تاثیرات مجازی سازی در امنیت اطلاعات

چکیده

مجازی‌سازی در صرفه‌جویی انرژی و منابع بسیار با اهمیت است و همچنین مدیریت اطلاعات مورد نیاز را به سادگی فراهم می‌کند. بااین‌حال، مسائل امنیت اطلاعات به یک نگرانی جدی تبدیل شده‌اند. پژوهش حاضر به بررسی کسب‌وکار پس از مجازی‌سازی از لحاظ امنیت سیستم می‌پردازد. یک پرسشنامه بر اساس 133 استاندارد اصول مدیریت کنترل ISO / IEC 27001 توسعه داده شده است و یک تکنیک نمونه برای جمع آوری پاسخ از افراد حرفه‌ای در زمینه IT با درک درستی از محیط مجازی‌سازی اطلاعات به کار گرفته شده است. نتایج به دست آمده نشان می‌دهد که مجازی‌سازی ممکن است در بخش‌های صنعتی برای در دست گرفتن مسائل مربوط به امنیت اطلاعات مفید واقع شود.

کلیدواژه‌ها: مجازی‌سازی، امنیت اطلاعات، ISO 27001، مدیریت امنیت اطلاعات، فناوری اطلاعات

1. معرفی

محاسبات ابری یکی از موضوعات مهم در حوزه IT در قرن 21 ام است. پس از سال‌ها بحث دقیق، محاسبات ابری به‌تدریج از معرفی به توسعه نرم‌افزار تکامل یافته است و در نتیجه به یکی از زمینه‌های امیدوارکننده در شرکت‌ها تبدیل شده است و صنعت فناوری اطلاعات شروع به سرمایه‌گذاری گسترده کرده است. ویژگی‌های فن‌آوری محاسبات ابری ممکن است شامل گسترشی بزرگ مقیاس، مقیاس‌پذیر پویا و مبتنی بر تقاضا باشد که در آن مجازی‌سازی نقش مهمی ایفا می‌کند. علاوه بر این، شرکت در جهت اهمیت مجازی‌سازی و سرمایه‌گذاری سنگین در اجرای آن شروع به

کار می کند [37]. با توجه به بررسی اخیر ESG 2011 IT، بیش از 60 درصد از سازمان‌های مورد بررسی هزینه‌های خود را در نرم‌افزار مجازی‌سازی در سال 2011 افزایش خواهند داد [15].

ظاهرا، صنعت فناوری اطلاعات در حال حاضر شروع به پذیرفتن مجازی‌سازی است. سوال - "چگونه کسب و کار می‌تواند از مجازی‌سازی بهره گیرد؟ "هنوز هم یکی از سوالات مهم برای پاسخ دادن است. در میان مزایای بالقوه آن، مجازی‌سازی در جهت متمرکز و یکپارچه‌سازی منابع IT کمک می‌کند. ذخیره‌سازی متمرکز داده‌ها موجب پشتیبان‌گیری آسان اطلاعات، مانع از افزونگی و بهبود کنترل می‌شود. همچنین موجب تسهیل انطباق با مقررات و مدیریت IT می‌شود. در مرحله دوم، مجازی‌سازی در جهت کاهش تعداد سرویس‌دهنده‌ها قدم برمی‌دارد و انجام این کار، منجر به کاهش استفاده از امکانات برق و خنک‌کننده می‌شود. کاهش تعداد سرورها و استفاده از برق نه تنها می‌تواند فشار بهره وری مدیریت فناوری اطلاعات را از بین ببرد، بلکه به روند فراگیر استفاده از انرژی سبز جهانی کمک می‌کند. با این منافع ذکر شده، بسیاری از مسائل وجود دارد که باید به آن پرداخته شود و اجرای یا تصویب مجازی‌سازی در مورد آن انجام گیرد. بدین معنی که، یکی از مهم‌ترین مسائل ممکن است نگرانی‌های امنیتی در مورد ماشین‌های مجازی و محیط‌های مجازی باشد. تحقیقات اخیر و مطالعات هر دو جنبه‌ی به چالش کشیده شده و مفید از مجازی‌سازی اطلاعات از لحاظ امنیتی را نشان می‌دهند [11،22،54،69]. علاوه‌براین، بسیار پیشنهاد شده است که اقدامات امنیتی باید اجرا شوند و به عنوان کسب‌وکاری در جهت مجازی‌سازی ایفای نقش کنند [42،66]. پیاده‌سازی اقدامات امنیتی،حال، برای پشتیبانی، ممیزی و نظارت نیاز به مقررات خاص دارد. استاندارد ISO / IEC 27001 [26] در حال حاضر یکی از محبوب‌ترین استانداردهای امنیت اطلاعات پذیرفته شده است در نتیجه به عنوان یک راهنما برای اجرا و ارزیابی اقدامات امنیت اطلاعات مختلف از سیستم‌های مجازی بسیار مناسب است.

این مطالعه بر روی تاثیرات محیط اطلاعات مجازی‌سازی شده در امنیت اطلاعات متمرکز است. کسب‌وکار ممکن است به علت سوء مدیریت در معرض تهدید و مشکلاتی باشد و اقدامات امنیتی به خطر بیافتد. برای درک کامل تاثیر مجازی‌سازی در امنیت اطلاعات، پرسشنامه‌ای براساس استاندارد ISO / IEC 27001 برای جمع‌آوری پاسخ از افراد حرفه‌ای و با تجربه IT در زمینه مجازی‌سازی یا یا صنعت خدمات IT طراحی شده است. ترکیبی از استاندارد ISO /

IEC27001 و پرسشنامه مبتنی بر دیدگاه‌های جمع‌آوری شده یک مسیر جدید برای آدرس‌دهی و بررسی مسائل مربوط به مجازی‌سازی و امنیت اطلاعات را فراهم می‌کند. نتایج بررسی پرسشنامه برای بعد از مجازی‌سازی و از چشم‌انداز امنیت کسب‌وکار و جنبه‌های امنیت سیستم در نظر گرفته شده است. به‌طورخلاصه، این مطالعه به سوالات پژوهش زیر پاسخ خواهد داد.

(1) از نظر امنیت فیزیکی و محیطی، کند اجرای مجازی‌سازی به طور قابل توجهی در امنیت اطلاعات تاثیر می‌گذارد؟

(2) از نظر ارتباطات و مدیریت عملیات، اجرای مجازی‌سازی به طور قابل توجهی در امنیت اطلاعات تاثیر می‌گذارد؟

(3) از نظر کنترل دسترسی، آیا اجرای مجازی‌سازی به طور قابل توجهی امنیت اطلاعات را تحت تاثیر قرار می‌دهد؟

(4) از نظر سیستم اطلاعات ، توسعه و نگهداری، آیا مجازی‌سازی به طور قابل توجهی امنیت اطلاعات را تحت تاثیر قرار می‌دهد؟

این مطالعه شامل شش بخش است. بخش 1 پیش‌زمینه و اهداف این مطالعه را بیان می‌کند. بخش بعدی به بررسی کارهای گذشته مرتبط با امنیت اطلاعات و مجازی‌سازی می‌پردازد. بخش 3 به توصیف روش تحقیق از جمله نمونه برداری و طرح پرسشنامه می‌پردازد. بخش 4 و 5 تجزیه و تحلیل آماری از بررسی نتایج و بحث براساس سوالات پژوهش را ارائه می‌دهد. در نهایت، آخرین بخش خلاصه یافته‌ها، مشارکت این مطالعه و برخی از جهات تحقیقات آینده را بحث می‌کند.

2. کارهای گذشته

این مطالعه به بررسی تاثیر مجازی‌سازی در امنیت اطلاعات می‌پردازد. این بخش عمدتا از دو بخش فرعی تشکیل شده که شامل امنیت اطلاعات و مجازی‌سازی است. اولی وضعیت فعلی تحقیقات امنیت اطلاعات و استاندارد ISO / IEC 27001 را معرفی می‌کند درحالی‌که دومی به بررسی این مطالعات در مورد مجازی‌سازی و تکنولوژی‌های مربوط می‌پردازد.

2.1. سیستم مدیریت امنیت اطلاعات (ISMS)

مسائل مربوط به امنیت اطلاعات در سال‌های اخیر در حال افزایش است و این واقعیت منجر به توسعه پژوهش‌های مرتبط با جنبه‌های مختلف امنیت اطلاعات شده است. جدول 1 تحقیقات مربوط به امنیت اطلاعات را که بنا به اطلاعات مختلف مسائل امنیتی دسته بندی شده‌اند نشان می‌دهد. برخی از مطالعات نیز به مجازی‌سازی مربوط می‌شود. زیرا ارتباط این دو موضوع، ابزار ارزیابی مناسبی برای ارزیابی مجازی‌سازی تحت تاثیر امنیت اطلاعات است. استاندارد ISO / IEC 27001 یکی از گسترده‌ترین استانداردهای حسابرسی پذیرفته شده برای ارزیابی امنیت اطلاعات است، بنابراین جهت استفاده و اقتباس این مطالعه به‌منظور بررسی اثرات مجازی‌سازی در امنیت اطلاعات مناسب است.

مجموعه استاندارد ISO / IEC 27000 از استانداردهای بین المللی منتشر شده توسط سازمان استاندارد (ISO) و کمیسیون بین‌المللی الکترونیکی (IEC)، استانداردهای اختصاص داده شده به امنیت اطلاعات می‌باشند. به‌طور خاص، استاندارد ISO / IEC 27001 (تکنولوژی اطلاعات - تکنیک‌های امنیت - سیستم‌های مدیریت امنیت اطلاعات – نیازمندی‌ها) تعریف مهم و مورد نیاز برای سیستم مدیریت امنیت اطلاعات را فراهم می‌کند (ISMS) [77]. در اصل تکامل یافته استاندارد BS 7799 از موسسه استاندارد بریتانیا (BSI)، نسخه فعلی استاندارد ISO / IEC 27001 از ISO / IEC27001:2005 است [4].

جدول 1 بررسی مشکل امنیتی اطلاعات.

مسائل امنیت اطلاعات	موضوع	کارهای گذشته
کسب‌وکار امنیت شبکه	ابزارهای امنیت شبکه، نرم‌افزار و محصولات: برای افزایش امنیت اینترنت و اینترانت، ابزارهای امنیتی، محصولات و/یا نرم‌افزارهایی که ممکن است استفاده شوند، اعتماد کاربر و امنیت در درک محیط آنلاین شبکه خصوصی مجازی (VPN): منابع آنلاین را می‌توان از راه دور از طریق VPN دید.	[8،49،53،61] [25،59،60] [10،75]
کسب‌وکار حفاظت از داده‌ها	هارددیسک و رمزگذاری در سطح فایل: با استفاده از ابزار رمزگذاری و/ یا نرم‌افزار برای به رمزدرآوردن دیسک و یا فایل ممکن است داده‌ها را از دسترسی‌های غیرمجاز نگه دارد.	[6،39]

	ممانعت از فاش اطلاعات: ساخت یک سیستم نظارت بر فاش شدن اطلاعات ممکن است استراق سمع خصمانه را کشف و/ یا جلوگیری کند. کنترل امنیت پایگاه داده: رمزگذاری داده‌ها و ممیزی دسترسی به پایگاه داده ممکن است احتمال نقض امنیتی را کاهش دهد.	[5،70] [14،62]
شناسایی پرسنل شرکت و کنترل دسترسی	مدیریت شناسایی پرسنل: ایجاد یک سیاست مدیریت شناسایی و رمز عبور پیشنهاد می‌شود. سرویس احراز هویت کاربر: روش‌هایی مانند sign on یک بار یا کارت‌های هوشمند احراز هویت ممکن است اجرا شود. وب‌سایت احراز هویت کاربر: این سیستم تنها اجازه می‌دهد تا کاربران مجاز به محتویات دسترسی داشته باشند و از sign on یک بار برای جلوگیری از تهدیدات هک استفاده می‌کند.	[46،67] [2،38] [9،55]
ممیزی امنیت، اجرا و استانداردها	ISO 27،001: شامل استانداردهای حسابرسی دستورالعمل‌ها و پیاده‌سازی. COBIT: به فرآیندهای IT تمرکز دارد.	[3،19] [12،56]
امنیت برنامه‌های کاربردی و پلتفرم	O.S. امنیت: یک O.S. امن منطقی برای امنیت رایانه‌های شخصی و سرورها بسیار حیاتی است. مدیریت ریسک: مدیریت و سؤال از نقاط ضعف ضروری است. امنیت ابر؛ امنیت مجازی‌سازی نگرانی‌های امنیتی و ارزیابی در مورد مجازی‌سازی.	[72،73] [48،52] [11،16،54،58] [22،41،69]
تهدید امنیت اطلاعات	بدافزار شامل ویروس‌ها، اسب‌های تروجان، کرم‌ها، نرم‌افزارهای جاسوسی، کامپیوتر، روت کیت‌ها و ابزارهای تبلیغاتی مزاحم. ابزار و ترفندهای هک: هکرها همیشه در حال توسعه ابزارهای جدید، مسیرها و فن‌آوری جدید حمله هستند. حملات در سطح کاربرد: بسیاری از هکرها در حال حاضر از حملات سطح O.S. به سرریز بافر و حملات برنامه نویسی سمت سایت بهره می‌برند.	[13،35،40] [33،51] [50،71]

استاندارد ISO / IEC 27001 از چرخه PDCA (طرح، انجام کار، بررسی و عمل) پیروی می‌کند و شامل 11 زمینه کنترل است. این زمینه‌ها عبارتند از (1) سیاست امنیتی، (2) سازمان امنیت اطلاعات، (3) مدیریت دارایی، (4) امنیت منابع انسانی، (5) امنیت فیزیکی و محیطی، (6) ارتباطات و مدیریت عملیات، (7) کنترل دسترسی، کسب سیستم‌های

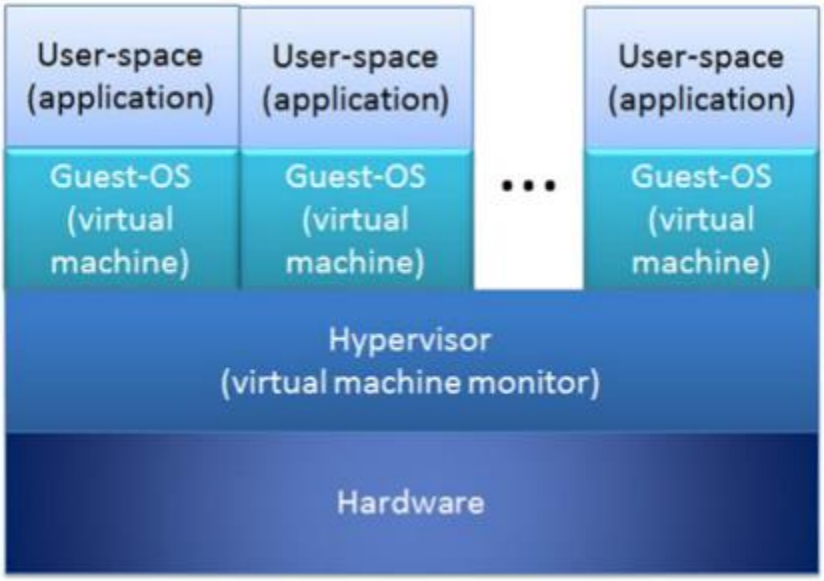
اطلاعات، (8) توسعه و تعمیر و نگهداری، (9) مدیریت حادثه امنیت اطلاعات، (10) مدیریت تداوم کسب‌وکار و (11) پیروی [4،77]. این استاندارد ارزیابی و حسابرسی پایه برای ایجاد، پیاده‌سازی و نگهداری ISMS است. تعدادی از مراجع صدور گواهینامه در سراسر جهان توسط ادارات استاندارد ملی برای انطباق ممیزی با ISO / IEC 27001 و گواهی موضوع به سازمان‌های شرکت‌کننده به رسمیت شناخته شده‌اند.

2.2. فن‌آوری‌های مجازی‌سازی

مفهوم مجازی‌سازی در سال 1960 زمانی که هزینه رایانه‌های بزرگ بسیار گران قیمت بود سرچشمه گرفته است. آی بی ام یک پردازنده مرکزی بزرگ یونیکس را به چند واحد منطقی تقسیم کرده است که کاربران را قادر به استفاده کامل از یک منبع محاسباتی پردازنده مرکزی می‌کند [63]. هر واحد منطقی در اصل یک ماشین مجازی (VM) و یا یک سیستم عامل مهمان (OS) است. همان طورکه سیستم عامل و یا سخت‌افزار کامپیوترهای پردازنده مرکزی ممکن است سازگاری مختلفی با ماشین‌های مجازی داشته باشند، یک مانیتور ماشین مجازی، به نام هایپروایزر، ممکن است به عنوان رابط بین ماشین‌های مجازی و سخت‌افزار فیزیکی مورد نیاز باشد[29]. همانطور که در شکل 1 نشان داده شده است، هر ماشین مجازی دارای منابع مجازی از جمله پورت I / O و کانال DMA است و این ماشین‌های مجازی قادر به اجرا در هر سیستم‌عاملی از طریق هایپروایزر هستند، همان‌گونه که سخت‌افزار توسط سیستم‌عامل [29] پشتیبانی می‌شود. به عبارت دیگر، هایپروایزر کلید است. به‌عنوان مثالی در راه حل VMware، هایپروایزر VMware، به‌نام لایه مجازی‌سازی VMware، قادر به میزبانی چندین ماشین مجازی با یک پردازنده به اشتراک گذاشته، حافظه، درایور شبکه و فضای هارد دیسک است. از سوی دیگر، هایپروایزر به ناچار باید در مورد آسیب‌پذیری امنیتی اطلاعاتی داشته باشد و حساس به حملات هکر باشد، بنابراین نیاز به یک سطح بالاتری از مدیریت امنیت اطلاعات دارد [21]. فن‌آوری‌های مجازی‌سازی در سال‌های اخیر به‌طور فزاینده‌ای افزایش یافته‌اند و تحقیقات در این زمینه در حال ظهور هستند. جدول 2 چند موضوعات تحقیقاتی مرتبط را ارائه می‌کند. به‌طورخاص، از نظر امنیت اطلاعات، مطالعه وان نیکولز [69] اشاره به مجازی‌سازی جهت ایجاد چالش‌های خاصی برای سازمان‌ها کرده است و پیشنهاد کرده است که

سازمان باید در سیستم‌های مجازی‌سازی خود را برای مسائل امنیتی مختلف دقیق‌تر نگاه کند. Hoesing [22] در بررسی خود از ارزیابی امنیتی تکنیک‌های مجازی‌سازی بیشتر استدلال کرده است که خطرات امنیتی مجازی‌سازی از یک محیط سرور فیزیکی نشات می‌گیرد، که با مجازی‌سازی با توجه به سرعت و سهولت استقرار منابع محاسباتی و ابزار مجازی‌سازی منحصربه‌فرد تقویت می‌شود. هوانگ و همکارانش [24] اثرات امنیتی شناخته شده مجازی‌سازی بر روی یک بستر شبکه را بررسی کردند و پیشنهاد کردند که تنظیمات صحیح، بهینه‌سازی مناسب و مدیریت اتصال باید در جهت به حداقل رساندن اثرات امنیتی اجرا شود. Zissis و Lekkas [76] عمده مسائل امنیتی مجازی‌سازی در محاسبات ابری را مورد ارزیابی قرار دادند و یک بخش سومی به‌عنوان راه‌حلی برای ارائه سرویس‌های امنیتی پایان به پایان با ایجاد سطح اعتماد لازم در سراسر شبکه پیشنهاد دادند.

از سوی دیگر، مجازی‌سازی نیز طرح‌های جدیدی از امنیت اطلاعات را به ارمغان می‌آورد. به‌عنوان مثال، Christodorescu و همکارانش [11] یک سیستم نظارت امنیتی ابر با طراحی جای دادن نظارت سیستم روی یک ماشین مجازی و نظارت بر سیستم ابر از خارج و از طریق مجازی ماشین درون نگری ارئه دادند.



شکل 1: بررسی اجمالی از محیط‌های مجازی [29].

جدول 2: بررسی کارهای گذشته در مجازی‌سازی

مسائل مجازی‌سازی سرور	موضوع	کارهای گذشته
ابزار مدیریتی مجازی‌سازی سرور	تنظیم ماشین مجازی: راه‌اندازی بسیار کارآمد و ماشین مجازی پاسخگو برای مدیران سیستم می‌تواند بسیار دشوار باشد.	[28،31]
نظارت بر امنیت و سیاست مجازی‌سازی سرور	نگرانی در مورد امنیت مجازی‌سازی. امنیت ابر از طریق مجازی‌سازی. نظارت بر خطر سرور مجازی : سیستم‌های مجازی خطرات امنیتی خود را دارند. O.S، ابزار مجازی‌سازی و شبکه همه سهمی در خطرات دارند. طراحی امنیت برای سیستم‌های مجازی، دستورالعمل مجازی‌سازی سرور: در برنامه مدیریتیIT ، سرورهای مجازی باید سیاست‌ها و قوانین را دنبال کنند.	[11،17،22،24،30،54،57،69،76]
زیرساخت‌ها و چارچوب مجازی‌سازی سرور	سرور و مجازی‌سازی: اگر مجازی‌سازی برای تحکیم استفاده از سرور مورد استفاده قرار گیرد، برخی از مشکلات زیرساخت باید نشان داده شود. مسائل مجازی‌سازی شبکه: حتی اگر نرم‌افزار مجازی‌سازی و سخت‌افزار سرور بالا استفاده شود، تنگناهای شبکه و/ یا سایر اشکالات فنی ممکن است کارآیی سیستم را پایین بیاورند.	[10،44،68،74]
پشتیبان‌گیری و فاجعه بازیابی برنامه‌ها برای سیستم‌های مجازی‌سازی شده	پشتیبان‌گیری و فاجعه بازیابی: سرور مجازی‌سازی شده نیاز به برنامه‌ریزی برنامه‌های پشتیبان‌گیری و بازیابی دارد.	[32،45]
مجازی‌سازی سرور برنامه‌ها و موارد استفاده	محاسبات ابری: معماری محاسبات ابری نیاز به ظرفیت سرور زیاد و قدرت محاسبات اولیه دارد.	[23،64،65]
مزایای مجازی‌سازی سرور	تثبیت سرور: مجازی‌سازی می‌تواند منجر به کاهش هزینه‌های سرور گردد.	[7،43]

چنین نظارت درون‌نگری اجازه می‌دهد تا ارزیاب، نظارت بر VM مهمان را در هر زمان از چرخه زندگی خود بدون دانستن سیستم عامل مهمان در پیشبرد و ارزیابی کد منبع سیستم‌عامل انجام دهد، که برای هر دو سیستم‌عامل ویندوز و لینوکس مناسب است [11]. لی و همکارانش [36] CyberGuarder را پیشنهاد دادند، که یک معماری تضمین امنیت مبتنی بر مجازی‌سازی برای محاسبات ابری سبز بود. CyberGuarder برای اجرا برروی سیستم‌عامل نرم‌افزار شبکه برای ارائه سه سرویس طراحی شده است: سرویس امنیت ماشین‌های مجازی، سرویس امنیت شبکه

مجازی و یک مدیریت اعتماد مبتنی بر سیاست سرویس، و آزمون مقدماتی از CyberGuarder نتایج امیدوارکننده‌ای نشان داد [36].

3. روش تحقیق

پژوهش حاضر تاثیرات مجازی‌سازی در امنیت اطلاعات را مطالعه می‌کند. در بخش آتی، طرح پژوهش، پرسشنامه طراحی شده، افراد تحقیق و نمونه‌گیری و روش تجزیه و تحلیل بیان شده‌اند. به‌طورخاص، در طراحی پرسشنامه از تجزیه و تحلیل نسبت اعتبار محتوا (CVR) برای استخراج موارد مهم پرسشنامه از ISO / IEC 27001 استفاده شده است [34]. در این مطالعه، موارد توسط هیئتی از کارشناسان موضوع (SAES) بررسی شده‌اند.

3.1. طرح پژوهش

چارچوب تحقیق تحت کنترل ISO / IEC 27001 توسعه یافته است. شکل2 چارچوب تحقیق در این مطالعه را نشان می‌دهد. از طریق بررسی یک expertpanel با استفاده از تجزیه و تحلیل CVR، موارد پرسشنامه استخراج و متغیرهای وابسته یا مستقل شناخته شده‌اند.

3.2. موارد پژوهش و نمونه‌برداری

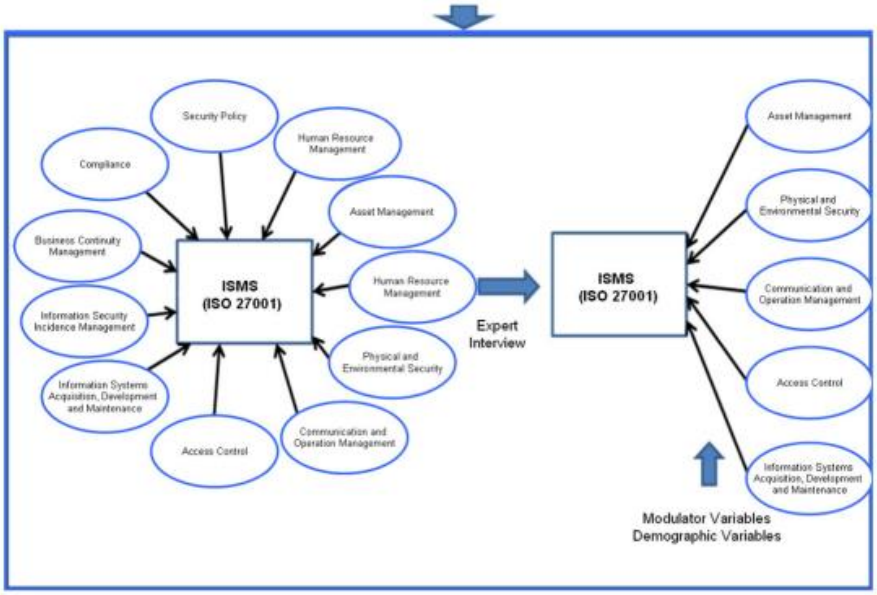
این مطالعه مستلزم مواردی دارای سطح خاصی از درک در مورد محیط مجازی‌سازی اطلاعات است. موارد تحقیق، روش نمونه‌گیری و نمونه گردش کار با جزئیات در بخش زیر شرح داده شده است.

3.2.1. موارد پژوهش

با چنین موضوع تحقیقی در مورد تکنولوژی خاصی، افراد این تحقیقات به متخصصان فناوری اطلاعات با درک درستی از محیط مجازی‌سازی اطلاعات محدود می‌شوند. بنابراین، این مطالعه جمعیت مورد تحقیق خود را از میان افراد صنعت IT و فناوری اطلاعات که در کار حرفه‌ای هستند انتخاب می‌کند.

3.2.2. نمونه برداری

نمونه‌برداری هدفمند، که پاسخ‌دهندگان به نظرسنجی از میان افراد حرفه‌ای انتخاب می‌شوند، برای ارائه یک بحث عمق در مورد مسائل مربوط به تمرکز پژوهشی به کار گرفته شده توسط این مطالعه برای استخراج اطلاعات در مورد تاثیر مجازی‌سازی در امنیت اطلاعات است. هر دو پرسشنامه کاغذی و مبتنی بر وب بین افراد انتخاب شده توزیع می‌شود. سوالات در ابتدای پرسشنامه برای فیلتر کردن کسانی است که دانش کافی از مجازی‌سازی دارند. توزیع و جمع‌آوری پرسشنامه‌ها در یک زمان خاصی در حدود 6 هفته پایان می‌یابد. در مجموع 133 پرسشنامه مبتنی بر وب معتبر از میان 400 ایمیل دعوت‌نامه جمع آوری می‌شود. علاوه براین، 17 پرسشنامه معتبر مبتنی بر کاغذ از 20 پرسشنامه توزیع‌شده جمع‌آوری می‌شود. در نتیجه، تعداد کل پرسشنامه‌های معتبر 150 است.



شکل 2: چارچوب تحقیق

3.3. طراحی ابزار اندازه‌گیری برای این پژوهش

3.3.1. طراحی پرسشنامه

این پژوهش در نظر دارد تاثیرات امنیت اطلاعات توسط مجازی‌سازی را مورد مطالعه قرار دهد. استاندارد ISO / IEC 27001 به‌عنوان چارچوبی برای سیستم‌های مدیریت امنیت اطلاعات به‌کار میشود. همانطور که پیش از این بحث شد، این تحقیق یک ارزیابی و حسابرسی ابزار پذیرفته شده برای امنیت سیستم‌های اطلاعاتی است. لذا این مطالعه، پرسشنامه‌ی پژوهش را براساس 133 کنترل استاندارد ISO / IEC 27001 توسعه می‌دهد. برای انتخاب موارد پرسشنامه از 133 کنترل، این مطالعه، تجزیه و تحلیل نسبت اعتبار محتوای (CVR) پیشنهاد شده توسط Lawshe [1،20،27،34] را برای بررسی اهمیت هر کنترل برای اهداف پژوهش به کار برده است.

یک گروه متشکل از 13 فرد متخصص برای انجام تجزیه و تحلیل CVR تشکیل شد. کارشناسان از متخصصان ارشد IT با حداقل 10 سال تجربه انتخاب شدند. هر کنترل ISO / IEC 27001 مورد بررسی قرار گرفت و به صورت "مورد نیاز" و یا "لازم نیست" مشخص شد. مقدار CVR این چنین محاسبه شد:

$$\mathrm{CVR} = \frac{\mathrm{n} - \frac{\mathrm{N}}{2}}{\frac{\mathrm{N}}{2}},$$

که در آن n تعداد کل کارشناسان در پاسخ به سوال "مورد نیاز" و یا دارای رای مثبت درکنترل ISO / IEC 27001 و N تعداد کارشناسان است. بنا به پیشنهاد Lawshe [34]، این مطالعه کمترین مقدار CVR قابل قبول را 0.54 در نظر گرفته است. برای این مطالعه، کنترل ISO / IEC 27001 ، مقدار CVR را بیش از 0.54 در نظر گرفته است که مربوط به موضوع تحقیق است و در نتیجه به یکی از موارد پرسشنامه تبدیل شده است. 32 کنترل ISO / IEC 27001واجد شرایط وجود دارد که می‌توانند به 5 بُعد طبقه‌بندی شوند: "مدیریت دارایی"، " امنیت فیزیکی و محیطی،" "مدیریت ارتباط و عملیات"،" کنترل دسترسی"و" اکتساب سیستم اطلاعات، توسعه و تعمیر و نگهداری". این پژوهش برای ارضای قابلیت اطمینان ابعاد، همسانی درونی موارد پرسشنامه را پس از چک کردن مقادیر کرونباخ

با یک مقدار عددی بزرگتر از 0.7 بررسی کرده است. این مطالعه 32 کنترل موجود را برای ایجاد پرسشنامه نهایی پژوهش به کار برده است (همانطور که در جدول 3 ذکر شده است).

3.3.2. محتویات پرسشنامه

پرسشنامه شامل سه بخش است (1) شخصی اطلاعات - از جمله جنس پاسخ‌دهنده، سن، پس زمینه آموزشی، عنوان شغلی، و زمان اشتغال در یک حوزه مربوط به IT؛ (2) اطلاعات شرکت - از جمله بخش صنعت، نوع کسب و کار کارمندان، مقیاس شرکت و تعدادی از فناوری‌های مربوط به شرکت مخاطب و (3) "بررسی امنیت اطلاعات سیستم اطلاعات مجازی‌سازی شده"- حاوی سوالات اقتباسی از 32 مورد واجد شرایط در کنترل ISO / IEC 27001 در مورد محیط اطلاعات مجازی‌سازی شده و امنیت اطلاعات. این مطالعه از یک مقیاس لیکرت 7 نقطه با ارزش از 1 تا 7 برای نشان دادن"بسیار مضر"، "مضر"، "کمی مضر"، "بی‌ربط"، "کمی مفید"، "مفید" و "بسیار مفید"، به‌منظور ارزیابی نظر مخاطب در مورد تاثیر مجازی‌سازی در هر یک از آیتم‌های پرسشنامه استفاده می‌کند. هر یک از آیتم‌های پرسشنامه نشان‌دهنده یکی از 32 کنترل ISO / IEC 27001 است، نمره بالا به معنی این است که مخاطب معتقد است اجرای مجازی‌سازی محیط اطلاعاتی در امنیت اطلاعات مفید است، درحالی که یک نمره کم نشان‌دهنده‌ی این است که مخاطب بر این باور است که اجرای محیط اطلاعات مجازی‌سازی ممکن است به نتیجه‌ی امنیت اطلاعات آسیب برساند.

3.3.3. آزمون قابلیت اطمینان برای پرسشنامه

پس از جمع‌آوری پرسشنامه، این مطالعه تبدیل به داده‌های معتبر به فرمت سازگار با نرم افزار SPSS (نرم‌افزار آماری برای علوم اجتماعی) می‌گردد و پس از آن تجزیه و تحلیل قابلیت اطمینان با استفاده از نرم افزار SPSS V18 برای ویندوز انجام می‌گیرد. ضریب آلفای کرونباخ برای بررسی همسانی درونی موارد پرسشنامه تحت طبقه‌بندی و یا ابعاد یکسانی استفاده می‌شود. برای پژوهش اکتشافی، موارد پرسشنامه تنها در صورتی که آلفا برابر یا بزرگتر از 0.7

[18،47] در نظر گرفته شود قابل اعتماد است. بُعد " مدیریت دارایی" تنها شامل یک مورد از پرسشنامه است، که برای تست قابلیت اطمینان مناسب نیست و در نتیجه در پرسشنامه گنجانده نشده است. ضریب آلفای کرونباخ برای مواردی در 4 بُعد دیگر (" امنیت فیزیکی و محیطی"، " مدیریت ارتباطات و عملیات"،" کنترل دسترسی"،" اکتساب سیستم اطلاعات، توسعه و نگهداری") بزرگتر از 0.7 در نظر گرفته شده است (جدول 3 را ببینید)، در نتیجه موارد پرسشنامه در این مطالعه قابل اعتماد در نظر گرفته شده‌اند.

4. تجزیه‌وتحلیل داده‌ها

همه داده‌های جمع‌آوری شده بااستفاده از نرم‌افزار V18 SPSS مورد تجزیه و تحلیل قرار گرفته‌اند. تجزیه و تحلیل آماری به کار گرفته شده شامل تست قابلیت اطمینان، آزمون T-test، ANOVA، مقایسه چندگانه Scheffe و تجزیه و تحلیل رگرسیون لجستیک است.

با مراجعه به جدول 4، توزیع‌های عمده از اطلاعات دموگرافیک ممکن است شامل اطلاعات زیر باشد. به‌طور خاص، (1) بیشتر شرکت‌کنندگان در این پرسشنامه مرد هستند (82.7٪). (2) سنین شرکت‌کنندگان عمدتا در محدوده 31 تا 40 است (71.3٪). (3) بسیاری از شرکت‌کنندگان مدرک دانشگاهی یا بالاتر دارند (72.7٪). (4) بیش از نیمی از شرکت‌کنندگان در علوم کامپیوتر یا رشته‌های مرتبط (59.4٪) تحصیل کرده‌اند. (5) تنها 19.3 درصد از شرکت‌کنندگان گواهینامه حرفه‌ای در مجازی‌سازی و امنیت اطلاعات دارند، درحالی‌که برخی دیگر از شرکت‌کنندگان دارای گواهینامه‌های مایکروسافت (33.3٪) هستند و برخی هیچ گواهی حرفه‌ای ندارند (36.7٪). (6) دو گروه عمده از موقعیت‌های شغلی شرکت‌کنندگان کارکنان شرکت فناوری اطلاعات (34.7٪) و یا مهندسین IT مشغول به کار در صنعت IT هستند (34.7٪). (7) بسیاری از شرکت‌کنندگان در زمینه فناوری‌های مربوط به مدت 5 سال یا بیشتر کار کرده‌اند (72.0٪). (8) بیش از نیمی از شرکت‌کنندگان کمتر از 5 سال در موقعیت شغل فعلی خود کار کرده‌اند (50.7٪) و (9) بیشتر کارفرمایان شرکت‌کنندگان در صنعت IT هستند (62.7٪).

جدول 5 میانگین و انحراف استاندارد از پاسخ به اقلام پرسشنامه در هر یک از چهار بُعد ISO / IEC 27001 را نشان داده است: " امنیت فیزیکی و محیطی"، " مدیریت ارتباطات و عملیات"،" کنترل دسترسی"و" اکتساب سیستم اطلاعات، توسعه و نگهداری". بنابراین واضح است که مجازی‌سازی می‌تواند به نفع امنیت اطلاعات از دیدگاه شرکت‌کنندگان باشد.

جدول 3: خلاصه‌ای از تحلیل‌ها در مورد قابلیت اطمینان

ابعاد	موارد پرسشنامه	مورد	آلفا کرونباخ
امنیت فیزیکی و محیطی	تجهیزات مکان و حفاظت امنیت کابل‌کشی تجهیزات تعمیر و نگهداری دفع امن و یا استفاده مجدد از تجهیزات	Q5 Q6 Q7 Q8	0.924
مدیریت ارتباطات و عملیات	جدایی از توسعه، تست و امکانات عملیاتی مدیریت ظرفیت سیستم پذیرش کنترل در برابر کد های مخرب تهیه اطلاعات نسخه پشتیبان شبکه کنترل مدیریت رسانه‌های قابل حمل دفع رسانه روشهای استفاده اطلاعات امنیت مستندات سیستم ورود به سیستم حسابرسی استفاده از سیستم مانیتورینگ حفاظت از اطلاعات ورود به سیستم مدیر و اپراتور لاگ‌های مربوط لاگ ورود هماهنگ‌سازی ساعت	Q9 Q10 Q11 Q12 Q13 Q14 Q15 Q16 Q17 Q18 Q19 Q20 Q21 Q22 Q23 Q24	0.952
کنترل دسترسی	ثبت نام کاربر مدیریت رمز عبور برای کاربران سیاست در استفاده از خدمات شبکه تشخیص از راه دور و حفاظت از پیکربندی پورت کنترل اتصال به شبکه انزوا حساس سیستم	Q25 Q26 Q27 Q28	0.927

	دورکاری	Q29 Q30 Q31	
سیستم اطلاعات، توسعه و تعمیر و نگهداری	کنترل نرم افزار کاربردی حفاظت از داده‌ها آزمون سیستم بررسی فنی برنامه های کاربردی پس از تغییراتی در سیستم عامل کنترل آسیب‌پذیری‌های فنی	Q32 Q33 Q34 Q35	0.913
مدیریت دارایی	استفاده قابل قبول از دارایی	در پرسشنامه نیست	

جدول 6 نتایج حاصل از آنالیز واریانس یک طرفه و آزمون Scheffe برای تفاوت در پاسخ شرکت‌کنندگان با عناوین شغل‌های مختلف و از بخش‌های مختلف صنعت است. نتایج حاصل از آنالیز واریانس آزمون F نشان می‌دهد که به جز "کنترل دسترسی،" درک قابل توجهی در امنیت اطلاعات از مجازی‌سازی وجود دارد.

جدول 4: خلاصه‌ای از توزیع جمعیتی شرکت‌کنندگان.

سوال	توزیع عمده	فراوانی	درصد ٪
جنسیت	مرد	124	82.7
سن	31 تا 35 ساله 36 تا 40 ساله	66 41	44.0 27.3
تحصیلات	دانشگاهی تحصیلات تکمیلی	64 45	42.7 30.0
پس‌زمینه تحصیلی	مربوط به IT	89	59.4
گواهی تخصصی	گواهی‌نامه حرفه‌ای مایکروسافت	50	33.3
موقعیت شغلی	کارکنان IT (شرکت) متخصصان IT (صنعت IT)	52 52	34.7 34.7
زمان صرف شده در زمینه مربوط به IT	5 تا 10 سال 10 سال به بالا	56 52	37.3 34.7
زمان صرف شده در موقعیت فعلی	1 تا 3 سال 3 تا 5 سال	40 36	26.7 24.0
بخش صنعت خود شرکت	صنعت اطلاعات	94	62.7
مقیاس شرکت شما	بیش از 500 کارمند	53	35.3
تعداد کارکنان شرکت در بخش IT	بیش از 10 نفر از کارکنان	79	52.7

جدول 5: توزیع امتیاز برای چهار بعد ISO / IEC.

ابعاد	میانگین امتیاز توزیع فرکانس	انحراف استاندارد از توزیع فرکانس
امنیت فیزیکی و محیطی	5.384	1.2753
مدیریت ارتباطات و عملیات	4.876	1.0918
کنترل دسترسی	4.885	1.1640
اکتساب سیستم اطلاعات، توسعه و نگهداری	5.060	1.2739

به طور خاص، آزمونScheff نتایج دقیق‌تری در هر موقعیت شغلی و صنعت نشان می‌دهد، که این اطلاعات عبارتند از: (1) در بُعد " مدیریت ارتباطات و عملیات،" تنها مهندسان در صنعت فناوری اطلاعات معتقدند که مجازی‌سازی تأثیر قابل توجهی در امنیت اطلاعات دارد؛ (2) در "کنترل دسترسی،" هر دو مدیران شرکت IT و مهندسان صنعت IT معتقدند که مجازی‌سازی تأثیر قابل توجهی در امنیت اطلاعات دارد؛ (3) در " امنیت فیزیکی و محیطی،" صنعت الکترونیک، IT و اتومبیل بر این باورند که مجازی‌سازی تأثیر قابل توجهی در امنیت اطلاعات دارد؛ و (4) تنها صنعت‌های IT و خودرو معتقدند که مجازی‌سازی تأثیر قابل توجهی در امنیت اطلاعات دارد.

برای انعکاس تفاوت ادراکی میان سطح تجربه‌های مختلف، یک متغیر وابسته جدید با تقسیم "مدت زمان حضور کاربر در IT حرفه‌های مرتبط " به دو مقدار (5تا10 سال در مقابل بیش از 10 سال) به کار بردیم و ابعاد استاندارد ISO / IEC به‌عنوان متغیرهای مستقل مورد استفاده قرار گرفت. رگرسیون لجستیک در این مطالعه محاسبه شده است (در جدول 7 نشان داده شده است). متغیرهای مستقل در این مطالعه دارای چهار بُعد هستند (به‌عنوان مثال، " امنیت فیزیکی و محیطی،" " مدیریت ارتباطات و عملیات"،" کنترل دسترسی"و" اکتساب سیستم اطلاعات،توسعه و تعمیر و نگهداری ")، و متغیر وابسته "زمان صرف شده در حرفه‌های مرتبط" است. تجزیه و تحلیل نتایج رگرسیونی نشان می‌دهد که " مدیریت ارتباطات و عملیات " یکی از موارد مهم و تعیین کننده در این مطالعه است.

4. بحث

پژوهش حاضر قصد دارد به درک تاثیرات مجازی‌سازی بر روی امنیت اطلاعات بپردازد. از طریق بررسی 32 کنترل انتخاب شده از ISO / IEC 27001، ابعاد خاصی از امنیت اطلاعات برای اجرای مجازی‌سازی، با برخی از تغییرات موجود در پس‌زمینه جمعیتی شرکت‌کنندگان شناسایی شده‌اند. چهار پرسش پژوهش پیشنهادی به شرح زیر عنوان می‌گردد.

(1) سوال 1 از منظر امنیت فیزیکی و محیطی است و برای بیان تاثیر پیاده‌سازی مجازی‌سازی در شرکت به منظور امنیت اطلاعات ارائه شده است.

جدول6: نتایج آزمون ANONA و Scheffe

Variable name	Physical and Environmental Security		Communication and Operation Management		Access Control		Information System Acquisition, Development and Maintenance	
	F	Scheffe	F	Scheffe	F	Scheffe	F	Scheffe
IT staff (Enterprise)	3.415*	No significant differences	3.101*	No significant differences	2.228	No significant differences	2.738*	No significant differences
IT manager (Enterprise)		No significant differences		No significant differences		significant differences		No significant differences
Engineer (IT industry)		No significant differences		significant differences		significant differences		No significant differences
Manager (IT industry)		No significant differences		No significant differences		No significant differences		No significant differences
IT personnel (IT industry)		No significant differences		significant differences		No significant differences		No significant differences
Electronics industry	4.357**	Significant differences	3.111*	No significant differences	3.41*	No significant differences	3.41*	No significant differences
IT industry		Significant differences		No significant differences		Significant differences		No significant differences
Automobile industry		Significant differences		No significant differences		Significant differences		No significant differences
Bank and securities industry		No significant differences		No significant differences		No significant differences		No significant differences
Other		Significant differences		No significant differences		No significant differences		No significant differences

* $P < 0.05$.
** $P < 0.01$.

جدول 7: نتایج تحلیل رگرسیون لجستیک.

سطح تاثیرگذاری	Df	Wald	S.E.	ضریب بتا	
0.265	1	1.243	1.436	-1.602	Intercept
0.683	1	0.167	0.288	0.118	امنیت فیزیکی و محیطی
⁎0.034	1	4.512	0.724	1.537	مدیریت ارتباطات و عملیات
0.322	1	0.983	0.509	-0.504	کنترل دسترسی
0.122	1	2.396	0.564	-0.873	اکتساب سیستم اطلاعات، توسعه و نگهداری

پاسخ برای صنعت‌های الکترونیک، IT، و خودرو مثبت است، اما برای صنعت بانکداری منفی است. امنیت اطلاعات یکی از بزرگترین نگرانی‌ها در صنعت بانکداری است و در اقدامات امنیتی سطح بالا همیشه برای همه عملیات بانکی استفاده

می‌شود. بنابراین می‌توان دریافت که اگر تحت اقدامات امنیتی سطح بالا یکسانی انجام گیرد تفاوت قابل توجهی در امنیت اطلاعات قبل و بعد از اجرای مجازی‌سازی وجود دارد.

(2) سوال 2 از منظر مدیریت ارتباطات و عملیات است، و برای مشاهده‌ی تاثیرات قابل توجه امنیت اطلاعات پیشنهاد شده است. نتایج نشان می‌دهد که شرکت‌کنندگان شاغل در صنعت IT به‌طور خاص در مورد نفوذ مجازی‌سازی در امنیت اطلاعات باخبر هستند. یکی از توجیهات ممکن این است که مجازی‌سازی یک محیط اطلاعات ایزوله شده برای توسعه و تست نرم افزار فراهم می‌کند. دلیل دیگر ممکن است پشتیبان‌گیری سریع و بازیابی فعال منجر به انجام تغییرات و بهبود سیستم‌های اطلاعات گردد.

(3) پرسش 3از منظر کنترل دسترسی است، و برای بررسی تاثیر قابل توجه مجازی‌سازی بر امنیت اطلاعات طراحی شده است. یافته‌های به‌دست آمده نشان می‌دهد که مجازی‌سازی تاثیراتی بر امنیت اطلاعات در مورد کنترل دسترسی در IT و صنایع خودرو دارد. در واقع، با اشاره به شکل 1، ماشین مجازی در هایپروایزر به خوبی ایزوله شده و این ویژگی منجر به کنترل دسترسی خوب می‌گردد.

(4) سوال 4 از منظر سیستم اطلاعات، توسعه و تعمیر و نگهداری نگران است و برای تاثیر قابل توجه مجازی‌سازی در امنیت اطلاعات ارائه شده است. بااین حال، نتایج نشان می‌دهد که تأثیرات معنی‌داری بر روی همه صنایع بررسی شده وجود دارد.

نتایج تجزیه‌وتحلیل داده‌ها نشان می‌دهد که متخصصان فناوری در موقعیت‌های مختلف شغلی تصور متفاوتی از نفوذ مجازی‌سازی در امنیت اطلاعات دارند. چنین تفاوتی ممکن است مربوط به تجربیات عملی مربوط به شغل / وظایف مختلف باشد.

6. نتیجه‌گیری

این پژوهش به بررسی تاثیر مجازی‌سازی اطلاعات در امنیت اطلاعات می‌پردازد. نتایج حاصل از تجزیه‌وتحلیل نشان می‌دهد که اجرای مجازی‌سازی در سازمان‌ها ممکن است منجر به اثبات امنیت اطلاعات گردد. آزمون Scheffe نشان

می‌دهد که برای صنایع الکترونیک، IT و خودرو، اجرای مجازی‌سازی اطلاعات تأثیر قابل توجهی در امنیت اطلاعات از نظر " امنیت فیزیکی و محیطی" دارد. برای صنایع IT و خودرو، مجازی‌سازی دارای تأثیر قابل توجهی در امنیت اطلاعات از منظر "کنترل دسترسی" دارد. افراد حرفه ای شاغل در صنعت IT و مدیران شرکت فناوری اطلاعات تصور تأثیر قابل توجهی از مجازی‌سازی در امنیت اطلاعات از منظر " مدیریت ارتباطات و عملیات" دارند. همانطور که برای بُعد " اکتساب سیستم‌های اطلاعات، توسعه و نگهداری "، معرفی فن‌آوری‌های مجازی‌سازی تاثیر قابل توجهی بر امنیت اطلاعات نمی‌گذارد.

برای کمک به مفاهیم، این مطالعه روش‌های جدید بررسی تاثیر مجازی‌سازی در امنیت اطلاعات را فراهم می‌کند. ترکیبی از یک پرسشنامه بر اساس ISO / IEC 27001 و نظرات از افراد شاغل در IT منجر به جنبه‌های جدیدی برای تحقیقات دانشگاهی آتی در حوزه مجازی‌سازی و امنیت اطلاعات می‌گردد. برای افراد شاغل در IT، اطلاعات در مورد تأثیرات مختلف مجازی‌سازی در امنیت اطلاعات و در ابعاد مختلف صنایع مختلف ممکن است برخی از دستورالعمل‌های امنیت اطلاعات مفیدی برای کاربران فناوری ارائه دهد.

با وجود این یافته‌ها، این مطالعه ممکن است برخی از آنها محدودیت ها را داشته باشد. هر دو اعتبار محتوا و اعتماد از جنبه‌های مطالعه‌ی انجام شده توسط یک اندازه نمونه کوچک و محدود هستند. تنها 13 کارشناس در دور اول برای مطالعه اعتبار شرکت کردند، که مانع استفاده دقیق CVR برای ایجاد آماره شده است. فرسایشی متعادل در فاز پایایی این مطالعه رخ داده است. حجم نمونه بزرگتر برای هر دو فاز اول و دوم موجب بهبود قدرت و اعتبار شده و کمک شایایینی به کاهش ساییدگی در فاز دوم کرده است. پس از جمع‌آوری تجربی بسیاری از داده‌ها، برخی از روش‌های تجزیه و تحلیل آماری پیشرفته می‌توانند برای ارزیابی پایداری مدل، و اعمال / بررسی وضعیت مدل / اندازه‌گیری موارد به محیط‌های متفاوت امنیتی اطلاعات مربوطه به کار گرفته شوند.

در زیر برخی از پیشنهادات ممکن برای آینده پژوهش‌ها آورده شده است.

(1) در حالی که این تحقیق از ISO 27001 به‌عنوان استاندارد حسابرسی به تصویب رسیده است، استانداردهای امنیت اطلاعات دیگر مانند COBIT و ITIL، ممکن است برای انجام اهداف این مطالعه به کار روند. انتخاب و یا مقایسه با استانداردهای مختلف ممکن است بینش بیشتری در مورد تاثیر مجازی‌سازی در امنیت اطلاعات ارائه دهد.

(2) با گسترش فن‌آوری‌های مجازی‌سازی، نمونه‌های بیشتری باید به‌عنوان سمبل سایر صنایع به منظور بهبود قابلیت اطمینان داده‌ها و اعتبار جمع‌آوری شود. بنابراین با انجام چنین عملی، برخی از پیشنهادات دقیق و یا اضافی ممکن است برای کسب و کار در حال برنامه‌ریزی در جهت اتخاذ و یا اجرای مجازی‌سازی ارائه شود.

(3) عوامل اکتشاف و تحلیل، باید در آینده‌ای نزدیک برای داشتن یک درک بهتر از مقیاس‌های اندازه‌گیری در مطالعه ارائه شده ارزیابی شوند. پژوهش‌های آینده ممکن است نیاز به تشخیص عوامل کلیدی منتسب به کارشناسان و کاربران IS / IT داشته باشند.

References

[1] D. Ary, L. Jacobs, A. Razavieh, Introduction to Research in Education, 7th Ed Wadsworth Publishing, New York, NY, 2005.

[2] M. Bogicevic, I. Milenkovic, D. Simic, Identity management—a survey, Innovative Management and Firm Performance: An Interdisciplinary Approach and Cases2014. (370).

[3] A. Calder, Implementing Information Security Based on ISO 27001/ISO 27002, Van Haren Publishing, Zaltbommel, NL, 2012.

[4] T. Carlson, Understanding ISO 27001. Available at http://www.orangeparachute. com/documents/Understanding_ISO_27001.pdf 2005.

[5] M. Carpenter, Integrated security risk management solution is a key to protecting government networks, Homel. Def. J. 5 (1) (2007) 40–41.

[6] E. Casey, G.J. Stellatos, The impact of full disk encryption on digital forensics, ACM SIGOPS Oper. Syst. Rev. 42 (3) (2008) 93–98.

[7] Q. Chen, R. Xin, Optimizing enterprise IT infrastructure through virtual server consolidation, Proc. 2005 Inf. Sci. IT Educ. Joint Conf., 19, 2005 (2009).

[8] R.M. Chen, K.T. Hsieh, Effective allied network security system based on designed scheme with conditional legitimate probability against distributed network attacks and intrusions, Int. J. Commun. Syst. 25 (5) (2012) 672–688.

[9] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B.F. Machado, A. Forget, R. Biddle, The MVP Web-based Authentication Framework. Financial Cryptography and Data Security (pp. 16–24), Springer, Berlin, DE, 2012.

[10] N.M. Chowdhury, R. Boutaba, A survey of network virtualization, Comput. Netw. 54 (5) (2010) 862–876.

[11] M. Christodorescu, R. Sailer, D.L. Schales, D. Sgandurra, D. Zamboni, Cloud security is not (just) virtualization security: a short paper, Proc. 2009 ACM Wkshp. Cloud Comput. Secur 2009, pp. 97–102.

[12] S. De Haes, W. Van Grembergen, R.S. Debreceny, COBIT 5 and enterprise governance of information technology: building blocks and research opportunities, J. Inf. Syst. 27 (1) (2013) 307–324.

[13] M. Egele, T. Scholte, E. Kirda, C. Kruegel, A survey on automated dynamic malwareanalysis techniques and tools, ACM Comput. Surv. (CSUR) 44 (2) (2012) 6.

[14] B. Elisa, S. Ravi, Database security—concepts, approaches, and challenges, IEEE Trans. Dependable Secur. Comput. 2 (1) (2005) 2–19.

[15] Enterprise Strategy Group, ESG Research Brief: 2011 Virtualization Software Spending Trends. Available at http://www.enterprisestrategygroup.com/2011/02/ esg-research-brief-2011- virtualization-software-spending-trends/ 2011.

[16] D.G. Feng, M. Zhang, Y. Zhang, Z. Xu, Study on cloud computing security, J. Softw. 22 (1) (2011) 71–83.

[17] B. Grobauer, T.Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Secur. Priv. 9 (2) (2011) 50–57.

[18] J.F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, Multivariate Data Analysis: A Global Perspective, 7th Ed. Pearson Prentice Hall, Upper Saddle River, NJ, 2010.

[19] D.A. Haworth, L.R. Pietron, Sarbanes–Oxley: achieving compliance by starting with ISO 17799, Inf. Syst. Manag. 23 (1) (2006) 73–87.

[20] S.N. Haynes, D.C.S. Richard, E.S. Kubany, Content validity in psychological assessment: a functional approach to concepts and methods, Psychol. Assess. 7 (3) (1995) 238–247.

[21] K.J. Higgins, VMs create potential risks. Available at http://www.darkreading.com/ security/security-management/208804369/index.html 2007.

[22] M.T. Hoesing, Virtualization security assessment, Inf. Secur. J.: Glob. Perspect. 18 (3) (2009) 124–130.

[23] C.T. Hsieh, Strategies for successfully implementing a virtualization project: a case with VMware, Commun. IIMA 8 (3) (2014) 1.

[24] Y.L. Huang, B. Chen, M.W. Shih, C.Y. Lai, Security impacts of virtualization on a network testbed, Proc. SERE 2012 2012, pp. 71–77.

[25] S. Iizuka, K. Ogawa, S. Nakajima, Factors affecting user reassurance when handling information in a public work environment, Int. J. Hum. Comput. Interact. 23 (1–2) (2007) 163–183.
[26] International Organization for Standardization, ISO/IEC 27001: 2005. Available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber= 42103 2005.
[27] B. Johnson, L. Christensen, Educational Research: Quantitative, Qualitative, and Mixed Approaches, 2nd ed. Pearson, New York, NY, 2004.
[28] T.A. Johnson, Server virtualization: information security considerations, Information Security Management Handbook, 6 2012, p. 101.
[29] T. Jones, Discover the Linux Kernel Virtual Machine. Available at: http://www-128. ibm.com/developerworks/linux/library/l-linux-kvm/ 2007.
[30] M. Kallahalla, M. Uysal, D. Swaminathan, E. Nigel, C.I. Dalton, F. Gittler, SoftUDC: a software-based data center for utility computing, IEEE Comput. Soc. 37 (11) (2004) 38–46.
[31] G. Khanna, Y. Beaty, G. Kar, A. Kochut, Application performance management in virtualized server environments, Proc. 10th IEEE/IFIP Netw. Oper. Manage. Symp 2006, pp. 373–381.
[32] M.A. Khoshkholghi, A. Abdullah, R. Latip, S. Subramaniam, M. Othman, Disaster recovery in cloud computing: a survey, Comput. Inf. Sci. 7 (4) (2014) 39.
[33] G. Kovacich, ISSO career development, Comput. Secur. 16 (6) (1997) 455–468.
[34] C.H. Lawshe, A quantitative approach to content validity, Pers. Psychol. 28 (4) (1975) 563–575.
[35] G. Lawton, Virus wars: fewer attacks, new threats, Computer 35 (12) (2002) 22–24.
[36] J. Li, B. Li, T. Wo, C. Hu, J. Huai, L. Liu, K.P. Lam, CyberGuarder: a virtualization security assurance architecture for green cloud computing, Futur. Gener. Comput. Syst. 28 (2012) 379–390.
[37] Q. Li, C. Yang, Development trends of MIS based on cloud computing environment, 2010 Int. Symp. Inf. Sci. Eng. (ISISE) 2010, pp. 145–148.
[38] T.E. Lindquist, K.A. Gary, H.E. Koehnemann, H. Naccache, Component framework for web-based learning environments, Front. Educ. Conf. 2 (1999) 23–28.
[39] W. Liu, Software protection with encryption and verification, Software Engineering and Knowledge Engineering: Theory and Practice, Springer, Berlin, DE, 2012. 131–138.
[40] P.Y. Logan, S.W. Logan, Bitten by a bug: a case study in malware infection, J. Inf. Syst. Educ. 14 (3) (2003) 301–305.
[41] F. Lombardi, R. Di Pietro, Secure virtualization for cloud computing, J. Netw. Comput. Appl. 34 (4) (2011) 1113–1122.
[42] R.M. Magalhaes, Security and virtualization. Available at: http://www.windowsecurity. com/articles/Security-Virtualization.html 2008.
[43] D. Marshall, Top 10 benefits of server virtualization, InfoWorld 2 (11) (2011).
[44] A. Menon, A.L. Cox, W. Zwaenepoel, Optimizing network virtualization in Xen, Proc. USENIX Annual Tech. Conf 2006, pp. 15–28.
[45] I. Mevag, Towards Automatic Management and Live Migration of Virtual MachinesMaster thesis University of Oslo, Norway, 2007.
[46] Personnel system identifies commendable actions and problematic trends, in: L. Miller, R. Pierce (Eds.),TechBeat Dated: Winter 2013 2013, p. 14.
[47] J.C. Nunnally, I.H. Bernstein, Psychometric Theory, 3rd Ed. McGraw-Hill, New York, NY, 1994.
[48] M. Nyanchama, Enterprise vulnerability management and its role in information security management, Inf. Secur. J.: A Glob. Perspect. 14 (3) (2005) 29–56.
[49] R. Oppliger, Internet security: firewalls and beyond, Commun. ACM 40 (5) (1997) 92–102.
[50] J. Park, B. Noh, Web attack detection: classifying parameter information according to dynamic web page, Int. J. Web Serv. Pract. 2 (1–2) (2006) 68–74.
[51] J. Pauli, The Basics of Web Hacking: Tools and Techniques to Attack the Web, Elsevier, Amsterdam, NL, 2013.
[52] C.L. Pritchard, Risk Management: Concepts and Guidance, 4th Ed. ESI International, Arlington, VA, 2010.

[53] Y. Qi, B. Yang, B. Xu, J. Li, Towards system-level optimization for high performance unified threat management, Int. Conf. Netw. Serv. (INCS) 7 (2007).
[54] E. Ray, E. Schultz, Virtualization security, Proc. 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, 2009.
[55] K. Renauda, Quantifying the quality of web authentication mechanisms: a usability perspective, J. Web Eng. 3 (2) (2004) 95–123.
[56] G. Ridley, J. Young, P. Carroll, COBIT and its utilization: a framework from the literature, Proc. 37th Annu. Hawaii Int. Conf. Syst. Sci., 8, 2004.
[57] F. Sabahi, Virtualization-level security in cloud computing, Proc. IEEE 3rd International Conference on Communication Software and Networks (ICCSN) 2011, pp. 250–254.
[58] D. Shackleford, Virtualization Security: Protecting Virtualized Environments, John Wiley & Sons, New York, NY, 2012.
[59] D.H. Shin, The dynamic user activities in massive multiplayer online role-playing games, Int. J Human–Comput. Interact. 26 (4) (2010) 317–344.
[60] D.H. Shin, Y.J. Shin, Consumers' trust in virtual mall shopping: the role of social presence and perceived security, Int. J Human–Comput. Interact. 27 (5) (2011) 450–475.
[61] H. Shiravi, A. Shiravi, A.A. Ghorbani, A survey of visualization systems for network security, IEEE Trans. Vis. Comput. Graph. 18 (8) (2012) 1313–1329.
[62] E. Shmueli, R. Vaisenberg, Y. Elovici, C. Glezer, Database encryption: an overview of contemporary challenges and design considerations, ACM SIGMOD Rec. 38 (3) (2010) 29–34.
[63] A. Singh, An introduction to virtualization. Available at: http://www.kernelthread. com/publications/virtualization/ 2004.
[64] A. Singh, M. Korupolu, D. Mohapatra, Server-storage virtualization: integration and load balancing in data centers, Conf. High Perform. Netw. Comput, 2008.
[65] J.C. Song, J.W. Ryu, B.J. Moon, H.K. Jung, Strategy for adopting server virtualization in the public sector, J. Inf. Commun. Converg. Eng. 10 (1) (2012) 61–65.
[66] Symantec, Information security trends forecast. Available at http://protectyoursecrets. symantec.com/zh/tw/about/news/release/article.jsp?prid=20090202_02 2009.
[67] C.W. Thompson, D.R. Thompson, Identity management, IEEE Internet Comput. 11 (3) (2007) 82–85.
[68] H.N. Van, F.D. Tran, J.M. Menaud, Performance and power management for cloud infrastructures, Proc. IEEE 3rd International Conference on Cloud Computing 2010, pp. 329–336.
[69] S.J. Vaughan-Nichols, Virtualization sparks security concerns, Computer 41 (8) (2008) 13–15.
[70] Q. Wang, W. Wu, Y. Gu, The application of Lucene in information leakage monitoring and querying system, IEEE 2010 2nd International Conference on Information Engineering and Computer Science (ICIECS 2010, pp. 1–4.
[71] X. Wang, J. Luo, M. Yang, Z. Ling, A potential HTTP-based application-level attack against Tor, Futur. Gener. Comput. Syst. 27 (1) (2011) 67–77.
[72] T. Yokoyama, M. Hanaoka, M. Shimamura, K. Kono, Simplifying security policy descriptions for internet servers in secure operating systems, Proc. 2009 ACM Symp. Appl. Comput 2009, pp. 326–333.
[73] G.U.I. Yong-Hong, Study and Applications of Operation System Security Baseline. (Available at http://en.cnki.com.cn/Article_en/CJFDTOTAL-DZJC201110009.htm) Computer Security, 2011–102011.
[74] O. Yoshihiko, Y. Tetsu, Server virtualization technology and its latest trends, Fujitsu Sci. Tech. J. 44 (1) (2008) 46–52.
[75] I.X. Zhang, Economic consequences of the Sarbanes–Oxley Act of 2002, J. Account. Econ. 44 (2) (2007) 74–115.
[76] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Futur. Gener. Comput. Syst. 28 (2012) 583–592.
[77] ISO 27001, “Information Technology, Security Techniques, Information Security Management Systems, Requirements,”, International Organization for Standardization ISO, Geneve, 2005.