



The identification of barriers to user privacy in the metaverse environment

Saeed Rezaei Sharifabadi¹ and Hadiseh Heidari²

1. Department of Information Science, Faculty of Education and Psychology, Alzahra University, Tehran, Iran. Email: srezaei@alzahra.ac.ir
2. Ph.D. Candidate in Information Science, Department of Information Science, Faculty of Education and Psychology, Alzahra University, Tehran, Iran (Corresponding Author). Email: h.heidari174@gmail.com

Article Info	ABSTRACT
<p>Article type: Review Article</p> <p>Article history: Received: 2025/12/04 Received in revised form: 2025/12/12 Accepted: 2026/01/21 Published online: 2026/01/28</p> <p>Keywords: Metaverse, barriers, users, privacy, challenges, Fuzzy Delphi.</p>	<p>Purpose: The metaverse has emerged as a widely discussed topic of public interest, with individuals and organizations alike contemplating its potential applications while being significantly concerned about privacy. User privacy in the metaverse environment includes control over personal information and data sharing, protection of digital identity, and prevention of unauthorized access to users' personal information, among other aspects. The aim of this research is to identify the barriers to user privacy in the metaverse environment.</p> <p>Methods: This research is applied in terms of purpose and survey in terms of data collection method. First, by reviewing the literature in the field of metaverse, privacy barriers in the field of metaverse were identified, and then in order to identify the most important barriers that affect the development of metaverse and that experts agree on, fuzzy Delphi techniques were used for data analysis. The statistical population of the present study consists of experts in the fields of metaverse, privacy, law, artificial intelligence, information science, and epistemology. To determine the sample, the judgmental sampling method and the opinions of 16 experts in this field were used. To identify privacy barriers in the field of metaverse, the researchers first extracted 44 barriers to user privacy in the metaverse environment by reviewing the literature and research background, and then the experts were asked to determine the impact of the indicators based on a five-point Likert scale using a semi-structured questionnaire. To collect the opinions of the experts at the end of the six research components, an open question was written at the end and the experts were asked to state if they had any other indicators in mind that were related to the research objective in addition to the mentioned indicators. After selecting the appropriate method and defuzzifying the values, a tolerance threshold should be considered for screening the items. The threshold for confirming the components is 0.75 percent. In this study, each of the barriers to user privacy was ranked using the Cocosu method.</p> <p>Findings: According to the experts, the higher the number of points given to each of the barrier components, the greater the importance of the component, and it has been confirmed. Also, using the Delphi-Fuzzy method, 26 barriers were screened and selected for the final analysis, and 3 barriers were identified based on the scores obtained. The costs of data protection, personal information leakage, and lack of interactivity of graphics and hardware were the most important, respectively. The findings showed that protecting privacy in the metaverse space has become a multifaceted challenge that requires attention to cultural, educational, and technological issues. One of the most obvious and important barriers identified in the present study is the cost of data protection. This barrier actually reflects the complexities and economic and technical challenges related to collecting, storing, processing, and transferring user data in the metaverse world. Data protection systems require advanced technology infrastructures that incur costs for implementation and</p>

maintenance. Especially in the metaverse space, where data exchange takes place extensively and in real time, the need for security systems that can effectively protect users' personal information and identity is felt more than ever. The second obstacle is related to the leakage of personal information in the metaverse environment. The leakage of personal information in the metaverse is one of the most complex and challenging security issues in today's digital world. Given the unique characteristics of this virtual space and the extensive interactions that take place in it, security threats in these environments can be much more complex and impactful than in other online spaces. The third obstacle is also related to the lack of interoperability of graphics and hardware in the metaverse environment. The lack of interoperability between graphics and hardware in the metaverse environment is one of the fundamental challenges that can directly affect the user experience and the efficiency of systems in this space. In other words, to create an efficient and scalable metaverse environment, it is necessary for developers, hardware manufacturers, and standardization bodies to cooperate to ensure the integration between graphics and hardware and to resolve existing problems.

Conclusion: Educating users about better strategies for maintaining privacy and ways to avoid security risks in the metaverse, as well as enhancing awareness of security and privacy issues, can lead to improved and responsible decision-making by users. The actions outlined in this research can help enhance users' privacy in the metaverse environment and increase their trust in this platform. Given the growing importance of the metaverse and its impact on daily life, addressing privacy barriers and striving to overcome them appears to be essential. This research can assist policymakers, developers, and users in gaining a better understanding of the challenges present in this space and contribute to creating a safer and more private environment for metaverse users.

Cite this article: Rezaei Sharifabadi, S., & et al. (2025)., The identification of barriers to user privacy in the metaverse environment. *Science and Technology of Information Management*, 11 (4). 130-151. DOI: <https://doi.org/10.22091/STIM.2025.11546.2176>



© The Author(s)

DOI: 10.22091/STIM.2025.11546.2176

Publisher: University of Qom



شناسایی موانع حریم خصوصی کاربران در محیط متاورس

سعید رضایی شریف آبادی^۱ و حدیثه حیدری^۲

۱. گروه علم اطلاعات و دانش‌شناسی، دانشکده روان‌شناسی و علوم تربیتی، دانشگاه الزهراء، تهران، ایران. رایانامه: srezaei@alzahra.ac.ir

۲. دانشجوی دکتری علم اطلاعات و دانش‌شناسی گرایش بازیابی اطلاعات و دانش، دانشگاه الزهراء، تهران، ایران (نویسنده مسئول). رایانامه: h.heidari174@gmail.com

اطلاعات مقاله	چکیده
نوع مقاله: مقاله مروری	هدف: متاورس موضوعی است که به‌طور گسترده مورد علاقه عموم قرار گرفته است. افراد و سازمان‌ها به‌طور یکسان در مورد کاربردهای بالقوه آن فکر می‌کنند و به‌شدت نیازمند حریم خصوصی است. حریم خصوصی کاربران در محیط متاورس شامل کنترل اطلاعات شخصی و اشتراک‌گذاری داده‌ها، حفاظت از هویت دیجیتال، و جلوگیری از دسترسی‌های غیرمجاز به اطلاعات شخصی کاربران و از این قبیل است. هدف از این پژوهش، شناسایی موانع حریم خصوصی کاربران در محیط متاورس است.
تاریخ دریافت: ۱۴۰۴/۰۹/۱۳	روش‌شناسی: این پژوهش از نظر هدف کاربردی و از لحاظ شیوه گردآوری داده‌ها پیمایشی است. ابتدا با بررسی ادبیات حوزه متاورس، موانع حریم خصوصی در این حوزه مشخص شدند و سپس برای شناسایی مهمترین موانع که بر توسعه متاورس مؤثر هستند و خبرگان در مورد آن‌ها اتفاق نظر دارند، از فنون دلفی فازی برای تحلیل داده‌ها، استفاده شده است. جامعه آماری پژوهش حاضر را خبرگان صاحب‌نظر در زمینه متاورس، حریم خصوصی، حقوق، هوش مصنوعی، و علم اطلاعات و دانش‌شناسی تشکیل می‌دهند. برای تعیین نمونه از روش نمونه‌گیری قضاوتی و از نظرات ۱۶ نفر از خبرگان در این حوزه استفاده شده است. پژوهشگران برای شناسایی موانع حریم خصوصی در حوزه متاورس، ابتدا با استفاده از مرور ادبیات و پیشینه پژوهش، تعداد ۴۴ مانع برای حریم خصوصی کاربران در محیط متاورس استخراج کردند و سپس با یک پرسش‌نامه نیمه‌ساختارمند از خبرگان درخواست شد که براساس طیف پنج‌تایی لیکرت، تأثیر شاخص‌ها را مشخص کنند. برای گردآوری نظرات خبرگان در انتهای شش مؤلفه پژوهشیک سؤال باز نوشته شده و از خبرگان خواسته شد که علاوه بر شاخص‌های گفته‌شده اگر شاخص‌های دیگری در نظر دارند که با هدف پژوهش در ارتباط است، بیان کنند. پس از انتخاب روش مناسب و فازی‌زدایی مقادیر، برای غربال آیتم‌ها باید یک آستانه تحمل در نظر گرفت. حد آستانه در تأیید مؤلفه‌ها ۰/۷۵ درصد در نظر گرفته شده است. در این پژوهش با استفاده از روش کوکوسو هر یک از موانع حریم خصوصی کاربران رتبه‌بندی شد.
تاریخ بازنگری: ۱۴۰۴/۰۹/۲۱	یافته‌ها: با توجه به نظر خبرگان، هرچه تعداد امتیاز داده‌شده به هر یک از مؤلفه‌های موانع موردنظر بیشتر باشد، اهمیت مؤلفه بیشتر شده و تأیید شده است. همچنین موانع با استفاده از روش دلفی فازی غربال و ۲۶ مانع برای تحلیل نهایی انتخاب شدند و براساس نمرات کسب‌شده سه مانع شناسایی شد. هزینه‌های حفاظت از داده‌ها، نشت اطلاعات شخصی، تعامل‌پذیر نبودن گرافیک‌ها و سخت‌افزارها به ترتیب، بیشترین اهمیت را داشتند. یافته‌ها نشان داد که حفاظت از حریم خصوصی در فضای متاورس به یک چالش چندوجهی تبدیل شده که نیازمند توجه به مسائل فرهنگی، آموزشی، و فناورانه است. یکی از بارزترین و مهمترین موانع شناسایی‌شده در پژوهش حاضر، هزینه‌های حفاظت از داده‌ها است. این مانع در واقع بازتاب‌دهنده پیچیدگی‌ها و چالش‌های اقتصادی و فنی مربوط به جمع‌آوری، ذخیره‌سازی، پردازش، و انتقال داده‌های کاربران در دنیای متاورس است. سیستم‌های حفاظت از داده‌ها نیازمند زیرساخت‌های فناوری پیشرفته‌ای هستند که هزینه‌هایی را برای پیاده‌سازی و نگهداری به‌دنبال دارند. به‌ویژه در فضای متاورس که تبادل داده‌ها به‌شیوه‌ای گسترده و در زمان واقعی انجام می‌شود، نیاز به سیستم‌های امنیتی که بتوانند به‌طور مؤثر از اطلاعات شخصی و هویتی کاربران حفاظت کنند، بیشتر از هر زمان دیگری احساس می‌شود. مانع دوم مربوطه به نشت اطلاعات شخصی در محیط متاورس است. نشت اطلاعات شخصی در متاورس یکی از پیچیده‌ترین و چالش‌برانگیزترین مسائل امنیتی در دنیای دیجیتال کنونی است. با توجه به ویژگی‌های منحصر به فرد این فضای مجازی و تعاملات گسترده‌ای که در آن انجام می‌شود، تهدیدات
تاریخ پذیرش: ۱۴۰۴/۱۱/۰۱	
تاریخ انتشار: ۱۴۰۴/۱۱/۰۸	

کلیدواژه‌ها:

متاورس، موانع، کاربران، حریم خصوصی، چالش‌ها، دلفی فازی.

امنیتی در این محیط‌ها می‌توانند بسیار پیچیده‌تر و تأثیرگذارتر از سایر فضاهای آن‌لاین باشند. همچنین مانع سوم مربوط به تعامل پذیرنبودن گرافیک‌ها و سخت‌افزارها در محیط متاورس است. تعامل پذیرنبودن گرافیک‌ها و سخت‌افزارها در محیط متاورس یکی از چالش‌های اساسی است که می‌تواند به‌طور مستقیم بر تجربه کاربران و کارایی سیستم‌ها در این فضا تأثیر بگذارد. به‌عبارتی برای ایجاد یک محیط متاورس کارآمد و مقیاس‌پذیر، نیاز به همکاری توسعه‌دهندگان، تولیدکنندگان سخت‌افزار، و نهادهای استانداردسازی است تا یکپارچگی میان گرافیک‌ها و سخت‌افزارها تضمین شود و مشکلات موجود را برطرف سازند.

نتیجه‌گیری: حفاظت از حریم خصوصی در متاورس تنها با رویکرد جامع و چندبُعدی امکان‌پذیر است. این رویکرد باید شامل ترکیبی از افزایش آگاهی عمومی، توسعه فناوری‌های ایمنی، و در نظر گرفتن تفاوت‌های فرهنگی در طراحی سیاست‌های حریم خصوصی باشد. با توجه به اینکه متاورس در حال گسترش و تبدیل به بخش مهمی از زندگی دیجیتال کاربران است، توجه به این مسائل نه‌تنها برای حفاظت از حریم خصوصی افراد، بلکه برای ایجاد محیطی امن و قابل اعتماد در این فضا، امری ضروری است.

استناد: رضایی شریف آبادی، سعید و دیگران. (۱۴۰۴). «شناسایی موانع حریم خصوصی کاربران در محیط متاورس». *علوم و فنون مدیریت اطلاعات*. دوره ۱۱، شماره ۴، صص: ۱۵۱-۱۳۰. <https://doi.org/10.22091/STIM.2025.11546.2176>



۱. مقدمه

امروزه صحبت از فضای مجازی یا سایبری، فضای دیجیتال، فضای اینترنتی، فضای الکترونیکی، و غیره امری معمول و واقعیتی انکارناپذیر به شمار می‌رود. فضاهای نوین مبتنی بر فناوری اطلاعات و ارتباطات بازنمونی از واقعیت‌های فیزیکی را در قالب‌های دیجیتال، چندرسانه‌ای، چندوجهی و انعطاف‌پذیر، توسعه داده‌اند. سالیان درازی است که انسان‌ها در فضاهای نوین یادشده حضور دارند و تعامل از راه بازنمون‌های مجازی بسیار گسترده‌تر از تعاملات فیزیکی بوده است (بحرینی و دیگران، ۱۴۰۱). توسعه شبکه‌های اجتماعی و عمومی شدن حضور در فضاهای مجازی سطح تعاملات و تنوع آن را به شکل شگفت‌انگیزی افزایش داده است.

متاورس^۱ یک فضای آن‌لاین، سه‌بعدی، و دیجیتالی است که از ترکیب واژه یونانی متا^۲ + ورس^۳ به معنای جهان مجازی سه‌بعدی تشکیل شده است. در واقع، ترکیبی از دنیاهای مجازی، بازی‌های آن‌لاین، واقعیت افزوده، و شبکه‌های اجتماعی است که کاربران می‌توانند در آن ورود کنند و به انجام فعالیت‌های مختلف خود بپردازند. این فعالیت‌ها ممکن است اجتماعی، فرهنگی، سیاسی، مذهبی، آموزشی، و مواردی از این قبیل باشند. اصطلاح متاورس، اولین بار در رمان علمی تخیلی نیل استنفسون^۴ با عنوان «سقوط برف» در سال ۱۹۹۲ به کار رفت. در این کتاب، متاورس به مثابه آخرین تیر از کمان اینترنت بر پیکر نیمه جان دنیای سنتی شلیک شده است، تعبیری فلسفی از اهمیت واقعیت مجازی که در آن هر تعامل دیجیتال می‌تواند بر دنیای واقعی تأثیری مستقیم داشته باشد. متاورس یک دنیای مجازی است که با ترکیب مفاهیم واقعیت مجازی^۵ و واقعیت افزوده^۶، به دنبال این است تا به کاربران خود این فرصت را بدهد تا هر آن‌چه را که در دنیای واقعی انجام می‌دهند بدون نیاز به حضور فیزیکی در متاورس انجام دهند. در واقع، می‌توان متاورس را یک جهان برتر معرفی کرد که در آن محدودیت‌های دنیای فیزیکی از بین خواهند رفت و شاید انسان‌ها بتوانند در دنیای آرمانی خود زندگی کنند. لذا، متاورس بدون آن‌که فرد یا سازمان خاصی مالک آن باشد، وجود دارد. حتی در سال‌های آینده که سهام‌داران مختلفی اعم از افراد و شرکت‌های تجاری در توسعه و بهره‌برداری متاورس مشارکت بیشتری خواهند داشت، هیچ کس مالک متاورس نخواهد بود. اما می‌توان پیش‌بینی کرد که شرکت‌های بزرگ مانند مایکروسافت در شکل‌گیری آن نقش پررنگی خواهند داشت (رضایی‌نور و کریمیان، ۱۴۰۳؛ حسن‌زاده، ۱۴۰۱؛ شاه‌مرادی، ۱۴۰۱؛ میستاکیدیس^۷، ۲۰۲۳؛ میلر^۸ و همکاران، ۲۰۱۹؛ میر اشرفی، ۱۴۰۱؛ اورلند^۹، ۲۰۲۱). متاورس در زمینه‌های متعددی از جمله آموزش، شغل و کسب‌وکارها، تجارت، سرگرمی، پزشکی، مسائل اجتماعی، پژوهش‌های علمی، دولت، هنر، و فرهنگ کاربرد دارد. پژوهشگران داخلی و خارجی همچون یگانه و سعیدیان (۱۴۰۱) در پژوهش خود به موانعی از قبیل نقض حق کپی‌رایت و مالکیت معنوی، نبود قوانین روشن برای مالکیت معنوی، و هویت و جعل هویت توجه کردند. شاید^{۱۰} (۲۰۲۳) در پژوهش خود به مواردی همانند ایجاد شکاف اجتماعی، انزوای اجتماعی، و پرهیز از زندگی واقعی و فیزیکی توجه کرده‌اند. مرادی‌برلیان (۱۴۰۱) به هزینه‌های حفاظت از داده‌ها، هزینه‌های آگاهی، هزینه‌های امنیتی، و هزینه‌های اجرای قوانین، و دوویدی و دیگران^{۱۱} (۲۰۲۳) جرایم مالی توجه کرده‌اند. میراشرفی (۱۴۰۱) به موانع تأثیر نامحسوس بر امنیت فرهنگی و سیاسی یک کشور گذاشتن، حملات سایبری، و نشست داده‌ها و کیم و دیگران^{۱۲} (۲۰۲۳) نشست اطلاعات شخصی، شنود، دسترس غیرمجاز، فیشینگ، تزریق داده، احراز هویت شکسته، و طراحی ناامن را در کانون توجه خود

1. META VERSE

2. META

3. VERSE

۴. Neal Stephenson

۵. Virtual Reality (VR)

6. Augmented Reality (AR)

7. Mystakidis

8. Miller

9. Orland

10. Said

11. Dwivedi et al

12. Kim et al

قرار داده‌اند محمداقاری و سیدباقری (۱۴۰۱) به موانع تلفن همراه هوشمند، هدست واقعیت‌های مجازی، و عینک‌های دیجیتال، ساید (۲۰۲۳) به هدست با میکروفون زنده و دوربین و ردیاب چشم، هزینه‌های بالای تجهیزات، نبود دسترسی به اینترنت پرسرعت و پهنای باند بالا توجه کرده‌اند. رضایی‌نور و کریمیان (۱۴۰۳) به موانع استفاده از فناوری‌ها از سوی مدیریت برای تصمیم‌گیری، ضعف در دانش فنی مدیران، ناتوانی در جمع‌آوری اطلاعات و آمار، بی‌ثباتی مدیریتی، و شی و زو^۱ (۲۰۲۴) به افزایش ریسک پرداخته‌اند. شاه‌مرادی (۱۴۰۱) سوءاستفاده و آزار و اذیت، غوطه‌وری و اعتیاد، افشاگری اطلاعات شخصی، و شرمندگی و پشیمانی، داراب‌پور (۱۴۰۲) به نبود پوشش نامناسب، جین پاتل^۲ (۲۰۲۴) به تأثیر بر سلامت روان و مراقبت‌های بهداشتی توجه کرده‌اند. از این‌رو، یکی از مباحثی که امروزه در همه کشورهای در زمینه فناوری‌ها به‌ویژه فناوری متاورس دغدغه و نگرانی برای کشورها ایجاد کرده مسئله حریم خصوصی است.

حریم خصوصی در معرض تهدیدهایی قرار دارد که کاربران را با چالش‌هایی زیادی روبه‌رو می‌کند. در واقع، حریم خصوصی نقش بسزایی در شکل‌گیری فناوری‌ها از جمله متاورس دارد. در شبکه‌های اجتماعی قدیمی کاربران این امکان را داشتند که به شیوه خصوصی و با اختیار خود اطلاعات و پیام‌هایی را با مخاطبین خود به اشتراک بگذارند. همچنین حفظ حریم خصوصی در این نوع شبکه‌های اجتماعی به دلیل دسترسی نداشتن دیگر کاربران به اطلاعات به اشتراک گذاشته شده ساده بود اما در متاورس حفظ حریم خصوصی به این سادگی امکان پذیر نیست، زیرا در متاورس فضایی اجتماعی حاکم است و حفظ حریم خصوصی به یک موضوع چالش‌برانگیز تبدیل شده است. از این‌رو، کاربران برای ایجاد و القای تجربه در متاورس از دستگاه‌های پوشیدنی متفاوتی نظیر کاله ایمنی، و عینک‌های واقعیت مجازی استفاده می‌کنند که این دستگاه‌های پوشیدنی همواره در برابر خطر از طرف دشمنان و مهاجمان قرار دارند، به این نحو که مهاجمان با هک کردن این دستگاه‌ها و ردیابی اطلاعات شخصی کاربران، نظیر آدرس محل سکونت کاربران که، حسگرهای عینک‌های واقعیت مجازی آن را جمع‌آوری کرده‌اند، دسترسی پیدا می‌کنند و حریم خصوصی کاربر را با تهدید و چالش‌هایی روبه‌رو می‌کنند. چالشی که در این دستگاه‌های پوشیدنی وجود دارد این است که در صورت وجود مشکل یا آسیب دیدگی در این دستگاه‌های پوشیدنی، تبدیل به یک ورودی برای نفوذ به داده‌ها و تهاجم بدافزارها می‌شوند (شون^۳، ۲۰۲۲؛ رضایی‌ملال و مرتضائی‌دکاهی، ۱۴۰۱). از این‌رو، هنوز هیچ مقرراتی برای حریم خصوصی کاربر وجود ندارد. با توجه به جمع‌آوری و تجزیه و تحلیل داده‌ها و اینکه داده‌های زیادی به‌طور مداوم از سوی کاربران ناشناخته برای کاربر واقعیت مجازی به اشتراک گذاشته می‌شود، مقررات در این زمینه اهمیت بیشتری پیدا می‌کند، اما اکنون، حفاظت یا اشتراک‌گذاری آن داده‌ها کاملاً به مالک پلتفرم بستگی دارد. لذا، مسئله اصلی این پژوهش شناسایی موانع حریم خصوصی کاربران در محیط متاورس است.

۲. پیشینه پژوهش

در پژوهش حاضر برای بررسی پیشینه پژوهش از کلیدواژه‌های همچون متاورس و حریم خصوصی، خطرات حریم خصوصی، چالش‌های حریم خصوصی، چالش‌های فرهنگی، چالش‌های اجتماعی، چالش‌های اقتصادی، چالش‌های سیاسی، چالش‌های امنیتی، چالش‌های حقوقی، چالش‌های مدیریتی، چالش‌های فناورانه، چالش‌های روان‌شناختی، چالش‌های دینی حریم خصوصی، حریم خصوصی داده‌ها، سرقت هویت، امنیت سایبری، اخلاق حریم خصوصی، و قانون و حریم خصوصی در متاورس، در پایگاه اطلاعاتی داخلی (نورمگز، مگیران، علم‌نت، گنج) و خارجی (اسکوپوس^۴، وب‌اوساینس^۵) در جدول (۱) و جدول (۲) هدف‌بازایی و بررسی آن‌ها است.

1. Shi & Zhu
2. Jane Patel
3. Shaun
4. Scopus
5. Web Of Science

جدول ۱. راهبرد جستجوی پژوهش

راهبرد جستجو
TITLE(" Privacy and Metaverse" OR "Privacy barriers" OR "Challenges to privacy" OR "Political Challenges of Privacy" OR "Risks to privacy" OR "Data privacy" OR "Identity theft" OR "Cybersecurity" OR "Ethics of privacy" OR "Law and privacy" OR "Social challenges of privacy" OR "Cultural challenges of privacy" OR "Economic challenges of privacy" OR "Environmental intelligence*" OR "Privacy Security Challenges" OR "Legal challenges of privacy" OR "Privacy management challenges" OR "Technological challenges of privacy" OR "Psychological challenges of privacy" OR "Religious challenges to privacy" in the "Metaversity*" OR "Metaworth*" OR "Metaverse*" OR "Metavers*")
TI=(" Privacy and Metaverse" OR "Privacy barriers" OR "Challenges to privacy" OR "Political Challenges of Privacy" OR "Risks to privacy" OR "Data privacy" OR "Identity theft" OR "Cybersecurity" OR "Ethics of privacy" OR "Law and privacy" OR "Social challenges of privacy" OR "Cultural challenges of privacy" OR "Economic challenges of privacy" OR "Environmental intelligence*" OR "Privacy Security Challenges" OR "Legal challenges of privacy" OR "Privacy management challenges" OR "Technological challenges of privacy" OR "Psychological challenges of privacy" OR "Religious challenges to privacy" in the "Metaversity*" OR "Metaworth*" OR "Metaverse*" OR "Metavers*")

جدول ۲. پیشینه پژوهش

روش پژوهش	منبع	مؤلفه
کتابخانه‌ای	یگانه و فامیل سعدیان (۱۴۰۱).	نقض حق کپی‌رایت و مالکیت معنوی؛ نبود قوانین روشن برای مالکیت معنوی؛ هویت و جعل هویت
پدیدارشناختی	ساید (۲۰۲۳).	ایجاد شکاف اجتماعی؛ انزوای اجتماعی؛ پرهیز از زندگی واقعی و فیزیکی
تحلیلی_توصیفی	محمودی و صادقی (۱۴۰۱).	جعل هویت افراد؛ حذف لذت‌های فیزیکی؛ عدم انطباق و ناسازگاری برخی افراد؛ کمبود آگاهی
تحلیلی_توصیفی	میراشرفی (۱۴۰۱).	حذف لذت‌های فیزیکی؛ نبود انطباق و سازگاری برخی افراد؛ مالکیت معنوی
تحلیلی_توصیفی	دوویدی و همکاران (۲۰۲۳).	شمول اجتماعی؛ سرقت هویت؛ محتوای بازاریابی گمراه‌کننده و فریبنده؛ جعل هویت؛ کمبود آگاهی
تحلیلی_توصیفی	وانگ و همکاران ^۱ (۲۰۲۲)؛ شی و زو (۲۰۲۴)؛ دیزجی و دیزجی ^۲ (۲۰۲۳).	جعل هویت
روش اسکن تجربی (کمی)	تورال و کوچاک ^۳ (۲۰۲۳).	کمبود سطح آگاهی و کسب هویت دیجیتال
تحلیلی_توصیفی	محمدباقری و سیدباقری (۱۴۰۱).	حفظ نشدن حقوق مالکیت معنوی؛ آواتارها و هویت‌های مجازی؛ نبود هویت دیجیتال قابل اعتماد؛ ارزش متفاوت فرهنگ‌ها؛ ترس از نظارت؛ خطرات سوء استفاده از داده‌ها؛ نبود کنترل کاربران بر داده‌هایشان

۱. Wang et al

۲. Dizaji & Dizaji

۳. Tural & Koçak

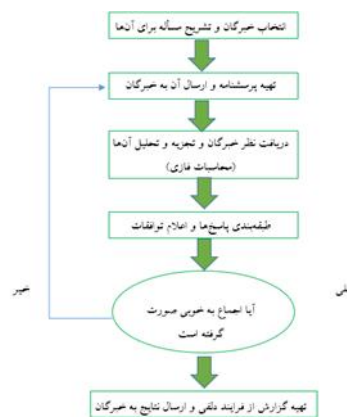
روش پژوهش	منبع	مؤلفه
تحلیلی_توصیفی	داراب‌پور (۱۴۰۲).	ناشناختگی هویت؛ خطرات تبعیض؛ نبود تعادل بین دنیای واقعی و مجازی؛ نبود فرهنگ حریم خصوص
تحلیلی_توصیفی	مرادی برلیان (۱۴۰۱).	نبود حقوق مالکیت
تحلیلی_توصیفی	پاشایی (۱۳۹۹).	هزینه‌های تکنولوژی؛ استفاده از رمز ارزها برای تراکنش‌ها؛ نبود مقررات برای رمز ارزها
تحلیلی_توصیفی	شهریاری (۱۴۰۱).	هزینه‌های زیاد فن
تحلیلی_توصیفی	دوویدی و همکاران (۲۰۲۳).	جرایم مالی
تحلیلی_توصیفی	مرادی برلیان (۱۴۰۱).	هزینه‌های حفاظت از داده‌ها؛ هزینه‌های آگاهی؛ هزینه‌های امنیتی؛ هزینه‌های اجرای قوانین
پدیدارشناختی	ساید (۲۰۲۳).	هزینه حفاظت از داده‌ها
توصیفی-پیمایشی	شاه‌مرادی (۱۴۰۱).	هزینه بالای تجهیزات
تحلیلی_توصیفی	محمودی و صادقی (۱۴۰۱).	قوانین سخت‌گیرانه دولت‌ها در بخش فناوری؛ خطرات پول‌شویی و تأمین مالی تروریسم
تحلیلی_توصیفی	شهریاری (۱۴۰۱).	نبود قوانین و مقررات؛ نبود امنیت؛ نبود آگاهی از خطرات؛ نبود قوانین و مقررات مشخص؛ نبود هماهنگی بین کشورها
تحلیلی_توصیفی	کیم و دیگران (۲۰۲۳).	نشت اطلاعات شخصی؛ نشود؛ دسترسی غیرمجاز؛ فیشینگ؛ تزریق داده؛ احراز هویت شکسته؛ طراحی ناامن
تحلیلی_توصیفی	جین پاتل (۲۰۲۴).	ردیابی و نظارت؛ حریم خصوصی و امنیت داده‌ها؛ رضایت آگاهانه
تحلیلی_توصیفی	دوویدی و همکاران (۲۰۲۳).	تبلیغات تهاجمی؛ اطلاعات نادرست؛ کلاهبرداری فیشینگ
تحلیلی_توصیفی	وانگ و همکاران (۲۰۲۲).	امنیت، نظارت؛ ردیابی؛ حملات سایبری؛ تمهیدات برای پاسخ‌گویی
تحلیلی_توصیفی	داراب‌پور (۱۴۰۲).	اعمال نشدن مقررات قانونی مربوط به رضایت کاربر
تحلیلی_توصیفی	میراشرفی (۱۴۰۱).	گذشتن تأثیر نامحسوس بر امنیت فرهنگی و سیاسی یک کشور؛ حملات سایبری؛ نشت داده‌ها
تحلیلی_توصیفی	لطیف‌زاده و قبولی‌درافشان (۱۴۰۲). دوویدی و همکاران (۲۰۲۳).	نظارت، حملات سایبری، حفاظت از داده‌ها
تحلیلی_توصیفی	دوویدی و همکاران (۲۰۲۳).	فعالیت‌های تروریستی؛ امنیت داده‌ها
تحلیلی_توصیفی	شی و زو (۲۰۲۴).	نشت داده‌ها، امنیت

روش پژوهش	منبع	مؤلفه
کتابخانه‌ای و میدانی	دیزجی و دیزجی (۲۰۲۳).	جرایم علیه اموال مانند کلاهبرداری؛ انتقال مال؛ سرقت؛ پول‌شویی و حتی جرایم علیه امنیت ملی مانند تبلیغ تروریسم؛ آدم‌ربایی
تحلیلی_توصیفی	مرادیان، و پورغفاری‌بشری (۱۴۰۱).	نبود مدیریت هویت
تحلیلی_توصیفی	کیم و دیگران (۲۰۲۳).	مدیریت هویت و احراز هویت
کیفی	رضایی‌نور و کریمیان (۱۴۰۲).	استفاده از فناوری‌های از سوی مدیریت برای تصمیم‌گیری، ضعف در دانش فنی مدیران؛ ناتوانی در جمع‌آوری اطلاعات و آمار؛ نبود ثبات مدیریتی؛ نبود هماهنگی و شتاب‌زدگی بین بخش‌های مختلف مدیریت؛ نبود رقابت عملیاتی هوشمندسازی در بین مدیران؛ نبود هنجارهای نظارتی در سیاست‌های عملیاتی
تحلیلی_توصیفی	شی و زو (۲۰۲۴).	افزایش ریسک
تحلیلی_توصیفی	محمودی و صادقی (۱۴۰۱).	هدست واقعیت مجازی؛ عینک هوشمند واقعیت مجازی؛ اینترنت پرسرعت؛ کلاهبرداری با استفاده از فناوری بالا؛ استراق‌سمع آوارت‌های نامرئی؛ نبود امنیت داده‌ها
کیفی	رضایی‌نور و کریمیان (۱۴۰۲).	چارچوب و استانداردهای لازم برای تولید محتوای دیجیتالی؛ طراحی دنیای گرافیکی خارج از واقعیت فیزیکی؛ فناوری‌های احراز هویت؛ نبود دسترسی به هدست‌های واقعیت مجازی؛ نیازمند بودن به عینک هوشمند واقعیت مجازی
تحلیلی_توصیفی	محمدباقری و سیدباقری (۱۴۰۱).	تلفن همراه هوشمند؛ هدست واقعیت‌های مجازی؛ عینک‌های دیجیتال
کتابخانه‌ای	حدادعراقی (۱۴۰۱).	نظارت و ردیابی؛ نبود کنترل بر داده‌ها؛ استانداردهای ضعیف فنی؛ فناوری‌های جدید؛ نبود زیرساخت‌های مقیاس‌پذیر.
تحلیلی_توصیفی	مرادیان و پورغفاری‌بشری (۱۴۰۱).	آسیب‌پذیری دستگاه‌ها مانند هولولنز
تحلیلی_توصیفی	شهریاری (۱۴۰۱).	اینترنت پرسرعت؛ هدست‌های گران قیمت؛ تعامل‌پذیر نبودن گرافیک‌ها و سخت‌افزارها
پدیدارشناختی	ساید (۲۰۲۳).	هدست با میکروفون زنده و دوربین و ردیاب چشم، هزینه بالا تجهیزات؛ در دسترس نبودن اینترنت پرسرعت و پهنای باند بالا
توصیفی-پیمایشی	شاه‌مرادی (۱۴۰۱).	آوارت‌های جعلی و سرقت هویت
تحلیلی_توصیفی	دوویدی و همکاران (۲۰۲۳).	دسترسی به فناوری پرهزینه؛ آسیب‌پذیری فناوری و مصرف‌کننده؛ رابط انسان و رایانه؛ نقض داده‌ها
تحلیلی_توصیفی	پاشایی (۱۳۹۹).	اضطراب؛ افسردگی؛ حواس‌پرتی؛ از دست دادن حس هویت؛ خطرات برای ایمان و اخلاقیات

با توجه به جدول (۲)، به مرور پیشینه‌ها، بیشتر پژوهش‌ها به روش تحلیلی-توصیفی انجام شده‌اند. پژوهش حاضر از روش مرور نظام‌مند و دلفی فازی استفاده کرده که از این راه نظرات خبرگان حوزه در زمینه متاورس، حریم خصوصی، حقوق، هوش مصنوعی، و علم اطلاعات و دانش‌شناسی در رابطه با مؤلفه‌ها جمع‌آوری شده است. با توجه به این‌که پژوهش‌های پیشین به موانع حریم خصوصی تنها به‌مثابه یک مؤلفه در پژوهش خود توجه کرده‌اند، این پژوهش به‌صورت ویژه به شناسایی موانع حریم خصوصی کاربران در محیط متاورس می‌پردازد.

۳. روش‌شناسی

این پژوهش از نظر هدف کاربردی و از لحاظ شیوه گردآوری داده‌ها پیمایشی است. در پژوهش حاضر ابتدا با بررسی ادبیات حوزه متاورس، موانع حریم خصوصی در این حوزه مشخص شدند و سپس برای شناسایی مهمترین موانع که بر توسعه متاورس مؤثر هستند و خبرگان در مورد آن‌ها اتفاق نظر دارند، از روش دلفی فازی استفاده شده است. در روش دلفی فازی به دلیل ناقص و نادقیق بودن اطلاعات در تصمیم‌گیری‌ها و ذهنی بودن تصمیم‌های گرفته‌شده از سوی خبرگان، از اعداد فازی به جای اعداد قطعی استفاده می‌شود. در دلفی فازی تک مرحله‌ای اطلاعات مفید به دلیل این‌که تمام نظرات کارشناسان مد نظر قرار می‌گیرد، از دست نمی‌رود (ضرغام‌پروجنی و عزیزی، ۱۳۹۶). جامعه آماری پژوهش حاضر را ۳۰ نفر از خبرگان صاحب‌نظر در زمینه فناوری اطلاعات (متاورس، هوش مصنوعی)، حقوق، علم اطلاعات و دانش‌شناسی تشکیل می‌دهند. با توجه به این‌که تنها ۱۶ نفر از خبرگان پاسخ سؤالات را دادند، برای تعیین نمونه از روش نمونه‌گیری قضاوتی (هدف‌مند) بهره گرفته شده و از نظرات این ۱۶ نفر از خبرگان استفاده شد. پژوهشگران برای شناسایی موانع حریم خصوصی در حوزه متاورس، ابتدا با استفاده از مرور ادبیات و پیشینه پژوهش، تعداد ۴۴ مانع برای حریم خصوصی کاربران در محیط متاورس را استخراج کردند و سپس با یک پرسش‌نامه نیمه‌ساختارمند از خبرگان درخواست کردند که براساس طیف پنج‌تایی لیکرت، تأثیر شاخص‌ها را مشخص کنند. بنابراین برای گردآوری نظرات خبرگان در انتهای شش مؤلفه پژوهش، یک سؤال باز نوشته شده و از خبرگان خواسته شد که علاوه بر شاخص‌های یادشده اگر شاخص‌های دیگری در نظر دارند که با هدف پژوهش در ارتباط است، بیان کنند. دو نوع روایی در این حوزه در کانون توجه قرار گرفته است: روایی بیرونی و روایی درونی. اعتبار بیرونی را شامل می‌شود. در ارتباط با روایی درونی، استفاده از روش‌هایی مانند دلفی فازی باعث ایجاد هم‌گرایی بین مشارکت‌کنندگان می‌شود. یکی دیگر از روش‌های تعیین اعتبار پرسش‌نامه، بررسی روایی محتوا است. اعتبار محتوا به سؤال‌های تشکیل‌دهنده ابزار اندازه‌گیری بستگی دارد. در این پژوهش برای سنجش روایی محتوا، از نظر ۱۶ نفر از خبرگان علمی و اجرایی در حوزه متاورس و هوش مصنوعی استفاده شده است. پس از انتخاب روش مناسب و فازی‌زدایی مقادیر، برای غربال آیت‌ها باید یک آستانه تحمل در نظر گرفت. حد آستانه در تأیید مؤلفه‌ها ۰/۷۵ درصد در نظر گرفته شده است. در این پژوهش با استفاده از روش کوسو^۱ هر یک از موانع حریم خصوصی کاربران رتبه‌بندی شدند. الگوریتم اجرای دلفی فازی به شرح تصویر (۱) است:



شکل ۱. الگوریتم اجرای دلفی فازی

یکی از فواید تکنیک دلفی فازی نسبت به تکنیک دلفی سنتی، برای غربال شاخص‌ها، آن است که می‌توان از یک مرحله برای تلخیص و غربال متغیرها استفاده کرد. از این‌رو، الگوریتم اجرای تکنیک دلفی فازی شامل گام‌های شکل ۱ است (حبیبی، ایزدیار و سرافزای، ۱۳۹۳، ۳۳؛ نقل در راهداری، نصر، ۱۳۹۶). شناسایی طیف مناسب برای فازی‌سازی عبارات کلامی عبارتند از تجمیع

فازی مقادیر فازی شده، فازی‌زدایی مقادیر، انتخاب شدت آستانه و غربال معیارها است. متغیرهایی که ارزش آن‌ها را لغات یا جملات زبان طبیعی یا زبان‌های مصنوعی تشکیل می‌دهند، متغیر زبانی نامیده می‌شوند (قلی‌پور و محمدزاده، ۱۳۹۳، ۶۸). در جدول (۳) اعداد فازی مثلثی معادل طیف لیکرت پنج‌درجه بیان شده است.

جدول ۳. اعداد فازی مثلثی معادل طیف لیکرت پنج‌درجه

خیلی مهم	مهم	متوسط	کم اهمیت	خیلی کم اهمیت
(۰/۷۵، ۱، ۱)	(۰/۵، ۰/۷۵، ۱)	(۰/۵، ۰/۷۵) (۰/۲۵)	(۰، ۰/۲۵، ۰/۵)	(۰، ۰، ۰/۲۵)

در پژوهش حاضر روش میانگین فازی برای تجمیع دیدگاه خبرگان استفاده شده است. اگر دیدگاه هر خبره به صورت عدد فازی مثلثی (l, m, u) نمایش داده شود، میانگین فازی n عدد فازی مثلثی به صورت رابطه (۱) محاسبه خواهد (حبیبی و همکاران، ۱۳۹۳):

$$F = (l, m, n) \quad \text{رابطه (۱)}$$

پس از تجمیع فازی دیدگاه خبرگان باید به فازی‌زدایی مقادیر به‌دست‌آمده پرداخت. روش‌های مختلفی برای فازی‌زدایی وجود دارد. در این پژوهش از رابطه (۲ و ۳) برای فازی‌زدایی استفاده خواهد شد.

$$X = \frac{l + m + u}{3} \quad \text{رابطه (۲)}$$

$$F_{AVE} = \frac{\sum L}{n}, \frac{\sum m}{n}, \frac{\sum u}{n} \quad \text{رابطه (۳)}$$

۴. یافته‌ها

در این مرحله اطلاعات جمعیت شناختی شرکت‌کنندگان پژوهش حاضر در جدول (۴) قابل مشاهده است:

جدول ۴. اطلاعات جمعیت‌شناختی شرکت‌کنندگان

متغیر	سن			جنسیت		رشته		مدرک تحصیلی		
	۴۰ تا ۵۰	۵۰ تا ۶۰	بالتر از ۵۰ سال	مرد	زن	علم‌اطلاعات و دانش‌شناسی	حقوق	فناوری اطلاعات	کارشناسی ارشد	دکتری
فراوانی	۴	۷	۵	۱۰	۶	۶	۵	۵	۴	۱۲

از این‌رو، در فهرست مؤلفه‌های تأیید شده از سوی صاحب‌نظران به روش دلفی فازی، از ۴۴ مانع استخراج شده، در مجموع ۲۶ مانع در حوزه حریم خصوصی در محیط متاورس در سه مرحله نظر سنجی با روش دلفی فازی تأیید شدند. تعداد پاسخ‌ها در هر مؤلفه به‌ازای ۱۶ خبره که متشکل از شش زن (۳۷/۵ درصد) و ۱۰ مرد (۶۲/۵ درصد) که چهار نفر در مقطع کارشناسی ارشد (۲۵ درصد) و ۱۲ نفر دکتری (۷۵ درصد) پاسخ داده شده است. هرچه تعداد امتیاز داده‌شده به هر یک از مؤلفه‌های حریم خصوصی در محیط متاورس بیشتر باشد، اهمیت مؤلفه بیشتر و تأیید شده است.

جدول (۵) تعداد پاسخ‌ها را در هر مؤلفه به‌ازای ۱۶ خبره پاسخ‌دهنده نشان می‌دهد.

جدول ۵. نتایج شمارش پاسخ‌های مرحله نخست نظر سنجی

مؤلفه‌ها	تعداد ۱	تعداد ۲	تعداد ۳	تعداد ۴	تعداد ۵
ارزش‌های متفاوت فرهنگ‌ها	۰	۰	۰	۰	۱۶

۱۶	۰	۰	۰	۰	کمبود آگاهی
۱۴	۰	۰	۲	۰	نبود فرهنگ حریم خصوصی
۱۲	۰	۲	۲	۰	پرهیز از زندگی واقعی و فیزیکی
۱۴	۰	۰	۲	۰	جعل هویت
۱۵	۰	۰	۱	۰	نبود قوانین مالکیت معنوی
۱۰	۰	۱	۳	۲	انزوای اجتماعی
۱۲	۰	۰	۳	۱	هزینه‌های زیاد تکنولوژی
۱۴	۰	۰	۱	۱	نبود مقررات برای رمز ارزها در تراکنش‌ها
۹	۰	۰	۴	۳	جرایم مالی
۱۴	۰	۰	۲	۰	هزینه‌های حفاظت از داده‌ها
۱۳	۰	۰	۳	۰	هزینه بالای تجهیزات
۱۱	۰	۱	۳	۱	هزینه‌های اجرای قوانین
۱۲	۰	۲	۲	۰	هزینه‌های امینتی
۹	۰	۰	۵	۲	قوانین سخت‌گیرانه دولت‌ها در بخش فناوری
۱۵	۰	۰	۱	۰	خطرات پول‌شویی و تأمین مالی تروریسم
۱۳	۰	۰	۲	۱	نبود قوانین و مقررات بین‌المللی و هماهنگی بین کشورها
۱۵	۰	۰	۱	۰	نشت اطلاعات شخصی
۱۴	۰	۰	۲	۰	شنود، ردیابی، و نظارت
۱۶	۰	۰	۰	۰	کلاهبرداری فیشینگ
۱۱	۰	۰	۳	۲	حفاظت از داده‌ها
۱۳	۰	۰	۳	۰	تبلیغات تهاجمی
۱۴	۰	۰	۲	۰	حملات سایبری
۱۲	۰	۰	۳	۱	نبود مدیریت هویت
۱۵	۰	۰	۰	۱	ضعف در دانش فنی مدیران
۱۱	۰	۰	۲	۳	نبود رقابت عملیاتی هوشمندسازی در بین مدیران
۱۴	۰	۰	۲	۰	افزایش ریسک
۱۰	۰	۰	۰	۶	هدست واقعیت مجازی
۱۱	۰	۰	۰	۵	عینک هوشمند واقعیت مجازی
۱۴	۰	۰	۰	۲	اینترنت پرسرعت
۱۰	۰	۰	۱	۵	استراق سمع آوارتاهای نامرئی
۱۴	۰	۰	۰	۲	نبود امنیت داده‌ها
۱۴	۰	۰	۰	۲	فناوری‌های احراز هویت
۱۴	۰	۰	۱	۱	نبود زیرساخت‌های مقیاس‌پذیر
۱۴	۰	۰	۰	۲	آسیب‌پذیری دستگاه‌ها مانند هولولنز

۱۳	۰	۰	۰	۳	تعامل پذیر نبودن گرافیک‌ها و سخت‌افزارها
۱۱	۰	۰	۰	۵	تأثیرات از خود بیگانگی
۱۲	۰	۰	۰	۴	تأثیر بر سلامتی (اضطراب، افسردگی، حواس پرتی، اختلال شخصیت)
۱۱	۰	۰	۰	۵	سوء استفاده و آزار جنسی
۱۱	۰	۰	۰	۵	اعتیاد به فناوری، قتل، و جنایات خشونت‌آمیز
۱۵	۰	۰	۰	۱	تأثیر بر سلامت جسمی (خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی)
۱۲	۰	۰	۰	۴	نبود پوشش مناسب (اسلامی، ایران)
۱۲	۰	۰	۰	۴	خطرات افراط‌گرایی و ترویج نفرت
۱۲	۰	۰	۰	۴	خطرات برای ایمان و اخلاقیات

تأیید و غربال‌گری شاخص‌ها با مقایسه مقدار ارزش اکتسابی هر شاخص با مقدار آستانه S انجام می‌شود. مقدار آستانه با استنباط ذهنی تصمیم‌گیرنده معین می‌شود و مستقیم بر تعداد عواملی که غربال می‌شوند تأثیر خواهد داشت. هیچ راه ساده و قانونی برای تعیین مقدار آستانه وجود ندارد. در این پژوهش مقدار $0/75$ به‌عنوان مقدار آستانه در نظر گرفته شده است (راهداری و نصر، ۱۳۹۶). برای این کار ابتدا باید مقادیر فازی مثلثی نظرهای خبرگان محاسبه شده، سپس برای محاسبه میانگین نظرات n پاسخ‌دهنده، میانگین فازی آن‌ها محاسبه شود. محاسبه عدد فازی T برای هر یک از شاخص‌ها با استفاده از روابط زیر انجام می‌شود (راهداری و نصر، ۱۳۹۶؛ سیف‌الدین و دیگران، ۱۳۹۶)

$$\bar{t}_{ij} = (a_{ij} \cdot b_{ij} \cdot c_{ij}). \quad i = 1.2. \dots n \quad j = 1.2. \dots m \quad 3-1$$

$$a_j = \sum \frac{a_{ij}}{n} \quad 3-2$$

$$b_j = \sum \frac{b_{ij}}{n} \quad 3-3$$

$$c_j = \sum \frac{c_{ij}}{n} \quad 3-4$$

در روابط بالا اندیس i به فرد خبره و اندیس j به شاخص تصمیم‌گیری اشاره دارد. همچنین مقدار دلفی فازی شده میانگین عدد فازی از رابطه زیر به دست می‌آید (راهداری و نصر، ۱۳۹۶).

$$Crisp = \frac{a + b + c}{3} \quad 3-5$$

جدول (۶). میانگین فازی، میانگین قطعی، و وضعیت نهایی مؤلفه‌ها را براساس میانگین قطعی فازی شده نشان می‌دهد.

جدول ۶. نتایج فازی‌زدایی پاسخ‌های مرحله دوم نظرسنجی

مؤلفه‌ها	میانگین فازی	میانگین قطعی	وضعیت
ارزش‌های متفاوت فرهنگ‌ها	۱/۰۰۰	۰/۹۱۷	تأیید
کمبود آگاهی	۱/۰۰۰	۰/۹۱۷	تأیید

تأیید	۰/۸۳۳	۰/۹۳۸	۰/۹۰۶	۰/۶۵۶	نبود فرهنگ حریم خصوصی
تأیید	۰/۷۸۱	۰/۹۰۶	۰/۸۴۴	۰/۵۹۴	پرهیز از زندگی واقعی و فیزیکی
تأیید	۰/۸۳۳	۰/۹۳۸	۰/۹۰۶	۰/۶۵۶	جعل هویت
تأیید	۰/۸۷۵	۰/۹۶۹	۰/۹۵۳	۰/۷۰۳	نبود قوانین مالکیت معنوی
رد	۰/۶۶۱	۰/۷۹۷	۰/۷۰۳	۰/۴۸۴	انزوای اجتماعی
رد	۰/۷۴۰	۰/۸۵۹	۰/۷۹۷	۰/۵۶۳	هزینه‌های زیاد تکنولوژی
تأیید	۰/۸۲۳	۰/۹۲۲	۰/۸۹۱	۰/۶۵۶	نبود مقررات برای رمز ارزها در تراکنش‌ها
رد	۰/۵۹۴	۰/۷۳۴	۰/۶۲۵	۰/۴۲۲	جرایم مالی
تأیید	۰/۸۳۳	۰/۹۳۸	۰/۹۰۶	۰/۶۵۶	هزینه‌های حفاظت از داده‌ها
تأیید	۰/۷۹۲	۰/۹۰۶	۰/۸۵۹	۰/۶۰۹	هزینه بالای تجهیزات
رد	۰/۷۱۴	۰/۸۴۴	۰/۷۶۶	۰/۵۳۱	هزینه‌های اجرای قوانین
تأیید	۰/۷۸۱	۰/۹۰۶	۰/۸۴۴	۰/۵۹۴	هزینه‌های امنیتی
رد	۰/۶۰۴	۰/۷۵۰	۰/۶۴۱	۰/۴۲۲	قوانین سخت‌گیرانه دولت‌ها در بخش فناوری
تأیید	۰/۸۷۵	۰/۹۶۹	۰/۹۵۳	۰/۷۰۳	خطرات پول‌شویی و تأمین مالی تروریسم
تأیید	۰/۷۸۱	۰/۸۹۱	۰/۸۴۴	۰/۶۰۹	نبود قوانین و مقررات بین‌المللی و هماهنگی بین کشورها
تأیید	۰/۸۷۵	۰/۹۶۹	۰/۹۵۳	۰/۷۰۳	نشست اطلاعات شخصی
تأیید	۰/۸۳۳	۰/۹۳۸	۰/۹۰۶	۰/۶۵۶	شنود، ردیابی، و نظارت
تأیید	۰/۹۱۷	۱/۰۰۰	۱/۰۰۰	۰/۷۵۰	کلاهبرداری فیشینگ
رد	۰/۶۸۸	۰/۸۱۳	۰/۷۳۴	۰/۵۱۶	حفاظت از داده‌ها
تأیید	۰/۷۹۲	۰/۹۰۶	۰/۸۵۹	۰/۶۰۹	تبلیغات تهاجمی
تأیید	۰/۸۳۳	۰/۹۳۸	۰/۹۰۶	۰/۶۵۶	حملات سایبری
رد	۰/۷۴۰	۰/۸۵۹	۰/۷۹۷	۰/۵۶۳	نبود مدیریت هویت
تأیید	۰/۸۶۵	۰/۹۵۳	۰/۹۳۸	۰/۷۰۳	ضعف در دانش فنی مدیران

رد	۰/۶۷۷	۰/۷۹۷	۰/۷۱۹	۰/۵۱۶	نبود رقابت عملیاتی هوشمندسازی در بین مدیران
تأیید	۰/۸۳۳	۰/۹۳۸	۰/۹۰۶	۰/۶۵۶	افزایش ریسک هدست واقعیت مجازی
رد	۰/۶۰۴	۰/۷۱۹	۰/۶۲۵	۰/۴۶۹	عینک هوشمند واقعیت مجازی
تأیید	۰/۸۱۳	۰/۹۰۶	۰/۸۷۵	۰/۶۵۶	اینترنت پرسرعت استراق سمع آوارتاهای نامرئی
رد	۰/۶۱۵	۰/۷۳۴	۰/۶۴۱	۰/۴۶۹	نبود امنیت داده‌ها فناوری‌های احراز هویت
تأیید	۰/۸۱۳	۰/۹۰۶	۰/۸۷۵	۰/۶۵۶	نبود زیرساخت‌های مقیاس پذیر آسیب پذیری
تأیید	۰/۸۱۳	۰/۹۰۶	۰/۸۷۵	۰/۶۵۶	دستگاه‌ها مانند هولولنز تعامل پذیر نبودن
تأیید	۰/۷۶۰	۰/۸۵۹	۰/۸۱۳	۰/۶۰۹	گرافیک‌ها و سخت افزارها تأثیرات از خود بیگانگی
رد	۰/۶۵۶	۰/۷۶۶	۰/۶۸۸	۰/۵۱۶	تأثیر بر سلامتی (اضطراب، افسردگی، حواس پرتی، اختلال شخصیت)
رد	۰/۷۰۸	۰/۸۱۳	۰/۷۵۰	۰/۵۶۳	سوء استفاده و آزار جنسی اعتیاد به فناوری، قتل، و جنایات خشونت آمیز
رد	۰/۶۵۶	۰/۷۶۶	۰/۶۸۸	۰/۵۱۶	تأثیر بر سلامت جسمی (خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی)
تأیید	۰/۸۶۵	۰/۹۵۳	۰/۹۳۸	۰/۷۰۳	نبود پوشش مناسب (اسلامی، ایران)
رد	۰/۷۰۸	۰/۸۱۳	۰/۷۵۰	۰/۵۶۳	

خطرات افراط‌گرایی و ترویج نفرت	۰/۵۶۳	۰/۷۵۰	۰/۸۱۳	۰/۷۰۸	رد
خطرات برای ایمان و اخلاقیات	۰/۵۶۳	۰/۷۵۰	۰/۸۱۳	۰/۷۰۸	رد

م‌شاهده می‌شود مواردی که میانگین قطعی آن‌ها بیشتر از ۰/۷۵ محاسبه شده، تأیید شده‌اند. جدول (۷)، موارد تأیید شده را به‌ترتیب میانگین قطعی نشان می‌دهد.

جدول ۷. فازی‌شده پاسخ‌های مرحله سوم نظرسنجی و تأییدشده

مؤلفه‌ها	میانگین فازی			میانگین قطعی	وضعیت
ارزش‌های متفاوت فرهنگ‌ها	۰/۷۵۰	۱/۰۰۰	۱/۰۰۰	۰/۹۱۷	تأیید
کمبود آگاهی	۰/۷۵۰	۱/۰۰۰	۱/۰۰۰	۰/۹۱۷	تأیید
کلاهبرداری فیشینگ	۰/۷۵۰	۱/۰۰۰	۱/۰۰۰	۰/۹۱۷	تأیید
نبود قوانین مالکیت معنوی	۰/۷۰۳	۰/۹۵۳	۰/۹۶۹	۰/۸۷۵	تأیید
خطرات پول‌شویی و تأمین مالی تروریسم	۰/۷۰۳	۰/۹۵۳	۰/۹۶۹	۰/۸۷۵	تأیید
نشست اطلاعات شخصی	۰/۷۰۳	۰/۹۵۳	۰/۹۶۹	۰/۸۷۵	تأیید
ضعف در دانش فنی مدیران	۰/۷۰۳	۰/۹۵۳	۰/۹۵۳	۰/۸۶۵	تأیید
تأثیر بر سلامت جسمی (خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی)	۰/۷۰۳	۰/۹۵۳	۰/۹۵۳	۰/۸۶۵	تأیید
نبود فرهنگ حریم خصوصی	۰/۶۵۶	۰/۹۰۶	۰/۹۳۸	۰/۸۳۳	تأیید
جعل هویت	۰/۶۵۶	۰/۹۰۶	۰/۹۳۸	۰/۸۳۳	تأیید
هزینه‌های حفاظت از داده‌ها	۰/۶۵۶	۰/۹۰۶	۰/۹۳۸	۰/۸۳۳	تأیید
شنود، ردیابی، و نظارت	۰/۶۵۶	۰/۹۰۶	۰/۹۳۸	۰/۸۳۳	تأیید
حملات سایبری	۰/۶۵۶	۰/۹۰۶	۰/۹۳۸	۰/۸۳۳	تأیید
افزایش ریسک	۰/۶۵۶	۰/۹۰۶	۰/۹۳۸	۰/۸۳۳	تأیید
نبود مقررات برای رمز ارزها در تراکنش‌ها	۰/۶۵۶	۰/۸۹۱	۰/۹۲۲	۰/۸۲۳	تأیید
نبود زیرساخت‌های مقیاس‌پذیر	۰/۶۵۶	۰/۸۹۱	۰/۹۲۲	۰/۸۲۳	تأیید
اینترنت پرسرعت	۰/۶۵۶	۰/۸۷۵	۰/۹۰۶	۰/۸۱۳	تأیید
نبود امنیت داده‌ها	۰/۶۵۶	۰/۸۷۵	۰/۹۰۶	۰/۸۱۳	تأیید
فناوری‌های احراز هویت	۰/۶۵۶	۰/۸۷۵	۰/۹۰۶	۰/۸۱۳	تأیید
آسیب‌پذیری دستگاه‌ها مانند هولولنز	۰/۶۵۶	۰/۸۷۵	۰/۹۰۶	۰/۸۱۳	تأیید
هزینه بالای تجهیزات	۰/۶۰۹	۰/۸۵۹	۰/۹۰۶	۰/۷۹۲	تأیید
تبلیغات تهاجمی	۰/۶۰۹	۰/۸۵۹	۰/۹۰۶	۰/۷۹۲	تأیید
پرهیز از زندگی واقعی و فیزیکی	۰/۵۹۴	۰/۸۴۴	۰/۹۰۶	۰/۷۸۱	تأیید
هزینه‌های امنیتی	۰/۵۹۴	۰/۸۴۴	۰/۹۰۶	۰/۷۸۱	تأیید
نبود قوانین و مقررات بین‌المللی و هماهنگی بین کشورها	۰/۶۰۹	۰/۸۴۴	۰/۸۹۱	۰/۷۸۱	تأیید
تعامل‌پذیر نبودن گرافیک‌ها و سخت‌افزارها	۰/۶۰۹	۰/۸۱۳	۰/۸۵۹	۰/۷۶۰	تأیید

برای دستیابی و شناخت بهتر و وضعیت و تعیین اولویت موانع حریم خصوصی کاربران بر اساس رتبه‌بندی به دست آمده از مدل کوکوسو و به لحاظ برخورداری از شاخص‌های مطالعه، در چهار سطح کم برخورداری، نیمه برخورداری، برخورداری و خیلی برخورداری طبقه بندی شدند. در نهایت آخرین جدول (۸)، امتیازات نهایی هر عامل را نشان می‌دهد و ملاک اولویت‌بندی نهایی خواهد بود.

جدول ۸. رتبه‌بندی عوامل

Ranks	K	Ranks	KC	Ranks	kb	Ranks	ka	شاخص‌ها
۱۹	۲/۹۳۹۴۲۹۶۰۷	۲۲	۰/۸۷۶۳۸۲۹۹۱	۱۹	۶/۱۵۲	۲۱	۰/۰۳۷	ارزش‌های متفاوت فرهنگ‌ها
۲۲	۲/۷۶۱۲۹۶۷۲	۸	۰/۹۴۷۴۳۱۳۷۴	۲۳	۵/۵۱۶	۸	۰/۰۴	کمبود آگاهی
۲۵	۲/۳۳۳۱۹۷۸۸۹	۲۵	۰/۷۸۰۳۹۵۹۰۹	۲۵	۴/۷۰۲	۲۵	۰/۰۳۳	کلاهبرداری فیشینگ
۱۸	۳/۰۳۲۶۵۳۳۹۴	۱۹	۰/۹۲۷۵۷۶۱۰۲	۱۸	۶/۲۹۹	۱۵	۰/۰۳۹	نبود قوانین مالکیت معنوی
۲۳	۲/۷۵۳۴۳۸۶۹۹	۲۳	۰/۸۶۱۴۹۱۵۳۸	۲۲	۵/۶۸۱	۲۳	۰/۰۳۶	خطرات پول‌شویی و تأمین مالی تروریسم
۲	۳/۳۱۵۱۰۳۲۳۹	۲	۰/۹۹۸۹۸۳۳۱۴	۲	۶/۹۱۸	۱	۰/۰۴۲	نشت اطلاعات شخصی
۱۱	۳/۱۵۰۷۷۱۲۳۶	۱۳	۰/۹۳۹۴۷۷۳۰۴	۱۰	۶/۵۸۹	۸	۰/۰۴	ضعف در دانش فنی مدیران
								تأثیر بر سلامت جسمی (خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی)
۱۰	۳/۱۵۷۵۷۵۴۱۷	۱۲	۰/۹۳۹۸۹۵۹۳۹	۹	۶/۶۰۷	۸	۰/۰۴	نبود فرهنگ حریم خصوصی
۲۱	۲/۸۹۵۷۱۵۹۴۹	۲۰	۰/۹۱۵۶۷۴۹	۲۱	۵/۹۴۳	۱۵	۰/۰۳۹	جعل هویت
۱	۰/۳۳۱۷۳۴۵۶۸	۱	۱	۱	۶/۹۶۲	۱	۰/۰۴۲	هزینه‌های حفاظت از داده‌ها
۲۶	۰/۹۷۲۶۴۴۹۷۹	۲۶	۰/۳۰۶۰۲۲۳۶۷	۲۶	۲	۲۶	۰/۰۱۳	شوند، ردیابی و نظارت
۶	۳/۱۹۹۳۴۶۱۹۳	۹	۰/۹۴۳۴۸۴۲۴۱	۶	۶/۷۱۶	۸	۰/۰۴	حملات سایبری
۱۴	۳/۰۶۵۰۳۸۵۶۶	۱۵	۰/۹۳۳۲۵۷۵۸	۱۴	۶/۳۷۹	۱۵	۰/۰۳۹	افزایش ریسک
۱۲	۳/۱۱۶۱۳۸۵۳۸	۱۴	۰/۹۳۵۶۴۹۷۸۲	۱۲	۶/۵	۸	۰/۰۴	نبود مقررات برای رمز ارزها در تراکنش‌ها
۱۷	۳/۰۴۰۹۸۴۶۱	۱۸	۰/۹۳۱۴۰۳۶۲۴	۱۷	۶/۳۱۶	۱۵	۰/۰۳۹	نبود زیرساخت‌های مقیاس‌پذیر
۸	۳/۱۷۵۳۵۱۵۸۱	۶	۰/۹۸۷۶۸۰۱۶۳	۱۱	۶/۵۵۳	۱	۰/۰۴۲	اینترنت پرسرعت
۱۵	۳/۰۵۶۷۹۹۵۴۸	۱۶	۰/۹۳۲۸۹۸۷۵	۱۵	۶/۳۵۷	۱۵	۰/۰۳۹	نبود امنیت داده‌ها
۴	۳/۲۹۰۴۶۳۳۶۸	۴	۰/۹۹۶۷۱۰۷۲۳	۴	۶/۸۵۴	۱	۰/۰۴۲	فناوری‌های احراز هویت
۹	۳/۱۵۹۵۶۶۹۶۳	۱۱	۰/۹۴۰۱۹۴۹۶۴	۸	۶/۶۱۲	۸	۰/۰۴	آسیب‌پذیری دستگاه‌ها مانند هولولنز
۷	۳/۱۹۲۴۸۸۰۶۳	۱۰	۰/۹۴۲۹۴۵۹۹۶	۷	۶/۶۹۸	۸	۰/۰۴	هزینه بالای تجهیزات
۲۴	۲/۶۲۶۸۹۰۹۴۷	۲۴	۰/۸۵۲۸۱۹۸۰۷	۲۴	۵/۳۴۹	۲۳	۰/۰۳۶	تبلیغات تهاجمی
۲۰	۲/۹۲۶۸۵۱۹۵۵	۲۱	۰/۸۷۶۷۴۱۸۲۲	۲۰	۶/۱۱۷	۲۱	۰/۰۳۷	پرهیز از زندگی واقعی و فیزیکی
۱۶	۳/۰۴۴۱۰۵۶۶۲	۱۷	۰/۹۳۲۴۲۰۳۱	۱۶	۶/۳۲۳	۱۵	۰/۰۳۹	هزینه‌های امنیتی

۱۳	۳/۱۱۰۲۶۸۹۳	۷	۰/۹۸۲۶۵۶۵۴	۱۳	۶/۳۸۳	۱	۰/۰۴۲	نبود قوانین و مقررات بین‌المللی و هماهنگی بین کشورها
۳	۳/۳۰۸۶۲۸۶۷۱	۳	۰/۹۹۸۵۰۴۸۷۴	۳	۶/۹۰۱	۱	۰/۰۴۲	تعامل‌پذیر نبودن گرافیک‌ها و سخت‌افزارها

بر اساس امتیازات هر عامل در جدول (۸)، هزینه‌های حفاظت از داده‌ها، نشت اطلاعات شخصی، تعامل‌پذیر نبودن گرافیک‌ها و سخت‌افزارها به‌ترتیب دارای بیشترین اولویت هستند.

۵. بحث و نتیجه‌گیری

متاورس یکی از موضوعات مهم قرن حاضر است که تمام جنبه‌های اقتصادی، اجتماعی، فرهنگی، سیاسی، امنیتی، روان‌شناختی، و دینی دنیای واقعی را فرا گرفته است. در واقع متاورس، نحوه تعامل افراد با یکدیگر و فناوری را تغییر می‌دهد و یکی از مباحث خیلی مهمی که در این فناوری مطرح است حریم خصوصی کاربران است. از این‌رو، پژوهش حاضر با هدف شناسایی موانع حریم خصوصی کاربران در محیط متاورس انجام شده است. ابتدا با مرور پیشینه‌ها و مصاحبه با خبرگان در زمینه متاورس، حریم خصوصی، حقوق، هوش مصنوعی، علم اطلاعات و دانش‌شناسی، و فناوری‌های نوین، ۴۴ مانع شناسایی شد. این موانع با توزیع پرسش‌نامه در بین خبرگان و با استفاده از روش دلفی فازی غربال و ۲۶ مانع برای تحلیل نهایی انتخاب شدند. براساس نمرات کسب شده سه مانع شامل هزینه‌های حفاظت از داده‌ها، نشت اطلاعات شخصی، و تعامل‌پذیر نبودن گرافیک‌ها و سخت‌افزارها به‌ترتیب دارای بیشترین اولویت هستند.

یافته‌ها نشان داد که حفاظت از حریم خصوصی در فضای متاورس به یک چالش چندوجهی تبدیل شده است که نیازمند توجه به مسائل فرهنگی، آموزشی و فناورانه، سیاسی، مدیریتی و غیره است. یکی از بارزترین و مهمترین موانع شناسایی شده در پژوهش حاضر، هزینه‌های حفاظت از داده‌ها است. این مانع در واقع بازتاب‌دهنده پیچیدگی‌ها و چالش‌های اقتصادی و فنی مربوط به جمع‌آوری، ذخیره‌سازی، پردازش، و انتقال داده‌های کاربران در دنیای متاورس است. سیستم‌های حفاظت از داده‌ها نیازمند زیرساخت‌های فناوری پیشرفته‌ای هستند که هزینه‌هایی را برای پیاده‌سازی و نگهداری به‌دنبال دارند. این زیرساخت‌ها شامل سیستم‌های رمزنگاری، فایروال‌ها، نرم‌افزارهای امنیتی، و پروتکل‌های امنیتی پیچیده‌ای هستند که همه آن‌ها مستلزم سرمایه‌گذاری‌های کلان در زمینه سخت‌افزار و نرم‌افزار هستند. به‌ویژه در فضای متاورس که تبادل داده‌ها به صورت گسترده و در زمان واقعی انجام می‌شود، نیاز به سیستم‌های امنیتی که بتوانند به‌طور مؤثر از اطلاعات شخصی و هویتی کاربران حفاظت کنند، بیشتر از هر زمان دیگری احساس می‌شود. از این‌رو، پژوهش‌های مختلف در داخل و خارج کشور از جمله یگانه و فامیل‌سعدیان (۱۴۰۱)، محمودی و صادقی (۱۴۰۱)، میراشرفی (۱۴۰۱)، مرادی‌برلیان (۱۴۰۱)، محمدباقری و سیدباقری (۱۴۰۱)، داراب‌پور (۱۴۰۲) و پژوهش‌های خارجی از جمله دوویدی و همکاران (۲۰۲۳)، وانگ و همکاران (۲۰۲۳)، تورال و کوچاک (۲۰۲۳)، که در پژوهش‌های خود به هزینه‌های حفاظت از داده‌ها پرداخته‌اند هم‌سو هستند. و در پژوهش‌های داخلی شهریاری (۱۴۰۱)، و شاه‌مرادی (۱۴۰۱) و در پژوهش‌های خارجی سایید (۲۰۲۳) و زو (۲۰۲۴) نیز به‌طور مشترک بر این مسئله تأکید کرده‌اند که نیاز به هزینه‌های حفاظت از داده‌ها در این حوزه از اهمیت بالایی برخوردار است.

مانع دوم مربوط به نشت اطلاعات شخصی در محیط متاورس است. نشت اطلاعات شخصی در متاورس یکی از پیچیده‌ترین و چالش‌برانگیزترین مسائل امنیتی در دنیای دیجیتال کنونی است. با توجه به ویژگی‌های منحصر به فرد این فضای مجازی و تعاملات گسترده‌ای که در آن انجام می‌شود، تهدیدات امنیتی در این محیط‌ها می‌توانند بسیار پیچیده‌تر و تأثیرگذارتر از سایر فضاهای آنلاین باشند. این تهدیدات نه تنها حریم خصوصی کاربران را تهدید می‌کنند، بلکه می‌توانند به اعتبار و شهرت پلتفرم‌های متاورس آسیب‌های جبران‌ناپذیری وارد کنند. پژوهش‌های مختلف از جمله لطیف‌زاده و قلوبولی‌درافشان (۱۴۰۲)، دوویدی و همکاران (۲۰۲۲)، کیم و همکاران (۲۰۲۳)، جین پاتل (۲۰۲۴)، شی و زو (۲۰۲۴)، و دیزجی و دیزجی (۲۰۲۴) در پژوهش خود به نشت اطلاعات شخصی پرداخته‌اند که با یافته این پژوهش هم‌سو است.

مانع سوم مربوط به تعامل پذیر نبودن گرافیک‌ها و سخت‌افزارها در محیط متاورس است. تعامل پذیر نبودن گرافیک‌ها و سخت‌افزارها در محیط متاورس یکی از چالش‌های اساسی است که می‌تواند به‌طور مستقیم بر تجربه کاربران و کارایی سیستم‌ها در این فضا تأثیر داشته باشد. در واقع، متاورس به‌طور اساسی بر تجربه‌های بصری، صوتی، و حسی استوار است که نیازمند هماهنگی دقیق میان سخت‌افزار و نرم‌افزار است. به عبارتی برای ایجاد یک محیط متاورس کارآمد و مقیاس پذیر، لازم است که توسعه‌دهندگان، تولیدکنندگان سخت‌افزار، و نهادهای استاندارد سازی همکاری کنند تا یکپارچگی میان گرافیک‌ها و سخت‌افزارها را تضمین کنند و مشکلات موجود را برطرف سازند. همچنین نتایج این مانع با نتایج پژوهش شهریاری و همکاران (۱۴۰۱) هم‌سو است.

برای رفع موانع حریم خصوصی کاربران در محیط متاورس، می‌توان اقدامات و تدابیری را در نظر گرفت. در واقع، تعیین وضوح درباره حقوق حریم خصوصی کاربران با قوانین و مقررات متاورس، به‌ویژه در قسمت‌هایی که به جمع‌آوری، استفاده، و انتقال داده‌های شخصی مرتبط است. این قوانین باید به‌طور کامل و قابل فهم برای تمام کاربران در دسترس باشند. فراهم کردن ابزارها و تنظیمات مدیریت دقیق دسترسی‌ها و اطلاعات شامل کنترل‌های خصوصی، مدیریت مجوزها، و قابلیت‌های انتخابی برای کاربران است تا حریم خصوصی آن‌ها بهتر حفظ شود. استفاده از استانداردهای قوی رمزنگاری برای حفاظت از داده‌های شخصی در حین انتقال و ذخیره‌سازی ضروری است. همچنین، تضمین امنیت فنی برای جلوگیری از دسترسی غیرمجاز به اطلاعات شخصی و ارائه اطلاعات به کاربران درباره جمع‌آوری، استفاده و به اشتراک‌گذاری داده‌ها، به‌همراه توضیحات مربوط به اهداف و مدت زمان نگهداری اطلاعات، از اهمیت بالایی برخوردار است. در نهایت، باید اطمینان حاصل شود که کاربران از حقوق خود و نحوه محافظت از حریم خصوصی‌شان آگاه هستند. ارائه ابزارها و گزینه‌هایی به کاربران برای دسترسی، اصلاح، و حذف داده‌های شخصی‌شان به آن‌ها این امکان را می‌دهد که به راحتی داده‌های خود را مدیریت کنند. همچنین، آموزش در مورد روش‌های حفظ حریم خصوصی و اجتناب از خطرات امنیتی در محیط متاورس، آگاهی کاربران را تقویت و به تصمیم‌گیری مسئولانه آن‌ها کمک می‌کند. این اقدامات می‌توانند به بهبود حفظ حریم خصوصی و افزایش اعتماد کاربران به پلتفرم‌های متاورس منجر شوند. همچنین پیشنهاد می‌شود پژوهشگران به بررسی حریم خصوصی در بلاک‌چین‌ها و هوش مصنوعی پرداخته و چالش‌ها و موانع موجود را شناسایی کرده و راهکارهایی برای رفع آن‌ها ارائه دهند.

۶. فهرست منابع

- بحرینی، م.، نوروزی، ف.، صابری، ن.، و فولادی‌قلعه، ک. (۱۴۰۱). نقش سایبرنتیک در پیدایش هوش مصنوعی. فلسفه علم، پژوهشگاه علوم انسانی و مطالعات فرهنگی دو فصلنامه علمی، ۱۲(۱)، ۲۵-۳. doi:10.30465/ps.2022.42060.1618
- پاشایی، ص. (۱۳۹۹). دنیای متاورس. فصلنامه دانش انتظامی آذربایجان شرقی، ۱۰(۳۹)، ۱۸۱-۲۱۳. http://eastaz.jrl.police.ir/article_99095.html
- حبیبی، الف.، ایزدیار، ص.، و سرافرازی، الف. (۱۳۹۳). تصمیم‌گیری چندمعیاره فازی. کتبه گیل.
- حدادعراقی، س. (۱۴۰۱). کاربرد متاورس در آموزش (ویژگی‌ها، فرصت‌ها و چالش‌ها). هفتمین کنفرانس ملی رویکردهای نوین (آموزش و پژوهش مازندران). <https://civilica.com/doc/1619874/>. ۱۱-۱
- حسن‌زاده، م. (۱۴۰۱). متاورس و سرنوشت سامانه‌های اطلاعاتی. علوم و فنون مدیریت اطلاعات، ۸(۱)، ۷-۱۴. doi: 10.22091/stim.2022.2139
- داراب‌پور، م. (۱۴۰۲). متاورس؛ چیستی و چالش‌های حقوقی (اداره، اشخاص و اموال). فصلنامه حقوق فناوری‌های نوین، ۴(۷)، ۶۵-۸۱. doi: 10.22133/MTLJ.2023.366623.1130
- رضایی نور، ج. و کریمی‌ان، ر. (۱۴۰۳). شناسایی موانع توسعه‌ای متاورس در کتابخانه‌های دیجیتال مبتنی بر نظریه مبنایی. فصلنامه بازیابی دانش و نظام‌های معنایی. doi: 10.22054/jks.2023.76141.1617۰
- رضائی ملال، س. و مرتضائی‌دکاهی، ق. (۱۴۰۱). مطالعه روش‌های امنیت و حفظ حریم خصوصی در متاورس. سیزدهمین کنفرانس بین‌المللی راهکارهای نوین در مهندسی. علوم اطلاعات و فناوری در قرن پیش‌رو. <https://civilica.com/doc/1595469>
- راهداری، ع. و نصر، م. (۱۳۹۶). چالش‌های اتاق فکر در ایران. فرایند مدیریت و توسعه، ۳۰(۲)، ۵۴-۲۳. <https://jmdp.ir/article-1-2727-fa.html>
- شاه‌مرادی، و. (۱۴۰۱). ارزیابی و رتبه‌بندی عوامل موثر بر پیاده‌سازی متاورس در بخش کنترل و بازرسی کشتی‌ها استان هرمزگان. پژوهش‌های نوین علوم مهندسی، ۷(۵)، ۶۰-۴۷. <http://nres.ir/post.aspx?id=796>
- شهریاری، ح. (۱۴۰۱). هستی و چیستی متاورس پیوند میان خیال و واقعیت. فصلنامه اطلاع‌رسانی، آموزش، و مطالعات رایانه‌ای، ۷۸، ۱-۱۳. <https://www.rahavardnoor.ir/index.php/component/k2/item/1029-hasti-va-chisti-metaverse>

- ضرغام‌پروجنی، ح.، و عزیزی، ف. (۱۳۹۶). ارزیابی عوامل مؤثر بر توسعه گردشگری محوطه‌های باستانی- تاریخی (رویکرد فازی). تاریخ و فرهنگ، (۲)۴۹، ۳۲-۹. doi: 10.22067/jhc.v49i2.73024
- محمدزاده، ل.، و قلی‌پور، م. (۱۳۹۳). منطق فازی برای دانشجویان مدیریت. آتی‌نگر.
- لطیف‌زاده، م. و قیولی‌درفشان، م. (۱۴۰۲). معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل. مطالعات حقوق خصوصی، (۲)۵۳، ۳۴۹-۳۷۲. doi: 10.22059/jlq.2023.353867.1007743
- محمدباقری، ز.، و سیدباقری، م. (۱۴۰۱). مد سریع در جهان مادی و متاورس. فصلنامه علمی مطالعات حقوقی فضای مجازی، (۴)۱، ۶۵-۷۶. doi: 10.30495/CYBERLAW.2023.699220
- محمودی، م. و صادقی، س. (۱۴۰۱). متاورس و تأثیر آن بر سبک زندگی. فصلنامه مطالعات حقوقی فضای مجازی، (۲)۱، ۶۲-۴۴. doi: 10.30495/cyberlaw.2022.693926
- مرادی برلیان، م. (۱۴۰۱). درآمدی بر پیامدها و چالش‌های حقوقی متاورس. فصلنامه حقوقی و ویژه‌نامه حقوق و فناوری. doi: 10.52547/JLR.2022.228286.2279
- مردیان، ع.، و پورغفاری‌بشری، ع. (۱۴۰۱). بررسی رویکرد نظامی در متاورس و چالش‌های امنیتی پیش‌رو. نخستین کنفرانس بین‌المللی فناوری متاورس، بلاکچین و ارزش‌های دیجیتال، تهران، اسفند. ۱-۶. <https://civilica.com/doc/1661492/>
- میراشرفی، الف. (۱۴۰۱). بررسی و تحلیل علمی دنیای متاورس و چشم‌انداز آینده آن. فصلنامه رهیافت نوین در مطالعات اسلامی، ۴۰۴-۳۸۸. <https://civilica.com/doc/1880162>
- یگانه، ح.، و فامیل‌سعدیان، ف. (۱۴۰۱). بررسی و تحلیل چالش‌های حقوقی آواتارها در زیست بوم متاورس. فصلنامه نشاء علم، (۱)۱۳، ۳۳-۴۲. https://www.sciencecultivation.ir/article_701765.html?lang=fa

References

- Anidjar, L. Y., Packin, N. G., & Panezi, A. (2023). The Matrix Of Privacy: Data Infrastructure In The Ai-Powered Metaverse. *Harvard Law & Policy Review*, 18, 1-55. doi: 10.2139/ssrn.4363208
- Babai, S., Bahreini, M., Norouzi, F., Saberi, N., & Fouladi, K. (2022). The role of Cybernetics in the emergence of artificial intelligence. *Philosophy of Science*, 12(1), 1-25. doi: 10.30465/ps.2022.42060.1618. [In Persian]
- Dizaji, A., & Dizaji, A. (2023). Metaverse and its legal challenges. *Synesis*, 15(1), 138-151. <https://link.gale.com/apps/doc/A780930134/AONE?u=anon~8b2a4c19&sid=sitemap&xid=9e859794>
- Darabpour, M. R. (2023). Metaverse; Nature and Legal Challenges (Governance, Persons and Property). *Modern Technologies Law*, 4(7), 65-81. doi: 10.22133/mtlj.2023.366623.1130. [In Persian]
- Durkstra, S. (2023). *Navigating the Ethical Minefield of the Metaverse: Exploring the Privacy, Safety and Security of the Virtual World*. (Bachelor's thesis, University of Twente).
- Dwivedi, Y. K., Kshetri, N., Hughes, L., Rana, N. P., Baabdullah, A. M., Kar, A. K., ... & Yan, M. (2023). Exploring the darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. *Information Systems Frontiers*, 25(5), 2071-2114. doi: 10.1007/s10796-023-10400-x
- Habibi, A., Izdiyar, S., & Serafraz, A. (2013). *Fuzzy multi-criteria decision making*. Gil inscription. [In Persian]
- Haddad-Iraqi, S. (2022). Application of metaverse in education (features, opportunities and challenges). *The 7th National Conference on New Approaches (Education and Research, Mazandaran)*. 1-11. [In Persian]
- Hassanzadeh, M. (2022). Metaverse and the Fate of Information Systems. *Sciences and Techniques of Information Management*, 8(1), 7-14. doi: 10.22091/stim.2022.2139. [In Persian]
- Jane Patel, N. (2024). Exploring the implications of the metaverse: opportunities and challenges for dance movement therapy. *Body, Movement and Dance in Psychotherapy*, 1-12. doi: 10.1080/17432979.2024.2306581
- Kim, M., Oh, J., Son, S., Park, Y., Kim, J., & Park, Y. (2023). Secure and Privacy-Preserving Authentication Scheme Using Decentralized Identifier in Metaverse Environment. *Electronics*, 12(19), 4073. doi: 10.3390/electronics12194073

- Latifzadeh, M., & qabuli dorafshan, S. M. M. (2023). Introducing Digital Identity in Metaverse, Identifying Related Legal Challenges and Solutions. *Law Quarterly*, 53(2), 349-372. doi: 10.22059/jlq.2023.353867.1007743. [In Persian]
- Mahmoudi, M., & Sadeghi, S. (2022). Metaverse and Its Impact on Lifestyle. *Legal Studies of Cyberspace*, 1(2), 44-62. doi: 10.30495/cyberlaw.2022.693926. [In Persian]
- Miller, MR., Jun, H., Herrera, F., Yu Villa, J., Welch, G., & Bailenson, JN. (2019) Social interaction in augmented reality. *PLoS ONE*, 14(5), e0216290. doi: 10.1371/journal.pone.0216290
- Mirasharafi, A. H. (2022). Scientific review and analysis of the Metaverse world and its future prospects. *New Approach in Islamic Studies Quarterly*, 388-404. <https://civilica.com/doc/1880162>. [In Persian]
- Mohammadbagheri, Z., & Seyed Bagheri, M. (2022). Fast Fashion in Real World and Metaverse. *Scientific Quarterly Journal of Legal Studies of Virtual Space*, 1(4). 65-76. doi: 10.30495/CYBERLAW.2023.699220. [In Persian]
- Mohammadzadeh, L., & Gholipour, M. (2014). Fuzzy Logic for Management Students. *Ati-Negar*. [In Persian]
- Mosco, V. (2023). Into the metaverse: technical challenges, social problems, utopian visions, and policy principles. *Javnost-The Public*, 30(2), 161-173. doi: 10.1080/13183222.2023.2200688
- Moradian, A., & Pourghafari Bushra, A. (2022). Investigation of the military approach in the metaverse and upcoming security challenges. *The first international conference on Metaverse technology, blockchain and digital currencies*, Tehran, February. 1-6. <https://civilica.com/doc/1661492/> [In Persian]
- Moradiberelian, M. (2023). An Introduction to the Implications and Legal Challenges of Metaverse. *Legal Research Quarterly*, 25(Special Issue of Law & Technology), 363-392. doi: 10.52547/jlr.2022.228286.2279. [In Persian]
- Mystakidis, S. (2023). Metavers. *Encyclopeedia*. 2(1). 486-497. doi.: 10.3390/encyclopedia2010031
- Orland, K. (2021). So what “the metaverse. exactly? *Ars Technica*. <https://arstechnica.com/gaming/2021/11/everyonepitchingthemetaversehasadifferentideaofwhatitis/#:~:text=In%20an%20idealized%20metaverse%2C%20every,subset%20of%20users%20can%20interact>.
- Pashaei, S. (2021). Metaverse world. *East police Azarbaijan science*, 10(39), 181-213. http://eastaz.jrl.police.ir/article_99095.html?lang=en. [In Persian]
- Rahdary A, Nasr M. (2017). Challenges of Think Tanks in Iran. *JMDP*, 30(2), 23-54. <http://jmdp.ir/article-1-2727-fa.html>. [In Persian]
- Rezaemalal, S., & Mortezaadekahi, Q. (2022). Study of security and privacy protection methods in Metaverse.. *The 13th international conference on new solutions in engineering*. Information science and technology in the coming century. <https://civilica.com/doc/1595469>. [In Persian]
- Rezaeenour, J., & Karimian, R. (2024). Identifying Metaverse Developments in Digital Libraries Based on Library Theory. *Knowledge Retrieval and Semantic Systems*, 11(39), 67-108. doi: 10.22054/jks.2023.76141.1617. [In Persian]
- Said, G. R. E. (2023). Metaverse-based learning opportunities and challenges: a phenomenological Metaverse human-computer interaction study. *Electronics*, 12(6), 1379. doi: 10.3390/electronics12061379
- Shahmoradi, V. (2022). Evaluation and ranking of factors affecting the implementation of Metaverse in the ship control and inspection department of Hormozgan province. *New Researches in Engineering Sciences*, 7(5), 47-60. <http://nres.ir/post.aspx?id=796>. [In Persian]
- Shahriari, H. (2022). The existence and whatness of the metaverse is the link between fantasy and reality. *Quarterly Journal of Information, Education, and Computer Studies*, 78, 1-13. <https://www.rahavardnoor.ir/index.php/component/k2/item/1029-hasti-va-chisti-metaverse>. [In Persian]
- Shaun Nichols. (2022). Metaverse rollout brings new security risks, challenges. <https://www.techtarget.com/searchsecurity/news/252513072/Metaverserolloutbringsnew-securityrisks-challenges>
- Shi, L., & Zhu, H. (2024). A study of user data privacy protection algorithms in the context of metaverse based on emotional AI IoT. *Applied Mathematics and Nonlinear Sciences*, 9(1), 1-18. doi: 10.2478/amns.2023.2.00636

- Tural, A., & Koçak, N. (2023). Awareness levels of social studies pre-service teachers regarding metaverse use. *Advanced Education*, 69-86. doi: 10.20535/2410-8286.284683
- Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. *IEEE Communications Surveys & Tutorials*, 25(1), 319-352. doi.: 10.1109/COMST.2022.3202047
- Yeganeh, H., & Famil Saeedian, F. (2022). Investigating and Analyzing the Legal Challenges of Avatars in The Metaverse Ecosystem. *Science Cultivation*, 13(1), 33-41. https://www.sciencecultivation.ir/article_701765.html?lang=en
- Zargham Borujeni, H., & Azizi, F. (2017). Evaluation of the Factors Effective on Development of Ancient-Historical Sites Tourism (Fuzzy Approach). *Journal of History and Culture*, 49(2), 9-32. doi: 10.22067/jhc.v49i2.73024. [In Persian]