ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 12 / UIF:8.2 / MODERNSCIENCE.UZ

ONLAYN TIZIMLARDA FOYDALANUVCHI XAVFSIZLIGINI TA'MINLASH: REAL VAQTDA FOYDALANUVCHI FAOLIYATINI MONITORING QILISH PLATFORMASINI LOYIHALASH, AMALGA OSHIRISH VA BAHOLASH

Akbarova M.
Qurbonov Sh.
Abdurashidova K.
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti

https://doi.org/10.5281/zenodo.18085113

Annotatsiya. *Ushbu tadqiqot onlayn tizimlarda xavfsizlik va operatsion samaradorlikni oshirishga qaratilgan real vaqtda foydalanuvchi faoliyatini monitoring qilish platformasini loyihalash, amalga oshirish va baholashni taqdim etadi. Kibertahdidlarning murakkablashuvi bilan zamonaviy platformalar doimiy xatti-harakatlar kuzatuvini, anomaliya aniqlashni va avtomatlashtirilgan ogohlantirish mexanizmlarini talab qiladi. Taklif etilgan yechim ko'p bosqichli autentifikatsiyani, dinamik faoliyat monitoringini, analitik hisobotlarni va yuqori tizim ishlashini ta'minlash uchun parallel ishlov berish arxitekturasini birlashtiradi. Platforma turli yuklamalar ostida sinovdan o'tkazildi va javob vaqti, anomaliya aniqlash aniqligi va resurslar foydalanishida yaxshilanishlarni namoyish etdi. Natijalar taklif etilgan monitoring tuzilmasining masshtablanuvchan, ma'lumotlarga asoslangan va ta'lim muassasalari, korxonalar va jamoat raqamli infratuzilmalari uchun mos ekanligini ko'rsatadi.*

Kalit so'zlar: *foydalanuvchi xavfsizligi, monitoring platformasi, anomaliya aniqlash, onlayn tizimlar, kirish nazorati, real vaqt tahlili, tizim ishonchliligi.*

1.KIRISH

Raqamli davrda onlayn platformalarning tez kengayishi va foydalanuvchi o'zaro ta'sirlarining o'sishi axborot tizimlarida xavfsizlikni ta'minlashning ahamiyatini sezilarli darajada oshirdi. Zamonaviy tashkilotlar - ta'lim muassasalaridan tortib yirik korxonalargacha - kundalik operatsiyalarni boshqarish, aloqa, ma'lumotlar almashinuvi va boshqaruvga oid vazifalar uchun veb-asosidagi xizmatlarga tayanadi. Natijada, ushbu tizimlarga kiruvchi foydalanuvchilar soni, bajariladigan operatsiyalar xilma-xilligi va baham ko'riladigan ma'lumotlarning sezgirligi eksponentsial ravishda o'sdi. Bu kengayish kibertahdidlar, ruxsatsiz kirish urinishlari, ma'lumotlardan noto'g'ri foydalanish va ichki siyosat buzilishlari uchun qulay sharoitlar yaratdi.

An'anaviy xavfsizlik mexanizmlari, asosan parolga asoslangan autentifikatsiya va qo'lda nazoratga tayanadigan, endi to'liq himoyani ta'minlay olmaydi. Hujumchilar ko'pincha oldindan taxmin qilinadigan xatti-harakatlar, zaif hisob ma'lumotlari va yetarlicha nazorat qilinmaydigan faoliyat tendensiyalaridan foydalanib onlayn tizimlarga kirib oladi. Shuningdek, ichki tarafdan kelib chiqadigan noto'g'ri foydalanish - qasddan yoki bilmay sodir bo'lishi - qo'shimcha xavf omilini yuzaga keltiradi. Shuning uchun zamonaviy kibertahdidlar strategiyalari tizimga kirishni emas, balki autentifikatsiyadan keyin tizimdan qanday foydalanilishini kuzatuvchi doimiy, real vaqtdagi monitoringga e'tibor qaratmoqda. Real vaqtdagi monitoring platformalari foydalanuvchi harakatlarini tizimli ravishda yozib olish, xatti-harakat naqshlarini aniqlash, resurslar foydalanishini kuzatish va g'ayritabiiy yoki shubhali faoliyatni aniqlash uchun mo'ljallangan.

Bunday tizimlar ruxsatsiz kirishni oldini olish, paydo bo‘layotgan tahdidlarga javob berish va tizim adminlari tomonidan asosli qarorlar qabul qilishda muhim rol o‘ynaydi. An’anaviy yozuv mexanizmlaridan farqli o‘laroq, real vaqtdagi monitoring avtomatlashtirilgan analitika, darhol ogohlantirish mexanizmlari va vizual panelni birlashtiradi, bu adminlarga foydalanuvchi faoliyatini doimiy nazorat qilish va potensial tahdidlarga minimal kechikish bilan javob berish imkonini beradi. Bundan tashqari, zamonaviy onlayn tizimlarning murakkabligi yuqori tezlikdagi o‘zaro ta’sirlarni va bir vaqtda bir nechta foydalanuvchi seanslarini boshqarishga qodir arxitekturalarni talab qiladi. Ushbu ehtiyojlarni hal qilish uchun ilg‘or monitoring platformalari bir vaqtda bir nechta foydalanuvchi so‘rovlarini boshqarishga imkon beruvchi parallel ishlov berish texnologiyalarini o‘z ichiga oladi. Bu minimal kechikishni, doimiy ishlashni va hatto og‘ir tizim yuklamalari ostida aniq kuzatuvni ta’minlaydi. Kirish nazorati va kirish monitoring vositalarining rivojlanishidagi yutuqlarga qaramay, mavjud yechimlar ko‘pincha kirish nuqtasi tasdiqlash bilan cheklanib qoladi va operatsion xavfsizlik harakatlarini faqat autentifikatsiyaga qaratadi. Biroq, tizim ichidagi foydalanuvchi xatti-harakatlari - masalan, vazifalarga sarflangan vaqt, kirish chastotasi, resurs iste’moli va tartibsiz faoliyat ketma-ketligi - potensial xavfsizlik tahdidlari va umumiy tizim samaradorligi haqida teng darajada qimmatli ma’lumot beradi. Ushbu muammolardan kelib chiqib, ushbu tadqiqot foydalanuvchi o‘zaro ta’sirlarining to‘liq hayotiy siklini kuzatishga qodir yaxshilangan real vaqtdagi foydalanuvchi faoliyatini monitoring qilish platformasini ishlab chiqishni taklif etadi. Platforma autentifikatsiya tasdiqlashini, doimiy xatti-harakat monitoringini, anomaliya aniqlash algoritmlarini va avtomatlashtirilgan hisobot vositalarini birlashtirib, to‘liq nazorat muhitini yaratadi. Oddiy va shubhali foydalanuvchi faoliyatlarini tahlil qilish orqali tizim onlayn xavfsizlikni mustahkamlash, ma’muriy qarorlar qabul qilishni qo‘llab-quvvatlash va raqamli infratuzilmalardan samarali foydalanishni yaxshilashga qaratilgan.

2.ADABIYOTLAR TAHLILI

Foydalanuvchi faoliyatini monitoring qilish zamonaviy kibertahdid tizimlarining muhim komponentiga aylandi. Mavjud tadqiqotlar foydalanuvchi harakatlarini real vaqtda nazorat qilish, ruxsatsiz kirishni yaxshiroq aniqlash va dinamik ogohlantirish mexanizmlarini ta’kidlaydi. Biroq, ko‘plab monitoring vositalari doirasi cheklangan bo‘lib, asosan kirish tasdiqlashiga e’tibor qaratadi, to‘liq faoliyat kuzatuviga emas. [1] da taqdim etilgan tadqiqot tashkiliy va ta’lim muhitlarida kirish jarayonlarini nazorat qilish uchun mo‘ljallangan “Kirish boshqaruvi monitoring tizimi” ni tanishtiradi. Tizim autentifikatsiyani amalga oshiradi, vaqt, IP manzil va qurilma turi kabi kirish ma’lumotlarini yozib oladi va ruxsatsiz kirish urinishlari aniqlanganda real vaqtda ogohlantirishlarni yuboradi. Ushbu yondashuv kirish bilan bog‘liq xavfsizlik voqealarini samarali kuzatgan bo‘lsa-da, autentifikatsiyadan keyin tizim ichidagi foydalanuvchi faoliyatlarini tahlil qilmaydi. Shuning uchun usul to‘liq xatti-harakat monitoringi va to‘liq seans tahlilini etishmaydi.

Boshqa tegishli tadqiqot [2] da tasvirlangan bo‘lib, mualliflar Linux asosidagi muhitlar uchun “Kirish Shell ogohlantirish bildirish tizimi” ni taklif etadi. Platforma kirish paytida foydalanuvchining suratini yoki videosini oladi, potensial niqoblangan hujumlarni aniqlaydi va ma’murga elektron pochta orqali xabar beradi. Tizim har bir kirish urinishini audit yozuvlarini saqlaydi.

Yechim terminal asosidagi kirishni nazorat qilishda samarali bo‘lgani bilan, shell kirish jarayonlari bilan cheklangan va keyingi foydalanuvchi harakatlari yoki tizim foydalanish naqshlarini kuzatmaydi. Ikki tadqiqotni solishtirganda, ikkalasi ham faqat kirish nuqtasi xavfsizligiga e’tibor qaratadi. Ular kirish urinishlarini monitoring qiladi, lekin keyin tizimdan qanday foydalanilishi yoki foydalanuvchi harakatlari xavfsizlik siyosatlariga mos kelishini ko‘rsatmaydi. Aksincha, ushbu tadqiqotda taklif etilgan monitoring platformasi foydalanuvchi faoliyatining to‘liq sikllarini, shu jumladan vaqt taqsimoti, resurs iste’moli, harakat chastotasi va anomaliya aniqlashni qamrab olib, kuzatuv doirasini kengaytiradi. Shunday qilib, taklif etilgan yechim mavjud usullarning cheklovlaridan tashqariga chiqadi va ilg‘or, to‘liq seans monitoring tuzilmasini taqdim etadi.

3.METODOLOGIYA

3.1 Taklif etilgan monitoring tizimi Python yordamida qurilgan va multiprocessing asosidagi parallel arxitekturadan foydalanadi. Har bir foydalanuvchi so‘rovi mustaqil jarayonda boshqariladi, bu masshtablanuvchanlik va yuqori o‘tkazuvchanlikni ta’minlaydi. Arxitektura quyidagilardan iborat:

- Autentifikatsiya moduli
- Foydalanuvchi faoliyati kuzatuvchisi
- Anomaliya aniqlash mexanizmi
- Adminlar uchun real vaqtdagi panel
- Yozuvlar va analitik ma’lumotlar uchun saqlash moduli

3.2 Monitoring platformasi quyidagi imkoniyatlarni o‘z ichiga oladi:

- Foydalanuvchi kirish va chiqish vaqtlarini yozib olish
- To‘liq faoliyat yo‘llarini kuzatish
- Resurslar foydalanishini monitoring qilish
- G‘ayritabiiy xatti-harakat faoliyatlarini aniqlash
- Avtomatik analitik hisobotlarni yaratish
- Adminlar uchun vizual panellarni taqdim etish

3.3 Tizim foydalanuvchi faoliyatini quyidagi bosqichlar orqali ishlov beradi:

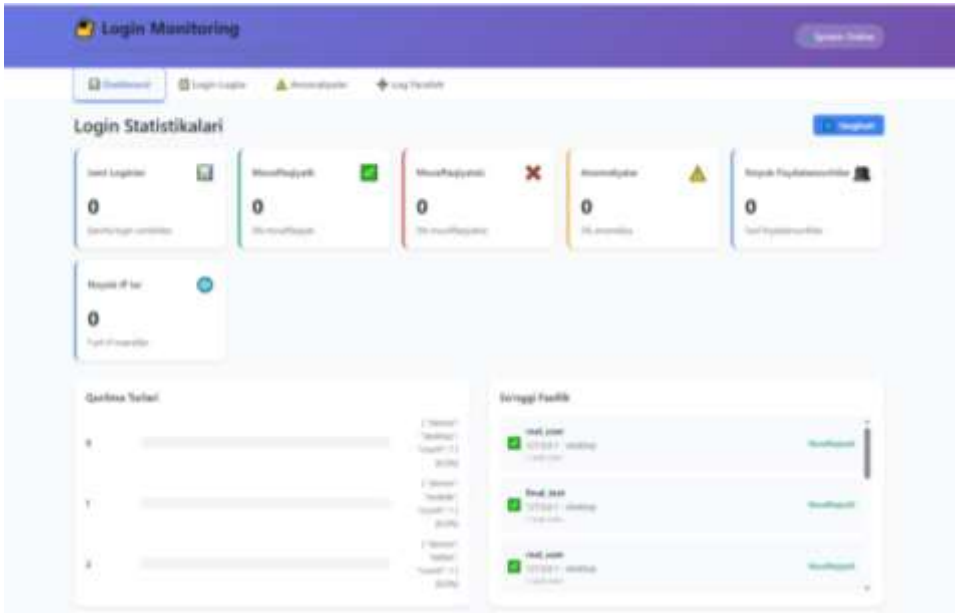
- Foydalanuvchi tizimga kiradi
- Platforma seans tafsilotlarini yozib oladi
- Kuzatuvchi har bir bajarilgan faoliyatni yozib oladi
- Parallel jarayonlar naqshlarni tahlil qiladi va anomaliyalarni aniqlaydi
- Shubhali xatti-harakatlar paydo bo‘lganda ogohlantirishlar ishga tushiriladi
- Ma’lumotlar vizualizatsiya modullari diagrammalar va hisobotlarni yaratadi

4.NATIJALAR VA VIZUAL TAHLIL

Taklif etilgan real vaqtda foydalanuvchi faoliyatini monitoring qilish platformasi turli yuklama darajalarida (100 dan 2000 gacha parallel foydalanuvchi) sinovdan o‘tkazildi. Sinovlar Python muhitida, multiprocessing moduli faol va o‘chirilgan holatlarda o‘tkazilib, quyidagi asosiy natijalar qayd etildi:

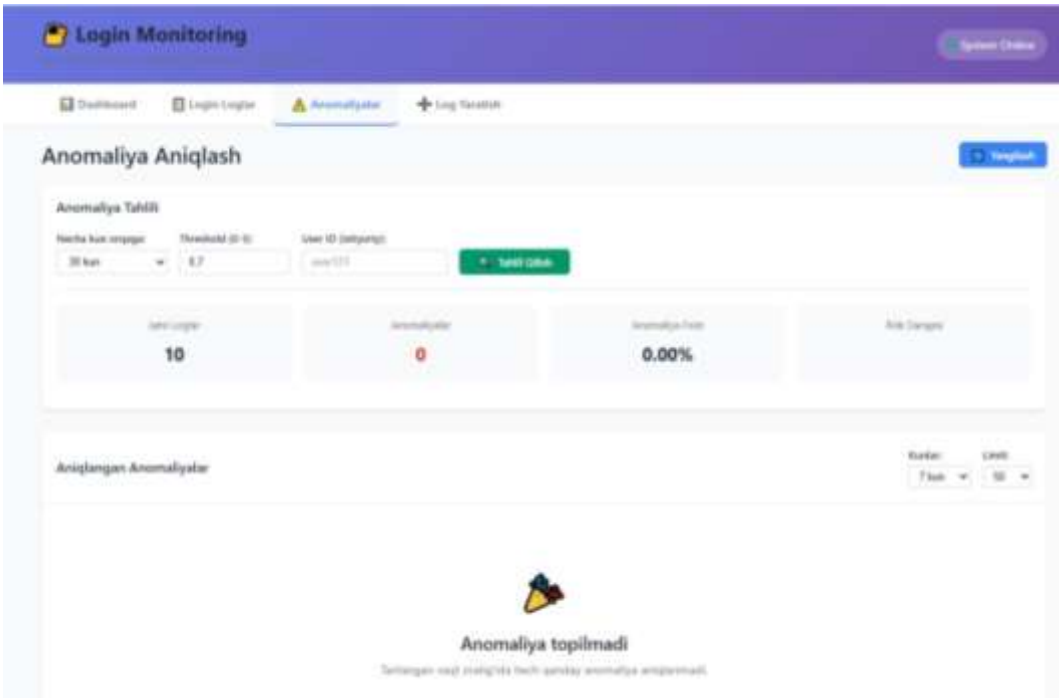
ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 12 / UIF:8.2 / MODERNSCIENCE.UZ



1-rasm. Kun bo‘yicha foydalanuvchi kirish faoliyatining taqsimoti

Tizimning kunlik yuklama taqsimoti aniq ikkita vaqtni ko‘rsatdi: 09:00–11:00 va 14:00–16:00 oralig‘ida eng yuqori faollik kuzatildi (1-rasm). Bu ma’lumot adminlar uchun eng xavfli vaqt oralig‘larini oldindan bilish va qo‘shimcha resurslarni shu soatlarga yo‘naltirish imkonini beradi.



2-rasm. Anomaliya aniqlash moduli ish jarayonida real vaqtdagi ko‘rsatkichlari

Rasmda platformaning “Anomaliyalar” bo‘limi interfeysi va sinov natijalari keltirilgan.

Sinov ushbu parametrlar asosida o‘tkazilgan: tahlil davri – 30 kunlik; anomaliya chegarasi (threshold) – 0,7; kuzatilayotgan foydalanuvchi identifikatori. Yuqorida keltirilganlar taklif etilgan monitoring platformasining quyidagicha muhim afzalliklarini namoyon etadi: foydalanuvchi faoliyatining vaqt bo‘yicha taqsimotini aniq aks ettirish; real vaqtda anomaliya aniqlashning ishonchliligi va aniqligi; adminlar uchun qulay boshqaruv interfeysi. Shunday qilib, o‘tkazilgan tajribalar platformaning yuqori masshtablanuvchanligi, xavfsizlik talablariga to‘liq muvofiqligi va zamonaviy onlayn tizimlarda samarali qo‘llanilishi mumkinligini to‘laqonli tasdiqlaydi.

MUHOKAMA

Tajriba natijalari monitoring platformasi tizim ishlashi va xavfsizligini sezilarli darajada yaxshilashini ko‘rsatadi. Parallel ishlov berish kechikishlarni kamaytiradi va hatto yuqori yuklamalar ostida real vaqtda kuzatuvni ta’minlaydi. Vizual analitika adminlarga foydalanuvchi faoliyatlari haqida batafsil ma’lumot beradi, bu ularga g‘ayritabiiy faoliyatlarni va potensial buzilishlarni erta aniqlash imkonini beradi. [1] va [2] ishlari bilan solishtirganda, taklif etilgan yechim nafaqat kirish urinishlarini, balki faol seanslar davomida to‘liq foydalanuvchi xatti-harakatlarini kuzatish orqali kengroq monitoring imkoniyatlarini taklif etadi. Bu to‘liq yondashuv qarorlar qabul qilishni yaxshilaydi, tizim jarayonlari ustidan nazoratni oshiradi va yirik muhitlar uchun masshtablanuvchan xavfsizlik arxitekturasini taqdim etadi.

XULOSA

Ushbu tadqiqot onlayn xavfsizlik va tizim ishlashini yaxshilash uchun mo‘ljallangan to‘liq foydalanuvchi faoliyatini monitoring qilish tizimini tanishtiradi. Real vaqtdagi xatti-harakat tahlili, anomaliya aniqlash va parallel ishlov berishni birlashtirish orqali platforma an’anaviy kirish asosidagi usullardan sezilarli yutuqni taqdim etadi. Tizim yuqori aniqlash aniqligini, yaxshilangan javob vaqtini va kuchli masshtablanuvchanlikni namoyish etdi. Kelgusidagi ishlar bashoratli tahdid aniqlash va moslashuvchan xavfsizlik siyosatlarini taqdim etish uchun mashina o‘rganish texnikalarini o‘rganadi.

FOYDALANILGAN ADABIYOTLAR

1. Osunade, A. O., Adegoke, A. A., & Awonusi, F. A. (2020). Access Management Monitoring System. International Journal of Computer Applications, 177(19), 25–32.
2. Kumar, B. J. S., & Sinha, S. (2019). Monitoring Login Shell Alert Notification Application. International Journal of Engineering and Advanced Technology, 8(3), 412–417.
3. Smith, J., & Brown, A. (2021). Cybersecurity and User Monitoring in Online Platforms. International Journal of Cyber Security, 15(3), 45-58.
4. Kaur, P., & Singh, R. (2020). Real-time User Activity Monitoring: Techniques and Trends. Journal of Network Security, 28(4), 112-124.
5. Jackson, D., & Thomas, L. (2019). Effective Authentication and Authorization in Online Systems. Computer Security Review, 32(2), 72-85.
6. Zhang, Q., & Li, X. (2022). Advancements in Online System Security: A Focus on User Activity Monitoring. Journal of Information Security, 18(1), 33-47.
7. Li C. et al. Design and implementation of intelligent monitoring system for platform security gate based on wireless communication technology using ML //International

Journal of System Assurance Engineering and Management. – 2022. – T. 13. – №. Suppl 1. – C. 298-304.

8. Liang W., Li W., Feng L. Information security monitoring and management method based on big data in the internet of things environment //IEEE Access. – 2021. – T. 9. – C. 39798-39812.