Assessing and Ranking Cloud Computing Security Risks Based On a Hybrid Approach Based On Pairwise Comparisons

Mehdi Soltanifar*
PhD in Applied Mathematics; Assistant Professor;
Islamic Azad University; Semnan Branch; Semnan, Iran;
Email: Soltanifar@khayam.ut.ac.ir

Seyed Mohammad Zargar
PhD in Management; Assistant Professor; Islamic Azad University;
Semnan Branch; Semnan, Iran Email: zargar@semnaniau.ac.ir

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Vol. 37 | No. 1 | pp. 27-58
Autumn 2021

Received: 23, Oct. 2020 **Accepted: 14, Mar. 2021**

Abstract: Today, despite many benefits of cloud computing technology, including cost savings, agility, increased flexibility and scalability the issue of information security is the main obstacle to the tendency of organizations towards cloud computing. In addition to infrastructure issues and political factors in Iran, there are many security risks in cloud computing technology. Therefore, the purpose of this study is to extract and rank these security risks. In this regard, by studying the theoretical foundations related to the research topic, these factors are extracted and categorized according to the opinion of experts, and then by designing questionnaires of different pairwise comparisons, collecting comments and combining different weighting methods based on pairwise comparisons by Copeland aggregation method, security risks were ranked. In this ranking, data privacy risk was the first priority of cloud computing security risks.

Keywords: Security, Cloud Computing, Multi Attribute Decision Making, Pairwise Comparisons, Copeland Method

ارزیابی و رتبه‌بندی ریسک‌های امنیتی رایانش ابری بر اساس یک رویکرد ترکیبی مبتنی بر مقایسه‌های زوجی

مهدی سلطانی‌فر
دکتری ریاضی کاربردی- تحقیق در عملیات؛ استادیار؛ دانشگاه آزاد اسلامی؛ واحد سمنان؛ سمنان، ایران؛ پدیدآور رابط soltanifar@khayam.ut.ac.ir

سید محمد زرگر
دکتری مدیریت صنعتی، مدیریت سیستم‌ها؛ استادیار؛ دانشگاه آزاد اسلامی؛ واحد سمنان؛ سمنان، ایران؛ m.zargar@semnaniau.ac.ir

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

دریافت: ۱۳۹۹/۰۸/۰۲ **پذیرش:** ۱۳۹۹/۱۲/۲۴ مقاله برای اصلاح به مدت ۱۳ روز نزد پدیدآوران بوده است.

نشریهٔ علمی | رتبهٔ بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، ISC، و SCOPUS
jipm.irandoc.ac.ir
دورهٔ ۳۷ | شمارهٔ ۱ | ص‌ص ۲۷-۵۸
پاییز ۱۴۰۰

چکیده: امروزه، با وجود مزایای بسیار فناوری رایانش ابری از جمله ایجاد صرفه‌جویی اقتصادی، چابکی، افزایش انعطاف‌پذیری و مقیاس‌پذیری، مسئلهٔ امنیت اطلاعات مانع اصلی گرایش سازمان‌ها به سمت رایانش ابری است. افزون بر مسائل مربوط به زیرساخت و عوامل سیاسی موجود در ایران، ریسک‌های امنیتی زیادی در فناوری رایانش ابری وجود دارد. هدف پژوهش حاضر، استخراج و رتبه‌بندی این ریسک‌های امنیتی است. در این راستا با مطالعهٔ مبانی نظری مرتبط با موضوع پژوهش، این ریسک‌ها استخراج و با توجه به نظر خبرگان دسته‌بندی شد. پرسشنامه‌های مقایسه‌ها زوجی مختلف بر اساس عوامل استخراج‌شده طراحی و نظرات خبرگان جمع‌آوری شد. سپس، با تلفیق روش‌های مختلف وزن‌دهی بر پایهٔ مقایسه‌ها زوجی و به کمک روش ادغامی «کپ‌لند»، ریسک‌های امنیتی رتبه‌بندی گردید. بر اساس نتایج این رتبه‌بندی، ریسک محرمانگی داده، احراز هویت، و موقعیت داده به‌ترتیب در رتبهٔ اول تا سوم قرار گرفتند و رتبهٔ سایر ریسک‌ها نیز مشخص شد.

کلیدواژه‌ها: امنیت، رایانش ابری، تصمیم‌گیری چند شاخصه، مقایسه‌ها زوجی، کپ‌لند

۱. مقدمه

امروزه، رایانش ابری در جوامع علمی و صنعتی توجه بسیاری به خود جلب کرده است. در مطالعهٔ انجام شده توسط «گارتنر» رایانش ابری، بین ده فناوری برتر جهان، رتبهٔ اول را به خود اختصاص داده است (Hashizume et al. 2013 به نقل از Gartner 2011).

رایانش ابری یکی از نوآوری‌های چشمگیر در عرصهٔ فناوری اطلاعات است. توانایی بالقوهٔ این فناوری در افزایش کارایی و صرفه‌جویی در هزینه‌ها باعث جذب و استقبال از به‌کارگیری آن به سازمان‌ها شده است. رایانش ابری در نحوهٔ تأمین منابع فعالیت‌های رایانشی سازمان تغییر اساسی ایجاد کرده و ارائهٔ انواع مختلف خدمات رایانشی از طریق اینترنت را دربرمی‌گیرد (Abdlrazaq & Varol 2021).

رایانش ابری فناوری مهمی است که امروزه برنامه‌های زیادی در بستر آن در حال اجراست. بر اساس مشاهدات، پیش‌بینی می‌شود که در سال‌های نه‌چندان دور استفاده از پردازش محلی مقرون‌به‌صرفه نبوده و رایانش ابری فراگیر خواهد شد. هرچند فراگیرشدن رایانش ابری مشکلات خاص خود را پدید می‌آورد، اما تدبیر دولت‌ها و سازمان‌ها منجر به اتخاذ رویکرد مناسب در استفادهٔ اثربخش از این فناوری خواهد شد (زرگر و شهریاری ۱۳۹۷).

رایانش ابری امکان اشتراک منابع، ذخیره‌سازی، دسترسی به شبکه، برنامه‌ها و نرم‌افزارها را از طریق اینترنت فراهم می‌کند. کاربران ابر می‌توانند منابع متعدد را بر اساس نیازهای خود اجاره کرده و فقط برای خدماتی که استفاده می‌کنند، هزینه پرداخت کنند (Kazim & Zhu 2015). رایانش ابری یک فناوری پیشرفتهٔ جدید است که برای کسب‌وکارها و سازمان‌های دولتی کوچک و متوسط، مزایای بسیاری فراهم کرده و بدین‌ترتیب، موجب کاهش پیچیدگی تنظیمات اصلی سیستم عامل‌های رایانه‌ای و کاهش هزینه می‌گردد (Khalil, Khreishah & Azeem 2014). ابرها مزایای زیادی از جمله صرفه‌جویی اقتصادی، تسهیل سازوکارهای برون‌سپاری، اشتراک منابع، دسترسی به منابع در هر زمان و هر مکان، انعطاف‌پذیری مقیاس بر اساس تقاضا و انعطاف‌پذیری خدمات دارند. ابرها به‌دلیل داشتن کمترین جزئیات فنی مانند ارتقای نرم‌افزار، مجوز و تعمیر و نگهداری درگیری کاربر را به حداقل می‌رسانند (Tripathi & Mishra 2011).

اگرچه به‌کارگیری فناوری رایانش ابری دارای مزیت‌های فراوانی است، با وجود

این، موانع قابل توجهی نیز بر سر راه استفاده از آن وجود دارد. یکی از مهم‌ترین موانع پیش روی این فناوری، مسائل مرتبط با امنیت، انطباق با مقررات داده‌های ابری، حفظ حریم خصوصی و مسائل حقوقی و قانونی است (Hashizume et al. 2013; Khalil, Khreishah & Azeem 2014; Kazim & Zhu 2015). با وجود اینکه رایانش ابری با فراهم‌ساختن امکان اشتراک منابع ارزشمند در میان چندین کاربر، مشکل محدودیت منابع را حل کرده و هزینهٔ خدمات را کاهش می‌دهد، اما قابلیت اطمینان و عملکرد منابع مستلزم داشتن بستر مناسب در برابر تهدیدات امنیتی است (Subramanian & Jeyaraj 2018).

ظهور فناوری رایانش ابری منجر به شکل‌گیری راه‌های جدید در اطلاعات و مسائل مربوط به حریم خصوصی داده‌های کاربران شده است، زیرا داده‌ها روی ابر ذخیره و منتقل می‌شوند و همین موضوع تهدیدی برای کاربران رایانش ابری بوده و موجب ایجاد نگرانی‌های بسیار جدی در مورد امنیت داده می‌شود (Abbas, Maennel & Assar 2017). اشتراک داده بین سازمان‌های مختلف، به‌عنوان اصلی‌ترین مزیت فناوری رایاناش ابری، خطراتی مانند ایجاد امکان سوء استفاده از داده‌ها را به همراه دارد. این در حالی است که اولویت اصلی هر سازمانی حفاظت از اطلاعات و داده‌های شخصی و سازمانی است (Tadapaneni 2020).

از آنجا که رایانش ابری یک مدل محاسباتی کمابیش جدید است، عدم اطمینان بسیاری در مورد اینکه چگونه امنیت در همهٔ سطوح (مانند شبکه، برنامه، داده) می‌تواند به‌دست آید و همچنین دربارهٔ نحوهٔ امنیت برنامه‌ها وجود دارد (Rosado et al. 2012). نگرانی‌های امنیتی به حوزه‌های پرخطر مانند ذخیره‌سازی خارجی داده، وابستگی به اینترنت عمومی، عدم کنترل و ادغام با امنیت داخلی مربوط است (Rittinghouse & Ransome 2009).

محاسبات ابری را می‌توان با توجه به ویژگی‌های آن طبقه‌بندی کرد. رایانش ابری سه نوع است: ابرهای خصوصی، ابرهای عمومی و ابرهای ترکیبی. در ابرهای خصوصی شرکت با یک مرکز اطلاعات خاص خودش سروکار دارد یا منابع تنها به یک یا چند سازمان محدود اختصاص می‌یابد. بنابراین، زیرساخت در این ابرها به‌طور کامل تحت کنترل و مدیریت است. تعریف رابطهٔ بین مشتریان و تأمین‌کنندگان و کشف خطرات امنیتی در ابرهای خصوصی بسیار آسان‌تر است. در ابر عمومی، شرکت‌ها، دولت‌ها یا مؤسسات از ابرهای عمومی استفاده می‌کنند. از این رو، حفاظت از داده و اطلاعات و دفاع از حملات

مختلف دشوارتر خواهد بود. ابرهای ترکیبی یک ابر خصوصی را فراهم می‌کنند که می‌توانند به بیش از یک سرویس خارجی متصل شود. با این حال، اطلاعات و برنامه‌ها به هم پیوسته و به‌طور متمرکز اداره می‌شوند. فرایند امنیتی یک ابر ترکیبی قابل اعتمادتر از یک ابر عمومی است (AlMendah & Alzahrani 2021).

با توجه به آنچه بیان شد، امنیت رایانش ابری مسئلهٔ بسیار مهمی است که استفاده از این فناوری برتر را با مشکل مواجه خواهد کرد. از این رو، شناخت خطرهای امنیت رایانش ابری از اهمیت زیادی برخوردار است. در مقالهٔ حاضر با بررسی پژوهش‌های پیشین عوامل خطرآفرین در بخش امنیتی رایانش ابری استخراج شده، این عوامل با استفاده از نظر خبرگان و اساتید با تجربه دسته‌بندی و سرانجام رتبه‌بندی شده است. سپس، وزن‌دهی خطرهای امنیتی با به‌کارگیری جدیدترین روش‌های رتبه‌بندی، بر پایهٔ مقایسه‌ها زوجی و با استفاده از نظرات خبرگان و بر مبنای تمامی روش‌های ذکر شده ارائه خواهد شد. در انتها، نتایج روش‌های مختلف با استفاده از روش ادغامی «کپلند»[1] تلفیق و رتبه‌بندی نهایی ارائه خواهد شد. همچنین در پایان، بحث دربارهٔ نتایج به‌دست‌آمده و نتیجه‌گیری کلی بیان می‌گردد.

۲. پیشینهٔ نظری و تجربی پژوهش

«مؤسسهٔ ملی استانداردها و فناوری آمریکا»، رایانش ابری را این‌گونه تعریف می‌کند: رایانش ابری نوعی فناوری است که دسترسی آسان و مبتنی بر تقاضا را از طریق شبکه برای به اشتراک گذاشتن منابع محاسباتی قابل تنظیم (مثل شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و خدمات) فراهم می‌کند. این دسترسی می‌تواند با حداقل تلاش مدیریتی و تعامل ارائه‌دهندهٔ خدمات به‌سرعت فراهم شود (Mell & Grance 2018). رایانش ابری یک برنامهٔ کاربردی نرم‌افزاری است که به‌جای آنکه روی کامپیوتر محلی یک کاربر خاص نصب شود، به‌صورت آنلاین وجود دارد و از طریق اینترنت در دسترس کاربران مختلف قرار می‌گیرد. کاربران بدون نیاز به سخت‌افزاری که این نرم‌افزارها روی آن نصب باشد، فقط با اتصال به اینترنت پُرسرعت می‌توانند به این برنامه‌ها دسترسی داشته باشند (Behrend et al. 2011). برنامهٔ رایانش ابری دارای

1. Copeland

چهار مدل اصلی استقرار و سه مدل ارائهٔ خدمات است. مدل‌های استقرار عبارت‌اند از: ۱) ابر خصوصی: یک بستر ابری که به یک سازمان خاص اختصاص داده شده است، ۲) ابر عمومی: یک بستر ابری که در دسترس عموم کاربران برای ثبت نام و استفاده از زیرساخت موجود است. ابرهای عمومی آسیب‌پذیرترین مدل استقرار هستند، زیرا برای عموم کاربران از جمله کاربران مخرب در دسترس هستند (Almorsy, Grundy & Muller 2016)، ۳) ابر گروهی: ابر گروهی مشابه ابر خصوصی است، با این تفاوت که منابع ابر بین اعضای یک گروه و یا چندین سازمان خصوصی با اشتراکات داده‌ای،استقرار می‌یابد. همچنین، ابر گروهی می‌تواند توسط شخص سومی اجرا شود (صدرالساداتی و کارگر ۱۳۹۲)، و ۴) ابر ترکیبی: یک ابر خصوصی است که می‌تواند برای استفاده از منابع در ابرهای عمومی گسترش یابد.

سه مدل ارائهٔ خدمات رایانش ابری عبارت‌اند از: ۱) زیرساخت به‌عنوان یک خدمت: در این مدل فراهم‌کنندگان سرویس‌های ابر، فضای ذخیره‌سازی، شبکه و ماشین‌های مجازی اینترنت‌محور را به کاربران ارائه می‌دهند، ۲) بستر به‌عنوان یک خدمت: هنگامی که فراهم‌کنندگان سرویس‌های ابری به مشتریان، سیستم‌عامل، ابزار و دیگر خدمات کسب‌وکار را ارائه می‌دهند تا آن‌ها را قادر سازند برنامه‌های کاربردی خود را توسعه دهند و مدیریت کنند؛ بدون اینکه هیچ سیستم‌عامل یا ابزار پشتیبانی را در کامپیوترهای شخصی خود نصب کرده باشند، و ۳) نرم‌افزار به‌عنوان یک خدمت: در این مدل فراهم‌کنندگان خدمات ابری بدون هیچ اجباری برای نصب برنامه‌های کاربردی روی رایانهٔ مشتری، برنامه‌های موجود در ساختار ابری را به کاربر نهایی ارائه می‌دهند (Almorsy, Grundy & Muller 2016). هر مدل ارائهٔ خدمات به‌نوعی خاص پیاده‌سازی می‌شود که توسعهٔ مدل امنیتی استاندارد برای همهٔ مدل‌های ارائهٔ خدمات را پیچیده می‌سازد. همچنین، این مدل‌های ارائهٔ خدمات ممکن است در یک بستر ابری همگام شوند و منجر به پیچیدگی بیشتر فرایند مدیریت امنیت شوند (همان). سازمان‌هایی که با استفاده از رایانش ابری، داده‌های بزرگ را جابه‌جا می‌کنند، همواره با خطر از بین رفتن امنیت، اعتماد و حفظ حریم خصوصی مواجه بوده‌اند (Chang, Kuo & Ramachandran 2016). با اینکه رایانش ابری موجب صرفه‌جویی در هزینه و زمان خواهد شد، اما در نهایت، اعتماد به رایانش ابری از هر چیزی مهم‌تر است؛ زیرا دارایی واقعی هر سازمان داده‌هایی است که به‌منظور استفاده از خدمات در ابر به اشتراک می‌گذارند. مسائل عمده در محاسبات ابر شامل امنیت

منابع، مدیریت منابع و نظارت بر منابع است. در حال حاضر، قوانین و مقررات استاندارد و کنترل استاندارد برای اعمال در ابر وجود ندارد. تکنیک‌های جدید متعددی در ابر برای امنیت طراحی و اجرا شده‌اند. با این حال، این تکنیک‌ها به‌دلیل پویایی محیط ابر، امنیت کامل را تأمین نمی‌کنند (Sun et al. 2014). امنیت و حریم خصوصی داده‌ها یکی از مهم‌ترین نگرانی‌های فناوری رایانش ابری است. ارائه‌دهندگان خدمات ابری باید حفاظت از مطالب را در برابر بدافزارهای مختلف بیمه کنند. بدین منظور، سیاست‌ها و سازوکارهای متفاوتی وجود دارد (Tadapaneni 2020). امنیت رایانش ابری، ترکیبی از محرمانه‌بودن، پیشگیری از افشای اطلاعات، یکپارچگی، پیشگیری از تغییر غیرمجاز اطلاعات، در دسترس بودن و جلوگیری از حذف غیرمجاز اطلاعات است (Sun et al. 2014; Avi˘zienis et al. 2004). به بیان دیگر، امنیت اطلاعات بدین معناست که اطمینان داشته باشیم تنها کاربران مجاز (محرمانگی)، به اطلاعات کامل و دقیق (جامعیت) در هنگام نیاز (دسترس‌پذیری) دسترسی دارند. امنیت اطلاعات دربرگیرندهٔ امنیت سامانه‌های فناوری اطلاعات و همچنین فرایندهای اطلاعاتی است که در تعامل با سامانه‌های فناوری اطلاعات هستند (نقیان فشارکی، طباطبایی و تمتاجی ۱۳۹۳). از سوی دیگر، مفاهیم جدیدی همچون چنداجاره‌ای[1]، اشتراک منابع و برون‌سپاری که در ارتباط با رایانش مطرح شده‌اند، خطرهای جدیدی را از لحاظ امنیتی ایجاد می‌کنند (Khalil, Khreishah and Azeem 2014). در ادامه، قصد داریم به تشریح خطرهای امنیتی رایانش ابری بپردازیم.

موقعیت داده: یکی از مسائل مهم پیش روی سازمان‌ها در استفاده از رایانش ابری، موقعیت مکانی داده‌هاست. یکی از ویژگی‌های خدمات رایانش ابری عدم اطلاع دقیق سازمان یا خدمت‌گیرنده از محل ذخیرهٔ داده‌ها و نحوهٔ دسترسی به آن‌هاست. بنابراین، اطمینان از تضمین کافی برای امنیت داده دشوار است. ممیزی‌های خارجی و صدور گواهینامه‌های امنیتی می‌تواند تا حدی این مسئله را حل کند، اما این نمی‌تواند یک راه حل قطعی باشد. هنگامی که اطلاعات از یک مرز ملی عبور کند، تضمین حفاظت از آن در قوانین و مقررات خارجی بسیار دشوار خواهد بود (Xiao & Xiao 2013).

دسترس‌پذیری: دسترس‌پذیری به این معناست که یک سازمان مجموعه‌ای کامل از منابع محاسباتی را برای همیشه در دسترس و قابل استفاده داشته باشد. عدم دسترسی به منابع

1. multitenancy

می‌توانـد کامـل یـا جزئـی و موقـت یـا دائمـی باشـد. عواملـی چـون قطـع بـرق و بلایـای طبیعـی می‌تواننـد از تهدیـدات دسـترس‌پذیری باشـند. در واقـع، می‌تـوان گفـت کـه دسـترس‌پذیری در ایـن معنـا، دسترسـی همیشـگی کاربـر مجـاز بـه داده‌هاسـت. یکـی از چالش‌هـای دسـترس‌پذیری، نیـاز همیشـگی بـه اینترنـت بـرای دسترسـی بـه اطلاعـات ابـری اسـت و دسـترس‌پذیری اینترنـت در همه‌جـا امکان‌پذیـر نیسـت (Biedermann & Katzenbeisser 2013).

چنداجـاره‌ای: ایـن مفهـوم بـه اشـتراک‌گذاری دسـتگاه‌های فیزیکـی و منابـع مجـازی میـان چنـد کاربـر مسـتقل (متعلـق بـه یـک سـازمان یـا سـازمان‌های مختلـف) اشـاره دارد (Gholami & Laure 2015).

کنتـرل دسترسـی: یکـی دیگـر از نقص‌هـای امنیتـی رایانـش ابـری از دسـت دادن کنتـرل داده‌هایـی اسـت کـه در مسـیر رفت‌وبرگشـت از سـازمان بـه تأمین‌کننـدهٔ خدمـات قـرار می‌گیرنـد. بنابرایـن، کاربـران کنتـرل کاملـی روی داده‌هـای خـود ندارنـد، و ایـن امـر موجـب می‌شـود کـه ارائه‌دهنـدگان خدمـات ابـری امـکان انجـام تغییـرات در اطلاعـات را داشـته باشـند. افـزون بـر ایـن، به‌دلیـل اینکـه اطلاعـات از مرکـز داده‌هـای مختلـف پشـتیبانی می‌شـود، کاربـران هنگامـی کـه اطلاعاتـی را حـذف می‌کننـد، نمی‌تواننـد مطمئـن باشـند کـه ایـن اطلاعـات به‌طـور کامـل از همه‌جـا حـذف شـده اسـت (همـان).

یکپارچگـی: ریسـک یکپارچگـی یعنـی یکپارچه‌نبـودن سیسـتم‌های فرسـتنده و گیرنـدهٔ داده‌هـا منجـر بـه دخـل و تصـرف تصادفـی یـا تعدیـل عامدانـه در داده‌هـا شـود. در ایـن خصـوص تکنیک‌هـای بسـیاری بـرای جلوگیـری از عـدم یکپارچگـی ماننـد امضـای دیجیتـال و احـراز هویـت وجـود دارد (Nishad et al. 2016).

محرمانگـی: محرمانگـی بدیـن معناسـت کـه داده‌هـا یـا اطلاعـات نبایـد به شـخص سـوم افشـا شـود (Kandukuri, Paturi & Rakshit 2009). بـر پایـهٔ سـازوکار محرمانـه بـودن، افـزون بـر اینکـه بقـای همیشـگی داده‌هـا تضمیـن می‌شـود، حفاظـت و نگهـداری از آن‌هـا در برابـر کاربـران غیرمجـاز نیـز فراهـم می‌شـود (Nishad et al. 2016).

بـرای حفـظ محرمانه‌بـودن از تکنیک‌هـای بسـیاری اسـتفاده می‌شـود. تکنیک‌هـای رمزگـذاری محبوب‌تریـن گزینـه بـرای امنیـت ابـر هسـتند. نقـض محرمانگـی داده و اطلاعـات بـه ایـن معناسـت کـه شـخص سـوم (هکـر) بتوانـد از داده‌هـای دیگـران بـرای منافـع شـخصی خـود اسـتفاده کنـد (Gellman 2009).

احراز هویت: یکی از جنبه‌های کلیدی امنیت رایانش ابری، احراز هویت است. تأیید هویت نشان می‌دهد که سیستم اعتباردهنده یا فرستنده قابل اطمینان است. تأیید هویت تضمین می‌کند که کاربر دقیقاً همان کسی است که ادعا می‌کند. یکی از راه‌های تأیید هویت استفاده از کلمهٔ عبور است. اما کلمهٔ عبور به‌طور کامل امن نیست؛ به همین دلیل، تکنیک‌های جدیدتری برای احراز هویت استفاده می‌شود (Kandukuri, Paturi and Rakshit 2009؛ Nishad et al. 2016).

رابط‌های ناامن: برنامهٔ کاربردی رابط برنامه، مجموعه‌ای از پروتکل‌ها و استانداردهاست که ارتباط بین برنامه‌های کاربردی نرم‌افزار را از طریق اینترنت تعریف می‌کند. رابط‌های ابر در تمام سطوح سرویس، زیرساخت، بستر و نرم‌افزار برای ارتباط با سرویس‌های دیگر استفاده می‌شود. امنیت سرویس‌های مختلف ابری بستگی به امنیت رابط‌ها دارد. ضعف رابط‌ها می‌تواند به مسائل امنیتی زیادی در ابر منجر شود. ارائه‌دهندگان ابر به‌طور معمول، رابط‌های خود را به شخص سومی که خدمات را به مشتریان می‌رساند، ارائه می‌کنند. رابط‌های ضعیف می‌توانند به دسترسی شخص سوم به کلیدهای امنیتی و اطلاعات حیاتی در ابر منجر شوند. با دسترسی به کلیدهای امنیتی، داده‌های رمزدارشدهٔ مشتری در ابر می‌تواند خوانده شود که به از دست دادن یکپارچگی داده‌ها، محرمانه‌بودن و دسترسی به آن منجر می‌شود. افزون بر این، احراز هویت و اصول کنترل دسترسی نیز می‌تواند از طریق برنامه‌های ناامن نقض شوند (Kazim & Zhu 2015).

حملات انکار سرویس[1]: به‌طور کلی، حملات انکار سرویس مهم‌ترین حملات در رایانش ابری است. در این نوع حمله، نفوذکننده حجم زیادی از منابع سرویس‌دهنده را مصرف می‌کند تا مانع از دسترسی کاربران به منابع رایانه‌ای، شبکه‌ای و اطلاعاتی شود (Redd & Bouzefrane 2014). حملات انکار سرویس برای جلوگیری از دسترسی کاربران غیرمجاز به شبکهٔ ابر، ذخیره‌سازی داده‌ها و سایر سرویس‌ها انجام می‌شود. حملات انکار سرویس در ۵ سال گذشته افزایش یافته است و ۸۱ درصد مشتریان، آن را تهدید مهمی در رایانش ابری می‌دانند (Kazim & Zhu 2015).

استانداردهای ابری: هرچه مقررات و استانداردهای رایانش ابری دقیق‌تر و مناسب‌تر باشد،

1. denial of service attacks

رغبت سازمان‌ها برای استفاده از آن بیشتر خواهد بود (Rashmi Rai, Sahoo & Mehfuz 2013). نبودِ استانداردهای کاربردی، داده‌های ذخیره‌شده در ابر را نیز تهدید می‌کند. استانداردهای معماری ارائه‌شده توسط ارائه‌دهندگان مختلف خدمات رایانش ابری به‌طور معمول ناسازگار است. این ناسازگاری مانع ایجاد چارچوب امنیتی استاندارد برای همهٔ ارائه‌دهندگان خدمات رایانش ابری می‌شود (Pearson 2012).

قابلیت حمل: هر ارائه‌دهندهٔ سرویس در ابر، قوانین خاصی برای تعامل با مشتریان خود دارد. مشتری بر اساس این قوانین، داده‌ها و برنامه‌های خود را نزد ارائه‌دهنده ذخیره می‌کند. از آنجا که همهٔ سازمان‌های ارائه‌دهندهٔ سرویس از یک استاندارد مشترک تبعیت نمی‌کنند، امکان مهاجرت مشتریان از یک ارائه‌دهنده به ارائه‌دهندهٔ دیگر در ابر امکان‌پذیر نیست (سلطان باغشاهی و همکاران ۱۳۹۱).

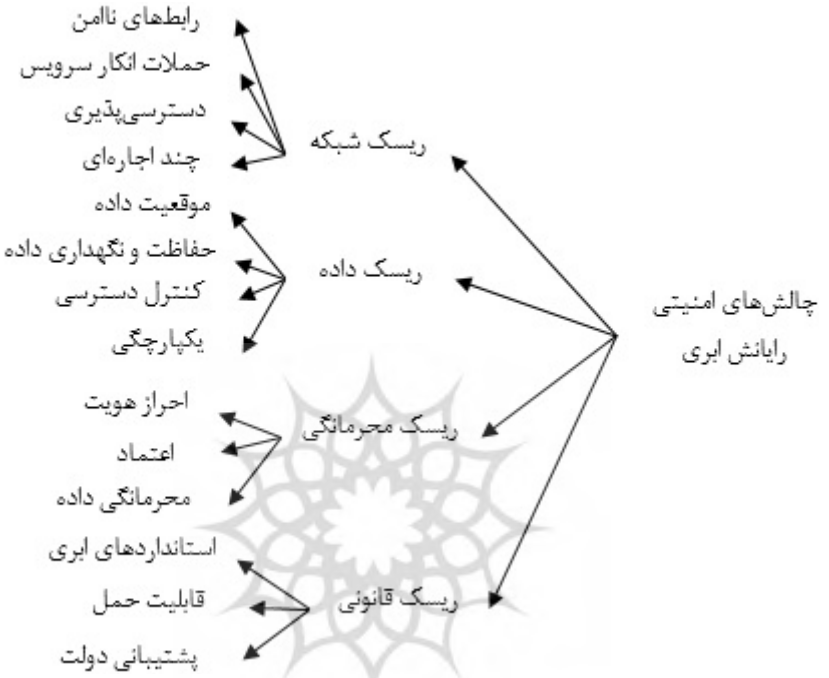
اعتماد: اعتماد به معنای تضمین این است که سرویس ابری از ابزار مکفی برای قابلیت رؤیت پروسه‌ها، کنترل‌های امنیتی و حفظ حریم خصوصی که توسط به‌وجودآورندهٔ ابر در طی زمان به‌کار گرفته می‌شود، برخوردار است (سلیمی ۱۳۹۸).

نگهداری و حفاظت از داده: این به معنای میزان کارآمدی سیستم رایانش ابری برای حفاظت و نگهداری از داده‌ها، به‌ویژه داده‌های بزرگ است (سلیمی ۱۳۹۸).

عدم پشتیبانی دولت: هنگامی که اطلاعات از مرز بومی عبور می‌کند، حفاظت از آن تحت قوانین و آئین‌نامه‌های خارجی به‌شدت مشکل‌ساز می‌شود. محدودیت ارتباطات میان سیستم‌های رایانه‌ای موجود در مرزهای ملی،که به‌منظور طبقه‌بندی داده‌های حساس و نیز حفاظت از داده‌های موجود قرار داده شده‌اند، باعث ایجاد قوانین و آئین‌نامه‌های امنیتی ملی و منطقه‌ای شده است. نگرانی اصلی این است که آیا این قوانین در حوزهٔ قضایی محل گردآوری داده‌ها اجرا می‌شود و آیا درخواست این قوانین بعد از انتقال داده‌ها ادامه می‌یابد یا نه (لطفی مرزناکی، حاجی‌باقری و محمدکاظم ۱۳۹۱). وجود قوانین و مقررات دولتی می‌تواند سازمان‌ها و کسب‌وکارها را به استفاده از فناوری رایانش ابری تشویق کند. برای مثال، قوانین ملی در کشور پرتغال (و اتحادیهٔ اروپا) مأموریت خاصی برای حفاظت از اطلاعات سازمان دارند (Amini 2014). دولت‌هایی که تمایل دارند رایانش ابری در سازمان‌ها پیاده‌سازی شود، ضمن حمایت از این فناوری، باید استانداردهای مرتبط با آن را نیز تدوین کنند. همچنین با توجه به اینکه رایانش ابری فراتر از مرزها گسترش یافته

است، روابط سیاسی دولت‌ها باید از شرایط مطلوبی برخوردار باشد (Avram et al. 2014).

پس از استخراج ریسک‌های امنیتی رایانش ابری از طریق مطالعهٔ پژوهش‌های پیشین و با نظر خبرگان حوزهٔ پژوهش، این عوامل دسته‌بندی شدند (شکل ۱).



شکل ۱. دسته‌بندی ریسک‌های امنیتی رایانش ابری

در پژوهشی که توسط «ولوی» و همکاران انجام شد، یک الگوی راهبردی برای مهاجرت سازمان‌های دفاعی به محیط رایانش ابری ارائه شد. در این پژوهش عواملی چون کارکرد، امنیت اطلاعات، حریم خصوصی داده‌ها، نظارت، دسترس‌پذیری، قابلیت حمل و یکپارچگی به‌عنوان ملاحظات امنیتی رایانش ابری در حوزهٔ دفاعی معرفی گردید (ولوی، موحدی‌صفت و کوشالشاه ۱۳۹۶). «سلطان باغشاهی و همکاران» کنترل دسترسی، وقفه در سرویس‌دهی، قابلیت حمل، چنداجاره‌ای، انتقال اطلاعات، رابط‌های ناامن و رابط مدیریت دسترسی از راه دور را به‌عنوان ریسک‌های امنیتی رایانش ابری معرفی کردند (۱۳۹۱). در پژوهش دیگری که توسط «یعقوبی، جعفری و شکوهی» انجام گرفته، ریسک‌های رایانش ابری در سازمان‌های دولتی، به ریسک‌های محسوس و نامحسوس تقسیم‌بندی

شده است. عواملی چون دسترس‌پذیری، جامعیت داده، زیرساخت، فروشنده و پشتیبانی تحقیقاتی در بخش ریسک‌های محسوس و عوامل تداوم خدمات، محرمانگی داده، مکانیزم ذخیره‌سازی، مکان داده و حفاظت از داده در بخش ریسک‌های نامحسوس قرار گرفتند (۱۳۹۴). به عقیدهٔ «تبریزچی و کوچکی رفسنجانی» برای دستیابی به امنیت گستردهٔ ابر، داده‌ها و زیرساخت‌های ابری باید در برابر حملات شناخته‌شده و ناشناخته در تمام اجزای ابر بررسی شوند. آن‌ها در پژوهشی مسائل و مشکلاتی را که رایانش ابری با آن دست‌وپنجه نرم می‌کند و خطرات و تهدیدات رایانش ابری (دستکاری، کلاهبرداری، افشای اطلاعات، انکار و اجتناب از خدمت) و حملات رایانش ابری را مورد بررسی قرار داده‌اند (Tabrizchi & Kuchaki Rafsanjani 2020). «تاداپاننی»، تکنیک‌ها و ریسک‌های امنیت داده‌ها و چگونگی محافظت از ابر را بررسی کرده است. به عقیدهٔ وی با اینکه ارائه‌دهندگان خدمات رایانش ابری، امنیت اطلاعات را هدف قرار داده‌اند و روزبه‌روز میزان امنیت رایانش ابری را افزایش می‌دهند، اما هکرها راه‌های نفوذ به اطلاعات را همچنان به‌دست خواهند آورد. به همین دلیل لازم است که محافظت از ابر با تکنیک‌های خاصی انجام شود (Tadapaneni 2020). «علی» و همکاران در پژوهش خود به ارزیابی خطرات امنیت اطلاعات در فضای ابری در کشور استرالیا پرداخته‌اند. طبق نتایج این مطالعه، استفاده از خدمات ابری در دولت استرالیا به‌دلیل نگرانی‌های امنیت داده، محدود شده است. در این مقاله نویسندگان عوامل مهم مرتبط با الزامات امنیت اطلاعات فناوری رایانش ابری را در دولت استرالیا بررسی، شناسایی و در نهایت، مدلی با ۴ مولفهٔ امنیت داده، ارزیابی ریسک، الزامات قانونی و انطباقی و الزامات تکنیکی و تجاری به‌منظور ایجاد دیدگاه متعادل دربارهٔ امنیت ابر برای دولت‌ها ارائه دادند. این مدل به دولت‌ها کمک می‌کند که با یکدیگر در بسترهای ابری کار کرده و الزامات امنیتی یکسانی را برای استفاده از خدمات ابری رعایت کنند (Ali et al. 2020). «روپرا و اومامو» یک چارچوب هشت‌مرحله‌ای ارزیابی امنیت اطلاعات در فضای رایانش ابری برای شرکت‌های کوچک و متوسط را ارائه داد (Rupra & Omamo 2020). مهم‌ترین ویژگی این چارچوب امنیتی توسعه‌یافته ایجاد مکانیزمی است که از طریق آن شرکت‌های کوچک و متوسط می‌توانند همراه با درک سطح امنیتی فعلی و تعریف وضعیت مطلوب در بستر ابری فعالیت داشته باشند. «وی‌پاتل، بویی و پاوار» در پژوهشی به بررسی جزئیات در خصوص خطرات امنیتی، حملات احتمالی و فنون پیشگیری از آن در استفاده از رایانش ابری پرداختند. بر پایهٔ نتایج به‌دست‌آمده، با وجود اینکه بسیاری از شرکت‌ها و مشاغل

در حال انتقال داده‌های خود از طریق ابر هستند، اما نگرانی‌های مربوط به امنیت داده همچنان پابرجاست. در این مطالعه، امنیت داده بزرگ‌ترین مانع پذیرش رایانش ابری معرفی شده است و نویسندگان سعی کرده‌اند یک معماری مفهومی از رایانش ابری ارائه دهند که در آن معیارهای اساسی ایمنی، خطرات امنیتی و حملات محتمل در به‌کارگیری رایانش ابری و راه‌های کاهش این حملات در نظر گرفته شود (V. Patel, Bhoi & Pawar 2020). مهم‌ترین تهدیداتی که «کازیم و ژو» در مطالعهٔ خود ارائه کردند، عبارت‌اند از: تهدید داده‌ها، شامل نقض داده‌ها و یا از دست دادن داده‌ها؛ تهدیدات شبکه، از جمله ربودن حساب یا سرویس و یا انکار سرویس؛ و تهدیدات خاص محیط ابری از جمله رابط‌های ناامن (Kazim & Zhu 2015). همچنین، «المرسی، گراندی و موللر» در پژوهش خود به بررسی مسائل امنیتی رایانش ابری پرداختند. آن‌ها ریسک‌های امنیتی موجود را تجزیه و تحلیل کرده و آن‌ها را با توجه به معماری، مدل ارائهٔ خدمات، ویژگی‌های ابری و مسائل مربوط به ذی‌نفعان سرویس‌های ابری گروه‌بندی کردند (Almorsy, Grundy & Muller 2016).

از مرور پیشینه‌ها می‌توان چنین نتیجه گرفت که اغلب پژوهش‌ها با استفاده از روش‌های کیفی مانند مرور نظام‌مند ادبیات پژوهش و یا روش‌های مبتنی بر جمع‌آوری داده از خبرگان، به شناسایی ریسک‌های رایانش ابری پرداخته‌اند (جدول ۱). لازم به ذکر است که در این پژوهش‌ها ارزیابی و رتبه‌بندی ریسک‌ها مورد توجه محققان قرار نگرفته است. در ادامه، روشی برای این منظور ارائه خواهد شد.

جدول ۱. مطالعات صورت‌گرفته در خصوص امنیت رایانش ابری

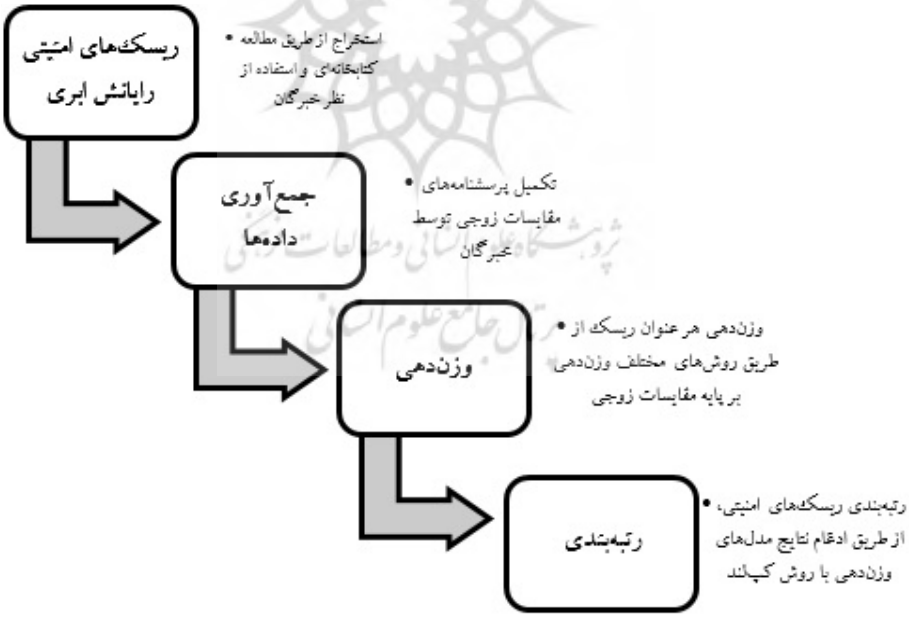
کنترل دسترسی	ولوی، موحدی‌صفت و باقری کوشالشاه (۱۳۹۶)؛ Catteddu (2010); Gholami & Laure (2015); Hashizume et al. (2013)
دسترس‌پذیری	نقیان فشارکی، طباطبایی و تمتاجی (۱۳۹۳)؛ Sun et al. (2014); Khalil, Khreishah & Azeem (2014); Paquette, Jaeger & Wilson (2010); ولوی، موحدی‌صفت و باقری کوشالشاه (۱۳۹۶)؛ Nishad et al. (2016)
یکپارچگی	Nishad et al. (2016) Sun et al. (2014);
نگهداری و حفاظت داده	Alcaraz Calero et al. (2010); Godfrey & Zulkernine (2014); Grobauer, Walloschek & Stocker (2011); Hong et al. (2015); Brender & Markov (2013)
اعتماد	صدرالساداتی و کارگر (۱۳۹۲)؛ ولوی، موحدی‌صفت و باقری کوشالشاه (۱۳۹۶)؛ Gholami & Laure (2015); Paquette, Jaeger & Wilson (2010); He et al. (2014); Hydara et al. (2015); Avram (2014)

محرمانگی	Nishad et al. (2016); Sun et al. (2014); Paquette, Jaeger & Wilson (2010); Sultan (2011)
احراز هویت	Nishad et al. (2016)؛ صدرالساداتی و کارگر (۱۳۹۲)، ولوی، موحدی‌صفت و باقری کوشالشاه (۱۳۹۶)
استانداردهای ابری	صدرالساداتی و کارگر (۱۳۹۲)؛ Godfrey & Zulkernine (2014)؛ Khalil, Khreishah & Azeem (2014); Doherty, Carcary & Conwa (2012); Gonzalez et al. (2012); Rashmi Rai, Sahoo & Mehfuz (2013)
قابلیت حمل	سلطان باغشاهی و همکاران (۱۳۹۱)، ولوی، موحدی‌صفت و باقری کوشالشاه (۱۳۹۶)
پشتیبانی دولت	Amini et al. (2014); Safari et al. (2015) Nishad et al. (2016);
موقعیت داده	Sen (2013); Islam, Manivannan & Zeadally (2016); Brender & Markov (2013); Wayne (2011)
رابط‌های نا امن	Khalil, Khreishah & Azeem (2014); Kazim & Zhu (2015)؛ سلطان باغشاهی و همکاران (۱۳۹۱)
حملات انکار سرویس	Jensen et al. (2009); Kazim & Zhu (2015); Reddy & Bouzefrane (2014)
چنداجاره‌ای	Catteddu (2010); Gholami & Laure (2015)؛ صدرالساداتی و کارگر (۱۳۹۲)

۳. روش پژوهش

پژوهش حاضر از لحاظ هدف، کاربردی و از حیث گردآوری داده، پیمایشی است. برای دستیابی به رتبه‌بندی نهایی ریسک‌های امنیتی رایانش ابری، نیاز به گروهی متشکل از خبرگان است. روش انتخاب‌شده برای رتبه‌بندی ریسک‌ها در واقع، ادغام نتایج روش‌های مبتنی بر مقایسه‌های زوجی است. روش‌های مبتنی بر مقایسه‌های زوجی نیازمند تعامل با خبرگان در چندین مرحله هستند. از این رو، گزینش مناسب خبرگان از اهمیت ویژه‌ای برخوردار است. خبرگان شرکت‌کننده در پژوهش حاضر، تعدادی از کارشناسان فناوری اطلاعات با حداقل ۱۰ سال سابقهٔ کاری و تحصیلات کارشناسی ارشد و بالاتر و مسلط به حوزهٔ رایانش ابری هستند. در روش‌های تعاملی، بر پایهٔ میزان تعامل با خبرگان، بین ۵ تا ۲۰ نفر انتخاب می‌شوند. در پژوهش پیش رو به‌دلیل تعامل مکرر در روش‌های مختلف مبتنی بر مقایسه‌های زوجی، این تعداد ۷ نفر تعیین شد. لازم به ذکر است که در روش‌های تعاملی به‌دلیل نیاز به حفظ انگیزهٔ خبرگان در ارائهٔ اطلاعات و تعاملات مورد نیاز پژوهش، استفاده از تعداد مناسب افراد خبرهٔ گزینش شده و مسلط به موضوع از اهمیت بسیاری برخوردار است. در این پژوهش با استفاده از بررسی ادبیات پژوهش، ریسک‌های امنیتی رایانش ابری استخراج و ترکیب نهایی آن‌ها پس از

تعامل با خبرگان، به روش دلفی استخراج و طبقه‌بندی شد. سپس، داده‌های پژوهش با به‌کارگیری پرسشنامه‌های مقایسه‌های زوجی و در تعامل با تیم خبرگان جمع‌آوری شد. در پژوهش‌های آماری مبتنی بر پرسشنامه لازم است دو ویژگی بسیار مهم پرسشنامه یعنی قابلیت اطمینان یا پایایی و اعتبار درونی یا روایی، با بهره‌گیری از روش‌های مختلف مورد سنجش قرار گیرد. پایایی، سازگاری پرسشنامه‌ها را اندازه‌گیری کرده، روایی میزان مطابقت نتایج حاصل از پرسشنامه‌ها با دنیای واقعی را تعیین می‌کند. در پرسشنامه‌های مربوط به روش‌های تصمیم‌گیری، به‌ویژه در پرسشنامه‌های مربوط به روش‌های مبتنی بر مقایسه‌های زوجی، که به‌صورت ماتریس‌های مقایسه‌های زوجی در اختیار خبرگان قرار می‌گیرند، پایایی پرسشنامه پس از نظرسنجی از اساتید دانشگاه، و روایی آن پس از محاسبهٔ نرخ ناسازگاری هر ماتریس تعیین می‌شود. در مطالعهٔ حاضر، پایایی پرسشنامه‌ها توسط اساتید مسلط به روش‌ها و موضوع مورد پژوهش تأیید شده است. همچنین، بر اساس معیارهای تعریف نرخ ناسازگاری در هر روش، سازگاری داده‌ها ارزیابی و تأیید شد. شکل ۲، مراحل مختلف پژوهش را نشان می‌دهد.



شکل ۲. مراحل مختلف پژوهش

٤. روش تحلیل سلسله‌مراتبی گروهی (GAHP)

روش GAHP[1] مانند آنچه در مغز انسان انجام می‌شود، به تحلیل مسائل می‌پردازد. این روش تصمیم‌گیرندگان را قادر می‌سازد که اثرات متقابل و همزمان بسیاری از وضعیت‌های پیچیده و نامعین را تعیین کنند. این فرایند تصمیم‌گیرندگان را یاری می‌کند تا اولویت را بر اساس اهداف، دانش و تجربهٔ خود تنظیم نمایند؛ به‌گونه‌ای که احساسات و قضاوت‌های خود را در نظر گیرند. برای حل مسائل تصمیم‌گیری با استفاده از GAHP باید مسئله را به‌دقت و با همهٔ جزئیات تبیین کرده و جزئیات آن را به‌صورت سلسله‌مراتبی رسم کرد. الگوریتم روش GAHP به‌صورت زیر است:

مرحلهٔ ۱) ساختن نمودار سلسله‌مراتبی: در این گام ابتدا باید شاخص‌ها و گزینه‌های مسئله را تعیین کرد. در زمان تصمیم‌گیری گروهی، گروه می‌بایست روی یک سلسله‌مراتب به توافق برسد. این امر با برگزاری جلسات متعدد و فایق آمدن تدریجی بر جنبه‌های مختلف موضوع توسط گروه محقق خواهد شد.

مرحلهٔ ۲) تشکیل ماتریس مقایسه‌های زوجی: در این مرحله عناصر هر سطح نسبت به سایر عناصر مربوط به خود در سطح بالاتر به‌صورت زوجی مقایسه شده و ماتریس‌های مقایسه‌های زوجی تشکیل می‌شوند. جهت تعیین اهمیت و ترجیح در مقایسه‌های زوجی از طیف ۱ تا ۹ Saaty (2008) استفاده می‌شود. ترجیحات در این مرحله باید در شرط معکوسی و شرط همگنی صادق باشند؛ یعنی اولاً اگر ترجیح عنصر A به عنصر B، برابر n باشد، آنگاه ترجیح عنصر B به عنصر A برابر $\frac{1}{n}$ باشد و ثانیاً ترجیحات عناصر نسبت به هم صفر یا بی‌نهایت نباشد. تصمیم‌گیری گروهی یا از طریق اتفاق آرا صورت می‌گیرد، یا ماتریس مقایسهٔ زوجی گروهی از میانگین هندسی ماتریس‌های مقایسهٔ زوجی فردی ساخته می‌شود. در این پژوهش شیوهٔ دوم به‌کار گرفته شده است.

مرحلهٔ ۳) محاسبهٔ اوزان نسبی: در این مرحله با استفاده از روش‌های مختلف وزن‌دهی، وزن نسبی شاخص‌ها و گزینه‌ها نسبت به هر شاخص به‌دست می‌آید. روش‌های متفاوتی برای وزن‌دهی وجود دارد؛ از آن جمله می‌توان به روش مجموع سطری، مجموع ستونی، میانگین حسابی، میانگین هندسی، بردار ویژه، کمترین مربعات معمولی و کمترین مربعات لگاریتمی اشاره کرد.

1. group analitic hierarchy process

مرحلهٔ ۴) محاسبهٔ نرخ ناسازگاری ماتریس‌های مقایسهٔ زوجی و نرخ ناسازگاری سلسله‌مراتبی. در این مرحله از آنجا که ممکن است قضاوت خبرگان منجر به تشکیل یک ماتریس مقایسهٔ زوجی ناسازگار شود، این است که یک نرخ تجربی برای پذیرش ناسازگاری ماتریس‌های مقایسهٔ زوجی و ناسازگاری سلسله‌مراتبی پیشنهاد شده است. در صورت عدم پذیرش، نتایج جهت بازبینی به خبرگان برگشت داده می‌شود. الگوریتم محاسبهٔ نرخ ناسازگاری یک ماتریس مقایسهٔ زوجی (D) به‌صورت زیر است.

a) محاسبهٔ بردار مجموع وزنی (WSV)[1]: ماتریس مقایسهٔ زوجی (D) را در بردار وزن‌های نسبی ضرب کنید. بردار حاصل، بردار مجموع وزنی خواهد بود.

b) محاسبهٔ بردار سازگاری (CV)[2]: عناصر بردار مجموع وزنی را بر بردار وزن‌های نسبی تقسیم کنید. بردار حاصل، بردار سازگاری خواهد بود.

c) محاسبهٔ بزرگ‌ترین مقدار ویژهٔ ماتریس مقایسهٔ زوجی (λ_{max}): میانگین عناصر بردار سازگاری، برابر λ_{max} خواهد بود.

d) محاسبهٔ شاخص ناسازگاری *(II)*: اگر فرض کنیم ماتریس مقایسهٔ زوجی *(D)* مورد بررسی، یک ماتریس $m \times m$ باشد، آنگاه شاخص ناسازگاری برابر $\frac{\lambda_{max}-m}{m-1}$ خواهد بود.

e) محاسبهٔ نرخ ناسازگاری *(IR)*: نرخ ناسازگاری برابر $\frac{II}{IRI}$ خواهد بود که در آن *IRI*، شاخص ناسازگاری تصادفی است و مقدار آن از جدول ۲، استخراج می‌شود. این جدول بر پایهٔ شبیه‌سازی به‌دست آمده است.

به پیشنهاد «ساعتی» اگر نرخ ناسازگاری کوچکتر یا مساوی ۰/۱ باشد، نتایج مقایسه‌ها زوجی قابل پذیرش و در غیر اینصورت برای تجدید نظر به خبره(خبرگان) عودت داده می‌شود (Saaty 1990).

جدول ۲. شاخص ناسازگاری تصادفی

M	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
I.R.I.	۰	۰	۰/۵۸	۰/۹۰	۱/۱۲	۱/۲۴	۱/۳۲	۱/۴۱	۱/۴۵	۱/۴۵	۱/۵۱	۱/۵۲	۱/۵۶	۱/۵۷	۱/۵۹

1. weighted sum vector (WSV) 2. consistency vector (CV)

مرحلهٔ ۵) محاسبهٔ اوزان مطلق گزینه‌ها: وزن مطلق هر گزینه برابر مجموع حاصل‌ضرب وزن نسبی آن گزینه نسبت به هرشاخص، در وزن نسبی آن شاخص است.

روش GAHP در سال‌های اخیر به‌طور مکرر و در نسخه‌های مختلف مورد استفادهٔ پژوهشگران قرار گرفته است، اما به‌کارگیری آن به‌ویژه در نسخهٔ گروهی آن، گاه می‌تواند بسیار زمان‌بر باشد. افزایش عناصر هر سطح، تشکیل ماتریس‌های مقایسهٔ زوجی را بسیار دشوار می‌سازد. در این شرایط، معیارهای تصمیم‌گیری را به زیرمعیارهایی تقسیم می‌کنند؛ ولی این کار نیز در بسیاری موارد مشکل را حل نمی‌کند. همچنین، تشکیل ماتریس‌های مقایسهٔ زوجی و رسیدن به نرخ ناسازگاری قابل پذیرش می‌تواند در بسیاری موارد زمان‌بر و خارج از حوصلهٔ خبرگان باشد.

۵. روش بهترین-بدترین (BWM)

یکی از روش‌های وزن‌دهی به شاخص‌ها بر پایهٔ مقایسه‌ها زوجی، روش بهترین-بدترین[1] است که «رضایی» ارائه کرده (Rezaei 2015) و از سوی بسیاری از پژوهشگران مورد توجه قرار گرفته است (Badri Ahmadi, Kusi-Sarpong & Rezaei 2020; Delice & Can 2020; Kumara, Aswin & Gupta 2020; Liang, Brunelli & Rezaei 2020; Rezaei 2020). در این روش پس از تعیین بهترین-بدترین شاخص، مقایسهٔ زوجی سایر شاخص‌ها با این دو شاخص، مبنای ارائهٔ یک مدل برنامه‌ریزی خطی شده و در نهایت، وزن شاخص‌ها از حل این مدل برنامه‌ریزی خطی استخراج می‌شود. همچنین، در این روش فرمولی برای محاسبهٔ نرخ ناسازگاری به‌منظور بررسی اعتبار مقایسه‌ها در نظر گرفته شده است. الگوریتم این روش به‌صورت زیر است:

مرحلهٔ ۱) شاخص‌های تأثیرگذار بر هدف مسئله را با تعامل با تصمیم‌گیرنده مشخص کنید $(\boldsymbol{C_1, C_2, \cdots, C_m})$.

مرحلهٔ ۲) بهترین $(\boldsymbol{C_B})$ و بدترین $(\boldsymbol{C_W})$ شاخص را از میان شاخص‌های نهایی برپایهٔ نظر تصمیم‌گیرنده و نیز در نظر گرفتن شاخص‌ها و زیرشاخص‌ها معین کنید.

مرحلهٔ ۳) ترجیحات بهترین شاخص را نسبت به سایرشاخص‌ها بر پایهٔ طیف ۱ تا ۹ Saatty

1. Best-worst method (BWM)

(1980) پس از تعامل با تصمیم‌گیرنده، مشخص کنید $\left(a_{Bj}, j = 1, 2, \cdots, m\right)$.

مرحلهٔ ۴) ترجیحات سایر شاخص‌ها نسبت به بدترین شاخص را بر پایهٔ طیف ۱ تا ۹ Saaty (1980) پس از تعامل با تصمیم‌گیرنده، مشخص کنید $\left(a_{jW}, j = 1, 2, \cdots, m\right)$.

مرحلهٔ ۵) اوزان شاخص‌ها را از حل مدل برنامه‌ریزی خطی (۱) به‌دست آورید.

$$\min \xi^L$$

$$s.t. \left|w_B - a_{Bj} w_j\right| \le \xi^L, \quad j = 1, 2, \cdots m.$$

$$\left|w_j - a_{jW} w_W\right| \le \xi^L, \quad j = 1, 2, \cdots m. \qquad (1)$$

$$\sum_{j=1}^{m} w_j = 1$$

$$w_j \ge 0, \quad j = 1, 2, \cdots m.$$

مدل (۱) معروف به مدل خطی روش بهترین-بدترین است (Rezaei 2016). لازم به ذکر است که نسخه‌های غیرخطی، تصادفی و مضربی نیز با این روش ارائه شده است. اما در این مقاله نسخهٔ خطی که در فهم و اجرا ساده‌ترین نسخهٔ روش بهترین- بدترین است، انتخاب شده است. اگر $\left(w_1^*, w_2^*, \ldots, w_m^*\right)$ جواب بهینهٔ مدل (۱) و ξ^{L^*} مقدار بهینهٔ آن باشد، آنگاه اوزان شاخص‌ها برابر $\left(w_1^*, w_2^*, \ldots, w_m^*\right)$ و ξ^{L^*} به‌عنوان نرخ ناسازگاری سیستم در نظر گرفته خواهد شد. هرچه نرخ ناسازگاری به صفر نزدیک‌تر باشد، اطمینان به قضاوت‌های صورت‌گرفته از سوی خبرگان بیشتر خواهد بود.

٦. روش «لیل»

الگوریتم روش «لیل» به‌صورت زیر است (Leal 2020).

مرحلهٔ ۱) ساختن نمودار سلسله‌مراتبی.

مرحلهٔ ۲) تعیین بهترین عنصر هر سطح: در این مرحله عناصر هر سطح نسبت به سایر عناصر مربوط خود در سطح بالاتر مقایسه شده و بهترین آن‌ها تعیین می‌شود.

مرحلهٔ ۳) تعیین ترجیحات بهترین عنصر هر سطح: ترجیحات بهترین شاخص (بهترین گزینه نسبت به هر شاخص) را نسبت به سایرشاخص‌ها (گزینه‌ها در سطح مورد نظر) بر پایهٔ طیف ۱ تا ۹ Saaty (1980) پس از تعامل با تصمیم‌گیرنده مشخص کنید $\left(a_{Bj}, j = 1, 2, \cdots, m\right)$.

مرحلهٔ ۴) محاسبهٔ اوزان نسبی: در این مرحله وزن نسبی شاخص‌ها و گزینه‌ها نسبت به هر شاخص را از حل رابطهٔ (۲) به‌دست می‌آوریم.

$$w_j = \frac{1/a_{Bj}}{\sum_{k=1}^{m} 1/a_{Bk}} \qquad j = 1, 2, \cdots, m \qquad (2)$$

مرحلهٔ ۵) محاسبهٔ اوزان مطلق گزینه‌ها.

در این روش، اطلاعات اخذشده از خبره (یا خبرگان) به تعیین بهترین عنصر هر سطح و انجام مقایسه‌ها زوجی سایر عناصر با بهترین عنصر محدود می‌شود. بدین ترتیب، حجم اطلاعات اخذشده از خبره (یا خبرگان) در این روش بسیار کمتر از حجم اطلاعات اخذشده در روش GAHP است. در واقع، در این روش در هر سطح که دارای m عنصر است به‌جای $\frac{(m^2-m)}{2}$ قضاوت مورد نیاز روش GAHP و یا $2m-1$ قضاوت روش *BMW*، تنها $m-1$ قضاوت مورد نیاز است.

۷. روش تحلیل سلسله‌مراتبی رأی‌گیری

«لیو و های» با جایگزین نمودن یک مدل تحلیل پوششی داده‌ها (رجوع شود به Cook & Kress 1990) به‌جای فرایند تشکیل ماتریس‌های مقایسهٔ زوجی در روش GAHP، اوزان نسبی شاخص‌ها و گزینه‌ها نسبت به هر شاخص را محاسبه نموده و روش تحلیل سلسله‌مراتبی رأی‌گیری VAHP[1] را ارائه کردند (Liu & Hai 2005). «هادی-ونچه و نیازی-مطلق» فرایند بهبودیافتهٔ VAHP را برای انتخاب تأمین‌کننده (Hadi-Vencheh & Niazi-Motlagh 2011) و «سلطانی‌فر و حسین‌زاده لطفی» این روش را برای رتبه‌بندی واحدهای تصمیم‌گیری کارا در تحلیل پوششی داده‌ها به‌کار بردند (Soltanifar & Hosseinzadeh Lotfi 2011). در روش VAHP تنها اولویت شاخص‌ها و گزینه‌ها نسبت به هر شاخص و نیز توابع شدت تشخیص برای تعیین فاصلهٔ بین هر اولویت از خبرگان اخذ می‌شود. از آنجا که تعیین مناسب توابع شدت تشخیص موجود در این مدل تحلیل پوششی داده‌ها، در اطمینان به نتایج نهایی بسیار تأثیرگذار است، از این رو، تعیین این توابع از اهمیّت ویژه‌ای برخوردار است. «گرین، دول وکوک» برای حل مشکل تعیین توابع شدت تشخیص و بی‌نیازی مدل از کسب اطلاعات بیشتر از خبرگان، برای هر کاندیدا تعداد آرا را به‌صورت تجمعی در نظر گرفتند. آن‌ها

1. voting analitic hierarch process

فرض کردند که $\sum_{k=1}^{r} v_{kq}$ که v_{kq} تعداد آرای کاندیدای q در اولویت kام باشد (Green, Doyle & Cook 1996). استفاده از انباشتگی در تعداد آرا، وزن‌ها را به‌صورت ضعیف مرتب می‌کند. از این رو، نیازی به نوشتن قیود ناحیهٔ اطمینان در مدل نخواهد بود. مدل «کوک و کرس» با فرض اینکه بخواهیم m کاندید را رتبه‌بندی کنیم، به‌صورت مدل (۳) تبدیل می‌شود (Cook & Kress 1990).

$$Z_p = max \sum_{r=1}^{m} W_r V_{rp}$$

$$s.t.$$

$$\sum_{r=1}^{m} W_r V_{rj} \leq 1, \quad j = 1, 2, \dots, m. \qquad (3)$$

$$W_r \geq 0, \qquad r = 1, 2, \dots, m$$

که در آن $W_r = \sum_{k=r}^{m} W_k$ وزن جایگاه رأی‌گیری rام خواهد بود. همچنین، «پیشچولوف و همکاران» نیز با ارائهٔ فرایندی به حل همین مشکل پرداخت (Pishchulov et al. 2019). بدین ترتیب، تنها با اخذ اولویت شاخص‌ها و نیز اولویت گزینه‌ها نسبت به هر شاخص، اوزان مطلق، گزینه‌ها تعیین می‌شود. الگوریتم این روش به‌صورت زیر است:

مرحلهٔ ۱) ساختن نمودار سلسله‌مراتبی.

مرحلهٔ ۲) تعیین اولویت شاخص‌ها و اولویت گزینه‌ها نسبت به هر شاخص: در این مرحله عناصر هر سطح نسبت به سایر عناصر مربوط خود در سطح بالاتر مقایسه شده و اولویت آن‌ها تعیین می‌شود.

مرحلهٔ ۳) محاسبهٔ اوزان نسبی: در این مرحله پس از حل مدل (۳) و به‌دست آوردن جواب بهینهٔ این مدل در هر سطح، وزن نسبی شاخص‌ها و گزینه‌ها نسبت به هر شاخص را از رابطهٔ (۴) به‌دست می‌آوریم.

$$w_j = \frac{Z_j^*}{\sum_{k=1}^{m} Z_k^*} \quad j = 1, 2, \cdots, m \qquad (4)$$

مرحلهٔ ۴) محاسبهٔ اوزان مطلق گزینه‌ها.

در این روش به‌دلیل اخذ حداقل اطلاعات از خبرگان، نیاز به بررسی سازگاری اطلاعات اخذشده نیست.

۸. روش «مکبث»

روش «مکبث»[1] یکی از روش‌های تصمیم‌گیری چندمعیارهٔ جبرانی است که توسط «کوستا و ونسنیک» ارائه شد. الگوریتم روش «مکبث» به‌صورت زیر است (Bana e Costa and Vansnick 1999):

مرحلهٔ ۱) دو سطح مرجع یعنی خوب (Good) و خنثی (Neutral) را برای مسئله در نظر بگیرید (x_N, x_G).

مرحلهٔ ۲) عناصر هر سطح را بر پایهٔ طیف ۷تایی جدول ۳، به‌صورت زوجی مقایسه کنید (a_{ij}).

جدول ۳. طیف ۷تایی روش «مکبث»

مقیاس کیفی	بی‌تفاوتی بین گزینه‌ها	برتری در حد خیلی ضعیف	برتری در حد ضعیف	برتری در حد متوسط	برتری در حد قوی	برتری در حد خیلی قوی	برتری در حد به‌شدت قوی
مقیاس عددی	۰	۱	۲	۳	۴	۵	۶

مرحلهٔ ۳) اوزان «مکبث» را از طریق حل مسئلهٔ (۵) برای هر گزینه محاسبه کنید.

$$\boldsymbol{min}[v(x_G) - v(x_N)]$$

$$\boldsymbol{s.t.}$$

$$v(x_N) = 0 \ (\boldsymbol{arbitrary\ score})$$

$$v(x_i) - v(x_j) = 0 \quad i,j \in \{1,2,\dots,n;G,N\} \& \ a_{ij} = 1 \qquad (5)$$

$$v(x_i) - v(x_j) \geq v(x_k) - v(x_l) + a_{ij} - a_{kl} \ i,j,k,l \in \{1,2,\dots,n;G,N\} \& \ a_{ij} > a_{kl} \geq 1$$

اگر مسئلهٔ (۵) نشدنی باشد، قضاوت‌های صورت‌گرفته ناسازگار خواهند بود. برای حل مسائل با این روش می‌توان از نرم افزار «ام-مکبث»[2] استفاده نمود.

1. the measuring attractiveness by a categorical based evaluation technique (MACBETH)
2. M-MACBETH

رتبه‌بندی ریسک‌های امنیتی رایانش ابری با ادغام نتایج روش‌های AHP، BWM، Leal، VAHP، MACBETH و مقایسهٔ نتایج این روش‌ها

در این بخش، روش‌های مختلف وزن‌دهی بر پایهٔ مقایسه‌ها زوجی برای وزن‌دهی ریسک‌های امنیتی رایانش ابری به‌کار گرفته شده و در نهایت، این نتایج با روش «کپ‌لند» ادغام خواهند شد. در جدول ۴، اوزان نهایی ریسک‌های امنیتی رایانش ابری که توسط روش‌های مختلف وزن‌دهی بر پایهٔ مقایسه‌های زوجی به‌دست آمده، درج شده است. لازم به ذکر است که مقایسه‌های زوجی جمع‌آوری‌شده از خبرگان بر اساس معیارهای طراحی‌شده هر روش سازگار بوده و قابل پذیرش است.

جدول ٤. اوزان ریسک‌های امنیتی رایانش ابری با استفاده از روش‌های مختلف وزن‌دهی

ریسک‌های امنیتی رایانش ابری	روش AHP	روش BWM	روش Leal	روش VAHP	روش MACBETH
احراز هویت	۰/۱۷۷	۰/۱۲۹۴۴۳۱۷	۰/۱۲۳۴۴۶	۰/۰۸۶۳۷۹	۰/۲۰۴۹۹۹۳۸
اعتماد	۰/۰۳۴	۰/۰۵۹۷۴۳	۰/۰۷۰۵۴۱	۰/۰۷۹۷۳۴	۰/۰۳۴۱۵۰۶۲
محرمانگی داده	۰/۳۰۹	۰/۴۶۷۹۸۶۸۳	۰/۴۹۳۷۸۶	۰/۱۱۹۶۰۱	۰/۲۳۹۱۵
موقعیت داده	۰/۱۷۲	۰/۰۸۲۴۴۲۳۴	۰/۰۷۰۵۴۱	۰/۰۸۸۸۷۴	۰/۱۲۴۴۵۸۷
حفاظت و نگهداری داده	۰/۰۱۸	۰/۰۱۳۱۹۰۷۷	۰/۰۱۴۱۰۸	۰/۰۵۰۷۸۵	۰/۰۱۳۸۴۵۶۵
کنترل دسترسی	۰/۰۹۹	۰/۰۴۹۴۶۵۴	۰/۰۳۵۲۷	۰/۰۷۵۵۴۳	۰/۰۹۶۸۲۸۲۶
یکپارچگی	۰/۰۵۸	۰/۰۲۴۷۳۲۷	۰/۰۱۷۶۳۵	۰/۰۶۰۳۰۸	۰/۰۶۹۱۶۷۳۹
رابط‌های ناامن	۰/۰۰۸	۰/۰۱۸۵۸۷۵۲	۰/۰۱۲۳۳۷	۰/۰۶۱۴۶۷	۰/۰۳۱۶۱۵۰۲
حملات انکار سرویس	۰/۰۰۴	۰/۰۰۷۳۳۷۱۸	۰/۰۰۸۸۱۲	۰/۰۱۸۷۰۷	۰/۰۰۷۹۱۲۴۵
دسترسی‌پذیری	۰/۰۵۶	۰/۰۷۲۱۴۸۹۲	۰/۰۶۱۶۸۴	۰/۰۷۴۸۳	۰/۰۷۹۰۳۷۵۵
چنداجاره‌ای	۰/۰۲	۰/۰۲۳۲۳۴۴	۰/۰۱۵۴۲۱	۰/۰۶۹۴۸۵	۰/۰۵۵۳۳۴۹۸
استانداردهای ابری	۰/۰۲۸	۰/۰۳۶۰۲۴۸	۰/۰۵۳۹۴۳	۰/۰۸۶۸۷۳	۰/۰۲۵۳۷۳۵۵
قابلیت حمل	۰/۰۰۴	۰/۰۰۴۶۹۸۸۹	۰/۰۰۸۹۹۱	۰/۰۵۷۹۱۵	۰/۰۰۳۶۲۷۹
پشتیبانی دولت	۰/۰۱۳	۰/۰۱۰۹۶۴۰۷	۰/۰۱۳۴۸۶	۰/۰۶۹۴۹۸	۰/۰۱۴۴۹۸۵۵

حال، با توجه به وزن‌دهی‌های به‌دست آمده، روش «کپ‌لند» (مؤمنی ۱۳۹۵، ۷۲) که مبتنی بر قاعدهٔ اکثریت است، برای رتبه‌بندی نهایی به‌کار گرفته می‌شود. نتایج اجرای این روش در جدول ۵، آمده است. در هر خانه از جدول، M نشان‌دهندهٔ برتری گزینهٔ

سطری به ستونی و X نشان‌دهندهٔ عدم برتری گزینهٔ سطری به ستونی خواهد بود. مجموع تعداد Mها در هر سطر، برابر با تعداد بُردهای گزینهٔ متناظر آن سطر و مجموع تعداد M ها در هر ستون، برابر تعداد باخت‌های گزینهٔ متناظر با آن ستون خواهد بود. در نهایت، امتیاز «کپ‌لند» برای هر گزینه، از کم کردن تعداد باخت‌های متناظر با آن گزینه از تعداد بُردهایش حاصل می‌شود. در بخش بعد، تفسیر نتایج و نتیجه‌گیری ارائه خواهد شد.

جدول ۵. نتایج روش «کپ‌لند» برای رتبه‌بندی ریسک‌های امنیتی رایانش ابری

ریسکهای امنیتی رایانش ابری	احراز هویت (a)	اعتماد (b)	محرمانگی داده (c)	موقعیت داده (d)	حفاظت و نگهداری داده (e)	کنترل دسترسی (f)	یکپارچگی (g)	رابط‌های نامن (h)	حملات انکار سرویس (i)	دسترس‌پذیری (j)	چند اجاره‌ای (k)	استانداردهای ابری (l)	قابلیت حمل (m)	پشتیبانی دولت (n)	جمع بردها
a	-	M	X	M	M	M	M	M	M	M	M	M	M	M	۱۲
b	X	-	X	X	M	M	M	M	M	X	M	M	M	M	۹
c	M	M	-	M	M	M	M	M	M	M	M	M	M	M	۱۳
d	X	M	X	-	M	M	M	M	M	M	M	M	M	M	۱۱
e	X	X	X	X	-	X	X	M	M	X	X	X	M	M	۴
f	X	X	X	X	M	-	M	M	M	M	M	M	M	M	۹
g	X	X	X	X	M	X	-	M	M	X	M	X	M	M	۶
h	X	X	X	X	X	X	X	-	M	X	X	X	M	X	۲
i	X	X	X	X	X	X	X	X	-	X	X	X	X	X	۰
j	X	M	X	X	M	M	M	M	M	-	M	M	M	X	۹
k	X	X	X	X	M	X	X	M	M	X	-	X	M	M	۵
l	X	X	X	X	M	X	M	M	M	X	M	-	M	M	۷
m	X	X	X	X	X	X	X	X	X	X	X	X	-	X	۰
n	X	X	X	X	X	X	X	M	M	X	X	X	M	-	۳
باخت	۱	۴	۰	۲	۹	۴	۷	۱۱	۱۲	۴	۸	۶	۱۲	۱۰	–
امتیاز	۱۱	۵	۱۳	۹	-۵	۵	-۱	-۹	-۱۲	۵	-۳	۱	-۱۲	-۷	–
رتبه	۲	۴	۱	۳	۸	۴	۶	۱۰	۱۱	۴	۷	۵	۱۱	۹	–

۹. بحث و نتیجه‌گیری

امروزه، استفاده از رایانش ابری در سازمان‌ها رواج یافته است. این است که توجه به ریسک‌های امنیتی استفاده از فناوری نوظهور از اهمیت بالایی برخوردار است. در مقال، حاضر پس از مرور مبانی نظری و مطالعهٔ تحقیقات پیشین، ریسک‌های مرتبط با عناوینی مانند رابط‌های ناامن، حملات انکار سرویس، دسترسی، چنداجاره‌ای، موقعیت، حفاظت و نگهداری، کنترل دسترسی، یکپارچگی، احراز هویت، اعتماد، محرمانگی داده، استانداردهای ابری، قابلیت حمل، و پشتیبانی دولت شناسایی شدند. این عوامل در یک قالب سلسله‌مراتبی در چهار دستهٔ ریسک شبکه، ریسک داده، ریسک محرمانگی، ریسک قانونی دسته‌بندی شدند. در مرحلهٔ بعد روش‌های مختلف مبتنی بر مقایسه‌های زوجی مورد بررسی و مقایسه قرار گرفتند. روش‌هایی مانند AHP، BWM، Leal و VAHP که به‌ترتیب، از بیشترین تا کمترین نیاز به کسب اطلاعات از افراد خبره مرتب شده‌اند، و همچنین روش «مکبث» در این مقاله مورد بررسی و استفاده قرار گرفت. این روش در کسب اطلاعات از خبرگان شبیه روش AHP عمل می‌کند، با این تفاوت که طیف مورد استفاده در روش AHP، ۹تایی و در این روش ۷تایی است. این روش در اجرا شباهت زیادی به روش BWM دارد؛ چرا که با تعریف دو سطح مرجع و یک مسئلهٔ برنامه‌ریزی خطی امتیاز نهایی را تشخیص می‌دهد. جدول ۶، روش‌های استفاده‌شده در این مقاله را از لحاظ پیچیدگی زمانی و حجم محاسبات نشان می‌دهد.

جدول ٦. مقایسه روش‌های تصمیم‌گیری بر پایهٔ مقایسه‌های زوجی

روش	مسئلهٔ برنامه‌ریزی خطی مورد نیاز برای حل	تعداد مقایسه‌های زوجی	محاسبات اضافی اوزان نسبی	ناسازگاری در قضاوت‌ها
AHP	*0*	$\frac{(n^2-n)}{2}$	بله	زیاد
BWM	*1*	*2n-2*	خیر	متوسط
Leal	*0*	*n-1*	خیر	خیر
VAHP	*n*	*0*	خیر	خیر
MACBETH	*1*	$\frac{(n^2-n)}{2}$	خیر	بسیار زیاد

در روش‌های Leal و VAHP که مسئله ناسازگاری در قضاوت‌ها مطرح نیست، نتایج

در اولین تعامل با خبرگان به‌دست می‌آید. بنابراین، روش‌ها با تکرار متناهی مرحله به جواب می‌رسند و از این لحاظ روش‌های کاملی هستند؛ اما در روش‌های AHP، BWM و «مکبث» که امکان ناسازگاری در قضاوت‌ها وجود دارد، ممکن است مراحل رسیدن به نتایج تا اخذ نتایج سازگار از خبرگان طولانی شود. بنابراین، کامل بودن این روش‌ها بستگی به دقت خبرگان در ارائهٔ اطلاعات لازم در قضاوت‌ها دارد. بحث بهینگی در کلیهٔ روش‌های مورد استفاده در این مقاله و در اغلب روش‌های MADM[1]، به‌دلیل وابسته بودن نتایج به قضاوت‌های خبرگان مطرح نیست، بلکه بحث مطلوبیت مطرح است. تمامی این روش‌ها جواب‌های مطلوبی را بر پایهٔ قضاوت خبرگان ارائه می‌کنند و نتیجه نهایی در روش «کپ‌لند» پس از ادغام به‌دست خواهد آمد. در خصوص پیچیدگی فضایی نیز لازم به ذکر است که در روش «لیل» محاسبات در یک مرحله و با اشغال کمترین میزان از حافظه صورت می‌گیرد. برای اجرای روش VAHP نیز از آنجا که الگوریتم‌های کارایی برای حل مسائل برنامه‌ریزی خطی وجود دارد، پیچیدگی فضایی برابر پیچیدگی فضایی الگوریتم‌های حل مسائل برنامه‌ریزی خطی مانند الگوریتم سیمپلکس خواهد بود. در سایر روش‌ها نیز اگر قضاوت‌ها سازگار باشند، پیچیدگی فضایی یا از پیچیدگی فضایی حل مسائل برنامه‌ریزی خطی ارائه‌شده در الگوریتم آن روش‌ها به‌دست می‌آید، یا برابر پیچیدگی فضایی مراحل ذکرشده در روش GAHP خواهد بود. اما اگر قضاوت‌ها ناسازگار باشند، از آنجا که قضاوت‌های ناسازگار نیاز به ذخیره در حافظهٔ دستگاه ندارند و به‌طور کامل توسط خبرگان بازبینی خواهند شد، پیچیدگی فضایی این روش‌ها نیز برابر پیچیدگی فضایی اجرای نتایج حاصل از قضاوت‌های سازگار است. در پژوهش حاضر، رتبه‌بندی نهایی ریسک‌ها با ادغام نتایج روش‌های مختلف تصمیم‌گیری بر پایهٔ مقایسه‌های زوجی، با استفاده از روش «کپ‌لند»، انجام شد. بر پایهٔ نتایج به‌دست‌آمده، ریسک محرمانگی داده، احراز هویت و موقعیت داده به‌ترتیب، در رتبهٔ اول تا سوم قرار گرفتند و رتبهٔ سایر ریسک‌ها نیز مشخص شد. بر این اساس، محرمانگی داده یکی از مهم‌ترین ریسک‌های رایانش ابری است. کاربران رایانش ابری در درجهٔ اول نگران این هستند که داده‌های حیاتی‌شان در دسترس افراد غیرمجاز قرار گیرد. در پژوهش‌های «یعقوبی، جعفری و شکوهی» (۱۳۹۳)؛ Khalil, Khreishah & Azeem (2014); Kazim & Zhu (2015)

1. multi-attribute decision making

و Nishad et al. (2016) نیز محرمانگی داده، مهم‌ترین ریسک رایانش ابری عنوان شده است. احراز هویت در این رتبه‌بندی در رتبهٔ دوم قرار گرفت. به‌عبارت دیگر، در صورتی که سیستم‌های رایانش ابری قادر به تشخیص کاربر مجاز نباشند، احتمال سوء استفاده از اطلاعات کاربر افزایش خواهد یافت. در پژوهش Nishad et al. (2016) نیز احراز هویت یکی از ریسک‌های مهم رایانش ابری معرفی شده است. موقعیت داده که در این پژوهش در رتبهٔ سوم قرار گرفت، موضوع مهمی برای سازمان‌هایی است که می‌خواهند بدانند داده‌ها و اطلاعات آن‌ها کجا ذخیره خواهد شد. به‌دلیل اینکه اطلاعاتی از مکان ذخیرهٔ داده در دسترس سازمان نیست و ارائه‌دهندگان خدمات ابری نمی‌توانند ضمانتی برای حفظ داده‌ها ارائه دهند، این وضعیت تبدیل به یک ریسک امنیتی برای سازمان‌ها شده است. «گارتنر» در دسته‌بندی که از ریسک‌های امنیتی رایانش ابری انجام داده، به موقعیت داده اشاره کرده است. اعتماد، دسترس‌پذیری و کنترل دسترسی در رتبهٔ چهارم ریسک‌های امنیتی رایانش ابری قرار گرفتند. حفاظت از داده‌ها به سطح مناسبی از کنترل دسترسی نیاز دارد. در صورت عدم کنترل کافی، خطر دسترسی ناخواسته به اطلاعات محرمانه توسط کاربران غیرمجاز وجود دارد. این امر می‌تواند منجر به دزدیده‌شدن یا آسیب به اطلاعات شود (Gartner 2011). کنترل دسترسی یکی از ریسک‌های امنیتی مهم رایانش ابری در تحقیقات Hashizume et al. (2013) و Gholami & Laure (2015) است. استاندارد ابری در رتبهٔ پنجم و یکپارچگی داده در این رتبه‌بندی در رتبهٔ ششم قرار گرفت. منظور از یکپارچگی این است که داده‌های اصلی موجود در سیستم رایانش ابری بدون کوچک‌ترین تغییری قابل دسترسی هستند. Nishad et al. (2016) و Sun et al. (2014) در پژوهش خود به این عامل به‌عنوان یکی از ریسک‌های امنیتی رایانش ابری اشاره کرده‌اند. مسئلهٔ کلیدی در این پژوهش شناختن ریسک‌های امنیتی رایانش ابری است تا کاربران این فناوری با شناخت کافی بتوانند از این ریسک‌ها دوری کنند. کاربران می‌توانند با انتخاب یک ارائه‌دهندهٔ خدمات مطمئن و با سابقه، ریسک‌های ناشی از حذف اطلاعات، آسیب اطلاعات، و دسترسی به اطلاعات توسط کاربران غیرمجاز را کاهش دهند. در صورت وجود استانداردها و قوانین دولتی مبنی بر نگهداری و حفاظت اطلاعات و رسیدگی به جرائم، مقابله با ریسک‌های امنیتی رایانش ابری آسان‌تر خواهد شد. در پژوهش حاضر، علاوه بر مطالعهٔ ریسک‌های امنیتی رایانش ابری، دسته‌بندی و رتبه‌بندی آن‌ها، روش‌های مختلف تصمیم‌گیری چندمعیاره بر پایهٔ مقایسه‌های زوجی نیز بررسی و تحلیل شد. از

این رو، اگر نظرات خبرگان بر اساس داده‌های کیفی و از طریق واژگان زبانی اخذ شود، می‌توان از نسخهٔ فازی روش‌های ذکر شده به‌عنوان پیشنهاد مطالعات آتی استفاده نمود و بدین‌ترتیب، از مزایای منطق فازی نیز بهره‌مند شد. از محدودیت‌های پژوهش حاضر می‌توان به جمع‌آوری داده‌ها با استفاده از پرسشنامهٔ مقایسه‌های زوجی توسط خبرگان اشاره کرد. این است که به پژوهشگران پیشنهاد می‌شود نتایج مطالعهٔ حاضر را با استفاده از روش‌های متکی بر داده‌های غیرنظری مورد آزمون قرار دهند.

فهرست منابع

زرگر، سید محمد، و زهرا شهریاری. ۱۳۹۷. ارائهٔ مدلی پویا برای پذیرش فناوری رایانش ابری با استفاده از روش دیماتل و رویکرد پویایی سیستم. *فصلنامه علمی-پژوهشی مدیریت فناوری اطلاعات* ۱۰ (۱): ۹۳-۱۱۶.

سلطان باغشاهی، سمیه، لیلا سلطان باغشاهی، احمد خادم‌زاده و سام جبه‌داری. ۱۳۹۱. تحلیل چالش‌های امنیتی و تأثیر آن بر رایانش ابری. اولین کارگاه ملی رایانش ابری ایران. تهران.

سلیمی، زهرا. ۱۳۹۸. بررسی و مقایسهٔ معمارهای امنیتی رایانش ابری در راستای ارائهٔ راهکارهایی جهت توسعهٔ سازمان‌های امنیتی. پژوهش‌های معاصر در علوم و تحقیقات ۱ (۸): ۱۸-۳۲.

صدرالساداتی، سید محسن، و محمدجواد کارگر. ۱۳۹۲. چالش‌های امنیتی در رایانش ابری و ارائهٔ راهکاری جهت بهبود امنیت آن در راستای توسعهٔ خدمات عمومی دولت الکترونیک. *هشتمین همایش بین‌المللی پیشرفت علم و فناوری*، مشهد، ایران.

لطفی مرزناکی، مونا، شادی حاجی‌باقری، و محبوبه محمدکاظم. ۱۳۹۱. بررسی خطرها، تهدیدها و آسیب‌پذیری‌ها در محاسبات ابری. *اولین کنفرانس دانشجویی پیشرفت‌های نوین مهندسی دانشگاه شریف. ایران.*

مؤمنی، منصور. ۱۳۹۵. *مباحث نوین تحقیق در عملیات*. تهران: مؤلف.

نقیان فشارکی، مهدی، سید غلامحسن طباطبایی، و مصطفی تمتاجی. ۱۳۹۳. ارائهٔ معماری مرجع امنیتی محیط رایانش ابر خصوصی سازمان. *فصلنامه علمی پژوهشی امنیت پژوهی* ۱۳ (۴۷): ۹۱-۱۱۳.

ولوی، محمدرضا، محمدرضا موحدی‌صفت، و ایمان باقری کوشالشاه. ۱۳۹۶. ارائهٔ الگوی راهبردی مهاجرت سازمان‌های دفاعی به محیط رایانش ابری. *فصلنامه مدیریت نظامی* ۱۷ (۶۵): ۱۰۶-۱۳۰.

یعقوبی نورمحمد، حمیدرضا جعفری، و جواد شکوهی. ۱۳۹۴. شناسایی و رتبه‌بندی عوامل ریسک رایانش ابری در سازمان‌های دولتی. *پژوهشنامهٔ پردازش و مدیریت اطلاعات* ۳۰ (۳) :۷۵۹-۷۸۴.

References

Abbas, H., O. Maennel, and S. Assar. 2017. Security and privacy issues in cloud computing. *Annals of Telecommunications* 72 (5-6): 233-235.

Abdlrazaq, A., and A. Varol. 2021. Cloud Computing's Impact on Enterprises. In Term of Security and Cost. *International Journal of Security* 12 (1): 1-14.

Alcaraz Calero, J. M., N. Edwards, J. Kirschnick, L. Wilcock, and M. Wray. 2010. Toward a multi-tenancy authorization system for cloud services. *IEEE Security & Privacy* 8 (6): 48–55.

Ali, O., A. Shrestha, A. Chatfield, and P. Murray. 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly* 37 (1): 1-20.

AlMendah, O., and S. Alzahrani. 2021. Cloud and edge computing security challenges, demands, known threats, and vulnerabilities. *Academic Journal of Research and Scientific Publishing* 2 (21): 156-175.

Almorsy, M., J. Grundy, and I. Muller. 2016. An analysis of the cloud computing security problem. In Proceedings ofthe APSEC 2010 Cloud Workshop, Sydney, Australia, 30 November 2010; pp. 1–6.

Amini, M., N. Safavi, R. Mirzaeyan Bahnamiri, M. Mirzaei Omran, and M. Amini. 2014. Development of an Instrument for Assessing the Impact of Environmental Context on Adoption of Cloud Computing for Small and Medium Enterprises. *Australian Journal of Basic and Applied Sciences* 8 (10): 129-135.

Avi˘zienis, A., J. Laprie, B. Randell, and C. Landwehr. 2004. Basic concepts and taxonomy of dependable and secure computing, *IEEE Transactions on Dependable and Secure Computing* 1 (1): 11-33.

Avram, M. G. 2014. Advantages and challenges of adopting cloud computing from an enterprise perspective. *Procedia Technology* 12: 529-534.

Badri Ahmadi, H., S. Kusi-Sarpong, and J. Rezaei. 2020. Assessing the social sustainability of supply chains using Best Worst Method, Resources. *Conservation & Recycling* 126: 99-106.

Bana e Costa, C. A. and J. C. Vansnick. 1994. MACBETH- an interactive path towards the construction of cardinal value functions, *International Transactions in Operational Research* 1: 489-500.

_____. 1999. The MACBETH Approach: Basic ideas, software, and an application. In: meskens n., roubens m. (eds) advances in decision analysis. *Mathematical Modelling: Theory and Applications* vol 4. Springer, Dordrecht. https://doi.org/10.1007/978-94-017-0647-6_9.

Behrend, T. S., E. N. Wiebe, J. E. London, and E. C. Johnson. 2011. Cloud computing adoption and usage in community colleges. *Behavior & Information Technology* 30 (2): 231-240.

Biedermann S., and S. Katzenbeisser. 2013. POSTER: event-based isolation of critical data in the cloud, in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp. 1383–1386. Berlin, Germany.

Brender, N., and I. Markov. 2013. Risk Perception And Risk Management In Cloud Computing: results from a case study of Swiss companies. *International journal of information management* 33 (5): 726-733.

Catteddu D. 2010. Cloud computing: benefits, risks and recommendations for information security, In Web Application Security, Ed. Berlin: Springer.

Chang, V., Y. Kuo, and M. Ramachandran. 2016. Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems* 57: 24-41.

Cook, W. D., and M. Kress. 1990. A data envelopment model for aggregating preference rankings. Management Science 36 (11): 1302–1310.

Delice, E. K., and G. F. Can. 2020. A new approach for ergonomic risk assessment integrating KEMIRA, best–worst and MCDM methods, Soft Computing, https://doi.org/10.1007/s00500-020-05143-9.

Doherty, E., M. Carcary, and G. Conwa. 2012. Risk management considerations in cloud computing adoption. Innovation Value Institute, Executive Briefing, Retrieved From: Eprints. Nuim. http://mural.maynoothuniversity.ie/4302/1/GC_Cloud_Computiong_Adoption.pdf , (accessed Dec. 16, 2020).

Gartner Inc Gartner identifies the Top 10 strategic technologies. 2011. Online. Available: http://www.gartner.com/it/page.jsp?id=1454221. (accessed July 15, 2020)

Gellman, R. 2009. Privacy in the clouds: Risks to privacy and confidentiality from cloud computing, The World Privacy Forum,. http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Re port.pdf (accessed Dec. 16, 2020)

Gholami, A., and E. Laure. 2015. Security and Privacy of Sensitive Data in cloud computing: a survey of recent developments. *Computer Science & Information Technology*. 131-150. DOI: 10.5121/csit.2015.51611

Godfrey, M., and M. Zulkernine. 2014. Preventing Cache-Based Side-Channel Attacks in a Cloud Environment. *IEEE Transactions on Cloud Computing* 2 (4): 395–408.

Gonzalez, N., M. Charles, R. Fernando, S. Marcos, C. Tereza, M. Näslund, M. Pourzandi. 2012. A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing* 1 (1): 1-18.

Green, R. H., J. R. Doyle, and W. D. Cook. 1996. Preference voting and project ranking using DEA and cross-evaluation. *European Journal of Operational Research* 90: 461-472.

Grobauer, B., V. Walloschek, and E. Stocker. 2011. Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy* 9 (2): 50–57.

Hadi-Vencheh, A., and M. Niazi-Motlagh.2011 . An improved voting analytic hierarchy process-data envelopment analysis methodology for suppliers selection, *International Journal of Computer Integrated Manufacturing* 24 (3): 189-197.

Hashizume, K., D. Rosado, E. B. Fernández-Medina, and E. Fernandez. 2013. An analysis of security issues for cloud computing. *Journal of Internet Services and Applications* 4 (5): 2-13.

He, H., R. Li, X. Dong, and Zh. Zhang. 2014. Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud. *IEEE Transactions on Cloud Computing* 2 (4): 471–484.

Hong, H., D. Chen, Ch. Huang, and Ch Kuan-Ta & Ch Hsu. 2015. Placing Virtual Machines to Optimize Cloud Gaming Experience. *IEEE Transactions on Cloud Computing* 3 (1): 42–53.

Hydara, I., A. Bakar, M. Sultan, H. Zulzalil, and N. Admodisastro. 2015. Current state of research on cross-site scripting (XSS) - A Systematic Literature Review. *Information & Software Technology* 58: 170–186.

Islam, T., D. Manivannan, and Sh. Zeadally. 2016. A classification and characterization of security threats in cloud computing. *International Journal of Next-Generation Computing* 7 (1): 1-17.

Jensen, M., J. Schwenk, N. Gruschka, andL. Iacono. 2009. On technical security issues in cloud computing, in IEEE ICCC, Bangalore, 2009, 109-116.

Kandukuri, B. R., R. V. Paturi, and A. Rakshit. 2009. Cloud Security Issues, IEEE International Conferenceon Services Computing, Bangalore, India, September21-25, 2009. In Proceedings of IEEE, SCC'2009.pp.517-520, 2009.

Kazim, M., and Sh. Y. Zhu. 2015. A survey on top security threats in cloud computing. *International Journal of Advanced Computer Science and Applications* 6 (3): 109-113.

Khalil, I., A. Khreishah, and M. Azeem. 2014. Cloud Computing Security: A Survey. *Computers* 3: 1-35.

Kumara, A., A. Aswin, and H. Gupta. 2020. Evaluating green performance of the airports using hybrid BWM and VIKOR methodology. *Tourism Management* 76:1-16. https://doi.org/10.1016/j.tourman.2019.06.016.

Leal, J. E. 2020. AHP-express: A simplified version of the analytical hierarchy process method. *MethodsX*: 7. https://doi.org/10.1016/j.mex.2019.11.021

Liang, F., M. Brunelli, and J. Rezaei. 2020. Consistency issues in the best worst method: Measurements and thresholds. *Omega* 96: https://doi.org/10.1016/j.omega.2019.102175

Liu, F., H., F., and H. Hai.2005 . The voting analytic hierarchy process method for selecting supplier. *International Journal of Production Economics* 97 (3): 308–317.

Mell P., T. Grance. 2018. SP 800-145, The NIST Definition of cloud computing | CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publi catio ns/detai l/sp/800-145/final (accessed Dec. 11, 2020)

Nishad, L. S., G. Akriti, J. Paliwal, R. Pandey, S. Beniwal, S. Kumar. 2016. Security, Privacy Issues and challenges In Cloud Computing: A Survey. In Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies (ICTCS '16). ACM, New York, NY, USA, Article 47, 7 pages. DOI: http://dx.doi.org/10.1145/2905055.2905253

Paquette, S., P. Jaeger, and S. Wilson. 2010. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly* 27 (3): 245-253.

Pearson, S. 2012. Privacy, security and trust in cloud computing. *Privacy and Security for Cloud Computing*: 3-42. doi:10.1007/978-1-4471-4189-1_1

Pishchulov, G., A. Trautrims, T. Chesney, S. Gold, and L. Schwab. 2019. The voting analytic hierarchy process revisited: a revised method with application to sustainable supplier selection. *International Journal of Production Economics* doi: 10.1016/j.ijpe.2019.01.025.

Rashmi Rai, S., G. Sahoo, & S. Mehfuz. 2013. Securing Software as a Service Model of Cloud Computing: Issues and Solutions. *International Journal on Cloud Computing: Services and Architecture (IJCCSA*,3 (4): 1-11.

Reddy, P., and S. Bouzefrane. 2014. Analysis and detection of dos attacks in cloud computing by using qse algorithm. 2014 IEEE International Conference on High Performance Computing and Communications. Paris, France.

Rezaei, J. 2015. Best- worst multi criteria decision making methods. *Omega* 53: 49–57.

2016 ._____. Best-worst multi-criteria decision-making method: Some properties and a linear model, *Omega* 64: 126-30.

2020 ._____. A concentration ratio for nonlinear best worst method, *International Journal of Information Technology & Decision Making* 19. DOI: 10.1142/S0219622020500170.

Rittinghouse, J. W., and J. F. Ransome. 2009. Security in the Cloud. In: Cloud Computing. Implementation, Management, and Security, CRC Press. Boca Raton- Florida

Rosado, D. G., R. Gómez, D. Mellado, and E. Fernández-Medina. 2012. Security analysis in the migration to cloud environments. *Future Internet* 4 (2): 469–487.

Rupra, S., and A. Omamo. 2020. A Cloud Computing Security Assessment Framework for Small and Medium Enterprises. *Journal of Information Security*. 11: 201-224.

Saaty, T. L. 1980. *The analytic hierarchy*. New York: McGraw-Hill.

2008 ._____. The analytical hierarchy and analytical network measurement processes: application to decisions under risk. *European Journal of Pure and Applied Mathematics* 1 (1): 122-196.

_____. 1990. How to Make a Decision: The Analytic Hierarchy Process. European Journal of Operational Research, 48, 9-26. http://dx.doi.org/10.1016/0377-2217 (90) 90057-I

Safari, N., F. Safari, M. Kazemi, S. Ahmadi, and A. Hasanzadeh. 2015. Prioritisation of cloud computing acceptance indicators using fuzzy AHP. *International Journal of Business Information Systems* 19 (4): 488-504.

Sen, J. 2013. Security and privacy issues in cloud computing, Architectures and Protocols for Secure Information Technology Infrastructures. GI Global: Hershey, PA, USA, 2013., pp.1- 45. DOI: 10.4018/978-1-4666-4514-1.ch001

Singh Nishad, L., J. Akriti Paliwal, R. Pandey, S. Beniwal, and S. Kumar. 2016. Security, privacy issues and challenges in cloud computing: a survey. proceedings of the second international conference on information and communication technology for competitive strategies. Article No. 47. New York, USA.

Soltanifar M., and F. Hosseinzadeh Lotfi. 2011. The voting analytic hierarchy process method for discriminating among efficient decision making units in data envelopment analysis. *Computers & Industrial Engineering* 60 (4): 585-592.

Subramanian, N., and A. Jeyaraj. 2018. Recent security challenges in cloud computing. *Computers & Electrical Engineering* 71: 28–42

Sultan, N. A. 2011. Reaching for the "cloud": how SMEs can manage. *International Journal of Information Management*. 31 (3): 272–278.

Sun, Y., J. Zhang, Y. Xiong, and G. Zhu. 2014. Data Security and Privacy in Cloud Computing. *International Journal of Distributed Sensor Networks*. Volume 2014, Article ID 190903, 9 pages 10 (7): 1-9.

Tabrizchi, H., and M. Kuchaki Rafsanjani. 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing* 79: 9493- 9532.

Tadapaneni, N. R. 2020. Cloud computing Security challenges. *International journal of Innovations in Engineering research and Technology* 7 (6): 1-5.

Tripathi, A., and A. Mishra. 2011. Cloud computing security considerations. In Proceedings of the 2011. *IEEE International Conference on Signal Processing, Communications and Computing* (ICSPCC), Xi'an, China, 14–16 September 2011; pp. 1–5.

V. Patel, R., D. Bhoi, and G. S. Pawar. 2020. Security hazards, attacks and its prevention techniques in cloud computing: a detail review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology 6 (4): 48-58.

Wayne, J. 2011. Cloud hooks: Security and privacy issues in cloud computing. In System Sciences (HICSS), 2011 44th Hawaii International Conference on, pp. 1-10. IEEE. Kauai, HI, USA.

Xiao, Z., and Y. Xiao. 2013. Security and privacy in cloud computing, *IEEE Communications Surveys & Tutorials* 15 (2): 843–859.

مهدی سلطانی‌فر

متولد سال ۱۳۶۰، دارای مدرک تحصیلی دکتری در رشتهٔ ریاضی کاربردی گرایش تحقیق در عملیات از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران است. ایشان هم‌اکنون استادیار گروه علوم پایهٔ دانشگاه آزاد اسلامی واحد سمنان است.

تحلیل پوششی داده‌ها، روش‌های تصمیم‌گیری چندشاخصه و شبکه‌های جریان از جمله علایق پژوهشی وی است.

سید محمد زرگر

متولد سال ۱۳۶۰، دارای مدرک تحصیلی دکتری در رشتهٔ مدیریت سیستم‌ها از دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران است. ایشان هم‌اکنون استادیار گروه مدیریت دانشگاه آزاد اسلامی واحد سمنان است.

مدیریت استراتژیک، سیستم‌های اطلاعاتی و پویایی سیستم‌ها از جمله علایق پژوهشی وی است.