

VEB-ILOVA ORQALI FAYL HASH QIYMATLARINI SOLISHTIRISH VA XAVFSIZLIKNI KUCHAYTIRISH YO'LLARI

Qurbonov Abduxalim Choriyevich

+998996838383

Annotatsiya: *Ushbu maqola SHA-256 hash algoritmiga asoslangan fayl yaxlitligini tekshirish uchun veb-ilova yaratishga qaratilgan. Foydalanuvchilar ikki faylning hash qiymatlarini solishtirib, ularning mosligini aniqlay oladilar. Ko'p tilli interfeys (o'zbek, ingliz, rus, qoraqalpoq) esa foydalanishni osonlashtiradi. Loyiha ma'lumot xavfsizligi va foydalanuvchi maxfiyligini ta'minlashga xizmat qiladi.*

Kalit so'zlar: *SHA-256, hash algoritmi, fayl yaxlitligi, kriptografiya, veb-ilova, ko'p tilli interfeys, ma'lumot xavfsizligi, fayl solishtirish, foydalanuvchi maxfiyligi.*

Abstract: *This article focuses on the development of a web application for verifying file integrity based on the SHA-256 hash algorithm. Users can compare the hash values of two files to determine their consistency. The multilingual interface (Uzbek, English, Russian, and Karakalpak) facilitates ease of use. The project aims to ensure data security and user privacy.*

Keywords: *SHA-256, hash algorithm, file integrity, cryptography, web application, multilingual interface, data security, file comparison, user privacy.*

Fayl yaxlitligini tekshirish zamonaviy axborot xavfsizligi sohasining eng dolzarb va strategik jihatlaridan biri hisoblanadi. Axborot texnologiyalarining keskin rivojlanishi, raqamli transformatsiya jarayonlarining tezlashuvi va global tarmoqlar orqali ma'lumotlar almashinuvining kengayib borishi natijasida ma'lumotlar o'zgarmasligini saqlash masalasi tobora ko'proq e'tibor talab qilmoqda. Ayniqsa, axborot resurslarining ko'pligi va ularning tezkor aylanishi sharoitida har qanday ma'lumot, xoh u shaxsiy fayl, muhim hujjat, moliyaviy hisobot yoki maxfiy axborot bo'lsin o'zining asl holatida, o'zgartirilmagan shaklda saqlanishi muhim ahamiyat kasb etadi.

Kompyuter tarmoqlari orqali amalga oshiriladigan uzatishlar, shuningdek, bulutli texnologiyalar asosida tashkil etilgan saqlash tizimlari, foydalanuvchilarga ma'lumotlardan istalgan joyda va vaqtda foydalanish imkonini bersa-da, ayni vaqtda ularni ruxsatsiz o'zgartirishlar, zararli dasturlar, tashqi xakerlik hujumlari va texnik nosozliklar orqali buzib qo'yish xavfi ham ortadi. Shunday holatlarda axborot resursining yaxlitligini, ya'ni uning o'zgarishsiz, asl holatda saqlanayotganligini aniqlash va nazorat qilish imkoniyatiga ega bo'lish katta ahamiyatga ega. Bu texnologik ehtiyojlar fonida, mustahkam algoritmlarga asoslangan, ishonchli va qulay dasturiy yechimlar ishlab chiqilishi dolzarb muammoga aylangan.

Fayl yaxlitligi deganda, eng avvalo, uning mazmuni, ichki tuzilmasi va atributlari o'zgarishsiz, to'liq va buzilmagan holatda saqlanayotganligi tushuniladi. Bu holatga erishish axborot tizimining ishonchliligini, ma'lumotlar ishonchliligi darajasini va

foydalanuvchi hamda tizim o'rtasidagi o'zaro ishonchni ta'minlaydi. Aksincha, agar biror faylga uchinchi tomon aralashuvi sodir bo'lgan bo'lsa, ya'ni u noto'g'ri o'zgartirilgan, ma'lumotlar yo'qotilgan, virus bilan zararlangan yoki zararli kodlar kiritilgan bo'lsa, bu holat fayl yaxlitligining buzilganini anglatadi. Bu esa o'z navbatida, tizimning umumiy xavfsizlik darajasini pasaytiradi va foydalanuvchilar orasida ishonchsizlikni keltirib chiqaradi.

Shunday holatlarning yuzaga kelishi axborot xavfsizligi uchun jiddiy tahdid hisoblanadi, chunki foydalanuvchi yoki tashkilot muhim, ishonchli va haqqoniy bo'lgan deb hisoblagan ma'lumot aslida buzilgan bo'lishi mumkin. Bu esa noto'g'ri qarorlar qabul qilinishiga, texnik xatolarga, hatto yirik moliyaviy yo'qotishlar va huquqiy mas'uliyatlarga olib kelishi ehtimoli yuqori. Shu sababli, zamonaviy axborot tizimlarida fayl yaxlitligini tekshirish mexanizmlarini joriy qilish, ularni avtomatlashtirish hamda foydalanuvchilar uchun qulay vositalar orqali taqdim etish strategik muhim vazifaga aylanmoqda. Aynan shu maqsadda, ilg'or kriptografik algoritmlar, jumladan, SHA-256 algoritmidan foydalanish orqali muammoning yechimi taklif etilmoqda.

Saytning markaziy funksiyalaridan biri bu — foydalanuvchiga fayl yaxlitligini ishonchli tarzda tekshirish imkoniyatini beruvchi fayl solishtirish tizimidir. Bu tizim foydalanuvchining kompyuteridagi fayllarni SHA-256 algoritmi asosida tahlil qilib, ularning o'zgartirilgan yoki asl holatda saqlanayotganligini aniqlashga yordam beradi. Bu jarayon nafaqat texnik jihatdan, balki axborot xavfsizligini ta'minlash nuqtai nazaridan ham muhim rol o'ynaydi. Chunki zamonaviy kompyuter tizimlarida hujjatlar, multimedia fayllari, dasturiy paketlar va boshqa raqamli resurslar ko'plab xavf-xatarlar ostida ishlaydi. Har qanday tashqi aralashuv, xususan zararli dasturlar yoki noto'g'ri foydalanuvchi harakatlari natijasida fayl tarkibida hatto bitta bayt o'zgaradigan bo'lsa, bu butun faylning ishonchliligini so'roq ostiga qo'yadi.

Shu sababli, fayllarning hash qiymatlari asosida solishtirish usuli, ya'ni kriptografik nazorat mexanizmi, fayllarning o'zgarmaganligini tekshirishning eng ishonchli usullaridan biri hisoblanadi. Aynan SHA-256 algoritmi bu maqsadlar uchun keng qo'llaniladi. U 256 bitli xavfsiz xesh qiymatini hisoblab chiqaruvchi algoritm bo'lib, bir xil mazmundagi fayllar uchun har doim aynan bir xil hash qiymatini hosil qiladi. Agar faylda kichik bir o'zgarish sodir bo'lsa, algoritm natijasida butunlay boshqa xesh qiymati hosil bo'ladi. Bu holat foydalanuvchiga fayl yaxlitligining buzilganligi haqida darhol xabar beradi. Aynan mana shu xususiyati tufayli SHA-256 algoritmi bugungi kunda turli axborot tizimlarida, jumladan, blokcheyn, raqamli imzo, antiviruslar va xavfsizlik tahlil vositalarida keng qo'llaniladi.

Fayllarni tanlash va ularni tahlil qilish jarayoni asosan saytning frontend qismida boshlanadi. Foydalanuvchi maxsus interfeys orqali o'z qurilmasidan ikkita faylni tanlaydi. Tanlangan fayllar foydalanuvchi tomonidan qo'lda yuklanishi yoki avtomatik tarzda tizim tomonidan aniqlanishi mumkin. Ushbu fayllar dastlab JavaScript orqali maxsus tayyorlangan shaklda backend serveriga yuboriladi. Backend qismida esa Python

dasturlash tili va uning tarkibidagi hashlib kutubxonasi yordamida har bir fayl ustida xesh hisoblash operatsiyasi amalga oshiriladi.

Hash hisoblashning texnik bosqichlari quyidagicha amalga oshiriladi: avvalo, har bir fayl baytlar ko'rinishida ochiladi va bu baytlar ketma-ketligi SHA-256 algoritmgacha uzatiladi. Algoritm fayldagi ma'lumotlarning butun tuzilmasini tahlil qilib, ularni 256 bitli o'zgarish uzunlikdagi qiymatga aylantiradi. Natijada, har bir fayl uchun noyob, aniqlovchi (identifikator) sifatida xizmat qiluvchi xesh qiymati hosil bo'ladi. Bu jarayon faylning hajmidan qat'i nazar, doimiy va yuqori aniqlikdagi xesh natijani beradi.

Hisoblangan xesh qiymatlari qayta frontendga yuboriladi. Sayt foydalanuvchiga ushbu xesh qiymatlarni taqqoslash imkoniyatini beradi: agar ikki faylning xesh qiymatlari aynan bir xil bo'lsa, bu ularning mazmuni ham mutlaqo bir xil ekanligini bildiradi; aks holda esa, hech bo'lmaganda biror kichik o'zgarish yuz berganini anglatadi. Bu esa foydalanuvchiga faylni qayta tekshirish, zaxira nusxasini tiklash yoki xavfsizlik choralarini ko'rish zarurligini bildiradi.

Ushbu jarayonning uzviyligi va real vaqt rejimida ishlashi uchun saytning frontend va backend qismlari o'rtasidagi aloqa mustahkam va ishonchli tashkil etilgan. Frontend HTML, CSS va JavaScript texnologiyalaridan foydalangan holda foydalanuvchiga sodda, tushunarli va qulay interfeysni taqdim etadi. Ayniqsa, JavaScript yordamida fayl tanlash, ko'rinadigan animatsiyalar va real vaqt natijalarni ko'rsatish imkoniyatlari foydalanuvchi tajribasini sezilarli darajada oshiradi. Backend esa, o'z navbatida, xavfsiz, tezkor va xatolarsiz hisob-kitobni ta'minlaydi.

Natijada, sayt foydalanuvchilarga nafaqat faylni solishtirish, balki uni xavfsiz saqlash, buzilishlardan ogohlantirish va potentsial tahdidlarni oldindan aniqlash imkoniyatini beradi. Bu tizim raqamli axborotni himoyalashning ishonchli mexanizmi sifatida xizmat qiladi va foydalanuvchilarga o'z ma'lumotlariga nisbatan yuqori darajadagi ishonchni taqdim etadi.

Saytning yana bir muhim funksional elementi bu — ko'p tilli qo'llab-quvvatlash tizimidir. Bu funksiya orqali sayt global auditoriyaga moslashtirilgan bo'lib, foydalanuvchilarga o'z ona tillarida xizmatlardan foydalanish imkonini yaratadi. Ko'p tilli interfeys foydalanuvchilarning tajribasini yaxshilaydi, ularning ehtiyojlariga mos keluvchi muhit yaratadi hamda saytdan foydalanish jarayonini soddalashtiradi.

Sayt ingliz, rus, o'zbek va qoraqalpoq tillarini qo'llab-quvvatlaydi. Bu esa nafaqat mahalliy, balki xorijiy foydalanuvchilarni ham jalb etishga xizmat qiladi. Foydalanuvchi sayt interfeysida kerakli tilni tanlaganida, barcha matn elementlari avtomatik ravishda shu tilga moslashtiriladi. Masalan, ingliz tilini tanlagan foydalanuvchi saytning barcha menyulari, tugmalari, xabar oynalari va boshqa matnlarini ingliz tilida ko'radi.

Texnik nuqtai nazardan, til tanlash funksiyasi backend va frontend qismlarining o'zaro hamkorligi asosida amalga oshiriladi. Backendda har bir til uchun alohida JSON yoki Python formatidagi tarjima fayllari yaratiladi (masalan, uz.json, en.json, ru.json, kk.json). Bu fayllar tegishli interfeys elementlari uchun tarjima matnlarini o'z ichiga oladi.

Foydalanuvchi tilni tanlaganda, server ushbu faylni yuklab olib, tegishli matnlar frontendga uzatiladi.

Frontend qismida esa foydalanuvchiga til tanlash imkonini beruvchi grafik interfeys yaratilgan. JavaScript yordamida foydalanuvchi tanlovi qayd etiladi va shu asosda sayt mazmuni mos ravishda yangilanadi. Bunday tizim foydalanuvchilarga qulay va shaxsiylashtirilgan xizmat ko'rsatish imkonini beradi. Bundan tashqari, saytni ko'p tilli qilish, uning xalqaro miqyosda ommalashuvi va foydalanuvchilar bazasining kengayishi uchun muhim shart hisoblanadi.

Tadqiqot doirasida ishlab chiqilgan SHA-256 algoritmiga asoslangan veb-ilova real fayl namunalarida sinovdan o'tkazildi. Sinovlar davomida foydalanuvchi tomonidan tanlangan fayllarning hash qiymatlari hisoblab chiqildi va ular o'zaro taqqoslandi. Quyidagi asosiy natijalar qayd etildi:

-Fayl mazmunida hech qanday o'zgarish bo'lmagan hollarda hash qiymatlari to'liq mos tushdi va tizim buni to'g'ri aniqladi (100% aniqlik).

-Faylning atigi bitta bayt birligida o'zgarish kiritilgan holatlarda ham, tizim tomonidan hash qiymatlaridagi tafovutlar aniq qayd etildi, bu esa yuqori sezuvchanlik darajasini ko'rsatadi.

-Veb-ilova interfeysi foydalanuvchiga real vaqt rejimida rangli vizual indikatorlar orqali natijalarni tez va tushunarli ko'rinishda yetkazdi.

-Ko'p tillilik funksiyasi (o'zbek, ingliz, rus, qoraqalpoq tillarida) muvaffaqiyatli sinovdan o'tkazildi hamda foydalanuvchilarga moslashtirilgan interfeys taqdim etildi.

Natijalar veb-ilovaning funksional jihatdan barqarorligini va uning hash solishtirish mexanizmi yuqori aniqlikda ishlashini tasdiqladi.

Olingan natijalar SHA-256 algoritmiga asoslangan veb-ilovaning fayl yaxlitligini tekshirishda ishonchli va amaliy yechim ekanligini ko'rsatdi. Algoritmning har qanday, hatto kichik o'zgarishlarni aniqlash xususiyati, foydalanuvchi uchun axborotning haqiqiyligini tekshirishda muhim afzallik yaratadi. Hash qiymatlarini solishtirish asosidagi yondashuv kriptografik nazorat vositasi sifatida o'zini to'liq oqladi.

Tizim interfeysi foydalanuvchi tajribasini inobatga olgan holda ishlab chiqilgan bo'lib, vizual aniqlik, intuitiv dizayn va ko'p tillilik asosida ishlaydi. Bu esa tizimdan foydalanish samaradorligini oshiradi va uni turli auditoriyalar uchun qulay qiladi.

Shunga qaramay, mavjud yechimni yanada takomillashtirish bo'yicha quyidagi istiqbolli yo'nalishlar mavjud:

- Kriptografik asosni mustahkamlash: SHA-512 yoki BLAKE2 algoritmlarini integratsiya qilish orqali xavfsizlik darajasi oshiriladi.

- Avtonom ish rejimi: Client-side hashing texnologiyasini joriy etish orqali serverga fayl yubormasdan, hash natijalarini foydalanuvchi qurilmasida hisoblash imkoniyati yaratiladi.

- Interaktivlikni kengaytirish: Natijalarni grafik ko'rinishda taqdim etish, foydalanuvchi xatolarini tahlil qilish va qo'shimcha statistik modullarni kiritish.

- Autentifikatsiya va imzolash: Raqamli imzo va ikki faktorli autentifikatsiya texnologiyalarini qo'shish orqali tizimning ishonchlilik darajasi oshiriladi.

Umuman olganda, veb-ilovaning natijalari uni amaliyotda qo'llash uchun yetarli darajada tayyor ekanligini ko'rsatdi. Biroq, foydalanuvchi ehtiyojlari, texnik imkoniyatlar va xavfsizlik talablari ortib borayotgan sharoitda, tizimni doimiy ravishda yangilab borish dolzarb vazifa bo'lib qoladi.

Xulosa sifatida aytish mumkinki, mazkur veb-ilova foydalanuvchilarga SHA-256 algoritmiga asoslangan fayl yaxlitligini aniq va ishonchli tekshirish imkoniyatini beradi. Ilovaning asosiy vazifasi — ikki faylning hash qiymatlarini solishtirib, ularning mos yoki mos emasligini tez va samarali aniqlashdan iborat. Bu jarayon kriptografiyaning yuqori aniqlik va xavfsizlik tamoyillariga asoslangan bo'lib, foydalanuvchilar ma'lumotlarining yaxlitligi va autentifikatsiyasini ta'minlaydi.

Saytda mavjud til tanlash funksiyasi esa foydalanuvchi interfeysining qulayligi va ko'p tillilikni ta'minlash orqali mintaqaviy hamda xalqaro auditoriyani qamrab olishga xizmat qiladi. Ingliz, rus, o'zbek va qoraqalpoq tillarining qo'llab-quvvatlanishi saytni kengroq foydalanuvchilar uchun moslashtirish imkonini yaratadi hamda UX (foydalanuvchi tajribasi) darajasini oshiradi.

Loyihaning hozirgi bosqichi ikki asosiy modulga asoslangan bo'lsa-da, uning kelajakda yanada rivojlantirilishi uchun katta salohiyat mavjud.

Masalan, client-side hashing texnologiyasini joriy etish orqali foydalanuvchi ma'lumotlarining maxfiyligi oshiriladi, serverda fayllarni saqlashdan qochiladi.

Bundan tashqari, fayl hash natijalarini vaqtinchalik saqlash, raqamli imzo qo'shish va avtomatik .hash fayl yaratish funksiyalari ham integratsiya qilinishi mumkin.

Natijada, mazkur veb-ilova nafaqat texnik nuqtai nazardan yuqori sifatli yechim bo'lib, balki amaliy ehtiyojlarni qondiruvchi, axborot xavfsizligi sohasida muhim qo'llanma hisoblanadi.

Ochiq arxitekturasini, foydalanuvchiga qulay interfeysi va ko'p tilli qo'llab-quvvatlashi uni keng auditoriyaga moslashtirishda kuchli platformaga aylantiradi.

Ushbu loyiha zamonaviy axborot texnologiyalari sohasidagi ilmiy-amaliy ishlarning namunasi sifatida yuqori baholanishi mumkin.

FOYDALANILGAN ADABIYOTLAR RO'YXATI:

1. DR.H.Handschub and Dr.H.Gilbert, "Evaluation Report Security Level of Cryptography – SHA-256", Technical Report, Issy-les-Moulineaux, January 2002.
2. NIST, "Secure Hash Standard (SHS)", FIPS PUB 180-2, 2002.
3. J. Lee, D. Chang, E. Lee, H. Kim, D. Hong, J. Sung, S. Hong, and S. Lee, "A new 256-bit hash function DHA-256 – Enhancing the security of SHA-256," Presented at NIST Cryptographic Hash, Workshop, 2005
4. A.D. Moore, Python GUI programming with Tkinter: Develop responsive and powerful GUI applications with Tkinter. Packt Publishing Ltd, 2018.

5. D.P. Pasca, A. Aloisio, M.M. Rosso, and S. Sotiropoulos, "PyOMA and PyOMA_GUI: A Python module and software for operational modal analysis," SoftwareX, vol. 20, Dec. 2022, doi: 10.1016/j.softx.2022.101216.