تحلیل چالش‌های امنیتی فناوری متاورس و کاربردها

رحیم اصغری *[۱]، رؤیا کاظمی[۲]

۱- استادیار دانشگاه فنی و حرفه‌ای ایران، تهران

rasghari@tvu.ac.ir

۲- کارشناسی ارشد مهندسی برق گرایش مخابرات امن و رمزنگاری، دانشگاه صنعتی مالک اشتر تهران

Royakazemigorji@gmail.com

چکیده

متاورس یک محیط مجازی است که در آن کپی‌های مجازی افراد واقعی در تعامل و ارتباط هستند .آن‌ها مانند دنیای واقعی، با شکل مجازی خود به نام «آواتار» کارهایی را در دنیای مجازی انجام می‌دهند .این‌یک نوع دنیای موازی است . اکنون، ازنظر فنی، متاورس یک فضای مجازی است که با همگرایی بسیاری از فناوری‌های مختلف ایجادشده است .به واقعیت مجازی ، واقعیت افزوده ،HMD ، اینترنت اشیا، محاسبات فضایی، هوش مصنوعی و غیره نیاز دارد. متاورس به‌سرعت در حال تبدیل‌شدن به مفهوم ضروری بعدی است که شرکت‌ها به دنبال بهبود تعامل و UX برای کارمندان،مشتریان و شرکا هستند و درحالی‌که متاورس هنوز به اینجا نرسیده است،این بدان معنا نیست که شرکت‌ها نمی‌توانند چالش‌های امنیتی را در نظر بگیرند.

مفاهیم و توجیهات کلیدی برای متاورس شناخته‌شده است.خطرات مختلف امنیت سایبری و مسائل مربوط به حریم خصوصی ممکن است در این دنیای مجازی جدید وجود داشته باشد،اما کمتر موردتوجه قرارگرفته است.

این مقاله به بررسی برخی از مسائل مربوط به حریم خصوصی و امنیتی می‌پردازد که شرکت‌ها می‌توانند هنگام استفاده از متاورس انتظار داشته باشند با آن‌ها برخورد کنند و اینکه اکنون برای آماده شدن برای آن‌ها چه باید کرد.

کلمات کلیدی: متاورس، امنیت سایبری، زنجیره بلوکی.

۱. مقدمه

ایده متاورس اتفاق تازه‌ای نبوده است، چراکه، قبلاً در رمان‌های علمی تخیلی مانند تصادف برفی (استفنسون، ۱۹۹۲) نام و ایده آن شنیده‌شده بود. با نسخه سینمایی این رمان با عنوان یک بازیکن آماده تصویر روشن‌تری از متاورس در ذهن پژوهشگران این عرصه ایجاد شد. قبلاً هم نمونه‌های شناخته‌شده و محبوبی مانند زندگی دوم و بازی آنلاین چندنفره جهان وارکرفت، وجود داشت که توجه میلیون‌ها نفر را به خود جلب کرد .بااین‌حال، زمانی که مارک زاکربرگ به‌طور رسمی پروژه متاورس را در اکتبر ۲۰۲۱ اعلام کرد، متاورس تبدیل به یک کلمه کلیدی شد. بسیاری از مربیان و محققان چندین برنامه و سناریوهای اجرایی برای شیوه‌های یادگیری ارائه کردند. ایده‌های خلاقانه و نگاهی به چشم‌انداز آموزشی نشان می‌دهد ممکن است طیف وسیعی از امکانات ازجمله فضای مجازی که بازنمایی‌های واقعی از خود ارائه می‌دهد که احتمالاً جنبه اجتماعی

* **Corresponding author: Rahim Asghari**
Email: rsghari@tvu.ac.ir

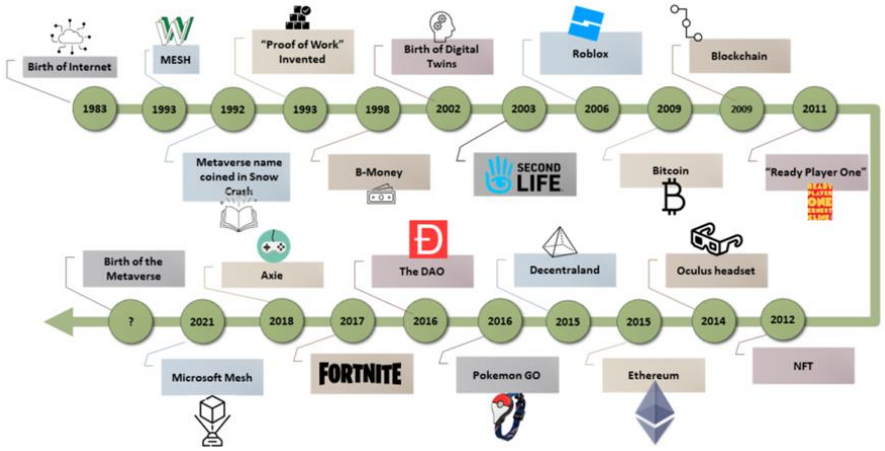
آموزش و یادگیری را هم افزایش می‌دهد، با فضای آموزش ترکیب شود. بااین‌حال، این مفاهیم نسبتاً جدید است و نیاز به بررسی پیشرفته‌ترین تحقیقات در مورد متاورس وجود دارد.

متاورس ترکیبی از پیشوند متا که به معنای فراتر رفتن و کلمه جهان است که یک محیط موازی یا مجازی مرتبط با جهان فیزیکی را توصیف می‌کند. متاورس اولین بار در سال ۱۹۹۲ توسط نیل استفنسون در رمان علمی تخیلی خود ابداع شد که یک جایگزین مبتنی بر واقعیت مجازی برای اینترنت را در نظر گرفته است. در این رمان، مردم سعی می‌کنند با کاوش در دنیای دیجیتال از طریق چندین آواتار دیجیتال از درد دنیای واقعی فرار کنند. از آن زمان متاورس به روش‌های گوناگون تعریف و بررسی‌شده است، ازجمله فضای جمعی در مجازی دنیای آینه‌ای، اینترنت تجسم‌یافته/اینترنت فضایی، جهان پسا واقعیت، یک محیط چندکاربره دائمی و پایدار که واقعیت فیزیکی را با مجازی دیجیتال ادغام می‌کند از آقای نینگ .

نوآوری‌ها در علوم رایانه تأثیر زیادی بر زندگی روزمره مردم‌دارند زیرا نحوه تعامل، برقراری ارتباط و تجارت افراد با یکدیگر را تغییر داده و بهبود می‌بخشند[1, 2, 3].

از دیدگاه کاربران نهایی، سه موج عمده فنّاورانه بر روی معرفی رایانه‌های شخصی، تبلت ها، اینترنت و دستگاه‌های تلفن هوشمند متمرکزشده است که به فناوری‌های فضایی و سه‌بعدی مانند واقعیت مجازی، واقعیت افزوده، واقعیت ترکیبی شهرت دارندکه آقای کامانوف آن‌ها را به‌خوبی بررسی کرده است. انتظار می‌رود این فناوری‌ها که پتانسیل آموزش، مراقبت‌های بهداشتی، ورزش، کسب‌وکار، سرگرمی و استفاده روزمره انسان، به‌ویژه کاربردهای آن برای بهبود آموزش برای بشریت را دارد، آینده دنیای فنّاوری را روشن‌تر کنند. کلمه متاورس یک کلمه ترکیبی بسته با دو جزء متا و جهان است. متاورس تکرار بعدی از اینترنت است که از محیط‌های مجازی سه‌بعدی آنلاین پشتیبانی می‌کند که در آن تجربیات دنیای واقعی را در یک محیط مجازی حس می‌کنیم و در دسترس عموم، از طریق واقعیت مجازی و واقعیت افزوده و همچنین از طریق دستگاه‌های رایانه شخصی و دستگاه‌های تلفن هوشمند قرار خواهد گرفت[4, 5].

متاورس هنوز در مرحله توسعه است و شرکت‌ها سرمایه‌گذاری انبوهی برای تبدیل این فضای تجاری و اجتماعی مناسب انجام می‌دهند.در شکل زیر یک جدول زمانی از متاورس نشان داده‌شده است.



شکل۱. جدول زمانی متاورس

۲. ویژگی‌های متاورس

هنگامی‌که متاورس خود را ایجاد می‌کنید، کنترل کامل برای تصمیم‌گیری و اجرای آنچه می‌خواهید دارید .چون یک فضای دیجیتال با کاراکترهای دیجیتال است.بااین‌حال، اگر این آزادی کامل نباشد، متاورس جذابیت خود را از دست خواهد داد . بنابراین وقتی یک برنامه متاورس ایجاد می‌کنید، باز بودن باید در قلب آن باشد. برای اطمینان از شفافیت در طول توسعه برنامه متاورس، شش ویژگی زیر ضروری است:

- قابلیت تعامل :قابلیت حمل‌ونقل داده‌ها و دارایی‌های دیجیتالی کاربر بدون محدودیت پلتفرم‌ها و برنامه‌های کاربردی.
- عدم تمرکز :کاربران باید کنترل کامل داده‌ها و دارایی‌های خود را داشته باشند.
- مداوم :متاورس باید دارای عناصر پایدار باشد .باید در اطراف فضای دیجیتال شما وجود داشته باشد، درست مانند منابع طبیعی اطراف شما.
- فضایی :دارایی‌های دیجیتال باید قابل یافتن و به‌راحتی قابل جستجو باشند.
- عامل جامعه :متاورس باید جامعه‌محور باشد و برندهای درگیر باید عامل جامعه در متاورس را تصدیق کنند.
- فردیت :کاربر یک فرد دیجیتالی در یک متاورس است .ازاین‌رو، تمام قوانین طبیعی فردیت مانند حریم خصوصی، حفاظت شخصی و خصوصی باید قابل‌اجرا باشد.

۳. نحوه عملکرد متاورس

درست مانند زندگی واقعی، متاورس لایه‌های زیادی دارد .درک این لایه‌ها برای به دست آوردن یک ایده عملی در مورد نحوه عملکرد متاورس مهم است.تاکنون ما متاورس را به‌عنوان یک جهان موازی دیده‌ایم .حال، اجازه دهید آن را از طریق ویژگی‌های بسیاری که نشان می‌دهد ببینیم .این ویژگی‌ها به شما نشان می‌دهند که چگونه درزمینهٔ اجتماعی و فناوری موجود، اپلیکیشن‌هایی برای متاورس بسازید.[6, 7]

○ تجربیات

این دروازه ورود به هر برنامه مجازی است .اشکال سه‌بعدی یا دوبعدی، نوع تجربه‌ای را که کاربر از متاورس به دست می‌آورد، تعریف می‌کند .می‌توان آن را به زبان ساده به‌عنوان فعالیتی که کاربر می‌تواند در متاورس شرکت کند تعریف کرد.به‌عنوان‌مثال، می‌تواند یک مسابقه اتومبیل‌رانی، یک تجربه خرید، بازی آنلاین یا هر نوع تعامل اجتماعی دیگری باشد.

○ کشف

ما به‌عنوان انسان عاشق کشف چیزها هستیم .زیرا هیچ‌چیز مانند کشف نیست که باعث شادی شود .بنابراین، هنگامی‌که در حال ساختن یک اپلیکیشن متاورس هستید، باید حملات مداومی از اکتشاف را برای کاربران ارائه دهید.به‌عنوان‌مثال یک نقشه درون برنامه‌ای گنج است .میراث خانوادگی که کشف کردید یا افرادی که غرفه‌ها را پیدا می‌کنند، و غیره .بخش کشف متاورس می‌تواند عنصر اجتماعی را برای جذاب‌تر کردن آن برای کاربران به کار گیرد.

- **اقتصاد خالق**

اقتصاد خلاق به آن گروه نوظهور سازندگان مانند توسعه‌دهندگان، تولیدکنندگان محتوا، طراحان و غیره اشاره دارد .ویژگی اصلی اقتصاد خلاق این است که ابزارها و بسترهای زیادی برای ایجاد فضاهای متاورس دارد .و این ابزارها به هیچ تجربه برنامه‌نویسی نیاز ندارند.

- **محاسبات فضایی**

محاسبات فضایی شامل محو کردن مرز بین واقعی و مجازی در فضای دیجیتال است .تجربه‌های واقعیت مجازی و واقعیت افزوده می‌توانند ترکیب شوند تا این امکان را فراهم کنند .محاسبات فضایی کاربران را قادر می‌سازد تا کنترل بیشتری بر مکان‌های سه‌بعدی داشته باشند و اشیاء دیجیتال را کشف کنند

- **عدم تمرکز**

متاورس در یک محیط غیرمتمرکز، باز و توزیع‌شده کار می‌کند .سازمان غیرمتمرکز خودمختار با مالکیت باز در مرکز آن قرار دارد.بلاک چین راه‌حلی برای گرایش متمرکز متاورس است .در حال حاضر بسیاری از پروژه‌های مجازی از قدرت بلاک چین استفاده می‌کنند. نمونه کاملی از این سناریو Decentraland است که بر روی بلاک چین اتریوم اجرا می‌شود.

- **رابط انسانی**

رابط انسانی جایی است که کاربر فرا جهان را کاوش می‌کند .تعامل انسان و رایانه شامل هدست های واقعیت مجازی، فناوری‌های لمسی، عینک‌های هوشمند و غیره است.

- **زیرساخت**

این پایه برای تمام لایه‌های فوق است .به‌کارگیری شبکه نسل پنجم مخابرات برای ظرفیت بهتر شبکه، تأخیر و کاهش تراکم.دستگاه‌های رابط انسان و ماشین باید ازMEMS ، باتری‌های کوچک و بادوام ساخته شوند .وای فای، بلاک چین، هوش مصنوعی، پردازنده‌های گرافیکی، معماری ابری و غیره زیرساخت‌های ضروری دیگر را تشکیل می‌دهند.

۴. فناوری‌های مورداستفاده برای ایجاد متاورس

فن‌آوری‌های کلیدی که متاورس را تشکیل می‌دهد عبارت‌اند از:

- هوش مصنوعی

هوش مصنوعی با پتانسیل خود برای پردازش داده‌ها با سرعت‌بالا برای توسعه برنامه‌های کاربردی متاورس بسیار مهم است . تکنیک‌های یادگیری ماشین و الگوریتم‌های هوش مصنوعی را برای ایجاد یک جهان مجازی مثال‌زدنی ترکیب می‌کند.

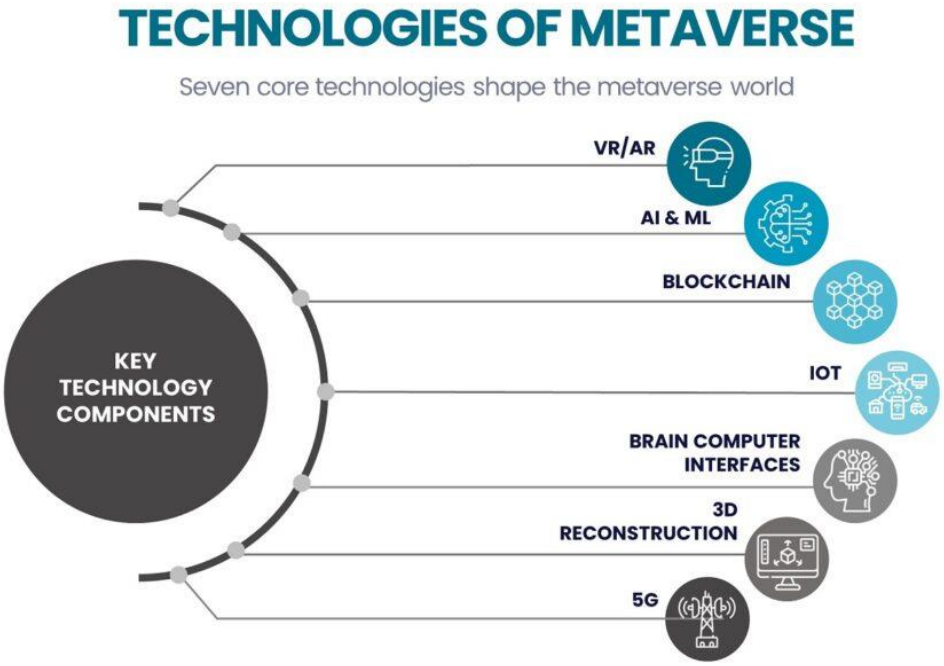
- بلاک چین

نقش فناوری بلاک چین در ساخت اپلیکیشن متاورس بی‌نظیر است .ویژگی‌های کلیدی متاورس مانند عدم تمرکز، شفافیت، مالکیت دیجیتال، اثبات آن، حاکمیت، انتقال ارزش، قابلیت همکاری، دسترسی و غیره به آن بستگی دارد.

- واقعیت مجازی

چیزی که با عنوان واقعیت مجازی شناخته می‌شود یک کامپیوتر یک محیط واقعی را در بستر مجازی تقلید می‌کند. اکثر تجربه واقعیت مجازی شامل تجسم است که می‌تواند بر روی یک مانیتور کامپیوتر یا یک دستگاه نمایشگر سه‌بعدی نمایش

داده شود. کاربران می‌توانند با استفاده از محیط مجازی با محیط واقعی درگیر شوند. گجت‌های واقعیت مجازی می‌توانند یک محیط شبیه‌سازی‌شده بسیار شبیه به دنیای واقعی را برای شما تجسم کنند، مانند شبیه‌سازی که برای آموزش خلبانان استفاده می‌شود. از طرف دیگر، یک محیط شبیه‌سازی‌شده نیز می‌تواند بسیار متفاوت از دنیای واقعی باشد، مانند بازی‌هایی که امروزه توسط توسعه‌دهندگان بازی در حال ساخت است. به دلیل محدودیت‌های فنی، مانند محدودیت‌های مربوط به قدرت پردازش و وضوح تصویر، تولید یک تجربه واقعیت مجازی که تا حد امکان در عمل واقعی باشد، بسیار چالش‌برانگیز است. از سوی دیگر، پیش‌بینی می‌شود که چنین محدودیت‌هایی در آینده‌ای نه‌چندان دور درنتیجه پیشرفت‌ها در فناوری‌های مربوط به ارتباطات بصری و داده‌ای و همچنین قدرت پردازش حذف شوند.



شکل۲. فناوری های کلیدی بکار رفته در متاورس [2]

- واقعیت افزوده

واقعیت افزوده فناوری جدیدی است که دنیای واقعی را با دنیای مجازی از طریق استفاده از دستگاه‌های مختلف مانند وب کم، دوربین موبایل یا رایانه همراه با استفاده از نرم‌افزارهای مختلف، ترکیب می‌کند که امکان دیدن تصاویری را که شبیه اشیاء هستند، به‌صورت اشیاء سه‌بعدی در بالای سطح واقعی روی صفحه‌نمایش ، ممکن می‌سازد. واقعیت افزوده با ترکیب دنیای واقعی با دنیای مجازی ایجادشده است. علاوه بر این، واقعیت افزوده را می‌توان با نمایش ورودی از حس‌گرهای دوربین یکپارچه در هدست های واقعیت مجازی شکل داد که این باعث می‌شود بینندگان این تصور را ایجاد کنند که در یک رویداد "واقعی" شرکت می‌کنند.

- واقعیت ترکیبی

واقعیت ترکیبی نقاط قوت فن‌آوری‌های واقعیت مجازی و واقعیت افزوده را باهم ترکیب می‌کند و با ایجاد تجسم‌هایی که کاربران آن می‌توانند در محیطی که دنیای واقعی را با دنیای مجازی ترکیب می‌کند، تعامل داشته باشند، آن را به سطح

بعدی می‌برد. با استفاده از فناوری لمس و تصویربرداری ، واقعیت ترکیبی به ما اجازه می‌دهد تا دنیای اطراف خود را حتی در هنگام تعامل با محیط مجازی بدون نیاز به برداشتن عینک، با دست خود ببینیم و تجربه کنیم. این فناوری به کاربران این امکان را می‌دهد که یک‌پا یا دست خود را در دنیای واقعی قرار دهند و طرف دیگر را در دنیای مجازی قرار دهند.

- بازسازی سه‌بعدی

یکی از سؤالات کلیدی که توسعه‌دهندگان نتوانستند به آن پاسخ دهند این بود :چگونه می‌توان یک متاورس نزدیک به تجربه واقعی ایجاد کرد؟ پاسخ به این امر در قالب بازسازی سه‌بعدی آمد.

با استفاده از این فناوری می‌توانید فضاهای واقعی و طبیعی ایجاد کنید .دوربین‌های سه‌بعدی ویژه به شما این امکان را می‌دهند که دنیای اطراف خود را به‌صورت آنلاین بچرخانید .این به ایجاد دوقلو دیجیتال دنیای واقعی ما کمک می‌کند.

۵. نگرانی‌های امنیتی متاورس

هنگامی‌که شما متاورس را ایجاد می‌کنید، دنیایی درست مانند دنیای واقعی، با تمام نواقص و چالش‌هایش ایجاد می‌کنید . بنابراین، اکنون زمان آن است که به نگرانی‌های امنیتی کلیدی متاورس نگاه کنیم.

دو مدل اصلی در متاورس وجود دارد:

واقعیت مجازی یک واقعیت مصنوعی را از طریق یک هدست VR ارائه می‌کند، که میدان دید کاربر را برای ارائه یک تجربه فراگیر در اختیار می‌گیرد .سایر اشکال تجربه‌های غوطه‌ور شامل ردیابی صوتی و موقعیت بدن برای فعال کردن دست‌ها یا سایر اعضای بدن فرد برای تعامل با محیط مجازی است.

واقعیت افزوده (AR) نسبت به VR غوطه‌ورتر است. از طریق یک نوع لنز، پوشش‌های مجازی را در بالای دنیای واقعی اضافه می‌کند .کاربران همچنان دید معمولی از محیط اطراف خوددارند .نمونه‌های واقعیت افزوده شامل تلفن هوشمندی با استفاده از برنامه Waze یا ابزارهای پوشیدنی مانند هولولنز مایکروسافت است .میزبان می‌تواند موقعیت مکانی کاربر را ببیند و می‌تواند نیت آن‌ها را حدس بزند.

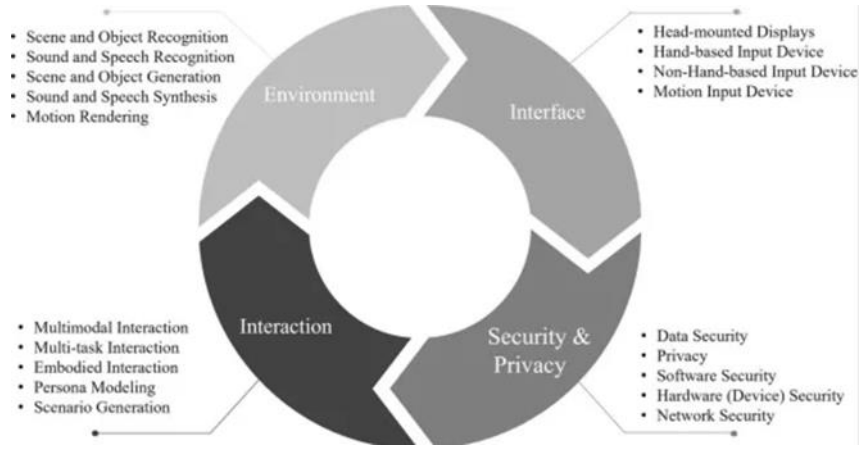
توجه به این نکته مهم است که در تجربیات VR به‌طورکلی، در حال حاضر نباید انتظاری از حقوق حریم خصوصی وجود داشته باشد .در محیط‌هایAR ، جایی که جای پایی در دنیای فیزیکی وجود دارد، حقوق حریم خصوصی روی زمین محکم‌تر است.

۵.۱.خطرات امنیتی دستگاه‌های واقعیت افزوده و واقعیت مجازی

مهم‌ترین خطراتی که دستگاه‌های واقعیت افزوده و واقعیت مجازی با آن روبرو هستند عبارت‌اند از:

- حریم خصوصی
- مهندسی اجتماعی
- امنیت داده‌ها
- بدافزار و باج افزار
- محتوای غیرقابل‌اعتماد
- آسیب فیزیکی

- چالش‌های اعتدال : در متاورس، هیچ دسترسی پشتیبانی وجود ندارد .این می‌تواند کاربران را در یک دنیای دیجیتال گسترده سرگردان کند.
- Darkverse: دقیقاً مانند دارک وب، دارک ورس در داخل متاورژن وجود دارد .حضور شبه فیزیکی کاربران آن را مهیب و خطرناک‌تر می‌کند .سرقت هویت و جعل در دنیای تاریک نیز یک تهدید واقعی است.
- کلاه‌برداری مالی: متاورس حجم عظیمی از تجارت الکترونیکی را هدایت می‌کند و درنتیجه خطر کلاه‌برداری مالی را به همراه خواهد داشت .افرادی که تمایلات جنایی دارند احتمالاً به سمت آن‌ها کشیده می‌شوند.
- مسائل مربوط به حریم خصوصی: NFT ها به‌نوعی مالکیت دارایی‌های دیجیتال را تنظیم می‌کنند، اما نمی‌توانند برای آن‌ها ذخیره‌سازی کنند .ازاین‌رو، امکان حملات باج را باز می‌کند .باج افزار می‌تواند فایل‌های NFT را رمزگذاری کرده و بدون تغییر مالکیت آن‌ها، آن‌ها را برای کاربران غیرقابل‌دسترس کند.
- مهندسی اجتماعی : شامل دست‌کاری روانی کاربران برای فریب دادن آن‌ها به ارائه داده‌های حساس است .و سپس با این اطلاعات حساس، هکرها می‌توانند به اطلاعات خصوصی، رمز عبور و غیره کاربران دسترسی پیدا کنند. برخلاف دنیای واقعی که اسنادی برای اثبات هویت وجود دارد، کاربران متاورس باید با استفاده از فیلم‌های ویدئویی، ضبط صدا و عصاره‌های ویژگی‌های چهره خود را با کمک انسان‌های دیجیتال شناسایی کنند .این نمایش‌های دیجیتال ابزاری هستند که کاربران می‌توانند از طریق دستگاه‌های XR با یکدیگر ارتباط برقرار کنند . متأسفانه، هکرها می‌توانند با استفاده از تکنیک‌ها و ترفندهایی که افراد در زندگی واقعی قربانی آن می‌شوند، کاربران را فریب دهند تا اطلاعات شخصی آن‌ها را فاش کنند.
- باج افزار: این‌یکی دیگر از نگرانی‌های امنیتی است که می‌توان آن را به مؤلفه VR متاورس نسبت داد. هکرها می‌توانند ویژگی‌ها و قابلیت‌های خاصی را در پلتفرم‌ها و دستگاه‌های VR ادغام کنند و کاربر را ترغیب کنند تا اطلاعات شخصی خود را آشکار کند و آسیب‌پذیری‌ها را برای انجام یک حمله باج افزار کشف کند.



شکل۳. متاورس با محیط، رابط، تعامل، امنیت و حریم خصوصی

- تهدیدات فیزیکی سایبری : وب فضایی که یک محیط محاسباتی مبتنی بر سه‌بعدی است که در آن میلیاردها دستگاه متصل رابط‌های VR/AR/MR/XR ایجاد می‌کنند .ازآنجایی‌که این‌یک دامنه تعاملی خواهد بود، برنامه‌های کاربردی متاورس مستعد حملات سایبری-فیزیکی خواهند بود.

- سرقت مدارک و هویت :سرنوشت متاورس می‌تواند به سطح امنیتی‌ای که ارائه می‌کند بستگی داشته باشد .با توجه به اینکه پلتفرم‌های رسانه‌های اجتماعی موجود را می‌توان با حساب‌های ساختگی متعدد آغشته کرد، به‌احتمال‌زیاد متاورس از چنین حادثه‌ای فرار نخواهد کرد.در متاورس، کاربران با قصد مجرمانه می‌توانستند هویت هرکسی را که می‌خواهند با سهولت نسبی فرض کنند .این‌یکی از بزرگ‌ترین چالش‌های متاورس خواهد بود زیرابه این معنی است که کاربران می‌توانند اطلاعات مالی و شخصی خود را در معرض خطر قرار دهند .علاوه بر این، هکرهایی که به‌خوبی مجهز هستند، می‌توانند با استفاده از داده‌های دستگاه‌هایXR ، نسخه‌های تکراری دیجیتالی از شخصیت متاورس تولید کنند و می‌توانند تجربه کاربر دیگر را همپوشانی کنند و درنتیجه یک حمله مهندسی اجتماعی انجام دهند.

انواع حملات سایبری در متاورس عبارت‌اند از:

- فیشینگ
- بدافزار و باج افزار
- امنیت ابر داده
- امنیت وب ۳
- هک آواتار
- دیپ فیک
- جعل NFT

۵.۲. سه مؤلفه پیاده‌سازی امنیت سایبری در متاورس

سه مؤلفه برای امنیت سایبری در متاورس وجود دارد :امنیت سایبری پلتفرم میزبانی، امنیت سایبری اموال (اجاره‌کنندگان در پلتفرم) و امنیت سایبری کاربران دارایی (مصرف‌کنندگانی که در داخل ملک تعامل دارند). خطرات اصلی مرتبط با هر جزء و نحوه رسیدگی به آن‌ها را بیان کنیم.

1. صاحبان پلت فرم

فقدان مقررات: بزرگ‌ترین غول‌های فناوری در حال سرمایه‌گذاری در ساخت پلتفرم‌های متاورس هستند .بااین‌حال، به دلیل فقدان مقررات، اقدامات امنیتی و حفظ حریم خصوصی متناقض هستند .این منجر به شکستگی و ناسازگاری UX و انتظارات می‌شود. نحوه رسیدگی به خطر: دارندگان پلتفرم باید از فرصت برای همکاری در مجموعه‌ای از دستورات استفاده کنند و موافقت کنند که به یک کد رفتاری سخت‌گیرانه پایبند باشند .این نشان‌دهنده رهبری و آگاهی از چالش‌های امنیت سایبری در متاورس است .درنهایت، به پذیرش پلت فرم نیز کمک می‌کند.

نظارت بر پلتفرم‌های متاورس نیاز به مداخله فعال و واکنشی دارد .یک تیم نظارتی جامع ایجاد کنید که توسط یک استراتژی امنیتی فعال‌شده توسط هوش مصنوعی پشتیبانی می‌شود .از بینش‌های هوش مصنوعی برای شناسایی فعال هرگونه سوءاستفاده، سوء رفتار یا ارائه نادرست استفاده کنید و به‌سرعت اقدام کنید .همچنین باید مکانیسم‌هایی برای صاحبان املاک و مشتریان آن‌ها وجود داشته باشد تا مسائل امنیتی و حریم خصوصی را مطرح کنند.

2. صاحبان املاک / اجاره دهندگان

فقدان دانش در مورد بهترین شیوه‌های امنیت سایبری متاورس: کاربران املاک مجازی شامل مشتریان، شرکا و میهمانان هستند که همه یا برخی از آن‌ها مبتدی به متاورس هستند .در بسیاری از موارد، صاحبان املاک/اجاره‌کنندگان نیز تازه‌وارد هستند و فضایی را ایجاد می‌کنند که در آن بهترین شیوه‌های امنیت سایبری و حریم خصوصی یا نادیده گرفته می‌شوند یا اشتباه تفسیر می‌شوند، نادرست معرفی می‌شوند یا صرفاً نادیده گرفته می‌شوند.[7, 8]

نحوه رسیدگی به خطر :صاحبان املاک باید برای درک امنیت و حریم خصوصی پلتفرمی که در آن میزبانی می‌شوند، وقت بگذارند، سرویس‌هایی را که در حال ساخت و/یا در پلتفرم استفاده می‌کنند بررسی کنند و برای اطمینان از امنیت و حریم خصوصی گام‌هایی بردارند .آن خدمات گام مهم بعدی، ترجمه خط‌مشی به کاربران دارایی آن‌ها به شکلی قابل‌فهم است.

داده‌های کاربر در متاورس شامل حسگر، مکان، داده‌های فیزیولوژیکی و اجتماعی است .مهم است که صاحبان دارایی درک کنند که چه داده‌های کاربر توسط ارائه‌دهنده پلتفرم جمع‌آوری می‌شود و سپس روی‌داده‌های کاربری که جمع‌آوری می‌کنند نیز لایه‌بندی کنند .سپس آن‌ها باید - به شکل قابل‌فهم برای کاربر - ارائه دهند که این داده‌ها چیست، چرا جمع‌آوری می‌شوند و مشتریانشان چه حقوق داده‌ای دارند.

3. مصرف‌کنندگان/کاربران

عدم‌حمایت از مصرف‌کننده استفاده از هدست‌هایی که دارای حسگرها و ردیاب‌ها برای ارائه تجربه‌ای فراگیر هستند، می‌تواند باعث شود مصرف‌کنندگان متوجه نحوه و میزان جمع‌آوری داده‌های شخصی خود نشوند یا به آن توجه نکنند . مصرف‌کنندگان در معرض خطر هستند، زیرا برخلاف دنیای واقعی که قوانین حفظ حریم خصوصی داده‌ها را تقویت می‌کند، مانند GDPR وCCPA ، چنین معادلی در متاورس وجود ندارد.

فقدان فرآیندهای تأیید اعتبار، به‌ویژه برای نمایش آواتار، مصرف‌کنندگان را در معرض خطر قرار می‌دهد .دیپ‌فیک‌ها در ویدیوها رایج‌تر می‌شوند، مانند جعل هویت در تماس‌های کنفرانسی .متاورس چالش بزرگ‌تری را ارائه می‌دهد.

همچنین، حقوق ارتباط بسته به پلت فرم متاورس متفاوت است .در دنیای واقعیت افزوده، حقوق ارتباطی تعاملات فیزیکی به مجازی و همچنین تعاملات مجازی به مجازی را پوشش می‌دهد .در دنیایVR ، همه تعاملات مجازی هستند.

نحوه رسیدگی به خطر :مصرف‌کنندگان باید تلاش کنند تا حفاظت‌های امنیتی و حریم خصوصی را که توسط ارائه‌دهنده پلتفرم و مالک ملک استفاده می‌شود، درک کنند .این وظیفه مصرف‌کننده است که از ارائه‌دهنده پلتفرم و صاحب‌ملک سؤال بپرسد .چه داده‌هایی در حال جمع‌آوری است؟ تا کی قراراست ذخیره شود؟ چه حقوق داده‌ای برای پاک‌سازی این داده‌ها وجود دارد؟

مصرف‌کنندگان نیز باید در به اشتراک‌گذاری هرگونه اطلاعات هوشیار و مراقب باشند .آن‌ها باید فعالانه با صاحبان املاک تماس بگیرند تا در صورت وجود هرگونه شک و تردید، تأیید شود.

۵.۳. چالش‌های امنیتی منحصربه‌فرد VR وAR

محیط‌های واقعیت مجازی و واقعیت افزوده سؤالات امنیتی و حریم خصوصی بسیاری را مطرح می‌کنند .چالش‌ها شامل موارد زیر است.

- **چالش‌های امنیتیVR**

تکیه: فقدان استانداردها و خدمات مشترک در متاورس نوپا به این معنی است که کاربران یک محصول یا پلتفرم برای ایمنی تجربه به مالک پلتفرم متکی هستند .به‌عنوان‌مثال، شرکت‌های اولیه‌ای که استفاده از Second Life را انتخاب کردند -یکی از اولین پلتفرم‌های متاورس - باید برای امنیت، حفاظت از هویت، حریم خصوصی و حتی تراکنش‌های مالی کاملاً به آن پلتفرم تکیه می‌کردند.

مسئولیت: ملکی که کاربر در یک محیط VR خریداری یا اجاره می‌کند، چالش‌های امنیتی و حریم خصوصی بسیاری را ایجاد می‌کند که نیاز به حل دارد .چه کسی اجازه ورود یا مسدود شدن در ملک را دارد؟ آیا مالک ملک حق دارد تصمیم بگیرد که چه کسی می‌تواند و چه کسی نمی‌تواند وارد شود؟ در داخل این املاک چه اتفاقی می‌افتد؟ آیا معاملات مالی یا غیرقانونی در داخل ممکن است رخ دهد؟

احراز هویت: شناخت موجودیت‌ها همان کسانی هستند که می‌گویند آن‌ها چالش‌برانگیز است .چگونه ثابت می‌کنید افرادی که با آن‌ها در ارتباط هستید همان‌هایی هستند که ادعا می‌کنند هستند؟ برای مثال پزشکی از راه دور را در نظر بگیرید . چگونه بیماران می‌دانند فردی که با او در ارتباط هستند یک متخصص پزشکی است؟ چگونه یک مالک ملک می‌تواند قبل از اجازه دادن به پزشکان، اعتبارنامه‌های پزشکان را واجد شرایط کند؟

مسئولیت: اگر کلاه‌برداری، آزار و اذیت یا سایر اشکال سوءاستفاده رخ دهد، آیا صاحب محیط واقعیت مجازی پاسخگو است؟

حریم خصوصی: هیچ مقرراتی برای محیط‌های VR وجود ندارد - هنوز .با توجه به جمع‌آوری و تجزیه‌وتحلیل داده‌های تهاجمی صاحب پلتفرم VR و این واقعیت که بسیاری از داده‌ها دائماً توسط کاربران ناشناخته برای کاربر VR به اشتراک گذاشته می‌شوند، مقررات به‌سرعت پایین خواهند آمد؛ اما اکنون حفاظت یا اشتراک‌گذاری این داده‌ها کاملاً در اختیار صاحب پلتفرم است.

فیدهای تبلیغاتی مالک متاورس کنترل کاملی بر این دارد .دقیقاً مانند دنیای واقعی که در آن‌یک بنر تبلیغاتی می‌تواند جلوی فروشگاه فیزیکی شما نصب شود، تبلیغات مجازی نیز می‌توانند جلوی ویترین فروشگاه مجازی شما نمایش داده شوند .این تبلیغات ممکن است توسط مشتریان شما قدردانی شود یا خیر، اما شما کنترلی روی آن ندارید.

اکانت های ممتاز و هک: تسخیر حساب‌های پشتیبانی مشتری یا مدیریت می‌تواند منجر به خطر افتادن یک محیط واقعیت مجازی شود که اگر شناسایی نشود، می‌تواند به بسیاری از کاربران آسیب برساند.

به خطر افتادن نقطه دسترسی ازآنجایی‌که ورود به متاورس VR معمولاً از طریق یک هدست انجام می‌شود، به خطر افتادن نقطه پایانی هدست می‌تواند منجر به تسخیر کامل آواتار آن کاربر شود.

جاسوسی آواتارها می‌توانند ظاهر را تغییر دهند، به این معنی که جلسات، چت‌های شخصی و سایر تعاملات بدون اطلاع طرف‌های آسیب‌دیده در معرض جاسوسی و نفوذ هستند.

- **چالش‌های امنیتیAR**

یکپارچگی دادهAR : شامل همپوشانی داده‌های شخص ثالث است، بنابراین هرگونه مصالحه در یکپارچگی داده‌ها می‌تواند چالش بزرگی باشد .برای مثال، اگر یک برنامه مکان که روی یک هدست قرار داده‌شده است از داده‌های مکان معیوب استفاده کند، می‌تواند منجر به راهنمایی‌های نادرست به کاربر شود.

امنیت فیزیکی: کاربران معمولاً در دنیای واقعی با پوشش AR حرکت می‌کنند و امنیت فیزیکی را به یک نگرانی تبدیل می‌کند .اگر کاربران بیش‌ازحد در فضاهای مجازی غوطه‌ور شوند، ممکن است به خود یا اطرافیانشان آسیب وارد کنند.

۵.۴. راه‌حل‌هایی برای امنیت سایبری در متاورس

برخی از راه‌حل‌های بالقوه برای مسائل امنیت سایبری متاورس عبارت‌اند از:

- **توسعه پروتکل‌های امنیتی قوی**: توسعه‌دهندگان متاورس باید با اجرای پروتکل‌های امنیتی قوی برای محافظت از داده‌های شخصی و مالی کاربران، امنیت را در اولویت قرار دهند. این شامل استفاده از فناوری‌های رمزگذاری، احراز هویت دومرحله‌ای و کانال‌های ارتباطی امن برای جلوگیری از دسترسی غیرمجاز به اطلاعات حساس است.
- **آموزش کاربران:** آموزش کاربران در مورد خطرات امنیت سایبری و بهترین شیوه‌ها برای ترویج رفتار ایمن در متاورس ضروری است. این شامل ارائه منابع و دستورالعمل‌هایی در مورد امنیت رمز عبور، مرور ایمن، و حملات مهندسی اجتماعی برای حفظ امنیت است.
- ایجاد کردن یک استراتژی اعتدال مبتنی بر جامعه تا کاربران را قادر سازد، رفتار نامناسب را قبل از تشدید گزارش کنند.
- ابزارهای امنیتی مجهز به هوش مصنوعی را برای شناسایی ناهنجاری‌ها و تهدیدات مبتنی بر رفتار به کار بگیرید زیرابه شما این امکان را می‌دهد که تهدیدها را شناسایی کرده و از حملات قبل از وقوع سریع جلوگیری کنید.

۶. مراجع

[1] Pranto Saha, Kh. Tanveer Iftekhar, Md Sohidul Islam, Khandaker Raiyan Rahman, Sholaiman Khan Shitol, " Use of Metaverse Technology in Education Domain ", Journal of Metaverse , 2023.
[2] "Metaverse: Threat or Opportunity for Our Social World? In understanding Metaverse on sociological context", Journal Metaverse, 2023.
[3] L.-H. Lee, T. Braud, P. Zhou, L. Wang, D. Xu, Z. Lin, A. Kumar,C. Bermejo, and P. Hui, “All one needs to know about metaverse: A complete survey on technological singularity", virtual ecosystem, and research agenda,” arXiv preprint arXiv:2110.05352, 2021.
[4] R. Asghari. "A modified continuous lightweight authentication to increase the information security on internet of Things." *Computational Sciences and Engineering*, 2021, 1.2: 109-121.
[5] B. Fathi Vajargah, R. Asghari, "Application of chaotic maps in designing cryptographic pseudo random number generators", Journal of Optoelectronics and Advanced Materials, 2017, 109-116.
[6] B. Fathi Vajargah, R. Asghari, "A novel pseudo-random number generator for cryptographic applications", Indian Journal of Science and Technology, 2016, 1-5.
[7] B. Fathi Vajargah, R. Asghari, "Application of chaotic maps in designing cryptographic pseudo random number generators", Journal of Optoelectronics and Advanced Materials, 2017, 109-116.
[8] A. Emami, H. Yajam, M. A. Akhaee, R. Asghari, " A scalable decentralized privacy-preserving e-voting system based on zero-knowledge off-chain computations", Journal of Information Seurity and Applications, 2023.