INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.2 №6 (2024). June
innovativepublication.uz

MODULLI YIG’INDILAR BO’YICHA XIMOYALOVCHI INFORMATSIYA ISHONCHLILIGINI OSHIRISH ALGORITM VA DASTURIY VOSITALARNI YARATISH

Sayfullayev Jo'rabek Sadin o'g'li
Samarqand davlat Universiteti Intellektual tizimlar va kompyutr texnologiyalari fakulteti Kompyuter ilmlari va dasturlash texnologiyalari yo'nalishi

Annotatsiya: Siyosatchilar, muassasalar, tashkilotlar va boshqalarning elektron hujjat aylanishi tizimlarining (EHAT) samaradorligi elektron hujjatlarni (EH) qayta ishlash sifati ko'rsatkichlarining yuqori darajasini, xususan, ma'lumotlarning xavfsizligi, ishonchliligi, to'liqligi, dolzarbligini ta'minlash orqali erishiladi.

Kalit so’zlar: elektron hujjat, axborotni himoya qilish va ishonchlilik, algoritmik tizim, blok-guruh yondashuvi, amalga oshirish, ortiqcha kodlash, tizimli va tabiiy ortiqchalik, dasturiy ta'minot paketi.

An'anaviy tizimlarda, masalan, ma'lum bo'lgan "blokcheyn" texnologiyasida ma'lumotlarning himoyasini ta'minlash uchun raqamlar, belgilar, so'zlar, iboralar bilan aniqlanishi mumkin bo'lgan kalit tasodifiy o'zgaruvchilar (KTO’) qo'llaniladiAxborot obyektlarini kodlash va keyin shifrlash amalga oshiriladi: belgilar, harflar, raqamlar, matnlar.

Tadqiqot kodlangan xabar matritsasini kodlash va dekodlashning asosiy mexanizmini tashkil etuvchi (KTO’) submatritsasi ko'rinishida tizimli kod ortiqcha foydalanishga qaratilgan yondashuvni taklif qiladi. Mantiqiy ikkilik yig'indi, ixtiyoriy ko'plikning modulli yig'indisi usullari bilan tekshirish bilan shovqinga chidamli ortiqcha kodlash

kontseptsiyasidan foydalanish asosida axborotning ishonchliligini oshirish bilan birga Strukturaviy kodni ortiqcha ishlatish taklif etiladi.

Bu vazifalar ikkilik (o‘nlik, butun, arifmetik) sanoq sistemasida berilgan belgilar uzunligi bilan dastlabki kodni ko‘paytirish operatsiyasi bilan bog‘liq bo‘lgan kod o‘zgartirish tushunchalari bo‘yicha hal qilinadi. Axborotning xavfsizligi va yuqori ishonchliligini ta'minlash funksiyasini bajarishga qaratilgan umumlashtirilgan kodlash (shifrlash) va dekodlash (dekodlash) algoritmi ishlab chiqilgan.

Asl ma'lumot *1 x n* o'lchamli matritsa orqali uzatish uchun taqdim etiladi, *n* - belgilar soni. Elementlar o'lchami *k x k* bo'lgan kodlovchi *G* matritsa hosil bo'ladi, unda kk elementlar soni elementlar sonidan n ko'p bo'lishi kerak, ya'ni $k \geq n$ shartni bajarish kerak. Masalalarni yechish uchun *k* elementlari submatritsalar bilan ifodalanadi.

Kodlash matritsalarini qurishda ko'paytirish va qo'shish amallari bajariladi va kodlangan tasvirning elementlarini ko'rsatishda bit bo'yicha mantiqiy qo'shish, ko'paytirish yoki modul yig'ish usullari qo'llanilishi mumkin.

n ta satr va *k* ta ustunga ega bo'lgan ikki o'lchovli Ψ matritsa sifatida hosil bo'ladi

$$\Psi = \begin{bmatrix} M_{11} & M_{21} & \dots & M_{1k} \\ M_{21} & M_{22} & \cdots & M_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ M_{n1} & M_{n2} & \dots & M_{nk} \end{bmatrix}.$$

Uni $M_{i1}, M_{i2}, ..., M_{ik}$ vektorli ixtiyoriy formatda olish mumkin. Matritsaning qisqartirilgan yozuvi shaklda yoziladi

$\Psi = [M_{ij}]$ or $\Psi = [M_{ij}]_{\text{n×k}}$.

Modulli arifmetika asosida kiritilgan ma'lumotlarning ishonchliligini oshirishga qaratilgan yondashuv taklif etiladi. Yondashuvda ma'lumotlar hujjatda ikkilik bo'lmagan modulli kodning (MK) bir elementi sifatida ko'rib chiqiladi. Kod ortiqcha qoldiq tizimidagi raqamlarni ifodalaydi.

1. .

Modulli yig'indi asosida kiritilgan ma'lumotlarning ishonchliligini oshirishga qaratilgan yondashuv taklif etiladi

E'tibor bering, algoritmik tizimda kodlash matritsalarini ifodalash uchun blok kod turlariga, yig'ish modullariga qarab qurilgan. Asl kodlangan ma'lumot matritsaga aylantiriladi. $1\times k$

$$B = A\times G.$$

Manba kodining matritsa shaklida teskari o'zgarishi shakldagi matritsaga ko'paytirilishi bilan bog'liq.

B matritsasi shaklidagi A manba kodining teskari o'zgarishi B ning shakldagi G^{-1} matritsasiga ko'paytirilishi bilan bog'liq.

$$G: A = B\times G^{-1} = A\times G\times G^{-1}$$

bu erda G - hosil qiluvchi matritsa; G^{-1} - tekshirish matritsasi.

Yaratuvchi matritsani yaratish printsipi G , n x n o'lchamli g submatritsasini tanlash G^{-1} teskari matritsalarni qurish usuli bilan aniqlanadi!

$$G^{-1} = \begin{pmatrix} g_{11} & g_{12} & \cdot & g_{1n} & \cdot & g_{1k} \\ g_{21} & g_{22} & \cdot & g_{2n} & \cdot & g_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{n1} & g_{n2} & \cdot & g_{nn} & \cdot & g_{nk} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{k1} & g_{k2} & \cdot & \cdot & \cdot & g_{kk} \end{pmatrix}$$

Tadqiqotning ikkita tomoni amalga oshirilmoqda. Birinchi variant axborotni himoya qilish uchun kripto-transformatsiyani amalga oshirishga qaratilgan.

Ta'kidlanishicha, k o'lcham dastlabki kod uzunligidan oshib ketgan n keyin G matritsasining elementlarini shakllantirish va manba kodining uzunligini k ga etkazish mumkin. Shu munosabat bilan G n x n matritsadagi uzunligi n ta belgi va g submatritsasining dastlabki

kodi dastlabki matnni kriptografik o'zgartirishlar (shifrlash) imkonini beradi. Manba kodi kodlash matritsasi bilan ko'paytiriladi, ya'ni kriptografik transformatsiya natijalari bo'yicha. Axborot xavfsizligining asosiy muammosi kalit – KTO' dan foydalanish hisoblanadi.

KTO' submatritsasining elementlari ham xavfsizlikni oshirish, ham axborot ishonchliligini oshirish uchun ishlatiladi. Dastlabki ma'lumotlarning ishonchliligini oshirish mexanizmida $k>n$ o'lchamli oldingi yangi kodlangan matritsasi qo'llaniladi.

Algoritmik tizim n ta belgidan iborat boshlang'ich kod so'zini uzunlikdagi k belgilar kodiga aylantiradi, shuningdek, G - hosil qiluvchi matritsalarni hosil qiladi. n uzunlikdagi belgilarning boshlang'ich kodini $r=(k-n)$ ko'rinishidagi uzunlikdagi k belgilarning dastlabki kod so'ziga qo'shimcha bilan o'zgartirish xatoliklarni to'g'irlovchi ortiqcha kodlashni qo'llash tamoyilini belgilaydi.

$$G=\begin{pmatrix} 1 & 0 & . & 0 & . & g_{1k} \\ 0 & 1 & . & 0 & . & g_{2k} \\ . & . & . & . & . & . \\ 0 & 0 & . & 1 & . & g_{nk} \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \end{pmatrix}.$$

G_{kk} elementlari bo'lgan generativ submatritsalar qo'shimcha qatorlar va ustunlar bilan identifikatsiya matritsasidan tuzilgan. Dastlabki kod so'zini qo'shimcha belgilar matritsasiga ko'paytirish natijasida qo'shimcha belgilar (boshqaruv belgilari) ko'rinishida ko'rsatilgan tizimli ortiqchalikka ega bo'lgan k simvolik kod tuziladi. Bundan tashqari, n qatordagi elementlar axborot xavfsizligi va ishonchliligini oshirish uchun foydalaniladigan xatoliklarni tuzatuvchi ortiqcha kodning xususiyatini belgilaydi. Bunda xatoni tuzatuvchi ortiqcha kod matritsasining birinchi n elementi qo'shimcha ortiqcha r boshqaruv belgilarini o'z ichiga olmaydi, manba kodining mos keladigan elementlari bilan mos keladi.

$$G = \begin{pmatrix} 1 & 0 & . & 0 & . & 1 \\ 0 & 1 & . & 0 & . & 1 \\ . & . & . & . & . & . \\ 0 & 0 & . & 1 & . & 1 \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \end{pmatrix}.$$

Matritsadagi boshqaruv belgilari bit bo'yicha mantiqiy yig'ish yoki yig'ish moduli asosida olinadi 2^b , manba kod belgilarining ikkilik uzunligi, barcha n elementning bitlari uzunligi bilan berilgan.

Kriptogramma xususiyatidan foydalanishga asoslangan ma'lumotlarning ishonchliligini oshirish mexanizmining o'ziga xos xususiyati shundan iboratki, kodlangan so'zni tekshirish matritsasi G^{-1} bilan ko'paytirganda, xatolar qator vektori olinadi, uning elementlari tuzatiladi: mavjudligi, joyi, buzilish kattaligi, kod turi.

Mexanizmning samaradorligi xatoni aniqlash ehtimoli qiymati P_{ed} bilan belgilanadi, va ma'lumotlarning ortiqcha miqdori (KTO' submatritsasidan nazorat belgilarining soni). Mustaqil kod buzilishlari sodir bo'lganda, aniqlanmagan xatolar ehtimoli tomonidan beriladi

$$P_{ud} = 1 - P_{ed} = 1 - 2^{-br}.$$

Aniqlab bo'lmaydigan xatolar ehtimolini baholashni quyidagi usullar bilan olamiz: ramziy, raqamli, modulli ikkilik, modulli o'nli yig'indilar.

Tadqiqotning uchinchi versiyasi ketma-ket kodlash, kripto-transformatsiya va matnni dekodlashdan iborat bo'lgan shifrlangan ma'lumotlarning kripto himoyasini oshirishga qaratilgan. Qabul qiluvchi tomondagi algoritmik tizim bloki axborotning yaxlitligini tekshiradi, keyin esa matnning shifrini ochadi.

Shu sababli, manba kodi bir belgi bilan kengaytiriladi $a_k=0$. Va kodlash matritsasining elementlari $\{c_i\}_{pj}$ kichik to'plamidan qiymat bilan ifodalanadi, ya'ni.

$$g_{ij} = \{c_i\}_{p_j},$$

Bu yerda $\{c_i\}_{pj}$ c_i ni p_j ga bo‘lishdan keyingi qoldiqlar bo‘lib, ular p_j ning qoldiq sinflarida sanoq tizimining asosiga mos keladi.

O'zgartirilgan kodning belgilarini hisoblash a_i moduli p_j amalga oshiriladi. Bunda $A = a_1, a_2, ..., a_n$,manba kodi, $A = a_1, a_2, ..., a_n$,qoldiq sinflaridagi raqamga aylantiriladi, unga nisbatan axborot ishonchliligini nazorat qilish mexanizmlari qo'llanilishi mumkin.

O'zgartirilgan kodning belgilarini hisoblash a_i moduli p_j amalga oshiriladi. Bunday holda, manba kodi $A = a_1, a_2, ..., a_n$, $A = a_1, a_2, ..., a_n$ qoldiq sinflarida raqamga aylantiriladi, unga nisbatan axborot ishonchliligini nazorat qilish mexanizmlari qo'llanilishi mumkin.

Shunisi qiziqki, p_j bazasini tanlash qoidasi yoki bu asoslarning qiymatlari noma'lum bo'lsa, taklif qilingan yondashuv kriptografik jihatdan xavfsiz deb hisoblanadi.

Xulosa. Modulli yig’indilarni himoyalash va ortiqcha kodlash asosidagi mexanizmlaridan foydalanish, SWR matritsalaridan foydalanish, axborotning ishonchliligini himoya qilish va nazorat qilish uchun joriy qilingan qo‘shimcha boshqaruv belgilaridan foydalanish orqali axborot ishonchliligini oshirish bo‘yicha konstruktiv yondashuvlar, tamoyillar va usullar ishlab chiqildi.

Axborot xavfsizligini nazorat qilishni tashkil etishning asosiy asosini tashkil etuvchi va tabiiy xarakterdagi buzilishlarning ko‘plab guruhlarini aniqlash imkonini beruvchi axborot ishonchliligini blok-guruh nazorati usuli taklif etilmoqda va joriy etilgan.

Axborotning xavfsizligi va ishonchliligini nazorat qilish uchun kod bloklarining uzunligi kodli xabar uzunligidan oshmasligi kerak. Katta va uzoq muddatli ma'lumotlar buzilishlari sharoitida muammoni hal qilish uchun an'anaviy axborot uzatish texnologiyalarida xatolarni to'g'rilash kodining tuzatuvchi xususiyatlaridan yuqori bo'lgan birlashtirilgan kodlardan foydalanish taklif etiladi.

Foydalanilgan adabiyotlar:

2. Kumar va boshq. (2020). "Modulli yig'indilarda bashoratli parvarishlash uchun mashinani o'rganish."Sanoat Informatika bo'yicha IEEE operatsiyalari.

3. Li va boshq. (2019). "Modulli yig'indilarda Real vaqtda Monitoring va nosozliklarni aniqlash uchun raqamli egizaklarga asoslangan yondashuv."Aqlli ishlab chiqarish jurnali.

4. Dev va boshq. (2018). "Sanoat IoT tizimlari uchun ma'lumotlar integratsiyasi platformalarida so'rov."IEEE aloqa tadqiqotlar & Tutorials.

5. Zhang va boshq. (2017). "Modulli yig'ilishlarda adaptiv boshqaruv uchun mustahkamlashni o'rganish."Automatica.

6. Modelika Assotsiatsiyasi. (nd.). Modelica: murakkab tizimlar uchun modellashtirish Tili.

7. Mat ishlari. (nd.). Simulink: simulyatsiya va modelga asoslangan dizayn