SIMSIZ TARMOQLAR XAVFSIZLIGIGA TAHDIDLAR

Po’latov Doston Normurod o’g’li
Roziqov Abdug’ani Ilhomjon o’g’li
Jumaboyev Javlonbek Sherqul o’g’li
Ayupova Diana Anatolevna
Yoqubova Madinabonu Abdushukur qizi

Annotatsiya:*Biometrik identifikatsiya va autentifikatsiya tizimlari, foydalanuvchilar uchun ishonchli va yuqori darajada xavfsiz bir identifikatsiya usulini ta'minlayan tizimlardir. Ular foydalanuvchining unikal biometrik ma'lumotlarini, masalan, yuz, parmak izi, ovoz yoki retina skanerlari yordamida o'qish orqali identifikatsiya qilishga imkon beradi. Bu tizimlar foydalanuvchilar uchun qulaylik, tezlik va unikal identifikatsiya imkoniyatini beradi. Ularning kamchiliklari esa ma'lumotlarning xavfsizligi va xatoliklarni aniqlashda muammo yarata bilishi.*

Kalit so’zlar:*biometrik identifikatsiya, biometrik autentifikatsiya, yuz skaneri, parmak izi skaneri, ovoz skaneri, retina skaneri, unikal ma'lumotlar, xavfsizlik, identifikatsiya usuli, foydalanuvchi identifikatsiyasi, foydalanuvchi autentifikatsiyasi*.

Abstract:*Biometric identification and authentication systems are systems that provide a reliable and highly secure identification method for users. They allow identification by reading a user's unique biometric data, such as face, fingerprint, voice or retina scanners. These systems provide convenience, speed and unique identification for users. Their disadvantages are data security and error detection.*

Keywords:*biometric identification, biometric authentication, face scanner, fingerprint scanner, voice scanner, retina scanner, unique data, security, identification method, user identification, user authentication.*

KIRISH

Simsiz tarmoqlar xavfsizligiga muhim tahdidlar:

1. Hacking: Tarmoqda faollatilayotgan bir nechta cibernetik tajovuzlar, hakerlar yoki kiber-jinoyatchilar tarmoqqa kirish uchun ustunliklarni qo'ldan chiqarishga harakat qilishi mumkin. Ular tarmoqda ma'lumotlarni yo'qotish, o'zgartirish yoki yoqilg'isini o'zgartirishga harakat qilishi mumkin.

2. Malware va Viruslar: Simsim tarmoqlar viruslar, trojanlar, fidolar yoki boshqa zararli dasturlar orqali nufuz qilishi mumkin. Bu zararli dasturlar tarmoqdagi qurilmalarga yoki ularga bog'liq ma'lumotlarga zarar yetkazish, ma'lumotlar yo'qotish yoki so'nggi foydalanuvchilar tomonidan qo'llanilishi mumkin.

3. DoS (Distributed Denial of Service) hujum: Bu turiy hujum tarmoqdagi xizmatlarni ta'minlaydigan resurslarni sarf etish orqali tarmoqni qo'lda tutadi. Bu hujum sharoitda,

foydalanuvchilar tarmoqdagi xizmatlarga kirishni ta'minlayolmaydi va xizmatlar mavjud bo'lmaydi.

4. Phishing: Bu turdagi tajovuzlar kuzatuvchilarni kutilmagan shaxslar tomonidan yaratilgan yolg'on web-saytlarga, elektron pochta xabarlariga yoki boshqa aloqalar orqali e'lon qilinadigan ma'lumotlarni olish uchun yo'naltiriladi. Bu usul bilan foydalanuvchilarning shaxsiy ma'lumotlari, kirish kalitlari yoki to'lov karta ma'lumotlari bilan foydalanish haqida foydalanuvchilarni g'ururlovchi ma'lumotlar olish mumkin.

5. Man-in-the-Middle (MitM) hujum: Bu hujumda hujumchi orqali yo'l tutib, foydalanuvchi va tarmoqdagi server o'rtasida bo'g'lanishni to'liq ta'minlaydi. Ular foydalanuvchi bilan server o'rtasida jo'nli bog'lanishni o'rnatib, foydalanuvchining ma'lumotlarini o'zgartirishi yoki ulardan foydalanishi mumkin.

6. Ma'lumot so'qliqligi yo'qotish: Tarmoqdagi ma'lumotlar zaharlashgan yoki chori qilingan bo'lishi mumkin. Bu qo'llanish, xavfsizlik protokollari va kimyoviy algoritmlar yordamidagi ma'lumotlar.

Foydalanuvchilar uchun simsim tarmoqlarining xavfsizligini ta'minlash uchun quyidagi usullar tavsiya etiladi:

1. Parolni kuchaytirish: Foydalanuvchilar uchun qulay va xavfsiz parollar yaratishni ta'lim eting. Ular uchun unikal parollar, katta va kichik harflar, sonlar va belgilar kombinatsiyasidan iborat bo'lishi kerak.

2. Kirish autentifikatsiyasini mustahkamlash: Ikki bosqichli autentifikatsiya protsesslarini qo'llash, masalan, parol bilan birga telefon raqamini yoki foydalanuvchi nomini kiritish.

3. Sertifikatli autentifikatsiya: Foydalanuvchilar sertifikatlar orqali autentifikatsiyalashni amalga oshirishlari mumkin. Sertifikatlar ma'lumotlar to'plamini to'g'ri kasbiy shaxsga bog'lab turadi.

4. Biometrik autentifikatsiya: Foydalanuvchilarni biometrik ma'lumotlar bilan (qo'l izi, ko'z sifati, yuz kiritishi, ovoz kiritishi kabi) autentifikatsiyalash texnologiyalari ham mavjud.

5. Yordamchi uskunalar: Foydalanuvchilarga yordamchi uskunalar berish orqali katta xavfsizlik muammolaridan saqlash mumkin. Misol uchun, parol menedjerlari yoki yonaltirilgan autentifikatsiya uskunalaridan foydalanish.

6. Simsiz tarmoqlarini yangilash: Tarmoq operatorlari va xavfsizlik kasbiy shaxslari simsim tarmoqlarining xavfsizligini ta'minlash uchun yangiliklar va parolni yangilashni taklif etishadi.

7. Ma'lumotlarni shifrlash: Tarmoqda uzatilayotgan ma'lumotlarni yuqori darajada shifrlash yoki xavfsizlik protokollari yordamida himoya qilish tavsiya etiladi.

8. Xavfsizlik ta'limi: Foydalanuvchilarga xavfsizlik masalalari haqida ta'lim berish, phishingle va boshqa tajovuzlarga qarshi ehtiyojlar va doimiy xavfsizlik ta'limi olib borish tavsiya etiladi.

Bu usullar foydalanuvchilarni muhim ma'lumotlarni himoya qilishga yordam berishi va simsim tarmoqlarining xavfsizligini mustahkamlashga qaratilgan.

Simsiz tarmoqlar xavfsizligi, barcha sohalarda afzalliklarga ega bo'lishi bilan birga, bir nechta tahdidlarga ham uchraydi. Quyida simsiz tarmoqlar xavfsizligiga oid afzalliklar va kamchiliklarni ko'rib chiqamiz:

Afzalliklar:

1. Xavfsizlik: Simsiz tarmoqlar xavfsizlik sohasida muhim ustunliklarga ega bo'lishi bilan ajralib turadi. Bu, ma'lumotlar to'g'risida xavfsizlikni ta'minlash, moliyaviy operatsiyalarni muhofaza qilish, foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish va hokazo.

2. Foydalanish osonligi: Simsiz tarmoqlar foydalanishni osonlashtiradi, chunki ular foydalanuvchilarga xavfsiz va ishonchli autentifikatsiya imkonini beradi. Biometrik identifikatsiya (qo'l izi, yuz tanovlari, ovoz tanovlari) va asimmetrik shifrlash texnologiyalari foydalanishni yanada osonlashtiradi.

3. Eng yuqori darajada ishonchli autentifikatsiya: Biometrik identifikatsiya, parollar va boshqa identifikatsiya usullari bilan solishtirganda, biometrik identifikatsiya ishonch darajasida avvalo boradir. Foydalanuvchilar uchun autentifikatsiya jarayonini oson va ishonchli qilish uchun biometrik identifikatsiya tizimlaridan foydalanish afzalliklariga ega.

Kamchiliklar:

1. Maxfiylik: Foydalanuvchilarning biometrik ma'lumotlari maxfiylik muammo sifatida ko'rinishi mumkin. Bunday ma'lumotlarning yopishma va noyobligi shart bo'lgan holda, ulardan tashqari faqatgina kritik holatlar uchun foydalanish tavsiya etiladi.

2. Xatoliklarga xavf: Biometrik identifikatsiya sistemlari bazalarida o'zgarishliklar va xatoliklar bo'lishi mumkin. Bu xatoliklar natijasida yomon to'lov yoki ishonchsiz autentifikatsiya voqea yuzaga kelishi mumkin. Bu kamchilikni qo'llash uchun qattiq ishlab chiqish va monitorlash zarur bo'ladi.

3. So'rov va saqlashning katta miqdordagi ma'lumotlarni talab qilishi: Biometrik identifikatsiya tizimlari foydalanuvchilarning shaxsiy ma'lumotlarini, masalan, yuz, ovoz, qo'l izi kabi ma'lumotlarni talab qiladi.

Quyidagi misollar biometrik identifikatsiya va autentifikatsiya tizimlariga misollar bilan bog'liq:

1. Biometrik identifikatsiya: Foydalanuvchilarni yuz tanovlari yoki ovoz tanovlari asosida identifikatsiya qilish. Misol uchun, aklliy telefonlarda yuz tanovlari bilan ochish funktsiyasi yoki bankomatda qo'l izi skaneri.

2. Biometrik autentifikatsiya: Foydalanuvchilarning biometrik ma'lumotlarini ishlatib autentifikatsiya qilish. Misol uchun, aklliy telefonlarda parolni kiriting o'rniga yuz skaneri yoki ovoz tanovlari bilan autentifikatsiya.

3. Parmak izi skaneri: Parmak izi ma'lumotlarini o'qib olish uchun sensor yordamida foydalanish. Misol uchun, pasportlarda yoki aklliy telefonlarda parmak izi skaneri.

4. Retina skaneri: Retina qoplamasini skanlab uning unikal xususiyatlarini foydalanuvchini identifikatsiya qilish uchun ishlatish. Misol uchun, xususiy xavfsizlik sohasida, yashash maydonlarida yoki qulayliklar masofasida foydalanish.

5. Ovoz tanovlari: Foydalanuvchining ovozining unikal xususiyatlarini foydalanib identifikatsiya qilish. Misol uchun, telekomunikatsiya sohasida ovozli qo'llanmalar yoki aloqa markazlarida foydalanish.

6. Yuz tanovlari: Foydalanuvchining yuzining unikal xususiyatlarini aniqlab, identifikatsiya qilish. Misol uchun, hujjat berish markazlarida, nazorat kamerasi sistemlarida yoki mobil qurilmalarda foydalanish.

Bu misollar biometrik identifikatsiya va autentifikatsiya tizimlarining faollashtirilishi uchun bir nechta amaliyotlardan faqat bir qismini ta'minlayadi. Bunda, ma'lumotlar himoyasi, xususiy ma'lumotlarni to'plash va saqlashning tekshiruvi, ma'lumotlarga nusxa qo'yilmaganligi va boshqalar kabi muhim muammo va masalalar dikkatga olinishi kerak.

Simsiz qurilmalarni qo'llanish sohasi

Simsiz qurilmalar (IoT) bir qator sohalarda keng qo'llaniladi. Bu sohalardan ba'zilari quyidagilardir:

1. Uy va buyurtma tizimlari: Uy va buyurtma tizimlarida simsiz qurilmalar, uyotish mashinalari, termostatlar, amalga oshirish to'plamlari va boshqalar kabi vositalar orqali uy va ofis tizimlarini avtomatlashtirish uchun qo'llaniladi. Misol uchun, o'tkazma buyurtmalarni avtomatik ravishda qabul qilish, havoni tekshirish, yo'l-yo'riq ma'lumotlarini taqdim etish va boshqalar.

2. Transport va logistika: Transport va logistika sohasida IoT qurilmalari, transport vositalarini, konteynerlarini, transport xizmatlari monitoringini va boshqalarini birlashtirish uchun ishlatiladi. Bu qurilmalar orqali transport vositalarining joylashuvi va holati, yuklarning yurishini monitoring qilish, tezkor yo'l-yo'riq ma'lumotlari, xavfsizlikni nazorat qilish, oqimlarni optimallashtirish va boshqalar amalga oshiriladi.

3. Soha va bog'liqlik: Simsiqlik sohasida IoT qurilmalari, binolar, mahalliy tarmoqlar, havo muhitini boshqarish tizimlari va boshqalar kabi vositalar orqali ishlatiladi. Bu qurilmalar orqali binolardagi energiya iste'moli, uyg'unlik, xavfsizlik, tarmoqlardagi suv, energiya va gaz iste'moli, joriyati va qurilmalar monitoringini ta'minlash mumkin.

4. Sog'lomlik va kasb-hunar sohasi: Sog'lomlik va kasb-hunar sohasida IoT qurilmalari, shaxsiy qurilmalar, barqarorlik monitorlari, kasb-hunar ta'lim tizimlari, telemedicine vositalari va boshqalar kabi vositalar orqali foydalaniladi. Bu qurilmalar orqali shaxsiy sog'lomlik monitoringi, sport mashg'ulotlari monitoringi, kasb-hunar uskunalari bilan ishlash va boshqalar amalga oshiriladi.

5. Ishlab chiqarish sohasi: Ishlab chiqarish sohasida IoT qurilmalari, mahsulotni takomillashtirish, avtomatik ishlab chiqarish jarayonlarini monitoring qilish, iste'molchilar talablari va holatini nazorat qilish, eskiyuvchi va qurilmalarni texnik ta'minotini o'rganish uchun foydalaniladi. Bu qurilmalar orqali ishlab chiqarish.

6. Energia boshqaruv: Simsiz qurilmalar energiya boshqaruv sohasida ham keng qo'llaniladi. Bu sohada, energetika sohasidagi IoT qurilmalari, energiya iste'moli monitoringi, energiya samaradorligi, tarmoqning tarqatish va tarqatishini ta'minlash, energetika tizimlarini avtomatlashtirish va boshqalar kabi vazifalarda foydalaniladi.

7. Agro-sanoat sohasi: Agro-sanoat sohasida IoT qurilmalari, fermerlik, korxonalar, suv resurslari boshqarish tizimlari, avtomatik irrigatsiya tizimlari va boshqalar kabi vositalar orqali foydalaniladi. Bu qurilmalar orqali ekinlar va hosilalar monitoringi, suv resurslarini samarali ishlatish, to'liq uvuqqa ega xaridorlar uchun xizmat taqdim etish va boshqalar amalga oshiriladi.

8. Smart City: Simsiz qurilmalar smart city (axborot-kommunikatsiya texnologiyalari yordamida aqlli shahar) loyihalarida ham keng qo'llaniladi. Bu loyihalar shahar tarkibidagi muhim sohalar, masalan, transport, ayrim qurilmalarning ish vaqti, energetika, qurilish boshqarish, xavfsizlik va surveillance, suv resurslari boshqarish, yoritish tizimlari va boshqalar uchun simsiz qurilmalardan foydalanishni o'z ichiga oladi.

9. Smart Home: Smart home (axborot-kommunikatsiya texnologiyalari yordamida aqlli uy) tizimlari ham simsiz qurilmalar orqali ishlatiladi. Uy tarkibidagi mashinalar, elektronika, energiya boshqarish tizimlari, isharoatlar, ko'ra ko'p ishlatiladigan qurilmalar (smart TV, smart maishiy texnika, smart osimliklar va boshqalar) va boshqalar orqali uyotish jarayonini avtomatlashtirish, xavfsizlikni ta'minlash va iste'molchilarning mug'oya talablari va talablari bilan moslashish uchun foydalaniladi.

10. Kuzatuv va hujjat boshqarish: Kuzatuv va hujjat boshqarish sohasida ham simsiz qurilmalardan foydalaniladi. Bu qurilmalar, xaridorlar, logistik tizimlar, ma'lumotlarni kuzatuv va analitikasi, ma'lumotlar almashinuvini, xavfsizlik va hujjatlar boshqarishini avtomatlashtirish uchun ishlatiladi.

11. Xavfsizlik va himoya: Simsiz qurilmalar qo'llanish sohasida xavfsizlik va himoya muhim o'rin tutadi. Qurilmalar o'rtasidagi ma'lumot almashinuvining xavfsizligini ta'minlash, foydalanuvchilarning shaxsiy ma'lumotlarini himoya qilish, xavfsizlik ta'qiqlanishlarini aniqlash, kimni yo'qotishga urish jarayonlarini nazorat qilish va boshqalar kabi vazifalarda simsiz qurilmalardan foydalaniladi.

12. Ma'lumotlar analitikasi: Simsiz qurilmalar orqali to'plangan ma'lumotlar analitikasi va ma'lumotlar tahlili amaliyotlari olib boriladi. Qurilmalar ma'lumotlarini tahlil qilish, ma'lumotlardan ma'lumot olish, ma'lumotlarni birlashtirish, ma'lumotlarni vizualizatsiya qilish, ma'lumotlar ustida prognostika qilish va boshqalar kabi amaliyotlar maqsadida foydalaniladi.

13. Internetga ulanish va kommunikatsiya: Simsiz qurilmalar, internetga ulanish va kommunikatsiya sohasida ham o'rnatiladi. Bu qurilmalar orqali qurilmalar o'rtasidagi ma'lumot almashinuvi, boshqa tizimlar bilan o'zaro kommunikatsiya, internetga ulanish va boshqalar amalga oshiriladi.

14. Mashina o'qish va yoritish: Simsiz qurilmalar, mashina o'qish va yoritish sohasida ham keng qo'llaniladi. Bu qurilmalar avtomobillarda o'qish va yoritish tizimlarini avtomatlashtirish, mashinalar o'rtasidagi kommunikatsiyani ta'minlash, avtomobil davomida xavfsizlikni nazorat qilish va boshqalar uchun ishlatiladi.

15. Ijtimoiy sohalar: Simsiz qurilmalar ijtimoiy sohalar, masalan, festival va tadbirlarda, turizm sohasida, yashash qo'ng'iroqlarida, sport tadbirlarida va boshqalar kabi

tashqi tadbirlarda ham foydalaniladi. Bu qurilmalar orqali tadbirlarni avtomatlashtirish, yashash tajribasini yaxshilash, xaridorlarni yoqish va qiziqtirish, xavfsizlikni ta'minlash va boshqalar amalga oshiriladi.

Simsiz qurilmalar qo'llanish sohasi juda keng bo'lib, yuqorida keltirilganlar faqat ba'zi asosiy sohalardan iborat. Bu sohalar uchun simsiz qurilmalardan foydalanish sohasidagi yutuqlar yana ham rivojlantirilmoqda. Yangi innovatsiyalar va ilg'or texnologiyalar jamiyatning turli sohalarida yutuq berishga imkoniyat yaratayotgan bo'lsa-da, keyinroqda paydo bo'lgan yutuqlar quyidagilardan iborat bo'lishi mumkin:

16. Moliyaviy tizimlar: Simsiz qurilmalar, moliyaviy sohada ham qo'llaniladi. Moliyaviy institutlarda, banklarda, kassalarda, hisob-kitoblarda va boshqa moliyaviy tizimlarda tahlillash va boshqarish amalga oshirish uchun foydalaniladi. Bu qurilmalar orqali moliyaviy operatsiyalar, hisob-kitob va audit jarayonlari, to'lov va pul mablag'larini monitoring qilish, xavfsizlikni ta'minlash va boshqalar amalga oshiriladi.

17. Huquqiy soha: IoT, huquqiy sohada ham rivojlanmoqda. Avtomatlashtirilgan yuridik xizmatlar, elektronik imzolar, huquqiy asbob-uskunalar, sertifikatlash va autentifikatsiya tizimlari, ma'lumotlar yig'ilishi va arxivlashning xavfsizligi, huquqiy analitika va boshqalar kabi vositalar IoT asosida ishlab chiqariladi.

18. Ma'suliyat boshqarish: Simsiqlik va ma'lumotlar almashinuvi asosida qurilgan simsiz qurilmalar, ma'suliyat boshqarish sohasida ham qo'llaniladi. Bu qurilmalar, ma'suliyat boshqarish tizimlarini avtomatlashtirish, ma'suliyat hisobotlarini tayyorlash, ma'lumotlarni tahlil qilish, ma'suliyat bo'yicha risklarini nazorat qilish va boshqalar amalga oshirish uchun foydalaniladi.

19. O'zaro ma'lumot almashinuvi: IoT qurilmalari o'zaro ma'lumot almashinuvi sohasida ham yutuq beradi. O'zaro bog'liqlik tizimlari, ma'lumot almashinuvi tizimlari, tarmoq tizimlari va boshqalar orqali ma'lumot almashinuvi jarayonlari olib boriladi. Bu qurilmalar orqali ma'lumot almashinuvi protokollari, ma'lumot almashinuvi tahlillari, ma'lumot almashinuvi analitikasi va boshqalar kabi xizmatlar amalga oshiriladi.

20. O'z-o'zini boshqaruv: Simsiz qurilmalar, o'z-o'zini boshqarish sohasida ham yutuq beradi. Bu, avtomatlashtirilgan tizimlar va algoritmlar orqali qurilmalar o'z-o'zini boshqarishini ta'minlashga imkon beradi. Misol uchun, smart avtomobillar, o'z-o'zini boshqaruvli energetika tizimlari, o'z-o'zini boshqaruvli uyotish tizimlari kabi vositalar bu sohada ishlatiladi. Bu qurilmalar o'zaro ma'lumot almashinuvi, avtomatik ishga tushirish, o'z-o'zini tuzatish, o'z-o'zini o'rganish va o'z-o'zini optimallashtirish imkoniyatlarini ta'minlaydi.

21. Uzluksizlik: IoT qurilmalari, uzluksizlik sohasida ham yutuq beradi. Uzluksizlik tizimlari va qurilmalari orqali avtomatik xavfsizlik monitoringi, uzluksizlik nazorati, muvozanat va o'zaro ishonch tizimlari, muvozanatning avtomatik ravishda ta'minlanishi va boshqalar amalga oshiriladi. Bu qurilmalar masofaviy nazorat, muvozanat analitikasi, havfsizlik kameralari, uzluksizlik sensorlari va boshqalar kabi vositalar orqali uzluksizlikni ta'minlashga yordam beradi.

22. Markaziy boshqaruv: IoT qurilmalari markaziy boshqaruv sohasida ham yutuq beradi. Qurilmalar o'rtasidagi ma'lumot almashinuvi va kommunikatsiya, ma'lumotlar tahlili, ma'lumotlarni birlashtirish, ma'lumotlarni boshqarish va boshqalar amalga oshirish uchun markaziy boshqaruv vositalari va platformalardan foydalaniladi. Bu, avtomatlashtirilgan ma'lumot analitikasi, ma'lumot almashinuvi platformalari, boshqaruv paneli va boshqalar kabi vositalar orqali asosiy jarayonlarni boshqarish va birlashtirish imkoniyatlarini ta'minlaydi.

23. Kreativlik va innovatsiya: Simsiz qurilmalar kreativlik va innovatsiya sohasida ham yutuq beradi. Bu, innovatsiyalarni oshirish, yangiliklarni taklif qilish, yangi biznes modellari va mahsulotlar yaratish uchun avtomatlashtirilgan texnologiyalardan foydalanishni ta'minlaydi.

24. Saqlash va logistika: IoT qurilmalari saqlash va logistika sohasida ham yutuq beradi. Bu qurilmalar orqali omborlar, transport tizimlari, loyihalash va resurs boshqaruv tizimlari avtomatlashtiriladi. Bu imkoniyatlar orqali xaridorlarga to'g'ri vaqtda mahsulot taqdim etish, omborlar va logistika jarayonlarini nazorat qilish, ma'lumotlarni saqlash va boshqarish, ta'kidlash va boshqalar amalga oshirish uchun foydalaniladi.

25. Sog'liqni saqlash: IoT qurilmalari sog'liqni saqlash sohasida ham yutuq beradi. Bu qurilmalar tibbi uskunalar, shifoxonalar, klinikalar, shaxsiy sohalar va boshqa sohalarda foydalaniladi. Sog'liqni monitoring qilish, tibbi ma'lumotlar to'plamini o'rganish, shaxsiy tarbiyalash va takliflar berish, avtomatik kasalliklar diagnositi, narxlarni monitoring qilish va boshqalar kabi vazifalarda IoT qurilmalardan foydalaniladi.

26. O'qish va ta'lim: IoT qurilmalari o'qish va ta'lim sohasida ham yutuq beradi. Bu qurilmalar maktablar, oliy o'quv yurtlari, universitetlar, darsliklar, yangi ta'lim usullari va boshqalar orqali ta'lim jarayonlarini avtomatlashtirish, o'quv ma'lumotlarini birlashtirish, ta'limni monitoring qilish, o'quvchilarga ma'lumotlarni taqdim etish va boshqalar kabi vazifalarda foydalaniladi.

27. Akidalar va restoranlar: IoT qurilmalari akidalar va restoranlar sohasida ham yutuq beradi. Bu qurilmalar orqali restoranlar o'rtasidagi ma'lumot almashinuvi, xaridorlarga xizmat ko'rsatish, kuzatuv va nazorat, atrofdagi muhitning monitori va boshqalar amalga oshiriladi. Akidalar tarmoqlari, restoran tizimlari, buyurtma va yetkazib berish tizimlari va boshqalar kabi vositalar IoT asosida ishlab chiqariladi.

28. Transport va logistika: IoT qurilmalari transport va logistika sohasida ham keng qo'llaniladi. Bu qurilmalar orqali transport tizimlarini monitoring qilish, loyihalash, navigatsiya, transportning ish vaqtini va o'zaro aloqani ta'minlash, transportning xavfsizligini nazorat qilish

29. Energohavo sohasi: Simsiz qurilmalar energohavo sohasida ham yutuq beradi. Bu qurilmalar orqali energiya iste'moli, energiya tarmoqlari, boshqaruv tizimlari va havosozlikning avtomatlashtirilishi amalga oshiriladi. Energiya ta'minoti, energiya iste'molining monitoringi, qulaylik va energiya samaradorligini oshirish, energiya sarfiyatini kamaytirish va boshqalar uchun IoT qurilmalardan foydalaniladi.

30. Kishilarga xizmat ko'rsatish: Simsiz qurilmalar, kishilarga xizmat ko'rsatish sohasida ham rivojlanmoqda. Bu qurilmalar orqali xususiy xizmatlarni avtomatlashtirish, xaridorlarga shaxsiy xizmat ko'rsatish, shaxsiy ko'rsatkichlar va talablar to'g'risidagi ma'lumotlarni yig'ish, shaxsiy tahlillar va takliflar berish, shaxsiy tajriba va tanishlikni oshirish va boshqalar amalga oshiriladi.

Bu yutuqlar faqat bir necha sohalardan iborat bo'lib, simsiz qurilmalar asosan biznes, kommunikatsiya, xavfsizlik, o'zaro bog'liqlik, ma'lumotlar analitikasi, o'z-o'zini boshqaruv, uzluksizlik va boshqa sohalarda o'rnatiladi. Har bir sohada yutuqlar va imkoniyatlar kengayib borayotganidek, bu sohalardagi innovatsiyalar va yangiliklar jamiyatning turli sohalarida o'z o'rnatishini topmoqda.

Simsiz qurilmalar qo'llanish sohasidagi yutuqlar

Simsiz qurilmalar (IoT) qo'llanish sohasidagi yutuqlar quyidagilardir:

1. Barcha qurilmalarni birlashtirish: Simsiz qurilmalar qo'llanish sohasida, barcha qurilmalarni birlashtirish va ularga alohida to'plamlar yaratish muhimdir. Ushbu to'plamlar tarmoq asosida aks ettiriladi va ularga boshqarish tizimi orqali qo'llaniladi.

2. Ma'lumotlar to'plami tahlili: Simsiz qurilmalar ko'plab ma'lumotlarni to'playdi. Bu ma'lumotlar IoT tizimlarda tahlil qilinishi, ma'lumotlar analitikasi va tahlili jarayonlarida muhim rol o'ynayadi. Ma'lumotlar to'plami tahlili tizimga yaxshi tushuntirish, narx tahlili, foydalanuvchi odatlari va talablarini aniqlash va boshqalar kabi maqsadlarda foydalaniladi.

3. Xavfsizlik va farovonlik: Simsiz qurilmalar qo'llanish sohasida xavfsizlik va farovonlikning kuzatilishi muhim ahamiyatga ega. Tizimdagi qurilmalarning xavfsizlik protokollarini qo'llab-quvvatlash, ma'lumotlarni shifrlash, autentifikatsiya usullarini amalga oshirish, tizimdan tashqariga nusha saqlash va boshqalar kabi chora-tadbirlar xavfsizlik va farovonlikni ta'minlash uchun zarurdir.

4. Otomatlashtirish va oddiylik: IoT tizimlari oddiylikni oshirish, ish faolligini oshirish va yordam berishda muhim rol o'ynayadi. Tizimdagi qurilmalar avtomatik ravishda xodimlar bilan kommunikatsiya qilish, topshiriqlarni bajarish, holatlarni avtomatik nazorat qilish, oddiy hisob-kitobni bajarish va boshqalar kabi vazifalarni muximlashtirish uchun ishlatiladi.

5. Energia samaradorligi: IoT qurilmalari kuchli energiya iste'mol qiladi, shuning uchun energiya samaradorligini yuqori tutish muhimdir. Qurilmalar energiya samaradorligini yuqori tutish orqali batafsil hisobot berish, kuchli energetikalar bilan ishlash, energiya iste'moli monitoringini amalga oshirish va energiya sarflarini minimalizatsiya qilishga yordam beradi.

6. Protokollar va standardlar: IoT tizimlari uchun mavjud protokollar va standardlar orqali birlashtirish va interoperatsiya tarmoqlar.

7. Bulut xizmatlardan foydalanish: Simsiz qurilmalar qo'llanish sohasida bulut xizmatlardan foydalanish muhimdir. Bulut xizmatlar, ma'lumotlarni saqlash, ma'lumotlar analitikasi, ma'lumotlar o'zaro almashinuvini ta'minlash va boshqalar kabi amalga oshiriladigan funksiyalarni taqdim etishda foydalaniladi.

8. Ma'lumotlar tomoshabinligi va avtomatik analitika: Simsiz qurilmalar tomonidan to'plangan ma'lumotlar avtomatik ravishda tahlil qilinadi va bu ma'lumotlardan foydalanuvchilarga foydali ma'lumotlar olib chiqariladi. Ma'lumotlar tomoshabinligi va avtomatik analitika, yo'nalishlarni aniqlash, iste'molchilar odatlari va talablarini tahlil qilish, maslahatlar berish va boshqalar kabi vazifalarda foydalaniladi.

9. Kommunikatsiya va tarmoq protokollari: Simsiz qurilmalar bir-biriga va kengaytirilgan tarmoqlarga bog'liq bo'lishi uchun kommunikatsiya va tarmoq protokollari muhimdir. Bu protokollar, qurilmalar orasidagi ma'lumot almashishni, komanda berishni, ma'lumotlar almashinuvi va sinxronizatsiyani amalga oshirishda foydalaniladi.

10. Integatsiya va yo'qotish: Simsiz qurilmalar qo'llanish sohasida mavjud tizimlarga integratsiya qilish va ularga bog'liqlikni yo'qotish muhimdir. Bu yo'qotish jarayonida eskirgan, muzlatilgan yoki ishlamaydigan qurilmalar erkakini identifikatsiya qilish, qurilmalarning avtomatik ravishda to'plamlar bilan bog'lanishini yo'qotish va boshqalar kabi muammolarni hal qilish uchun foydalaniladi.

11. Xavf-xatarlarni tahlil qilish va xavf-xatarlarga qarshi tadbirlar: Simsiz qurilmalar qo'llanish sohasida xavf-xatarlarni tahlil qilish va ularga qarshi tadbirlarni amalga oshirish muhimdir. Xavf-xatarlarni tahlil qilish, qurilmalarning xavf-xatarlarga qarshi hisob-kitobini o'rnatish, ularga qarshi tadbirlarni amalga oshirish, yonishlar yoki yangilanishlar uchun ta'limlarni tuzish va boshqalar kabi vazifalarda foydalaniladi.

Ushbu yutuqlar:

12. Dasturiy ta'minot: Simsiz qurilmalar qo'llanish sohasidagi dasturiy ta'minot ham muhimdir. Qurilmalarga moslashuvchan dasturlar va to'plamlar yaratish, ularga yangilash va yangilanishlarga tez reagirov berish, dasturlar ustida to'plam, skriptlar yoki interfeyslar yaratish va boshqalar kabi muammolar yechish uchun foydalaniladi.

13. Boshqaruv va monitoring: Simsiz qurilmalar qo'llanish sohasida tizimni boshqarish va monitoring amaliyotlari muhimdir. Qurilmalar ustida monitoring qilish, holatlarni nazorat qilish, qurilmalar orqali ishga tushirish va boshqarishni avtomatlashtirish, xavf-xatarlarni aniqlash, alarm va bildirishnomalar tashlash va boshqalar kabi vazifalarda foydalaniladi.

14. Tashqi aloqalar va integratsiya: Simsiz qurilmalar qo'llanish sohasidagi tashqi aloqalar va integratsiya ham muhimdir. Qurilmalar tashqi tizimlarga integratsiya qilinishi, uchuvchi vositalar bilan aloqalar, API va protokollar orqali tizimlarga ulanish, tashqi ma'lumotlar bazalariga kirish va boshqalar kabi vazifalarda foydalaniladi.

15. Sifat va iste'molchilar odatlari: Simsiz qurilmalar qo'llanish sohasida sifat va iste'molchilar odatlari ham muhimdir. Qurilmalar sifatini ta'minlash, ishga tushirish, to'g'ridan-to'g'ri qo'llash, foydalanuvchi interfeysi va tajribasi, foydalanuvchilarning odatlari va talablari bilan moslashuvchan bo'lish va boshqalar kabi vazifalarda foydalaniladi.

Bu yutuqlar, simsiz qurilmalar qo'llanish sohasidagi asosiy muammolar va vazifalarga oiddir. Xususan, tizimning birlashtirilishi, ma'lumotlar to'plami tahlili, xavfsizlik va farovonlik, energiya samaradorligi, protokollar va standardlar, ma'lumotlar tomoshabinligi,

kommunikatsiya protokollari, integatsiya va yo'qotish, dasturiy ta'minot, boshqaruv va monitoring, tashqi aloqalar va integratsiya, sifat va iste'molchilar odatlari kabi muhim tushunchalar va amaliyotlar keng qo'llaniladi.

XULOSA

Biometrik identifikatsiya va autentifikatsiya tizimlari, foydalanuvchilar uchun yuqori darajada xavfsiz va ishonchli bir identifikatsiya va autentifikatsiya usuli ko'rsatishda katta potentsialga ega. Ular shaxsiy ma'lumotlarni himoya qilishda, parollar yoki kartalar kabi kimlik tekshiruv usullaridan farqli ravishda foydalanishlariga asoslangan. Bu usullar foydalanuvchining biometrik ma'lumotlarini, masalan, yuz, parmak izi, ovoz yoki retina skanerlari yordamida o'qishni va ulardan unikal identifikatorlar yaratishni o'z ichiga oladi.

FOYDALANILAGAN ADABIYOTLAR:

Axborot xavfsizligi tizimini qurish metodologiyasi va xavf-xatarlarni tahlil qilish va boshqarish sohasida foydalaniladigan bazilar adabiyotlar:

Rossouw, R., & von Solms, R. (2016). Information Security Governance: A Practical Development and Implementation Approach. Auerbach Publications.

Whitman, M. E., & Mattord, H. J. (2016). Principles of Information Security. Cengage Learning.

Pfleeger, C. P., & Pfleeger, S. L. (2018). Security in Computing. Pearson.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. National Institute of Standards and Technology (NIST) Special Publication.

ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27002:2013. Information technology — Security techniques — Code of practice for information security controls.

NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems and Organizations.

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons.

Anderson, R. (2008). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.

«Axborot texnologiyasi. Ma’lumotlami kriptografik muho- fazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» O‘zbekiston Davlat standard. 0‘z DSt 1092:2005.

«Axborot texnologiyasi. Axborotlami kriptografik muhofazasi. Ma’lumotlami shifrlash algoritmi» 0‘zbekiston Davlat standard. 0‘zDSt 1105:2006

«Axborot texnologiyasi. Ochiq tizimlar o‘zaro bogMiqligi. Elek tron raqamli imzo ochiq kaliti sertifikati va atribut sertifikatining tuzil- masi» 0‘zbekiston Davlat standarti. 0‘zDSt 1108:2006.

С.В. Симонов. Анализ рисков в информационнмх систе- мах. Практические советь! // Конфидент. -2001. -№2.

S.S.Qosimov. Axborottexnologiyalari. 0‘quvqoMlanma. - T.: «Aloqachi», 2006.

S.K.G‘aniyev, M.M. Karimov. Hisoblash sistemalari va tar- moqlarida informatsiya himoyasi. Oliy o‘quv yurt.talab. uchun o‘quv qoMlanma. —Toshkent Davlat texnika universiteti, 2003.

"Information Security Management Handbook" - Harold F. Tipton va Micki Krause tomonidan yozilgan bu kitob, umumiy xavfsizlik prinsiplarini va xavfsizlikni tahlil qilishning asosiy aspektlarini o'z ichiga oladi.

"Principles of Information Security" - Michael E. Whitman va Herbert J. Mattordning ushbu kitobi, xavfsizlikni qo'llab-quvvatlashning amaliyotga yo'naltirilgan prinsiplarini, tahlil qilish usullarini va xavf-xatarlarni boshqarishning muhim aspektlarini taqdim etadi.

"Security Engineering: A Guide to Building Dependable Distributed Systems" - Ross J. Andersonning bu kitobi, xavfsizlikni tizimni qurish va boshqarishning muhim xususiyatlari, tahlil qilish usullari, xavf-xatarlarni identifikatsiya qilish va ularga javob berishning yollari haqida tafsilotlar beradi.

"The Art of Computer Virus Research and Defense" - Peter Szorning ushbu kitobi, xavf-xatarlarni tahlil qilish va ularga qarshi ko'rsatkichlarni ishlab chiqishning yollari, viruslarni aniqlash va ularga qarshi muomala qilishning tajribali usullarini taqdim etadi.