چالش‌های اجتماعی و امنیتی در توسعه متاورس

جمشید نصرت آبادی[۱]، مجید سلیمانی ساسانی[۲]، امیرمحمدشیرخدا[۳]

[۱]استادیار و عضو هیئت علمی دانشگاه فارابی، تهران، ایران
dr.nosratabadi110@gmail.com
[۲]استادیار و عضو هیئت علمی دانشگاه تهران، تهران، ایران
msoleimani@ut.ac.ir
[۳]دانشجوی کارشناسی ارشد، دانشگاه فارابی، تهران، ایران
ariadata@ymail.com

چکیده

با توجه به گسترش روز افزون دانش و فناوری، مفاهیم و واژگان جدیدی جای واژگان قدیمی را پر می‌کنند. پس از شکست پروژه زندگی دوم، آرزوها و دست‌نیافتنی‌های واقع در ذهن بشر تمام نشد، بلکه جای خود را با مفهومی کامل‌تر و جامع‌تر به نام متاورس تکمیل کرد. توجه به پیوست اجتماعی و اخلاقی تکنولوژی‌های نوظهور از مهم‌ترین عوامل رشد و توسعه آنها می‌باشد. اما در متاورس فعلی فقط شاهد تغییر در تجارت دارایی‌های مجازی به‌صورت آنلاین و در بازی‌های آنلاین هستیم، جایی که کاربران می‌توانند دارایی‌های دیجیتال مانند لوازم جانبی برای آواتارها را ایجاد و یا خرید و فروش کنند. ما در این پژوهش ضمن بازخوانی مفاهیم مطرح شده برای کلیدواژه متاورس و تکنولوژی‌های در دسترس، به بیان چالش‌ها و مشکلات اجتماعی و امنیتی که در راه تکامل این تکنولوژی و یا مفهوم آن به‌کار می‌آید با دسته‌بندی کپی‌رایت، حریم‌خصوصی، نگهداری و حفاظت از داده‌ها در بخش امنیتی و هویت افراد، تبعیض و سوگیری، سلامت افراد، قطبیت در جامعه، آزادی، قوانین و حکومت‌ها در بخش اجتماعی می‌پردازیم. لازم به ذکر است این مقاله با استفاده از مطالعات کتابخانه‌ای مقالات معتبر متعدد در این حوزه تنظیم شده است.

کلمات کلیدی: متاورس، چالش‌های متاورس، اخلاق در متاورس، فراجهان، دنیاهای مجازی، واقعیت مجازی، هوش‌مصنوعی، حریم‌خصوصی.

۱ مقدمه

شاید بتوانیم فیلم‌ها و داستان‌های علمی خیلی، از فیلم‌های سفر به اعماق زمین گرفته تا موضوعات مرتبط با تکامل تکنولوژی از قبیل ماتریکس (The Matrix) در سال ۱۹۹۹، بازیکن شماره یک (Ready Player One) در سال ۲۰۱۸ و ... را اولین نمایش و تعریف از تکامل خواسته‌ها و آرزوهای بشر دانست [Hutson ،۷ and other, 2023: 2]. در طول ۲۰ تا ۳۰ سال گذشته، الگوی رابط کاربری محصولات تکنولوژی، به تدریج

از مردم سازگار با فن‌آوری به فن‌آوری سازگار با مردم تغییر کرده است. در این میان زبان‌های برنامه‌نویسی پیچیده به متن‌های ساده، که غنی از رابط‌های گرافیکی مانند پنجره‌ها، مرورگرها، برنامه‌ها و صداها است و باعث ایجاد تکامل در رابط‌های شناختی می‌شود، تغییر یافت [۴، Benjamins and other, 2023: 691].

رابط‌های سه بعدی تنها تکامل بعدی همین مفهوم هستند که از تکنولوژی‌های جدید (واقعیت مجازی – VR، واقعیت افزوده – AR، واقعیت ترکیبی – MR) و قابلیت‌های (به‌عنوان مثال، محاسبات با کارایی بالا، فضای ابری و اتصال با سرعت بالا) بهره می‌برند. در آینده، علاوه بر بینایی و شنوایی، رابط کاربری ممکن است شامل عناصری از سه حس دیگر مانند لمس (تا حدی که در حال حاضر از طریق رابط‌های لمسی در دسترس است)، چشایی و بویایی نیز باشد (همان).

متاورس اخیرا اهمیت خود را در فضای وب افزایش داده است. پلتفرم‌های آنلاین مانند دسنترالند و سندباکس، اولین دنیای مجازی مستقر شده با استفاده از ابزارهای غیرمتمرکز (به عنوان مثال، بلاک‌چین) را به نمایش می‌گذارند. همچنین پلتفرم‌های متعددی در این مسیر وجود دارند که در علاقه‌مندی‌های اخیر به متاورس نقش داشته‌اند؛ مانند: سکندلایف، ماینکرفت و روبلاکس؛ و شرکت‌هایی مانند نیانتیک، مایکروسافت (با مش) و اخیرا متا (که قبلا با نام فیسبوک شناخته می‌شد) [۱، Fernandez and other, 2022: 1].

با وجود علاقه‌مندی‌های بوجود آمده و گسترش روزافزون این پلتفرم‌ها، همواره در کنار چالش تکنولوژی برای دستیابی به جهانی فراتر از جهان فعلی، چالش‌های اجتماعی و امنیتی نیز وجود داشته است. شناسایی و معرفی چالش‌های موجود در تکنولوژی خود مقدمه‌ای برای بهبود بهره‌برداری کامل از متاورس است. در این مطلب به چالش‌های مهمی می‌پردازیم که متاورس از نظر امنیت و حریم‌خصوصی، اخلاقی و اجتماعی با آن‌ها مواجه خواهد شد.

۲ امنیت در متاورس

متاورس برای ارائه تجربه‌های همه جانبه، از داده‌های جمع‌آوری شده‌ی دنیای واقعی استفاده می‌کند و کاربران با سنسورهای متصل شده (مثلا ژیروسکوپ برای ردیابی حرکات سر) می‌توانند به صورت واقع‌گرایانه آواتار خود را کنترل کنند. علاوه بر این، متاورس چالش‌های جدیدی را نیز در دنیای مجازی عظیم خود باز می‌کند که در آن کاربران می‌توانند در معرض حملات حریم خصوصی مانند استراق سمع توسط دیگر کاربران پلتفرم قرار بگیرند [۱، Fernandez and other, 2022: 1].

۱.۲ کپی رایت

چه کسی حق چاپ و فروش یک اثر هنری تولید شده توسط یک سیستم هوش مصنوعی را دارد؟ مانند یک آهنگ یا یک نقاشی ایجاد شده توسط Dall.e2.4[۱] یا یک متن توسط LaMDA[۲] یا حتی یک قطعه کد برنامه

[۱] یکی از جدیدترین پیشرفت‌ها در حوزه هوش‌بصری، هوش مصنوعی Dall-E است؛ هوش مصنوعی‌ای که می‌تواند تصاویر منحصربه‌فردی را بر اساس دستور متنی شما ایجاد کند.

[۲] مخفف عبارت Language Model for Dialog Application می‌باشد. به زبان ساده‌تر، یک مدل یادگیری ماشینی زبان بوده که به‌طور خاص برای ایجاد گفتگوی طبیعی طراحی شده است.

نویسی توسط Copilot۵ که بصورت کاملا طبیعی و با استفاده از تکنولوژی در حال تکامل هوش‌مصنوعی تولید شده است [۴، Benjamins, 2023: 693].

برای مثال، در سپتامبر ۲۰۲۲ یک نقاشی با نام Theatre D'opera Spatial در مسابقه‌ی سالانه هنرهای زیبای نمایشگاه ایالت کلرادو برنده می‌شود، درحالی که داوران و تحسین‌کنندگان آن زمان نمی‌دانستند که این محصول تخیل یک نقاش نبوده است و محصول یک هوش مصنوعی است.

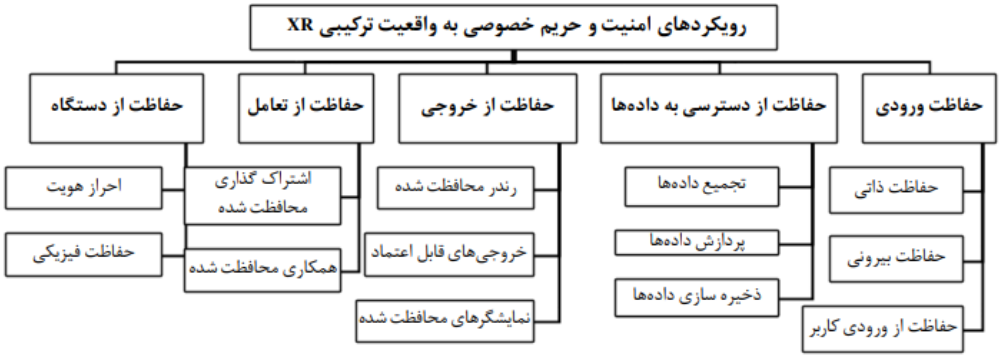
پس از آنکه طوفان اعتراضات و بحث‌های داغ در نشریه‌ای به راه افتاد و در آن به تقلب و ارسال اثری بدون مهارت، هنر یا پیام متهم شد، جیسون ام آلن خالق اثر این واقعیت را آشکار کرد. یکی از جدیدترین مدل‌های هوش مصنوعی با کیفیت «تصویر مبتنی بر متن» برنده این جایزه بود. تنها کاری که باید انجام دهید این است که یک نمای کلی به‌صورت مکتوب از آنچه می‌خواهید ترسیم کنید را به هوش مصنوعی بدهید. رایانه همه کارها را انجام خواهد داد [۱۰، Roose, 2022].

در مثال‌هایی دیگر؛ برخی از کشورهای اطراف ساحل مدیترانه مدعی مالکیت تصاویر تاریخی در کشورهای خود هستند. تلاش بنگلادش برای ساختن ماکت تاج محل با مخالفت هند مواجه شد. شیکاگو عکاسان حرفه‌ای را از عکاسی از پارک هزاره شهر بدون اجازه منع کرد و ادعا کرد که این پارک توسط قوانین کپی رایت محافظت می‌شود (Chen, 2023:5). علاوه بر تولیدات هوش مصنوعی، بحث فروش مالکیت برندها و یا آثار تولید شده توسط اشخاص در متاورس هم مطرح است، که البته با وجود NFT بخشی از این موضوع قابل حل است و در موارد کمی هم قوانین تجارت الکترونیکی در کشورها راه‌گشا خواهند بود. [۴، Benjamins, 2023: 696]

۲.۲ حریم خصوصی

رابطه و تعاملات اجتماعی می‌تواند برای استنباط عادات، فعالیت‌ها و انتخاب‌های کاربران در متاورس ارزشمند باشد. مشابه داده‌های بیومتریک، این اطلاعات می‌تواند روان کاربران را توصیف کنند. علاوه بر این، فراداده‌های ذاتی در هر تعامل اجتماعی با سایر آواتارها (مانند: مکالمات، واکنش‌ها) خطرات حریم‌خصوصی را برای کاربران به همراه دارند. این اطلاعات می‌تواند برای ردیابی و تنظیم رفتار کاربران مفید باشد. چه کسی کنترل همه این اطلاعات را در دست دارد [۱، Fernandez and other, 2022: 4]؟ تبلیغات هدفمند و نگرانی‌های مربوط به حفظ حریم‌خصوصی داده‌ها سر به فلک کشیده و این باور وجود دارد که این اطلاعات می‌توانند بسیار مزاحم شوند [۴، Benjamins, 2023: 693].

فناوری‌های XR چندین تهدید حریم‌خصوصی و امنیتی را برای کاربران و تماشاگران ایجاد می‌کنند. این فناوری‌ها معمولاً از حسگرها برای اسکن و نظارت بر محیط اطراف کاربران استفاده می‌کنند. این اسکن‌ها می‌توانند اطلاعاتی را جمع‌آوری کنند که ممکن است برای کاربران و تماشاگرانی که در منطقه تحت پوشش مانیتورینگ قرار دارند، محسوس باشد. نمایشگرهای روی سر (HMDها) که معمولاً برای نمایش متاورس استفاده می‌شوند، می‌توانند برخی از داده‌های بیومتریک (حرکت سر، ردیابی چشم) را جمع‌آوری کنند که برای کاربران محسوس نیست. به عنوان مثال، زل زل نگاه کردن به کاربران دیگر می‌تواند ترجیحات جنسی کاربران را از بین ببرد. داده‌های بیومتریک جمع‌آوری شده، شخصی‌ترین جنبه‌های روان ما را در معرض خطر



شکل ۱: دسته بندی داده محور از کارها یا رویکردهای مختلف امنیت و حریم خصوصی در واقعیت ترکیبی و فناوری‌های مرتبط [De Guzman, 2019: 9 ،۸]

قرار می‌دهد. بنابراین، این دستگاه‌ها باید با داده‌ها مطابق اصولی رفتار کنند که از حریم‌خصوصی کاربران محافظت می‌کند. [Fernandez and other, 2022: 4 ،۱] از طرفی پیش بینی می‌شود همان شرکت‌های بزرگی که تا پیش از این نیز در نگه داشت، امنیت و فروش داده‌ها سابقه‌ی خوبی نداشته‌اند وارث این اطلاعات باشند که خود از موانع و چالش‌های مهم گسترش و پذیرش متاورس در میان افراد می‌باشد.

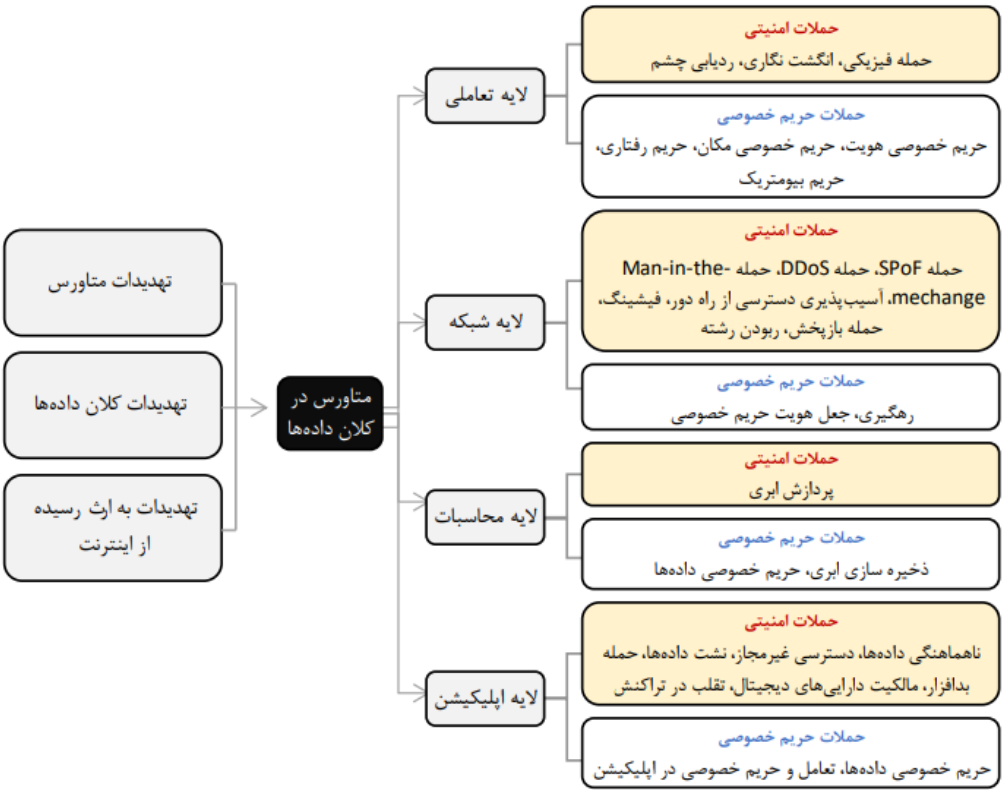
۳.۲ حفاظت و نگهداری از داده‌ها

از آنجایی که متاورس جدیدترین فناوری‌ها و سیستم‌های ساخته شده را ادغام می‌کند، آسیب‌پذیری‌ها و نقص‌های ذاتی آن فناوری‌ها نیز ممکن است به ارث برسد. حوادثی از فناوری‌های نوظهور مانند ربودن دستگاه‌های پوشیدنی یا فضای ذخیره‌سازی ابری، سرقت ارزهای مجازی و سوء رفتار هوش مصنوعی برای تولید اخبار جعلی وجود داشته است. ثانیاً، با درهم آمیختن فناوری‌های مختلف، تأثیرات تهدیدات موجود می‌تواند در دنیای مجازی تقویت شده و شدیدتر شود، در حالی که تهدیدهای جدیدی که در فضاهای فیزیکی و سایبری وجود ندارند، می‌توانند مانند تعقیب مجازی و جاسوسی مجازی و ... در متاورس ایجاد شوند [wang and others, 2022: 1 ،۱۱].

باید توجه داشته باشیم روش‌های فعلی ذخیره ابری اطلاعات حساس به حریم خصوصی، در سرورهای ابری و رایانش مرزی (Edge computing) نیز تهدیداتی برای حفظ حریم خصوصی در حفاظت از اطلاعات دارد. به‌عنوان مثال، پایگاه داده Second Life (یک بازی متاورس) هک شده بود و مقدار زیادی از اطلاعات کاربران، از جمله جزئیات پرداخت و رمز عبور، به بیرون درز پیدا کرده بود [Chen, 2023: 7 ،۵].

متاورس دارای ویژگی‌های اجتماعی قوی مانند: بازی‌های چند نفره و همکاری از راه دور است و کاربردهای آن معمولاً چند کاربره است. نحوه دستیابی به اشتراک گذاری محتوای ایمن و کارآمد در محیط XR در متاورس به چالشی در استفاده از داده تبدیل می‌شود. علاوه بر این، به اشتراک گذاری و پردازش محتوای تولید شده توسط کاربر (UGC) نیز در متاورس مهم است. چگونگی کاهش بار ارتباطی، بدون تأثیر

بر اعتبارسنجی محتوا نیز چالشی برای متاورس است [همان].



شکل ۲: جدول تهدیدات امنیتی و حریم خصوصی و دسته‌بندی در کلان‌داده‌ی متاورس برای لایه‌های مختلف [Sun, 2022: 10 ،۳]

۳ اجتماع در متاورس

متاورس علاوه بر این‌که انواع جدیدی از فعالیت‌ها را ممکن می‌سازد، می‌تواند میزبان تقریباً تمام فعالیت‌هایی (مانند: معاشرت، کار، یادگیری، سرگرمی، خرید، تولید محتوا و ...) باشد که ما به‌صورت روزمره در آن‌ها شرکت داریم [Benjamins, 2023: 690 ،۴]. متاورس این پتانسیل را دارد که جامعه فعلی ما را متحول کند، جایی که کانال‌های جدیدی برای بیان خود و تعامل با دیگران بدون هیچ محدودیتی (مکان، زمان، نژاد، جنسیت) وجود دارد [Fernandez and other, 2022: 4 ،۱]. اما در این‌میان چالش‌هایی نیز وجود دارد، که در ادامه به بررسی آنها می‌پردازیم.

۱.۳ هویت افراد

در متاورس می‌توانید به جهان‌های مجازی مختلف با هویت یکسان دسترسی داشته باشید، بنابراین پیامدهای منفی جعل هویت بسیار شدیدتر از آن چیزی است که در حال حاضر در سرویس‌های دیجیتال وجود دارد و هر سرویس نام کاربری متفاوتی دارد [۴، Benjamins, 2023: 695].

اگر هویت شما ربوده شود، در برابر باج‌افزارها و اخاذی آسیب‌پذیرتر هستید. با سرویس‌های دیجیتال می‌توانید رمز عبور خود را تنظیم کنید؛ با این حال، در متاورس نمی‌توانید به سادگی آواتار خود را تغییر دهید چرا که مستقیما به وجود مجازی شما متصل است و تکنیک‌های جعل عمیق در سرقت هویت شما نقش خواهند داشت [همان].

۲.۳ سلامت افراد

علاوه بر اینکه ممکن است دستگاه‌های پوشیدنی در متاورس از نظر سلامتی، به متخصصان پزشکی کمک کند تا داده‌های فیزیولوژیکی بیماران مانند: دمای بدن، ضربان قلب و فشار خون را بررسی و نظارت کنند، این توانایی را نیز دارد که فرد متوفی را با استفاده از داده‌های بیومتریک او «احیا کند» [۵، Chen, 2023: 2]. اما باید بدانیم در این بین چالش‌هایی وجود دارد که در ادامه به آن می پردازیم:

برخی الگوریتم‌های پیشنهاد به قدری خوب هستند که کاربران نمی‌توانند از محتوای ارائه شده توسط آن‌ها جدا شوند. از نمونه‌های خاص می‌توان به اینستاگرام و تیک‌تاک اشاره کرد که ویدئو را به صورت کاملاً شخصی‌سازی شده به علاقه‌مندان ارائه می‌دهند. برخی از افراد به خصوص جوانان ممکن است به این اپلیکیشن‌های شبکه‌های اجتماعی اعتیاد پیدا کنند. آنها می‌توانند ساعت‌های زیادی در روز را صرف این موارد کنند و زمانی که در نهایت قطع ارتباط می‌کنند، احساس اضطراب می‌کنند و باید در اسرع وقت دوباره به هم متصل شوند. گیمینگ هم چالش مشابهی دارد، زمانی که هوش‌مصنوعی تجربه را بسیار بهینه می‌کند، مردم نمی‌توانند بازی را متوقف کنند و وقتی این کار را می‌کنند، احساس ناراحتی می‌کنند [۴، Benjamins, 2023: 694 as cited in Merkx, 2021]. اعتیاد به فن‌آوری را در سلامتی نباید دست‌کم گرفت، زیرا قدرت الگوریتم‌های تعامل (توصیه) در یک محیط همه جانبه مانند متاورس بسیار زیاد است؛ توصیه‌ها در یک پلتفرم متاورسی می‌توانند به قدری خوب باشند که فراتر از یک نقطه خاص، افراد ممکن است ترک فضا را در زمانی که باید/ می‌خواهند (بیش از حد) دشوار بدانند.

استفاده وسواسی از متاورس برای فرار از دنیای واقعی: افرادی که در دنیای واقعی شاد نیستند، ممکن است جایگزین جذابی در دنیای مجازی پیدا کنند که بتوانند همان کسی باشند که می‌خواهند باشند. آنها به‌جای اینکه برای بهبود زندگی واقعی خود تلاش کنند، از آن فرار می‌کنند و زندگی واقعی را به‌طور فزاینده‌ای بدتر می‌بینند.

کودکان به‌خصوص در برابر فناوری‌های فراگیر آسیب‌پذیر هستند، زیرا احتمال دارد واقعیت را با دنیای مجازی اشتباه بگیرند.

آزار و اذیت سایبری احتمالاً افزایش می‌یابد و تأثیر منفی بزرگ‌تری از طریق تجربه دیجیتالی پیشرفته و

فراگیر خواهد داشت که تقریباً به عنوان واقعیت درک می‌شود.

ناراحتی پس از واقعیت مجازی ایجاد می‌شود به‌طوری که دنیای واقعی ناامید کننده می‌شود و مردم احساس غم و اندوه را تجربه می‌کنند. واقعیت مجازی «خماری» یا بیماری سایبری، حتی گاهی با نشانه‌های فیزیکی همراه است که نشان‌دهنده احساس تهوع، خستگی، سرگیجه و بی‌نظمی بدنی است [۴، Benjamins, 2023: 694].

۳.۳ تبعیض و سوگیری

صدها مقاله در مورد این موضوع نوشته شده است که در آن سیستم‌های هوش مصنوعی، ممکن است براساس سوگیری، به تبعیض نامطلوب/غیرقانونی گروه‌های آسیب‌پذیر منجر شوند. در سیستم قضایی آمریکا با سیاه‌پوستان متفاوت از سفیدپوستان رفتار می‌شود، زنان وام‌های کمتری از بانک‌ها دریافت می‌کنند و کمتر توسط شرکت‌ها استخدام می‌شوند، فقط به خاطر جنسیتشان، و ... [۴، Benjamins, 2023: 692].

متاورس پر از اپلیکیشن‌هایی خواهد بود که از هوش مصنوعی برای پیش‌بینی و طبقه‌بندی استفاده می‌کنند و بنابراین این چالش نیز چالشی برای متاورس است [همان].

۴.۳ قطبیت در جوامع

الگوریتم‌های پیشنهاد می‌توانند حباب‌های فیلتری (Filter Bubbles) ایجاد کنند که در آن افراد تنها آنچه را که به آن علاقه دارند ببینند، تفکر خود را تقویت کنند و آن‌ها را از دیدگاه‌های جایگزین دور کنند. همان‌طور که در برخی از انتخابات‌ها و دیگر رویدادهای مهم دموکراتیک دیده‌ایم، الگوریتم‌های هوش‌مصنوعی می‌توانند در زمان نزدیک بودن انتخابات در بینش افراد تفاوت ایجاد کنند. باتوجه به تجربه همه‌جانبه متاورس، این ریسک احتمالا افزایش خواهد یافت [۴، Benjamins, 2023: 694].

۵.۳ آزادی

اگر متاورس ملزم به پیروی از قوانین محلی باشد، ماژول‌ها بر این اساس عوض می‌شوند؟ سؤال این است که چگونه با کاربران سایر مکان‌های جغرافیایی رفتار می‌شود و چگونه می‌توان این قوانین محلی را در متاورس اعمال کرد و دنیای مجازی جهانی را هدف گرفت. آیا تعاریف کشورهای مختلف از آزادی یکسان است؟ آیا کشورهای مدعی آزادی باید به قوانین سایر کشورها در این حوزه احترام بگذارند [۱، Fernandez and other, 2022: 4]؟

همان‌طور که دیدیم، یک عنصر کلیدی متاورس، واقعیت ترکیبی (MR) است، ترکیبی از دنیای دیجیتال و واقعی با استفاده از فناوری‌های واقعیت مجازی (VR) و واقعیت افزوده (AR). در نهایت، این ترکیب ممکن است آنقدر فراگیر شود که زندگی مجازی و واقعی مردم به هم گره بخورد و قابل تشخیص نباشد. اگر این اتفاق بیفتد، هر کسی که (بخش قابل توجهی از) متاورس را کنترل کند، می‌تواند بخش قابل توجهی از واقعیت را کنترل کند [۴، Benjamins, 2023: 695] و باید در نظر داشته باشیم ایجاد تعادل مناسب بین

آزادی بیان و پرهیز از محتوای مخرب برای انتشار در متاورس بسیار سلیقه‌ای و پیچیده است. [۵، Chen، ۲۰۲۳:۴]

۶.۳ قوانین و حکومت‌ها

اینترنت حقوق حاکمیت دولت‌ها را به چالش کشیده است، درنتیجه دولت‌ها می‌کوشند تا از روش‌های گوناگون حقوق حاکمیتی خود را بر اینترنت افزایش دهند [۱۳، حسنی، ۱۴۰۱: ۱۶۵ برگرفته از Puyvelde and Brantly,2019]. باتوجه به قوانین مختلف حاکم بر کشورها و فرهنگ و آداب و رسوم خاص هر حاکمیتی، چشم‌انداز متاورس تنها در یک مدل چندذی‌نفعی، با چندین طرف و ارائه‌دهندگان خدمات که برای ارائه طیف ارزش کاربران نهایی همکاری می‌کنند، تحقق می‌یابد. یکی از جنبه‌های مهم، که بر پذیرش گسترده متاورس حاکم است، امنیت و همچنین نگرانی‌های مرتبط با آن مانند اعتماد، حریم خصوصی و کنترل است [۹، Gupta and others, 2023: 2].

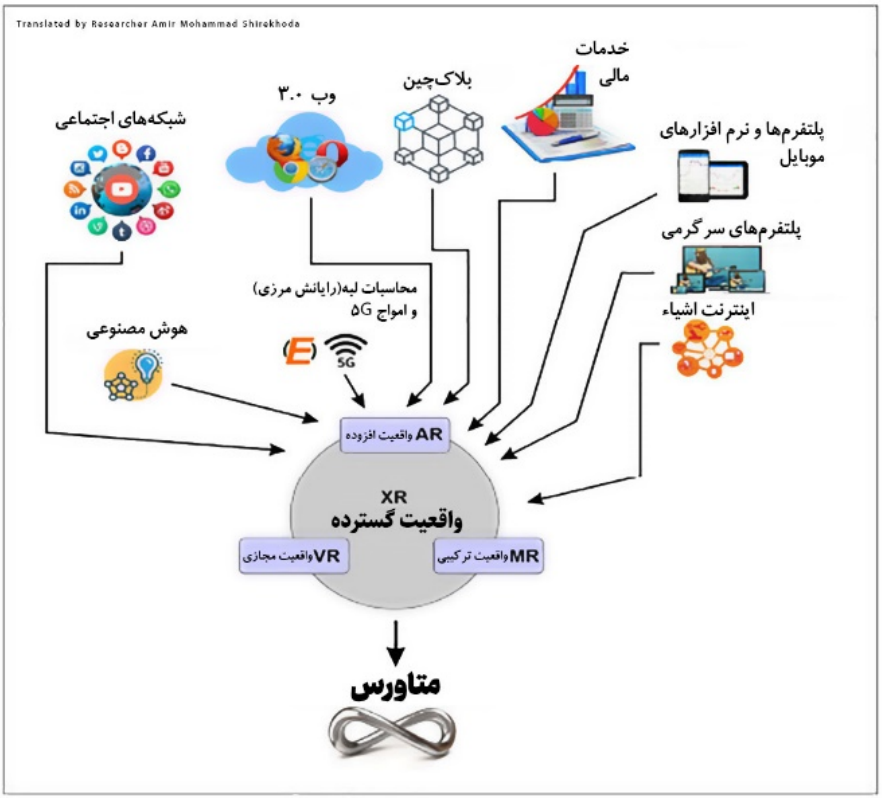
بنابراین ذی‌نفعان چندین کشور که باهم در ارتباط هستند، دور هم جمع می‌شوند، تا در مورد این که چگونه فن‌آوری می‌تواند یک ریسک اجتماعی یا اخلاقی را شکل دهد گفتگو کنند و توصیه‌هایی را به شرکت‌ها و دولت‌ها برای مقابله با آن‌ها صادر کنند. مثال‌هایی از چنین ابتکاراتی برای هوش‌مصنوعی عبارتند از: اصول هوش‌مصنوعی OECD و توصیه هوش‌مصنوعی یونسکو. سپس سازمان‌های فردی می‌توانند به دستورالعمل‌ها پایبند باشند. ما به شدت بر اهمیت چنین بحث‌های بین رشته‌ای و جهانی در مورد ریسک‌های اجتماعی و اخلاقی متاورس، از جمله مشارکت‌های عمومی خصوصی تاکید می‌کنیم. این بحث‌ها ورودی ضروری مقررات بالقوه هستند [۴، Benjamins, 2023: 695]. از آنجایی که دنیای متاورس بزرگتر از وب ۰.۲ است، هزینه نظارت نیز یک مشکل کلیدی است که باید حل شود. ما می‌توانیم از مقررات ضعیف فعلی رسانه‌های اجتماعی یاد بگیریم که شرکت‌های بزرگ فناوری همیشه سود را بر حقوق یا اخلاق ترجیح می‌دهند. بنابراین، شرکت‌هایی که بسترهای آموزشی متاورس را ارائه می‌دهند، تنها می‌توانند اپراتور باشند و نباید رگولاتور مطلق باشند. اینکه آیا تخلفی وجود دارد یا خیر، باید توسط اکثریت قریب به اتفاق کاربران درگیر تعیین شود. باید بین منافع شرکت و کاربران تعادل ایجاد کند [۶، lin، ۲۰۲۲:۸].

رگولاتوری و یا مقررات‌گذاری به این معنی است که برخی از کاربردهای این فن‌آوری توسط قانون کنترل شود. GDPR (مقررات حفاظت از داده اروپا) و قانون AI (مقررات آتی هوش مصنوعی اروپا) نمونه‌هایی از این موارد هستند. و البته یک رویکرد مبتنی بر ریسک به مقررات نشان می‌دهد که هر چه ریسک بالاتر باشد، قوانین بیشتری اعمال می‌شود. با توجه به تأثیر گسترده بالقوه متاورس، عاقلانه است که در مورد خطرات مهمی که ما - به عنوان جوامع - می‌خواهیم مطمئناً از آن‌ها اجتناب کنیم، فکر کنیم. اگر تنظیم متاورس خیلی زود انجام شود، این خطر وجود دارد که هنوز تجربه واقعی کمی از تأثیر اجتماعی و اخلاقی آن داشته باشیم [۴، Benjamins, 2023: 695].

۷.۳ مدل سامانه و فرضیات

اگرچه متاورس همان‌طور که پیش‌بینی می‌شد امروزه وجود ندارد، اما بسیاری از تکنولوژی‌های پشتیبانی کننده در حال رشد و توسعه آن می‌باشند. ادغام این فناوری‌ها همراه با پیشرفت‌های جدید، به تحقق چشم‌انداز آینده متاورس کمک خواهد کرد.

اکوسیستم فن‌آوری که در شکل ۳ نمایش داده شده است، متاورس را فعال می‌کند. کاملاً واضح است که فن‌آوری AR / VR / MR و XR بسترهای متاورس هستند و به کاربران اجازه می‌دهند به یک دنیای مجازی سه بعدی دسترسی داشته باشند. متاورس ممکن است در اولین دیدار، مجموعه‌ای از برنامه‌های کاربردی وب ۳.۰ با یک روکش واقعیت گسترده باشد که تجربه واقعیت مجازی محدودی را فراهم می‌کند. انتظار می‌رود شبکه‌های اجتماعی جزو اولین شبکه‌هایی باشند که به متاورس مهاجرت می‌کنند و به کاربران اجازه اشتراک‌گذاری و مصرف محتوای فراگیر همراه با وب ۳.۰ را می‌دهند. همچنین این فن‌آوری به کسب‌وکارها اجازه می‌دهد تجربه جدیدی از محصول را به کاربران ارائه دهند [۹، Gupta and others, 2023: 5].



شکل ۳: اکوسیستم فن‌آوری که متاورس را فعال می‌کند. [۹، Gupta،۲۰۲۳:۶]

۴ نتیجه‌گیری

متاورس در حال تکامل است و هنوز به بلوغ مورد انتظار خود نرسیده است و دولت‌ها و شرکت‌های مختلفی درصدد ایجاد و تکامل آن هستند. اما در این میان چالش‌هایی با توجه به تکنولوژی‌ها و فن‌آوری‌های فعلی برای ایجاد آن از لحاظ اجتماعی و امنیتی وجود دارد.

کپی رایت و این که چه کسی حق چاپ و فروش یک اثر هنری تولید شده توسط یک سیستم هوش مصنوعی را دارد؟ و یا جعل‌های آثاری که توسط هوش مصنوعی در دنیای فیزیکی فعلی و دنیای متاورسی قرار دارد از چالش‌های متاورس است. جمع‌آوری داده‌ها و اطلاعات شخصی افراد توسط سخت‌افزارهای پوشیدنی متاورس، دزدیده شدن ابزار، پول‌ها و اعتبار مجازی، حملات امنیتی در لایه تعامل، شبکه، محاسبات و اپلیکیشن، جعل هویت و اخاذی سایبری، تبعیض‌های نژادی، جنسیتی و ... هوش مصنوعی در متاورس، از بین رفتن سلامتی با استاده نادرست از پوشیدنی‌ها و یا ابزارهای متاورسی، اعتیاد نوجوانان و جوانان به الگوریتم‌های پیشنهاد قوی و وقت گذرانی دائمی در این فضا و عدم توانایی در برنامه‌ریزی صحیح و درست در زندگی فیزیکی واقعی، آزار و اذیت سایبری، شکل‌دهی به افکارعمومی و ایجاد قطبیت در جامعه، تعریف متفاوت حکمرانان از آزادی در این فضا، در نظر گرفته نشدن قوانین کشورها، احترام نگذاشتن به آداب و رسوم و فرهنگ جوامع و الزام به رعایت قوانین محلی اپلیکیشن در سطح جهانی از چالش‌های اجتماعی و امنیتی متاورس با توجه به سخت‌افزارها و نرم‌افزارهای موجود می‌باشد.

مراجع

[۱] حسنی، حسین، ۱۴۰۱، چالش‌های نوظهور دولت‌ها برای حکمرانی فضای سایبر، پیامدهای پلتفرمی شدن و پیدایش متاورس، نشریه علوم سیاسی، سال بیست و پنجم، شماره نود و هشتم، تابستان ۱۴۰۱.

[2] C. B. Fernandez and P. Hui, “Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse”, 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Bologna, Italy, 2022, pp. 272-277, doi: 10.1109/ICDCSW56584.2022.00058.

[3] Sun, J., Gan, W., Chen, Z., Li, J. and Yu, P.S., 2022. Big data meets metaverse: A survey. arXiv preprint arXiv:2210.16282.

[4] Benjamins, R., Rubio Viñuela, Y. and Alonso, C. Social and ethical challenges of the metaverse. AI Ethics 3, 689–697 (2023). https://doi.org/10.1007/s43681-023-00278-5

[5] Chen, C., Li, Y., Wu, Z., Mai, C., Liu, Y., Hu, Y., Zheng, Z. and Kang, J., 2023. Privacy Computing Meets Metaverse: Necessity, Taxonomy and Challenges. arXiv preprint arXiv:2304.11643.

[6] Lin, H., Wan, S., Gan, W., Chen, J., & Chao, H.C., 2022, December. Metaverse in education: Vision, opportunities, and challenges. In 2022 IEEE International Conference on Big Data (Big Data) (pp. 2857-2866). IEEE.

[7] Hutson, J., Banerjee, G., Kshetri, N., Odenwald, K., & Ratican, J., 2023. Architecting the Metaverse: Blockchain and the Financial and Legal Regulatory Challenges of Virtual Real Estate. Journal of Intelligent Learning Systems and Applications, 15.

[8] De Guzman, J.A., Thilakarathna, K., & Seneviratne, A., 2019. Security and privacy approaches in mixed reality: A literature survey. ACM Computing Surveys (CSUR), 52(6), pp. 1-37.

[9] Gupta, A., Khan, H.U., Nazir, S., Shafiq, M., & Shabaz, M., 2023. Metaverse Security: Issues, Challenges and a Viable ZTA Model. Electronics, 12(2), p. 391.

[10] Roose, K., 2022. An AI-generated picture won an art prize. Artists aren't happy. The New York Times, 2 September.

[11] Wang, Yuntao, Zhou Su, Ning Zhang, Dongxiao Liu, Rui Xing, Tom H. Luan, & Xuemin Shen, 2022. A Survey on Metaverse: Fundamentals, Security, and Privacy.

[12] Merkx, C., Jeroen, N. 2021. Virtual reality tourism experiences: addiction and isolation. Tour. Manag. 87, 104.

[13] Puyvelde, D.V. and Brantly, A.F., 2019. Cybersecurity: Politics, Governance and Conflict in Cyberspace. Cambridge: Polity Press.