Sciences and Techniques of
Information Management
Volume 11, Issue 4, 2025
https://stim.qom.ac.ir

# The identification of barriers to user privacy in the metaverse environment

**Saeed Rezaei Sharifabadi[1] and Hadiseh Heidari[2]✉**

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**

**Article type:**
Review Article

**Article history:**
Received: 2025/12/04
Received in revised form: 2025/12/12
Accepted: 2026/01/21
Published online: 2026/01/28

**Keywords:**
Metaverse, barriers, users, privacy, challenges, Fuzzy Delphi.

**ABSTRACT**

**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.

**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.

**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

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


DOI: 10.22091/STIM.2025.11546.2176

**Publisher**: University of Qom

علوم و فنون مدیریت اطلاعات

دوره ۱۱، شماره ۴، ۱۴۰۴

https://stim.qom.ac.ir

# شناسایی موانع حریم خصوصی کاربران در محیط متاورس

سعید رضایی شریف‌آبادی[۱] و حدیثه حیدری[۲]✉

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

۲. دانشجوی دکتری علم اطلاعات و دانش‌شناسی، گروه علم اطلاعات و دانش‌شناسی، دانشکده علوم تربیتی و روان‌شناسی، دانشگاه الزهرا (نویسندهٔ مسئول). رایانامه: h.heidari174@gmail.com

**اطلاعات مقاله**

**نوع مقاله:** مقاله مروری

**تاریخ دریافت:** ۱۴۰۴/۰۹/۱۳

**تاریخ بازنگری:** ۱۴۰۴/۰۹/۲۱

**تاریخ پذیرش:** ۱۴۰۴/۱۱/۰۱

**تاریخ انتشار:** ۱۴۰۴/۱۱/۰۸

**چکیده**

**هدف:** متاورس موضوعی است که به‌طور گسترده مورد علاقهٔ عموم قرار گرفته است.افراد و سازمان‌ها به‌طور یکسان در مورد کاربردهای بالقوهٔآن 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.

**روش‌شناسی:** این پژوهش از نظر هدف کاربردی و از لحاظ شیوهٔ گردآوری داده‌ها پیمایشی است. ابتدا با بررسی ادبیات حوزهٔ متاورس، موانع حریم خصوصی در این حوزه مشخص شدند و سپس برای شناسایی مهمترین موانع که بر توسعهٔ متاورس مؤثر هستند و خبرگان در مورد آن‌ها اتفاق نظر دارند، از فنون دلفی فازی برای تحلیل داده‌ها، استفاده شده است. جامعهٔ آماری پژوهش حاضر را خبرگان صاحب‌نظر در زمینهٔ متاورس، حریم‌خصوصی، حقوق، هوش‌مصنوعی، 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 حوزهٔ متاورس، ابتدا با استفاده از مرور ادبیات و پیشینهٔ پژوهش، تعداد ۴۴ مانع برای حریم خصوصی کاربران در محیط متاورس استخراج کردند و سپس با یک پرسش‌نامهٔ نیمه‌ساختارمند از خبرگان درخواست شد که براساس طیف پنج‌تایی لیکرت، تأثیر شاخص‌ها را مشخص کنند. برای گردآوری نظرات خبرگان در انتهای شش مؤلفهٔ پژوهشیک سؤال باز نوشته شده و از خبرگان خواسته شد که علاوه‌بر 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.

**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، تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها به‌ترتیب، 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 درواقع بازتاب‌دهندهٔ 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

**کلیدواژه‌ها:**

متاورس، موانع، کاربران، حریم خصوصی، چالش‌ها، دلفی‌فازی.

است. با توجه به ویژگی‌های منحصربه‌فرد 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. همچنین مانع سوم مربوط به تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها در محیط متاورس است. تعامل‌پذیرنبودنِ 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 شـــامل ترکیبی از افزایش آگاهی عمومی، توســـعهٔ 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 اســت، توجه به این مســائل نه‌تنها برای حفاظت از حریم خصــوصــی افراد، بلکه برای ایجاد محیطی امن و قابل اعتماد در این فضا، امری ضروری است.

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

ناشر: دانشگاه قم

## ۱. مقدّمه

امروزه صحبت از فضای مجازی یا سایبری، فضای دیجیتال، فضای اینترنتی، فضای الکترونیکی، و غیره امری معمول و واقعیتی انکارناپذیر به شمار می‌رود. فضاهای نوینِ مبتنی‌بر 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). توسعهٔ 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، سه‌بُعدی، و دیجیتالی است که از ترکیب واژه یونانی متا[۲] + ورس[۳] به‌معنای جهان مجازی سه‌بُعدی 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، اولین‌بار در رمان علمی تخیلی نیل استفنسون[۴] با عنوان «سقوط برف» در سال ۱۹۹۲ به کار رفت. در این کتاب، متاورس به‌مثابه 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 مفاهیمواقعیت مجازی[۵] و واقعیت افزوده[۶]، به‌دنبال 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، نبودِ قوانین روشن برای مالکیت معنوی، و هویت و جعل هویت توجه کردند. سعید[۱۰] (۲۰۲۳) در پژوهش خود به مواردی همانند ایجاد شکاف اجتماعی، انزوای اجتماعی، و پرهیز اززندگی واقعی و فیزیکی توجه کرده‌اند. مرادی‌برلیان (۱۴۰۱) به هزینه‌های حفاظت از داده‌ها، هزینه‌های آگاهی، هزینه‌های امنیتی، و هزینه های 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 نشت داده‌ها و کیم و دیگران[۱۲] (۲۰۲۳) نشت اطلاعات شخصی، شنود، دسترسی 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 محمدباقری 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، هزینهٔ بالای تجهیزات، نبودِ دسترسی به اینترنت پُرسرعت و پهنای باند بالا توجه کرده‌اند. رضایی‌نور و کریمیان (۱۴۰۳) به موانع استفاده از فناری‌ها از سوی مدیریت برای تصمیم‌گیری، ضعف در دانش فنی مدیران، ناتوانی در جمع‌آوری اطلاعات و آمار، بی‌ثباتی مدیریتی، و شی و زو[1] (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 نبودپوشش نامناسب، جین پاتل[2] (۲۰۲۴) به تأثیر بر سلامت روان و مراقبت‌های بهداشتی توجه کرده‌اند. از این‌رو، یکی از مباحثی که امروزه در همهٔ کشورها در زمینهٔ فناوری‌ها به‌ویژه فناوری متاورس دغدغه و نگرانی برای کشورها ایجاد کرده مسئلهٔ حریم خصوصی است.

حریم خصوصی در معرض تهدیدهایی قراردارد 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 شیوهٔخصوصی و با اختیار خود اطلاعات و پیام‌هایی را با مخاطبین خود به اشتراک گذارند. 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 چالش‌برانگیر تبدیل شده است. از این‌رو، کاربران برای ایجاد و القای تجربه در متاورس از دستگاه‌های پوشیدنی متفاوتی نظیر کالهٔ 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 آسیب‌دیدگی در این دستگاه‌های پوشیدنی، تبدیل به یک ورودی برای نفوذ به داده‌ها و تهاجم بدافزارها می شوند ( شون[3]، ۲۰۲۲؛ رضایی‌ملال و مرتضائی‌دکاهی، ۱۴۰۱). از این‌رو، هنوز هیچ مقرراتی برای حریم خصوصی کاربر وجود ندارد. با توجه به جمع‌آوری و تجزیه‌وتحلیل 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، مسئلهٔ اصلی این پژوهش شناسایی موانع حریم خصوصی کاربران در محیط متاورس است.

## ۲. پیشینهٔ پژوهش

در پژوهش حاضر برای بررسی پیشینهٔ 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[4]، وب‌آوساینس[5]) در جدول (۱) و جدول (۲) هدف بازیابی و بررسی آن‌ها است.

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

**جدول ۱. راهبرد جست‌وجوی 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*") |

**جدول۲. پیشینهٔ پژوهش**

| مؤلفه | منبع | روش پژوهش |
| --- | --- | --- |
| نقض حق کپی‌رایت و مالکیت معنوی؛ نبودِ قوانین روشن برای مالکیت معنوی؛ هویت و جعل هویت | یگانه و فامیل‌سعدیان (۱۴۰۱). | **کتابخانه‌ای** |
| ایجاد شکاف اجتماعی؛ انزوای اجتماعی؛ پرهیز از زندگی واقعی و فیزیکی | ساید (۲۰۲۳). | **پدیدارشناختی** |
| جعل هویت افراد؛ حذف لذت‌های فیزیکی؛ عدم انطباق و ناسازگاری برخی افراد؛ کمبود آگاهی | محمودی و صادقی (۱۴۰۱). | **تحلیلی_توصیفی** |
| حذف لذت‌های فیزیکی؛ نبودِانطباق و سازگاری برخی افراد؛ مالکیت معنوی | میراشرفی (۱۴۰۱). | **تحلیلی_توصیفی** |
| شمول اجتماعی؛ سرقت هویت؛ محتوای بازاریابی گمراه‌کننده و فریبنده؛ جعل هویت؛ کمبود آگاهی | دوویدی و همکاران (۲۰۲۳). | **تحلیلی_توصیفی** |
| جعل هویت | وانگ و همکاران[1] (۲۰۲۲)؛ شی و زو (۲۰۲۴)؛ دیزجی و دیزجی[2] (۲۰۲۳). | **تحلیلی_توصیفی** |
| کمبود سطح آگاهی و کسب هویت دیجیتال | تورال و کوچاک[3] (۲۰۲۳). | **روش اسکن تجربی (کمی)** |
| 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؛ نبودِکنترل کاربران بر داده‌هایشان | محمدباقری و سیدباقری (۱۴۰۱). | **تحلیلی_توصیفی** |

۱. Wang et al

2. Dizaji & Dizaji

3. Tural & Koçak

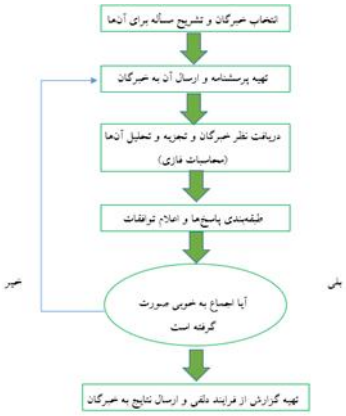
| مؤلفه | منبع | روش پژوهش |
|---|---|---|
| ناشناختگی هویت؛ خطرات تبعیض؛ نبودِ تعادل بین دنیای واقعی و مجازی؛ نبود فرهنگ حریم خصوص | داراب‌پور (۱۴۰۲). | **تحلیلی_توصیفی** |
| نبود حقوق مالکیت | مرادی برلیان (۱۴۰۱). | **تحلیلی_توصیفی** |
| هزینه‌های تکنولوژی؛ استفاده از رمز ارزها برای تراکنش‌ها؛ نبودِ مقررات برای رمز ارزها | پاشایی (۱۳۹۹). | **تحلیلی_توصیفی** |
| هزینه‌های زیاد فن | شهریاری (۱۴۰۱). | **تحلیلی_توصیفی** |
| جرایم مالی | دوویدی و همکاران (۲۰۲۳). | **تحلیلی_توصیفی** |
| هزینه‌های حفاظت از داده‌ها؛ هزینه‌های آگاهی؛ هزینه‌های امنیتی؛ هزینه‌های اجری قوانین | مرادی برلیان (۱۴۰۱). | **تحلیلی_توصیفی** |
| هزینهٔ حفاظت از داده‌ها | ساید (۲۰۲۳). | **پدیدارشناختی** |
| هزینهٔ بالای تجهیزات | شاه‌مرادی (۱۴۰۱). | **توصیفی-پیمایشی** |
| قوانین سخت‌گیرانهٔ دولت‌ها در بخش فناوری؛ خطرات پول‌شویی و تأمین مالی تروریسم | محمودی و صادقی (۱۴۰۱). | **تحلیلی_توصیفی** |
| نبودِ قوانین و مقررات؛ نبودِ امنیت؛ نبود آگاهی از خطرات؛ نبودِ قوانین و مقررات مشخص؛ نبودِ هماهنگی بین کشورها | شهریاری (۱۴۰۱). | **تحلیلی_توصیفی** |
| نشت اطلاعات شخصی؛ شنود؛ دسترسی غیرمجاز؛ فیشینگ؛ تزریق داده؛ احراز هویت شکسته؛ طراحی ناامن | کیم و دیگران (۲۰۲۳). | **تحلیلی_توصیفی** |
| ردیابی و نظارت؛ حریم خصوصی و امنیت داده‌ها؛ رضایت آگاهانه | جین پاتل (۲۰۲٤). | **تحلیلی_توصیفی** |
| تبلیغات تهاجمی؛ اطلاعات نادرست؛ کلاهبرداری فشینگ | دوویدی و همکاران (۲۰۲۳). | **تحلیلی_توصیفی** |
| امنیت، نظارت؛ ردیابی؛ حملات سایبری؛ تمهیدات برای پاسخ‌گویی | وانگ و همکاران (۲۰۲۲). | **تحلیلی_توصیفی** |
| اعمال نشدنِ مقررات قانونی مربوط به رضایت کاربر | داراب‌پور (۱۴۰۲). | **تحلیلی_توصیفی** |
| گذاشتنِ تأثیر نامحسوس بر امنیت فرهنگی و سیاسی یک کشور؛ حملات سایبری؛ نشت داده‌ها | میراشرفی (۱۴۰۱). | **تحلیلی_توصیفی** |
| نظارت، حملات سایبری، حفاظت از داده‌ها | لطیف‌زاده و قبولی‌درافشان (۱۴۰۲).<br>دوویدی و همکاران (۲۰۲۳). | **تحلیلی_توصیفی** |
| فعالیت‌های تروریستی؛ امنیت داده‌ها | دوویدی و همکاران (۲۰۲۳). | **تحلیلی_توصیفی** |
| نشت داده‌ها، امنیت | شی و زو (۲۰۲٤). | **تحلیلی_توصیفی** |

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

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 زمینهٔ متاورس، حریم‌خصوصی، حقوق، هوش‌مصنوعی، و علم اطلاعات و دانش شناسی در رابطه با مؤلفه‌ها جمع‌آوری شده است. با توجه به این‌که پژوهش‌های پیشین به موانع حریم خصوصی تنها به‌مثابهیک 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 شیوهٔ گردآوری داده‌ها پیمایشی است. در پژوهش حاضر ابتدا با بررسی ادبیات حوزهٔ متاورس، موانع حریم خصوصی در این حوزه مشخص شدند و سپس برای شناسایی مهمترین موانع که بر توسعهٔ 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 (ضرغام‌بروجنی و عزیزی، ۱۳۹۶). جامعهٔ آماری پژوهش حاضر را۳۰ نفر از خبرگان صاحب‌نظر در زمینهٔ فناوری اطلاعات (متاورس، هوش‌مصنوعی)، 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 حوزهٔ متاورس، ابتدا با استفاده از مرور ادبیات و پیشینهٔ پژوهش، تعداد ۴۴ مانع برای حریم خصوصی کاربران در محیط متاورس را استخراج کردند و سپس با یک پرسش‌نامهٔ نیمه‌ساختارمند از خبرگان درخواست کردند که براساس طیف پنج‌تایی لیکرت، تأثیر شاخص‌ها را مشخص کنند. بنابراین برای گردآوری نظرات خبرگان در انتهای شش مؤلفهٔ پژوهش، یک سؤال باز نوشته شده و از خبرگان خواسته شد که علاوه‌بر 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 تشکیل‌دهندهٔ ابزار اندازه‌گیری بستگی دارد. در این پژوهش برای سنجش روایی محتوا، از نظر ۱۶ نفر از خبرگان علمی و اجرایی در حوزهٔ متاورس و هوش‌مصنوعی استفاده شده است. 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[1] 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 ا ستفاده کرد. از این‌رو، الگوریتم اجرای تکنیک دلفی فازی شامل گام‌های شکل ۱ ا ست (حبیبی، ایزدیار و سرافزای، ۱۳۹۳، ۳۳؛ نقل در راهداری، نصر، ۱۳۹۶). شناسایی طیف مناسب برای فازی‌سازی عبارات کلامی عبارتند از تجمیع

1. COCOSO

فازی مقادیر فازی‌شده، فازی‌زدایی مقادیر، انتخاب شدت آستانه و غربال معیارها است. متغیرهایی که ارزش آن‌ها را لغات یا جملات زبان طبیعی یا زبان‌های مصنوعی تشکیل می‌دهند، متغیّر زبانی نامیده می‌شوند (قلی‌پور و محمّدزاده، 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 به‌صورت عدد فازی مثلثی(I,m,u) نمایش داده شود، میانگین فازی n عدد فازی مثلثی به‌صورت رابطه (۱) محاسبه خواهد (حبیبی و همکاران، ۱۳۹۳: ۳۳):

$$F = (l, m, n)$$

رابطه (۱)

پس از تجمیع فازی دیدگاه خبرگان باید به فازی‌زدایی مقادیر به‌دســت‌آمده پرداخت. روش‌های مختلفی برای فازی‌زدایی وجود دارد. در این پژوهش از رابطه (۳و۲) برای فازی‌زدایی استفاده خواهد شد.

$$X = \frac{l + m + u}{3}$$

رابطه (۲)

$$F_{AVE} = \frac{\sum l}{n}, \frac{\sum m}{n}, \frac{\sum u}{n}$$

رابطه (۳)

## ٤. 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 | |
|---|---|---|---|---|---|---|---|---|---|---|
| | ۳۰تا۴۰ | ۴۰تا۵۰ | بالاتر از ۵۰ سال | زن | مرد | علم اطلاعات و دانش‌شناسی | حقوق | فناوری اطلاعات | کارشناسی‌ارشد | دکتری |
| فراوانی | ٤ | ۷ | ۵ | ٦ | ۱۰ | ٦ | ۵ | ۵ | ٤ | ۱۲ |

از این‌رو، در فهرست مؤلفه‌های تأییدشده از سوی صاحب‌نظران به روش دلفی‌فازی، از ۴۴ مانع استخراج شده، در مجموع ۲۶ مانع در حوزهٔ حریم خصوصی در محیط متاورس در سه مرحله نظرسنجی 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 پاسخ‌دهندهٔ نشان می‌دهد.

**جدول ۵. نتایج شمارش پاسخ‌های مرحلهٔ نخست نظرسنجی**

| مؤلفه‌ها | تعداد ۱ | تعداد ۲ | تعداد ۳ | تعداد ٤ | تعداد ۵ |
|---|---|---|---|---|---|
| **ارزش‌های متفاوت فرهنگ‌ها** | ۰ | ۰ | ۰ | ۰ | ۱٦ |

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

| | | | | | |
|---|---|---|---|---|---|
| **تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها** | ۳ | ۰ | ۰ | ۰ | ۱۳ |
| **تأثیرات از خود بیگانگی** | ۵ | ۰ | ۰ | ۰ | ۱۱ |
| **تأثیر بر سلامتی(اضطراب، افسردگی، حواس‌پرتی، اختلال شخصیت)** | ٤ | ۰ | ۰ | ۰ | ۱۲ |
| **سوءاستفاده و آزار جنسی** | ۵ | ۰ | ۰ | ۰ | ۱۱ |
| **اعتیاد به فناوری، قتل، و جنایات خشونت‌آمیز** | ۵ | ۰ | ۰ | ۰ | ۱۱ |
| **تأثیر بر سلامت جسمی(خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی)** | ۱ | ۰ | ۰ | ۰ | ۱۵ |
| **نبودِ پوشش مناسب(اسلامی، ایران)** | ٤ | ۰ | ۰ | ۰ | ۱۲ |
| **خطرات افراط‌گرایی و ترویج نفرت** | ٤ | ۰ | ۰ | ۰ | ۱۲ |
| **خطرات برای ایمان و اخلاقیات** | ٤ | ۰ | ۰ | ۰ | ۱۲ |

تأیید و غربال‌گری شاخص‌ها با مقایسهٔ مقدار ارزش اکتسابی هر شاخص با مقدار آستانهٔ $S$ انجام می شود. 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 ۰/۷۵ 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 محاسبهٔ میانگین نظرات n پاسخ‌دهنده، میانگین فازی آن‌ها محاسبه شود. محاسبهٔ عدد فازی $\tau$ برای هر یک از شاخص‌ها با استفاده از روابط زیر انجام می‌شود (راهداری و نصر، ۱۳۹۶؛ سیف‌الدین و دیگران، ۱۳۹۶)

$$\tilde{\tau}_{ij} = (a_{ij}.\, b_{ij}.\, c_{ij}). \quad i = 1.2. \ldots . n \quad j = 1.2. \ldots . m \qquad ۳-۱$$

$$a_j = \sum \frac{a_{ij}}{n} \qquad ۳-۲$$

$$b_j = \sum \frac{b_{ij}}{n} \qquad ۳-۳$$

$$c_j = \sum \frac{c_{ij}}{n} \qquad ۳-٤$$

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

$$Crisp = \frac{a + b + c}{3} \qquad ۳-۵$$

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

**جدول ۶. نتایج فازی‌زدایی پاسخ‌های مرحلهٔ دوم نظرسنجی**

| 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 |

| | | | | | |
|---|---|---|---|---|---|
| نبودِ فرهنگ حریم خصوصی | ۰/٦٥٦ | ۰/۹۰٦ | ۰/۹۳۸ | ۰/۸۳۳ | تأیید |
| پرهیز از زندگی واقعی و فیزیکی | ۰/٥۹٤ | ۰/۸٤٤ | ۰/۹۰٦ | ۰/۷۸۱ | تأیید |
| جعل هویت | ۰/٦٥٦ | ۰/۹۰٦ | ۰/۹۳۸ | ۰/۸۳۳ | تأیید |
| نبود قوانین مالکیت معنوی | ۰/۷۰۳ | ۰/۹٥۳ | ۰/۹٦۹ | ۰/۸۷٥ | تأیید |
| انزوای اجتماعی | ۰/٤۸٤ | ۰/۷۰۳ | ۰/۷۹۷ | ۰/٦٦۱ | رد |
| هزینه‌های زیاد تکنولوژی | ۰/٥٦۳ | ۰/۷۹۷ | ۰/۸٥۹ | ۰/۷٤۰ | رد |
| نبودِ مقررات برای رمز ارزها در تراکنش‌ها | ۰/٦٥٦ | ۰/۸۹۱ | ۰/۹۲۲ | ۰/۸۲۳ | تأیید |
| جرایم مالی | ۰/٤۲۲ | ۰/٦۲٥ | ۰/۷۳٤ | ۰/٥۹٤ | رد |
| هزینه‌های حفاظت از داده‌ها | ۰/٦٥٦ | ۰/۹۰٦ | ۰/۹۳۸ | ۰/۸۳۳ | تأیید |
| هزینه بالای تجهیزات | ۰/٦۰۹ | ۰/۸٥۹ | ۰/۹۰٦ | ۰/۷۹۲ | تأیید |
| هزینه‌های اجرای قوانین | ۰/٥۳۱ | ۰/۷٦٦ | ۰/۸٤٤ | ۰/۷۱٤ | رد |
| هزینه‌های امنیتی | ۰/٥۹٤ | ۰/۸٤٤ | ۰/۹۰٦ | ۰/۷۸۱ | تأیید |
| قوانین سخت‌گیرانهٔ دولت‌ها در بخش فناوری | ۰/٤۲۲ | ۰/٦٤۱ | ۰/۷٥۰ | ۰/٦۰٤ | رد |
| خطرات پول‌شویی و تأمین مالی تروریسم | ۰/۷۰۳ | ۰/۹٥۳ | ۰/۹٦۹ | ۰/۸۷٥ | تأیید |
| نبودِ قوانین و مقررات بین‌المللی و هماهنگی بین کشورها | ۰/٦۰۹ | ۰/۸٤٤ | ۰/۸۹۱ | ۰/۷۸۱ | تأیید |
| نشت اطلاعات شخصی | ۰/۷۰۳ | ۰/۹٥۳ | ۰/۹٦۹ | ۰/۸۷٥ | تأیید |
| شنود، ردیابی، و نظارت | ۰/٦٥٦ | ۰/۹۰٦ | ۰/۹۳۸ | ۰/۸۳۳ | تأیید |
| کلاهبرداری فیشینگ | ۰/۷٥۰ | ۱/۰۰۰ | ۱/۰۰۰ | ۰/۹۱۷ | تأیید |
| حفاظت از داده‌ها | ۰/٥۱٦ | ۰/۷۳٤ | ۰/۸۱۳ | ۰/٦۸۸ | رد |
| تبلیغات تهاجمی | ۰/٦۰۹ | ۰/۸٥۹ | ۰/۹۰٦ | ۰/۷۹۲ | تأیید |
| حملات سایبری | ۰/٦٥٦ | ۰/۹۰٦ | ۰/۹۳۸ | ۰/۸۳۳ | تأیید |
| نبودِ مدیریت هویت | ۰/٥٦۳ | ۰/۷۹۷ | ۰/۸٥۹ | ۰/۷٤۰ | رد |
| ضعف در دانش فنی مدیران | ۰/۷۰۳ | ۰/۹۳۸ | ۰/۹٥۳ | ۰/۸٦٥ | تأیید |

| | | | | | |
|---|---|---|---|---|---|
| نبود رقابت عملیاتی هوشمندسازی در بین مدیران | ۰/۵۱۶ | ۰/۷۱۹ | ۰/۷۹۷ | ۰/۶۷۷ | رد |
| افزایش ریسک | ۰/۶۵۶ | ۰/۹۰۶ | ۰/۹۳۸ | ۰/۸۳۳ | تأیید |
| هدست واقعیت مجازی | ۰/۴۶۹ | ۰/۶۲۵ | ۰/۷۱۹ | ۰/۶۰۴ | رد |
| عینک هوشمند واقعیت مجازی | ۰/۵۱۶ | ۰/۶۸۸ | ۰/۷۶۶ | ۰/۶۵۶ | رد |
| اینترنت پُرسرعت | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| استراق سمع آوارتاهای نامرئی | ۰/۴۶۹ | ۰/۶۴۱ | ۰/۷۳۴ | ۰/۶۱۵ | رد |
| نبودِ امنیت داده‌ها | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| فناوری‌های احراز هویت | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| نبودِ زیرساخت‌های مقیاس‌پذیر | ۰/۶۵۶ | ۰/۸۹۱ | ۰/۹۲۲ | ۰/۸۲۳ | تأیید |
| آسیب‌پذیری دستگاه‌ها مانند هولولنز | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها | ۰/۶۰۹ | ۰/۸۱۳ | ۰/۸۵۹ | ۰/۷۶۰ | تأیید |
| تأثیرات از خود بیگانگی | ۰/۵۱۶ | ۰/۶۸۸ | ۰/۷۶۶ | ۰/۶۵۶ | رد |
| تأثیر بر سلامتی(اضطراب، افسردگی، حواس‌پرتی، اختلال شخصیت) | ۰/۵۶۳ | ۰/۷۵۰ | ۰/۸۱۳ | ۰/۷۰۸ | رد |
| سوءاستفاده و آزار جنسی | ۰/۵۱۶ | ۰/۶۸۸ | ۰/۷۶۶ | ۰/۶۵۶ | رد |
| اعتیاد به فناوری، قتل، و جنایات خشونت‌آمیز | ۰/۵۱۶ | ۰/۶۸۸ | ۰/۷۶۶ | ۰/۶۵۶ | رد |
| تأثیر بر سلامت جسمی (خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی) | ۰/۷۰۳ | ۰/۹۳۸ | ۰/۹۵۳ | ۰/۸۶۵ | تأیید |
| نبودِ پوشش مناسب (اسلامی، ایران) | ۰/۵۶۳ | ۰/۷۵۰ | ۰/۸۱۳ | ۰/۷۰۸ | رد |

| | | | | | |
|---|---|---|---|---|---|
| **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 می شود مواردی که میانگین قطعی آن‌ها بیشتر از۰/۷۵ محاسبه شده، تأیید شده‌اند. جدول (۷)، موارد تأیید شده را به‌ترتیب میانگین قطعی نشان می‌دهد.

**جدول ۷. فازی‌شدهٔ پاسخ‌های مرحلهٔ 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 |
| **نشت 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 |
| **نبودِ 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 |
| **نبودِ مقررات برای رمز ارزها در تراکنش‌ها** | ۰/۶۵۶ | ۰/۸۹۱ | ۰/۹۲۲ | ۰/۸۲۳ | تأیید |
| **نبودِ زیرساخت‌های مقیاس‌پذیر** | ۰/۶۵۶ | ۰/۸۹۱ | ۰/۹۲۲ | ۰/۸۲۳ | تأیید |
| **اینترنت پُرسرعت** | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| **نبودِ امنیت داده‌ها** | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| **فناروی‌های احراز هویت** | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| **آسیب‌پذیری دستگاه‌ها مانند هولولنز** | ۰/۶۵۶ | ۰/۸۷۵ | ۰/۹۰۶ | ۰/۸۱۳ | تأیید |
| **هزینهٔ 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 |
| **نبودِ قوانین و مقررات بین‌المللی و هماهنگی بین کشورها** | ۰/۶۰۹ | ۰/۸۴۴ | ۰/۸۹۱ | ۰/۷۸۱ | تأیید |
| **تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها** | ۰/۶۰۹ | ۰/۸۱۳ | ۰/۸۵۹ | ۰/۷۶۰ | تأیید |

برای دستیابی و شناخت بهتر وضعیت و تعیین اولویت موانع حریم خصوصی کاربران براساس رتبه‌بندی به‌دست‌آمده از مدل کوکوسو و به لحاظ برخورداری از شاخص‌های مطالعه، در چهار سطح کم برخوردار، نیمه برخوردار، برخوردار و خیلی برخوردار 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**

| شاخص‌ها | ka | Ranks | kb | Ranks | KC | Ranks | K | Ranks |
|---|---|---|---|---|---|---|---|---|
| ارزش‌های متفاوت فرهنگ‌ها | ۰/۰۳۷ | ۲۱ | ٦/۱۵۲ | ۱۹ | ۰/۸۷۶۳۸۲۹۹۱ | ۲۲ | ۲/۹۳۹۴۲۹۶۰۷ | **۱۹** |
| کمبود آگاهی | ۰/۰٤ | ۸ | ۵/۵۱٦ | ۲۳ | ۰/۹۴۷۴۳۱۳۷۴ | ۸ | ۲/۷۶۱۲۹۶۷۲ | **۲۲** |
| کلاهبرداری فیشینگ | ۰/۰۳۳ | ۲۵ | ٤/۷۰۲ | ۲۵ | ۰/۷۸۰۳۹۵۹۰۹ | ۲۵ | ۲/۳۳۳۱۹۷۸۸۹ | **۲۵** |
| نبود قوانین مالکیت معنوی | ۰/۰۳۹ | ۱۵ | ٦/۲۹۹ | ۱۸ | ۰/۹۲۷۵۷۶۱۰۲ | ۱۹ | ۳/۰۳۲۶۵۳۳۹۴ | **۱۸** |
| خطرات پول‌شویی و تأمین مالی تروریسم | ۰/۰۳٦ | ۲۳ | ۵/٦۸۱ | ۲۲ | ۰/۸۶۱۴۹۱۵۳۸ | ۲۳ | ۲/۷۵۳۴۳۸۶۹۹ | **۲۳** |
| نشت اطلاعات شخصی | ۰/۰٤۲ | ۱ | ۶/۹۱۸ | ۲ | ۰/۹۹۸۹۸۳۳۱۴ | ۲ | ۳/۳۱۵۱۰۳۲۳۹ | **۲** |
| ضعف در دانش فنی مدیران | ۰/۰٤ | ۸ | ۶/۵۸۹ | ۱۰ | ۰/۹۳۹۴۷۷۳۰۴ | ۱۳ | ۳/۱۵۰۷۷۱۲۳۶ | **۱۱** |
| تأثیر بر سلامت جسمی(خستگی چشم، سردرد، حالت تهوع و سرگیجه، چاقی، بیماری‌های قلبی) | ۰/۰٤ | ۸ | ۶/۶۰۷ | ۹ | ۰/۹۳۹۸۹۵۹۳۹ | ۱۲ | ۳/۱۵۷۵۷۵۴۱۷ | **۱۰** |
| نبودِ فرهنگ حریم خصوصی | ۰/۰٤۲ | ۱ | ۶/۸۲۲ | **۵** | ۰/۹۹۵۵۱۴۶۲۲ | **۵** | ۳/۲۷۸۱۰۶۴۱۹ | **۵** |
| جعل هویت | ۰/۰۳۹ | ۱۵ | ۵/۹۴۳ | ۲۱ | ۰/۹۱۵۶۷۴۹ | ۲۰ | ۲/۸۹۵۷۱۵۹۴۹ | **۲۱** |
| هزینه‌های حفاظت از داده‌ها | ۰/۰٤۲ | ۱ | ۶/۹۶۲ | ۱ | ۱ | ۱ | ۰/۳۳۱۷۳۴۵۶۸ | **۱** |
| شنود، ردیابی و نظارت | ۰/۰۱۳ | ۲٦ | ۲ | ۲٦ | ۰/۳۰۶۰۲۲۳۶۷ | ۲٦ | ۰/۹۷۲۶۴۴۹۷۹ | **۲٦** |
| حملات سایبری | ۰/۰٤ | ۸ | ۶/۷۱۶ | ٦ | ۰/۹۴۳۴۸۴۲۴۱ | ۹ | ۳/۱۹۹۳۴۶۱۹۳ | **٦** |
| افزایش ریسک | ۰/۰۳۹ | ۱۵ | ۶/۳۷۹ | ۱٤ | ۰/۹۳۳۲۵۷۵۸ | ۱۵ | ۳/۰۶۵۰۳۸۵۶۶ | **۱٤** |
| نبودِ مقررات برای رمز ارزها در تراکنش‌ها | ۰/۰٤ | ۸ | ۶/۵ | ۱۲ | ۰/۹۳۵۶۴۹۷۸۲ | ۱٤ | ۳/۱۱۶۱۳۸۵۳۸ | **۱۲** |
| نبودِ زیرساخت‌های مقیاس‌پذیر | ۰/۰۳۹ | ۱۵ | ۶/۳۱۶ | ۱۷ | ۰/۹۳۱۴۰۳۶۲۴ | ۱۸ | ۳/۰۴۰۹۸۴۶۱ | **۱۷** |
| اینترنت پُرسرعت | ۰/۰٤۲ | ۱ | ۶/۵۵۳ | ۱۱ | ۰/۹۸۷۶۸۰۱۶۳ | ٦ | ۳/۱۷۵۳۵۱۵۸۱ | **۸** |
| نبودِ امنیت داده‌ها | ۰/۰۳۹ | ۱۵ | ۶/۳۵۷ | ۱۵ | ۰/۹۳۲۸۹۸۷۵ | ۱٦ | ۳/۰۵۶۷۹۹۵۴۸ | **۱۵** |
| فناوری‌های احراز هویت | ۰/۰٤۲ | ۱ | ۶/۸۵۴ | ٤ | ۰/۹۹۶۷۱۰۷۲۳ | ٤ | ۳/۲۹۰۴۶۳۳۶۸ | **٤** |
| آسیب‌پذیری دستگاه‌ها مانند هولولنز | ۰/۰٤ | ۸ | ۶/۶۱۲ | ۸ | ۰/۹۴۰۱۹۴۹۶۴ | ۱۱ | ۳/۱۵۹۵۶۶۹۶۳ | **۹** |
| هزینهٔ بالای تجهیزات | ۰/۰٤ | ۸ | ۶/۶۹۸ | ۷ | ۰/۹۴۲۹۴۵۹۹۶ | ۱۰ | ۳/۱۹۲۴۸۸۰۶۳ | **۷** |
| تبلیغات تهاجمی | ۰/۰۳٦ | ۲۳ | ۵/۳۴۹ | ۲٤ | ۰/۸۵۲۸۱۹۸۰۷ | ۲٤ | ۲/۶۲۶۸۹۰۹۴۷ | **۲٤** |
| پرهیز از زندگی واقعی و فیزیکی | ۰/۰۳۷ | ۲۱ | ۶/۱۱۷ | ۲۰ | ۰/۸۷۶۷۴۱۸۲۲ | ۲۱ | ۲/۹۲۶۸۵۱۹۵۵ | **۲۰** |
| هزینه‌های امنیتی | ۰/۰۳۹ | ۱۵ | ۶/۳۲۳ | ۱٦ | ۰/۹۳۲۴۲۰۳۱ | ۱۷ | ۳/۰۴۴۱۰۵۶۶۲ | **۱٦** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| نبودِ قوانین و مقررات بین‌المللی و هماهنگی بین کشورها | ۰/۰۴۲ | ۱ | ۶/۳۸۳ | ۱۳ | ۰/۹۸۲۶۵۶۵۴ | ۷ | ۳/۱۱۰۲۶۸۹۳ | **۱۳** |
| تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها | ۰/۰۴۲ | ۱ | ۶/۹۰۱ | ۳ | ۰/۹۹۸۵۰۴۸۷۴ | ۳ | ۳/۳۰۸۶۲۸۶۷۱ | **۳** |

بر اساس امتیازات هر عامل در جدول (۸)، هزینه‌های حفاظت از داده‌ها، نشت اطلاعات شخصی، تعامل‌پذیرنبودنِ 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، نحوهٔ 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 زمینهٔ متاورس، حریم‌خصوصی، حقوق، هوش‌مصنوعی، 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 تعامل‌پذیرنبودنِ 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 درواقع بازتاب‌دهندهٔ 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 همهٔ آن‌ها مستلزم سرمایه‌گذاری‌های کلان در زمینهٔ 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 ساید (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 منحصربه‌فرد 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 نه‌تنها حریم خصوصی کاربران را تهدید می‌کنند، بلکه می‌توانند به اعتبار و شهرت پلتفرم‌های متاورس آسیب‌های جبران‌ناپذیری وارد کنند. پژوهش‌های مختلف از جمله لطیف‌زاده و قبلولی‌درافشان (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 یافتهٔ این پژوهش هم‌سو است.

مانع سوم مربوط به تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها در محیط متاورس است. تعامل‌پذیرنبودنِ گرافیک‌ها و سخت‌افزارها در محیط متاورس یکی از چالش‌های اساسی است که می‌تواند به‌طور مستقیم بر تجربهٔ 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. به‌عبارتی برای ایجاد یک محیط متاورس کارآمد و مقیاس‌پذیر، 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 دربارهٔ 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 ارائهٔ اطلاعات به کاربران دربارهٔ 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 نحوهٔ محافظت از حریم خصوصی‌شان آگاه هستند. ارائهٔ ابزارها و گزینه‌هایی به کاربران برای دسترسی، اصلاح، و حذف داده‌های شخصی‌شان به آن‌ها این امکان را می‌دهد که به‌راحتی 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. کتیبه گیل.

حدادعراقی، س. (۱۴۰۱). کاربرد متاورس در آموزش(ویژگی‌ها، فرصت‌ها و چالش‌ها). هفتمین کنفرانس ملی رویکردهای نوین(آموزش و پژوهش مازندران). ۱-۱۱. https://civilica.com/doc/1619874/

حسن‌زاده، م. (۱۴۰۱). متاورس و سرنوشت سامانه‌های اطلاعاتی. علوم و فنون مدیریت اطلاعات، ۸(۱)، ۷-۱۴. doi: 10.22091/stim.2022.213914

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.2023.76141.1617

رضائی‌ملال، 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

ضرغام‌بروجنی، ح.، و عزیزی، ف. (۱۳۹۶). ارزیابی عوامل مؤثر بر توسعه گردشگری محوطه‌های باستانی- تاریخی (رویکرد فازی). تاریخ و فرهنگ، ۴۹(۲)، ۹-۳۲. doi: 10.22067/jhc.v49i2.73024

محمدزاده، ل.، و قلی‌پور، م. (۱۳۹۳). منطق فازی برای دانشجویان مدیریت.آتی‌نگر.

لطیف‌زاده، م. و قبولی‌درافشان، م.(۱۴۰۲). معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل. مطالعات حقوق خصوصی، ۵۳(۲)، ۳۷۲-۳۴۹. 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، ۱(۴)، ۷۶-۶۵. doi: 10.30495/CYBERLAW.2023.699220

محمودی، م. و صادقی، س. (۱۴۰۱). متاورس و تأثیر آن بر سبک زندگی. فصلنامه مطالعات حقوقی فضای مجازی، ۱(۲)، ۴۴-۶۲. doi: 10.30495/cyberlaw.2022.693926

مرادی برلیان، م.(۱۴۰۱). درآمدی برپیامدها و چالش‌های حقوقی متاورس. فصلنامه حقوقی و ویژه‌نامه حقوق و فناوری. ۲۶۳-۳۹۱. doi: 10.52547/JLR.2022.228286.2279

مرادیان، ع.، و پورغفاری‌بشری، ع. (۱۴۰۱). بررسی رویکرد نظامی در متاورس و چالش‌های امنیتی پیش‌رو. نخستین کنفرانس بین المللی فناوری متاورس، بلاکچین و ارزهای 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، ۳۸۸-۴۰۴. https://civilica.com/doc/1880162

یگانه، ح.، و فامیل‌سعدیان، ف. (۱۴۰۱). بررسی و تحلیل چالش هاي حقوقی آواتارها در زیست بوم متاورس. فصلنامه نشاء علم، ۱۳(۱)،۴۲-۳۳. 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). *ModernTechnologies 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., & Serafrazi, 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., & Mortezadekahi, 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]