RAQAMLI FAYLLAR METAMA'LUMOTLARINI HIMOYALASHDA ZAMONAVIY ALGORITMIK YONDASHUVLAR

Sodiqova Dilnoza Jumanazarovna
Muxammad al – Xorazmiy nomidagi TATU "Kiberxavfsizlik va kriminalistika" kafedrasi assistenti.
Email: sodiqovadilnoza655@gmail.com

Annotatsiya. Raqamli axborot almashinuvi jarayonlarining jadal rivojlanishi fayl metama'lumotlarining xavfsizligini ta'minlash masalasini dolzarb muammolardan biriga aylantirdi. Metama'lumotlar faylning mazmunidan tashqari uning muallifi, yaratilgan vaqti, joylashuvi, tahrir tarixi kabi muhim axborotni o'z ichiga oladi va ko'pincha maxfiy ma'lumotlarning oshkor bo'lishiga sabab bo'ladi. Mazkur maqolada raqamli fayllar metama'lumotlarini himoyalashga qaratilgan zamonaviy algoritmik yondashuvlar tahlil qilinadi, ularning afzallik va cheklovlari ko'rsatib beriladi hamda axborot-kommunikatsiya tizimlarida qo'llash imkoniyatlari yoritiladi.

Kalit so'zlar: metama'lumotlar, axborot xavfsizligi, raqamli fayllar, algoritmik himoya, kriptografiya, axborot-kommunikatsiya tizimlari.

Аннотация. Стремительное развитие процессов цифрового информационного обмена обусловило актуальность задачи обеспечения безопасности метаданных файлов. Метаданные, помимо содержательной части файла, включают сведения об авторе, времени создания, местоположении, истории редактирования и других параметрах, которые во многих случаях могут приводить к раскрытию конфиденциальной информации. В данной статье проводится анализ современных алгоритмических подходов к защите метаданных цифровых файлов, рассматриваются их преимущества и ограничения, а также освещаются возможности их применения в информационно-коммуникационных системах.

Ключевые слова: метаданные, информационная безопасность, цифровые файлы, алгоритмическая защита, криптография, информационно-коммуникационные системы.

Abstract. The rapid development of digital information exchange processes has made ensuring the security of file metadata one of the most pressing challenges. In addition to file content, metadata include critical information such as authorship, creation time, location, and editing history, which can often lead to the disclosure of sensitive information. This paper analyzes modern algorithmic approaches to protecting digital file metadata, highlights their advantages and limitations, and discusses their applicability within information and communication systems.

ISSN 3030-3907

Keywords: metadata, information security, digital files, algorithmic protection, cryptography, information and communication systems.

KIRISH

Zamonaviy axborot-kommunikatsiya tizimlarida raqamli fayllar bilan ishlash jarayonlari hajm va murakkablik jihatidan sezilarli darajada kengayib bormoqda. Elektron hujjat aylanishi, bulutli texnologiyalar, mobil qurilmalar va global tarmoqlar orqali ma’lumotlar almashinuvi axborot xavfsizligini ta’minlash masalasini muhim strategik vazifaga aylantirmoqda. An’anaviy yondashuvlarda axborot xavfsizligi asosan fayl mazmunining maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan bo‘lsa-da, amaliy tajriba faylga biriktirilgan metama’lumotlar ham xavfsizlik nuqtai nazaridan kam ahamiyatga ega emasligini ko‘rsatmoqda.

Fayl metama’lumotlari raqamli ob’ektlarning yaratilishi, saqlanishi va qayta ishlanishi bilan bog‘liq bo‘lgan muhim atributlarni o‘z ichiga oladi. Bunday atributlarga muallif haqidagi ma’lumotlar, yaratilgan va tahrirlangan sanalar, foydalanilgan dasturiy vositalar, fayl joylashuvi hamda texnik parametrlar kiradi. Ushbu ma’lumotlar ko‘pincha foydalanuvchi yoki tashkilot faoliyati haqida bilvosita, biroq muhim axborotni oshkor etadi. Natijada metama’lumotlar orqali tizim arxitekturasi, ish jarayonlari yoki foydalanuvchi xatti-harakatlarini tahlil qilish imkoniyati paydo bo‘ladi, bu esa kiber tahdidlar va maqsadli hujumlar uchun qulay sharoit yaratadi.

Axborot xavfsizligi sohasida olib borilgan tadqiqotlar shuni ko‘rsatadiki, ko‘plab kiberhujumlar aynan metama’lumotlar asosida rejalashtiriladi yoki kuchaytiriladi. Shu sababli metama’lumotlarni himoyalash masalasi mustaqil tadqiqot yo‘nalishi sifatida qaralib, u faqat texnik muammo emas, balki axborot xavfsizligining konseptual va algoritmik asoslarini qayta ko‘rib chiqishni talab etadi. Ayniqsa, raqamli fayllar bilan ishlovchi zamonaviy axborot-kommunikatsiya tizimlarida metama’lumotlarni himoyalashning samarali mexanizmlarini ishlab chiqish dolzarb ilmiy-amaliy vazifa hisoblanadi.

Bugungi kunda metama’lumotlarni himoyalashda turli yondashuvlar mavjud bo‘lib, ular orasida kriptografik algoritmlar, metama’lumotlarni minimallashtirish va anonimlashtirish usullari, shuningdek gibrid va adaptiv algoritmik modellar alohida o‘rin egallaydi. Har bir yondashuv o‘zining afzallik va cheklovlariga ega bo‘lib, ularni tanlash tizimning xavfsizlik talablari, foydalanish muhiti va resurs imkoniyatlariga bog‘liqdir. Shu nuqtai nazardan, zamonaviy algoritmik yondashuvlarni kompleks tahlil qilish va ularning samaradorligini baholash muhim ilmiy ahamiyat kasb etadi.

ASOSIY ALGORITMIK MEXANIZMLAR

ISSN 3030-3907

Kriptografik algoritmlar asosidagi metama'lumotlarni himoyalash yondashuvi bir nechta asosiy algoritmik mexanizmlarga tayanadi. Ushbu mexanizmlar metama'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta'minlashga qaratilgan bo‘lib, ularning har biri axborot-kommunikatsiya tizimlarining xavfsizlik talablariga muvofiq holda qo‘llaniladi. Metama'lumotlarni himoyalash jarayonida algoritmik mexanizmlarning to‘g‘ri tanlanishi va ularning o‘zaro uyg‘un ishlashi tizim xavfsizligi darajasini belgilovchi asosiy omillardan biri hisoblanadi.

Birinchi asosiy mexanizm shifrlash algoritmlaridan foydalanish bo‘lib, u metama'lumotlarni ruxsatsiz o‘qish va tahlil qilishdan himoyalashga xizmat qiladi. Shifrlash jarayonida metama'lumotlar kriptografik o‘zgartirishlar orqali tushunarsiz ko‘rinishga keltiriladi va faqat tegishli kalit mavjud bo‘lgandagina tiklanishi mumkin. Amaliyotda simmetrik (AES, ChaCha20) va assimetrik (RSA, ECC) shifrlash algoritmlari qo‘llaniladi. Simmetrik algoritmlar tezkorligi bilan ajralib tursa, assimetrik algoritmlar kalitlarni xavfsiz taqsimlash imkonini beradi.

Ikkinchi muhim algoritmik mexanizm kalitlarni boshqarish tizimlari hisoblanadi. Kalitlarni yaratish, saqlash, taqsimlash va yangilash jarayonlari noto‘g‘ri tashkil etilgan taqdirda, eng kuchli kriptografik algoritmlar ham samarasiz bo‘lib qolishi mumkin. Shu sababli zamonaviy axborot tizimlarida markazlashtirilgan yoki taqsimlangan kalitlarni boshqarish mexanizmlari qo‘llaniladi. Ushbu mexanizmlar metama'lumotlarni himoyalashda foydalaniladigan kriptografik kalitlarning xavfsizligini ta'minlaydi.

Uchinchi algoritmik mexanizm xesh-funksiyalar asosida yaxlitlikni nazorat qilishga qaratilgan. Xesh-algoritmlar yordamida metama'lumotlar uchun noyob raqamli iz hosil qilinadi va ushbu iz orqali metama'lumotlarning o‘zgartirilmaganligi tekshiriladi. Agar metama'lumotlar ruxsatsiz ravishda o‘zgartirilsa, xesh qiymatlarining mos kelmasligi aniqlanadi va bu xavfsizlik hodisasi sifatida qayd etiladi. Mazkur mexanizm metama'lumotlarning ishonchliligini ta'minlashda muhim rol o‘ynaydi.

To‘rtinchi mexanizm raqamli imzolar va autentifikatsiya algoritmlariga asoslanadi. Raqamli imzolar metama'lumotlarning muallifligini tasdiqlash va ularning soxtalashtirilishining oldini olish imkonini beradi. Bu mexanizm ayniqsa huquqiy ahamiyatga ega bo‘lgan elektron hujjatlar va rasmiy fayllar bilan ishlashda muhim hisoblanadi. Autentifikatsiya algoritmlari esa metama'lumotlarga faqat ruxsat etilgan foydalanuvchilarning kirishini ta'minlaydi.

Beshinchi mexanizm kriptografik himoyalashning gibrid algoritmik modellarida qo‘llanilishi bilan bog‘liq. Gibrid modellar simmetrik shifrlashning tezkorligi va assimetrik shifrlashning yuqori xavfsizlik darajasini birlashtiradi. Bu

ISSN 3030-3907

yondashuv metama'lumotlarni himoyalashda samaradorlik va ishonchlilik o'rtasidagi muvozanatni ta'minlashga xizmat qiladi.

Yuqorida keltirilgan algoritmik mexanizmlar kompleks tarzda qo'llanilganda, raqamli fayllar metama'lumotlarini himoyalashning yuqori darajasi ta'minlanadi. Shu bilan birga, ushbu mexanizmlarning samaradorligi tizim arxitekturasi, tahdid modeli va foydalanish muhiti bilan bevosita bog'liq bo'lib, ularni tanlash va moslashtirish ilmiy asoslangan yondashuvni talab etadi.

Kriptografik algoritmlar asosidagi yondashuvlarning afzalliklari va cheklovlari

Kriptografik algoritmlar metama'lumotlarni himoyalashda yuqori darajadagi xavfsizlikni ta'minlovchi asosiy texnologik yechimlardan biri hisoblanadi. Ushbu yondashuvlar metama'lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta'minlash imkonini bergan holda, turli axborot-kommunikatsiya muhitlarida qo'llanilishi bilan ajralib turadi. Biroq ularning samaradorligi faqat afzalliklar bilan emas, balki muayyan cheklovlar bilan ham belgilanadi.

Kriptografik yondashuvlarning eng muhim afzalliklaridan biri — yuqori darajadagi matematik asoslangan himoya mexanizmlariga ega ekanligidir. Zamonaviy shifrlash algoritmlari metama'lumotlarni ruxsatsiz o'qish, tahlil qilish va o'zgartirish ehtimolini minimal darajaga tushiradi. Ayniqsa, gibrid kriptografik modellar yordamida xavfsizlik va samaradorlik o'rtasida optimal muvozanatga erishish mumkin.

Shu bilan birga, kriptografik algoritmlarni joriy etish va ekspluatatsiya qilish jarayonida kalitlarni boshqarish, hisoblash resurslariga bo'lgan talab hamda tizim murakkabligining ortishi kabi muammolar yuzaga keladi. Bu holatlar, ayniqsa, cheklangan resurslarga ega bo'lgan muhitlarda (mobil va IoT tizimlari) sezilarli ahamiyat kasb etadi.

Quyidagi jadvalda kriptografik algoritmlar asosidagi yondashuvlarning asosiy afzalliklari va cheklovlari tizimli tarzda keltirilgan.

1-Jadval.

Kriptografik algoritmlar asosidagi yondashuvlarning afzalliklari va cheklovlari

Mezon	Afzalliklari	Cheklovlari
Xavfsizlik darajasi	Metama'lumotlarning yuqori darajada maxfiyligi va yaxlitligi ta'minlanadi	Kalit kompрometatsiyasi holatida xavfsizlik pasayadi
Algoritmik ishonchlilik	Matematik jihatdan asoslangan va isbotlangan algoritmlar qo'llaniladi	Murakkab algoritmlar noto'g'ri sozlansa,

ISSN 3030-3907

		zaifliklar yuzaga kelishi mumkin
Moslashuvchanlik	Turli tizim va platformalarga integratsiya qilish imkoniyati mavjud	Integratsiya jarayoni qo‘shimcha xarajat va vaqt talab qiladi
Unumdorlik	Simmetrik algoritmlar yuqori tezlikda ishlaydi	Assimetrik algoritmlar hisoblash resurslarini ko‘p talab qiladi
Amaliy qo‘llanish	Davlat, korporativ va bulutli tizimlarda keng qo‘llaniladi	IoT va mobil muhitlarda optimallashtirish zarur

Kriptografik algoritmlar asosidagi yondashuvlar metama’lumotlarni himoyalashda eng ishonchli va universal yechimlardan biri hisoblanadi. Ular axborot-kommunikatsiya tizimlarida yuqori xavfsizlik talablarini qondiradi va metama’lumotlar orqali yuzaga keladigan tahdidlarni samarali kamaytiradi. Shu bilan birga, mazkur yondashuvlarni qo‘llashda tizim resurslari, kalitlarni boshqarish va ishlash muhitining xususiyatlarini hisobga olish zarur. Aynan shu omillar keyingi bo‘limda ko‘rib chiqiladigan metama’lumotlarni minimallashtirish va anonimlashtirish algoritmik yondashuvlarini qo‘llash zaruratini yuzaga keltiradi.

Metama’lumotlarni minimallashtirish va anonimlashtirish algoritmlari

Minimallashtirish va anonimlashtirish yondashuvi metama’lumotlarni shifrlashdan ko‘ra, ularning xavf tug‘diruvchi qismini aniqlash, kamaytirish yoki shaxsni identifikatsiya qilmaydigan ko‘rinishga keltirishga asoslanadi. Bu yondashuv ayniqsa fayllar ochiq muhitga chiqariladigan holatlarda (veb platforma, ijtimoiy tarmoqlar, ochiq elektron arxivlar, ilmiy almashinuv) juda muhim: foydalanuvchi fayl mazmunini tekshirsa ham, ko‘pincha metama’lumotlar orqali maxfiy detallar oshkor bo‘lib qoladi.

Minimallashtirish algoritmlari quyidagi mantiqda ishlaydi: avvalo fayl formatiga mos ravishda metama’lumotlar ajratib olinadi (aniqlash), keyin atributlar xavf darajasi bo‘yicha tasniflanadi (masalan: “yuqori xavf – o‘rta – past”), so‘ng keraksiz yoki xavfli atributlar o‘chirib tashlanadi. Masalan, “muallif”, “tahrir tarixi”, “lokatsiya”, “dastur versiyasi” kabi atributlar ochiq tarqatiladigan fayllarda ko‘pincha olib tashlanadi.

Anonimlashtirish esa metama’lumotni butunlay o‘chirmasdan, uni foydalanuvchini aniqlab bo‘lmaydigan darajada o‘zgartiradi. Bunda:

- umumlashtirish (aniq sana o‘rniga oy/yil),
- maskalash (identifikatorning bir qismini yashirish),
- psevdonimlashtirish (real identifikatorni sun’iy identifikatorga almashtirish),

ISSN 3030-3907

- shovqin qo‘shish (statistik tahlilni qiyinlashtirish) abi usullar qo‘llanadi.

Afzalligi shundaki, bu yondashuv tezkor, resurs talab qilmaydi va “ochiq muhitda xavfni kamaytirish” uchun juda qulay. Cheklovi esa — ayrim vaziyatlarda metama’lumotlarni bilvosita manbalar orqali qayta tiklash ehtimoli saqlanib qoladi (masalan, fayl nomlash uslubi, versiya tarixi boshqa tizim loglarida qolishi va h.k.). Shuning uchun minimallashtirish/anonimlashtirish ko‘pincha kriptografiya bilan birga qo‘llanadi.

GIBRID ALGORITMIK MODELLAR

Gibrid algoritmik modellar — metama’lumotlarni himoyalashda eng amaliy va ko‘p qatlamli yondashuv bo‘lib, u kriptografik himoya va metama’lumotlarni boshqarish/minimallashtirish mexanizmlarini yagona modelga integratsiyalashga asoslanadi. Bu modelning ustunligi shundaki, u turli tahdid ssenariylari uchun “bitta yo‘l” bilan emas, balki xavf darajasiga mos moslashuvchan himoya bilan javob beradi.

Gibrid model odatda quyidagi bosqichlarda quriladi:

1. Metama’lumotlarni ajratib olish va klassifikatsiya (qaysi atributlar mavjud?)
2. Xavf baholash (qaysi atributlar oshkor bo‘lsa qanday zarar?)
3. Himoya strategiyasini tanlash:
4. ba’zilari o‘chiriladi (minimallashtirish),
5. ba’zilari anonimlashtiriladi,
6. eng muhimlari shifrlanadi yoki imzolanadi.

Audit/monitoring: metama’lumot o‘zgargan-o‘zgarmaganligini tekshirish, log yuritish.

Gibrid yondashuv korporativ va davlat axborot tizimlarida, bulutli saqlash infratuzilmasida, elektron hujjat aylanishida ayniqsa samarali, chunki u “ham xavfsizlik, ham funksionallik” talablarini muvozanatlashtiradi. Cheklovi esa — modelni joriy etish murakkabligi: siyosatlar (policy)ni to‘g‘ri belgilash, standartlarga moslashtirish, tizimlararo moslik, foydalanuvchi rollari va ruxsatlarini to‘g‘ri konfiguratsiya qilish talab etiladi.

Intellektual va adaptiv algoritmlar

Intellektual va adaptiv algoritmlar metama’lumotlar xavfsizligini ta’minlashda sun’iy intellekt/mashinali o‘rganish yondashuvlariga tayanib, tahdidlarni oldindan aniqlash, anomaliyani topish va himoya parametrlarini real vaqt rejimida moslashtirish imkonini beradi. An’anaviy yondashuvlarda ko‘p narsa “qoidalar”ga (rule-based) bog‘liq bo‘lsa, intellektual yondashuvlar ma’lumotlar oqimini o‘rganib, xavfli holatlarni avtomatik topishga harakat qiladi.

Bu algoritmlar quyidagi vazifalarda samarali:

ISSN 3030-3907

- metama’lumotdagi g‘ayrioddiy o‘zgarishlarni aniqlash (masalan, muallif maydoni kutilmagan qiymatga o‘zgargan);
- “normal profil”dan chetga chiqishni topish (masalan, bir xil turdagi fayllar odatda bitta dasturda yaratiladi, birdan boshqa muhit paydo bo‘ladi);
- foydalanuvchi xatti-harakati bilan metama’lumotlar o‘rtasidagi nomuvofiqlikni aniqlash.

Adaptivlik shundan iboratki, tizim xavf darajasi oshganda (masalan, tashqi tarmoqdan kirish ko‘payganda) metama’lumotlarni himoyalash darajasini kuchaytirishi mumkin: masalan, anonimlashtirishdan shifrlashga o‘tish, audit chastotasini oshirish, qo‘shimcha autentifikatsiya talab qilish. Ushbu yondashuv ayniqsa katta hajmdagi ma’lumotlar bilan ishlovchi muhitlarda foydali, chunki qo‘lda nazorat qilish qiyin bo‘ladi.

Cheklovlari ham mavjud: sifatli model uchun ma’lumotlar (dataset) kerak bo‘ladi, noto‘g‘ri sozlangan model false positive/false negative holatlarini keltirib chiqarishi mumkin, shuningdek izohlanish (explainability) talabi yuqori bo‘lgan tizimlarda “nega bu holat xavfli deb topildi?” savoliga asosli javob berish muhim.

TAHLIL NATIJALARI

Keltirilgan tahlillar shuni ko‘rsatadiki, metama’lumotlarni himoyalashda yagona universal algoritm mavjud emas. Har bir yondashuv muhit, tahdid modeli va resurs imkoniyatlariga bog‘liq. Masalan, ochiq muhitda tezkor tarqatiladigan fayllar uchun minimallashtirish/anonimlashtirish yetarli bo‘lishi mumkin, lekin huquqiy yoki strategik ahamiyatga ega hujjatlarda kriptografik himoya talab etiladi. Katta korporativ tizimlarda esa ko‘p hollarda gibrid model eng oqilona tanlov bo‘lib, intellektual algoritmlar monitoring va moslashuvchanlikni kuchaytiradi.

Shu nuqtai nazardan, istiqbolli yechim sifatida integratsiyalashgan (gibrid) va adaptiv (AI-assisted) modellar ajralib turadi. Ular nafaqat himoyani kuchaytiradi, balki xavf dinamik o‘zgarganda ham tizimni moslashtirish imkonini beradi.

XULOSA

Raqamli fayllar metama’lumotlarini himoyalash axborot-kommunikatsiya tizimlarida xavfsizlikni ta’minlashning muhim yo‘nalishlaridan biri hisoblanadi. Metama’lumotlar ko‘pincha mazmunga nisbatan “ko‘rinmas” bo‘lsa-da, amaliy jihatdan ko‘plab tahdidlarning boshlang‘ich nuqtasi bo‘lib xizmat qiladi. Zamonaviy algoritmik yondashuvlar kriptografik himoya, minimallashtirish va anonimlashtirish, gibrid modellar hamda intellektual/adaptiv usullar metama’lumotlarning maxfiyligi, yaxlitligi va boshqaruvini ta’minlashga qaratilgan.

ISSN 3030-3907

Tadqiqot mantiqiy natijasi sifatida shuni aytish mumkinki, gibrid va intellektual yondashuvlarning integratsiyasi metama'lumotlar xavfsizligini sezilarli darajada oshiradi. Kelgusida algoritmlarni resurs jihatidan optimallashtirish, real tizimlarga moslash, hamda riskga asoslangan boshqaruv (risk-based policy) mexanizmlarini takomillashtirish bo'yicha izlanishlar olib borish maqsadga muvofiqdir.

FOYDALANILGAN ADABIYOTLAR

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, Geneva, 2022.
2. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology, USA, 2020.
3. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed., Pearson Education, 2023.
4. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd ed., Wiley, New York, 2015.
5. Garfinkel S. L. Metadata anonymization: A survey of problems and techniques // IEEE Security & Privacy. Vol. 13, No. 3, 2015. – pp. 12–20.
6. Narayanan A., Shmatikov V. Robust de-anonymization of large sparse datasets // Proceedings of the IEEE Symposium on Security and Privacy. IEEE, 2008. – pp. 111–125.
7. Dwork C., Roth A. The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science, Vol. 9, No. 3–4, 2014.
8. Agrawal R., Srikant R. Privacy-preserving data mining // ACM SIGMOD Record. Vol. 29, No. 2, 2000. – pp. 439–450.
9. Zhou B., Pei J. Preserving privacy in social networks against neighborhood attacks // Proceedings of the IEEE International Conference on Data Engineering. IEEE, 2008. – pp. 506–515.
10. Al-Fedaghi S., Alsumait A. Metadata management and security issues in digital information systems // Journal of Information Security. Vol. 9, No. 2, 2018. – pp. 89–102.
11. Sodiqova D. J. Integration of Cryptographic Models and Network Security Algorithms for Protecting Metadata in Digital Documents // Scientific Journal of Research and Education. Vol. 3, Issue 4, 2024. – pp. 151–153.
12. Chen M., Mao S., Liu Y. Big data: A survey // Mobile Networks and Applications. Vol. 19, No. 2, 2014. – pp. 171–209.

ISSN 3030-3907

13. Buczak A. L., Guven E. A survey of data mining and machine learning methods for cybersecurity intrusion detection // IEEE Communications Surveys & Tutorials. Vol. 18, No. 2, 2016. – pp. 1153–1176.
14. Goodfellow I., Bengio Y., Courville A. Deep Learning. MIT Press, Cambridge, MA, 2016.
15. Kahn R., Wilensky R. A framework for distributed digital object services // International Journal on Digital Libraries. Vol. 6, No. 2, 2006. – pp. 115–123.

ISSN 3030-3907