MOBIL ILOVALAR XAVFSIZLIGINI TA’MINLASHNING ZAMONAVIY USULLARI

Jizzax shahar Yoshlar ishlari bo‘limi referenti
Sarbon Universiteti
“Davlat va jamiyat boshqaruvi”
yo‘nalishi 1-kurs talabasi
Aliyeva Durdona Jamshid qizi

Annotatsiya

Mazkur maqolada mobil ilovalar xavfsizligini ta’minlashning zamonaviy usullari, mobil qurilmalar orqali ma’lumotlar almashinuvida yuzaga keladigan xavfsizlik tahdidlari hamda ularni bartaraf etish mexanizmlari tahlil qilingan. Shuningdek, mobil ilovalarda uchraydigan asosiy kiberxavf turlari, jumladan, zararli dasturlar, fishing hujumlari, ma’lumotlar sizib chiqishi, autentifikatsiya zaifliklari va tarmoq xavfsizligi bilan bog‘liq muammolar ko‘rib chiqilgan. Maqolada mobil ilovalar xavfsizligini oshirishda zamonaviy shifrlash algoritmlari, ko‘p bosqichli autentifikatsiya, biometrik himoya tizimlari hamda sun’iy intellekt texnologiyalaridan foydalanishning samaradorligi ilmiy jihatdan asoslab berilgan. Tadqiqot natijalari mobil ilovalar xavfsizligini takomillashtirish va foydalanuvchi ma’lumotlarini ishonchli himoya qilishda muhim ahamiyat kasb etadi.

Kalit so‘zlar: Mobil ilovalar, axborot xavfsizligi, kiberxavfsizlik, autentifikatsiya, biometrik himoya, shifrlash algoritmlari, zararli dasturlar, fishing hujumlari, ma’lumotlarni himoyalash, mobil texnologiyalar, sun’iy intellekt, tarmoq xavfsizligi, raqamli himoya, mobil platformalar, foydalanuvchi ma’lumotlari.

Kirish

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida mobil qurilmalar va mobil ilovalar inson hayotining ajralmas qismiga aylandi. Bugungi kunda smartfon va planshet qurilmalari nafaqat aloqa vositasi, balki moliyaviy operatsiyalarni amalga oshirish, elektron tijorat, masofaviy ta’lim, sog‘liqni saqlash, davlat

xizmatlaridan foydalanish hamda ijtimoiy kommunikatsiyalarni olib borishda muhim vosita sifatida keng qo‘llanilmoqda. Shu bilan birga, mobil ilovalarning ommalashuvi ularning xavfsizligini ta’minlash masalasini dolzarb muammolardan biriga aylantirmoqda.

Mobil ilovalar orqali katta hajmdagi shaxsiy va maxfiy ma’lumotlarning qayta ishlanishi kiberjinoyatchilar uchun yangi imkoniyatlarni yuzaga keltirmoqda. Xususan, foydalanuvchilarning shaxsiy ma’lumotlari, bank rekvizitlari, login va parollar, geolokatsiya ma’lumotlari hamda boshqa muhim axborotlarning noqonuniy o‘zlashtirilishi jiddiy xavf tug‘diradi. Natijada, zararli dasturlar (malware), fishing hujumlari, ma’lumotlarning sizib chiqishi, ruxsatsiz kirish va tarmoq hujumlari kabi tahdidlar soni ortib bormoqda.

Mobil ilovalar xavfsizligi — bu mobil platformalarda ishlovchi dasturiy mahsulotlarning foydalanuvchi ma’lumotlari, tizim resurslari va aloqa kanallarini turli kiberxavflardan himoya qilishga qaratilgan texnologiyalar hamda usullar majmuasidir. Ushbu yo‘nalishda xavfsizlikni ta’minlashning zamonaviy yondashuvlari sifatida ma’lumotlarni shifrlash, xavfsiz autentifikatsiya tizimlari, ko‘p faktorli himoya mexanizmlari, biometrik texnologiyalar va sun’iy intellekt asosidagi monitoring tizimlari keng qo‘llanilmoqda.

Mazkur maqolaning asosiy maqsadi mobil ilovalarda uchraydigan xavfsizlik tahdidlarini tahlil qilish, mavjud himoya usullarini ilmiy jihatdan o‘rganish hamda mobil ilovalar xavfsizligini oshirishning zamonaviy mexanizmlarini yoritishdan iborat. Tadqiqot davomida mobil platformalarda xavfsizlikni ta’minlashning dolzarb muammolari va istiqbolli texnologiyalari ko‘rib chiqiladi.

Mobil ilovalarda uchraydigan asosiy xavfsizlik tahdidlari

Mobil ilovalardan foydalanish ko‘lamining kengayishi bilan bir qatorda turli xil kiberxavfsizlik tahdidlari ham ortib bormoqda. Ushbu tahdidlar foydalanuvchi ma’lumotlarining maxfiyligi, yaxlitligi va mavjudligiga salbiy ta’sir ko‘rsatishi mumkin.

Shu sababli mobil ilovalar xavfsizligiga tahdid soluvchi asosiy omillarni aniqlash va ularni oldini olish muhim ahamiyat kasb etadi.

Birinchi navbatda, **zararli dasturlar (malware)** mobil ilovalar uchun asosiy xavf manbalaridan biri hisoblanadi. Bunday dasturlar foydalanuvchi qurilmasiga yashirin tarzda o‘rnatilib, shaxsiy ma’lumotlarni o‘g‘irlashi, bank ma’lumotlarini qo‘lga kiritishi yoki qurilma faoliyatiga zarar yetkazishi mumkin. Ayniqsa, norasmiy manbalardan yuklab olingan ilovalar zararli kodlarni o‘z ichiga olishi ehtimoli yuqori bo‘ladi.

Ikkinchi muhim tahdid — **fishing (phishing) hujumlari** hisoblanadi. Fishing usulida foydalanuvchilar qalbaki ilovalar yoki soxta havolalar orqali aldab, ularning login, parol va bank ma’lumotlari qo‘lga kiritiladi. So‘nggi yillarda mobil banking va elektron to‘lov tizimlari rivojlanishi bilan bunday hujumlar soni sezilarli darajada oshgan.

Uchinchidan, **ma’lumotlarning sizib chiqishi (data leakage)** mobil ilovalarda keng uchraydigan muammolardan biridir. Ayrim ilovalar foydalanuvchi roziligisiz shaxsiy ma’lumotlarni yig‘ishi yoki himoyasiz serverlarda saqlashi natijasida maxfiy axborotlar uchinchi shaxslarga oshkor bo‘lishi mumkin. Bu esa foydalanuvchilarning axborot xavfsizligiga jiddiy tahdid tug‘diradi.

To‘rtinchidan, **zaif autentifikatsiya tizimlari** ham mobil ilovalarda xavfsizlik darajasini pasaytiruvchi omillardan biri hisoblanadi. Oddiy parollar, bir bosqichli tasdiqlash tizimlari va kuchsiz xavfsizlik siyosati foydalanuvchi akkauntlariga noqonuniy kirish ehtimolini oshiradi.

Bundan tashqari, **ochiq Wi-Fi tarmoqlari orqali amalga oshiriladigan hujumlar** ham mobil qurilmalar uchun xavf tug‘diradi. Himoyalanmagan internet tarmoqlari orqali uzatilayotgan ma’lumotlar uchinchi tomon tomonidan tutib olinishi yoki o‘zgartirilishi mumkin. Shu sababli xavfsiz tarmoq protokollaridan foydalanish muhim hisoblanadi.

Foydalanilgan adabiyotlar

1. Computer Security: Principles and Practice / William Stallings. *Computer Security: Principles and Practice*. 4th Edition. — Pearson Education, 2018.
2. Cryptography and Network Security / William Stallings. *Cryptography and Network Security: Principles and Practice*. 7th Edition. — Pearson, 2017.
3. OWASP. *Mobile Application Security Testing Guide (MASTG)*. — Mobil ilovalar xavfsizligi bo‘yicha xalqaro metodik qo‘llanma.
4. Android Developers Security Guide — Android platformasida xavfsizlikni ta’minlash bo‘yicha rasmiy qo‘llanma.
5. Apple Developer Security Documentation — iOS ilovalari xavfsizligi bo‘yicha rasmiy hujjatlar.
6. Mobile Application Security / Dominic Chell, Tyrone Erasmus. *Mobile Application Security*. — McGraw-Hill Education, 2015.
7. International Telecommunication Union (ITU). *Global Cybersecurity Index Reports*. — Kiberxavfsizlik statistik ma’lumotlari va xalqaro tahlillar.
8. National Institute of Standards and Technology (NIST). *Guidelines on Mobile Device Security*. — Mobil qurilmalar xavfsizligi bo‘yicha tavsiyalar.
9. Cisco. *Annual Cybersecurity Report*. — Zamonaviy kiberxavfsizlik tahdidlari bo‘yicha tahliliy hisobot.
10. Kaspersky. *Mobile Threat Landscape Report*. — Mobil tahdidlar bo‘yicha zamonaviy hisobotlar.