم افزار به عنوان یک سرویس ، که بنا بر مدل فرق می کنند. مجازی سازی که اشتراک یک سرور فیزیکی را برای چندین کاربر ممکن می سازد، یکی از دغدغه های اصلی برای کاربران ابر می باشد. همچنین، چالش دیگر این است که انواع متفاوتی از تکنولوژی های مجازی سازی وجود دارد، و هر نوع ممکن است رویکرد متفاوتی به مکانیزم های امنیتی داشته باشد. شبکه های مجازی نیز، به خصوص به هنگام ارتباط با ماشین های مجازی راه دور، هدف برخی حمله ها می باشند. از دیدگاه نویسندگان این مقاله ،شمارش مسائل امنیتی کافی نبوده ، لذا رابطه ای بین آسیب پذیری و تهدیدات ایجاد کردیم، تا بتوانیم مشخص کنیم چه آسیب پذیری هایی در اجرای این تهدیدات نقش داشته تا در نهایت بتوانیم سیستم را قوی تر سازیم .

بنابر یافته های این تحقیق سازمانهایی که در حال حاضر از مفهوم رایانش ابری در فرآیندهای کاری خود استفاده می‌کنند با ریسکهای امنیتی نظیر : سرقت اکانت یا سرویس ، مهار داده ها ، نشت داده ها ، محرومیت از سرویس ، انحراف داده های مشتری ، کنترل هایپروژن ، ایجاد ماشین مجازی مخرب ، مهاجرت ناامن ماشین مجازی ، Sniffing/ spoofing شبکه های مجازی رو به رو می شوند که با شناسایی این تهدیدات می توان راهکارهایی را جهت عدم بروز این تهدیدات یافت .

منابع ومراجع :

۱. صادق زاده ، پیام ؛ بهره پور، داوود ؛ صادق زاده ، پیمان (۱۳۹۲) . "تحلیل و بررسی چالش های امنیتی موجود در محاسبات ابری".
۲. حقشناسی ، مهدی ؛ کارگر ، محمدجواد . "بررسی و تحلیل امنیت در فضای رایانش ابری و ارائه راهکار" .

۳. صدرالساداتی ، سیدمحسن ؛ کارگر ، محمدجواد . "چالشهای امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن درراستای توسعه خدمات عمومی دولت الکترونیک" .

۴. Gartner Inc Gartner identifies the Top ۱۰ strategic technologies for(۲۰۱۱).

۵. Zhang S, Zhang S, Chen X, Huo X ;(۲۰۱۰) .Cloud Computing Research andDevelopment Trend. Second International Conference on Future.

۶.Marinos A, Briscoe G;(,۲۰۰۹).Community Cloud Computing.۱stInternational Conference on Cloud Computing (CloudCom), Beijing, China.

۷. KPMG ;(,۲۰۱۰) From hype to future: KPMG's ۲۰۱۰ Cloud Computing survey..

۸. Rosado DG, Gómez R, Mellado D, Fernández-Medina E;(۲۰۱۲).Security analysis in the migration to cloud environments.

۹. Li W, Ping L;(۲۰۰۹). Trust model to enhance Security and interoperability ofCloud environment. Proceedings of the ۱st International conference onCloud Computing.Springer Berlin Heidelberg, Beijing, China.

۱۰. Zhang Q, Cheng L, Boutaba R; (,۲۰۱۰) .Cloud Computing: state-of-the-art andresearch challenges. Journal of Internet Services Applications.

۱۱. Cloud Security Alliance;(,۲۰۱۱) . Security guidance for critical areas of focus inCloud Computing V۳.

۱۲. Owens D;(۲۰۱۰) . Securing elasticity in the Cloud .

۱۳.Subashini S, Kavitha V;(۲۰۱۱). A survey on Security issues in service deliverymodels of Cloud Computing.

۱۴. Rittinghouse JW, Ransome JF;(۲۰۰۹).Security in the Cloud.CloudComputing.Implementation, Management, and Security, CRC Press.

۱۵.Mather T, Kumaraswamy S, Latif S;(,۲۰۰۹) .Cloud Security and Privacy. O'Reilly, Media, Inc., Sebastopol, CA .

۱۶. Morsy MA, Grundy J, Müller I;(۲۰۱۰) . An analysis of the Cloud ComputingSecurity problem.Proceedings of APSEC ۲۰۱۰ Cloud Workshop.APSEC,Sydney, Australia.

۱۷. Ertaul L, Singhal S, Gökay S ;(۲۰۱۰). Security challenges in Cloud Computing.Proceedings of the ۲۰۱۰ International conference on Security and Management SAM'۱۰.CSREA Press, Las Vegas, US.

۱۸. Chandramouli R, Mell P;(۲۰۱۰).State of Security readiness.

۱۹. Dahbur K, Mohammad B, Tarakji AB ;(۲۰۱۱) . A survey of risks, threats andvulnerabilities in Cloud Computing.Proceedings of the ۲۰۱۱International conference on intelligent semantic Web-services andapplications. Amman, Jordan.

۲۰. Jaeger T, Schiffman J ;(۲۰۱۰) .cloudy with a chance of Securitychallenges and improvements. IEEE Security Privacy .

۲۱. Dawoud W, Takouna I, Meinel C;(,۲۰۱۰) . Infrastructure as a service security:Challenges and solutions. the ۷th International Conference onInformatics and Systems (INFOS), Potsdam, Germany. IEEE ComputerSociety, Washington, DC, USA .

۲۲. Reuben JS ;(۲۰۰۷) . A survey on virtual machine Security.Seminar on NetworkSecurity. Technical report, Helsinki University of Technology, October ۲۰۰۷ .

۲۳. Jasti A, Shah P, Nagaraj R, Pendse R ;(۲۰۱۰). Security in multi-tenancy cloud.In: IEEE International Carnahan Conference on Security Technology (ICCST), KS,USA. IEEE Computer Society, Washington,DC, USA .

۲۴. Hashizume K, Yoshioka N, Fernandez EB;(,۲۰۱۳). Three misuse patterns forCloud Computing. Rosado DG, Mellado D, Fernandez-Medina E, PiattiniM (ed) Security engineering for Cloud Computing: approaches and Tools.IGI Global, Pennsylvania, United States .

۲۵. Ranjith P, Chandran P, Kaleeswaran S;(,۲۰۱۲) . On covert channels betweenvirtual machines. Journal in Computer Virology Springer .

۲۶. Grobauer B, Walloschek T, Stocker E;(۲۰۱۱) .Understanding CloudComputing vulnerabilities. IEEE Security Privacy .

۲۷.Rittinghouse JW, Ransome JF;(,۲۰۰۹) . Security in the Cloud.CloudComputing. Implementation, Management, and Security, CRC Press .

۲۸. Bezemer C-P, Zaidman A ;(۲۰۱۰) . Multi-tenant SaaS applications:maintenance dream or nightmare? .Proceedings of the Joint ERCIMWorkshop on Software Evolution (EVOL) and International Workshop onPrinciples of Software Evolution (IWPSE), Antwerp, Belgium. ACM New York,NY, USA .

۲۹. ENISA ;(,۲۰۰۹).Cloud Computing: benefits, risks and recommendations forinformation Security.

۳۰. Viega J;(,۲۰۰۹) . Cloud Computing and the common Man.

۳۱. Winkler V;(,۲۰۱۱) . Securing the Cloud: Cloud computer Security techniquesand tactics. Elsevier Inc, Waltham, MA .

۳۲. Jansen WA;(۲۰۱۱). Cloud Hooks: Security and Privacy Issues in CloudComputing. In: Proceedings of the ۴۴th Hawaii International Conference onSystem Sciences, Koloa, Kauai, HI. IEEE Computer Society, Washington, DC,USA .

۳۳. Ranjith P, Chandran P, Kaleeswaran S;(,۲۰۱۲) .On covert channels betweenvirtual machines. Journal in Computer Virology Springer .

۳۴. Garfinkel T, Rosenblum M;(۲۰۰۵) .When virtual is harder than real: Securitychallenges in virtual machine based computing environments. In:Proceedings of the ۱۰th conference on Hot Topics in Operating Systems, SantaFe, NM. volume ۱۰. USENIX Association Berkeley, CA, USA

۳۵. Wang Z, Jiang X;(۲۰۱۰). HyperSafe: a lightweight approach to providelifetime hypervisor control-flow integrity. In: Proceedings of the IEEEsymposium on Security and privacy. IEEE Computer Society, Washington,DC, USA .

۳۶. Wu H, Ding Y, Winer C, Yao L;(,۲۰۱۰).Network Security for virtual machine inCloud Computing.۵th International conference on computer sciencesand convergence information technology (ICCIT). IEEE Computer Society .

۳۷. Somani U, Lakhani K, Mundra M (۲۰۱۰) Implementing digital signature withRSA encryption algorithm to enhance the data Security of Cloud in CloudComputing. ۱st International conference on parallel distributed and gridComputing (PDGC). IEEE Computer Society Washington, DC, USA .

۳۸. Tebaa M, El Hajji S, El Ghazi A;(,۲۰۱۲). Homomorphic encryption methodapplied to Cloud Computing. National Days of Network Security andSystems (JNS۲). IEEE Computer Society, Washington, DC, USA .

۳۹. Naehrig M, Lauter K, Vaikuntanathan V;(۲۰۱۱) . Can homomorphic encryptionbe practical? .Proceedings of the ۳rd ACM workshop on CloudComputing Security workshop. ACM New York, NY, USA .

۴۰. Harnik D, Pinkas B, Shulman-Peleg A;(,۲۰۱۰) .Side channels in Cloud services:deduplication in Cloud Storage. IEEE Security Privacy .

۴۱.Wei J, Zhang X, Ammons G, Bala V, Ning P ;(۲۰۰۹) .Managing Security ofvirtual machine images in a Cloud environment. Proceedings of the ۲۰۰۹ACM workshop .

۴۲. Zhang F, Huang Y, Wang H, Chen H, Zang B;(۲۰۰۸) . SecurityPreserving VM Live Migration for Systems with VMM-enforced Protection. Trusted Infrastructure Technologies Conference, ۲۰۰۸. APTC'۰۸, Third Asia-Pacific. IEEE Computer Society, Washington, DC, USA .

۴۳. Xiaopeng G, Sumei W, Xianqin C;(۲۰۱۰).a Network Security sandboxfor virtual Computing environment. IEEE youth conference oninformation Computing and telecommunications (YC-ICT). IEEE ComputerSociety, Washington DC, USA .