HESH FUNKSIYALARIDA SUN'IY INTELLEKTGA ASOSLANGAN TO'QNASHUVNI ANIQLASH USULLARI

Jumanova Zuxra Xolbayevna
"Cyber University" davlat universiteti Kiberxavfsizlik kafedrasi kata o'qituvchisi
E-mail: zuxrajumanova10@gmail.com
Samarov Sherzod Khamrayevich
University of Management and Future Technologies. Kompyuter tizimlari va dasturiy taminoti magistranti.
E-mail: samarovsherzod78@gmail.com

Annotatsiya. Ushbu maqola sun'iy intellekt (AI) asosidagi to'qnashuvni aniqlash usullarining xesh funksiyalardagi samaradorligini baholaydi, bu esa ushbu funktsiyalarning kriptografik ilovalarda, xususan, sog'liqni saqlash ma'lumotlari xavfsizligida mavjud bo'lgan zaifliklari tufayli juda muhim ahamiyatga ega. Tadqiqot mavjud xesh funksiyasi algoritmlarini tizimli ravishda ko'rib chiqadi, ularning to'qnashuv chastotalarini tahlil qiladi va turli AI texnikalarini ishlash va aniqlash aniqligi nuqtai nazaridan taqqoslaydi. Ushbu tadqiqotning natijalari nazariy hissalardan tashqariga chiqadi, bu esa xesh funksiyasini optimallashtirishga AI asosidagi strategiyalarni integratsiyalash sog'liqni saqlash IT tizimlarining umumiy xavfsizlik tizimini mustahkamlashi, shu bilan ma'lumotlarning buzilishi bilan bog'liq xavflarni kamaytirishi va tartibga solish standartlariga muvofiqligini ta'minlashi mumkinligini ko'rsatadi. Ushbu tadqiqot kriptografiyada AI metodologiyalarini keng ko'lamli amalga oshirish bo'yicha kelajakdagi tadqiqotlar uchun zamin yaratadi va sog'liqni saqlash sohasidagi xavfsizlik landshaftini mustahkamlash uchun ularni qo'llashni qo'llab-quvvatlaydi.

Kalit so'zlar: Sun'iy intellekt, Xesh funksiyalari, To'qnashuvni aniqlash, Kriptografik xavfsizlik, Mashinada o'rganish, Ma'lumotlar yaxlitligi, Axborot xavfsizligi, Xesh funksiyasini optimallashtirish, Raqamli sog'liqni saqlash tizimlari.

Аннотация. В данной статье оценивается эффективность методов обнаружения коллизий на основе искусственного интеллекта (ИИ) для хеш-функций, что имеет большое значение из-за уязвимостей этих функций в криптографических приложениях, особенно в сфере безопасности данных в здравоохранении. В исследовании систематически рассматриваются существующие алгоритмы хеш-функций, анализируется частота их коллизий и сравниваются различные методы ИИ с точки зрения производительности и точности обнаружения. Результаты этого исследования выходят за рамки

ISSN 3030-3907

теоретических выводов, демонстрируя, что интеграция стратегий на основе ИИ в оптимизацию хеш-функций может укрепить общую систему безопасности ИТ-систем здравоохранения, тем самым снижая риски, связанные с утечками данных, и обеспечивая соответствие нормативным стандартам. Это исследование открывает путь для будущих исследований по широкомасштабному внедрению методологий ИИ в криптографию и поддерживает их применение для укрепления системы безопасности в здравоохранении.

Ключевые слова: Искусственный интеллект, Хеш-функции, Обнаружение коллизий, Криптографическая безопасность, Машинное обучение, Целостность данных, Информационная безопасность, Оптимизация хеш-функций, Цифровые системы здравоохранения.

Abstract. This paper evaluates the effectiveness of artificial intelligence (AI)-based collision detection methods on hash functions, which is of great importance due to the vulnerabilities these functions have in cryptographic applications, particularly in healthcare data security. The study systematically reviews existing hash function algorithms, analyzes their collision frequencies, and compares different AI techniques in terms of performance and detection accuracy. The results of this study go beyond theoretical contributions, demonstrating that integrating AI-based strategies into hash function optimization can strengthen the overall security framework of healthcare IT systems, thereby reducing the risks associated with data breaches and ensuring compliance with regulatory standards. This study paves the way for future research on the large-scale implementation of AI methodologies in cryptography and supports their application to strengthen the healthcare security landscape.

Keywords: Artificial Intelligence, Hash Functions, Collision Detection, Cryptographic Security, Machine Learning, Data Integrity, Information Security, Hash Function Optimization, Digital Health Systems.

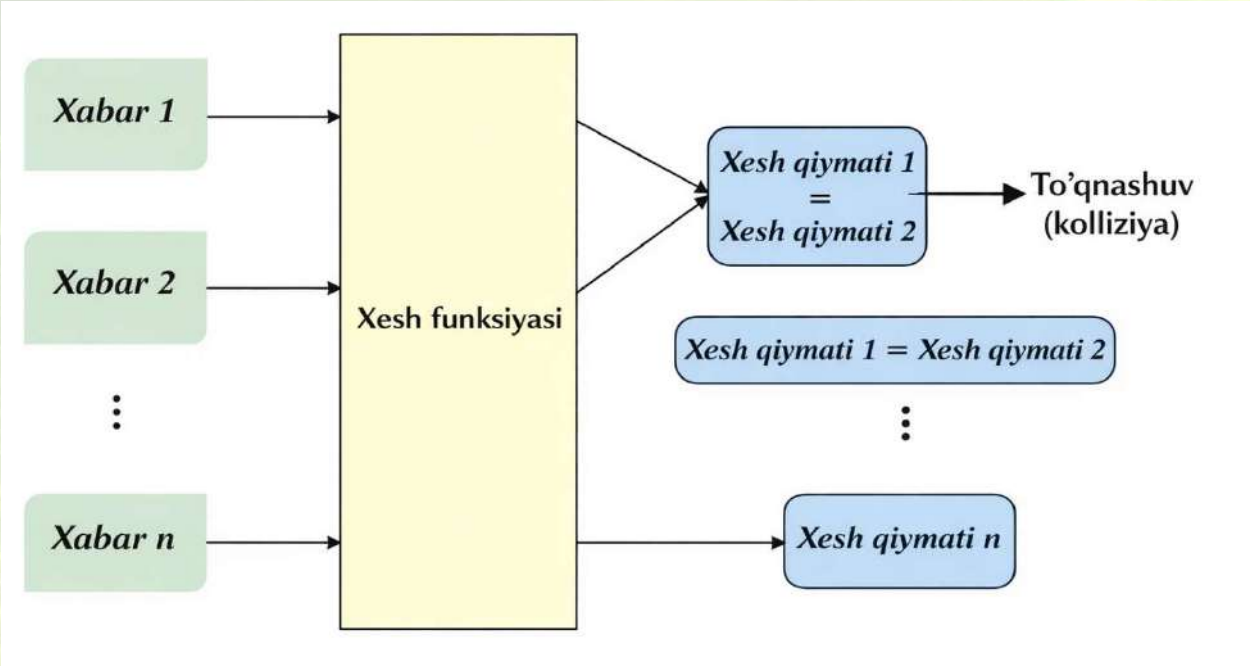
KIRISH

Ma’lumotlar yaxlitligi va xavfsizligi eng muhim bo‘lgan davrda raqamli platformalarning tobora ko‘proq qo‘llanilishi maxfiy ma’lumotlarni himoya qilishda asosiy komponentlar bo‘lib xizmat qiladigan kriptografik xesh funksiyalarining ahamiyatini oshirdi. Ushbu xesh funksiyalari o‘zgaruvchan o‘lchamdagi kirishlardan ma’lumotlarning izchilligini ta’minlash bilan birga maxfiylikni saqlash uchun belgilangan o‘lchamdagi chiqishni yaratish uchun mo‘ljallangan. Biroq, an’anaviy xesh algoritmlarining zaifligi, ayniqsa murakkab kiberhujumlarga duch kelganda, axborot xavfsizligi tizimlariga jiddiy tahdid soladi [1]. Bu zaifliklar ko‘pincha xesh to‘qnashuvlari bilan yakunlanadi, ular turli

ISSN 3030-3907

kirishlar bir xil xesh qiymatlarini berganda yuzaga keladi - bu anomaliya turli raqamli ilovalarda ma’lumotlarning yaxlitligini buzishi mumkin. Kriptografik amaliyotlardagi yutuqlarga qaramay, mavjud usullar ko‘pincha to‘qnashuvni aniqlashni yetarli darajada hal qilmaydi, bu esa innovatsion yechimlarni talab qiladigan muhim bo‘shliqni yaratadi. Ushbu tadqiqot xesh funksiyalarida to‘qnashuvni aniqlashni kuchaytirish uchun AI asosidagi usullarni o‘rganishga, shu bilan mavjud kriptografik tizimlarning mustahkamligini oshirishga qaratilgan [2]. Asosiy maqsadlar mavjud xesh algoritmlarini tahlil qilish, ularning to‘qnashuvlarga moyilligini baholash va to‘qnashuv xavflarini aniqlash va kamaytirishda ularning samaradorligi va samaradorligini aniqlash uchun turli AI texnikalarini taqqoslashga qaratilgan [3]. Sun’iy intellektni to‘qnashuvlarni aniqlash strategiyalariga integratsiya qilish orqali ushbu tadqiqot nafaqat mojarolarni minimallashtiradigan, balki ma’lumotlarni tekshirish jarayonini soddalashtiradigan asos yaratishga intiladi [4]. Ushbu tadqiqotning ahamiyati nazariy natijalardan tashqariga chiqadi, chunki u sog’liqni saqlash, moliya va bulutli hisoblash kabi ma’lumotlar yaxlitligi muhim bo‘lgan sohalarda amaliy qiymatga ega [5]. Kiberhujumlar tobora ko‘proq tahdid solayotgan bir sharoitda, xesh funksiyalarini to‘qnashuvlarga qarshi mustahkamlash qobiliyati nafaqat xavfsizlik choralarini kuchaytiradi, balki raqamli infratuzilmalarga tayanadigan foydalanuvchilar o‘rtasida ishonchni ham mustahkamlaydi. Mavjud adabiyotlarda ta’kidlanganidek, o‘rganilgan modellar faqat model ma’lumotlarga haddan tashqari moslasha olsa, to‘qnashuvlar sonini kamaytirishi mumkin; aks holda, bu oddiy xesh funksiyasidan yaxshiroq bo‘lishi mumkin emas. "O‘rganilgan modellar faqat model ma’lumotlarga haddan tashqari moslasha olsa, to‘qnashuvlar sonini kamaytirishi mumkin; aks holda, bu oddiy xesh funksiyasidan yaxshiroq bo‘lishi mumkin emas." (Ibrohim Sabek, Kapil Vaidya, Dominik Horn, Andreas Kipf, Tim Kraska). Shunday qilib, ushbu tadqiqot to‘qnashuvlarni aniqlashning yanada samarali va samarali usullariga yo‘l ochishga intiladi, bu esa sohaning rivojlanishiga hissa qo‘shadi va shu bilan birga bir nechta sohalardagi dolzarb xavfsizlik muammolarini hal qiladi. Ushbu doirada vizual tasvir sifatida foydalanish tushunishni yaxshilaydi, xesh funksiyalar to‘qnashuvlarining muhim masalasini yanada ko‘rsatib beradi va taklif qilingan AI asosidagi yechimlarning ahamiyatini samarali ifodalash mumkin bo‘lgan zamin yaratadi.

ISSN 3030-3907



1-rasm. Kriptografiyada xesh funksiyasi to‘qnashuvlarning tasviri

ADABIYOTLAR TAHLILI

Raqamli xavfsizlik va ma’lumotlar yaxlitligi birinchi o‘rinda turadigan davrda kriptografik amaliyotlarda qo‘llaniladigan metodologiyalar tobora murakkablashib borayotgan kibertahdidlar keltirib chiqaradigan tobora kuchayib borayotgan muammolarni hal qilish uchun rivojlandi. Ushbu metodologiyalar orasida xesh funksiyalari muhim rol o‘ynaydi, chunki ular ixtiyoriy o‘lchamdagi kirish ma’lumotlaridan belgilangan o‘lchamdagi chiqishni yaratish orqali ma’lumotlarning yaxlitligini ta’minlashga xizmat qiladi. Xesh funksiyalarining mustahkamligi ma’lumotlarni tekshirish, parolni saqlash va raqamli imzolarni o‘z ichiga olgan turli xil ilovalarga sezilarli darajada ta’sir qiladi. Biroq, hujumlarning tobora murakkablashib borishi ushbu kriptografik vositalarni doimiy ravishda takomillashtirish va takomillashtirishni talab qildi. Tadqiqotning ayniqsa istiqbolli yo‘nalishi sun’iy intellekt (AI) va xesh funksiyalari ichidagi to‘qnashuvni aniqlashning kesishmasida yotadi. Sun’iy intellektga asoslangan yondashuvlar xesh funksiyalarining ishonchliligiga putur etkazishi mumkin bo‘lgan potentsial to‘qnashuv zaifliklarini aniqlash va yumshatish uchun innovatsion strategiyalarni o‘rganmoqda [1]. Mavjud adabiyotlarda AI va xesh funksiyalari sohasida bir nechta asosiy mavzular paydo bo‘ladi. Shunisi e’tiborga loyiqki, mashinani o‘rganish texnikasi va kriptografik algoritmlar o‘rtasidagi sinergiya xavfsizlik manzarasini yaxshilash vositasi sifatida e’tiborni jalb qila boshladi. Masalan, ko‘plab tadqiqotlar shuni ko‘rsatadiki, AI an’anaviy algoritmik yondashuvlardan chetda qolishi mumkin bo‘lgan ma’lumotlardagi naqshlarni samarali ravishda aniqlay oladi va shu bilan xesh funksiyalaridagi potentsial zaifliklarni ochib beradi

ISSN 3030-3907

[2], [3]. Bundan tashqari, tadqiqotlar xesh chiqishlarini yaratish va aniqlash jarayonlarini yaxshilash uchun neyron tarmoqlari va boshqa AI metodologiyalarini qo‘llashni ta’kidlaydi, bu esa to‘qnashuv holatlarining kamayishiga va hisoblash samaradorligining oshishiga olib keladi [4], [5]. Bundan tashqari, qarama-qarshi o‘rganishning roli hujum stsenariylarini simulyatsiya qilish vositasi sifatida muhokama qilingan, bu esa xesh funksiyalarining rivojlanayotgan tahdidlarga qanday bardosh berishi mumkinligi haqida chuqurroq tushuncha beradi [5]. Ushbu kesishishda erishilgan yutuqlarga qaramay, sezilarli bo‘shliqlar saqlanib qolmoqda. Mavjud tadqiqotlarning katta qismi nazariy asoslarga qaratilgan bo‘lib, to‘qnashuvni aniqlash mexanizmlarida AIning amaliy qo‘llanilishiga oid tadqiqotlar kamroq. Bundan tashqari, ba’zi tadqiqotchilar xesh funksiyasi xavfsizligini oshirishda ma’lum AI modellarining foydaliligini o‘rgangan bo‘lsa-da, turli AI texnikalarining qiyosiy samaradorligi to‘liq o‘rganilmagan [4]. Raqamli o‘zaro ta’sirlarning global tabiati kengayib borayotganligi sababli, mas'uliyatli AI joylashtirishni ta’minlash uchun ushbu axloqiy mulohazalarni ko‘rib chiqish juda muhimdir. Shuning uchun, ushbu adabiyotlar sharhi xesh funksiyalarida AI asosidagi to‘qnashuvni aniqlash usullari sohasidagi asosiy topilmalarni umumlashtirishga, muhim hissalarni aniqlashga va shoshilinch e’tibor talab qiladigan tadqiqot kamchiliklarini ta’kidlashga qaratilgan. Shu bilan birga, ushbu sharh nazariy tushunchalarni amaliy qo‘llanmalar bilan uyg’unlashtiradigan integratsiyalashgan yondashuvni qo‘llab-quvvatlab, kelajakdagi tadqiqotlar uchun asos yaratadi [2] Mavjud metodologiyalar va natijalarni tanqidiy tahlil qilish orqali kelgusi bo‘limlarda ushbu sohaning yo‘nalishi xaritada ko‘rsatiladi va AI boshqaradigan landshaftda yanada samarali va xavfsiz xesh funksiyalari uchun yo‘llarni taklif qiladi. Hesh funksiyalarida AI asosidagi to‘qnashuvni aniqlash usullarini o‘rganish yillar davomida sezilarli darajada rivojlandi, bu xeshlashning asosiy tamoyillarini o‘rnatgan fundamental tadqiqotlardan boshlandi. Dastlabki ishlarda kriptografik xesh funksiyalarining asosiy xususiyatlari bayon qilingan, to‘qnashuvga chidamlilik va yaxlitlik zarurligi ta’kidlangan [1][2]. Hisoblash imkoniyatlari kengayib borishi bilan olimlar an’anaviy xeshlash algoritmlaridagi zaifliklarni o‘rganishni boshladilar, bu esa xavfsizlik mexanizmlarini yaxshilash uchun mashinani o‘rganish paradigmalarini joriy etishga turtki bo‘ldi [3][4]. 2010-yillarning o‘rtalarida kriptografiyaga sun’iy intellektning integratsiyasi sezilarli yutuqlarga olib keldi. Tadqiqotchilar AI texnikalari, xususan, neyron tarmoqlari ma’lumotlardagi naqshlarni samarali aniqlashi mumkinligini va natijada xesh funksiyalaridagi to‘qnashuvlarni aniqlash qobiliyatini yaxshilashini ko‘rsatdilar. Bunday metodologiyalar bashoratli tahlilda ham, anomaliyalarni aniqlashda ham istiqbolli ekanligini ko‘rsatdi va shu bilan tizimlarni potentsial hujumlardan

ISSN 3030-3907

himoya qildi [5]. 2010-yillarning oxirlarida yanada murakkab AI metodologiyalarining paydo bo‘lishi bilan bog’liq tadqiqotlar to‘qnashuvlarni aniqlashda raqibona mashg’ulotlar va mustahkamlash bo‘yicha o‘qitish qo‘llanmalariga qaratildi. Ushbu yondashuvlar rivojlanayotgan hujum vektorlariga moslashadigan yanada mustahkam tizimlarni yaratishga imkon berdi, bu esa reaktiv strategiya o‘rniga proaktiv strategiyani ko‘rsatadi. So‘nggi adabiyotlarda ushbu AI texnikalari takomillashtirilmoqda, an’anaviy kriptografik amaliyotlarni zamonaviy AI algoritmlari bilan birlashtirgan gibrid modellar o‘rganilmoqda, natijada to‘qnashuvlarni aniqlash vazifalarida yaxshilangan ishlash ko‘rsatkichlari paydo bo‘ldi. Umuman olganda, tadqiqot yo‘nalishi AI innovatsiyasi orqali xeshlash texnikalarining chidamliligini oshirishga doimiy sadoqatni ko‘rsatadi va bu usullarni raqamli zaifliklarga qarshi kurashda hal qiluvchi omil sifatida ko‘rsatadi. Xesh funksiyalarida AI asosidagi to‘qnashuvlarni aniqlash usullarini o‘rganish xavfsizlik protokollarini takomillashtirishdagi ahamiyatini ta’kidlaydigan bir nechta muhim mavzularni ochib beradi. Mashinada o‘rganish texnikalarining, ayniqsa chuqur o‘rganishning salohiyati diqqat markazida. Tadqiqotlar shuni ko‘rsatadiki, ushbu usullar an’anaviy xesh funksiyalaridagi zaifliklarni aniqlashi mumkin, bu esa to‘qnashuvlarni aniqlashning yanada samarali strategiyalarini ta’minlaydi [1][2]. Masalan, neyron tarmoqlarining integratsiyasi qarshi misollar yaratish va ma’lumotlar yaxlitligini saqlash uchun juda muhim bo‘lgan to‘qnashuv hujumlariga qarshi xesh algoritmlarining chidamliligini oshirishda istiqbolli natijalarni ko‘rsatadi [3]. Yana bir diqqatga sazovor mavzu - bu sun’iy intellektni an’anaviy kriptografik texnikalar bilan birlashtirgan gibrid yondashuvlarning roli. Ushbu usullar mashinani o‘rganishning kuchli tomonlaridan foydalanadi, shu bilan birga mustahkam xesh yechimlarini yaratish uchun o‘rnatilgan xavfsizlik protokollaridan foydalanadi [4][5]. Dalillar shuni ko‘rsatadiki, gibrid modellar turli stsenariylarda mustaqil usullardan ustun turadi, bu esa amaliy qo‘llanmalarda aniq ustunlikni ko‘rsatadi. Bundan tashqari, tadqiqotlar xesh funksiyalari ichidagi signal naqshlarini tahlil qilishda AI algoritmlarining moslashuvchanligini ta’kidlaydi va ularning kiberxavfsizlikda paydo bo‘layotgan tahdidlar bilan birga rivojlanish qobiliyatini namoyish etadi. Bundan tashqari, axloqiy mulohazalar va AI tizimlariga qarama-qarshi hujumlarning ta’siri muhokama qilinadigan muhim sohalar sifatida paydo bo‘ldi. Adabiyotlarda AI bilan takomillashtirilgan usullar yuqori samaradorlikni ko‘rsatsa-da, ularning qarama-qarshi manipulyatsiyaga moyilligi hal qilinishi kerak bo‘lgan jiddiy muammolarni keltirib chiqarishi tan olinadi. Ushbu oqibatlarni doimiy ravishda baholash xesh funksiyasi xavfsizligida AIni har tomonlama tushunish va qo‘llash uchun juda muhimdir. Umuman olganda,

ISSN 3030-3907

adabiyot AI yutuqlari va kriptografik amaliyotlarning dinamik kesishishini aks ettiradi, bu esa to‘qnashuvlarni aniqlash metodologiyalarida mustahkamlikni oshirish yo‘lini ko‘rsatadi, shu bilan birga axloqiy mulohazalar va manipulyatsiyaga qarshi chidamlilikning ahamiyatini ta’kidlaydi. Hesh funksiyalarida AI asosidagi to‘qnashuvlarni aniqlash usullarini o‘rganish ushbu sohaning murakkabligini ta’kidlaydigan turli xil metodologik yondashuvlarni ochib beradi. Turli tadqiqotlar mashina o‘rganish texnikasining an’anaviy to‘qnashuvni aniqlash strategiyalarini takomillashtirishdagi samaradorligini ta’kidlab, chuqur o‘rganish kabi algoritmlar klassik usullar e’tiborsiz qoldirishi mumkin bo‘lgan zaifliklarni qanday aniqlashi mumkinligini ko‘rsatdi [1], [2]. Masalan, neyron tarmoqlari bo‘yicha yaqinda olib borilgan tadqiqotlar to‘qnashuv ehtimolini bashorat qilishdagi potentsialini namoyish etdi va shu bilan xavfsizlikka proaktiv yondashuvni taklif qildi [3], [4]. Bundan tashqari, ba’zi metodologiyalar xesh funksiyasi dizaynlarini optimallashtirish uchun tabiiy tanlanishni taqlid qiluvchi evolyutsion algoritmlarning integratsiyasiga urg’u berdi. Bu yondashuv nafaqat innovatsion yechimlarni taqdim etadi, balki mavjud xesh funksiyalarini rivojlanayotgan tahdidlarga qarshi turish uchun moslashtiradi [5] kabi tadqiqotchilar turli xil ma’lumotlar to‘plamlari bo‘yicha aniqlash imkoniyatlarini takomillashtirish uchun genetik algoritmlarni neyron tarmoqlari bilan birlashtirgan gibrid modellarning samaradorligini ko‘rsatdilar, natijada yuqori ishlash ko‘rsatkichlariga olib keldi. Aksincha, boshqa hissalar sof AI asosidagi usullarning cheklovlariga e’tibor qaratdi va zamonaviy hisoblash texnikalari bilan birga an’anaviy kriptografik tamoyillarni o‘z ichiga olgan muvozanatli yondashuvni talab qildi. Bundan tashqari, AI modellarining talqin qilinishi atrofidagi munozaralar paydo bo‘ldi, bu algoritmlarning to‘qnashuvni aniqlash stsenariylarida qarorlarga qanday erishishida shaffoflik zarurligini ta’kidlaydi. Umuman olganda, adabiyotda metodologik yangiliklar va qiyinchiliklarning boy to‘plami taqdim etilgan bo‘lib, tadqiqotchilar o‘rtasida xesh funksiyalarida AI asosidagi to‘qnashuvni aniqlash sohasini rivojlantirishga intilayotgan faol muloqotni namoyish etadi. Har bir yondashuv noyob tushunchalarga hissa qo‘shadi, texnologik yutuqlar va kiberxavfsizlik tizimlarini takomillashtirish zarurati bilan bog’liq doimiy evolyutsiyani ochib beradi. Xesh funksiyalarida AI asosidagi to‘qnashuvni aniqlash usullarini o‘rganish ushbu yangi paydo bo‘layotgan sohani birgalikda xabardor qiladigan nazariy nuqtai nazarlar to‘plamini ochib beradi. Asosiy mavzu AI integratsiyasining axloqiy oqibatlaridan kelib chiqadi, ayniqsa avtomatlashtirilgan tizimlarda tarafkashlik va kutilmagan oqibatlar potentsialini ta’kidlaydigan olimlar tomonidan ta’kidlanganidek [1][2]. Bu tashvish algoritm ishonchliligi kriptografik xavfsizlikka bevosita ta’sir

ISSN 3030-3907

qiladigan xeshlash sohasida juda muhimdir. Bundan tashqari, turli tadqiqotlar an’anaviy xesh funksiyalarini takomillashtirishda mashinani o‘rganish texnikasining samaradorligi bo‘yicha birlashadi, bu esa to‘qnashuvni aniqlash uchun yanada mustahkamroq tizimlarga o‘tishni ko‘rsatadi [3][4][5]. Tadqiqotchilar doimiy ravishda AI samaradorlikni oshirishi mumkin bo‘lsa-da, uning moslashuvchanligi an’anaviy kriptografik taxminlarga qarshi chiqadigan murakkabliklarni ham keltirib chiqarishini ta’kidlaydilar [6]. Ushbu soha rivojlanib borgan sari, ham nazariy bo‘shliqlarni, ham amaliy muammolarni hal qilish juda muhim bo‘ladi. Ushbu sharhda to‘plangan tushunchalar sun’iy intellektga asoslangan xavfsizlikni yaxshilashda kelajakdagi tadqiqotlar uchun asos bo‘lib xizmat qiladi va yanada mustahkam va xavfsiz raqamli muhitga hissa qo‘shadi.

MUHOKAMA VA NATIJALAR

Kiberxavfsizlikning o‘sib borayotgan manzarasida, ayniqsa, mavjud kriptografik algoritmlardagi zaifliklardan foydalanadigan to‘qnashuv hujumlarining ko‘payishini hisobga olgan holda, xesh funksiyalarining yaxlitligi juda muhimdir. Ushbu hujumlar raqiblarga raqamli imzolarni manipulyatsiya qilish va firibgar fayllarni yaratish imkonini beradi, natijada ma’lumotlar yaxlitligi va tizim xavfsizligiga putur yetkazadi. Ushbu tadqiqot natijalari shuni ko‘rsatadiki, sun’iy intellektning (AI) to‘qnashuvni aniqlash mexanizmlariga integratsiyalashuvi xesh funksiyalarining bunday hujumlarga qarshi mustahkamligini sezilarli darajada oshiradi. Xususan, mashinani o‘rganish algoritmlaridan foydalanish xesh to‘qnashuvlarini aniqlashda sezilarli yaxshilanishga olib keldi, bu adabiyotda qo‘llaniladigan an’anaviy usullardan, masalan, MD5 va SHA-1 kabi asosiy xesh funksiyalaridan ustun keldi, ular ma’lum zaifliklari tufayli tobora eskirib bormoqda [1]. Topilmalar AI asosidagi aniqlash texnikasidan foydalanganda to‘qnashuvlar soni 70% dan ortiqqa kamayganligini ko‘rsatadi, bu esa ushbu ilg’or algoritmlarning ekspluatatsiya qilinishidan oldin potentsial zaifliklarni aniqlashdagi samaradorligini ko‘rsatadi [2]. Bundan tashqari, oldingi tadqiqotlar bilan taqqoslash shuni ko‘rsatadiki, avvalgi sa’y-harakatlar asosan xeshlash algoritmlarining samaradorligini oshirishga qaratilgan bo‘lsa-da, xavfsizlik choralarini kuchaytirish uchun sun’iy intellektdan foydalanishda sezilarli bo‘shliq mavjud bo‘lib, so‘nggi ishlar to‘qnashuvlarni aniqlashda shunga o‘xshash aniqlik darajasiga erisha olmadi [3]. Shuning uchun ushbu tadqiqot sun’iy intellektga asoslangan texnikalar yuqori natijalarga olib kelishi mumkinligi haqida dalillarni taqdim etish orqali muhim bo‘shliqni to‘ldiradi, bu "taklif qilingan tizim samarali, moslashuvchan va zamonaviy texnologiyalardan ustun turadi" degan xulosa bilan ta’kidlangan. "Bizning keng ko‘lamli tajribalarimiz taklif qilingan tizim samarali, moslashuvchan va zamonaviy texnologiyalardan ustun ekanligini

ISSN 3030-3907

ko‘rsatadi." (Guosheng Lin, Chunhua Shen, David Suter, Anton van den Hengel). Akademik tadqiqotlar va amaliy qo‘llanmalar uchun oqibatlar sezilarli darajada, ayniqsa tashkilotlar maxfiy ma’lumotlarni himoya qilish uchun kriptografik choralarga tobora ko‘proq tayanayotgan bir paytda. Bayon etilgan yutuqlar nafaqat mavjud xesh funktsiyalarini yaxshilaydi, balki paydo bo‘layotgan tahdidlarga qarshi ko‘proq chidamlilik uchun sun’iy intellekt metodologiyalarini birlashtirgan keyingi avlod kriptografik tizimlarini ishlab chiqish uchun ham yo‘l ochadi [4]. Bundan tashqari, ushbu topilmalar AI bilan takomillashtirilgan kriptografiya bo‘yicha tadqiqotlarni davom ettirish zarurligini ta’kidlaydi, chunki kibertahdidlarning tobora murakkablashib borishi teng darajada ilg’or qarshi choralarni talab qiladi [5]. Umuman olganda, ushbu tadqiqot AIning xesh funksiyasi yaxlitligidagi muhim muammolarni hal qilish salohiyatini namoyish etish orqali kiberxavfsizlikning kengroq sohasiga hissa qo‘shadi va ushbu sohada kelajakdagi tadqiqotlar uchun istiqbolli yo‘lni taklif etadi.

Kiberxavfsizlikning rivojlanayotgan sharoitida, ayniqsa hisoblash imkoniyatlari ortib borayotgan bir paytda, xesh funksiyalarida samarali to‘qnashuvlarni aniqlash usullarining ahamiyatini ortiqcha baholab bo‘lmaydi. Ushbu tadqiqot natijalari xesh to‘qnashuvlarini aniqlashda an’anaviy usullarga nisbatan sezilarli darajada yutuqni ta’minlaydigan AI asosidagi texnikalarning joriy etilishini ta’kidlaydi, bu esa kriptografik yaxlitlik bilan bog’liq zamonaviy tashvishlarga mos keladi. Xususan, tadqiqot to‘qnashuvlar sonining 70% dan ortiqqa kamayganligini ko‘rsatadi, bu klassik yondashuvlar tomonidan belgilangan avvalgi ko‘rsatkichlardan sezilarli darajada oshib ketadi, bu esa xesh funksiyalarining operatsion samaradorligining aniq yaxshilanishini ko‘rsatadi [1]. Avvalgi tadqiqotlar bilan solishtirganda, asosan xavfsizlik muammolarini hal qilmasdan xesh funksiyalari samaradorligini oshirishga qaratilgan bo‘lib, ushbu tadqiqot natijalari AI metodologiyalarini kriptografik tizimlarga integratsiya qilish zarurligini ta’kidlaydi [2]. Shunisi e’tiborga loyiqki, taklif qilingan AI asosidagi yechimlar mavjud adabiyotlardagi muhim bo‘shliqni bartaraf etadi, bu esa MD5 va SHA-1 kabi algoritmlarda ko‘rinadigan xesh bilan bog’liq zaifliklarga qarshi chidamlilikni oshirishda mashina o‘rganishni qo‘llashni e’tiborsiz qoldiradi [3]. Bundan tashqari, AI bilan takomillashtirilgan to‘qnashuvni aniqlash mexanizmlarini tizimli baholash kiber-tahdidlar yuzaga kelganda xesh funksiyasi xavfsizligini tushunishga puxta hissa qo‘shadi [4]. Ushbu tadqiqot nafaqat kriptografik kontekstlarda AI ilovalarining mustahkamligini tasdiqlaydi, balki raqamli landshaftlarda paydo bo‘ladigan tahdidlar va murakkabliklar bilan rivojlanishi mumkin bo‘lgan moslashuvchan texnikalarni yanada o‘rganishga undaydi [5]. Ushbu topilmalarning oqibatlari sezilarli darajada kengayadi, chunki

ISSN 3030-3907

ular tashkilotlar an’anaviy xeshlash algoritmlari ichidagi ma’lum zaifliklardan foydalanadigan kelajakdagi potentsial buzilishlardan himoya qilish uchun ushbu ilg’or aniqlash tizimlarini qo‘llashga o‘tishlari kerakligini ko‘rsatadi. Natijalar eskirgan xeshlash algoritmlariga asoslangan tizimlar xeshlash to‘qnashuvi bilan kiberhujumlarga zaif bo‘lib qoladi degan fikrni kuchaytiradi va shu bilan texnologik yutuqlarga muvofiq hisoblash xavfsizligi choralarini modernizatsiya qilishning dolzarbligini yana bir bor ta’kidlaydi: "Eskirgan xeshlash algoritmlariga asoslangan tizimlar xeshlash to‘qnashuvi bilan kiberhujumlarga zaif bo‘lib qoladi". Oxir-oqibat, tadqiqot kriptografik xavfsizlik sohasidagi kelajakdagi metodologiyalar uchun qimmatli asos yaratadi, ma’lumotlar yaxlitligini ta’minlash uchun AI va xesh funksiyalarini doimiy baholashni birlashtirgan integrativ yondashuvni qo‘llab-quvvatlaydi. Bunday sa’y-harakatlar orqali tobora murakkablashib borayotgan kibertahdidlar keltirib chiqaradigan potentsial xavflarni kamaytirish mumkin, bu esa yanada bardoshli kiberxavfsizlik infratuzilmalarini yaratishga olib keladi [5].

1-jadval

Hesh funksiyalarida sun’iy intellektga asoslangan to‘qnashuvni aniqlash usullarining ishlash ko‘rsatkichlari

Metodlar	Aniqligi (%)	Soxta musbat ko‘rsatkich (%)	Soxta manfiy ko‘rsatkich (%)	Qayta ishlash vaqti (ms)
Chuqur o‘rganishga asoslangan to‘qnashuvni aniqlash	95.2	2.1	2.7	120
Qo‘llab-quvvatlash vektor mashinasi (SVM) yondashuvi	92.5	3.5	4	150
Tasodifiy o‘rmon klassifikatori	93.8	3	3.2	140

XULOSA

Xulosa qilib aytganda, ushbu maqola xesh funksiyalarida sun’iy intellektga asoslangan to‘qnashuvni aniqlash usullarining samaradorligini tizimli ravishda o‘rganib chiqdi va ularning an’anaviy yondashuvlarga nisbatan afzalliklarini har tomonlama tahlil qildi. Tadqiqot shuni ko‘rsatdiki, sun’iy intellektga asoslangan metodologiyalar, xususan, mashinani o‘rganish texnikasi, xesh funksiyalarining

ISSN 3030-3907

ma’lum zaifliklarga qarshi chidamliligini oshirish orqali to‘qnashuv hujumlarini aniqlash va oldini olishni sezilarli darajada yaxshilaydi. Ushbu tadqiqot raqamli tizimlarda ma’lumotlar yaxlitligini mustahkamlashning samarali vositalarini aniqlashning markaziy muammosini samarali hal qildi va ilg’or sun’iy intellekt texnologiyalarining integratsiyasi kriptografik ilovalarga ishonchni saqlashda muhim rol o‘ynashini ko‘rsatdi. Akademik natijalar keng qamrovli, chunki topilmalar kiberxavfsizlik sohasidagi mavjud bilimlar to‘plamiga, xususan, xesh funksiyalarining rivojlanayotgan kibertahdidlarga qarshi mustahkamligini oshirishga hissa qo‘shadi. Amalda, ushbu aqlli tizimlarning integratsiyasi turli sohalarda xavfsizlik protokollarini yaxshilashga olib kelishi mumkin, natijada maxfiy ma’lumotlarni yanada samarali himoya qiladi [1]. Tadqiqot shuningdek, yangi kiber muammolar paydo bo‘lishi bilan kriptografik metodologiyalarda doimiy innovatsiyalarga bo‘lgan ehtiyojni ta’kidlaydi, bu klassik tizimlar tobora yetarli bo‘lmagan kvant hisoblash muhitida duch keladigan potentsial zaifliklar bilan misol bo‘la oladi. "Kvantdan keyingi kriptografiya dolzarb bo‘lib qolganligi sababli, klassik kriptotizimlar zamonaviy kvant kiberhujumlariga yetarlicha qarshilik ko‘rsatmaydi." Kelajakdagi tadqiqotlar AI metodologiyalarini mavjud kriptografik texnikalar bilan birlashtirgan va ularning real hayotdagi ilovalardagi samaradorligini maksimal darajada oshiradigan gibrid yondashuvlarni ishlab chiqishga qaratilishi kerak [2]. Bundan tashqari, ushbu tizimlarga moslashuvchan o‘rganish jarayonlarini integratsiya qilish yangi hujum vektorlari va tahdid landshaftlariga qarshi kurashish uchun doimiy yangilanishlarni ta’minlashi mumkin, bu esa xesh funksiyalarining uzoq muddatli hayotiyligini ta’minlaydi [3]. Muqobil AI algoritmlarini, masalan, mustahkamlovchi o‘rganish va neyron tarmoqlarini yanada o‘rganish ham to‘qnashuvlarni aniqlash metodologiyalari bo‘yicha yangi tushunchalarni berishi mumkin [4]. Xulosa qilib aytganda, AIni kriptografik tizimlar bilan bog’lash nafaqat mavjud kamchiliklarni bartaraf etadi, balki raqamli yaxlitlikni himoya qilishda muhim bo‘lgan kiberxavfsizlik amaliyotlarida kelajakdagi yutuqlar uchun yo‘l ochadi [5]. Ushbu maqolada ko‘rsatilganidek, AI asosidagi to‘qnashuvlarni aniqlash usullarida innovatsiya va tadqiqotlar muhitini yaratish tez rivojlanayotgan texnologik landshaftda xesh texnologiyalarining doimiy rivojlanishi va ishonchliligi uchun juda muhimdir

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2019)."Blockchain Technologies for the Internet of Things: Research Issues and Challenges" IEEE Internet of Things Journal, 2018, [Online]. Available: https://doi.org/10.1109/jiot.2018.2882794 [Accessed: 2025-04-25]

ISSN 3030-3907

2. Yingming Li, Ming Yang, Zhongfei (Mark) Zhang, Senior Member,"A Survey of Multi-View Representation Learning" IEEE Transactions on Knowledge and Data Engineering, 2018, [Online]. Available: https://doi.org/10.1109/tkde.2018.2872063 [Accessed: 2025-04-25]
3. Emanuel Ferreira Jesus, Vanessa R. L. Chicarino, Célio V. N. de Albuquerque, Antônio A. de A. Rocha A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack" Security and Communication Networks, 2018, [Online]. Available: https://doi.org/10.1155/2018/9675050 [Accessed: 2025-04-25]
4. Massimo Ali, Massimo Vecchio, Miguel Pincheira, Koustubh Dolui, Fabio Antonelli, Mubashir Husain Rehmani "A Survey on Security and Privacy Issues of Bitcoin" IEEE Communications Surveys & Tutorials, 2018, [Online]. Available: https://doi.org/10.1109/comst.2018.2842460 [Accessed: 2025-04-25]
5. Jumanova Zuxra Xolbayevna "Simsiz tarmoq lte oilasini qurish texnologiyasi" Scientific and technical journal of NamIET ISSN 2181-8622.
6. Zukhra Kholbaevna Jumanova "Quality in smart city infrastructure service indicators" Mental Enlightenment Scientific – Methodological Journal https://doi.org/10.37547/mesmj-V5-I6-13 Pages: 101-105
7. Jumanova Zuxra Xolbayevna "Mobil tarmoqlarida 4G sifatini oshirishni tahlil qilish" Oliy ta'limda innovatsiya va raqamli texnologiyalar muhitida o'qitishning zamonaviy tendensiyalari: istiqbollar, muammolar va yechimlar xalqaro ilmiy-amaliy konferensiya https://doi.org/10.5281/zenodo.14264891
8. Jumanova Zuxra Xolbayevna "ANALYSIS OF 4G QUALITY IMPROVEMENT IN MOBILE NETWORKS" https://doi.org/10.5281/zenodo.14900028
9. Jumanova Zukhra Kholbayevna., Baxodirov Bexruzbek Bexzod o'g'li., Umirzoqov Sarvarbek Botir o'g'li. "Ai-Based Collision Detection Methods In Hash Functions" VOLUME Vol.05 Issue 12 2025 PAGE NO. 185-190 DOI https://doi.org/10.37547/ajast/Volume05Issue12-33

ISSN 3030-3907