INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 04 (2025)

IJTIMOIY TARMOQLARDAGI MAXFIYLIK VA XAVFSIZLIK ALGORITMLARI

Shaydullayev Jahongir Qudrat ugli

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti

Shaydullayevjahongir579@gmail.com

Annotatsiya: Ushbu maqolada ijtimoiy tarmoqlardagi maxfiylik va xavfsizlik algoritmlari. haqida fikr yuritilgan.

Kalit so‘zlar: Kontekstdan xabardor tizimlarda maxfiylikni saqlash, Ijtimoiy media uchun multimodal foydalanuvchi interfeysini modellashtirishda maxfiylik va xavfsizlik, Maxfiylikni saqlash, Insider tahdid, Havolalarni qayta qurish hujumi: Havola bashoratidan foydalanish Ijtimoiy tarmoqlarning maxfiyligini buzish algoritmlari, Klassik tahdidlar, Zamonaviy tahdidlar, Kombinatsiyalangan tahdidlar.

Аннотация: Аннотация: В данной статье рассматриваются алгоритмы конфиденциальности и безопасности в социальных сетях.

Ключевые слова: Конфиденциальность в контекстно-зависимых системах, Конфиденциальность и безопасность в моделировании мультимодального пользовательского интерфейса для социальных сетей, Конфиденциальность, Инсайдерская угроза, Атака восстановления ссылок: использование алгоритмов прогнозирования ссылок для нарушения конфиденциальности социальных сетей, Классические угрозы, Современные угрозы, Комбинированные угрозы.

Abstract: Abstract: This article discusses privacy and security algorithms in Social Networks.

Keywords: Privacy in Context-Aware Systems, Privacy and Security in Multimodal User Interface Modeling for Social Media, Privacy, Insider Threat, Link Reconstruction Attack: Using Link Prediction Algorithms to Break Social Media Privacy, Classic Threats, Modern Threats, Combined Threats .

Bugungi kunda Facebook, Twitter va LinkedIn kabi onlayn ijtimoiy veb-saytlar Internetda keng foydalaniladigan asosiy saytlardir. Maxfiylik va xavfsizlik dasturiy ta'minotni ishga tushirish yoki o‘rnatish kabi IT-ilovadagi asosiy muammolardir. Muhim vazifa - foydalanuvchining shaxsiy ma'lumotlarini yer qonuni va ma'lumotlar huquqlari bo‘yicha siyosatga muvofiq ruxsatsiz shaxslardan himoya qilishdir. Ijtimoiy tarmoq oxirgi foydalanuvchi profilining shaxsiy ma'lumotlarini oshkor qilmasligi kerak. Maxfiylik muammosi odatda faqat bitta yo‘nalishda ko‘rinadi, chunki insonning shaxsiy hayotiga nafaqat tashqaridan hujum qilinadi, balki aslida 80% hujum ehtimoli inson xatolari tufayli sodir bo‘ladi. Bu foydalanuvchilarning o‘zlari taqdim etgan shaxsiy ma'lumotlarning oqibatlarini tushunmasliklari sababli sodir bo‘ladi. Joylashuv, harakat, harorat va yaqin atrofdagi boshqa odamlar kabi atrof-muhitni suratga olish uchun foydalaniladigan GPS kabi foydalanuvchining shaxsiy ma'lumotlarini himoya qilish metodologiyasini ishlab chiqish zarur. Kameralar, giroskoplar, akselerometrlar, mikrofonlar va boshqalar kabi kontekstdan xabardor tizimda joylashuvni bilish muhim rol o‘ynaydi.

Resurs almashish ijtimoiy tarmoqlarda juda keng tarqalgan. Foydalanuvchilar kirish uchun barcha resurslarni ko‘rishlari mumkin, ammo ba'zilari shaxsiy yoki ommaviydir. Foydalanuvchi interfeysini tavsiflash tili (UIDL) dizaynerlarga ko‘p modali va ko‘p platformali foydalanuvchi

interfeyslarini ishlab chiqish imkonini beradi. Ijtimoiy tarmoqlarda mobil qurilmalarning ko‘payishi va imkoniyatlari maxfiylikka ta'sir qilishi mumkin.

Smartfon foydalanuvchilar sonining ko‘payishiga ijtimoiy tarmoq saytlariga kirish imkoniyatini beradi, ularda ular ma'lumotlarni saqlash, ijtimoiy tarmoq saytlariga ma'lumotlarni taqdim etish/qabul qilish uchun 4G ulanishlaridan foydalanadilar. Biznes jarayonlarini modellashtirishda insayder tahdidlar boshqariladigan jarayon orqali tashkilotga zarar etkazadi. Insayder tahdidni aniqlashning turli xil yondashuvlari mavjud, masalan, biznes jarayonlarini kuzatish va ular haqida ma'lumotni ro‘yxatga olish. Onlayn monitoring insayder tahdidini yumshatishga yordam beradi, chunki boshqa texnik yondashuvlardan farqli o‘laroq, u inson omilini ham hisobga oladi. Onlayn ijtimoiy tarmoqlarda o‘zaro changlanish degan atama mavjud bo‘lib, bu jarayonda gulchanglar turli o‘simliklardan, genezisi turlicha bo‘lgan o‘simliklar bilan birga bir gulga yetkaziladi, xuddi shu tarzda ijtimoiy media provayderlariga yordam beradi. tizimlarini takomillashtirish va tarmoqlar bo‘ylab axborot almashish uchun yangilangan vositalarni ishlab chiqish. O‘zaro changlanadigan tarmoqlar onlayn ijtimoiy tarmoqlarda tarqalishning vaqtinchalik va topologik xususiyatlarini kuzatib boradi. Internet orqali ma'lumotlarni himoya qilish uchun tarmoq virtualizatsiyasi va media mustaqilligi texnologiyasi qo‘llaniladi. Ommaviy axborot vositalarining mustaqilligi tufayli mobillikdan xabardor ilovalarni taqdim etish uchun tarmoq operatsiyalarini soddalashtirish uchun belgilangan mavhum xizmatlar to‘plami mavjud.

Mobil qurilma uchun FAME (Mobil uchrashuvlar uchun yuz autentifikatsiyasi) – bu tekshirish va identifikatsiyani, jumladan, ijtimoiy faoliyatni qo‘llab-quvvatlash uchun identifikatsiyani boshqarishni ta’minlovchi o‘rnatilgan ilovadir.

Kontekstdan xabardor tizimlarda maxfiylikni saqlash

Ilgari tizim asosan joylashuvga e'tibor qaratgan, ammo keyingi yangi model foydalanuvchilarning joylashuvi, qurilmalari va foydalanuvchi ishtirok etadigan boshqa taxminiy faoliyatni hisobga oladigan yanada kengroq va yuqori darajadagi kontekst tushunchasi bilan foydalanilgan. Maxfiylik va xavfsizlikni ta’minlash uchun qurilma o‘z konteksti haqidagi bilimlarni baham ko‘radigan va birlashtiradigan hamkorlikda ma’lumot almashishdan foydalanish asosiy element hisoblanadi. Buning uchun Semantic Web Technologies-dan foydalanish va turli xil sensorlar-telefon, onlayn manbalardan ma'lumotlarni jamlaydigan va dinamik foydalanuvchi kontekstidan xulosa chiqaradigan prototip tizimini yaratish. Ma'lumotlarga imtiyozli foydalanuvchilar kirishadi va noqonuniy foydalanuvchiga kirishni rad etadi. Guruh ro‘yxatidagi foydalanuvchilar sonini o‘zgartirdi va so‘rovchiga kirish darajasini ta'minlash uchun tizim tomonidan kirish vaqtini qayd etdi.

Quyida biz faqat vakolatli foydalanuvchilar tomonidan sezilgan ma'lumotlarni himoya qilish va kirish uchun ba'zi fikrlarni ko‘rib chiqamiz:

- Imtiyozli foydalanuvchining kirishiga ruxsat berish va noqonuniy foydalanuvchini cheklash orqali tizim asosiy mezonlarga javob beradimi yoki yo‘qligini ko‘rish uchun,
- Mobil qurilmalarda mulohaza yuritishning haqiqiy hisoblash vaqti maqbulligini tekshirish uchun.
- Foydalanuvchi ma'lumotlarining turli o‘lchamiga ega o‘lchovlarni topish uchun.

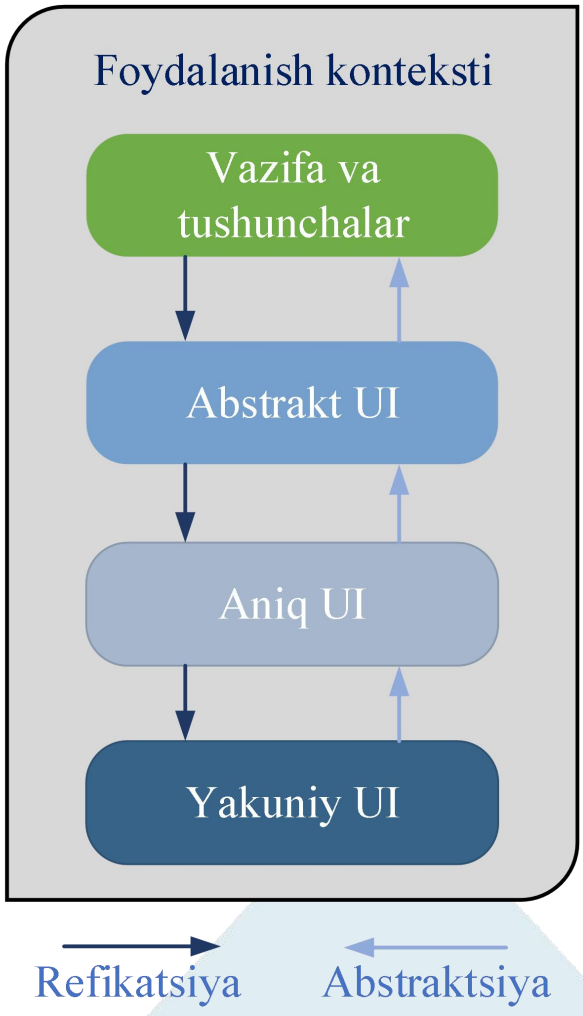
Ijtimoiy media uchun multimodal foydalanuvchi interfeysini modellashtirishda maxfiylik va xavfsizlik

INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 04 (2025)

Ushbu qismda ular foydalanuvchi interfeysini modellashtirishda xavfsizlik va maxfiylik masalalariga e'tibor qaratishadi, buning uchun ular Ui-ni ishlab chiqish uchun Cameleon Reference Framework (CRF) dan foydalanadilar. UsiXML foydalanuvchi interfeysini kontseptual modellashtirishni qo‘llab- quvvatlash uchun quyidagi modellar to‘plamiga ega.

- TaskModel vazifalar o‘rtasidagi pastki vazifalarga bo‘linishni, shuningdek, vazifalar o‘rtasidagi vaqtinchalik munosabatlarni ifodalaydi .
- DomainModel tizim bilan o‘zaro aloqada bo‘lgan foydalanuvchi tomonidan boshqariladigan ob'ektlar sinflarini tavsiflaydi.
- MappingModel semantik jihatdan bog'liq bo‘lgan modellararo munosabatlarni to‘playdi.
- contextModel foydalanuvchini, muhitni va ilova platformasini tavsiflaydi.

Ushbu modellarning aksariyati bir vaqtning o‘zida turli xil abstraktsiya darajalarida UIda xavfsizlik va maxfiylikni qo‘llab-quvvatlash uchun kontekstda qo‘llanilmasligidan aziyat chekmoqda. Shu sababli ular PriS kontseptual modelini ham xavfsizlik, ham maxfiylikka yo‘naltirilgan texnologiyalar uchun moslashtiradilar.



1-rasm. **To‘rt qavatli konseptual ramkalar**

Yuqoridagi 2.7-rasmda UI ning mavhumlik darajasi tasvirlangan:

a) Vazifalar va tushunchalar: Ushbu qatlam foydalanuvchining vazifalari va ushbu vazifalarni bajarish uchun domenga yo‘naltirilgan tushunchalarini tavsiflaydi.

b) Abstrakt UI: Bu qatlam mavhum konteynerlarni va UI ning alohida komponentlarini va konteyner guruhini vazifa modelining strukturaviy naqshlari, semantik munosabatlarni aniqlash va kognitiv yuk tahlili bo‘yicha quyi vazifalarni tavsiflaydi.

c) Aniq UI: U vidjet maketlarini va interfeys navigatsiyasini belgilaydi. U Yakuniy UI ni UI ta'rifiga aylantiradi va shuningdek, platformaga nisbatan Abstrakt UI ni tuzatish sifatida ko‘rib chiqiladi.

d) Yakuniy UI: U ma'lum bir hisoblash platformasida bajarilishi bo‘yicha ishlaydigan operatsion interfeysni ifodalaydi.

Ommaviy ijtimoiy mediada katta ma'lumotlarning maxfiyligi muammolari

Ushbu bo‘limda ular GPS-ni qo‘llab-quvvatlaydigan mobil qurilmadan foydalanmoqda, foydalanuvchi o‘zining shaxsiy hayotiga tegishli deb hisoblagan paytlarda uning o‘rnini mahalliy kuzatish uchun qo‘riqchi mijozni faollashtirishi mumkin, so‘ngra qurilma foydalanuvchi manfaatdor bo‘lgan vaqtda unga ommaviy axborot vositalarini ko‘rsatishni so‘rashi mumkin. uning onlayn maxfiyligi holatiga ko‘ra, kuzatuv xizmati uch xil usulda ishlashi mumkin:

- Birinchi turdagi oddiy foydalanuvchi hisobi bo‘lishi mumkin, u barcha ochiq rasmlarni, shuningdek, cheklangan, ammo foydalanuvchiga ko‘rinadigan barcha rasmlarni ko‘rishi mumkin. Ijtimoiy tarmoq ularning qachon va qayerdaligini va onlayn maxfiyligini himoya qilishni istagan mijozlarni biladi.

- Ikkinchi turdagi qo‘riqchi qidiruvni amalga oshirish uchun foydalanuvchi hisobini talab qilmaydi va uni anonim tarzda so‘rash mumkin. U kichikroq hajmga ega bo‘ladi va faqat ommaviy axborot vositalariga kirishi mumkin.

- Uchinchi tur, uchinchi tomon tomonidan boshqarilishi mumkin bo‘lgan mustaqil xizmat bo‘lishi mumkin, masalan, indekslash, qidiruv mashinasi, ommaviy axborot vositalarini skanerlash va metadata bo‘lib, ushbu ma'lumotlar bazasini so‘rashga imkon beradi.

Ushbu har xil turdagi kuzatuv xizmati foydalanuvchi nazoratsiz ommaviy axborot vositalarining onlayn bo‘lishini istamasa, kuzatib borishi kerak bo‘lgan tegishli media qismlari sonini kamaytirish uchun ishlatiladi.

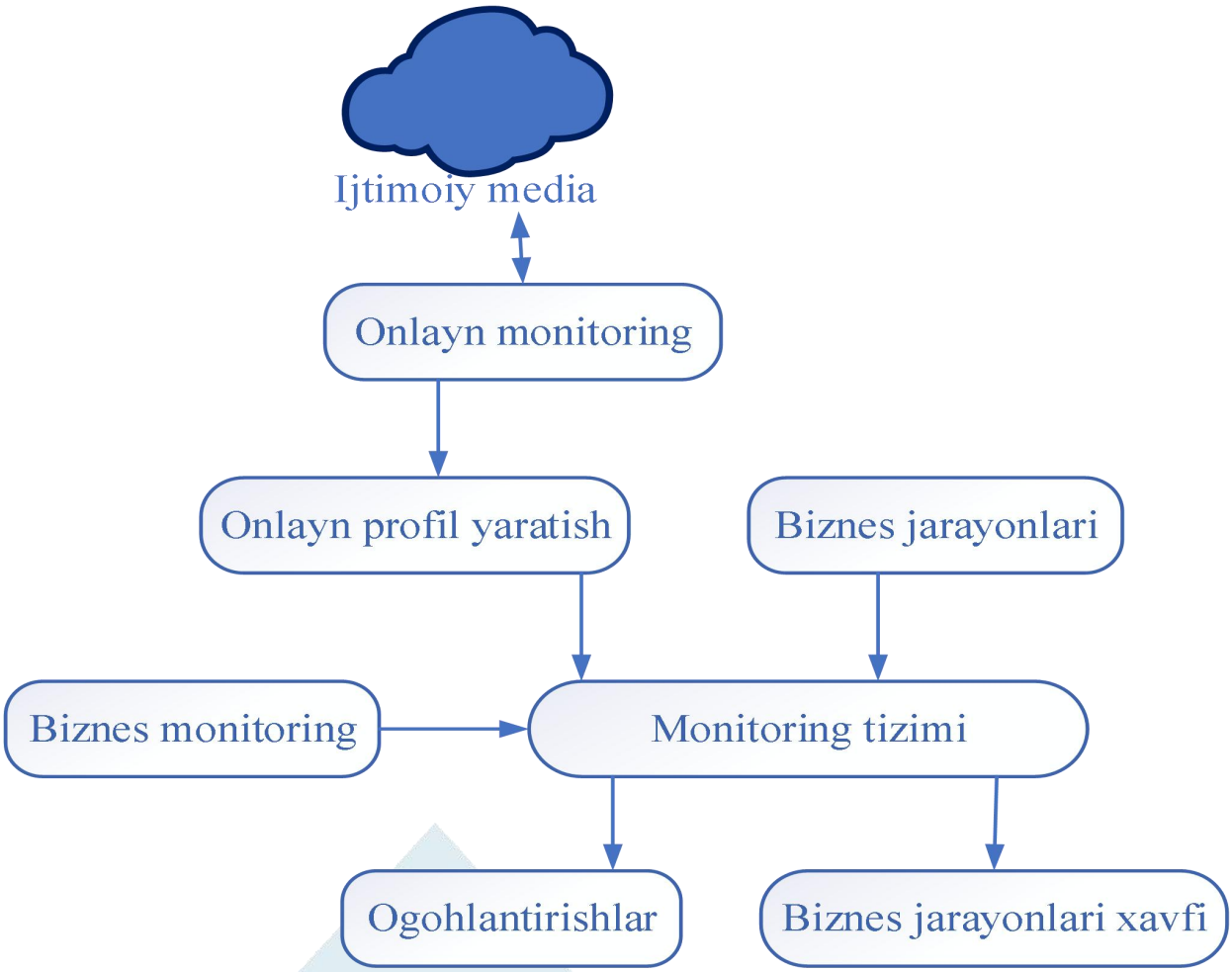
Maxfiylikni saqlash - virtual xususiy ijtimoiy media uchun mobil kirishlar. Izdoshlar munosabatlarini himoya qilish uchun joy va vaqtga bog'liq bo‘lgan virtual xususiy ijtimoiy media (VPSM) texnikasini taklif qildi. Avtorizatsiya siyosati ommaviy axborot vositalari xizmatlariga kirish va tarqatish qobiliyati, joylashuv va vaqt oralig'i tushunchasi bilan birgalikda harakat qilish uchun belgilanadi. Ushbu maqolaning asosiy maqsadi foydalanuvchilarning ijtimoiy media resursining kichik guruhlariga joy va vaqtga dinamik kirishini nazorat qilish, shuningdek, kuzatishga ruxsat berish yoki bermaslikni aniqlashdir.

Insider tahdid: Ijtimoiy tarmoqlar orqali BPMni yaxshilash

Maqsadiga qarab tashkilotga zarar etkazishi mumkin bo‘lgan insayder tashkilotning biznes jarayoniga qaratilgan. Ular jarayon darajasida monitoringni ijtimoiy media orqali psixososyal monitoring bilan birlashtirgan tizimli usulni taklif qildilar. CERT tadqiqoti diagramma bilan quyida tavsiflangan ko‘p sonli insayder tahdidlarni tahlil qilishga qaratilgan:

- Tashkilot monitoringi: Insayder tahdidlar holati va tashkilot bilan sodir bo‘lgan voqea haqida ma'lumot to‘playdi.
- Xodimlarni monitoring qilish: Ushbu natijalar himoyalangan bo‘lishi va kamsitish maqsadlarida emas, balki resurslarni optimallashtirish maqsadida ishlatilishi kerak.
- Optimallashtirilgan monitoringdan foydalaning: Tashkilot o‘z infratuzilmasini qisqa vaqt ichida ichki hujumlar aniqlanishi uchun sozlashi kerak.
- Texnik va xulq-atvor monitoringini birlashtirish: Insayder tahdidlarni aniqlash samaradorligini oshiradi. Ogohlantirish almashish va tashkilot ichidagi barcha ma'lumotlarga kirish huquqiga ega ishonchli jamoalar.
- Tashqi ma'lumot manbasidan foydalaning: Bu tashqi ma'lumot manbalaridan foydalanishni taklif qiladi.

Ular tashqi axborot manbalarini (masalan, ijtimoiy media) texnik va xulq-atvor namunalari bilan birlashtirish orqali mavjud monitoring vositalarini yanada takomillashtirishga qaratilgan.

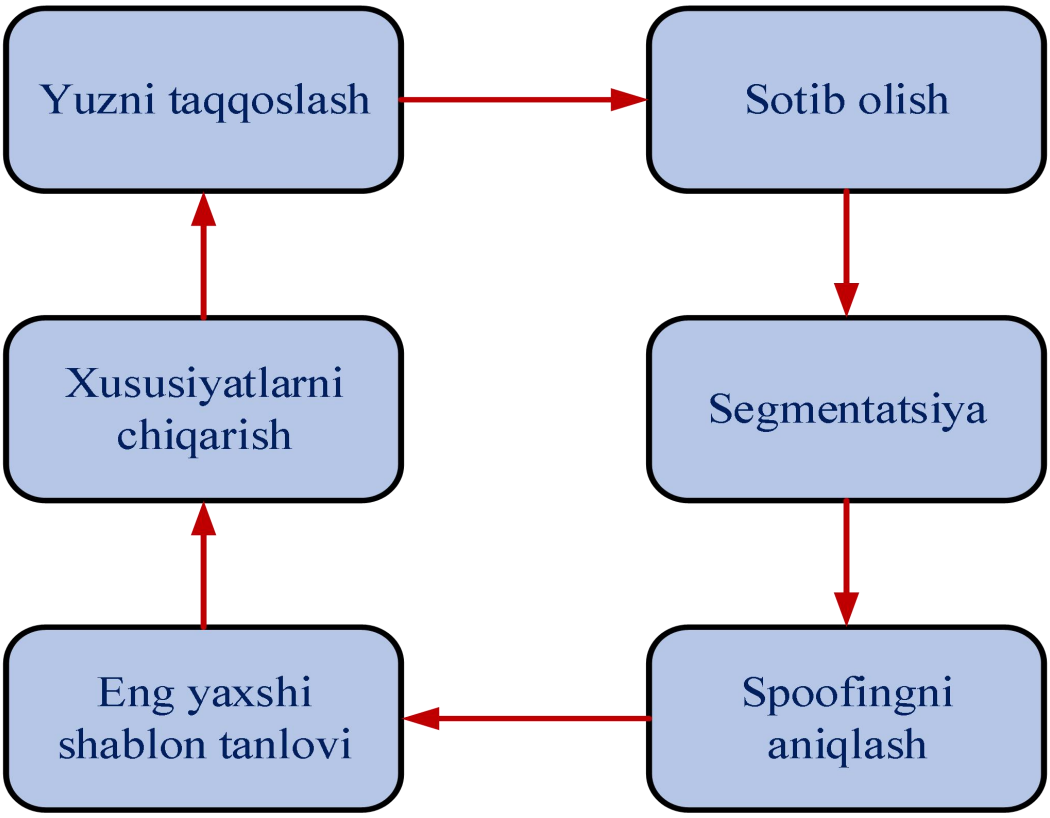


2-rasm. **Monitoring tizimi arxitekturasi**

Ushbu 2-rasmda chiqish potentsial hodisalar haqida ogohlantirishlar va tashkilot jarayonlarini tavsiflovchi xavf ko‘rinishida keladi.

FAME: Mobile Encounter uchun yuz autentifikatsiyasi

Ushbu tadqiqot ishida ular mobil uchrashuvlar uchun yuz autentifikatsiyasini Android-dan foydalanadigan mobil qurilmalar uchun o‘rnatilgan dastur sifatida topdilar, u ijtimoiy faoliyatni qo‘llab-quvvatlaydigan tekshirish va identifikatsiyani boshqarishni ta'minlaydi, masalan, ijtimoiy tarmoqda dublonlar topish. FAME firibgarlikka qarshi, tasvir olish, yuzni segmentatsiyalash, yuzni aniqlash, xususiyatni ajratib olish va yuzni moslashtirishdan iborat bo‘lib, ular yordamida foydalanuvchi qabul qilishini, maqbulligini, foydalanish qulayligini, ishonchliligini, maxfiyligini va xavfsizligini ko‘rsatadi.



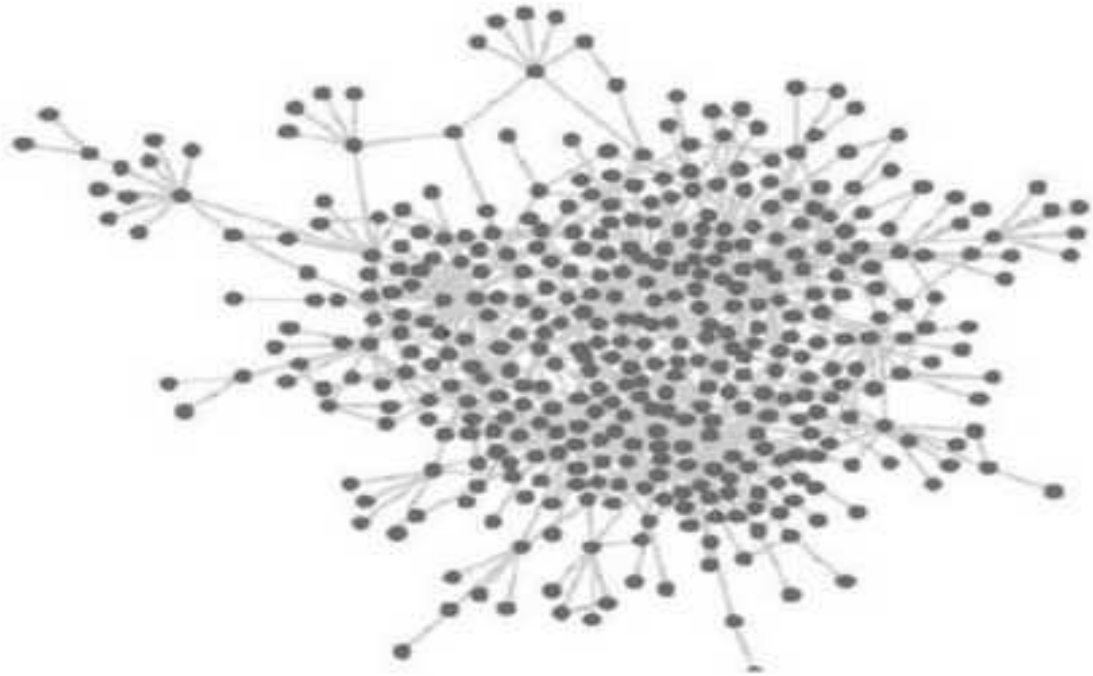
3-rasm. **FAME arxitekturasi**

2.9-rasmdagi aylanma naqsh salbiy javobdan so‘ng foydalanuvchi uchun shaffof bo‘lgan tizim tomonidan ikkinchi urinish avtomatik ravishda ishga tushirilishini ko‘rsatadi.

Havolalarni qayta qurish hujumi: Havola bashoratidan foydalanish Ijtimoiy tarmoqlarning maxfiyligini buzish algoritmlari

Maykl Fire ijtimoiy tarmoqni buzish uchun havolalarni bashorat qilish algoritmini hal qildi, unda ijtimoiy tarmoqlardagi havolalarni bashorat qilishning turli usullari mavjud va foydalanuvchi havolalarini qayta tiklash uchun uni turli xil ijtimoiy tarmoq jamoalarida sinab ko‘rish mumkin. Bog'lanishni qayta tiklash hujumini taklif qiladi, chunki ular avvalgi usulda ruxsatsiz hujumlar ehtimoli uchun kamroq xavfsizlik bor deb o‘ylashadi. Shunday qilib, bu usul hisoblash oson topologik xususiyatlarning kichik to‘plamiga o‘rgatilgan mashinani o‘rganish tasniflagichiga asoslangan. Ular ikkita to‘plamni yaratdilar: biri oson o‘quv to‘plami, ikkinchisi esa har bir jamoa uchun qattiq o‘quv to‘plami bo‘lib, unda ikkalasi ham 50% ijobiy va 50% salbiy havolalarni o‘z ichiga oladi. Ijobiy aloqalar jamiyat ichida mavjud bo‘lganlardir va salbiy aloqalar mavjud emas. Oson ta'lim to‘plamida salbiy havolalar tasodifiy tanlab, ular orasida bog'lanmagan ikkita tugun tomonidan yaratiladi. Qattiq o‘quv majmuasida salbiy aloqalar jamiyatda bir-biridan ikki

masofaga ega bo‘lgan ikkita tugunni tanlash orqali yaratiladi. Har bir jamoaning kichikligi sababli, har bir o‘quv majmuasining hajmi har bir jamoadagi mavjud bo‘g'inlar sonidan ikki baravar katta bo‘lar edi.



3-rasm. **Facebook hamkasblari jamoasi ijtimoiy tarmog'i**

Yuqoridagi 3-rasmda ular Facebook-ning asosiy do‘stlik grafigiga ishora qiladilar, unda tasniflagichlar o‘zlarining Facebook profil sahifalariga ko‘ra o‘sha mashhur yuqori texnologiyali kompaniyada ishlagan kichik hamkasblar jamoasi uchun baholanadi. Facebook foydalanuvchilari shaxsiy profil yaratishlari, do‘stlar qo‘shishlari va boshqa a’zolar bilan muloqot qilishlari mumkin. Ikki a'zo o‘rtasidagi do‘stlik aloqasi o‘zaro bo‘lishi kerakligi sababli, A a'zosi va B a'zosi o‘rtasida o‘zaro bog'liqlik mavjud. Shuning uchun hamkasblar hamjamiyatining tarmoq grafigi 410 ta tugun va 635 ta havolani o‘z ichiga olgan; u 2012 yil yanvar oyi boshida veb-brauzer yordamida olingan.

Ular uchun ular F-o‘lchovlari va egri o‘lchovlar ostidagi maydonni aylantirish o‘rmon algoritmi bilan ishlatadilar, bu esa jamoa ma'lumotlar to‘plamini sinab ko‘rish uchun ishlatiladi. Bu usul faqat foydalanuvchining boshqalarga yuqori aniqlik bilan ulanishi va foydalanuvchi maxfiyligini yashirish uchun mo‘ljallangan.

Onlayn ijtimoiy media tarmog'idagi tahdidlar va yechimlar. Ijtimoiy media tarmog'ida tahdidlar va yechimlar bizning ma'lumotlarimizni soxta foydalanuvchilardan himoya qilish va maxfiylik yechimini yaxshilash uchun ishlatiladi. Ikki xil tahdid mavjud, biri klassik tahdid, ikkinchisi zamonaviy tahdid. Bugungi tajovuzkorlar ushbu ikki tahdidni birlashtirib, foydalanuvchining maxfiyligini halokatli hujumga nisbatan hurmatliroq qilishlari mumkin.

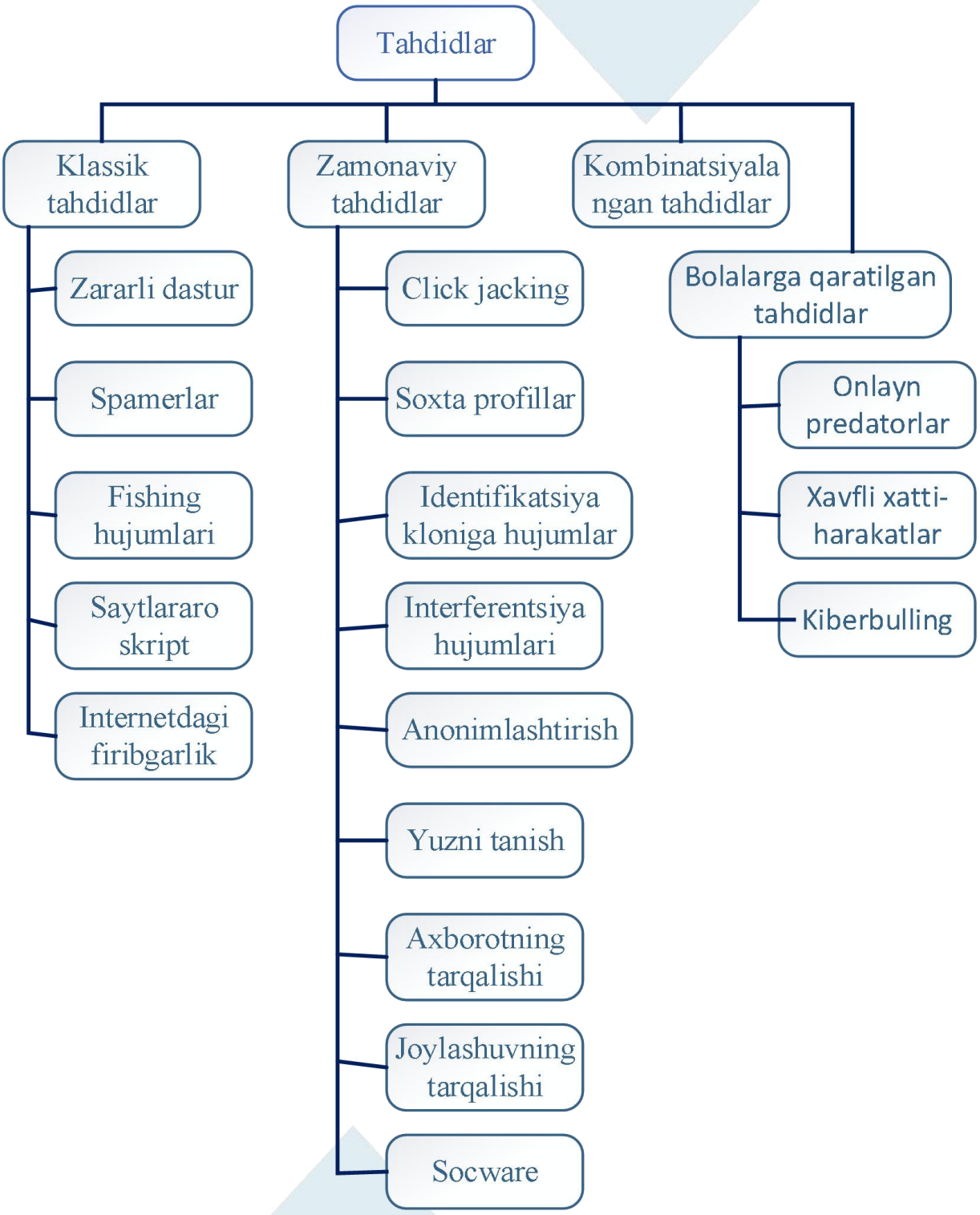
Yuqoridagi 4-rasmda asosan to‘rt toifaga bo‘lingan barcha tahdidlar ko‘rsatilgan:

- Klassik tahdidlar: Klassik tahdidlar foydalanuvchining ijtimoiy tarmoqlarda chop etilgan shaxsiy ma'lumotlaridan do‘stlarining shaxsiy ma'lumotlariga hujum qilish va hujum qilish uchun foydalanadi. U foydalanuvchi tarmog'i orasida juda tez tarqaladi.

- Zamonaviy tahdidlar: Bu, ayniqsa, foydalanuvchining shaxsiy ma'lumotlariga qaratilgan. Misol uchun, u soxta profil yaratish va boshqa maqsadli foydalanuvchiga so‘rov yuborish uchun ma'lumot to‘playdi.

- Kombinatsiyalangan tahdidlar: Bu klassik va zamonaviy tahdidlarning kombinatsiyasi. Masalan, foydalanuvchi parolini yig'ish va klik yordamida boshqa maqsadli foydalanuvchiga yuborish uchun fishing hujumidan foydalaning. Yashirin virus mavjud, shuning uchun maqsadli foydalanuvchi e'lon qilingan xabarni bosganda, u o‘rnatiladi.

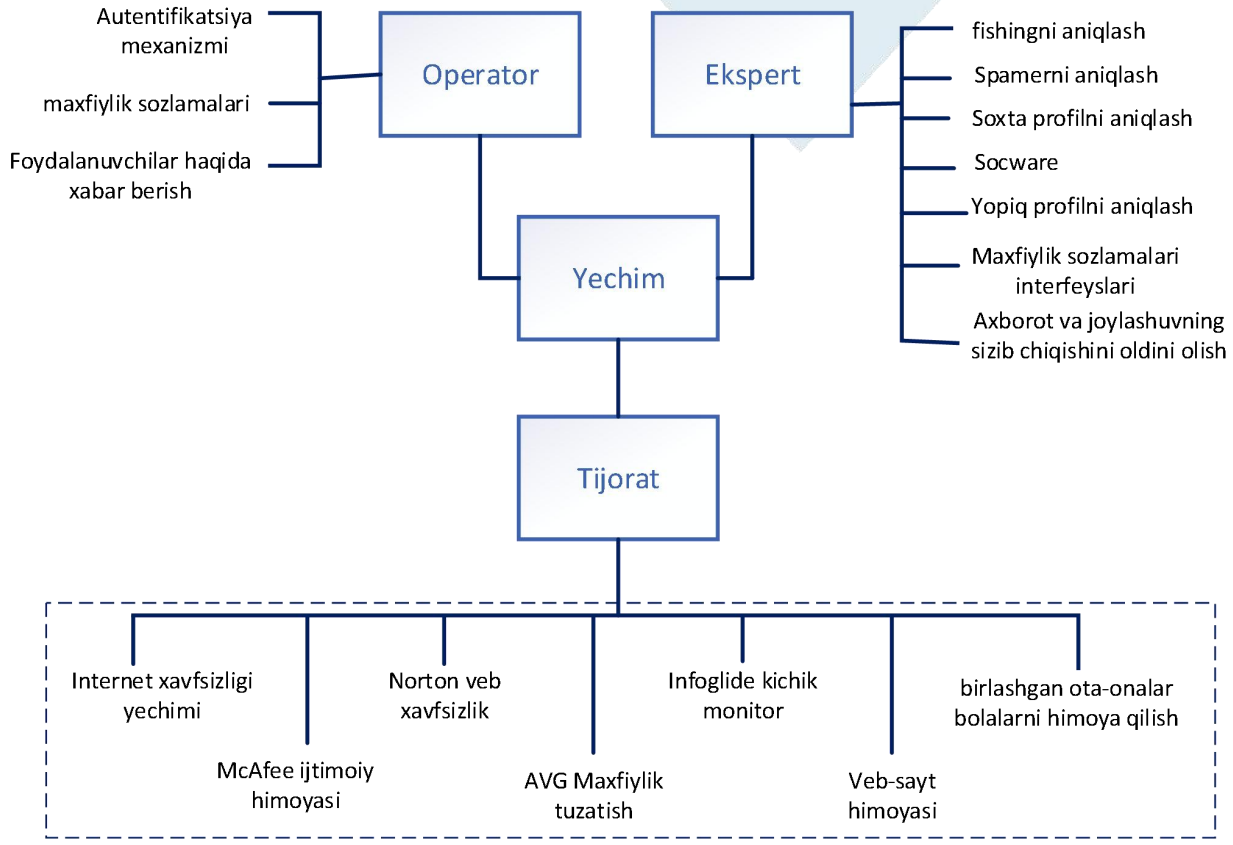
- Bolalarga qaratilgan tahdidlar: uning kichik yoshdagi bolalar uchun mo‘ljallangan, notanish odam bilan suhbatlashish va hokazo.



4-rasm. **Onlayn ijtimoiy media tarmoqlar foydalanuvchilariga tahdidlar**

Yashirin virus faollashtirilgan va shu tariqa tajovuzkorlar tomonidan foydalaniladigan foydalanuvchilar haqidagi shaxsiy ma'lumotlarni to‘playdigan yashirin chertish hujumini o‘z ichiga olgan troyandan foydalaniladi.

INTERNATIONAL MULTIDISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
SJIF 2019: 5.222 2020: 5.552 2021: 5.637 2022:5.479 2023:6.563 2024: 7,805
eISSN :2394-6334 https://www.ijmrd.in/index.php/imjrd Volume 12, issue 04 (2025)



5-rasm. **Onlayn ijtimoiy media va tarmoq uchun yechim**

Yuqoridagi 5-rasmda Facebook immunitet tizimini faollashtirish orqali foydalanuvchilarni va ma'lumotlarni zararli hujumlar, spamerlar, soxta profillar, firibgarlik va boshqa tahdidlardan himoya qilish uchun onlayn ijtimoiy media tarmog'i yechimi ko‘rsatilgan. Internet xavfsizligi yechimlari turli kompaniyalar tomonidan taqdim etilgan internet xavfsizligi yechimlarini ta'minlovchi AVG, Avira, Kaspersky, Panda, MacAfee va Symantec [19] tomonidan ta'minlanishi mumkin. Ba'zi usullar fishing veb-saytlari va URL manzillarini aniqlash uchun ishlatiladi; Net Nanny - bu bolalarni zararli kontentdan himoya qilish uchun dastur. NoScript Security Suite, Facebook uchun maxfiylik skaneri, defensio, YouTube'dan video spamerni aniqlash algoritmi, ma'lumotlar va joylashuvning sizib chiqishini oldini olish va boshqalar mavjud, barchasi tahdidlar uchun yechimdir.

1-jadvalda eng mashhur 5 ta ijtimoiy tarmoq saytlari, oylik tashrif buyuruvchilar soni raqobat darajasida ko‘rsatilgan. 1-jadval

1-jadval

No.	Saytlar	Taxminiy oylik tashrif buyuruvchilar	Raqobat darajasi
1.	Facebook	900,000,000	3
2.	Twitter	310,000,000	21
3.	LinkedIn	255,000,000	25

4.	Pinterest	250,000,000	27
5.	GooglePlus+	120,000,000	32

Kelajakda internet keng ko‘lamlilik, shaffoflik, harakatchanlik, mustahkamlik, xavfsizlik, turlichalik, xizmat ko‘rsatish sifati kabi turli jihatlarga oid bir nechta tashvishlarni yengish uchun statsionar va mobil ilovalar uchun shaffof transport xizmatlarini taklif qiluvchi yuqori o‘tkazuvchanlik tarmoq arxitekturasi tomon rivojlandi, qayta konfiguratsiya, kontekstdan xabardorlik, boshqarish, ma'lumotlarga markazlashish, iqtisod va boshqalar. Maxfiylik va xavfsizlik uchun biz yaqinlashib kelayotgan cheklovlar uchun joriy internet arxitekturasida evolyutsion yechim yaratdik. Intellektual mulk va mulkiy ma'lumotlarning yo‘qolishi tashkilot uchun xavf bo‘lishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. S.K.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: o‘quv qo‘llanma. – T.: «Aloqachi», 2020, 303 bet.

2. O‘zbekiston Respublikasining 2022-yil 25-fevralda qabul qilingan O‘RQ-764-son “Kiberxavfsizlik tog’risida”gi qonuni.

3."Hacking Exposed: Network Security Secrets & Solutions" - Stuart McClure, Joel Scambray, George Kurtz.

4. "Network Security: Private Communication in a Public World" - Charlie Kaufman, Radia Perlman, Mike Speciner.

5. "Cybersecurity: Attack and Defense Strategies" - Yuri Diogenes, Erdal Ozkaya.