KO‘P SATHLI XAVFSIZLIK MODELLARI.

Boltayev Ulug`bek Zafarovich
Muhhammad Al-Xoraxmiy nomidagi Toshkent Axborod Texnologiyalari Universiteti Dasturiy injiniringi fakulteti talabasi

Annotatsiya: *Ma'lumotlar xavfsizligi, ruxsatsiz foydalanish, ma'lumotlarni o'zgartirish yoki tarqatish kabi faoliyatlarni oldini olishga qaratilgan harakatlarni o'z ichiga oladi. Bu faqat ma'lumotlarni ushlash sifatida emas, balki yaxlitlik, mavjudlik va maxfiylik kabi muhim jihatlarning buzilishining oldini olish sifatida ham qaralishi kerak. Ushbu uchta asosiy elementdagi har qanday zaiflik ma'lumotlar xavfsizligini buzilish sifatida baholanadi. Ushbu tadqiqotda ko'p darajali kirish nazorati usuli ishlab chiqish maqsadida, yaxshilangan Bell-LaPadula xavfsizlik modeli tarqatilgan tizimlarga qabul qilingan va shuning uchun ma'lumotlar xavfsizligidagi uchta asosiy elementdan biri bo'lgan maxfiylik xususiyatining qanday ta'minlangani ko'rsatilgan. Tadqiqotda taklif qilingan model haqiqiy hayotdan olingan ma'lumotlar klasteriga tatbiq etilgan. Taklif qilingan modelning samaradorligi Rolga Asoslangan Kirish Nazorati va An'anaviy Kirish Nazorati modellari bilan solishtirilgan. Olingan natijalar taqqoslanganda, taklif qilingan model yordamida ma'lumotlar foydalanuvchilar tomonidan yanada xavfsiz va tezkor tarzda taqdim etilgan.*

Kalit so'zlar: *kirish nazorati modeli; Bell-LaPadula modeli; tarqatilgan ma'lumotlar bazalari; rolga asoslangan kirish nazorati*

KIRISH

Ma'lumotlar xavfsizligi, ruxsatsiz ma'lumotlarga kirish, ma'lumotlarni ishlatish, o'zgartirish yoki yo'q qilish kabi harakatlarning oldini olish sifatida ta'riflanadi va u maxfiylik, yaxlitlik va mavjudlik kabi asosiy elementlardan iborat. Maxfiylik, ma'lumotlarni ruxsatsiz shaxslar tomonidan kirish va o'qishdan himoya qilish bilan bog'liq. Yaxlitlik, ma'lumotlarni ruxsatsiz shaxslar tomonidan o'zgartirishdan saqlanish va uning asl holatini himoya qilish bilan bog'liq. Mavjudlik, ma'lumotlar faqat ruxsat berilgan shaxslar tomonidan kirish va ishlatilishi mumkin bo'lgan holatdir. Umuman olganda, ko'plab tahdidlar xavfsizlik zaifliklaridan foydalanib hujumga aylanadi va bunday hujumlarning operatsion tizimga zarar yetkazishini oldini olish uchun yuqorida sanab o'tilgan xavfsizlik elementlarini ta'minlash juda muhimdir. Shu sababli, tizim qanchalik xavfsiz himoyalangan bo'lsa ham, hujumlarga olib kelishi mumkin bo'lgan elementlarni aniqlash va zarur choralarni ko'rish muhimdir.

Hozirgacha, o'zlarining qo'llanilish sohalariga xos bo'lgan xavfsizlik modellari ishlab chiqilganini ko'rdik. Biroq, an'anaviy xavfsizlik modellari tez sur'atlar bilan ko'payayotgan

va murakkablashayotgan tizimlar talablariga javob bera olmaydi. Bunday holatga olib keladigan omillarni ko'rib chiqilganda, sezgir ma'lumotlar saqlanadigan muhitlarda juda qat'iy nazorat va tekshirishlarni o'tkazish majburiyligi muhim rol o'ynaydi, ma'lumotlar oqimini tekshirish kafolatlanmaydi, ma'lumotlar xavfsiz va tezkor tarzda bo'lishilmaydi va qo'llanilish sohasida sezilarli darajada moslashuvchanlik yo'qoladi.

Ushbu tadqiqotda kirishda moslashuvchanlikni yo'qotish va foydalanuvchilar o'rtasida resurslarni taqsimlashning kamayishi kabi muammolar muhokama qilinadi, bu haqiqiy tizimlar qo'llanilishida eng keng tarqalgan muammolar hisoblanadi. Mavjud kirish nazorati modellari ichida juda moslashuvchan tasdiqlash mexanizmining yo'qligi resurslarning mavjudligi va ish vaqtining samaradorligini pasaytirishi mumkin va ularning o'sishini cheklaydi . Ushbu tadqiqot, Bell-LaPadula modelidan taklif qilingan xavfsizlik siyosatlariga qo'shimcha ravishda yangi xavfsizlik siyosatlarini aniqlaydi. Taklif qilingan model bilan maqsad, yangi aniqlangan siyosatlar yordamida resurslardan foydalanishni nazoratli va xavfsiz tarzda oshirishdir.

Tarqatilgan tizimlar — bu turli joylarda saqlanayotgan, ammo kompyuter tarmog'i orqali bir-biri bilan bog'langan turli ma'lumotlar bazalari. Ko'plab yirik tashkilotlar va muassasalar ushbu tizimlarni afzal ko'radi.

Bizning tadqiqotimizda, haqiqiy tizimlar qo'llanilishida an'anaviy xavfsizlik modellari zaif tomonlarini hisobga olgan holda yanada funktsional va mos kirish nazorati modeli ishlab chiqilgan. Tadqiqotimizning asosiy hissasi tarqatilgan ma'lumotlar bazalari tizimlari tomonidan qabul qilinishi mumkin bo'lgan va Bell-LaPadula modelidan taklif qilingan xavfsizlik siyosatlariga qo'shimcha ravishda yangi va ko'p darajali kirish nazorati protseduralarini aniqlash orqali ishlab chiqilgan modeldir. Ayniqsa, tarqatilgan ma'lumotlar bazalari tizimlariga oid bo'lib, maqsad taklif qilingan modelni haqiqiy tizimlarga yanada moslashuvchan va samarali tarzda qabul qilish va ma'lumotlarga nisbatan maxfiylik talablarini ta'minlashdir.

Umumiy Malumotlar Ma'lumotlar bazalari va ayniqsa tarqatilgan ma'lumotlar bazalari bilan bog'liq xavfsizlik muammolari turli tadqiqotlarda baholangan . Ba'zi tadqiqotlarda, ayniqsa, har bir tizim turiga alohida e'tibor qaratilib, xavfsizlik nuqtai nazaridan har bir tizimning zaif tomonlari o'rganilgan . Ushbu tadqiqotlarda tarqatilgan ma'lumotlar bazalari tizimlari ko'p darajali kirish nazorati, maxfiylik, ishonchlilik, yaxlitlik va tiklash kabi turli xavfsizlik muammolariga duch kelishi ta'kidlangan.

Naeem va boshqalar umumiy bo'lishni oshirish maqsadida jamoa asosidagi kirish nazorati (TMAC) modelidan va kengaytirilgan rolga asoslangan kirish (RBAC) modelidan foydalanganlar. Bu yondashuvlar tarqatilgan tizimlar uchun xavfsizlikni ta'minlashda muhim ahamiyatga ega bo'lib, ruxsat berish mexanizmlarini yanada samarali qilishga yordam beradi.

Yana boshqa tadqiqotlarda, xavfsizlik masalalarini bartaraf etish uchun yangi yondashuvlar va texnikalar taklif qilingan, bu esa tarqatilgan ma'lumotlar bazalarining xavfsizligini oshirishga qaratilgan.

Umuman olganda, bu tadqiqotlar tarqatilgan tizimlar uchun xavfsizlikni yaxshilashda ko'plab imkoniyatlarni ochib beradi va kelajakda qo'llaniladigan modellarning samaradorligini oshirishga qaratilgan yangi yondashuvlarni ishlab chiqishga yordam beradi

Xavfsizlik va Maxfiylikni Ta'minlash Naeem va boshqalar tomonidan o'tkazilgan tadqiqotda, kirish nazorati va maxfiylik masalalari bo'yicha ikkita model, ya'ni jamoa asosidagi kirish nazorati (TMAC) va rolga asoslangan kirish (RBAC) modellari o'rtasida taqqoslashlar amalga oshirilgan. Ushbu tadqiqotda maxfiylik, bo'lishish va qoidalar asosidagi o'lchovlar ko'rib chiqilib, natijalar baholangan.

Boshqa bir tadqiqotda, rolga asoslangan kirish nazorati (RBAC) xavfsizlik modeliga oid maxfiylik va xavfsizlik talablarini ta'minlash muhokama qilingan. Xavfsiz sog'liq xizmatlarini qo'llab-quvvatlash maqsadida sog'liq xizmatlari integratsiya platformasi (u-HCSIP) ishlab chiqilgan va bu dizaynda RBAC asosidagi xavfsizlik modeli qo'llanilgan. Ish jarayonini tahlil qilish orqali taklif qilingan RBAC asosidagi u-HCSIP ning amaliyoti tasdiqlangan.

Hozirgi tarqatilgan boshqaruv tizimlarida (DCS), eng kam imtiyozlar prinsipiga amal qilish qiyin, chunki kirish nazorati qoidalari ko'p xilma-xil tizimlar o'rtasida taqsimlangan. Ba'zi tadqiqotlarda, tarqatilgan tizimlarda yanada to'liq va boshqarish oson kirish nazorati modeliga o'tishdagi asosiy qiyinchiliklar tilga olingan. Bir tadqiqotda, har bir kirishni eng kam imtiyozlar prinsipiga muvofiq siyosatlarga mos kelishi uchun sanoat boshqaruv tizimi (ICS) jamoasi tomonidan moslashtirilishi mumkin bo'lgan kirish nazorati arxitekturasi taqdim etilgan . Ushbu taklif qilingan arxitektura markaziy siyosatni boshqarish va har bir bog'langan maydon qurilmasini himoya qilish maqsadida ishlab chiqilgan.

Bertolissi va Fernandez tarqatilgan muhitlarning maxsus talablarini hisobga olgan holda kirish nazorati dizayni uchun metamodelni aniqladilar. Tadqiqotda, bir nechta joylardan iborat tarqatilgan tizimning har bir a'zosi tomonidan belgilangan lokal siyosatlarni hisobga olgan holda kirish nazorati siyosatlarini amalga oshirish uchun bir ramka taklif qilingan.

Dasgupta va boshqalar xodimlar o'rtasidagi o'zaro munosabatlar va ularning tashkilot ichidagi rollari asosida kirish nazorati grafikasini tashkil etdilar. Keyinchalik, foydalanuvchining kirish so'rovini ma'lum bir vaqtda tasdiqlash uchun bir qator tasdiqlash mexanizmlari ishlab chiqildi. Taklif qilingan ko'p foydalanuvchi tasdiqlash strategiyasi ikki empirik ma'lumotlar klasteri bilan baholandi va natijalar turli institut va muhit sharoitida foydalanuvchi kirishi uchun takrorlanmaydigan tasdiqlovchilarni tanlash imkoniyatini ko'rsatdi.

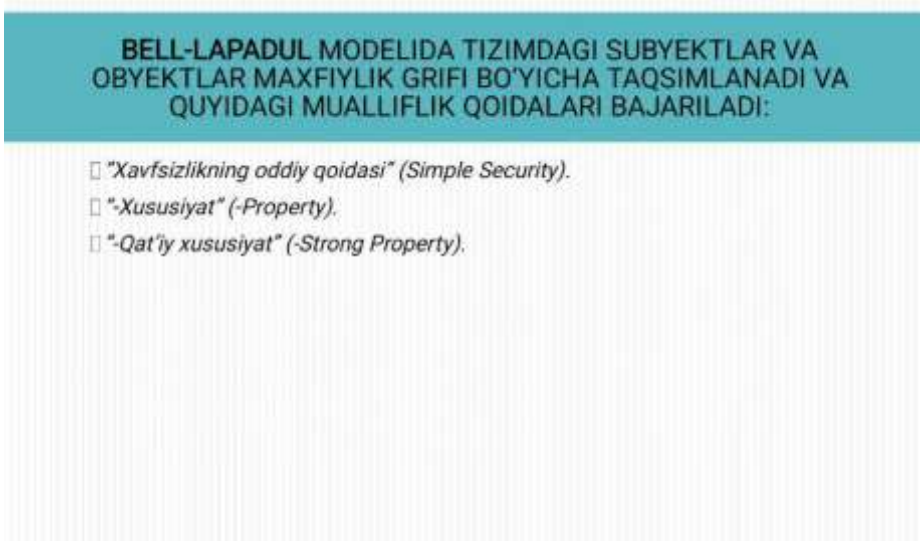
Bulut muhitida intruderlarni ular uylariga kirmasliklari uchun to'sqinlik qiladigan asalari xulqini hisobga olgan holda kirish nazorati mexanizmi ishlab chiqildi . Tadqiqotda, Bell-LaPadula modelidan ilhomlanib bulut xavfsizligi uchun yangi atributga asoslangan kirish nazorati taklif qilingan

Tarqatilgan ma'lumotlar bazasi tizimlarining asosiy afzalliklaridan biri shundaki, ular ma'lumotlarni bir joyda saqlashga muhtoj emaslar, bu esa ma'lumotlar xavfsizligini oshiradi va ishonchliligini ta'minlaydi. Har bir server mustaqil ishlasa ham, ular birgalikda ishlash orqali umumiy tizimga integratsiyalashadi.

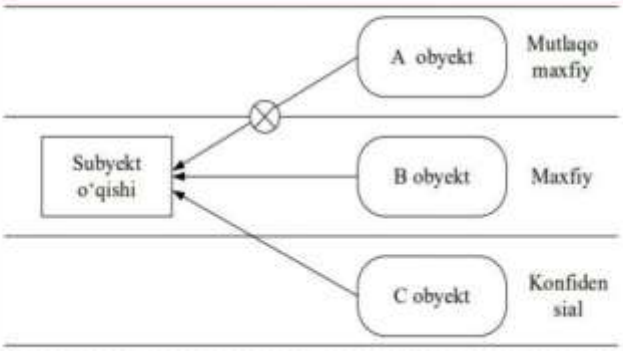
Tarqatilgan ma'lumotlar bazalari bilan bog'liq xavfsizlik masalalari, masalan, ma'lumotlarni ruxsatsiz kirishdan himoya qilish va ma'lumotlarning yaxlitligini saqlash, alohida e'tiborni talab qiladi. Bunday tizimlar uchun xavfsizlik protokollarini ishlab chiqish va amalga oshirish juda muhimdir, chunki har bir serverda ma'lumotlar alohida saqlanadi va bu ma'lumotlarning himoyalanishi alohida nazoratni talab qiladi.

Bell-Lapuda Modeli Subyektlar foydalanuvchilar va tizimlarni xavfsizlik nuqtai nazaridan belgilaydi. Ushbu tadqiqotda subyektlar foydalanuvchi yoki aktyor sifatida ta'riflangan. Ob'ektlar esa o'qish, yozish, o'chirish va yangilash kabi jarayonlar amalga oshiriladigan barcha turdagi manba ma'lumotlarini belgilaydi. Har bir ob'ekt va aktyor uchun aniq xavfsizlik darajasi belgilangan. Aktyor belgilangan xavfsizlik darajasida mavjud bo'lgan ob'ektlar ustida belgilangan jarayonlarni amalga oshirishi mumkin.

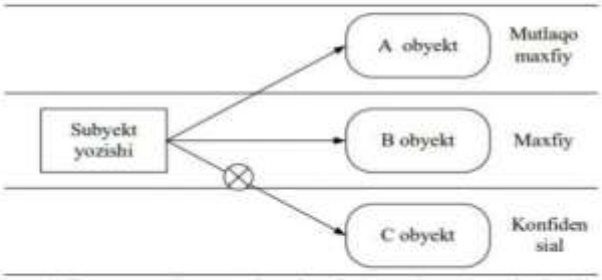
Bir nechta xavfsizlik darajasi belgilangan model turli operatsion tizimlarda maxfiylikni ta'minlash uchun ishlatilishi mumkin, shuningdek, xavfsizlik bilan bog'liq davlat idoralarida va harbiy qo'llanmalarda kirish nazoratini ta'minlash uchun zarur bo'lgan majburiy kirish modeli sifatida ham ko'rsatiladi. Modelda aktivlar ikki turdagi klasslardan iborat.



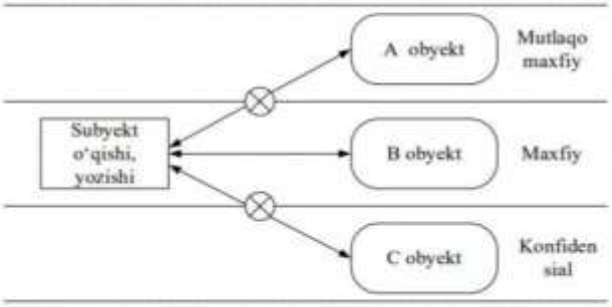
“SIMPLE SECURITY” XUSUSIYATI UCHUN AXBOROT OQIMLARI SXEMASI



“-PROPERTY” XUSUSIYATI UCHUN AXBOROT OQIMLARI SXEMASI



“-STRONG-PROPERTY” XUSUSIYATI UCHUN AXBOROT OQIMLARI SXEMASI



Tajribaviy Tadqiqot Ushbu tadqiqotda, sog'liq va adliya xizmatlarini taqdim etuvchi davlat muassasalaridan olingan haqiqiy ma'lumotlar to'plamlari ishlatilgan bo'lib, taklif qilingan kirish nazorati modelining samaradorligi va boshqa usullar natijalari har bir ma'lumotlar to'plamidan olingan natijalar asosida baholandi. Tadqiqotda ishlatilgan ikki xil sektordan olingan ma'lumotlar to'plamlari oldindan qayta ishlangan va har bir foydalanuvchi hamda ob'ekt xavfsizlik parametrlari bo'yicha tasniflangan. Tasniflash jarayoni bizneslarning haqiqiy tasniflash mezonlariga asoslangan. Sog'liq sektoridan olingan ma'lumotlar to'plami 430 foydalanuvchi va 55,300 ob'ektdan iborat bo'lsa, adliya sektoridan olingan ma'lumotlar to'plami 292 foydalanuvchi va 72,988 ob'ektdan iborat. Ushbu ma'lumotlar to'plamlari "Sog'liq Ma'lumotlar To'plami" va "Adliya Ma'lumotlar To'plami" deb ataladi.

Tajribaviy Tahlil Taklif qilingan model bilan birga, boshqa kirish nazorati modellari ham haqiqiy tarqatilgan tizimni taqdim etuvchi platformada sinovdan o'tkazildi va barcha modellarga uchta ma'lumotlar to'plamiga alohida amal qilindi. Har bir usulning samaradorlik darajalari, har bir ma'lumotlar to'plamiga tatbiq etilgan modellar uchun olingan kirish darajasi natijalari (o'qish, yozish, o'qish va yozish va boshqalar) sektordan olingan ma'lumotlar to'plami kirish darajasi natijalari bilan taqqoslanib tahlil qilindi. Ma'lumotlar to'plamlariga tatbiq etilgan usullar samaradorligini baholash, har bir usulning kirish darajasining aniqligi va kirish darajasini aniqlash foizlariga asoslangan.

Bu tahlil jarayoni va natijalar, taklif qilingan modelning samaradorligini va uni amaliyotda qo'llash imkoniyatlarini ko'rsatadi, shuningdek, boshqa kirish nazorati modellari bilan taqqoslanganda qanday afzalliklarni taqdim etishini baholashga imkon beradi.

Xulosa Ushbu tadqiqotda taklif qilingan yaxshilangan xavfsizlik modeli, tarqatilgan ma'lumotlar bazalarida ma'lumotlarning maxfiyligini ta'minlashga qaratilgan. Tadqiqot davomida haqiqiy ma'lumotlar to'plamlaridan foydalanilib, xavfsizlik siyosatlari analizi amalga oshirildi. Tarqatilgan tizimlarda foydalanuvchilar o'rtasida ma'lumotlarni xavfsiz va tezkor tarzda bo'lishish imkoniyati yaratildi, bu esa dasturlarda moslashuvchanlikni oshirdi.

Biroq, tadqiqotning zaif jihatlari ham mavjud bo'lib, xavfsizlik modeli asosan maxfiylikka qaratilgan, bu esa mavjudlik va yaxlitlik kabi boshqa xavfsizlik jihatlarini orqa planga olib chiqdi. Foydalanuvchilarning xavfsizlik darajalarini nazorat qilish va ruxsatlarni belgilash orqali ma'lumotlarga kirishni qat'iy boshqarish maqsad qilingan.

Kelgusidagi tadqiqotlar, mavjudlik va yaxlitlik jihatlarini ham o'rganish, shuningdek, boshqa xavfsizlik modellari tarqatilgan ma'lumotlar bazalariga qanday tatbiq etilishi masalalarini ko'rib chiqishga qaratilishi kutilmoqda. Bu jarayonlar, umumiy xavfsizlikni ta'minlashga va tarqatilgan tizimlarning samaradorligini oshirishga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR:

1.Andress, J. (2011). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Elsevier Inc., USA.

2.Nemati, H. (2007). *Information Security and Ethics: Concepts, Methodologies, Tools and Applications*. Information Science Reference, USA. https://doi.org/10.4018/978-1-59904-937-3

3.Whitman, M. E. & Mattord, H. J. (2012). *Principles Of Information Security*. Course Technology, Cengage Learning, USA.

4. Vijayalakshmi, K. & Javalakshmi, V. (2021). *Shared Access Control Models for Big Data: A Perspective Study and Analysis*. Advances in Intelligent Systems and Computing book series (AISC), 1272, 397-410. https://doi.org/10.1007/978-981-15-8443-5_33

5. Ghamdi, H. F. & Than, T. (2020). *Information security governance challenges and critical success factors: Systematic review*. Elsevier Computers & Security, 99, 1-39. https://doi.org/10.1016/j.cose.2020.102030

6. Gunjan, B., Vijayalakshmi, A., Jaideep, V., & Shamik, S. (2019). *Deploying ABAC Policies Using RBAC Systems*. Journal of Computer Security, 27(4), 483-506. https://doi.org/10.3233/JCS-191315

7. https://link.springer.com