METAVERSE VA IMMERSIV MUHITLARDA XAVFSIZLIK: RAQAMLI MAKONLARDA YANGI TAHDIDLAR ARXITEKTURASI

Muxtoraliyeva Nozima Shuxratovna

ISFT Samarqand

Annotatsiya.

Ushbu maqola metavers va immersiv muhitlarda xavfsizlik masalalarini ko'rib chiqadi, raqamli makonlarda yuzaga keladigan yangi tahdidlar arxitekturasini tahlil qiladi. Zamonaviy texnologiyalar, shu jumladan virtual haqiqat (VR) va kengaytirilgan haqiqat (AR) rivojlanishi bilan birga, insonlar uchun yangi tajribalar yaratish imkoniyatlari paydo bo'lmoqda. Biroq, bu yangi muhitlar kiberxavfsizlik va shaxsiy ma'lumotlarni himoya qilishda yangi tahdidlarga olib keladi. Maqolada metaversdagi potentsial xavf-xatarlar, foydalanuvchilarni himoya qilish uchun zarur bo'lgan strategiyalar va xavfsizlikni ta'minlashda innovatsion yondashuvlar muhokama qilinadi. Ushbu tadqiqot, raqamli makonlarda xavfsizlikni oshirishga qaratilgan tavsiyalar bilan yakunlanadi.

Kalit so‘zlar: Metavers, Immersiv muhitlar, Kiberxavfsizlik, Virtual haqiqat (VR), Kengaytirilgan haqiqat (AR), Tahdidlar arxitekturasi, Shaxsiy ma'lumotlarni himoya qilish

KIRISH.

Bugungi kunda texnologiyaning tezkor rivojlanishi bilan birga, metavers va immersiv muhitlar hayotimizning ajralmas qismiga aylanishmoqda. Ushbu yangi raqamli makonlar foydalanuvchilarga yanada boy tajribalar taqdim etadi, lekin ular bilan birga yangi xavf-xatarlar ham kelmoqda. Ushbu maqolada metavers va immersiv muhitlarda xavfsizlik masalalari, tahdidlar arxitekturasi va

foydalanuvchilarni himoya qilish strategiyalari ko'rib chiqiladi. Metavers — bu virtual haqiqat, kengaytirilgan haqiqat va boshqa raqamli texnologiyalar yordamida yaratilgan, foydalanuvchilarga interaktiv tajribalar taqdim etadigan keng qamrovli muhitdir. Ushbu muhitda foydalanuvchilar bir-biri bilan muloqot qilish, o'yin o'ynash, ish olib borish va hatto ijtimoiy hayot kechirish imkoniyatiga ega. Immersiv muhitlar esa foydalanuvchilarni real dunyodan ajratib, ularni virtual muhitga to'liq singdirishga qaratilgan. Metavers va immersiv muhitlar rivojlanishi bilan birga, kiberxavfsizlik sohasida yangi tahdidlar paydo bo'lmoqda. Ularning ba'zilari quyidagilar:

1. **Shaxsiy Ma'lumotlarni O'g'irlash**: Foydalanuvchilar o'z shaxsiy ma'lumotlarini (masalan, kredit karta raqamlari, parollar) kiritishlari kerak bo'lgan joylarda, bu ma'lumotlarning o'g'irlanishi xavfi mavjud. Virtual muhitda shaxsiy ma'lumotlarni himoya qilish juda muhimdir.

2. **Identifikatsiya va Avtorizatsiya Muammolari**: Foydalanuvchilar o'z hisoblarini boshqarishda qiyinchiliklarga duch kelishlari mumkin. Kiberhujumchilar foydalanuvchilarning hisoblariga kirish uchun ularning identifikatsiya ma'lumotlarini o'g'irlashi mumkin.

3. **Ijtimoiy Muammolar**: Metaversda ijtimoiy muammolar, masalan, bullying (kiberqilinichilik), zo'ravonlik va haqoratlar kabi xatti-harakatlar keng tarqalgan. Ushbu holatlar foydalanuvchilarni ruhiy jihatdan zarar etkazishi mumkin.

4. **Virtual Aktivlarni O'g'irlash**: Foydalanuvchilar virtual aktivlarga (masalan, raqamli san'at asarlari yoki o'yin ichidagi narsalar) ega bo'lishi mumkin. Bu aktivlar kiberhujumchilar tomonidan o'g'irlanishi yoki noqonuniy ravishda qo'lga kiritilishi mumkin.

5. **Texnik Muammolar**: Texnologik nosozliklar, dasturiy ta'minotdagi xatoliklar va serverlardagi nosozliklar foydalanuvchilarning tajribasini salbiy tomonga o'zgartirishi mumkin. Ushbu tahdidlardan himoya qilish uchun bir qator xavfsizlik strategiyalarini amalga oshirish zarur:

1. **Shaxsiy Ma'lumotlarni Himoya Qilish**: Foydalanuvchilarga o'z ma'lumotlarini himoya qilish uchun kuchli parollar yaratish va ikki faktorli autentifikatsiyani (2FA) qo'llash tavsiya etiladi. Shuningdek, shaxsiy ma'lumotlarni faqat ishonchli platformalarda taqdim etish kerak.

2. **Xavfsizlik Tizimlarini Takomillashtirish**: Metavers platformalarining xavfsizlik tizimlari doimiy ravishda yangilanib turishi kerak. Kiberhujumchilarga qarshi kurashish uchun ilg'or xavfsizlik protokollari va algoritmlardan foydalanish muhimdir.

3. **Foydalanuvchilarni O'qitish**: Foydalanuvchilarni kiberxavfsizlik asoslari haqida o'qitish, ularni potentsial tahdidlardan ogoh qilish va xavfsiz xatti-harakatlarni o'rgatish zarur.

4. **Ijtimoiy Xavfsizlik Mexanizmlari**: Metaversda ijtimoiy muammolarni hal qilish uchun foydalanuvchilarga hisobot berish mexanizmlarini taqdim etish kerak. Bu foydalanuvchilarga noqulay vaziyatlarga duch kelganda yordam berishi mumkin.

5. **Innovatsion Yondashuvlar**: Texnologiyalar rivojlanishi bilan birga, yangi xavfsizlik yechimlarini ishlab chiqish zarur. Masalan, sun'iy intellektdan foydalanib, anomal xatti-harakatlarni aniqlash va oldini olish mumkin. Metavers va immersiv muhitlar bizning hayotimizda yangi imkoniyatlar yaratishda davom etmoqda. Biroq, ushbu yangi raqamli makonlarda xavfsizlik masalalari ham jiddiy e'tibor talab qiladi. Foydalanuvchilarni himoya qilish uchun zamonaviy xavfsizlik strategiyalarini amalga oshirish va tahdidlar arxitekturasini tushunish juda muhimdir. Kelajakda

metaversda xavfsizlikni ta'minlash uchun innovatsion yondashuvlar va kuchli hamkorlik zarur bo'ladi. Bu nafaqat texnologik yechimlar, balki ijtimoiy mas'uliyatni ham talab qiladi. Raqamli makonlarda xavfsizlikni ta'minlash orqali biz yanada xavfsiz va qulay virtual muhitlarni yaratishimiz mumkin.

Insoniyat Internetning keyingi bosqichiga - **Metaverse** (Meta-olam) deb ataluvchi immersiv (sho‘ng‘ishli) raqamli olamga qadam qo‘ymoqda. Agar an’anaviy Internet bizga ma’lumotlarni "ko‘rish" imkonini bersa, Metaverse bizga ushbu ma’lumotlarning ichida "yashash" imkonini beradi. Virtual reallik (VR) va qo‘shimcha reallik (AR) texnologiyalari orqali yaratilgan bu muhitlar insonning kognitiv va sensor (sezgi) apparatiga bevosita ta’sir qiladi. Biroq, bu texnologik sakrash kiberxavfsizlik uchun mutlaqo yangi va murakkab xavf zonalari — **yangi tahdidlar arxitekturasini** yaratmoqda An’anaviy kiberxavfsizlik asosan ma’lumotlar (data), tarmoqlar va qurilmalarni himoya qilishga qaratilgan. Metaverse’da esa himoya obyekti o‘zgaradi. Endi himoya qilish kerak bo‘lgan narsa shunchaki "ma’lumot" emas, balki insonning **"raqamli mavjudligi" (digital presence)**, uning virtual tanasi, harakatlari va hatto hissiy holatidir. Metaverse’da xavf faqat kompyuter fayllariga emas, balki insonning virtual reallik ichidagi subyektiv tajribasiga yo‘naltirilgan bo‘lishi mumkin. Metaverse’da ijtimoiy muhandislik an’anaviy "fishing" (phishing) xabarlaridan ancha xavfli darajaga ko‘tariladi. Virtual muhitda inson o‘zini "haqiqiy" his qilgani sababli, uning himoya instinktlari pasayib ketadi.

- **Virtual qurbonlik:** Jinoyatchi virtual olamda sizning yaqin do‘stingiz yoki tanishingiz ko‘rinishida paydo bo‘lib, sizdan maxfiy ma’lumotlarni talab qilishi mumkin. Inson miyasi VR muhitida ko‘rib turgan narsani "haqiqat" deb qabul qilishga moyilligi (presence effect) tufayli, bunday manipulyatsiyadan omon qolish qiyinlashadi.

Xavfsizlikni ta’minlash strategiyalari

Metaverse’ning tahdidlar arxitekturasiga qarshi kurashish uchun yangi turdagi xavfsizlik protokollari zarur:

1. **Sensor ma’lumotlarni anonimlashtirish:** Biometrik ma’lumotlar to‘g‘ridan-to‘g‘ri serverga yuborilmasdan, foydalanuvchi qurilmasida (edge computing) qayta ishlanishi va faqat zaruriy qismlari shifrlangan holda uzatilishi shart.

2. **Avatar autentifikatsiyasi:** Avatarlar uchun ko‘p bosqichli va biometrik tasdiqlash tizimlari (masalan, real vaqt rejimidagi harakatlar algoritmi orqali) joriy etilishi lozim.

3. **Ekologik xavfsizlik (Environment Integrity):** Virtual muhitdagi ob'ektlar va qoidalar tizimi (physics engine) o‘zgartirib yuborilmasligini nazorat qiluvchi "virtual firewall"lar yaratish. Metaverse - bu cheksiz imkoniyatlar olami, ammo u bilan birga kiberxavfsizlikning mutlaqo yangi, ko‘rinmas va chuqur psixologik tahdidlari ham kelmoqda. Kelajakda kiberxavfsizlik mutaxassislari nafaqat kodlar va tarmoqlar, balki sensor signallari, inson kognitsiyasi va virtual reallikning fiziologik ta’sirlari bilan ham kurashishga majbur bo‘ladilar. Raqamli maḳonlarda xavfsizlikni ta’minlash — bu shunchaki texnik masala emas, balki insonning raqamli va biologik borlig‘ini himoya qilish masalasidir.

Metaverse va immersiv muhitlar zamonaviy texnologiyalar rivojlanishi bilan insonlarning kundalik hayoti, ish faoliyati va muloqoti uchun muhim platformalarga aylandi. Bu raqamli makonlar foydalanuvchilarga nafaqat keng va interaktiv tajriba taqdim etadi, balki xavfsizlikka oid yangi muammolarni ham yuzaga keltirmoqda. Bu maqolada metaverse va immersiv muhitlarning xavfsizlik muammolari, ularning arxitekturasi va kelajakdagi yangi tahdidlarni qanday oldini olish mumkinligi haqida

to'liq muhokama qilamiz. Metaverse - bu virtual, avatarning boshqaruvida bo'lgan va foydalanuvchilarga birgalikda ishlash, o'rganish, o'yin o'ynash va tijorat faoliyatlarini amalga oshirish imkonini beruvchi raqamli makon. Immersiv texnologiyalar esa VR (Virtual Reality), AR (Augmented Reality) va MR (Mixed Reality) yordamida foydalanuvchining muhit bilan to'liq integratsiyasini ta'minlaydi.

Ushbu texnologiyalar foydalanuvchilarga chinakamiga o‘zini virtual dunyoda his qilish imkoniyatini yaratadi. Shu bilan birga, ushbu platformalarning rivojlanishi bilan xavfsizlik va maxfiylik muammolari ham ortmoqda.

Xavfsizlik Muammolari va Tahdidlar

Metaverse va immersiv muhitlarda xavfsizlik muammolari keng ko'lamli bo‘lib, ularni quyidagicha guruhlash mumkin:

1. Maxfiylik va Ma'lumotlar Xavfsizligi:

Foydalanuvchilarning shaxsiy ma'lumotlari, joylashuvi, biometrik ma'lumotlari va faoliyatlari platformalarda saqlanadi. Bu ma'lumotlarning buzilishi yoki noto‘g‘ri qo‘llanilishi, shaxsiy hayotni buzishi mumkin.

2. Kiberjinoyatchilik va DDoS Hujumlar:

Metaverse platformalariga hujumlar, viruslar, DDoS (denial-of-service) hujumlari foydalanuvchi va platforma tizimlarini o‘tkazishga qodir.

3. Identifikatsiya va Avtorizatsiya Muammolari:

Foydalanuvchining haqiqiyligini tekshirish va uning hisobini himoyalash muhim ahamiyatga ega. Phishing, impersonation va hisoblarni olib qolish tahdidlariga duch kelishni taqiqlash muhim.

4. Psixologik Tahdidlar:

Metaverse ichida cyberbullying, haddan tashqari ta’sir qilish yoki manipulyatsiya kabi muammolar paydo bo‘lishi mumkin.

5. Hardware va Sensorlar Buzilishlari:

VR headsetlar va boshqa immersiv texnologiyalar bilan bog‘liq xavfsizlik

muammolari, jumladan, sensorlarning noto‘g‘ri ishlashi yoki zararli modifikatsiyalar xavfini keltirib chiqaradi.

Arxitektura Yechimlari va Yangi Tahdidlarning Oldini Olish

Xavfsiz metaverse muhitini yaratish uchun arxitektura yechimlari va xavfsizlik mexanizmlarini ishlab chiqish muhimdir. Quyidagi yondashuvlar muhim ahamiyatga ega:

1. Siyosat va Standartlarni Joriy Etish:

Xalqaro va mahalliy xavfsizlik standartlari (masalan, GDPR, ISO/IEC 27001) asosida platforma arxitekturasi ishlab chiqilishi kerak. Bu siyosatlarning muvofiqligi platformaning xavfsizligini ta'minlaydi.

2. Shifrlash va Ma'lumotlar Boshqaruvi:

Foydalanuvchi ma'lumotlari va muloqotlar shifrlanishi, xavfsizlik uchun keng qamrovli ma'lumotlar boshqaruvi va muhofaza qilish mexanizmlarini tatbiq etish lozim.

3. Foydalanuvchi Identifikatsiyasi va A'lo darajadagi Autentifikatsiya:

Biometrik autentifikatsiya, multifaktor autentifikatsiya va maxsus xavfsizlik protokollarini joriy qilish muhimdir.

4. Rivojlangan Monitoring va Hujumlarga Qarshi Qorovullik:

Sistemaning real vaqtda monitoringi va buzilishlarni erta aniqlash uchun avtomatlashtirilgan tizimlar va AI yordamida xavfsizlik tahlili qilish lozim.

5. Tavakkalchilikni Baholash va Vazifalar:

Sistemalar doimiy tarzda xavfsizlik tavakkulchiligi va tahdidlarga nisbatan baholanib turishi, yangi tahdidlar uchun yangi himoya mexanizmlari ishlab chiqilishi kerak

Raqamli dunyo rivojlanishi bilan metaverse va immersiv muhitlar uchun yangi tahdidlar paydo bo‘lishi kutilmoqda. Sun’iy intellekt, blockchain texnologiyalari va 5G kommunikatsiya infratuzilmasi ulkan imkoniyatlar bilan birga xavf-xatarlarni

ham orttiradi. Yangi tahdidlarning oldini olish uchun, arxitektura dizaynerlari va xavfsizlik mutaxassislari yangi texnologiyalar asosida yondashuvlar yaratadi. Misol uchun, blockchain texnologiyasini qo‘llash bilan identifikatsiya va ma'lumotlarni himoya qilish, smart kontraktlar yordamida siyosatlarni avtomatlashtirish mumkin. Shuningdek, immersiv muhitlar uchun ham AI yordamida tahdidlarni aniqlash va profilaktik chora-tadbirlar ko‘rish taklif etiladi. Bu esa xavfsizlikni ta'minlash uchun yangi arxitekturalarni va mexanizmlarni talab qiladi. Metaverse va immersiv muhitlar dastlabki imkoniyatlar bilan birga, yangi xavfsizlik muammolarini ham keltirmoqda. Ushbu raqamli makonlarning xavfsizligini ta’minlash uchun, arxitektura muhandisligi va xavfsizlik mexanizmlarining hamkorligi juda muhim. Siyosatlar, texnologiyalar va innovatsion yondashuvlar yordamida, foydalanuvchilar uchun xavfsiz va ishonchli muhit yaratish mumkin. Raqamli dunyo rivojlanishi davomida, xavfsizlikka bo‘lgan e’tibor ortib boraveradi va bu muhim bir ehtiyojga ayilmoqda. Yangi tahdidlar bilan kurashishda, doimiy innovatsiyalar va muvofiqlik strategiyalari asosiy omil bo‘lishi kerak. Metaverse va immersiv muhitlar uchun xavfsizlik arxitekturasi – bu faqat texnologik muammo emas, balki inson xavfsizligini ta’minlash va rivojlanishni davom ettirish uchun muhim jarayondir.

XULOSA.

Metaverse va immersiv muhitlar (VR/AR) o‘zining virtual arxitekturasi bilan an’anaviy kiberxavfsizlik chegaralarini kengaytirib, mutloq yangi tahdidlar tizimini yuzaga keltirmoqda. Biometrik ma’lumotlarning o‘g‘irlanishi, raqamli qiyofani soxtalashtirish (avatar hijacking) va 3D makondagi ijtimoiy muhandislik kabi xavflar foydalanuvchilar xavfsizligiga bevosita daxl qiladi. Immersiv muhitda xavfsizlikni ta’minlash nafaqat texnik himoya, balki kognitiv va huquqiy me’yorlarning uyg‘unligini talab etadi. Shuning uchun blokcheyn, sun’iy intellekt va Zero Trust (mutloq ishonchsizlik) tamoyillariga asoslangan xavfsizlik

arxitekturasini yaratish hamda immersiv olamda foydalanuvchilarning raqamli daxlsizligini huquqiy himoya qilish bugungi kunning eng dolzarb vazifasidir.

FOYDALANILGAN ADABIYOTLAR

1. Abdurahmonov, S. R. (2022). *Metaverse va immersiv texnologiyalarda kiberxavfsizlik asoslari*. Toshkent: Fan va Texnologiya. (b. 45–120).
2. Bekmurodov, R. N. (2023). *Raqamli makonlarda yangi avlod tahdidlari va ulardan himoyalanish strategiyalari*. Toshkent: O‘qituvchi. (b. 60–145).
3. Davronov, A. K. (2021). *Kengaytirilgan reallik (XR) va virtual muhitlarda shaxsiy ma’lumotlar daxlsizligi*. Samarqand: Ilmiy Nashr. (b. 88–160).
4. Gulyamov, S. S., & Shermuhamedov, A. T. (2022). *Raqamli iqtisodiyot va virtual dunyo: Metaverse platformalarining xavfsizlik muammolari*. Toshkent: Moliya. (b. 102–175).
5. Karimov, O. M. (2023). *Immersiv texnologiyalarda biometrik ma’lumotlar xavfsizligi va kiber-identifikatsiya tizimlari*. Toshkent: Yangi asr avlodi. (b. 75–138).
6. Rasulov, A. I. (2024). *Metaverse ekotizimida blokcheyn va aqlli shartnomalar xavfsizligi*. Toshkent: Innovatsiya. (b. 30–115).
7. Sodiqov, A. M. (2022). *Virtual va to‘ldirilgan borliqdagi kognitiv xavflar va ijtimoiy muhandislik tahdidlari*. Toshkent: Iqtisodiyot. (b. 50–122).
8. Xasanov, J. J. (2023). *Raqamli egzaklar (Digital Twins) va immersiv tizimlarda ma’lumotlar himoyasi*. Toshkent: Universitet. (b. 80–150).