BULUTLI HISOBLASH TIZIMLARIDA FOYDALANILGAN KRIPTOGRAFIK ALGORITMLAR TAHLILI

Imamaliyev Aybek Turapbayevich

Muhammad al-Xorazmiy nomidagi Toshkent axborot-texnologiyalari universiteti Kriptologiya kafedrasi O‘qituvchisi.

Eshto‘xtarov Suxrob Abdumalik o‘g‘li

G‘afurov Mehriddin G‘iyosovich

Yoqubov Dilshod Zoyir o‘g‘li

Toshkent axborot-texnologiyalari universiteti Kiberxavfsizlik fakulteti Talabalari.

Annotatsiya: *Ushbu maqolada bulutli hisoblash texnologiyalarida axborot xavfsizligini ta'minlashda qo‘llaniladigan kriptografik algoritmlarning ro‘li va samaradorligi tahlil qilinadi. Maqolada simmetrik va assimetrik kriptografiya, hashing (xesh) funksiyalari, shuningdek, zamonaviy kriptografik algoritmlar – AES, RSA, ECC, va SHA-256 kabi algoritmlarning ishlash prinsiplari va ularning bulutli muhitda qo‘llanilishi o‘rganiladi. Shuningdek, ushbu algoritmlarning afzalliklari, kamchiliklari va ularni tanlashda e’tiborga olinadigan muhim omillar ko‘rib chiqiladi. Tadqiqot natijalari shuni ko‘rsatadiki, ma’lumotlarni himoya qilishda samarali kriptografik algoritmlardan foydalanish bulutli xizmatlar xavfsizligini sezilarli darajada oshiradi.*

Kalit so‘zlar: *Bulutli hisoblash, kriptografiya, AES, RSA, ECC, SHA-256, axborot xavfsizligi, simmetrik shifrlash, assimetrik shifrlash, xesh funksiyalari.*

XXI-asrga kelib Internet va tarmoq xizmatlari soni va sifati kun sayin ortib bormoqda. Bu esa elektron ma’lumotlarni saqlash va qayta ishlash jarayonida keng imkoniyatlar taqdim etmoqda. Bu esa o‘z navbatida axbortlarni saqlash va ularni uzatish bilan bog‘liq zaifliklarni yuzaga kelishi muammosi dalzarbligini ortishiga olib keldi. Bulutli hisoblash Internet orqali turli xizmatlarni taklif qiluvchi eng tez rivojlanayotgan texnologiyadir. U korxonalarga resurslar, infratuzilma, platforma va boshqalar kabi ko‘plab xizmatlarni taqdim etishi mumkin, ular uchun talab bo‘yicha masshtabni kattalashtirish yoki kamaytirish qobiliyatiga ega bo‘lib, talab asosida pul to‘lash imkoniyati mavjud.

Shuningdek, xavfsizlik bulutli hisoblashni qabul qilishda asosiy muammo hisoblanadi. Bulutdagi ma’lumotlar xavfsizligi muammosini hal qilish uchun ko‘plab kriptografik algoritmlar mavjud. Algoritmlar ruxsatsiz foydalanishdan ma’lumotlarni himoya qiladi. Shifrlash algoritmlari bulutli hisoblashda ma’lumotlar konfidensilalligini ta’minlashda muhim ahamiyat kasb etadi.

Bulutli hisoblash texnologiyalari, ma’lumotlarni uzluksiz ravishda o‘rganish va ularga murojaat qilish uchun internet orqali moslashtirilgan xizmatlarni o‘z ichiga oladi. Bu, ma’lumotlarni lokal kompyuterlar yoki serverlarda emas, balki internet orqali aloqador serverlarda saqlashni o‘z ichiga oladi. Ma’lumotlar bazasi, serverlar, dasturiy ta’minot, tarmoq echimlari va tahlillarni o‘z ichiga olgan hisoblash xizmatlarini Internet orqali taqdim etish jarayoni. Shuningdek aloqa vositalariga tarmoqqa asoslangan kirishni o‘z ichiga oladi. Xoh bu Google Drive, Facebook Messenger yoki Gmail, bularning barchasi bulutli hisoblash xizmatlarining bir qismidir. Bulutli hisoblash korxonalarning ish unumdorligini avtomatlashtirishni ta’minlash orqali deyarli uzluksiz xizmatlarni taklif qilish imkonini beradi va foydalanuvchilarning talablari o‘zgarishi bilan avtomatik ravishda kengayadi yoki kamayadi. Bu, foydalanuvchilarning tizimlari

qilayotgan ishlari bilan mos keladigan saqlash, xotira va xizmatlarni ta’minlanlashini ta’minlaydi.[1]

Kriptografiya — bu ma’lumotlarni shifrlash va ularni ruxsatsiz kirishdan himoya qilish usullarini o‘rganuvchi fan sohasidir. Kriptografik algoritmlar uch asosiy turga bo‘linadi:

- Simmetrik shifrlash algoritmlari (AES, DES): bir xil kalit orqali ma’lumotlarni shifrlash va deshifrlash amalga oshiriladi.
- Assimetrik shifrlash algoritmlari (RSA, ECC): ikkita kalitdan foydalaniladi – ochiq (public) va yopiq (private).
- Xesh funksiyalari (SHA-1, SHA-256): ma’lumotlarni aniq uzunlikdagi, o‘zgarmas formatdagi qiymatga aylantiradi.

AES — simmetrik blokli shifrlash algoritmi bo‘lib, tez ishlashi va yuqori darajadagi xavfsizligi bilan ajralib turadi. Bulutli tizimlarda AES 128, 192 yoki 256 bitli kalitlar yordamida ma’lumotlarni shifrlash uchun keng qo‘llaniladi.

RSA-assimetrik shifrlash algoritmi bo‘lib, ko‘pincha kalitlar almashinuvi yoki ma’lumotlarni xavfsiz tarzda uzatishda ishlatiladi. U katta kalit uzunliklarini talab qiladi, lekin xavfsizlik darajasi yuqori.

ECC-RSA ga nisbatan kichikroq kalitlar bilan yuqori xavfsizlikni ta’minlaydi. ECC bugungi kunda mobil qurilmalar va bulutli tizimlarda samarali yechim sifatida qaralmoqda.

SHA-256-ma’lumotlarning yaxlitligini ta’minlash uchun qo‘llaniladi. Bulutli tizimlarda fayllarning o‘zgarmaganligini tekshirishda muhim rol o‘ynaydi.

Kriptografiya bulutli tizimlarda quyidagi jihatlar uchun muhim:

[1] Gulyamov, S.S. va b. (2019). Raqamli iqtisodiyotda blokcheyn texnologiyalari. -T.: Iqtisod-Moliya. 396 b.

- Ma’lumotlarni ruxsatsiz kirishdan himoya qilish.
- Maxfiylikni ta’minlash.
- Foydalanuvchi identifikatsiyasi va autentifikatsiyasi.
- Ma’lumot yaxlitligini ta’minlash.
- Raqamli imzolar orqali hujjatlarni ishonchli qilish.

Ma’lumotlarning maxfiyligi nafaqat bulutli tizim uchun balki barcha tizimlar uchun ham asosiy xavfsizlik masalasi hisoblanib kelgan. Shunday ekan ko‘pchilik korxona-tashkilotlar konfidensial ma’lumotlarni bulutli tizimlarda saqlashdan ko‘ra o‘z saytlariga joylashtirishni avzal ko‘rishadi. Konfidensiallik ma’lumotlar maxfiyligi bilan bog‘liq bo‘lib, ma’lumotlar faqat ruxsat berilgan foydalanuvchilar uchun ko‘rinishini ta’minlaydi. Ushbu ma’lumotlarning Konfidensialligini xizmat ko‘rsatuvchi provayderning javobgarligiga kiradi.

Biroq, Bulutli texnologiyalardan foydalanishda kamchiliklari. Doimiy Internet tarmog‘i bilan aloqada bo‘lishi lozim. Bulutli hisoblash texnologiyalaridan foydalanishda har vaqt tarmoq Internetga ulangan bo‘lishi lozim. Bundan tashqari bir necha ilovalar mavjud bo‘lib, ular kompyuterlarga yuklanadi va ulardan uzoq muddatgacha ishlash imkoniyati bo‘ladi. Boshqa holatlarda esa har doimgidek oddiy hisoblanib, ulanish bo‘lmasa ish ham bo‘lmaydi. Ko‘pchilikning fikricha bu bulutli hisoblashlarning eng katta kamchiligi deb yuritishadi. Iste‘molchilar tomonidan bulut texnologiyalariga qo‘yilgan har bir ma‘lumot xavfsizligi xavf ostida bo‘lishi mumkin.

Xulosa qilib aytganda, bulutli hisoblash tizimlarida kriptografik algoritmlardan foydalanish axborot xavfsizligini ta’minlashda muhim ahamiyatga ega. AES, RSA, ECC va SHA-256 kabi algoritmlar har xil maqsadlar uchun tanlanadi va ulardan foydalanish jarayonida tizimning samaradorligi va xavfsizlik

darajasi ortadi. Kelgusida yangi kvantga chidamli kriptografik algoritmlar ishlab chiqilishi bulutli xavfsizlikni yanada kuchaytiradi.

Foydalanilgan adabiyotlar

1. Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, “Comparative Analysis between DES and RSA Algorithm’s”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X
2. Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360- Degree Compared CoRR. abs/0901.01
3. Gulyamov, S.S. va b. (2019). Raqamli iqtisodiyotda blokcheyn texnologiyalari. -T.: Iqtisod-Moliya. 396 b.
4. Nunez, A. iCanCloud: A Flexible and Scalable Cloud Infrastructure Simulator / A. Nunez // J. Grid Comput. 2012. — Germany: Springer, 2012. — Vol. 10. — P. 185209.