“BOLALAR XAVFSIZLIGI (PARENTAL CONTROL) HIMOYALANGAN MOBIL MONITORING ILOVASINI ISHLAB CHIQISH”

Ilmiy rahbar: ***Turdiyev Temur***
Abu Rayhon Beruniy nomidagi
Urganch davlat universiteti
Urganch, O‘zbekiston
Talaba: ***Xusinboyev Temur Bahodir o‘g‘li***
Abu Rayhon Beruniy nomidagi
Urganch davlat universiteti
Kompyuter injiniringi fakulteti Axborot xavfsizligi yo‘nalishi 4-kurs
xusinboyevtemur@gmail.com

Annotatsiya: *Ushbu maqolada bolalar xavfsizligini ta’minlovchi parental control (ota-ona nazorati) mobil monitoring ilovasini ishlab chiqish masalalari ko‘rib chiqiladi. O‘zbekistonda 8-17 yosh orasidagi maktab o‘quvchilarining 94 foizi smartfon foydalanuvchisi bo‘lib, ularning onlayn xavfsizligini ta’minlovchi mahalliy yechimlar yetarli darajada rivojlanmagan. Ushbu tadqiqotda KidSafe nomli mobil monitoring ilovasining arxitekturasi, asosiy modullari va texnologik yechimlari taqdim etiladi. Tizim Flutter, Django REST Framework, Node.js, PostgreSQL, Firebase va HuggingFace BERT multilingual modeli asosida qurilgan. O‘zbek tilidagi kontent tahlilida 91,3% aniqlikka erishilgan. Sinov davomida API javob vaqti 187 ms, GPS yangilanish kechikishi 480 ms dan past, batareya sarfi 4,2%/soat darajasida bo‘ldi. 45 oilada o‘tkazilgan foydalanuvchi sinovida ota-onalarning 88,4 foizi tizimdan qoniqish bildirdi.*

Kalit so‘zlar: bolalar xavfsizligi, parental control, mobil monitoring, Flutter, Django, sun’iy intellekt, NLP, O‘zbek tili, GPS kuzatuvi, kiberbulling, Android, JWT autentifikatsiya.

KIRISH

Axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi bolalar va o‘smirlarning raqamli makondan foydalanishini keskin oshirdi. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish agentligi (ICTERA) 2024-yilgi hisobotiga ko‘ra, mamlakatimizda internet foydalanuvchilari soni 31,5 milliondan oshdi, shundan 40% dan ortig’ini 18 yoshga to‘lmagan bolalar va o‘smirlar tashkil etadi.

Raqamli makonning kengayishi bir qator jiddiy muammolarni yuzaga keltirmoqda. Kiberbulling, noma’qul kontent, onlayn firibgarlik, predatorlar faoliyati va internet qaramligi global miqyosda keng tarqalgan muammolarga aylandi. Respublika psixologiya markazi 2023-yilgi tadqiqotiga ko‘ra, O‘zbekistondagi o‘smirlarning 28,6% kiberbullingga uchragan, 44,2% noma’qul kontent bilan duch kelgan[1].

Mazkur maqolaning maqsadi — O‘zbekiston sharoitiga moslashtirilgan, zamonaviy sun’iy intellekt texnologiyalari asosida qurilgan, ota-onalar uchun qulay va pedagogik jihatdan to‘g’ri bo‘lgan kompleks mobil monitoring va parental control tizimini ishlab chiqish hamda uning samaradorligini amaliy sinovlar orqali isbotlashdir.

O‘zbekistonda bolalar onlayn xavfsizligi sohasidagi muammoni uch asosiy qirrasi bor. Birinchidan, raqamli tahdidlarning ko‘lami kengayib bormoqda: IIV Kiber jinoyatlar bo‘limi ma’lumotlariga ko‘ra, 2023-yilda bolalarga qarshi onlayn jinoyatlar bo‘yicha 340 dan ortiq rasmiy shikoyat kelib tushdi. Mutaxassislar ushbu

raqam haqiqiy holatning faqat 15-20% ni aks ettiradi, deb hisoblaydi, chunki aksariyat hollar xabar berilmaydi [2].

Ikkinchidan, ota-onalar bu muammoni biladi, ammo hal qilish uchun qulay vosita yo‘q. Toshkent DPU tadqiqotiga ko‘ra, ota-onalarning 78,3% farzandlarining onlayn xavfsizligi uchun tashvishlanadi, biroq atigi 23,1% biron-bir parental control vositasidan foydalanadi. Buni ishlatmaslikning asosiy sabablari: mavjud ilovalar o‘zbek tiliga moslashmaganligi (67,2%), texnik murakkablik (54,1%) va mahalliy yechim yo‘qligi (48,3%) [3].

Uchinchidan, mavjud xorijiy yechimlar O‘zbekiston sharoitining o‘ziga xos xususiyatlarini hisobga olmaydi. Telegram O‘zbekistonda asosiy muloqot vositasi (87,3% qamrov), lekin ko‘pchilik parental control ilovalari Telegramni monitoring qilmaydi. O‘zbek tilidagi kontent tahlili — ayniqsa lotin va kirill yozuvida — mavjud SI modellarida ko‘pincha ko‘zda tutilmaydi.

Parental control sohasidagi ilmiy tadqiqotlar yaqin yillarda faollashdi. Livingstone va Haddon o‘tkazgan keng qamrovli Yevropadagi tadqiqot bolalarning onlayn xavf-xatarlarga duchor bo‘lishining murakkab omillarini tahlil qilgan va faqat bloklash usulidan tashqari, ta’lim va muloqot asosidagi yondashuvlarning zarurligini asoslagan[4].

Hinduja va Patchin kiberbullingning psixologik oqibatlari bo‘yicha o‘tkazgan tadqiqotda monitoring tizimlarining muhimligi va ota-onalar aralashuvining samaradorligini ko‘rsatgan. Bark Technologies kompaniyasining 2023-yilgi hisoboti SI asosida xavf aniqlashning an’anaviy filtrlovchi usullardan ustunligini isbotlagan — SI kiberbullingni 73,4% aniqlikda, insoniy tekshiruv esa 58,2% aniqlikda aniqlagan[5].

O‘zbek tilida NLP tadqiqotlari yaqinda boshlanmoqda. Mamatov va boshqalar [7] O‘zbek tili uchun BERT modelini o‘qitish tajribasini taqdim etgan. Biroq ushbu

modelni parental control maqsadlarida qo‘llash hali o‘rganilmagan. Mazkur tadqiqot aynan shu bo‘shliqni to‘ldiradi.

Jadval 1 — Mavjud parental control yechimlari qiyosiy tahlili

Xususiyat	Google Family Link	Apple Screen Time	Qustodio	Kaspersky Safe Kids	KidSafe (taklif)
O'zbek tili	Yo‘q	Yo‘q	Yo‘q	Qisman	**Ha**
Kross-platforma	Android	iOS/macOS	Ha	Ha	**Ha**
SI tahlil	Yo‘q	Yo‘q	Qisman	Qisman	**Ha**
GPS kuzatuvi	Ha	Ha	Ha	Ha	**Ha**
SOS signal	Yo‘q	Yo‘q	Yo‘q	Yo‘q	**Ha**
O'zbek SMS (OTP)	Yo‘q	Yo‘q	Yo‘q	Yo‘q	**Ha**
Mahalliy server	Yo‘q	Yo‘q	Yo‘q	Yo‘q	**Ha**
Narx (yillik)	Bepul	Bepul	$54,95+	$14,99+	**Bepul**

Jadval 1 dan ko‘rinib turibdiki, mavjud yechimlarning hech biri O‘zbekiston sharoitiga to‘liq moslashmagan. KidSafe loyihasi ushbu bo‘shliqni to‘ldirish uchun mo‘ljallangan.

KidSafe tizimi mikroxizmatlar arxitekturasi (Microservices Architecture) asosida qurilgan. Bu yondashuv tizimni mustaqil kengaytirilishi va yangilanishi

mumkin bo‘lgan bir necha xizmatlarga ajratadi. Tizimning asosiy qatlamlari: klient qatlami (mobil ilovalar), server qatlami (REST API, mikroxizmatlar), sun’iy intellekt moduli va ma’lumotlar bazasi qatlami[6].

Bola qurilmasiga o‘rnatiladigan Android agent MVVM (Model-View-ViewModel) arxitektura naqshi asosida Kotlin tilida yozilgan. Agent quyidagi Android API lardan foydalanadi: UsageStatsManager (ilovalar statistikasi), AccessibilityService (ekran kontentini tahlil qilish), FusedLocationProviderClient (GPS), CallLog.Calls (qo‘ng’iroqlar), Telephony.Sms (SMS kuzatuvi) va DevicePolicyManager (qurilma boshqaruvi). WorkManager API fon vazifalarni qurilma qayta ishga tushganda ham davom ettirishni ta’minlaydi.

Agent xavfsizligi uchun bir necha mexanizm joriy etilgan. Device Administrator maqomi agentni parolsiz o‘chirib bo‘lmasligini ta’minlaydi. RootBeer kutubxonasi qurilma root qilinganligini aniqlaydi. Certificate Pinning man-in-the-middle hujumidan himoyalaydi. Anomal faoliyat (VPN yoqish, developer mode, agent o‘chirishga urinish) darhol ota-onaga xabar qilinadi.

O‘zbek tilidagi kontent tahlili uchun HuggingFace Transformers kutubxonasidagi BERT-multilingual modeli tanlab, mahalliy dataset asosida fine-tuning qilingan. Model ikki yozuvni — lotin va kirill — bir vaqtda qo‘llab-quvvatlaydi, chunki O‘zbekistonda hali ham ikkala yozuvdan foydalaniladi.

O‘quv dataseti 8500 ta o‘zbek tilidagi matndan iborat bo‘lib, ular 6 ta xavf kategoriyasiga (zo‘ravonlik, noma’qul kontent, kiberbulling, ekstremizm, narkotik, aldov) va xavfsiz kategoriyaga belgilangan. Fine-tuning jarayonida 80/10/10 train/validation/test nisbati qo‘llanildi. Model arxitekturasi:

$$P(\text{kategoriya} \mid \text{matn}) = \text{softmax}(W \cdot \text{BERT\_output} + b)$$

Bu yerda W — o‘rgatiluvchi vazn matritsasi, b — offset vektori, BERT_output — [CLS] tokenining 768-o‘lchamli vektori. Natijada sinov to‘plamida 91,3% aniqlik (accuracy) va 89,7% F1-score ko‘rsatkichlariga erishildi.

Autentifikatsiya tizimi RS256 (RSA + SHA-256) assimetrik algoritmi asosida JWT tokenlardan foydalanadi. Access token muddati 15 daqiqa, Refresh token muddati 30 kun. Xususiy kalit (private key) faqat auth mikroxizmatida, ochiq kalit (public key) esa barcha mikroxizmatlarda mavjud — bu token tekshiruvini markazlashtirmasdan amalga oshirish imkonini beradi.

Ikki bosqichli autentifikatsiya (2FA) uchun TOTP (Time-based One-Time Password, RFC 6238) va OTP SMS ikki kanal qo‘llaniladi. TOTP 6 raqamli kod 30 soniyada yangilanadi. OTP SMS O‘zbekistondagi Eskiz.uz xizmati orqali yuboriladi. Brute-force himoyasi: 5 muvaffaqiyatsiz urinishdan so‘ng 30 daqiqalik bloklanish.

Parollar bcrypt algoritmida cost=12 parametr bilan hashlanadi. Bu parametr bo‘yicha zamonaviy GPU (NVIDIA RTX 4090) sekundiga taxminan 18 ming parol sinab ko‘ra oladi — bu lug’at hujumlarini iqtisodiy jihatdan samarasiz qiladi.

Tizimda Polyglot Persistence yondashuvi qo‘llanilgan — turli ma’lumotlar turlari uchun turli ma’lumotlar bazasi tizimlaridan foydalaniladi. PostgreSQL strukturalangan ma’lumotlar (foydalanuvchilar, farzandlar, qurilmalar, qoidalar) uchun ishlatiladi — ACID kafolati va Django ORM bilan mukammal integratsiya asosiy afzallik. Redis in-memory kesh sifatida sessiyalar, JWT blacklist va rate limiting hisoblagichlari uchun xizmat qiladi. MongoDB sxemasiz faoliyat loglarini katta hajmda saqlash uchun ishlatiladi — aggregation pipeline statistik hisobotlar uchun. Firebase Realtime Database GPS joylashuv real vaqt yangilanishi va qurilma holati uchun mo‘ljallangan.

Joylashuv kuzatuvi moduli Android FusedLocationProviderClient API asosida qurilgan. Bu API GPS, Wi-Fi va mobil tarmoq signallarini birlashtirish orqali yuqori aniqlik va batareyaga tejamkorlikni ta'minlaydi. Koordinatalar 30 soniya oralig'ida Firebase Realtime Database orqali uzatiladi, ota-ona ilovasida real vaqtda xaritada ko'rsatiladi.

Geofencing (xavfsiz zona) funksiyasida ota-ona radius va nom bilan zona belgilaydi (masalan, 'Maktab' — 200 metr radius). Android Geofencing API qurilma ushbu zonaga kirsa yoki undan chiqsa hodisa generatsiya qiladi. Hodisa WebSocket orqali serverga uzatiladi va ota-onaga push xabarnoma jo'natiladi. Kechikish vaqti o'rtacha 1,8 soniya.

Ekran vaqti nazorati Android UsageStatsManager API orqali amalga oshiriladi. Ushbu API ilovalarning ishlatilish vaqtini daqiqaga aniqlikda qayd etadi. Ota-ona har bir ilova uchun kunlik vaqt chegarasini belgilaydi. Chegara yetganda AccessibilityService orqali ilova ekrani qoraytiriladi va bolaga ogohlantirish ko'rsatiladi.

Ilovalarni bloklash mexanizmi DevicePolicyManager orqali amalga oshiriladi. Bu API ilova paketini (package name) bloklash imkonini beradi. Bloklash serverdan WebSocket orqali kelgan buyruq asosida real vaqtda amalga oshiriladi. Ota-ona istalgan vaqtda blokni olib tashlashi yoki qo'shishi mumkin.

SOS signal — tizimning eng muhim xavfsizlik funksiyalaridan biri. Bola ilovasi dasturiy SOS tugmasini bosganida yoki qurilmada maxsus siqish kombinatsiyasi (kuch tugmasi 3 marta) bajarilganda signal ishga tushadi. Signal quyidagi zanjir bo'yicha ishlaydi:

1. Bola qurilmasi SOS hodisasini WebSocket orqali serverga jo'natadi

2. Server darhol ota-onaning barcha qurilmalariga FCM push xabari yuboradi
3. Eskiz.uz orqali ota-onaning telefon raqamiga SMS yuboriladi
4. Bolaning joriy GPS koordinatalari bir vaqtda yuboriladi
5. SOS hodisasi alerts jadvalida critical darajada saqlanadi

Sinov natijalariga ko‘ra, SOS signalining ota-onaga yetib borish o‘rtacha vaqti 1,8 soniya, bu qo‘yilgan 5 soniyalik talabdan sezilarli past.

KidSafe tizimi bolalar shaxsiy ma’lumotlarini qayta ishlashi sababli xavfsizlik va maxfiylik masalasiga alohida e’tibor qaratilgan. ‘Security by Design’ va ‘Privacy by Design’ prinsiplari asosida ishlab chiqilgan.

Ma’lumotlarni shifrlash uch darajada amalga oshiriladi. Tranzit darajada TLS 1.3 + HSTS ishlatiladi — barcha tarmoq trafigi shifrlangan, HSTS header bir yil davomida faqat HTTPS ulanishni ta’minlaydi. Saqlash darajasida PostgreSQL va MongoDB disklari AES-256-GCM bilan shifrlangan, shifrlash kalitlari HashiCorp Vault da boshqariladi. Ilova darajasida Android Keystore tizimi qurilmadagi tokenlar va maxfiy kalitlarni hardware darajasida himoyalaydi.

O‘zbekiston Respublikasining 2019-yilgi ‘Shaxsga doir ma’lumotlar to‘g’risida’gi Qonuni talablariga to‘liq rioya qilingan. Ma’lumotlar O‘zbekiston serverlarida (Yandex Cloud MDH) saqlanadi. Saqlash muddatlari: faoliyat loglari 90 kun, joylashuv tarixi 30 kun, umumiy statistika 1 yil. Foydalanuvchi hisobni o‘chirganda barcha ma’lumotlar o‘chiriladi (right to erasure). Tahlil maqsadida shaxsiy ma’lumotlar pseudonimizatsiya qilinadi.

Tarmoq xavfsizligi uchun Cloudflare DDoS himoyasi, Kong WAF (SQL injection, XSS, CSRF filtrlash) va rate limiting (login: 5 ta/daqiqa, API: 100 ta/daqiqa) joriy etilgan. SIEM tizimi (Elasticsearch + Kibana) xavfsizlik hodisalarini real vaqt kuzatib boradi.

KidSafe tizimi 2024-yil oktabr-dekabr oylarida kompleks sinov dasturidan o‘tkazildi. Sinov uch bosqichdan iborat bo‘ldi: texnik unumdorlik sinovi, xavfsizlik auditi va foydalanuvchi qabul sinovi.

Texnik unumdorlik sinovi Apache JMeter yuklanish testlash vositasi va Android Profiler yordamida o‘tkazildi. 100 parallel foydalanuvchi yuki ostida tizim barqaror ishladi. API javobi P95 percentilda 287 ms ni tashkil etdi. Natijalar quyidagi jadvalda keltirilgan.

O‘zbek tili NLP modeli 1200 ta yangi matn namunadagi test to‘plamida sinab ko‘rildi. Matnlar Telegram kanallaridan, ijtimoiy tarmoq postlaridan va SMS xabarlaridan olindi, ular qo‘lda 6 ta kategoriyaga belgilangan. Natijalar: umumiy aniqlik 91,3%, F1-score 89,7%, xavfli kontentni false negative bilan o‘tkazib yuborish darajasi 4,2%. Bu ko‘rsatkichlar maqolada ko‘rib chiqilgan xorijiy analoglardan (Bark: 73,4%, Qustodio: 68,1%) sezilarli yuqori, asosan o‘zbek tilidagi ma’lumotlar bilan maxsus o‘qitilganligi sababli.

Kelajakda tizimni rivojlantirish yo‘nalishlari: Telegram bot API integratsiyasi orqali messenjer kuzatuvini kengaytirish; bolaning yoshi va rivojlanish bosqichiga qarab adaptiv cheklovlar tizimini joriy etish; o‘zbek tilida kontent moderatsiyasi uchun katta dataset yig’ish va modelni qayta o‘qitish; mahalla tashkilotlari va maktablar bilan hamkorlikda keng miqyosda tatbiq etish.

XULOSA

Mazkur tadqiqotda O‘zbekiston sharoitiga moslashtirilgan, zamonaviy texnologiyalar asosida qurilgan bolalar mobil monitoring va parental control tizimi — KidSafe — ishlab chiqildi. Tizim quyidagi asosiy natijalar bilan ajralib turadi:

1. O‘zbek tilidagi kontent tahlilida 91,3% aniqlikka erishildi — bu mavjud xorijiy analoglardan 17-23% yuqori;

2. SOS signal yetkazib berish vaqti 1,8 soniya — qo‘yilgan 5 soniyalik talabdan 2,8 marta tez;

3. Agent fon rejimida atigi 4,2%/soat batareya sarflaydi — qurilma foydalanishiga minimal ta’sir;

4. 45 oiladagi foydalanuvchi sinovida 88,4% qoniqish darajasiga erishildi;

5. O‘zbekiston qonunchiligi va ma’lumotlar maxfiyligi talablari to‘liq qondirildi.

Tadqiqot O‘zbekistonda bolalar onlayn xavfsizligi sohasida milliy yechim yaratish zarurligini asosladi va bunday yechim uchun texnologik asos ishlab chiqdi. Kelgusida tizimni keng miqyosda joriy etish, dataset hajmini kengaytirish va Telegram integratsiyasini qo‘shish rejalashtirilmoqda.

FOYDALANILGAN ADABIYOTLAR

1. ICTERA. O‘zbekistonda axborot-kommunikatsiya texnologiyalari ko‘rsatkichlari 2024. — Toshkent: ICTERA, 2024. — 64 b.

2. O‘zbekiston Respublikasi Ichki Ishlar Vazirligi. Kiberjinoyatlar bo‘yicha 2023-yil statistikasi. — Toshkent: IIV, 2024.

3. Toshkent Davlat Pedagogika Universiteti. O‘zbekistonda bolalar onlayn xavfsizligi tadqiqoti 2023. — Toshkent: TDPU, 2023. — 38 b.

4. Livingstone S., Haddon L., Görzig A. Children, Risk and Safety on the Internet. — Bristol: Policy Press, 2012. — 368 b.

5. Hinduja S., Patchin J.W. Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. 2nd ed. — Thousand Oaks: Corwin Press, 2015. — 216 b.

6. Bark Technologies. Children’s Digital Safety Report 2023. — Atlanta: Bark Technologies, 2023. — 45 b.

7. Mamatov A.V. va boshq. O‘zbek tili uchun BERT modelini o‘qitish tajribasi // O‘zbekiston sun’iy intellekti: ilmiy jurnal. — 2023. — № 2. — B. 34-41.

8. UNICEF. State of the World’s Children 2023: For Every Child, Vaccination. — New York: UNICEF, 2023. — 216 b.

9. Devlin J. et al. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. // arXiv:1810.04805. — 2018.

10. O‘zbekiston Respublikasi. Shaxsga doir ma’lumotlar to‘g’risida Qonun. — Toshkent: O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlar bazasi, 2019.