İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi
Istanbul Sabahattin Zaim University Journal of the Institute of Science and Technology
https://dergipark.org.tr/tr/pub/izufbed

Metaverse: Sanal Dünyadan Gerçek Gizlilik ve Güvenlik Problemlerine

Tugay Mandal[a1,*], Ahmet Bedirhan Sağır[a2], Mehmet Nuri Alparslan Öztürk[a3], Muhammed Yusuf Uysal[a4], Murat Külekçi[a5], Banu Yeşim Büyükakıncı[b6]

[a] *İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü,, İstanbul, Türkiye*
[b] *İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Tekstil Mühendisliği Bölümü, İstanbul, Türkiye*

İstanbul Sabahattin Zaim Üniversitesi Fen Bilimleri Enstitüsü Dergisi (2022) 4 (2): 100-106
https://doi.org/10.47769/izufbed.1130284

[1] 0000-0002-9589-2712; [2] 0000-0001-6907-4807; [3] 0000-0002-5070-9822, [4] 0000-0003-1296-8417, [5] 0000-0002-0511-9161, [6] 0000-0001-7597-4406

YAYIN BİLGİSİ

Yayın geçmişi:
Gönderilen tarih: 13 Haziran 2022
Kabul tarihi:17 Temmuz 2022

Anahtar kelimeler:
Metaverse
Veri Güvenliği
Gizlilik
Sanal Gerçeklik
Artırılmış Gerçeklik
Kişisel Bilgi

ÖZET

Metaverse günümüzde çok sık karşılaşılan bir terim olsa da 1990'lardan beri var olan, gerçek dünya benzeri yapay dünyalar veya 3 boyutlu dünyalar konseptidir. Her on yılda bir bilgi ve iletişim teknolojilerinde yaşanan büyük sıçramalarla birlikte; sanal gerçeklik, artırılmış gerçeklik, Web 3.0 gibi yeni teknolojilerin ve toplumsal yönlendirmenin de etkisiyle, daha önceki sıçramalarla beraber yaşanan veri güvenliği ve özel hayatın gizliliği sorunları yeniden gün yüzüne çıkmıştır. Bu çalışmada henüz kavramsal olarak tüm çerçevesi çizilmemiş, "Metaverse" kavramı ve metaverse'te karşılaşılabilecek veri güvenliği ve gizlilik sorunları değerlendirilmiştir. Kullanıcı profili oluşturma, kullanıcı gizliliği ve gizliliğe karşı önlemler değerlendirilmiş, güvenlik konusunda kimlik yönetimi, kullanıcı bilgilerinin korunması ve toplum yönetimine dair araştırma yapılmıştır.

Metaverse: From Virtual Word to Real Security and Privacy Problems

ARTICLE INFO

Article history:
Received: 13 June 2022
Accepted: 17 July 2022

Key words:
Data Security
Privacy
Virtual Reality
Augmented Reality
Personal Information

ABSTRACT

Although the metaverse is a very common term encountered nowadays, it is the concept of real-world-like artificial worlds or 3-dimensional worlds that has existed since the 1990s. As well as with the great leaps happened in information and communication technologies in every ten years; with the effect of social guidance and new technologies such as virtual reality, augmented reality and Web 3.0, data security and right of privacy issues, experienced together with the previous leaps, have come to the daylight again. In this study, the concept of "Metaverse", which has not yet been conceptually outlined, and the data security and right of privacy issues that may be encountered in the metaverse are evaluated. User profile creation, user privacy and precautions against privacy were evaluated, and research was conducted on identity management, protection of user information and community management in terms of security.

1. Giriş

Metaverse, "meta" (öte) ve "verse" (İngilizce "universe" kelimesinin kısaltması: evren) kelimelerinin birleşmesiyle oluşturulmuş, tutarlı bir değer sistemine ve fiziksel dünyayla bağlantılı bağımsız bir ekonomik sisteme sahip, bilgisayar tarafından oluşturulan bir dünyadır. İlk olarak Neil Stephenson'un 1992 tarihli Snow Crash ismiyle kaleme aldığı romanın 22. sayfasında karşımıza çıkmıştır (Stephenson, 2003). Bu romanda, insanlar sanal gerçeklik ekipmanları ve dijital avatarlar (dijital kopyalar) aracılığıyla fiziki dünyadan çıkıp metaverse ismi verilen dijital dünyada yaşıyorlar. Ortaya çıktığı ilk günden beri metaverse konsepti çeşitli tanımlamalarla gelişmektedir. Bunları şu şekilde örneklendirebiliriz; İkinci hayat (Second Life) (Sanchez, 2007), 3D dijital dünyalar (Dionisio, III, & Gilbert, 2013) veya yaşam günlüğü (life-logging) (Stentoft, 2019). Genel olarak, metaverse kendi kendini sürdürebilen, tamamen

*Sorumlu yazar.
E-mail adresi: tugaymandal@stu.aydin.edu.tr (Tugay Mandal)

sürükleyici ve hiper uzay-zamansal olarak dile getirilmesiyle birlikte fiziki ve dijital dünyaları bir araya getirir (Ning, ve diğerleri, 2021) (Lee, ve diğerleri, 2021), her on yılda bir bilgi ve iletişim teknolojilerinde bir paradigma değişimi yaşandığını; 1990'larda bilgisayar ile iletişim, 2000'lerde web, 2010'larda mobilin değişim geçirdiğini ve 2020'lerin paradigmasının anahtar kelimesinin Metaverse olduğunu dile getirmektedir (Kuş, 2021).

Konseptin nasıl çalıştığından bahsetmek gerekirse, sensörler ve diğer fiziki araçlar aracılığıyla toplanan bilgiler internet veya başka bir yöntem aracılığıyla sunuculara iletilmekte ve dijital dünyadaki avatara aktarılmaktadır. Sunucular bu bilgileri işleyerek dijital dünyadaki çok sayıda kullanıcıya aktarır. Avatarların metaversete kurduğu etkileşimler sunucuyu beslemeye devam eder. Örneğin; bir avatar tarafından yaratılan bir sanat eserinin veya bir manzaranın bilgileri ve içeriği sunucuya aktarılır. Sunucu bu içeriği saklar ve belirtilen içeriği bütün kullanıcılara yayınlar. İçerik sunucular aracılığıyla kullanıcıların sensörlerine aktarılır ve sensörlerin bu içeriğe nasıl tepki vermesi gerektiği programlanabilir. Bu sayede gerçek dünyadaki bazı bedensel, işitsel ve sözel faaliyetlerin, dijital dünyada da yerine getirilebileceği, yorumlanabileceği ve dönüt verilebileceği anlaşılır.

Gerçek dünyada, metaverse evreninden birçok alanda yararlanılabilmektedir. Örneğin binlerce kilometre uzaklıktaki insanlar birbirlerine yakın iletişim kurabilir. Bir anda iş yerinden çıkıp sinema salonuna gidilebilir. Yakın tarihlerde meydana gelen virüs salgını nedeniyle, eğitim ve öğretim hayatını önemli derecede etkilenmesi sebebinden ötürü, farklı alanlarda bu sorunun çözülmesi amaçlanmıştır. Bulunan çözüm yollarından bir tanesi de metaverse evrenidir. Hem sanal gerçeklik hem de arttırılmış gerçeklik; şu anda eğitimde kullanım alanı açısından geniş bir yelpazeye sahip olup eğitimin devamlılığını sağlayan bir etkileşim aracı olarak kullanılmaktadır (Alan, 2021). Dijital dünya üzerinde gerçekleştirilen faaliyetler ister okul alanında olsun ister iş alanında olsun isterse hobi alanında olsun faaliyete katılan bireylere bilgi birikimlerini aktarabilmek için oldukça kullanışlıdır.

Sanal evren deneyimini yaşamak isteyen insanlar, bu evrende elde edecekleri avatar adı verilen dijital kopyalarını, gerçek dünyada var olan kimliklerinden farklı bir şekilde düzenleyebilirler. İnsanlar, sanal alemde sahip oldukları avatarları aracılığı ile kendilerini gösterirler (Davis, Murpy, Owens, Khazanchi, & Zigurs, 2009). Buna örnek vermek gerekirse; fiziksel engelli insanlar metaverse içerisinde diledikleri gibi hareket edebilirler. Genç ve yaşlılar arasında hiçbir fiziksel güç farkı bulunmamakla birlikte, cinsiyet kavramı ortadan kalkmakta ve vücut ölçüleri, deri rengi, ırkı, gibi insana özgü özellikler anında değiştirilebilmektedir.

Metaverse, bu avantajlara karşı çeşitli dezavantajları da beraberinde getiriyor. Bunlardan bazıları veri güvenliği ve gizlilik endişesi olarak sıralanabilir. Örneğin; online oyunlarda avatarlar diğerleriyle daha yakın ilişkiler içerisinde olduğu için farkında olarak veya olmayarak gerçek dünyaya ait bilgilerini tüzel kişilerin eline geçirebilirler. İkinci bir örnek ise bazı insanların farklılıkları (kültürel, ırksal vb.) yüzünden kendilerini diğerlerine göre dışlanmış hissedebilmeleri ve daha kötüsü bazı davranışların kimileri tarafından normal karşılanırken diğerleri tarafından taciz olarak algılanması gibi dışlanma, aşağılanma ve travmatik olayların sebebiyet vereceği sorunların ortaya çıkması olasılığı vardır. Üçüncü olarak; kişisel malvarlığı, yasadışı kopyalama ve metaverse evreninde ticaret, karşımıza çıkan yeni sorunlar arasında gösterilebilir. Bu ve bunun gibi güvenlik ve gizlilik sorunlarını çözmenin en kolay yollarından ilki kullanıcıları metaverse dünyasına girmekten alıkoymak olacaktır (Falchuck, Loeb, & Neff, 2018); fakat bu sert metod, getirdiği avantajların yanında kendisine çok yer edinememektedir.

Güvenlik ve gizlilik konuları ile ilgili olarak diğer bir çözüm ise kullanıcıların yeni medya ve dijital okur yazarlıkları ve metaverse kullanımı konusunda eğitilmeleridir.

Bu makalede metaverse'te ortaya çıkabilecek potansiyel güvenlik ve gizlilik sorunlarını ele alıp Metaverse'in getirdiği avantajlara zarar vermeden alternatif çözümler bulmaya çalışılacaktır (Stephenson, 2003). Makalenin ana hatları şu şekilde özetlenebilir.

- Metaverse konseptinin analiz edilmesi
- Metaverse'te ortaya çıkabilecek ciddi veri güvenliği ve gizlilik sorunları bulunup özetlenecek
  - Kişisel Bilginin Gizliliği: Fiziksel, tıbbi, psikolojik, ekonomik, kültürel ya da sosyal durumun açığa çıkmasına neden olabilecek her türlü bilgi
  - Davranışların gizliliği: hobiler, aktiviteler, seçimler vb. hakkında her türlü bilgi
  - İletişimin gizliliği: kişisel iletişim ile bağlantılı her türlü veri ve meta veri (Falchuck, Loeb, & Neff, 2018)
- Bu güvenlik ve gizlilik sorunlarına potansiyel çözümler aranacaktır.

2. Altyapısı ile İlgili Çalışmalar

Metaverse'in yapısını oluşturan birçok teknoloji, ilerlemiş düzeydeki gelişmeler olarak varlıklarını sürdürmektedirler. Ancak, pratikte kullanılabilmeleri için uzun yıllar geçmesi gerekmektedir. Metaverse'te bulunan ana elementler, nitelikler ve fonksiyonlar ile birlikte alışılagelmiş teknolojinin üzerinde olmasıyla ilgili 2 farklı konu üzerinde durulmaktadır.

2.1. Ana Elementleri, Nitelikleri ve Fonksiyonları

Aktiviteler: Metaverse tarafından ortaya çıkarılmış eşi benzeri görülmemiş ağ kurma fırsatları, bilhassa sosyal aktivitelere katılmak için işe yarar. Başka kullanıcıları arkadaş olarak ekleme veya sesli/yazışmalı/görüntülü sohbetlere katılma gibi geleneksel aktiviteler, metaverse'te mevcuttur.
Kapsamsal: Cihazlardan, sadece ekrana bakarak erişebildiğimiz sanal alemlere metaversen'in eklenmesiyle birlikte sanal gerçeklik ve artırılmış gerçeklik teknolojileri sayesinde 2 boyutlu ekrana bağlı kalmayıp, fiziksel olarak sanal alemin içerisinde çevrimiçi olabilmek mümkündür. Hem fiziksel hem de sözel etkileşimde bulunabildiğimiz bir evren olmasından dolayı, kapsamsal olarak diğer teknolojilere göre ilerlemiştir.
Birlikte Çalışılabilirlik: Uygulama olarak, kullanılabilecek

programlar ve servisler metaverse evreni içerisine gömülüdür. Bilgisayarda veya telefonda yapılan işlemlere benzer olarak, bu işlemler aynı anda birden fazla metaverse'te gerçekleştirilebilir. Bunun sebebi metaverse evreni ve içerisinde gerçekleştirilen aktiviteler birbirine bağlıdır.

2.2 Teknolojinin Ötesinde

Alışılagelmiş teknoloji ile yapılabilen özelliklerin dışında, metaverse yeni imkanlar ve öncülük edecek fonksiyonlar ortaya koymuştur. Bu fonksiyonların ikinci aşaması, her teknolojide olduğu gibi bilimsel ve mühendislik işlemlerinden geçerek belirlenecektir ve beklenen teknolojik gelişmeler, gelecek yıllarda da metaverse'e işlenecektir.

3. Gizlilik

Günümüzde İnternet'te, bir ürün veya hizmet için ödeme yapılmıyorsa, o zaman ürün kullanıcının kedisidir (veya daha doğrusu kullanıcının verileridir). Sosyal medya ve sosyal ağ platformları bu türe en önemli örnektir. Bu platformlar, tercihleri platformlar tarafından çok iyi bilinen ve kullanıcılara son derece doğru, mikro hedefli reklamlar gösterebilecekleri milyonlarca hatta milyarlarca kullanıcıyı içeren ücretsiz hizmetler sunmaktadır (Kosinski, Stillwell, & Graepel, 2013). Bu başarılı iş modeli, platformun içeriği ve diğer kullanıcılarla eylemlerini ve etkileşimlerini çerezlerin gelişimi ve genel olarak parmak izi teknikleri sayesinde analiz ederek, yalnızca platformun kullanıcılarını doğru bir şekilde profilleme yeteneği sayesinde mümkündür (Laperdrix, Bielove, Baundry, & Avoine, 2020). Bugünün teknolojisiyle bile, arkamızda bıraktığımız dijital kırıntılar, kişiliğimiz, zevklerimiz ve yönelimlerimiz (örneğin politik ve cinsel) hakkında zaten çok şey anlatıyor. Bu, neredeyse on yıl önce gerçekleştirilen ilk çalışmalardan bu yana belirgindi ve (Kosinski, Stillwell, & Graepel, 2013) (Conover, Goncalves, Ratkiewicz, Flammini, & Menczer, 2011) bu günlerde bu tür tahmin yetenekleri katlanarak gelişti. Bu varsayımlar göz önüne alındığında, metaverse'te ne olabilir? Aşağıdaki alt bölümde, metaverse tarafından etkinleştirilen veri toplama yeteneklerini ve ilgili uygulamalar örneklendirilmiştir.

3.1 Metaverse'te Kullanıcı Profili Oluşturma

Sosyal ağ kullanıcıları günümüz internetinin ürünüyse, metaverse'te kelimenin tam anlamıyla her şey ve herkes ürün olacaktır. Sosyal ağ platformları şu anda Web kullanıcıları için güçlü mıknatıslar işlevini görmektedir. Benzer şekilde, metaverse kullanıcılar için olduğu kadar içerik oluşturucular, girişimciler ve işletmeler için de katlanarak daha güçlü bir mıknatıs olacaktır. Başka bir deyişle, tutkularından ve tercih ettikleri uygulamalardan (örneğin okuyucular, oyuncular, öğrenciler, vb.) bağımsız olarak kullanıcılar için ve ayrıca bu tür uygulamaların geliştiricileri ve bunları çalıştıran işletmeler için birleşik bir meta-platform olacaktır. Ortaya çıkan düşünce, böylesine büyük bir platformun toplayabileceği verilerin miktarı ve türü konusunda büyük endişeler doğuruyor. İnternet 2.0, pazarlamacıların, kullanıcıların farelerini nerede hareket ettirdiklerini, ekranda nereye baktıklarını, belirli bir resimdeki öğeye ne kadar zaman harcadıklarını ve hangi ürünleri veya kullanıcıları beğendiklerini incelemelerine olanak tanıdı. Zaman zaman özellikle teknoloji okuma yazma bilmeyen kullanıcılar, bu tür kayıtların ve analizlerin gerçekleştiğinin farkında bile değildir ve bu nedenle, gizlilikleri beklenmedik şekillerde tehlikeye girebilir (Falchuck, Loeb, & Neff, 2018). Metaverse'te, mevcut veri toplama teknikleri ve ilgili analizler en iyi ihtimalle amatörce kabul edilecektir. Gerçekten de platform, vücut hareketlerimizi, fizyolojik tepkilerimizi, hatta muhtemelen beyin dalgalarımızı ve çevreyle olan gerçek ve sanal etkileşimlerimizi takip edebilecektir. Ayrıca, bu yetenekler halihazırda toplanmakta olan tüm diğer verilere ek olacaktır. Bu tür verilerin nasıl kullanılacağı ve kullanıcı gizliliğine yönelik risklerin neler olduğu ile ilgili bilgiler aşağıda paylaşılmıştır.

3.2 Kullanıcı Gizliliği

Metaverse'teki kullanıcı gizliliği ile ilgili olarak, üç alan özellikle önemlidir (Falchuck, Loeb, & Neff, 2018): (i) kişisel bilgiler; (ii) davranış ve (iii) iletişim. Önceki değerlendirmelerin bir sonucu olarak, yeni ve artan risklerle birlikte bu alanların her biri platformlara şu anda sahip olduklarından çok daha fazla veri sağlayacaktır. Örnek olarak, sosyal ağ platformlarından toplanan kişisel bilgiler zaten doxing (yani, bir mağdurun özel bilgilerinin gasp veya çevrimiçi utandırma amacıyla ifşa edilmesi uygulaması veya tehdidi) için kullanılmaktadır (Snyder, Doerfler, Kanich, & McCoy, 2017). Metaverse kullanıcıları hakkında yalnızca platformlara değil, diğer kullanıcılara da çok daha fazla kişisel bilgi sağlayacağı düşünüldüğünde, doxing'ten nasıl kaçınılacaktır? Özellikle, metaverse veri tabanından sızacak kişisel ve hassas bilgiler, kullanıcı alışkanlıkları ve fizyolojik özellikleri hakkında çok sayıda gerçek dünya bilgisini içerecektir. Bunları mevcut İnternet'te elde etmek zor olsa da tamamen imkansız değildir, sanal ve fiziksel dünyalar arasındaki daha sıkı bağın bir sonucu olarak metaverse veri tabanında çok daha kolay elde edilebilecektir. Bu kullanıcı davranışının gizliliğiyle ilgili riskleri ortaya koyacaktır.

Bu bağlamda, metaverse, çevrimdışı zararları ve sahtekarlıkları işlemek için çevrimiçi sürükleyici deneyimlerden ve etkileşimlerden yararlanılabilen benzeri görülmemiş fırsatlar sunacaktır. Gerçekten de, sosyal mühendislik saldırıları, COVID-19 salgını sırasında da ölçüldüğü üzere (Salahdine & Kaabouch, 2019), çevrimiçi olarak uğranan siber saldırıların en büyük payını oluşturmaktadır. Metaverse ile birlikte, sosyal mühendislik saldırıları muhtemelen daha kullanışlı ve güçlü ve dolayısıyla daha sık hale gelecektir. Sosyal mühendisliğe ek olarak, metaverse, kullanıcı davranışlarının gizliliğiyle ilgili ek endişeler doğurmaktadır. Casusluk (spying) ve takip (stalking) bu türe basit örneklerdir. Gerçek dünyada, birini gözlemek, takip etmek veya taciz etmek, başka bir kişiye fiziksel olarak yakın olma ve belirli yerlere taşınma ihtiyacı gibi fiziksel kısıtlamalar tarafından kısmen engellenebilir ve bu da bazı maliyetler (örneğin zaman, para) içerebilir. Özellikle, belirtilen cezalar genellikle mükemmel bir caydırıcılık işlevi görür. Ancak, aynı düşünceler metaverse'te geçerli değildir, bu da bu tür saldırıları daha uygun hale getirir. Ne yazık ki, bu, halihazırda çevrimiçi olarak çoğalan, bazıları genellikle birden fazla koordineli kullanıcı tarafından gerçekleştirilen ve büyük olasılıkla metaverse'te hızla artacak olan geniş bir dizi saldırı için geçerlidir (Nizzoli, Tardelli, Avvenuti, Cresci, & Tesconi, 2021) (Weber & Neumann, 2021). Bunların arasında koordineli taciz ve baskın, utandırma, siber zorbalık, görüntülü arama tacizleri ve kargaşa çıkarma sayılabilir (Ling,

Balcı, Blackburn, & Stringhini, 2021) (Flores-Sviaga, Keegan, & Savage, 2018). Bu davranışlardan bazıları halihazırda "hizmet reddi" biçimleri olarak kullanılmaktadır. Örneğin, çevrimiçi oyunlarda -metaverse'in birincil kullanımlarından biri olacak- birkaç toksik oyuncu, diğer tüm katılımcılar için oyunu tekrar tekrar mahvetmeye yeterlidir (Bakioglu, 2009). Dahası, başlangıçta belirli bir platformda veya belirli bir konuyla (örneğin bir oyunla) ilgili olarak başlayan birçok siber saldırı daha sonra diğer platformlara veya konulara da yayılabilir, böylece #Gamergate kampanyasında (Chatzakou, ve diğerleri, 2017) veya Second Life'ta (Falchuck, Loeb, & Neff, 2018) olduğu gibi ek kullanıcılar ve topluluklar da dahil olabilir (Bakioglu, 2009). Topluluklar, alanlar ve uygulamalar arasında çok sayıda ara bağlantı ile karakterize edilen bir metaverse veri tabanında, bu riskler kaçınılmaz olarak artar.

Sonuçta, daha fazla bağlantı, daha fazla kişilerarası iletişim anlamına gelir; bu da bilgilerin toplanabileceği ve kötüye kullanılabileceği ve siber suçların işlenebileceği sayı ve şekillerde bir artışa yol açar. Metaverse iletişimleriyle ilgili gizlilik endişeleri, kurumsal veri ihlallerinin bariz riskleriyle sınırlı değildir, aynı zamanda kullanıcılar arasındaki diğer iletişim biçimlerini de içerir. Örneğin, şu anda cep telefonları aracılığıyla gerçekleştirilen cinsel içerikli mesaj alışverişi yapılmaktadır (Geeng, Hutson, & Roesner, 2020). Zengin ve çok duyusal 3D dünyası sayesinde cinsel yönelimli iletişim ve etkileşimlerin diğer biçimleri de metaverse'te yaygınlaşabilir (Bardzell & Bardzell, 2007). Peki ya bu tür kişisel iletişimlerin gizliliği tehlikeye girerse? İnternet 2.0'da intikam pornosu-yani bireylerin rızası olmadan cinsel içerikli metinlerinin, resimlerinin veya videolarının dağıtımı-büyük ölçüde iş için güvenli olmayan (NSFW) belirli platformlarla sınırlıdır. Benzer şekilde, toksik kullanıcılar, uçtaki Web platformlarında veya benzer düşüncelere sahip akranlardan oluşan büyük ölçüde yalıtılmış topluluklarda kümelenir (Zannettou, ve diğerleri, 2018). Hoşnutsuz çalışanların, şirketlerinin itibarını ölçeklenebilir bir şekilde kamuya zarar vermek için sınırlı yolları vardır. Bununla birlikte, bu çok önemli (ancak şimdiye kadar, uç noktalardaki) sorunların her biri, büyük ölçüde birbirine bağlı metaverse veri tabanında ana akım haline gelebilir. Yukarıda açıklanan tehditleri ele almak için ne yapılabilir? Aşağıdaki alt bölümde bir ön tartışma sunulmaktadır.

3.3 Karşı Önlemler

Metaverse kullanıcılarının maruz kaldığı çok sayıda gizlilik riski göz önüne alındığında, bazı bilim adamları zaten 3D sosyal metaverse ortamlarında kullanıcı gizliliğini zorlamanın yollarını tasarlamaya başladılar (Lee, ve diğerleri, 2021). Bunlar arasında, üç temel stratejinin birleşimine dayanan birkaç çözüm önerilmiştir (Falchuck, Loeb, & Neff, 2018): (i) kendi etkinliklerini gölgelemek için bir manken veya avatarının birden çok klonunu yaratmak; (ii) kullanıcının münhasır kullanımı için bir kamusal alanın özel bir kopyasını veya diğer kullanıcıları bir kamusal alanda geçici olarak engellemek ve (iii) kullanıcı ışınlanmasına, görünmezliğe veya diğer kılık değiştirme biçimlerine izin verilmesi. Yukarıdaki stratejilerin anlamlı kombinasyonları da kullanılabilir; örneğin, bir örnek alandan çıktıktan sonra tanınmaktan ve takip edilmekten kaçınmak için avatarına kılık değiştirmek gibi. Bir metaverse veri deposunun uyguladığı gizlilik çözümlerinden bağımsız olarak, bu çözümler kullanıcılara (ör., bir gizlilik menüsü aracılığıyla) sunulmalıdır; böylece, istedikleri gizlilik düzeyini, ayrıca faaliyetlerine ve bunları nasıl kullanacaklarına bağlı olarak seçebilsinler ve seçilen gizlilik özelliklerini uygulayabilsinler. Bununla birlikte, şu ana kadar öngörülen tüm (birkaç) çözüm, şimdiye kadar var olan basit metaverse veri kaynakları için tasarlanmıştır. Bu nedenle, Zuckerberg'in Meta'sının öngördüğü gibi karmaşık, sürükleyici ve büyük ölçüde birbirine bağlı çoklu evrenlerin risklerine ve saldırılarına dayanmak için yeterli değiller. Bu bağlamda, heyecan verici ve göz korkutucu bir araştırma görevi olan yeni ve daha iyi çözümler geliştirilmelidir.

4. Güvenlik

Dijital bir teknoloji geliştirilirken güvenlik ve gizlilik problemlerinin açığa çıkması Metaverse'te de kaçınılmazdır. Bunlardan bazıları şöyle özetlenebilir.

4.1 Kimlik Doğrulama

Günümüzde sosyal platformlarda etkileşimlerin birçoğu önceden oluşturulmuş içerikler üzerinden veya sahte kişiler, yazılımlar tarafından sağlanıyor. Bunlara örnek olarak botlar veya başka kişiler tarafından idame ettirilen sahte hesaplar örnek gösterilebilir. Yazılım tarafından idame ettirilen sahte hesaplar tüzel kişileri sosyal medyada dijital olarak yeniden oluşturmaktadır ve dijital parmak izini kısmi veya tamamen kopyalamaktadır. Bu hesaplar ne diğer tüzel kişiler tarafından ne de algoritmalar tarafından bulunabilmektedir (Cresci, 2020). Ayrıca yapay zekada kaydedilen gelişmeler gelecekte bu hesapların insanlardan hiçbir farkının kalmayacağını göstermiştir (Boneh, Grotto, McDaniel, & Papernot, 2019). Metaverse'te ise bu makine ve insan etkileşimi daha da artacaktır, kimi zaman ise zorunlu olacaktır. Bir MMORPG (Devasa çevrim içi çok oyunculu oyun) oyunu ele alındığında daha gerçekçi bir etkileşim yaratmak için kullanılan botlar veya kullanıcı dışı karakterler bu duruma örnek gösterilebilir. Bu ve benzeri örnekler güvenlik endişelerini güçlendirmektedir. Bir kişinin yaşını, cinsiyetini, konuşma tarzını taklit etmek ne kadar kolay olmalı, insan ile makine-yazılım ayrımı nasıl yapılmalı? Aşağıda bu sorunların çözümüne ilişkin bazı yöntemler açıklanmıştır.

4.1.1 Kimlik Yönetimi

Genel olarak metaverse'te kullanıcı etkileşimi ve hizmet sağlamanın verimli ve güvenli yollarından birisi kimlik yönetimidir. Bunlar şu şekilde sınıflandırılır.

Merkezi Kimlik: Bu tip kimlikler tek bir kurum, kuruluş veya taraf vasıtası ile doğrulanır. Buna örnek olarak günümüzde yoğun olarak kullanılan e-posta sağlayıcıları, sosyal medya sağlayıcıları gösterilir.

Birleşik Kimlik (Jaatun, Jensen, & G., 2013): Bu tip kimlikler birden fazla kurum, kuruluş vasıtası ile yönetilir. Bu kimlikler kullanıcılar için platformlar arası kullanımlarda kişisel bilgileri birden fazla kullanma sürecini ortadan kaldırır. Bu sebeple kimlik doğrulama maliyetlerini belirli bir ölçüde düşürür.

Kendi Kendine Egemen Kimlik (SSI) (Samir, We, Azab, Xin, & Zhang, 2021): Bu tip kimlikler herhangi bir kuruluşa

bağlı olmadan tamamen kullanıcının kendisi tarafından idame ettirilir. Bu sayede platformlar arası işlemlerde kullanıcı izni dışında herhangi bir işlem yapılamaz. Kişinin bilgilerini paylaşması tamamen kendi inisiyatifindedir.

Merkezi ve Birleşik kimlikler tek bir sunucuda saklandığı için herhangi bir saldırı durumunda bu bilgilerin saldırganların eline geçmesi muhtemeldir. Bu sebepten ötürü metaverse'in kimlik doğrulama sistemleri Kendi Kendine Egemen kimlikler üzerine yapılacaktır.

4.1.2 Giyilebilir Cihazlar Üzerinde Anahtar Yönetimi

Giyilebilir cihazların metaverse'e giriş için kullanılacak yöntemler arasında pastadaki büyük payı alacağı bir gerçektir. Bu cihazlara eklenecek eşsiz kimlikler ve kullanılacak güvenlik algoritmaları sayesinde kişinin metaverse'teki etkileşimleri bu anahtar ile güvence altına alınır. Örneğin tüzel kişi kendi avatarını bu cihazdaki anahtar ile eşleştirir ve yaptığı her etkileşimde bu anahtar ile kendi hareketlerini eşsiz bir şekilde tanıtır. Tabi mevcut güvenlik algoritmalarının metaverse evrenine uygulandığında ne kadar verimli olacağı tartışma konusudur. Günümüzde hash algoritmalarının çıktıları bulunabilen veri tabanları mevcuttur. 128bit hash değeri kullanan MD5 algoritmasındaki çıktı sayısı yüksek bit değerli algoritmalara göre daha düşük olduğu için günümüzdeki bilgisayarların bu çıktıları taklit etmesi kolaylaşmıştır. Bunun önüne geçmek amacıyla kripto zincirlerindeki eşsiz hash değerleri kullanılabilir veya yüksek bit değerine sahip yeni algoritmalar oluşturulabilir.

4.2 Kullanıcı Bilgileri

Metaverse'te kullanıcının bilgisi, kişinin kullandığı araç üzerinden sisteme iletimi yapıldığı andan itibaren kanun dışı 3. parti tarafından risk altındadır. Bunun önüne geçmek amacıyla bilgiye, kullanılan araçtan çıkmadan önce çeşitli güvenlik önlemleri uygulanmalıdır. Buna ek olarak gizlilik kişiden kişiye, kültürden kültüre ve tercihe göre değişeceği için burada uygulanacak güvenlik yöntemleri değişmelidir. Bu duruma göre alınacak önlem kullanıcının kendi tercihlerine göre yapılmalıdır. Burada yapılabilecek işlemler aşağıdaki gibidir.

4.2.1 Genelleştirilmiş Koruma

Buradaki amaç gizlilik içerebileceği için belirli görsel içeriği korumaktır. Görsel içerikte sadece belirli alanlara ihtiyaç duyulabilir, geri kalanı ise gerekmemektedir veya paylaşılmaması gereken bilgiler içeriyor olabilir. Buna örnek olarak metaverse'te yapılan bir video konferansı verilebilir. Bu konferansta sadece insanların görünmesi gerekmektedir ve arkadaki diğer bilgilere gerek yoktur. Bu sorun matlaştırmayöntemi ile çözülür. Burada içeriğin gerekli kısmı alınır, geri kalan kısmı ise seçilen belirli bir yöntem ile karartılır veya matlaştırılır. Günümüzde metaverse aracılığı ile olmasa da mevcutta video konferans sağlayıcıları bu yöntemi uygulamaktadır. Bunun yanı sıra avatar veya yüz değiştirme kullanılabilecek yöntemler arasındadır.

4.2.2 Beyaz Liste Koruması

Beyaz listeye benzer olarak ve kullanıcının seçtiği bilgiye ek olarak her şeyin işlenmesi ve korunmasıdır. Genelleştirilmiş korumayla karşılaştırıldığında biraz daha spesifik bir yöntemdir. Buna örnek vermek gerekirse, en güzel saç şeklinin bulunacağı bir yarışma örnek gösterilebilir. Bu yarışma için kullanıcının sadece saçlarının bilgisi gereklidir. Yüzündeki veya vücudundaki geri kalan bilgiler gereksizdir. Bu durumda kullanıcının içeriğinden sadece saçlar çıkarılmalıdır. Bu durum için sadece gerekli bilgilerin alındığı ve geri kalan bilginin silindiği algoritmalar geliştirme aşamasındadır.

4.2.3 Kara Liste Koruması

Kara listeye benzer olarak kullanıcının seçtiği bilgiler dışında herhangi bir bilginin işlenmemesidir. Bu tip koruma yöntemleri metaverse'te genellikle yüz bölgesi çevresinde uygulanmaktadır.

4.3 Toplum Yönetimi

Bu bölümde toplum yönetimi konusunda var olan bazı sorunlar metaverse penceresinden incelenmektedir. Bunlardan bazıları şöyle sıralanabilir.

4.3.1 Yanlış Bilgilerin Yayılmasını Azaltma

Hızlı şekilde yayılan gerçeklik payı olmayan bilgiler gerçek dünyada olduğu gibi metaverse'te de bir toplumsal huzur ve yönetim sorunudur. Bunun önüne geçmek amacıyla (Zhu, Ni, & Wang, 2020) sosyal platformlardaki etkiyi minimize etmek için bazı kısımları sosyal platformdan bloke etmeyi önermiştir. Fakat bu yöntem sadece sabit sosyal platformlar için geçerlidir. Dinamik ve interaktif sosyal platformlarda bunu yönetmesi çok daha zordur.

4.3.2 İnsan Güvenliği ve Siber Sendromlar

Günümüzde sanal gerçeklik sistemleri ile metaverse kullanımında saldırganlar kişiyi, bilinçaltı farkında olmadan farklı fiziki ortamlara taşıyabilir. Bu durumda kişinin siber sendromlar yaşamasına olanak tanır. Bunun önüne geçmek amacıyla çeşitli sosyal sanal gerçeklik senaryoları ve modelleri geliştirilmektedir.

5. Sonuç

Gizlilik ve güvenlik problemleri bütün geliştirme süreçlerinde yaşanan bir durumdur ve bu durumun çözülmesi gereklidir. Bu makalede öncelikle metaverse konseptinin ne olduğunun tanımı yapılmıştır ve bu konseptin içinde karşılaşılabilecek güvenlik ve gizlilik problemleri analiz edilmiştir. Analiz edilen bu sorunların çözümlerine ilişkin yapılan araştırmalar ve bu çözümlere dair bilgiler sunulmuştur. Bu bilgiler ışığında gizlilik için kendi klonunu yaratmak veya diğer kullanıcıları belli bir alanda engellemek ve kamusal alanın kopyası yaratılacağı gibi, kılık değiştirme gibi yöntemler kullanılabilir. Güvenlik konusu ele alındığında ise, kullanıcı kimliği bir veya birden fazla kaynak tarafından yönetildiğinde çeşitli faydalar sağlasa da herhangi bir kurumdan bağımsız olarak kullanıcının kendisi tarafından yönetilen bir kimlikte güvenlik ve gizliliğin daha yüksek olacağı kanısına varılmıştır. Bunlara ek olarak beyaz liste ve kara liste uygulamasının da faydalı olacağı sonucu çıkarılmıştır. Toplum yönetimiyle ilgili çeşitli öneriler ortaya atılsa da henüz geliştirilme aşamasında olduğu sonucuna varılmıştır.

Kaynaklar

Alan, T. (2021). "Eğitimde Dijitalleşme ve Yeni Yaklaşımlar". Efe Akademi Yayınevi vol. 1,, 1-30.

B. Falchuk, S. L. (2018). "The social metaverse: Battle for privacy,". IEEE Technol. Soc. Mag., vol. 37, no. 2, 52-61.

Bakioglu, B. S. (2009). Spectacular interventions of Second Life: Goon culture, griefing, and disruption in virtual spaces. Journal for Virtual Worlds Research, 1(3).

Bardzell, S., & Bardzell, J. (2007). Docile avatars: Aesthetics, experience, and sexual interaction in Second Life. The 21st British HCI Group Annual Conference on People and Computers (BCS-HCI'07), (s. 1-11).

Boneh, D., Grotto, A. J., McDaniel, P., & Papernot, N. (2019). "How relevant is the Turing tes in the age of sophisbots?". IEEE Security & Privacy, vol. 17 no.6, 64-71.

Chatzakou, D., Kourtellis, N., Blackburn, J., De Cristofaro, E., Stringhini, G., & Vakali, A. (2017). "Measuring #gamergate: A tale of hate, sexism, and bullying. The 26th International Conference on World Wide Web (WWW'17 Companion), (s. 1285-1920).

Conover, M. D., Goncalves, B., Ratkiewicz, J., Flammini, A., & Menczer, F. (2011). Predicting the political alignment of Twitter users. The 3rd IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT'11) and the 3rd IEEE International Conference on Social Computing (SocialCom'11), (s. 192-199).

Cresci, S. (2020). "A decade of social bot detection". . Communications of the ACM, vol. 63 no. 10, 72-83.

Çelik, R. (2022:08). "Metaverse Nedir? Kavramsal Değerlendirme ve Genel Bakış".

Davis, A., Murpy, J. D., Owens, D., Khazanchi, D., & Zigurs, I. (2009). "Avatars, People, and Virtual Worlds: Foundations for Research in Metaverses",. Department of Information Systems and Quantitative Analysis,, 1-30.

Dionisio, J., III, W., & Gilbert, R. (2013). "3D virtual worlds and the metaverse: Current status and future possibilities,". ACM Computing Surveys (CSUR) vol. 45, no. 3, 1-38.

Falchuck, B., Loeb, S., & Neff, R. (2018). The social metaverse: Battle for privacy. IEEE Technology and Society Magazine, 37(2), 52-62.

Flores-Sviaga, C., Keegan, B., & Savage, S. (2018). Mobilizing the Trump train: Understanding collective action in a political trolling community. The 12th International AAAI Conference on Web and Social Media (ICWSM'18).

Geeng, C., Hutson, J., & Roesner, F. (2020). Usable sexurity: Studying people's concerns and strategies when sexting. 16th USENIX Symposium on Usable Privacy and Security (SOUPS'20), (s. 127-144).

Jaatun, Jensen, J., & G., M. (2013). "Federated identity management - we built it; why won't they come?". IEEE Security & Privacy vol. 11 no.2, 34-41.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes. Proceedings, 110(15), 5802-5805.

Kuş, O. (2021). Metaverse: 'Dijital Büyük Patlamada' Fırsatlar ve Endişelere Yönelik Algılar. Intermedia International e-Journal, 8(15) doi: 10.21645/intermedia.2021.109, 245-266.

Laperdrix, P., Bielove, B., Baundry, B., & Avoine, G. (2020). Browser fingerprinting: A survey. ACM Transactions on the Web, 14(2).

Lee, L. H., Braud, T., Zhou, P., Wang, L., Xu, D., Lin, Z., . . . Hui, P. (2021, 11 3). All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda. https://arxiv.org/: https://arxiv.org/abs/2110.05352 adresinden alındı

Ling, C., Balcı, U., Blackburn, J., & Stringhini, G. (2021). A first look at zoombombing. The 43rd IEEE Symposium on Security and Privacy (s. 1452-1467). IEEE.

Ning, H., Wang, H., Lin, Y., Wang, W., Dhelim, S., Farha, F., . . . Daneshmand, M. (2021). "A survey on metaverse: the state-of-the-art, technologies, applications, and challenges,". arXiv preprint arXiv:2111.09673, 2021.

Nizzoli, L., Tardelli, S., Avvenuti, M., Cresci, S., & Tesconi, M. (2021). Coordinated behavior on social media in 2019 UK General Election. The 15th International AAAI Conference on Web and Social Media (ICWSM'21) (s. 443-454). AAAI.

Ruoyu Zhao, Y. Z. (2022, 3 8). Metaverse: Security and Privacy Concerns. https://arxiv.org/: https://arxiv.org/abs/2203.03854 adresinden alındı

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89.

Samir, E., We, H., Azab, M., Xin, C. S., & Zhang, Q. (2021). "DT-SSIM: A decentralized trustworthy self-sovereigh identity management framework". IEEE Internet of Things Journal, doi:10.1109/JIOT.2021.3112537.

Sanchez, J. (2007). "Second life: An interactive qualitative analysis,". Society for Information Technology & Teacher Education International Conference, , 1240-1243.

Snyder, P., Doerfler, P., Kanich, C., & McCoy, D. (2017). Fifteen minutes of unwanted fame: Detecting and characterizing doxing. Internet Measurement Conference (IMC'17), (s. 432-444).

Stentoft, A. B. (2019). "Lifelogging in the wild: Participant experiences of using lifelogging as a research tool,". IFIP Conference on Human-Computer Interaction, 431-451.

Stephenson, N. (2003). Snow crash: A novel. Spectra.

Türk, G. D. (2022). Metaverse ve Benlik Sunumu. The Turkish Online Journal of Design Art and Communication, 12 (2), 316-333.

Weber, D., & Neumann, F. (2021). Amplifying influence through coordinated behaviour in social networks. Social Network Analysis and Mining, 11(1), 1-42.

Yuntao Wang, Z. S. (2022, 3 5). A Survey on Metaverse: Fundamentals, Security, and Privacy. https://arxiv.org/abs/2203.02662: https://arxiv.org/abs/2203.02662 adresinden alındı

Zannettou, S., Caulfield, T., Blackburn, J., De Cristofaro, E., Sivivianos, M., Stringhini, G., & Suarez-Tangil, G. (2018). “On the origins of memes by means of fringe Web communities. The 2018 Internet Measurement Conference (IMC’18), (s. 188-202).

Zhu, J., Ni, P., & Wang, G. (2020). "Activity minimization of misinformation influance in online social networks". IEEE Transactions on Computational social Systems, vol. 7 no.4, 897-906.