



Security Feasibility in Cloud Services, Challenges, Opportunities and Prospects

Marzeih Ahmadimoghadam

Computer Engineering Group, Zanjan Branch, Islamic Azad University, Zanjan, Iran

ABSTRACT

Received: 4 March 2022

Accepted: 29 May 2022

KEYWORDS:

Cloud Computing
Security
Service Agreement
Authentication
Authorization

Cloud computing is a new computing model that includes network computing, distributed computing; Parallel computing, virtualization technology, applied and auxiliary computing and other computer technologies originated. The security issue of cloud computing is very important and this issue can prevent the rapid development of cloud computing. If a security problem occurs for cloud computing, it can no longer be used on a large scale, and its rapid and widespread use by people will decrease. The two security issues of data privacy and service availability are among the issues that are raised about the security issue of cloud computing and are among its key security issues. Applying a security method alone cannot solve the security problem of cloud computing; Rather, a wide range of technologies, as well as new technologies and strategies, must be used together to protect the entire cloud computing system. This article introduces some fundamental cloud computing systems and the problem of security feasibility of cloud computing and existing risks and its related strategy as challenges, opportunities and perspectives of this field, according to the ideas and characteristics of cloud computing.

¹ Corresponding author



m.ahmadimoghadam@ziau.ac.ir



NUMBER OF REFERENCES

21



NUMBER OF FIGURES

1



NUMBER OF TABLES

0

امکان سنجی امنیت در خدمات ابری، چالش ها، فرصت ها و چشم اندازها

مرضیه احمدی مقدم

گروه مهندسی کامپیوتر، واحد زنجان، دانشگاه آزاد اسلامی، زنجان، ایران

چکیده:

رایانش ابری مدل رایانش جدیدی است که از رایانش شبکه ای، رایانش توزیعی؛ رایانش موازی، فناوری مجازی سازی، رایانش کاربرد پذیر و کمکی و دیگر فناوریهای کامپیوتری منشأ گرفته است. مسئله امنیتی رایانش ابری بسیار حائز اهمیت است و این مسئله می تواند مانع از توسعه سریع رایانش ابری شود. اگرچه مشکل امنیتی برای رایانش ابری رخ دهد، دیگر نمی توان در وسعت بالا از آن استفاده کرد و کاربرد سریع و وسیع آن توسط مردم کاهش می یابد. دو مسئله امنیت حریم خصوصی داده ها و هم چنین در دسترس بودن سرویس جزء مسائلی هستند که در مورد مسئله امنیتی رایانش ابری مطرح می شوند و از جمله مسائل کلیدی امنیتی آن به شمار می روند. به کارگیری روشی امنیتی به تنهایی قادر نیست مسئله امنیتی رایانش ابری را حل کند؛ بلکه باید فناوری های گسترده و زیادی و هم چنین فناوری ها و استراتژی های جدیدی را باید همراه با هم به کار گرفت تا بتوان از کل سیستم رایانش ابری محافظت کرد. این مقاله برخی از سیستم های رایانش ابری بنیادین را معرفی می کند و مسئله امکان سنجی امنیتی رایانش ابری و ریسکهای موجود و استراتژی مربوط به آن را بعنوان چالشها، فرصت ها و چشم اندازهای این حوزه با توجه به ایده ها و مشخصه های رایانش ابری مورد تجزیه و تحلیل قرار می دهد.

واژگان کلیدی:

پردازش ابری

امنیت

قرارداد خدمات

احراز هویت

مجوز



تعداد مراجع

۲۱



تعداد شکل ها

۱



تعداد جداول

۰

مقدمه

رایانش ابری به معنای ارائه سرویس‌های محاسباتی مانند سرورها، فضای ذخیره‌سازی، پایگاه‌های اطلاعاتی، شبکه‌ها، نرم‌افزارها، تجزیه و تحلیل‌ها و اطلاعات از طریق اینترنت برای ارائه نوآوری سریع‌تر و منابع انعطاف‌پذیر و صرفه‌جویی در مقیاس عظیم است. درواقع، شرکت‌ها به جای داشتن زیرساخت‌های محاسباتی یا مراکز داده خود، می‌توانند با استفاده از سرویس‌های ابری، به هر چیزی از برنامه‌های کاربردی تا فضای ذخیره‌سازی دسترسی اشتراکی و استیجاری داشته باشند [۱]. ارائه دهندگان خدمات ابری منابع و برنامه‌های فناوری محور را به عنوان یک سرویس در اختیار کاربران قرار می‌دهد و میزان آن را محاسبه می‌کنند که می‌توانند از طریق اینترنت از همان میزان محاسبه شده استفاده کنند. سرویس‌های ابری معمولاً شامل نرم افزار به عنوان سرویس (SaaS)، پلتفرم به عنوان سرویس (PaaS)، زیرساخت به عنوان سرویس (IaaS) می‌شوند، مانند قدرت محاسبات خام یا فضای ذخیره‌سازی ابری. این سرویس‌ها ابزارها و برنامه‌هایی مانند ذخیره‌سازی داده‌ها، سرورها، پایگاه‌های داده، شبکه و نرم‌افزار را دربر می‌گیرند. درحقیقت، ذخیره‌سازی مبتنی بر ابر به جای ذخیره و نگهداری فایل‌ها روی هارد دیسک اختصاصی یا دستگاه ذخیره‌سازی لوکال، امکان ذخیره‌سازی آن‌ها را در پایگاه داده از راه دور فراهم می‌کند. با استفاده از رایانش ابری، می‌توانید در زمان و مکان دلخواه فقط با استفاده از اتصال به اینترنت به داده‌ها و برنامه‌ها نرم‌افزاری دسترسی داشته باشید. از مزیت‌های مهم رایانش ابری که آن را به گزینه‌ای محبوب در بین کاربران و کسب‌وکارها تبدیل کرده است، می‌توان به مقرون به صرفه بودن، افزایش بهره‌وری، سرعت و کارایی، عملکرد و امنیت اشاره کرد. دلیل نام گذاری رایانش ابری این است که دسترسی به اطلاعات را از طریق فضای ابری یا فضای مجازی امکان پذیر می‌کند. شرکت‌هایی که سرویس‌های ابری ارائه می‌کنند، به کاربران امکان می‌دهند تا فایل‌ها و برنامه‌های کاربردی خود را روی سرورهای راه دور ذخیره کنند و سپس با استفاده از اینترنت در زمان و مکان مدنظرشان به اطلاعاتشان دسترسی داشته باشند. این یعنی کاربر به حضور در مکانی خاص برای دسترسی نیازی ندارد و از راه دور می‌تواند داده‌های ذخیره شده‌اش را به راحتی کنترل و مدیریت کند. رایانش ابری کارهای سنگین مربوط به پردازش داده‌ها را انجام می‌دهد و تمام این کارها را به کامپیوترهای بسیار دور در فضای مجازی منتقل می‌کند؛ در نتیجه، اینترنت به فضایی ابری تبدیل می‌شود و شما می‌توانید در هر نقطه‌ای از جهان با هر دستگاهی، به داده‌ها و فایل‌هایتان دسترسی داشته باشید [۲-۵].

امروزه با انتقال دستگاه‌ها، دیتاسنترها و فرایندهای تجاری به فضای ابری، امنیت ابری، اهمیت فزاینده‌ای پیدا کرده است. اطمینان از کیفیت داده‌های ابری از طریق سیاست‌های امنیت جامع، فرهنگ سازمانی و راه حل‌های امنیتی ابر حاصل می‌گردد. برای تجارت‌هایی که به فضای ابری منتقل می‌شوند، موضوعی مهم‌تر از امنیت وجود ندارد.

چالش‌ها، فرصت‌ها و چشم اندازهای امنیتی در ابر

چالش‌های امنیتی رایانش ابری یکی از مهمترین دغدغه‌های کاربران یا سازمان‌هایی است که قصد مهاجرت به فضای ابری را دارند. نگرانی آن‌ها قابل درک است. اینکه فرد نتیجه ماه‌ها و سال‌ها تلاش خود را جهت نگهداری به فرد دیگری بسپارد، کمی ترسناک است. براساس آمار Rightscale، این چالش ذهن بیش از ۷۵ درصد از کاربران بالقوه رایانش ابری را مشغول کرده است. از آنجا که ابر عمومی مرز مشخصی ندارد، چالش‌های امنیتی کاملاً متفاوتی را نیز در بر دارد. این امر با اتخاذ رویکردهای ابری مدرن مانند روش‌های ادغام مداوم خودکار و استقرار مداوم T معماری بدون سرور توزیع شده و دارایی‌های زودگذر مانند توابع به عنوان سرویس و حامل‌ها، چالش برانگیزتر می‌شود. لذا، برخی از چالش‌های امنیتی محیط‌های ابر و چندین لایه خطرانی که سازمان‌های ابر محور امروز با آن روبرو هستند عبارتند از [۶-۷]:

افزایش سطح حمله: فضای ابری عمومی برای هرکس که از اکسپلویت‌های ابر با ضعف ایمن برای دستیابی به داده‌های ابر استفاده می‌کنند، به یک سطح حمله بزرگ و بسیار جذاب تبدیل شده است. عدم وضوح و توانایی پیگیری: در مدل IaaS، ارائه دهندگان ابری کنترل کاملی بر لایه زیرساخت دارند و آن را در معرض دید مشتریان خود قرار نمی‌دهند. عدم دید و کنترل در مدل‌های ابری PaaS و SaaS بیشتر گسترش می‌یابد. مشتریان ابر اغلب نمی‌توانند دارایی‌های ابری خود را به طور موثر شناسایی کرده یا محیط ابر خود را تجسم کنند [۸].

بارکاری متغیر و پویا: دارایی‌های ابر به صورت پویا تهیه می‌شوند و از رده خارج می‌شوند. ابزارهای امنیتی سنتی به راحتی قادر به اجرای سیاست‌های حفاظتی در چنین محیط انعطاف‌پذیر و پویا با Workloads همیشه در حال تغییر و زودگذر نیستند.

اتوماسیون ابری: سازمانهایی که از فرهنگ کاملاً خودکار ابری استقبال کرده‌اند باید اطمینان حاصل کنند که کنترل‌های امنیتی مناسب در اوایل چرخه شناسایی و در کد و الگوها جاسازی شده‌اند. تغییرات مربوط به امنیت که پس از استفاده از حجم کار در تولید اعمال می‌شود، می‌تواند وضعیت امنیتی سازمان را تضعیف کند و همچنین باعث طولانی شدن زمان عرضه به بازار شود [۹].

مدیریت سطح دسترسی: معمولاً نقشهای کاربر ابر بسیار آزادانه پیکربندی می‌شوند و از امتیازات گسترده‌ای فراتر از آنچه که در نظر گرفته شده یا مورد نیاز است، اعطا می‌شوند. یک مثال متداول، دادن مجوز حذف یا نوشتن پایگاه داده به کاربران غیر آموزش دیده یا کاربرانی انجام می‌شود که نیازی به حذف یا افزودن دارایی‌های پایگاه داده ندارند. در سطح برنامه، کلیدها و امتیازات با تنظیمات نامناسب جلسات را در معرض خطرات امنیتی قرار می‌دهند.

محیط‌های پیچیده: مدیریت امنیت به روشی ثابت در محیط‌های ترکیبی و چند ابر که این روزها مورد پسند شرکت‌ها است، به روش‌ها

و ابزاری نیاز دارد که به طور یکپارچه در بین ارائه دهندگان ابر عمومی، ارائه دهندگان ابر خصوصی و استقرارهای پیش فرض کار کند - از جمله محافظت از دفتر شعبه برای سازمان های جغرافیایی توزیع شده.

سازگاری و مدیریت ابر: همه ارائه دهندگان خدمات ابری شناخته شده خود را با اکثر برنامه های معتبر شناخته شده هماهنگ کرده اند. با این حال، مشتریان مسئولیت اطمینان از انطباق حجم کار و فرآیندهای داده آنها را دارند. با توجه به دید ضعیف و همچنین پویایی محیط ابر، روند ممیزی انطباق به مأموریت نزدیک می شود مگر اینکه از ابزارهایی برای دستیابی به بررسی انطباق مداوم و صدور هشدارهای بی درنگ در مورد تنظیمات نادرست استفاده شود.

امنیت ابری مجموعه ای از اقدامات، راهکارها و فناوری هایی است که باهدف بهبود حفاظت از زیرساخت های ابری، داده های موجود در آنها و حریم خصوصی کاربران به کار گرفته می شوند. از آنجاکه زیرساخت های ابری بستری برای میزبانی داده های سازمان ها و پیشبرد اهداف آنها هستند، کارکرد بدون اختلال و حفظ امنیت بسیار مهم است. با این حال گاهی سازمان ها در خصوص میزان حفظ امنیت زیرساخت های ابری دچار تردید می شوند و درباره مهاجرت به ابر تردید می کنند. مزایای امنیت ابر از جمله دلایلی ست که افراد بسیاری را مجبور کرده به سمت استفاده از محصولات ابری بروند و در بیشتر محصولات امنیتی برای شناسایی مخاطرات، از سرویس های معتبر و مشهور استفاده می شود. تشخیص بدافزار براساس تحلیل نمونه ها و رفتار فایل های اجرایی بر روی رایانه های کلاینت انجام می شود. امنیت ابری به ما امکان می دهد رفتار برنامه های مخرب و نحوه توزیع آنها بر روی رایانه ها، کشورها و قاره های مختلف را در سطح جهان بررسی کنیم. مهم ترین مزایا و فرصت های ایجاد بستر امنیتی در فضای رایانش ابری عبارتند از [۱۲-۱۰].

امنیت متمرکز: همان طور که رایانش ابری، برنامه ها و داده ها را متمرکز می کند، امنیت ابری نیز برنامه های محافظتی را متمرکز می نماید. شبکه های تجاری مبتنی بر ابر شامل تعداد زیادی دستگاه و endpoint می باشند که مدیریت آن ها زمانی که با shadow IT سر و کار دارند، کاری دشوار می باشد. مدیریت این نهادها، به صورت متمرکز، باعث افزایش آنالیز ترافیک و وب فیلترینگ شده و نظارت بر وقایع شبکه را ساده سازی می نماید. در ضمن زمانی که برنامه های disaster recovery از یک مکان مدیریت شوند، به سادگی قابل اجرا هستند.

کاهش هزینه: یکی از مزایای استفاده از فضای ذخیره سازی ابری و امنیت این است که دیگر نیازی به سرمایه گذاری در سخت افزارهای اختصاصی نمی باشد. در ضمن علاوه بر کاهش هزینه ها در صرفه جویی زمان نیز بسیار موثر می باشد. در حالی که تیم IT به طور واکنشی به مسائل امنیتی می پردازد، امنیت ابری، ویژگی های امنیتی شبانه روزی و بدون هیچ گونه دخالت انسان را ارائه می دهد [۱۴-۱۳].

کاهش اقدامات مدیریتی: هنگامی که شما یک خدمات دهنده ی معتبر انتخاب می کنید، در حقیقت برای همیشه با تنظیمات دستی امنیتی و به روز رسانی های امنیتی خداحافظی می کنید. انجام این وظایف نیاز به منابع بسیاری دارد، اما زمانی که شما آن ها را به فضای ابری منتقل می کنید، مدیریت امنیت در یک مکان و با کنترل شما انجام می شود.

قابلیت اطمینان: خدمات محاسبات ابری از حداکثر قابلیت اطمینان برخوردار هستند. با در نظر گرفتن تدابیر مناسب امنیت ابر، کاربران می توانند با آسودگی خاطر به داده ها و برنامه های خود در داخل فضای ابری دسترسی داشته باشند و هیچ گونه اهمیتی ندارد که کجا هستند و یا از چه دستگاهی استفاده می کنند.

امروزه سازمان های بیشتری به مزایای انتقال سیستم هایشان به فضای ابری پی برده اند. محاسبات ابری این امکان را به سازمان ها می دهد که هزینه های خود را کاهش داده و از سیستم هایی استفاده کنند که به آن ها برتری رقابتی دهد. قابل ذکر است، سازمان ها می بایست به امنیت محاسبات ابری خود اطمینان داشته باشند و مطمئن باشند که تمامی داده ها، سیستم ها و برنامه ها در مقابل سرقت، نشت و حذف داده ها محافظت می گردند. این مطلب را نباید فراموش کرد که کلیه ی مدل های ابر در معرض تهدید هستند. دپارتمان های IT، همواره در مورد موضوع انتقال سیستم های بسیار مهم و حیاتی به فضای ابری، محتاط هستند و رعایت قوانین امنیتی برای استفاده از تمامی مدل های ابر ضروری می باشد. امنیت ابر، تمامی قابلیت های امنیت سنتی را ارائه می دهد و به مشاغل این امکان را می دهد که ضمن حفظ امنیت از مزایای بی شمار محاسبات ابری بهره مند گردند. در ضمن در مورد رعایت حریم خصوصی و الزامات انطباق آن ها نیز می توانند اطمینان کامل حاصل نمایند [۱۷-۱۵].

امکان سنجی امنیت در فضای ابری

امنیت ابری که تحت عنوان امنیت محاسبات ابری نیز شناخته می شود، مجموعه ای از سیاست ها، مدیریت ها، روش ها و فناوری هایی است که به منظور محافظت از سیستم ها، داده ها و همچنین زیرساخت های مبتنی بر ابر با یکدیگر کار می کنند. اقدامات امنیتی جهت محافظت از داده های ابری، حفظ حریم خصوصی مشتریان و همچنین تنظیم قوانینی جهت تایید اعتبار برای هر یک از کاربران و دستگاه ها به وجود آمده اند. شکل زیر ابعاد مهم امکان سنجی امنیت در محیط های مبتنی بر رایانش ابری را نمایش می دهد:



شکل ۱. ابعاد امکان سنجی امنیت در خدمات رایانش ابری

بیفتد، بعد از آن این نوع از کنترل‌ها سعی در پوشش حمله و کاهش خرابی امنیت سیستم می‌کند.

کنترل‌های تصحیح‌کننده: این کنترل سعی در کاهش اثر حمله دارد. برخلاف کنترل پیش‌گیرنده، کنترل تصحیح‌کننده در حین وقوع حمله، عکس‌العمل نشان می‌دهد [۲۱].

کنترل شناسایی‌کننده: این نوع از کنترل سعی در شناسایی حمله حین وقوع آن دارد. در زمان رخداد حمله، کنترل شناسایی‌کننده، سیگنالی برای کنترل‌های پیش‌گیرنده یا تصحیح‌کننده برای مشخص کردن مشکل ارسال می‌کند.

سایر توصیه‌ها عبارتند از: جهت افزایش امنیت ابرها برنامه‌ریزی کنید. تصور نکنید که از داده‌های موجود در ابر، نسخه پشتیبان تهیه شده است، در نتیجه به فکر نسخه پشتیبان باشید. رمزگذاری دو مرحله‌ای برای دسترسی به برنامه‌های ابری و موقعیت مکانی IP انجام دهید. عنصر انسانی یکی از بزرگ‌ترین تهدیدات برای امنیت شماست. در نتیجه در رابطه با مدیریت سیستم خود، قدرتمند عمل کنید. به واسطه پشتیبان گرفتن، در صورت از بین رفتن داده‌های ابری یا باج گرفتن، داده‌های خود را از نسخه‌های آفلاین حفظ کنید. با مراکز نظارت امنیتی نیز قرارداد ببندید تا بر داده‌های ابری شما مدیریت داشته باشند. از فناوری پیشرفته فایروال استفاده کنید. از خدمات برنامه، لایه‌بندی و تقسیم بندی برای محافظت داده‌های خود استفاده کنید. کسب و کارها باید از ارزیابی خطرات و مزایای امنیتی محاسبات ابری غافل نشوند. مشتریان باید بدانند که داده‌های آنها در کجا ذخیره می‌شود و از امنیت آن مطمئن شوند. همچنین مشتری باید به توافق‌نامه‌های سطح خدمات توجه کند و از مطمئن بودن آگاه شود. در هر حال تهدیدات در فضای ابری زیاد است و برای جلوگیری از این تهدیدات بهتر است روش‌های ذکرشده را در نظر بگیرید و جهت افزایش امنیت ابر از آنها استفاده کنید تا داده‌های خود را با آرامش خاطر بیشتری در این فضا قرار دهید.

امنیت ابری را می‌توان از تاییدیه اعتبار جهت دسترسی به ترافیک تا فیلتر کردن ترافیک با توجه به نیازهای مختلف تجاری، تنظیم نمود. از آن جا که می‌توان این قوانین را در یک محل تنظیم و مدیریت نمود، تاثیر بسزایی در کاهش هزینه‌ها دارد و در ضمن تیم فناوری اطلاعات فرصت کافی برای تمرکز بر سایر حوزه‌های تجاری پیدا می‌کند. نحوه ارائه امنیت ابری، بستگی به ارائه دهنده خدمات ابر یا راه حل‌های امنیت ابری دارد. هرچند که بهتر است پیاده‌سازی فرایند امنیت ابری، مسئولیتی مشترک بین تجار و ارائه دهنده‌ی خدمات باشد. تهدیدات امنیتی همواره در حال تکامل و پیچیده تر شدن می‌باشند و رایانش ابری به عنوان یک محیط پیش فرض همیشه در خطر می‌باشد. به همین دلیل، انتخاب ارائه دهنده‌ی خدمات ابری، بسیار حایز اهمیت می‌باشد تا بتواند بهترین سطح امنیت را به همراه زیرساخت‌های سفرashi شده، تامین نماید. یک رویکرد امکان سنجی خوب در زمینه تامین امنیت فضای ابری، یک راه‌حل مقیاس‌پذیر و قابل اندازه‌گیری ارائه می‌دهد که تهدیدات را پیش از رسیدن به مرکز داده شناسایی کرده و به رفع نگرانی‌های امنیتی کمک می‌کند. معماری امنیت ابری فقط در صورتی کاراست که پیاده‌سازی‌های دفاعی صحیح وجود داشته باشد. یک معماری امنیت ابری کارا باید مسائل امنیتی در سطح مدیریتی را شناسایی کند. مدیریت امنیت مسائل کنترل‌های امنیتی را نشان می‌دهد. این کنترل‌ها برای محافظت از هر نوع وضعی در سیستم و کاهش اثر یک حمله قرار داده شده‌اند. اگرچه که بسیاری از انواع کنترل، پشت معماری امنیتی محاسبات ابری وجود دارد، آن‌ها می‌توانند در دسته‌های زیر قرار گیرند [۲۰-۱۸]:

کنترل‌های بازدارنده: این کنترل‌ها به منظور جلوگیری از هر نوع حمله عمدی در یک سیستم محاسبات ابری تنظیم شده‌است. این کنترل‌ها، باعث کاهش آسیب‌پذیری واقعی یک سیستم نمی‌شوند. کنترل‌های پیش‌گیرنده: این کنترل‌ها به کمک مدیریت آسیب‌پذیری‌ها سبب افزایش قدرت سیستم می‌شوند. کنترل پیش‌گیرنده، از آسیب‌پذیری‌های سیستم محافظت خواهد کرد، اگر یک حمله اتفاق

نتیجه گیری

امروزه سازمان های بیشتری به مزایای انتقال سیستم هایشان به فضای ابری پی برده اند. محاسبات ابری این امکان را به سازمان ها می دهد که هزینه های خود را کاهش داده و از سیستم هایی استفاده کنند که به آن ها برتری رقابتی دهد. سازمان ها می بایست به امنیت محاسبات ابری خود اطمینان داشته باشند و مطمئن باشند که تمامی داده ها، سیستم ها و برنامه ها در مقابل سرقت، نشت و حذف داده ها محافظت می گردند. به دلیل تمرکز داده ها و منابع امنیتی بیشتر و پیچیده تر امنیت افزایش می یابد، اما نگرانیها به دلیل از دست دادن کنترل روی داده های حساس همچنان پابرجاست. امنیت در رایانش ابری اغلب بیشتر یا برابر با سیستمهای سنتی میباشد، زیرا ارائه دهندگان رایانش ابری به منابع اختصاصی امنیتی دسترسی دارند که بیشتر مشتریان از عهده خرید این منابع بر نمی آیند. این مقاله برخی از سیستم های رایانش ابری بنیادین را معرفی می کند و مسئله امکان سنجی امنیتی رایانش ابری و ریسکهای موجود و استراتژی مربوط به آن را بعنوان چالشها، فرصت ها و چشم اندازهای این حوزه با توجه به ایده ها و مشخصه های رایانش ابری مورد تجزیه و تحلیل قرار می دهد.

منابع

- system. *Front. Artif. Intell. Appl.* 295, 96–106 (2017)
- [9] Jambhekar, N.D., Misra, S., Dhawale, C.A.: Cloud computing security with collaborating encryption. *Indian J. Sci. Technol.* 9(21), 1–7 (2016)
- [10] Kaur, P. D., & Chana, I. (2014). Cloud-based intelligent system for delivering health care as a service. *Computer Methods and Programs in Biomedicine*, 113(1), 346–359.
- [11] Mora, N., Grossi, F., Russo, D., Barsocchi, P., Hu, R., Brunschweiler, T., Ciampolini, P., et al. (2019). IoT-based home monitoring: supporting practitioners' assessment by behavioral analysis. *Sensors*, 19(14), 3238.
- [12] Seth, B., Dalal, S., & Kumar, R. (2019). Securing bioinformatics cloud for big data: budding buzzword or a glance of the future. In *Recent advances in computational intelligence* (pp. 121–147). Springer.
- [13] Sahoo, P. K., Mohapatra, S. K., & Wu, S. L. (2018). SLA based healthcare big data analysis and computing in a cloud network. *Journal of Parallel and Distributed Computing*, 119, 121–135.
- [14] Chen, S. W., Chiang, D. L., Liu, C. H., Chen, T. S., Lai, F., Wang, H., & Wei, W. (2016). Confidentiality protection of digital health records in cloud computing. *Journal of Medical Systems*, 40(5), 124.
- [15] Mizani, M. A. (2017). Cloud-based computing. In *Key advances in clinical informatics* (pp. 239–255). Academic Press.
- [16] Kunal, S., Saha, A., & Amin, R. (2019). An overview of cloud-fog computing: Architectures, applications with security challenges. *Security and Privacy*, 2(4), e72.
- [17] Yi, S., Li, C., & Li, Q. (2015, June). A survey of fog computing: Concepts, applications, and issues. In *Proceedings of the 2015 Workshop on Mobile Big Data* (pp. 37–42).
- [18] Puthal, D., Obaidat, M. S., Nanda, P., Prasad, M., Mohanty, S. P., & Zomaya, A. Y. (2018). Secure and sustainable load balancing of edge data centers in fog computing. *IEEE Communications Magazine*, 56(5), 60–65.
- [19] Abbasi, M.A., Memon, Z.A., Durrani, N.M., Haider, W., Laeeq, K., Mallah, G.A.: A multi-layer trust-based middleware framework for handling interoperability issues in heterogeneous IoTs. *Clust. Comput.* 1–28 (2021)
- [20] Raman, A., Joglekar, S., Cristofaro, E.D., Sastry, N., Tyson, G.: Challenges in the decentralised web: the mastodon case. In: *Proceedings of the Internet Measurement Conference, IMC'19*, page 217–229, New York, NY, USA. Association for Computing Machinery. ISBN 9781-450369480. <https://doi.org/10.1145/3355369.3355572> (2019)
- [21]onoscenti, M., Vetrò, A., Martin, J.C.D.: Peer to peer for privacy and decentralization in the internet of things. In: *2017 IEEE/ACM 39th International Conference on Software Engineering Engineering Companion (ICSE-C)*, pp. 288–290 (2017)
- [1] Bayramusta, M., & Nasir, V. A. (2016). A fad or future of IT? A comprehensive literature review on cloud computing research. *International Journal of Information Management*, 36(4), 635–644.
- [2] Senyo, P. K., Addae, E., & Boateng, R. (2018). Cloud computing research: A review of research themes, frameworks, methods, and future research directions. *International Journal of Information Management*, 38(1), 128–139.
- [3] Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management*, 43, 146–158.
- [4] Usak, M., Kubiato, M., Shabbir, M. S., Viktorovna Dudnik, O., Jermisittiparsert, K., & Rajabion, L. (2020). Health care service delivery based on the Internet of Things: A systematic and comprehensive study. *International Journal of Communication Systems*, 33(2), e4179.
- [5] Zhou, J.: Analysis of Cloud Computing Security Problem. In: *APSEC 2013 Cloud Workshop*; Sydney, Australia (2013)
- [6] Ibrahim, B.: Auditing Cloud Computing: a Security and Privacy Guide, vol. 21 (2014)
- [7] Paul, P.: Security and cloud computing: identity management infrastructure for collaborative enterprises. In: *11th IEEE, Piscataway, New Jersey, United States*, pp. 26–29 (2013)
- [8] Odun-Ayo, I., Misra, S., Omogbe, N., Onibere, E., Bulama, Y., Damasevicius, R.: Cloud-based security-driven human resources management

