Arman Process Journal
(APJ)

Homepage: www.armanprocessjournal.ir

Toward Safe Virtualization Solutions in Cloud Computing Environments

***L. Akbari*[*,1]**

[1] *Department of Electrical Engineering, Raja University Of Qazvin, Qazvin, Iran*

ABSTRACT

Received: 2 March 2022

Accepted: 17 June 2022

KEYWORDS:

Cloud Computing,

Virtualization,

Security,

Infrastructure,

Protocol,

Cloud computing is a processing model that has attracted the attention of researchers due to its flexibility, rapid expansion and low cost, and it provides the shared use of services without the need for ownership and management of resources in the network environment. On the other hand, cloud computing is a pool of virtual computer resources. Resource virtualization in cloud computing allows heavy tasks to be performed faster and with less dependence on physical resources. Although cloud computing has become very popular among users, security problems are considered as a big obstacle for users to use cloud computing systems. Data security and virtualization security are two important security issues in cloud computing. In this article, we examine the dimensions of virtualization security in cloud computing environments.

[1] Corresponding author
akbari.elc@yahoo.com

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
15	0	0

فصلنامه تخصصی آرمان پردازش
(APJ)
Homepage: www.armanprocessjournal.ir

بسوی مجازی سازی ایمن در محیط های رایانش ابری

لاله اکبری[*،1]

[1] گروه مهندسی برق و کامپیوتر، موسسه آموزش عالی رجاء، قزوین، ایران

چکیده

رایانش ابری یک مدل پردازشی است که به‌دلایل قابلیت انعطاف‌پذیری، گسترش سریع و هزینه پایین، مورد توجه پژوهشگران قرارگرفته و استفاده اشتراکی سرویس‌ها را بدون نیاز به حق مالکیت و مدیریت منابع در محیط شبکه فراهم می‌نماید. از طرف دیگر محاسبات ابری استخری از منابع کامپیوتری مجازی می باشد. مجازی سازی منابع در محاسبات ابری اجازه می دهد تا وظایف سنگین با سرعت بیشتر و با وابستگی کمتری به منابع فیزیکی انجام شود. با اینکه محاسبات ابری بین کاربران محبوبیت زیادی یافت ولی مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم های محاسبات ابری قلمداد می شود. امنیت داده و امنیت مجازی سازی دو مسئله امنیتی مهم در محاسبات ابری می باشد. که ما در این مقاله به بررسی ابعاد امنیت مجازی سازی در محیط های رایانش ابری می پردازیم.

واژگان کلیدی:

پردازش ابری،

مجازی سازی،

امنیت،

زیر ساخت،

پروتکل،

تعداد جداول	تعداد شکل ها	تعداد مراجع
۰	۰	۱۵

مقدمه

اینترنت در کنار انقلاب‌های دیگراست، که در آن منابع در سطح جهان شبکه شده است و به‌راحتی می‌توان به اشتراک گذاشت. پردازش ابری جزء اصلی از این دیاگرام است، که یک مخزن بزرگ از اینترنت را ارائه می‌کند که در آن منابع برای هر کسی به عنوان سرویس در دسترس است. به‌طور خاص، گره‌های ابر به طور فزاینده‌ای محبوب هستند اگرچه امنیت و حریم خصوصی مسائل حل نشده موجب کم شدن سرعت پذیرش و موفقیت آن شده است. در واقع، صداقت، محرمانه بودن و نگرانی در دسترس بودن، هنوز هم از مشکلات باز است که نیاز به پاسخ و راه‌حل‌های کارآمد و موثر می‌باشد. گره ابر ذاتا به حملات اینترنتی نسبت به راه‌حل‌های سنتی، اندازه‌ی آنها و خدمات مربوط به پیچیدگی که به ارمغان می‌آورد، آسیب‌پذیرتر است. در واقع، ابر اینترنتی با تمام جوانب مثبت و منفی یک سیستم فراگیر است. در نتیجه، افزایش حفاظت گره‌های ابر یک کار چالش برانگیز است. بنابراین به رسمیت شناختن تهدیدات برای ایجاد فرآیندهای امنیتی برای محافظت از خدمات و سیستم‌عامل‌های میزبان حملات بسیار مهم است [۳-۱].

محاسبات ابری در حال حاضر از اهرم مجازی‌سازی برای بار تعادل از طریق تأمین پویا و مهاجرت ماشین مجازی در میان گره‌های فیزیکی استفاده می‌کند. ماشین‌های مجازی در اینترنت به انواع بسیاری از فعل و انفعالات که در معرض تکنولوژی مجازی‌سازی هستند می‌تواند کمک کند در حالی که فیلتر اطمینان درجه بالاتری از امنیت است. به‌طور خاص، مجازی‌سازی می‌تواند به عنوان یک جزء امنیتی استفاده شود. به عنوان مثال، ارائه‌ی نظارت بر ماشینهای مجازی، مدیریت آسان بر امنیت خوشه‌های پیچیده، مزارع سرور و زیرساخت محاسبات ابری [۶-۴]. با این‌حال، فن‌آوری‌های مجازی همچنین نگرانی‌های بالقوه‌ی جدیدی را با توجه به امنیت ارائه می‌کنند، همانطور که در بخش های بعدی مقاله خواهیم دید . توسعه محاسبات ابری جزء موارد امنیتی حل نشده است که ارائه‌دهنده و کاربران ابر را تحت تاثیر قرار می‌دهد. در این مقاله، نشان می‌دهیم که چگونه مجازی‌سازی می‌تواند با حفاظت از یکپارچگی ماشین‌های مجازی مهمان و اجزای زیرساخت ابری باعث افزایش امنیت محاسبات ابری شود. همچنین راهکارهائی توصیه می نمائیم که باعث تضمین افزایش امنیت در منابع ابر می‌شود.

هر چند که رایانش ابری در عصر حاضر یکی از کاربردی ترین تکنولوژهای ارائه شده توسط انسان می باشد، با این حال دغدغه امنیت بی شک قدم به قدم در کنار مزایای آن قابل طرح است . چیزی که بیش از پیش ذینفعان را در مورد استفاده از رایانش ابری دچار تردید می کند، امنیت این تکنولوژی می باشد . قبل از بحث امنیت در عرصه ابر به تعاریف پایه ای می پردازیم که ارتباط تنگاتنگی با امنیت دارند [۹-۷]:

امنیت اطلاعات : واژه امنیت اطلاعات حجم وسیعی از فعالیت های یک سازمان را تحت پوشش قرار می دهد . امنیت اطلاعات به معنای واقعی یعنی با استفاده از یک سری فرآیند ها از دسترسی غیر مجاز به اطلاعات و یا محصولات و اعمال تغییرات یا حذف کردن آنها جلوگیری کنیم .این عمل را می توان به نحوی حفاظت از منابع موجود، در موقعیت های مختلف توسط افرادی که مسئول امنیت اطلاعات هستند در نظر گرفت.

امنیت در مجازی سازی: تکنولوژی نرم افزاری است که به دسترسی به اجزای مختلف در محیط مجازی سازی را کنترل کرده و از دسترسی غیر مجاز و خرابکارانه جلوگیری میکند . امنیت محیط مجازی اشاره به ابزاری دارد که برای کنترل دستیابی به لایه های مختلف تکنولوژی مجازی لازم است.

در این بخش برخی از مدلهای جدید ارائه شده در مقوله امنیت داده رایانش ابری را ارائه میدهیم و آن ها را از دید طبقه بندی، رمزنگاری و کد تصدیق پیام بررسی میکنیم.

مدل امنیت داده ترکیبی

رویکرد ترکیبی جهت اطمینان از امنیت داده در رایانش ابری، یک راه برای محافظت داده و بررسی احراز هویت و جامعیت داده بوسیله سازوکارهای صنعتی ممکن را فراهم می سازد .این روش، تقسیم داده به چندین بخش، نمایسازی، رمزنگاری و کد تصدیق پیام و احراز هویت دومرحله ای یک کاربر توسط مالک داده و ابر را مطرح میکند. این مدل دسترس پذیری داده را توسط بسیاری از اعمال شبیه تشخیص دسترسی غیرمجاز از یک فراهم کننده سرویس ابر تأمین میکند . مدل پیشنهادی به دسترسی بالا، قابلیت اعتماد و جامعیت انتقال

داده از طریق مالک داده به ابر و از ابر به کاربر نایل می شود .علاوه بر این، انعطاف و توانایی بیشتری برای پاسخگویی به تقاضاهای روزمره پیچیده شبکه داشته و این قابلیت را به کاربر میدهد تا فایلهای مورد نظر را از ابر، به وسیله جستجو بر داده ها ی رمزشده بازیابی نماید.

مدل امنیت داده مبتنی بر سطح

مدل دیگر پیشنهادی به گونه ای طرح شده است که داده علاوه بر خود ابر، در حین انتقال نیز امنیت داشته باشد . مدل پیشنهادی از چهار بخش مالک داده، کاربر، ارائه دهنده سرویس ابر نامطمئن و شخص ثالث نامعتبر تشکیل شده است .داده در برابر نفوذگر شبکه، ارائه دهنده سرویس و کاربر غیرمجاز محافظت میشود. مؤلفه های مدل امنیت داده مبتنی بر سطح، به شرح ذیل هستند.

طبقه بندی : رمزنگاری داده، فن مورد استفاده در این مدل است . رمزنگاری داده با توجه به حساسیت و اهمیت داده انجام میشود . داده به دو نوع صفر و یک طبقه بندی میشود . داده نوع صفر، بیانگر غیرحساس بودن داده و داده نوع یک، بیانگر حساس بودن داده است . داده نوع یک، به خاطر حساس بودن لازم است قبل از بارگذاری در ابر رمزنگاری شود [۱۰].

رمزنگاری و رمزگشایی : در اینجا شخص ثالث نقش یک زیرساخت برای مدیریت کلید را ایفا میکند . مسئولیت شخص ثالث، مدیریت کلید و ذخیره سازی من است . ذخیره سازی کلید شامل تولید کلید، حفاظت و ذخیره کردن من است . مدیریت کلید نیز شامل ارائه کلید به کاربر مجاز است؛ یعنی بعد از تصدیق کلیدهایی که هویت کاربر را احراز میکنند . کلیدها با کد عبور، رمزنگاری میشوند . در این مدل فرض بر این است که شخص ثالث چیزی در رابطه با ارائه دهنده ب سرویس ابر نمیداند .

جامعیت داده : در راستای بررسی جامعیت داده، یعنی اینکه میان داده در مسیر انتقال روی شبکه دستکاری شده است یا خیر؛ کد تصدیق پیام محاسبه میشود . در این مدل بعد از عمل رمزنگاری، کد تصدیق پیام از روی داده رمزنگاری شده، محاسبه گردیده و حین بارگذاری در ابر، ضمیمه داده رمزنگاری شده میشود . زمانی که کاربر یا مالک داده به داده نیاز پیدا میکنند، متن را از ابر بارگیری کرده و بررسی میکنند . کاربر یا مالک، MAC جامعیت داده را با محاسبه ضمیمه شده تطبیق میدهد [۱۱].

احراز هویت : برای احراز هویت کاربر، ابتدا توسط شخص ثالث و سپس توسط مالک داده احراز هویت دومرحلهای انجام میشود . مالک داده فهرستی از کاربران مجاز را همراه با شناسه ورود و رمز عبور به شخص ثالث میدهد .شخص ثالث یک پایگاه داده برای اعتبارسنجی کاربر میسازد . زمانی که کاربر با شناسه کاربری و رمز عبور وارد پایگاه داده میشود، شخص ثالث کاربر را با بررسی پایگاه داده خود تصدیق میکند . اگر کاربر مجاز باشد، شخص ثالث کلید محرمانه را بدون کد عبور، صادرکرده و مالک داده را نیز باخبر میسازد . از این به بعد، احراز هویت توسط مالک داده انجام میشود . مالک داده کاربری را که از کارت هوشمند مورد تأیید استفاده میکند، تصدیق کرده و شناسه ورود به ابر، رمز عبور و کد عبور کلید محرمانه را در یک قالب رمزنگاریشده به کاربر ارائه میدهد . داده رمزنگاری شده با استفاده از کارت هوشمند رمزگشایی میشود .کاربر، شناسه کاربری را به ابر میفرستد تا ارائه دهنده سرویس ابر به کاربر، اجازه ورود به ابر و دسترسی به داده را بدهد . اکنون کاربر وارد ابر شده و به داده دسترسی پیدا میکند .یک روش دسترسی مبتنی بر نقش وجود دارد که کاربر میتواند با نقشی که مالک داده برای او تعریف میکند اعمال حذف، بهروزرسانی و خواندن را انجام دهد [۱۲].

مدل امنیت داده کسب وکار

یک مدل ارائه شده امن، سرویس ذخیره سازی داده را از سرویس رمزنگهاری و رمزگشایی جدا میکند سرویس ذخیره سازی توسط یک ارائه دهنده سرویس ابر و سرویس رمزنگاری و رمزگشایی توسط ارائه دهنده سرویس دیگر عرضه میشود . این جداسازی ضروری است؛ چراکه مدیران ارائه دهنده سرویس ابر ممکن است دسترسی غیرقانونی به داده کاربران داشته باشند .برای ممانعت از بروز چنین امری سرویسهایی مثل ذخیره سازی و رمزنگاری و رمزگشایی از یکدیگر جدا شده و به سرویس دهنده های ابر دیگر منتقل میشوند . در CRM قبل از هر چیز، گواهینامه های کاربران توسط سرویس ابر احراز هویت میشود . با هر دستورالعمل، کاربر ذخیره ساز

ابر ارتباط برقرار کرده و یک درخواست استفاده از داده ایجاد میکند .سپس سرویس ذخیره ساز ابر، درخواستی برای رمزگشایی داده به وسیله سرویس رمزنگاری و رمزگشایی میفرستد .سرویس رمزنگاری و رمزگشایی، داده رمزنگاری شده را گرفته و با رمزگشایی ، داده میفرستد [۱۳].

به سوی مجازی سازی ایمن در رایانش ابری

یکی از مسائل کلیدی مجازی سازی محاسبات ابری از دست دادن کنترل است .به عنوان یک مثال اول، کاربر خدمات (SU) نمی‌داند که اطلاعات آن در ابر دقیقا کجا ذخیره و پردازش می‌شود. محاسبات و داده‌های تلفن همراه است و می‌تواند به سیستم‌هایی مهاجرت کند که SU قادر به کنترل مستقیم آن نیست. بر روی اینترنت، عبور از مرزهای بین‌المللی برای داده‌ها رایگان است و این می‌تواند باعث افزایش تهدیدات امنیتی شود. نکته دوم از دست دادن کنترل این است که ارائه دهنده‌ی ابر (CP) می شود برای اجرای یک سرویسی که جزئیاتش را نمی‌داند هزینه پرداخت می‌کند. این، یک قسمت تاریک از مدل "زیرساخت به عنوان سرویس" از دیگر رویکردهای یک سرویس است. امنیت مجازی سازی رامی توان از دیدگاههای بنیادی زیر مورد بررسی قرار داد:

سیستم های امنیتی مبتنی بر مجازی سازی:

سیستم های امنیتی در یک ماشین معمولی به گونه ای هستند که یک نفوذگر پس از نفوذ به سیستم می تواند به سادگی سیستم های امنیتی را متوقف کرده،کنترل ماشین را به دست گیرد و حضور خود را در سیستم مخفی می کند . یکی از دلایل بروز این مشکل این است که سیستم امنیتی در همان ماشینی اجرا می شود که می خواهیم آن را نظارت کنیم [۱۴].

تشخیص نفوذ :

عبارت است از تحلیل بیدرنگ داده های شبکه به منظور تشخیص و ثبت و اخطار به هنگام بروز حملات و یا اقدامات مخرب امنیتی . سیستم یک دستگاه یا برنامه نرم افزاری است که بر فعالیت های شبکه یا سیستم برای فعالیت های مخرب و یا ناقص سیاست نظارت میکند جهت تولید گزارش برای ایستگاه مدیریت . ماشین مجازی سازگار با معماری سیستم تشخیص نفوذ به طور کلی شامل دو جزء میباشد : واحد مدیریت سیستم تشخیص نفوذ و سنسور سیستم تشخیص نفوذ.

معماری مدیریت یکپارچه سیستم تشخیص نفوذ ماشین مجازی:

این سیستم ها که با نام سیستمهای تشخیص و جلوگیری از نفوذ هم شناخته میشوند، ابزاری برای امنیت شبکه هستند که ممانعت از نفوذ فعالیتهای موجود در شبکه و یا سیستم را برای تشخیص و جلوگیری از فعالیتهای مخرب تحت نظر میگیرند . وظایف اصلی یک سیستم جلوگیری نفوذ شامل شناسایی فعالیتهای مخرب، ثبت اطلاعات در مورد این فعالیتها، اقدام به بلوکه و متوقف کردن این فعالیتها و ثبت گزارش کارهای انجام شده توسط خود سیستم میشوند. سیستمهای جلوگیری از نفوذ حالت ارتقاء یافته سیستمهای تشخیص نفوذ محسوب میشوند چرا که هر دو این سیستمها فعالیتهای شبکه و یا سیستم را برای یافتن فعالیتهای مخرب نظارت میکنند . تفاوت اصلی این سیستمها با سیستمهای تشخیص نفوذ در این است که این سیستمها میتوانند به صورت فعال مانع فعالیتهای مخرب شده و یا آنها را متوقف کنند .به طور دقیقتر میتوان گفت که یک سیستم جلوگیری نفوذ توانایی انجام کارهایی مانند ارسال هشدار، دور ریختن بستههای مخرب، بازنشاندن و یا بلوکه کردن ارتباط از طرف آدرسهای متخاصم را دارد [۱۵].

نظارت بر جامعیت فایل :

فایلهای سیستمی معمولا از اهداف حملات مخرب هستند، زیرا حاوی مقدار زیادی از داده های حساس، از جمله برنامه های اجرایی، پیکربندی و اطلاعات مجوز است .فایل های نظارت بر جامعیت یک روش موثر برای کشف رفتارهای تهاجمی با تشخیص اعمال تغییر بر روی فایل ها است.

درنهایت لازم به ذکر است بمنظور بهبود امنیت مجازی سازی در محیط های مبتنی بر رایانش ابری ابعاد کنترلی و مدیریتی زیر قابل توصیه می باشد:

–کنترل مدیریتی: عبارتند از سیاست ها، رویه ها، استانداردها و رهنمودها ی مکتوب که توسط مراجع مسئول تایید شده است

–کنترل منطقی: استفاده از نرم افزار، سخت افزار و داده ها برای نظارت و کنترل دسترسی به اطلاعات و سیستم های

کامپیوتری

–کنترل فیزیکی: حفاظت و کنترل محیط کار و تجهیزات کامپیوتری و نحوه دسترسی به آن ها است که جنبه فیزیکی دارند.

–کنترل رمزنگاری: اطلاعات به فرمی تبدیل شود که به غ یر از کاربر مجاز کس دیگری نتواند از آن اطلاعات استفاده کند حتی اگر به آن اطلاعات دسترسی داشته باشد.

در نهایت لازم به ذکر است، در دنیای امروز محاسبات ابری اهمیت بسیاری دارد و مورد توجه بسیاری از سازمان ها و افراد قرار گرفته است. محاسباتی ابری برای کاهش هزینه ها و در دسترس بودن اطلاعات معرفی شد و وارد بازار تکنولوژی گردید. از طرف دیگر محاسبات ابری استخری از منابع کامپیوتری مجازی می باشد. مجازی سازی منابع در محاسبات ابری اجازه می دهد تا وظایف سنگین با سرعت بیشتر و با وابستگی کمتری به منابع فیزیکی انجام شود. در واقع مجازی سازی به انتزاع منابع کامپیوتری اشاره می کند. با اینکه محاسبات ابری بین کاربران محبوبیت زیادی یافت ولی مشکلات امنیتی به عنوان یک مانع بزرگ در مقابل استفاده کاربران از سیستم های محاسبات ابری قلمداد می شود. امنیت داده و امنیت مجازی سازی دو مسئله امنیتی مهم در محاسبات ابری می باشد. که ما در این مقاله به بررسی امنیت مجازی سازی پرداختیم.

نتیجه گیری

مجازی سازی را میتوان به عنوان پایای برای ساخت یک ابر بکار برد ولی الزامی نیست و آن را می توان به عنوان یک لایه انتزاعی تعریف کرد، و مجازی سازی وجود داشته باشد . مجازی سازی هم یک فرصت است و هم یک تهدید، از آنجایی که ماشینهای مجازی در لایه IT میتواند در بخش هایی و یا در سراسر پشته زیرساخت محاسبات ابری قرار گرفته اند تضمین امنیت در این ماشین ها میتواند گام مؤثری در فراهم کردن اعتماد مشتریان باشد. رایانش ابری یک مدل پردازشی است که به‌دلایل قابلیت انعطاف‌پذیری، گسترش سریع و هزینه پایین، مورد توجه پژوهشگران قرارگرفته و استفاده اشتراکی سرویس‌ها را بدون نیاز به حق مالکیت و مدیریت منابع در محیط شبکه فراهم می‌نماید. با توجه به ذخیره و بازیابی داده‌های کاربران سرویس‌های ابر، امنیت داده یکی از چالش‌های عمده رایانش ابری محسوب می‌شود. برای مقابله با این چالش‌ها، مدل‌های مختلف امنیت داده در سطح ابر ارائه شده است که در این مقاله برخی از این مدل‌ها را بررسی کرده‌ایم. نتیجه بررسی ها نشان می‌دهد که مدل امنیت داده ترکیبی، بیشترین امنیت را زمانی داراست که داده‌ها علاوه‌بر رمزنگاری، طبقه‌بندی و نمایه‌گذاری نیز شوند . هم‌چنین مدل مبتنی بر سطح، با تقسیم داده به دو سطح و احراز هویت دومرحله‌ای راه حل کارائی درصدد امن‌کردن داده‌های سطح ابر است.

منابع و مآخذ

[1] Shackleford, D. (2012). Virtualization security: protecting virtualized environments. John Wiley & Sons.

[2] Manikandasaran, S. S., Balaji, K., & Raja, S. (2018). Infrastructure virtualization security architecture specification for private cloud. International Journal of Computer Sciences and Engineering, 6(02), 10-14.

[3] Tsai, H. Y., Siebenhaar, M., Miede, A., Huang, Y., & Steinmetz, R. (2011). Threat as a service?: Virtualization's impact on cloud security. IT professional, 14(1), 32-37.

[4] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[5] Mishra, A., Mathur, R., Jain, S., & Rathore, J. S. (2013). Cloud computing security. International Journal on Recent and Innovation Trends in Computing and Communication, 1(1), 36-39.

security risks and solutions of cloud computing via divide-conquer strategy. In 2011 Third International Conference on Multimedia Information Networking and Security (pp. 637-641). IEEE.

[14] AbdElRahem, O., Bahaa-Eldin, A. M., & Taha, A. (2016, December). Virtualization security: A survey. In 2016 11th International Conference on Computer Engineering & Systems (ICCES) (pp. 32-40). IEEE.

Luo, S., Lin, Z., Chen, X., Yang, Z., & Chen, J. (2011, December). Virtualization security for cloud computing service. In 2011 International Conference on Cloud and Service Computing (pp. 174-179). IEEE

[6] Ibrahim, A. S., Hamlyn-Harris, J., & Grundy, J. (2016). Emerging security challenges of cloud virtual infrastructure. arXiv preprint arXiv:1612.09059.

[7] Alwakeel, A. M., Alnaim, A. K., & Fernandez, E. B. (2018, April). A survey of network function virtualization security. In SoutheastCon 2018 (pp. 1-8). IEEE.

[8] Zhang, N., Liu, D., & Zhang, Y. (2013, November). A research on cloud computing security. In 2013 International Conference on Information Technology and Applications (pp. 370-373). IEEE.

[9] Pan, W., Zhang, Y., Yu, M., & Jing, J. (2012). Improving virtualization security by splitting hypervisor into smaller components. In Data and Applications Security and Privacy XXVI: 26th Annual IFIP WG 11.3 Conference, DBSec 2012, Paris, France, July 11-13, 2012. Proceedings 26 (pp. 298-313). Springer Berlin Heidelberg.

[10] Gurav, U., & Shaikh, R. (2010, February). Virtualization: a key feature of cloud computing. In Proceedings of the International Conference and Workshop on Emerging Trends in Technology (pp. 227-229).

[11] Kazim, M., Masood, R., Shibli, M. A., & Abbasi, A. G. (2013). Security aspects of virtualization in cloud computing. In Computer Information Systems and Industrial Management: 12th IFIP TC8 International Conference, CISIM 2013, Krakow, Poland, September 25-27, 2013. Proceedings (pp. 229-240). Springer Berlin Heidelberg.

[12] Chen, L., Xian, M., Liu, J., & Wang, H. (2020, April). Research on virtualization security in cloud computing. In IOP conference series: materials science and engineering (Vol. 806, No. 1, p. 012027). IOP Publishing.

[13] Luo, X., Yang, L., Ma, L., Chu, S., & Dai, H. (2011, November). Virtualization