DOI: https://doi.org/10.5281/zenodo.14556417

MOBIL BULUTLI HISOBLAR UCHUN SAMARALI VA XAVFSIZ SAQLASH AMALIYOTLARI

Shirinov Laziz Toxirovich
Muhammad Al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti PhD talabasi,
(Alfraganus universiteti katta o‘qituvchisi).

ANNOTATSIYA

Ushbu maqolada Ushbu muammoni hal qilish uchun samarali yechim bulutli xizmat ko‘rsatuvchi provayderlarga maxfiy ma’lumotlar mazmuni yoki kalitlarini oshkor qilmasdan og‘ir shifrlash va dekodlash hisoblarini autsorsing qilishdan iborat.

Kalit so‘zlar: *xavfsizlik, mobil qurilmalar, SSP, deshifrlash, atributlarga asoslangan shifrlash, kirish siyosati, atribut, hujum modeli.*

Kirish

Ushbu maqsadga erishish uchun ikkita parametrni ko‘rib chiqing:

1) Shifr konfidensialligini, shifrlash parametrlariga asoslangan siyosatni saqlang Maxfiylikni saqlash shifr siyosati atributiga asoslangan shifrlash (PP-CP-ABE)

PP-CP-ABE-dan foydalangan holda, engil qurilmalar ma’lumotlar mazmunini va foydalanilgan xavfsizlik kalitlarini oshkor qilmasdan, bulutli xizmat ko‘rsatuvchi provayderga ma’lumotlarni uzatishda og‘ir shifrlash va dekodlash operatsiyalarini xavfsiz tarzda amalga oshirishi mumkin.

2) Atributga asoslangan ma’lumotlarni saqlash tizimi (ABDS) kriptografik kirishni boshqarish mexanizmi sifatida.

Xususiyat, ABDS ma’lumotlarni boshqarish uchun aloqa xarajatlarini kamaytirish orqali bulut xizmatlari yukini kamaytiradi.

Tadqiqot natijalari

CP-ABE tuzilmasi har bir foydalanuvchiga bir nechta kirish va shifrlash parametrlarini tayinlash imkonini beradi. Bir nechta foydalanuvchi shifrlovchi qurilmaga “VA”, “YOKI” kabi mantiqiy operatorlar yordamida bir nechta parametrlarni tuzish orqali ma’lumotlarga kirish siyosatini aniqlash imkonini beruvchi umumiy parametrlarga ega bo‘lishi mumkin. Xabarni shifrini ochish uchun foydalanuvchi tutqichi parametrlari kirish siyosatini qondirishi kerak. CP-ABE ning ushbu noyob xususiyati ko‘p sonli foydalanuvchilar uchun ma’lumotlarga samarali kirish va boshqarishni talab qiluvchi bulutli xizmatlarda ma’lumotlarni saqlashni jozibador qiladi.

Simsiz aloqa texnologiyalarining jadal rivojlanishi bilan mobil bulut bulutli xizmat ko‘rsatish modelining [1] paydo bo‘lishiga aylandi, bunda mobil qurilmalar va sensorlar bulut infratuzilmasi uchun ma’lumotlarni yig‘ish va qayta ishlash tugunlari sifatida ishlatiladi.

CP-ABE bilan yangi muammo simsiz mobil qurilmalarni, ayniqsa mobil telefonlar va sensorlar kabi engil qurilmalarni bulut tizimiga qanday kiritishdir.

Bu yangi muammo, chunki CP-ABE sxemalari har doim intensiv hisoblash resurslari va dekodlash va shifrlash algoritmlarini talab qiladi.

Ushbu muammoni hal qilish uchun samarali yechim bulutli xizmat ko‘rsatuvchi provayderlarga maxfiy ma’lumotlar mazmuni yoki kalitlarini oshkor qilmasdan og‘ir shifrlash va dekodlash hisoblarini autsorsing qilishdir.

Yana bir tadqiqot muammosi shifrlangan ma’lumotlarni ko‘p sonli foydalanuvchilar bilan qanday almashishdir, unda ma’lumotlar almashish guruhi tez-tez o‘zgarishi mumkin. Misol uchun, foydalanuvchi faylga kirish huquqini bekor qilganda, u faylning kelajakdagi yangilanishlariga kirish huquqiga ega emas, ya’ni mahalliy nusxa (agar mavjud bo‘lsa) eskirib qoladi. Buning uchun yangilangan ma’lumotlar yangi shifrlash kaliti bilan shifrlangan bo‘lishi kerak.

Bundan tashqari, uchinchi tadqiqot vazifasi tizim bulutida saqlangan yangilangan shifrlangan ma’lumotlarni qanday yuklash/yuklab olishdir. Misol uchun, bir dan ba’zi ma’lumotlar maydonlari qachon shifrlangan ma’lumotlar bazasi o‘zgartirilsa, shifrlangan ma’lumotlarni bulutdan yuklab olish va keyin shifrini ochish kerak. Yangilash tugallangach, fayllar qayta shifrlanishi va bulut xizmatiga yuborilishi kerak. Tez-tez yuklab olish/yuklash operatsiyalari simsiz qurilmalarning cheklangan resurslariga katta yuk olib keladi. Shunday qilib, shifrlangan ma’lumotlarni boshqarish uchun uzatish va saqlash operatsion xarajatlarini muvozanatlash uchun xavfsiz va samarali boshqaruv sxemalarini ishlab chiqish maqsadga muvofiqdir [2].

PP-CP-ABE-dan foydalangan holda, foydalanuvchilar ma’lumotlar mazmuni va maxfiy kalitlarni oshkor qilmasdan bulutga hisoblash, CP-ABE intensiv shifrlash va shifrni ochish operatsiyalarini xavfsiz autsorsing qilishlari mumkin. Shu tarzda, cheklangan hisoblash resurslariga ega engil qurilmalar bulutli ma’lumotlar omborida saqlangan ma’lumotlarga kirishi va boshqarishi mumkin. Bundan tashqari, ABDS aloqa va saqlashni muvozanatlash uchun mobil kompyuterlar uchun mos keladi va shu tariqa mobil bulut tugunlari va saqlash xizmati provayderlari uchun ma’lumotlarni boshqarish operatsiyalari (masalan, yuklab olishlar, yangilanishlar va boshqalar) narxini pasaytiradi.

Tizimlar va modellar

1-jadval. Belgilar

Acronym	Descriptions
DO	Data Owner
ESP	Encryption Service Provider
DSP	Decryption Service Provider
SSP	Storage Service Provide
T.A.	Trust Authority
T	Access Policy Tree

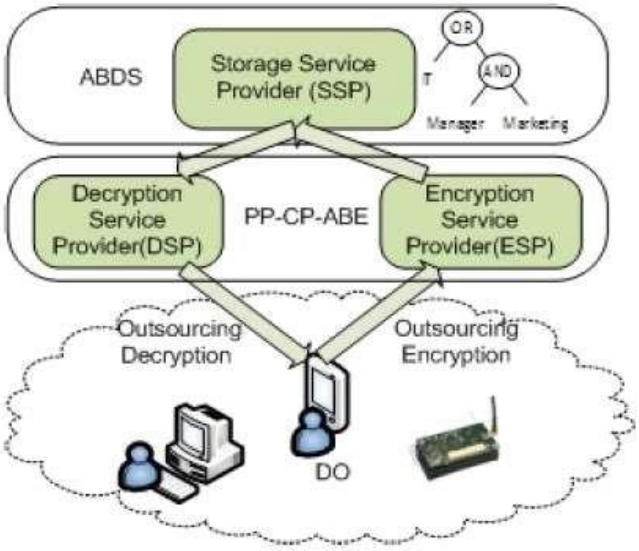
Tizim modeli:

1) Saqlash xizmati provayderiga (SSP) yuborishdan oldin ma’lumotlar shifrlangan bo‘lishi kerak;

2) Shifrlash xizmati provayderi (ESP) ma’lumotlar egasiga haqiqiy ma’lumotlarni shifrlash kalitini (DEK) bilmagan holda shifrlashni ta’minlaydi;

3) Deshifrlash xizmati provayderi (DSP) ma’lumotlar mazmunini bilmasdan foydalanuvchi ma’lumotlarining shifrini ochishni ta’minlaydi;

4) Hatto ESP, DSP va SSP ning kelishuvi ham foydalanuvchi ma’lumotlari tarkibiga kirishga ruxsat bermaydi.



1-rasm. *SSP, ESP va DSP taklif etilayotgan tizimning asosiy komponentlarini tashkil qiladi.*

1-rasmda ko‘rsatilganidek, SSP, ESP va DSP tavsiya etilgan tizimning asosiy komponentlarini tashkil qiladi. ESP va DSP PP-CP-ABE xizmatlarini taqdim etadi va Amazon S3 kabi SSP saqlash xizmatlarini taqdim etadi. Xususan, kuchliroq shaxsiy kompyuterlar va mobil telefonlar ma’lumot to‘playdigan sensorlar o‘rtasidagi aloqa uchun proksi-server vazifasini bajarishi mumkin.

Hujum modeli

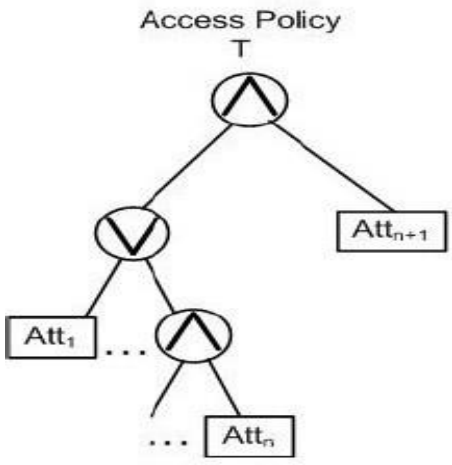
Biz ushbu ishda ishlatiladigan simmetrik shifrlash algoritmi va bir tomonlama xesh funksiyasi xavfsiz va diskret logarifm (DL) muammosi ikkala guruhda ham xavfsiz deb taxmin qilamiz, va murakkab. Bundan tashqari, TA kriptografik kalitlarni yuqori darajada himoyalangan va ishonchli tarzda tarqatish uchun javobgardir. Halol, ammo qiziquvchan bulutli xizmat ko‘rsatuvchi provayderlarni ko‘rib chiqing.

Boshqacha qilib aytganda, xizmat ko‘rsatuvchi provayderlar taklif qilingan protokollar bo‘yicha ishlaydi va to‘g‘ri hisoblash natijalarini qaytaradi. Biroq, xizmat ko‘rsatuvchi provayderlar imkon qadar ko‘proq muhim ma’lumotlarni (masalan, shaxsiy ma’lumotlar, kalitlar va h.k.) topishga harakat qiladilar va tajovuzkorlar bilan til biriktirishlari mumkin. Buzg‘unchilarning maqsadi bulutdagi ma’lumotlarni DO‘larning ruxsatisiz aniqlashdir. Bir nechta tajovuzkorlar hujumni amalga oshirish uchun kuchlarini birlashtirishi mumkin, ular shifrlangan matnning shifrini ochishga urinishlari va ular kirish huquqiga ega bo‘lmagan shifrni ochish kalitlarini buzishi mumkin. Bunday hujumga til biriktirish misol bo‘ladi [3].

Xususan, tajovuzkorlar Forward Maxfiylikni buzishi mumkin, bu quyidagicha aniqlanadi: foydalanuvchi faylga kirishni bekor qilgandan so‘ng, u faylning mahalliy nusxasiga ega bo‘lishi mumkin, ammo agar kirish bekor qilinsa, foydalanuvchi kelajakdagi yangilanishlarni olmasligi kerak. Fayl uchun Bulutdagi ma’lumotlarning yaxlitligi va topilishi ham muhim xavfsizlik talablari bo‘lsa-da, ushbu maqolada bu masalalar ko‘rib chiqilmaydi.

Kirish siyosati daraxti

Ushbu bo‘lim PP-CP-ABE da qo‘llaniladigan kirish siyosati daraxti modelini qisqacha tavsiflaydi. Bu daraxt barg tugunlari va ichki tugunlardan iborat. Har bir barg tugun atributni ifodalaydi va har bir ichki tugun mantiqiy elementni ifodalaydi, masalan, “VA”, “YOKI” va hokazo.



2-rasm. *Kirish siyosati*

Yechimlarimizni taqdim etishni osonlashtirish uchun bir nechta funksiya va shartlar quyidagicha aniqlanadi:

• parent(x): x tugunining asosiy tugunini qaytaradi;

• att(x) ma’lumotlarga kirishda x barg tuguniga bog‘langan parametrni bildiradi daraxt;

• T barg tugunlari (ya’ni parametrlar) va ichki tugunlar to‘plamidan iborat

(mantiqiy eshiklar) va ma’lumotlarga kirish siyosatini belgilaydi, ya’ni foydalanuvchi daraxtning ildizigacha bo‘lgan mantiqiy operatsiyalarini qanoatlantiradigan parametrlar to‘plamiga ega bo‘lsa, u T bilan himoyalangan ma’lumotlarga kirishi mumkin. Foydalanuvchi tegishli shaxsiy kalitlarga ega. xarakteristikalar (parametrlar) to‘plamiga. AND va OR eng ko‘p ishlatiladigan mantiqiy eshiklardir.

• numx - asosiy tugunlar soni. X tugunining bola tuguni 1 dan numx gacha bo‘lgan butun indeks(y) bilan aniqlanadi

• Chegara qiymati kx=numx-1 bu erda x AND va kx = 0 bu erda x YOKI tugun. kx chegarali bo‘linish sxemasi yordamida x tugunining darajali polinomi sifatida ishlatiladi.

Xulosa

Va nihoyat, ommaviy bulutda ma’lumotlarni boshqarishni ta’minlash uchun bulutli saqlash xizmatlari uchun yaxlit xavfsizlik tizimi taklif etiladi. Xususan, bizning yechimimiz yengillikka imkon beradi

Simsiz qurilmalar o‘zlarining ma’lumotlarini umumiy bulutda minimal xarajat bilan xavfsiz saqlash va tiklash uchun. Shu maqsadda foydalanuvchilarning shifrlangan ma’lumotlarini himoya qilish uchun Maxfiylikni saqlash shifr siyosati atributiga asoslangan shifrlash (PP-CP-ABE) sxemasi taklif qilindi. PP-CP-ABE-dan foydalangan holda, engil qurilmalar intensiv shifrlash va shifrni ochish operatsiyalarini bulutli xizmat ko‘rsatuvchi provayderlarga ishonchli tarzda tashqi manbalardan foydalanishi mumkin, bunda foydalanilgan ma’lumotlar mazmuni va xavfsizlik kalitlari ko‘rsatilmaydi. Bundan tashqari, Atributga asoslangan

ma’lumotlarni saqlash (ABDS) kriptografik kirishni boshqarish mexanizmi sifatida taklif qilingan. ABDS hisoblash, saqlash va aloqa xarajatlarini minimallashtirish nuqtai nazaridan optimal hisoblanadi. Xususiyat, ABDS bulutli xizmat ko‘rsatuvchi provayderlarning xarajatlarini, shuningdek, ma’lumotlarni boshqarish uchun aloqa xarajatlarini kamaytiradi. Ishlashni baholash hisoblash, uzatish va saqlash nuqtai nazaridan yechimning xavfsizligi va samaradorligini ko‘rsatadi.

Hozirgi vaqtda PP-CP-ABE BSW CP-ABE sxemasiga asoslangan bo‘lib, uning kamchiliklari shifrlangan matn hajmining chiziqli o‘sishidir. Doimiy shifrlangan matn hajmiga ega bo‘lgan CP-ABE sxemasi ko‘rib chiqildi va yangi CP-ABE sxemasining maxfiylikni saqlaydigan autsorsingi taklif qilindi.

ADABIYOTLAR:

1. G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. ACM Trans. Inf. Syst. Secur., 9(1):1-30, 2006

2. J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute - based encryption. In SP ‘07: Proceedings of the 2007 IEEE Symposium on Security and Privacy, pages 321-334, Washington, DC, USA, 2007. IEEE Computer Society.

3. D. Boneh, X. Boyen, and E.J. Goh. Hierarchical identity-based encryption with constant size ciphertext. Advances in Cryptology- EUROCRYPT 2005, pages 440-456, 2005.