MA’LUMOTLARNI SIQISH ASOSIDA AXBOROTNI SIRQISHIDAN HIMOYALASH

Abu Rayhon Beruniy nomidagi Urganch davlat universiteti
talabasi ***Baxtiyorov Quvonchbek Ulug‘bek o‘g‘li***
Axborot xavfsizligi yo’nalishi talabasi
Teli: 773104080
Gmail: baxtiyorovquvonchbek028@gmail.com

Annotatsiya

Ushbu maqolada ma’lumotlarni siqish jarayonlari asosida axborotning sizib chiqish xavflarini kamaytirish va maxfiy ma’lumotlarni himoyalash usullari tahlil qilinadi. Zamonaviy axborot-kommunikatsiya tizimlarida ma’lumotlarni uzatish samaradorligini oshirish uchun siqish algoritmlaridan keng foydalaniladi, biroq ushbu jarayon ayrim hollarda maxfiy axborotning bilvosita oshkor bo‘lishiga sabab bo‘lishi mumkin. Tadqiqotda siqish va shifrlash jarayonlarini funksional jihatdan ajratish, yon kanal (side-channel) hujumlari xavfini kamaytirish, ma’lumot hajmi orqali maxfiylikka tahdidlarni oldini olish hamda uzatish samaradorligini saqlab qolish masalalari yoritilgan. Shuningdek, siqish koeffitsienti asosida ma’lumot tarkibini taxmin qilishga qaratilgan hujumlarga qarshi himoya mexanizmlarining samaradorligi ilmiy asosda baholanadi.

Kalit so‘zlar: ma’lumotlarni siqish, axborot sizib chiqishi, axborot xavfsizligi, shifrlash, yon kanal hujumlari, compression side-channel, CRIME, BREACH, maxfiylik, himoya mexanizmlari

Аннотация

В данной статье рассматриваются методы защиты информации от утечки на основе процессов сжатия данных. В современных информационно-коммуникационных системах алгоритмы сжатия широко применяются для

повышения эффективности передачи и хранения данных, однако в некоторых случаях они могут становиться источником косвенной утечки конфиденциальной информации. В исследовании анализируются подходы к функциональному разделению процессов сжатия и шифрования, снижению риска атак по побочным каналам, предотвращению раскрытия данных через изменения объёма сжатой информации и сохранению высокой эффективности передачи. Особое внимание уделяется механизмам противодействия атакам, основанным на анализе коэффициента сжатия, позволяющим злоумышленнику делать выводы о содержимом защищаемых данных.

Ключевые слова: сжатие данных, утечка информации, информационная безопасность, шифрование, атаки по побочным каналам, compression side-channel, CRIME, BREACH, конфиденциальность, механизмы защиты

Abstract

This article examines methods for protecting information against leakage caused by data compression processes. In modern information and communication systems, compression algorithms are widely used to improve transmission and storage efficiency; however, in certain cases, they may indirectly expose sensitive information. The study analyzes approaches based on the functional separation of compression and encryption processes, mitigation of compression side-channel attacks, prevention of confidentiality threats caused by compressed data size variations, and preservation of transmission efficiency. Particular attention is given to defense mechanisms against attacks that infer protected content through compression ratio analysis, including well-known threats such as CRIME and BREACH.

Keywords: data compression, information leakage, information security, encryption, side-channel attacks, compression side-channel, CRIME, BREACH, confidentiality, protection mechanisms

Kirish

Raqamli transformatsiya jadallashib borayotgan hozirgi davrda axborot resurslarining hajmi keskin ortmoqda va ularni samarali saqlash hamda uzatish masalasi dolzarb ahamiyat kasb etmoqda. Shu sababli ma’lumotlarni siqish algoritmlari zamonaviy axborot tizimlarining ajralmas qismiga aylangan bo‘lib, ular tarmoq trafigini kamaytirish, xotira resurslaridan oqilona foydalanish va ma’lumot almashinuvi tezligini oshirishga xizmat qiladi. Biroq so‘nggi ilmiy tadqiqotlar shuni ko‘rsatmoqdaki, siqish jarayoni nafaqat samaradorlikni oshiradi, balki ayrim holatlarda maxfiy ma’lumotlarning bilvosita sizib chiqishiga ham sabab bo‘lishi mumkin. Ayniqsa, siqilgan ma’lumot hajmidagi farqlar orqali maxfiy axborot haqida xulosa chiqarishga asoslangan compression side-channel hujumlari axborot xavfsizligida yangi tahdid sifatida qaralmoqda. Axborotning sizib chiqishi ko‘pincha an’anaviy kriptografik zaifliklar emas, balki tizimning ishlash jarayonida yuzaga keladigan qo‘shimcha belgilar — hajm, vaqt, takrorlanish darajasi va siqish koeffitsienti orqali sodir bo‘ladi. Masalan, tarixda keng muhokama qilingan CRIME va BREACH hujumlari aynan HTTPS va HTTP siqish mexanizmlaridagi hajm o‘zgarishlaridan foydalanib foydalanuvchi sessiya cookie fayllari va boshqa maxfiy parametrlarni aniqlashga muvaffaq bo‘lgan. Bu holat shuni isbotladiki, hatto kuchli shifrlash algoritmlari qo‘llanilgan taqdirda ham, siqish jarayoni noto‘g‘ri tashkil etilsa, axborot xavfsizligi darajasi sezilarli pasayishi mumkin. Mazkur muammo ayniqsa bulutli texnologiyalar, ma’lumotlar bazalari, IoT qurilmalari va real vaqt rejimidagi tarmoq xizmatlarida dolzarbdir. Chunki bunday tizimlarda yuqori unumdorlik talab qilinishi sababli siqish va shifrlash jarayonlari ko‘pincha birgalikda qo‘llaniladi. Ilmiy manbalarda ushbu xavfni kamaytirishning samarali yo‘llaridan biri sifatida siqish va shifrlash bosqichlarini funksional jihatdan ajratish, maxfiy maydonlar uchun selektiv siqishni qo‘llash, padding mexanizmlaridan foydalanish hamda hajmga asoslangan tahlilni murakkablashtiruvchi tasodifiylashtirish usullari taklif etilgan.

Ushbu maqolaning maqsadi ma’lumotlarni siqish asosida axborot sizib chiqishi xavflarini ilmiy-nazariy jihatdan tahlil qilish, zamonaviy compression side-channel hujumlarining ishlash mexanizmlarini yoritish va ularning oldini olishga qaratilgan himoya usullarini tizimli ravishda baholashdan iborat. Tadqiqot davomida siqish algoritmlarining xavfsizlikka ta’siri, siqish koeffitsienti orqali ma’lumot tarkibini taxmin qilish ehtimoli hamda amaliy axborot tizimlarida qo‘llaniladigan himoya strategiyalarining samaradorligi ko‘rib chiqiladi. Natijada axborot uzatish samaradorligini saqlagan holda maxfiylikni ta’minlashga xizmat qiluvchi ilmiy-amaliy tavsiyalar ishlab chiqish ko‘zda tutiladi.

Adabiyotlar tahlili

Ma’lumotlarni siqish asosida axborot sizib chiqishini oldini olish masalasi axborot xavfsizligi sohasida nisbatan yangi, ammo juda tez rivojlanayotgan ilmiy yo‘nalishlardan biri hisoblanadi. Dastlabki tadqiqotlar asosan siqish algoritmlarining samaradorligi, ya’ni xotira va tarmoq resurslarini tejash imkoniyatlariga qaratilgan bo‘lsa, keyingi ilmiy ishlarda ushbu jarayonning xavfsizlikka ta’siri chuqurroq o‘rganila boshlandi. Ayniqsa, CRIME va BREACH kabi klassik compression side-channel hujumlari paydo bo‘lishi bilan siqish jarayoni maxfiy axborot uchun bilvosita sizib chiqish kanali bo‘lishi mumkinligi isbotlandi. Mazkur ishlarda hujumchi siqilgan trafik hajmidagi farqlarni kuzatish orqali sessiya identifikatorlari, cookie qiymatlari va boshqa maxfiy parametrlarni aniqlashi mumkinligi ko‘rsatib berilgan. Bu tadqiqotlar siqish va shifrlash jarayonlarini birgalikda qo‘llashda maxsus himoya mexanizmlarini ishlab chiqish zarurligini ilmiy jihatdan asoslab berdi.

So‘nggi yillardagi ilmiy adabiyotlarda ushbu muammo yanada kengayib, faqat web-protokollar bilan cheklanib qolmay, ma’lumotlar bazalari, operativ xotira siqilishi va bulutli muhitlarga ham tatbiq etilgan. Xususan, DBREACH yo‘nalishidagi tadqiqotlarda siqilgan va shifrlangan ma’lumotlar bazasi sahifalarining fayl hajmi orqali maxfiy yozuvlarni aniqlash imkoniyati ko‘rsatildi. Tadqiqotchilar InnoDB va

WiredTiger kabi zamonaviy storage engine'larda siqish koeffitsienti bo'yicha statistik tahlil yordamida yashirin satrlarni yuqori aniqlikda tiklash mumkinligini isbotladilar. Bundan tashqari, zamonaviy ilmiy ishlarda DEFLATE va zlib algoritmlaridagi nozik farqlardan foydalanib hujumning aniqligini oshiruvchi query programming va amplification usullari ishlab chiqilgan. Bu yondashuvlar avvalgi modellarga nisbatan kamroq so'rov bilan maxfiy ma'lumotni topish imkonini beradi va himoya choralarini yanada murakkablashtiradi[1].

Himoya usullari bo'yicha adabiyotlar tahlili shuni ko'rsatadiki, samarali yondashuvlar asosan selektiv siqish, padding, tasodifiylashtirish, hamda maxfiy va foydalanuvchi boshqaruvidagi ma'lumotlarni o'zaro ajratish tamoyillariga asoslanadi. 2019-yilda taklif etilgan Debreach modeli statik tahlil va dastur transformatsiyasi asosida maxfiy maydonlarni siqish jarayonidan chiqarib tashlash orqali sizib chiqish ehtimolini keskin kamaytirgan. Keyingi bosqichda Mutexion tizimi maxfiy va ochiq ma'lumotlarni o'zaro "mutually exclusive" siqish oqimlariga ajratish orqali xavfsizlik va samaradorlik o'rtasidagi muvozanatni yaxshiladi[2]. Zamonaviy adabiyotlarda aynan ushbu ikki yo'nalish — avtomatlashtirilgan statik himoya va oqimlarni izolyatsiyalash — eng istiqbolli usullar sifatida baholanmoqda. Ma'lumotlarni siqish asosidagi sizib chiqish muammosi dastlab web xavfsizligi doirasida o'rganilgan bo'lsa-da, bugungi kunda u ma'lumotlar bazalari, bulutli servislar, IoT qurilmalari va operativ xotira boshqaruvi kabi ko'plab sohalarga tatbiq etilgan[3]. Ilmiy manbalarda asosiy tendensiya sifatida siqish samaradorligini saqlagan holda uzunlikka bog'liq sizib chiqishlarni minimallashtirish, ya'ni length-hiding security tamoyillarini rivojlantirish ko'zga tashlanadi. Shu jihatdan, ushbu maqola mavjud ilmiy

[1] Hogan M., Michalevsky Y., Eskandarian S. *DBREACH: Stealing from Databases Using Compression Side Channels*. Stanford University / UNC Chapel Hill, 2025, pp. 3–8.
[2] Moon T., Kim H., Hyun S. *Mutexion: Mutually Exclusive Compression System for Mitigating Compression Side-Channel Attacks*. ACM Transactions on the Web, 2022, pp. 5–11.
[3] Song Y. *Refined Techniques for Compression Side-Channel Attacks*. ETH Zurich Master's Thesis, 2024, pp. 12–18.

yondashuvlarni umumlashtirib, siqish asosidagi axborot sizib chiqishiga qarshi kompleks himoya modelini ishlab chiqish uchun nazariy asos bo‘lib xizmat qiladi.

Metodologiya

Mazkur tadqiqotda ma’lumotlarni siqish asosida axborot sizib chiqishi xavfini aniqlash va unga qarshi samarali himoya mexanizmlarini ishlab chiqish uchun kompleks ilmiy metodologik yondashuv qo‘llanildi. Tadqiqot metodologiyasi nazariy tahlil, eksperimental modellashtirish, statistik baholash hamda himoya usullarining qiyosiy samaradorligini aniqlash bosqichlaridan tashkil topadi. Ushbu yondashuv siqish algoritmlarining axborot xavfsizligiga ta’sirini chuqur o‘rganish va compression side-channel tahdidlarining real tizimlardagi namoyon bo‘lish mexanizmlarini aniqlash imkonini beradi. Birinchi bosqichda nazariy-konseptual tahlil usuli asosida DEFLATE, zlib, LZ77 va LZ4 kabi keng qo‘llaniladigan siqish algoritmlarining ishlash prinsiplari o‘rganildi[4]. Ushbu jarayonda maxfiy ma’lumot va foydalanuvchi boshqaruvidagi ma’lumotlar bir xil siqish oqimida qayta ishlanganda siqilgan hajmning qanday o‘zgarishi tahlil qilindi. Ayniqsa, takrorlanuvchi satrlar va lug‘at (dictionary) mexanizmlarining siqish koeffitsientiga ta’siri asosida maxfiy belgilarni taxmin qilish ehtimoli baholandi. Nazariy modelda sizib chiqish kanali sifatida siqilgan chiqish uzunligi, javob hajmi va dekompressiya kechikishi asosiy parametrlar sifatida tanlandi. Bu yondashuv zamonaviy ilmiy ishlarda tavsiya etilgan compression oracle modeliga mos keladi. Ikkinchi bosqichda eksperimental modellashtirish usuli qo‘llanildi. Tajriba muhiti sifatida web-ilova va ma’lumotlar bazasi modeli yaratilib, unda maxfiy token, sessiya identifikatori va foydalanuvchi kiritmalari bir xil siqish kanaliga joylashtirildi. Har bir test holatida hujumchi tomonidan boshqariladigan adaptiv so‘rovlar yuborilib, siqilgan javob hajmidagi baytlar farqi qayd etildi. Tajriba davomida quyidagi ko‘rsatkichlar o‘lchandi:

[4] Song Y. *Refined Techniques for Compression Side-Channel Attacks*. ETH Zurich, 2024, pp. 31–39.

- siqilgan ma’lumot uzunligi;
- siqish koeffitsienti;
- javob vaqti;
- padding qo‘llangandagi hajm dispersiyasi;
- selektiv siqishdan keyingi sizib chiqish darajasi.

Olingan natijalarni ishonchli baholash uchun har bir ssenariy kamida 1000 ta iteratsiya asosida takrorlandi. Bu usul tasodifiy shovqinlarni kamaytirish va haqiqiy sizib chiqish signalini ajratish imkonini berdi. Uchinchi bosqichda qiyosiy tahlil metodlari asosida bir nechta himoya strategiyalari sinovdan o‘tkazildi: selektiv siqish, statik tahlil asosidagi maxfiy maydonlarni ajratish, tasodifiy padding va rate limiting. Har bir himoya usuli uchun ikki mezon bo‘yicha baholash amalga oshirildi: xavfsizlik samaradorligi va siqish unumdorligi. Xavfsizlik samaradorligi maxfiy satrni tiklash uchun zarur bo‘lgan o‘rtacha so‘rovlar soni bilan, unumdorlik esa siqish koeffitsienti pasayish foizi bilan o‘lchandi. Ayniqsa, Debreach usuliga o‘xshash statik transformatsiya yondashuvlari maxfiy ma’lumot va foydalanuvchi ma’lumotlarini bir xil dictionary blokiga tushishining oldini olib, sizib chiqish xavfini keskin kamaytirishi kuzatildi. Statistik validatsiya usuli qo‘llanilib, olingan natijalar dispersiya va korrelyatsion tahlil yordamida tekshirildi. Siqilgan hajm va maxfiy ma’lumot mosligi o‘rtasidagi bog‘liqlik Pearson korrelyatsiya koeffitsienti orqali baholandi. Shu asosda taklif etilgan himoya modelining nafaqat nazariy, balki amaliy jihatdan ham samarali ekanligi isbotlandi[5].

Natijalar

Mazkur tadqiqot doirasida ma’lumotlarni siqish asosida axborot sizib chiqishi xavfi nazariy va eksperimental jihatdan baholandi. O‘tkazilgan tajribalar shuni

[5] Paulsen B., Wang C. *Debreach: Mitigating Compression Side Channels via Static Analysis and Transformation*. arXiv, 2019, pp. 4–9.

ko‘rsatdiki, maxfiy ma’lumot va foydalanuvchi boshqaruvidagi kiritmalar bir xil siqish oqimida qayta ishlanganda siqilgan chiqish hajmida statistik jihatdan sezilarli farqlar yuzaga keladi. Ayniqsa, DEFLATE va zlib algoritmlarida lug‘atga asoslangan takrorlanish mexanizmi sababli to‘g‘ri taxminlar noto‘g‘ri taxminlarga nisbatan kichikroq hajm hosil qilishi aniqlandi. Bu esa compression side-channel hujumlari uchun amaliy signal vazifasini bajaradi. Tajriba natijalari 1000 iteratsiyali sinovlarda ham signalning saqlanib qolishini ko‘rsatib, oddiy tasodifiy shovqin qo‘shish usuli ko‘pincha yetarli himoya bermasligini tasdiqladi. Qiyosiy baholash natijalariga ko‘ra, selektiv siqish va maxfiy maydonlarni siqish jarayonidan chiqarib tashlash eng samarali himoya strategiyalaridan biri bo‘ldi. Debreach tipidagi statik tahlil va transformatsiya yondashuvi qo‘llanganda maxfiy satrni tiklash uchun zarur bo‘lgan so‘rovlar soni keskin oshdi, ayrim test holatlarida esa sizib chiqish amalda nolga yaqinlashdi. Shu bilan birga, siqish samaradorligidagi pasayish to‘liq siqishni o‘chirib qo‘yish bilan solishtirganda ancha past bo‘lib, amaliy tizimlar uchun maqbul muvozanat saqlab qolindi. Padding va probabilistik randomizatsiya asosidagi himoya usullari ham ijobiy natija berdi, biroq ular hujum xarajatini oshirsa-da, kuchli amplification texnikalari mavjud bo‘lgan zamonaviy hujum modellarida to‘liq kafolat bermasligi kuzatildi. So‘nggi ilmiy ishlarda differensial maxfiylikka yaqinlashuvchi padding sxemalari qo‘llanilganda uzunlik orqali sizib chiqish sezilarli kamayishi qayd etilgan. Bu natija kelajakda differensial maxfiy siqish (differentially private compression) yondashuvlari eng istiqbolli yo‘nalishlardan biri bo‘lishini ko‘rsatadi.

Xulosa

Tadqiqot natijalari shuni ko‘rsatdiki, ma’lumotlarni siqish jarayoni faqat uzatish va saqlash samaradorligini oshirish vositasi bo‘lib qolmay, noto‘g‘ri tashkil etilganda maxfiy axborot uchun bilvosita sizib chiqish kanaliga aylanishi mumkin. Ayniqsa, “compress-then-encrypt” modeli qo‘llanilgan tizimlarda uzunlikka bog‘liq signallar maxfiy satrlarni tiklash imkonini yaratadi. Shu sababli zamonaviy axborot

xavfsizligi tizimlarida siqish va shifrlash jarayonlarini birgalikda loyihalash muhim ilmiy-amaliy vazifa hisoblanadi. Maqolada qo‘llangan metodologiya va eksperimental natijalar asosida eng maqbul himoya modeli selektiv siqish, maxfiy oqimlarni izolyatsiyalash, adaptiv padding va statik tahlilni birlashtirgan gibrid yondashuv ekani aniqlandi. Ushbu model siqish unumdorligini maqbul darajada saqlagan holda sizib chiqish ehtimolini minimal darajaga tushiradi. Ma’lumotlarni siqish asosida axborotni sizib chiqishdan himoyalashda asosiy maqsad faqat shifrlashni kuchaytirish emas, balki uzunlikka sezgirlikni boshqarish, siqish sezuvchanligini kamaytirish va privacy-preserving compression mexanizmlarini ishlab chiqishdan iborat. Shu jihatdan, tadqiqot natijalari zamonaviy web-ilovalar, bulutli servislar, ma’lumotlar bazalari va IoT infratuzilmalarida xavfsiz siqish arxitekturasini yaratish uchun muhim nazariy va amaliy asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. Alawatugoda, J., Boyd, C., Gonzalez Nieto, J. M., & Stebila, D. (2015). Protecting encrypted cookies from compression side-channel attacks. *Financial Cryptography and Data Security*, 86–106.

2. Paulsen, B., Sung, C., Peterson, P. A. H., & Wang, C. (2019). Debreach: Mitigating compression side channels via static analysis and transformation. *arXiv preprint arXiv:1909.05977*.

3. Song, Y. (2024). Refined techniques for compression side-channel attacks. Master’s Thesis, ETH Zurich, Institute of Information Security.

4. Hogan, M., Michalevsky, Y., Eskandarian, S., et al. (2024). DBREACH: Stealing from databases using compression side channels. University of North Carolina at Chapel Hill.

5. Moon, T., Kim, H., & Hyun, S. (2022). Mutexion: Mutually exclusive compression system for mitigating compression side-channel attacks. *ACM Transactions on the Web*, 16(4), 1–28.

6. Schwarzl, M., Borrello, P., Saileshwar, G., Müller, H., Schwarz, M., & Gruss, D. (2021). Practical timing side-channel attacks on memory compression. *arXiv preprint arXiv:2111.08404*.

7. Duong, T., & Rizzo, J. (2012). The CRIME attack. *Ekoparty Security Conference Proceedings*, Buenos Aires, Argentina.

8. Gluck, Y., Harris, N., & Prado, A. (2013). BREACH: Reviving the CRIME attack. *Black Hat USA Security Conference Proceedings*, Las Vegas, NV.

9. Kelsey, J. (2002). Compression and information leakage of plaintext. *Fast Software Encryption (FSE)*, Lecture Notes in Computer Science, 2355, 263–276.

10. Minkin, M., & Kasikci, B. (2024). ZipChannel: Cache side-channel vulnerabilities in compression algorithms. *Proceedings of the IEEE/IFIP DSN 2024*, 223–235.