CLOUDDA MA’LUMOTLARNI KRIPTOGRAFIK HIMOYALASH ALGORITMLARINI TAHLILI

Samandar Yusupov Anvarovich
University of Management and Future Technologies universitedi magistranti Toshkent, 100208, O‘zbekiston Samandar75781111@gmail.com

Annotatsiya: *Ushbu maqolada bulutli hisoblash muhitida ma’lumotlarni kriptografik himoyalash algoritmlarini tahlil qilishga bag'ishlangan tadqiqot natijalari keltiriladi. Bulutli texnologiyalar hozirgi kunda foydalanuvchilar uchun katta qulayliklar yaratib, ma’lumotlarni masofadan boshqarish va saqlash imkoniyatini taqdim etmoqda. Biroq, bunday tizimlarda ma’lumotlarning xavfsizligi va maxfiyligini ta'minlash dolzarb muammolardan biri bo'lib qolmoqda. Maqolada ma’lumotlarni himoyalash uchun simmetrik va assimetrik kriptografiya algoritmlarining samaradorligi, ishlash tezligi, xavfsizlik darajasi va resurs talablarini solishtirish asosida tahlil qilinadi. Tadqiqot davomida AES, RSA, ECC kabi mashhur kriptografik algoritmlar bulutli muhitda qo'llanilishi mumkin bo'lgan samarali usullar sifatida ko'rib chiqildi. Shuningdek, ma’lumotlarni shifrlash va shifrdan chiqarish jarayonlarining samaradorligi, hisoblash xarajatlari va potensial zaifliklar ko'rib chiqildi. Tadqiqot natijalari bulutli xizmatlardan foydalanuvchilarga ma’lumotlar xavfsizligini ta'minlash uchun qaysi kriptografik algoritmlarni qo'llash bo'yicha tavsiyalarni taklif etadi.*

Kalit so‘zlar. AES, RSA, ECC, *Cipher text Policy Weighted Attribute-Based Encryption (CP-WABE). Attribute-Based Encryption, Key Policy ABE (KP-ABE), Cipher text policy ABE (CP-ABE), HASBE.*

Аннотация: *В данной статье представлены результаты исследования, посвященного анализу алгоритмов криптографической защиты данных в облачной вычислительной среде. Облачные технологии в настоящее время создают значительные удобства для пользователей, предоставляя возможности удаленного управления и хранения данных. Однако обеспечение безопасности и конфиденциальности данных в таких системах остается актуальной проблемой. В статье проводится анализ эффективности, скорости работы, уровня безопасности и требований к ресурсам симметричных и асимметричных криптографических алгоритмов для защиты данных. В ходе исследования рассмотрены такие известные криптографические алгоритмы, как AES, RSA, ECC, которые могут быть использованы в облачной среде в качестве эффективных методов. Также изучены эффективность процессов шифрования и расшифрования данных, вычислительные затраты и потенциальные уязвимости. Результаты исследования предлагают рекомендации для пользователей облачных сервисов по применению криптографических алгоритмов для обеспечения безопасности данных.*

Ключевые слова: *AES, RSA, ECC,шифрование на основе атрибутов, шифрование с политикой, основанной на шифротексте (CP-ABE), шифрование с политикой,*

основанной на ключах (KP-ABE), иерархическое шифрование на основе атрибутов (HASBE).

Annotation: *This article presents research findings dedicated to analyzing cryptographic algorithms for data protection in cloud computing environments. Currently, cloud technologies offer users significant conveniences by providing the ability to manage and store data remotely. However, ensuring the security and confidentiality of data in such systems remains a pressing issue. The article analyzes the efficiency, performance speed, security level, and resource requirements of symmetric and asymmetric cryptographic algorithms for data protection. The study examines well-known cryptographic algorithms such as AES, RSA, and ECC as effective methods applicable in cloud environments. Additionally, the efficiency of data encryption and decryption processes, computational costs, and potential vulnerabilities are reviewed. The research results offer recommendations for users of cloud services on which cryptographic algorithms to apply to ensure data security.*

Keywords: *AES, RSA, ECC,Ciphertext-Policy Weighted Attribute-Based Encryption (CP-WABE), Attribute-Based Encryption, Key-Policy ABE (KP-ABE), Ciphertext-Policy ABE (CP-ABE), Hierarchical Attribute-Based Encryption (HASBE).*

Kirish

Bugungi kunda bulutli texnologiyalar rivojlanishi bilan ma’lumotlarni masofadan boshqarish, ularga qulay tarzda kirish va saqlash imkoniyatlari sezilarli darajada oshdi. Ushbu texnologiyalar nafaqat shaxsiy foydalanuvchilar, balki yirik kompaniyalar va davlat tashkilotlari uchun ham muhim ahamiyat kasb etmoqda. Ammo bulutli muhitda ma’lumotlar xavfsizligini ta'minlash va maxfiy ma’lumotlarni uchinchi tomonlardan himoya qilish dolzarb masala bo'lib qolmoqda. Bu borada kriptografik usullar va algoritmlar ma’lumotlarni himoyalashda eng samarali vositalardan biri hisoblanadi.

Bulutli muhitda ma’lumotlarni himoyalash o'ziga xos qiyinchiliklarga ega. Birinchidan, foydalanuvchi tomonidan yuborilgan va saqlangan ma’lumotlar bulutli xizmat provayderlarining boshqaruvida bo'ladi, bu esa axborotning maxfiyligi va yaxlitligiga xavf solishi mumkin. Ikkinchidan, bulutli muhitda axborot hajmining o'sishi shifrlash algoritmlarining samaradorligini oshirishni talab etadi. Shuningdek, ma’lumotlarni masofadan uzatish va qayta ishlash jarayonlarida paydo bo'ladigan potentsial zaifliklar ham hisobga olinishi lozim.

Ushbu tadqiqotda zamonaviy kriptografik algoritmlarning bulutli muhitda qo'llanilishi o'rganiladi. Simmetrik (AES, DES) va assimetrik (RSA, ECC) algoritmlar, ularning ishlash tezligi, resurs talabchanligi va xavfsizlik darajasi tahlil qilinadi. Tadqiqotning asosiy maqsadi – bulutli texnologiyalar uchun ma’lumotlarni himoyalashda qo'llaniladigan eng samarali va xavfsiz algoritmlarni aniqlashdir.

Mazkur maqola bulutli muhitda ma’lumotlar xavfsizligini ta'minlashga qaratilgan tadqiqotlarga hissa qo'shadi hamda foydalanuvchilarga o'z ma’lumotlarini himoyalash

uchun eng maqbul usullarni tanlashda yordam beradi. Shu bilan birga, u mutaxassislar va tadqiqotchilar uchun yangi ilmiy yondashuvlarni shakllantirishga imkon yaratadi.

Asosiy qism

Cloudda xavfsizlikni ta`minlash uchun turli usullar va algoritmlardan foydalaniladi. Ular orasida eng asosiylaridan biri kriptografik himoyalash. Cloudda tatbiq etilgan ilg‘or shifrlash algoritmlari maxfiylikni mustahkamlaydi.

Atributga asoslangan shifrlash (ABE – Attribute-Based Encryption) yangi, zamonaviy ochiq kalitli kriptografik usuldir. Ochiq kalitli shifrlash usullarida shifrlangan ma`lumotlar uchinchi tomon serverlarida saqlanadi va ruxsat berilgan (vakolatga ega) foydalanuvchilarga shifrlarni ochish kalitlari tarqatiladi. Ammo bunda kamchiliklar mavjud:

Birinchidan, vakolatga ega foydalanuvchilarga maxfiy kalitlarni taqsimlashni samarali boshqarish qiyin.

Ikkinchidan, moslashuvchanlik va o‘lchamlarning yetishmasligi.

Uchinchidan, ma`lumotlar egalari ma`lumotlarni shifrlash, deshifrlash yoki maxfiy kalitlarni tarqatishda onlayn bo‘lishlari shart.

ABE internetdagi aloqa yukini kamaytirish va yirik tizimlar uchun moslashuvchanlik va ruxsatlarni nazoratlashni oshirish orqali yuqoridagi cheklovlarni kamaytiradi.

ABE arxitekturasida uchta yirik sub’ektlar ishtirok etadi:

1. Ma`lumot egasi yoki ma`lumotlar jo‘natuvchisi.
2. Foydalanuvchi yoki ma`lumotlarni oluvchi.
3. Oldindan belgilangan atributlarga ko‘ra jo‘natuvchi va qabul qiluvchining kalitlarini yaratuvchi.

ABEda xavfsizlik darajasi yuqori bo‘lib, quyidagilar ta`minlanadi:

Ma`lumotlar konfidensialligi: Ma`lumotlar Cloudga yuklashdan oldin shifrlanadi. Tasdiqlanmagan foydalanuvchilar ma`lumotlarga kira olmaydi.

Ruxsatlarni nazoratlash: Resurslardan xavfsiz foydalanish imkonini beradi.

O‘zgaruvchanlik: Vakolatli foydalanuvchilar ortishi tizim ishlashiga ta`sir qilmaydi.

Foydalanuvchilarning javobgarligi: Foydalanuvchilar maxfiy kalitlarini hech qachon noqonuniy foydalanuvchilar bilan bo‘lishmasligini ta`minlash mumkin.

Foydalanuvchini bekor qilish: Agar foydalanuvchi tizimdan chiqsa, tizim kirish huquqlarini to‘g‘ridan-to‘g‘ri bekor qiladi va foydalanuvchining saqlangan ma`lumotlarga kirish imkoni yo‘q.

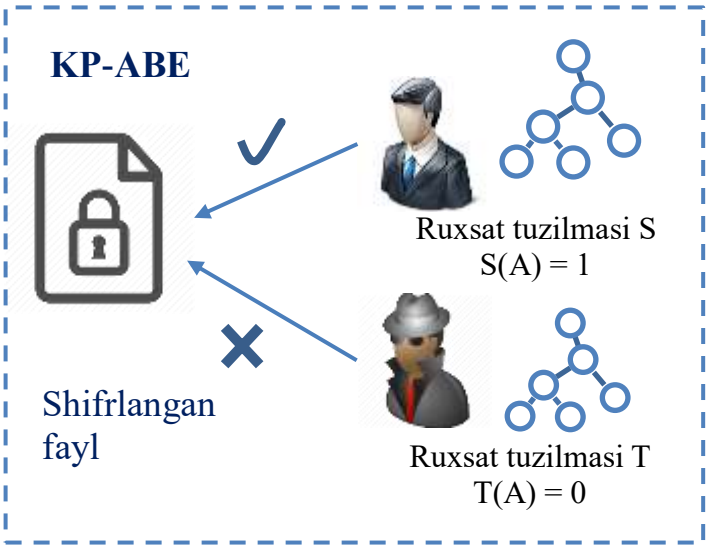
ABE ma`lumotlarni shifrlash va deshifrlash uchun identifikator sifatida atributlardan foydalanadi. Shifrlangan matn va foydalanuvchining maxfiy kaliti atributlarga bog‘liq. ABE 4 xil algoritmdan foydalanadi: sozlash, kalit generatsiyasi, shifrlash va deshifrlash.

ABE asosida yaratilgan ko‘plab usullar mavjud bo‘lib, quyida ularning har biri alohida ko‘rib chiqiladi.

Key Policy ABE (KP-ABE). KP-ABE asosiy ABE ning o‘zgartirilgan shaklidir. Dastlab xavfsizlik parametrlari 1-algoritmda ko‘rsatilganidek sozlanadi: shifrlanadigan matn M, tavsiflovchi atribut S, shifrlangan matn CT (cipher text).

1-algoritm

Setup (security parameter) -> PK, MK
Encrypt (PK, M, S) -> CT
KeyGen (MK, A) -> D
Decrypt (CT, D) -> M if S ∈ A
A = ruxsat tuzilmasi,
D = maxfiy kalit,
S = tavsiflovchi atribut,
M = xabar.



1-rasm. KP-ABE algartmi.

Faqatgina CT (cipher text – shifrlangan matn) ning atributlari foydalanuvchi maxfiy kalitiga 1-rasmdagidek mos kelsagina shifrlangan matnni deshifrlashni amalga oshirish mumkin.

KP-ABE quyidagi cheklovlarga ega:

- Yubruvchi ma`lumotlarni kimlar deshfrlay olishini belgilay olmaydi;
- Moslashuvchan emas.

Expressive Kep Policy (EKP-ABE). EKP-ABE 2-algoritmdagidek, monotonik bo‘lmagan ruxsat tuzilmalari qo‘llaniladigan KP-ABE ning kengaytmasi hisoblanadi.

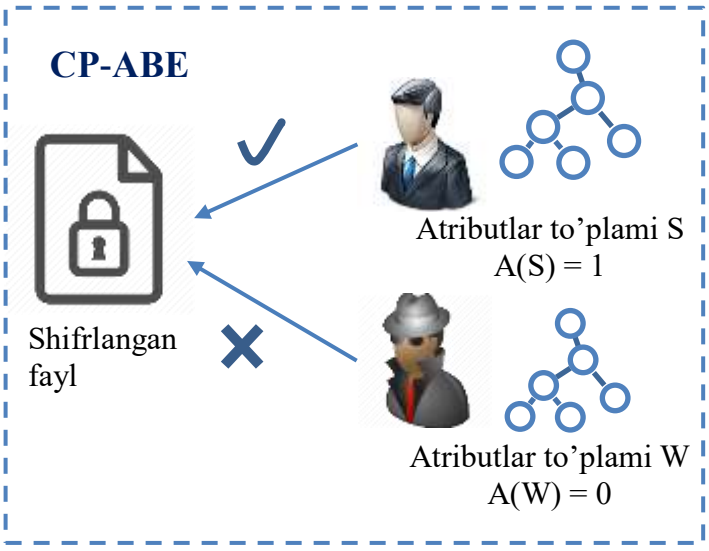
2-algoritm

Setup (security parameter) -> PK, MK
Encrypt (PK, M, S) -> CT
KeyGen (MK, Au) -> D
Decrypt (CT, D) -> M if S ∈ Au
Au = monotonik bo‘lmagan ruxsat tuzilmasi,
D = maxfiy kalit,
S = tavsiflovchi atribut,
M = xabar.

Monotonik bo‘lmagan ruxsat tizimida salbiy atributlar mavjud. Masalan, “CS AND Std NOT graduate” degani, “kompyuter fani talabasi, ammo bitiruvchi emas” degan ma`noni anglatadi. EKP-ABE atributga salbiy so‘z qo‘shish orqali yanada moslashuvchan kirish tizimi hosil qiladi, ya`ni bunday xususiyatlarga ega bo‘lgan shaxs ma`lumotni deshifrlay olmaydi. EKP-ABE ning asosiy cheklovi, u shifrlangan ma`lumotlarga aloqador bo‘lmagan, lekin shifrlangan ma`lumotlarda mavjud bo‘lishi mumkin bo‘lgan juda ko‘p salbiy atributlarni talab qiladi. Bu katta xarajatlarga olib kelishi mumkin.

Cipher text policy ABE (CP-ABE). CP-ABE bu KP-ABE ning teskari modelidir . CP-ABE da 3-algoritmda ko‘rsatilganidek, deshifrlash kaliti tavsiflovchi atributlar majmuasi bilan izohlansa, ruxsat tizimini shifrlangan ma`lumot bilan bog‘lash mumkin. Kalit shifrlangan matnni deshifrlashda ishlatilishi mumkin, agar 16-rasmda tasvirlanganidek foydalanish qoidalariga javob beradigan bo‘lsa. Ushbu yondashuv ishonchli server buzilgan bo‘lsa ham mustahkamroq ishlashda davom etadi. Shifrlangan ma`lumotlardan foydalanishni nazorat qilish jihatidan KP-ABE dan ustundir.

3-algoritm
Setup (security parameter) -> PK, MK Encrypt (PK, M, A) -> CT KeyGen (MK, S) -> D Decrypt (CT, D) -> M if S ∈ A A = ruxsat tuzilmasi, D = maxfiy kalit, S = tavsiflovchi atribut, M = xabar.

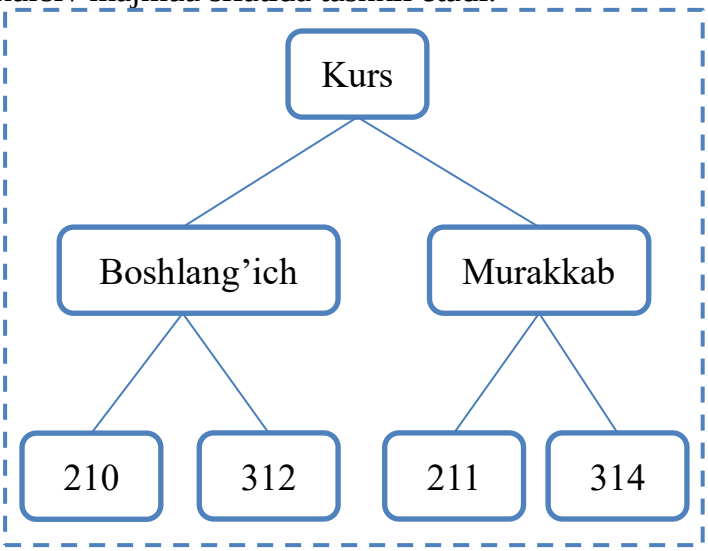


2-rasm. CP-ABE algoritmi.

Asosiy cheklovlar quyidagilar:

- Deshifrlash kaliti faqat bir tizimda mantiqiy ravishda tashkil etilgan foydalanuvchi atributlarini qo‘llab quvvatlaydi;
- CP-ABE ruxsatlarni nazoratlashda moslashuvchanlik va samaradorlikka ega bo‘lgan korxonalarning talablarini qondira olmaydi.

Cipher text Policy Attribute-Set-Based Encryption (CP-ASBE). CP-ASBE bu CP-ABE ning kengaytirilgan shakli bo‘lib, unda CP-ABE dan farqli o‘laroq, foydalanuvchi atributlarining rekursiv majmui asosida tuzilgan tizim ishlatiladi. Ko‘pgina real tizimlarda ko‘p sonli qiymatlar ko‘rsatilganidek, bitta atributga beriladi. Ushbu muammoni bartaraf etish uchun CP-ASBE sxemasidan foydalaniladi. CP-ASBE foydalanuvchi atributlarini rekursiv majmua sifatida tashkil etadi.



3-rasm. Bir nechta sonli atributlar algoritmi

Ushbu yondashuvning asosiy cheklovi shuki, berilgan kalitda, atributlarni, bir necha atributlar majmuasidan biriktirib olish juda qiyin.

Hierarchical Attribute-Based Encryption (HABE). Ushbu sxema HIBE va CP-ABE xususiyatlarini birlashtirib, ruxsatlarni nazoratlash, moslashuvchanlik va to‘liq vakillikni taqdim etadi [37]. HABE dizyunktiv falsafa asosida ishlaydi va bir konyunktivdagi barcha atributlar bir domen tomonidan boshqariladi.

Unda quyidagi cheklovlar mavjud:

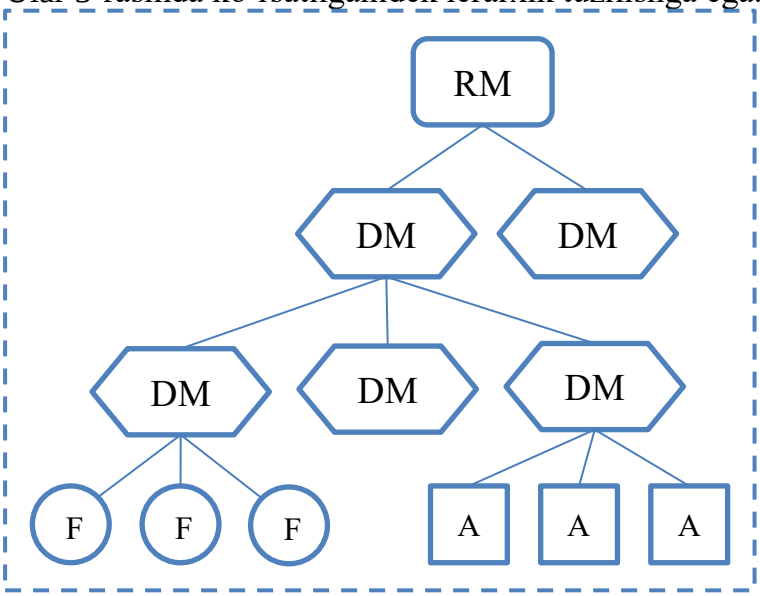
- Bir xil xususiyatlar bir nechta domen tomonidan boshqarilishi mumkin bo‘lsada, buni amalga oshirish qiyin;
- Kompleks atributlarni samarali qo‘llab quvvatlamaydi;
- Ko‘p miqdordagi vazifalarni qo‘llab-quvvatlamaydi.

Hierarchical Attribute-Set-Based Encryption (HASBE). Ushbu sxema HIBE va CP-ABE xususiyatlarini o‘zida birlashtiradi. HASBE da har bir ma`lumotdan foydalanuvchi va ma`lumot egasi domen ma`muriyati tomonidan boshqariladi. Tizimda ishtirok etishi mumkin bo‘lgan besh turdagi sub’ektlar mavjud:

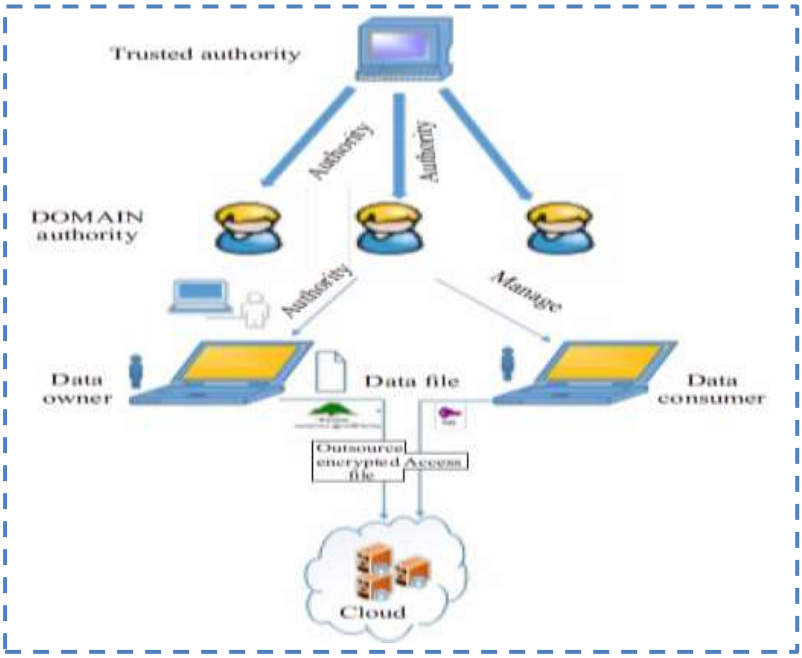
1. Ma`lumot egasi.
2. Ma`lumotdan foydalanuvchi.

3. Domen boshqaruvi.
4. Ishonchli vakil.
5. Cloud xizmati provayderi.

Ular 3-rasmda ko‘rsatilganidek ierarxik tuzilishga ega.



4-rasm. 3 bosqichli HABE tuzilishi.



5-rasm. HASBE modeli.

HASBE ning cheklovlari quyidagilar:

- Agar quyi darajali boshqaruv ishlamay qolsa, jarayon to‘liq to‘xtab qoladi.

- Domen ierarxiyasi juda murakkab va so‘rovni qabul qilish va amalga oshirish uchun ketadigan ortiqcha vaqt tizimi ish faoliyatini yomonlashtiradi.

Cipher text Policy Weighted Attribute-Based Encryption (CP-WABE). CP-WABE an’anaviy CP-ABE ning umumlashtirilgan shaklidir. CP-WABE kirishni ta`minlaydi va asosan taqsimlash tizimlarida ishlatiladi. Ushbu sxemani to‘rtta algoritmdan iborat bo‘lgan 4-algoritm misolida ko‘rish mumkin:

4-algoritm
1. Setup (1^{λ}, U) -> PK, MK (1^{λ} = xavfsizlik parametri, U = atribut) 2. Encrypt (M, A, PK) -> CT (CT talab qilingan atribut bilan bog‘liq) 3. KeyGen (MK, S) -> SK (S – talab qilingan atribut) 4. Decrypt (CT, SK) -> M
Agar SK da mavjud atributlar majmui ruxsat tuzilmasini qanoatlantirsa

CP-WABE dagi cheklovlar quyidagilar:

- Hisoblash qiymati juda yuqori.
- Shifrlangan matn uzunligi ba`zi ilovalarni ish faoliyatida ta`sir qiladi.

Key Policy Weighted Attribute-Based Encryption (KP-WABE). An’anaviy KP-ABE sxemasida ko‘rsatilgan atributlarning xarakteristikalari xir xil darajada. Real muhitda har bir atribut ahamiyatiga qarab turli talabga ega. KP-WABE hisoblashlarni va shifrlangan matn hajmini kamaytirish orqali CP-WABE tizimidagi kamchiliklarni bartaraf etadi. KP-WABE da, ma`lumot qabul qiluvchining maxfiy kaliti aniq bir turdagi talab etilgan ruxsat tuzilmasiga ega va ma`lumot egasi aniq atributlarga ega bo‘lgan barcha qabul qiluvchilar uchun ma`lumotlarni shifrlaydi.

KP-WABE 5-algoritmda keltirilgan to‘rt turdagi algoritmlardan iborat [40]:

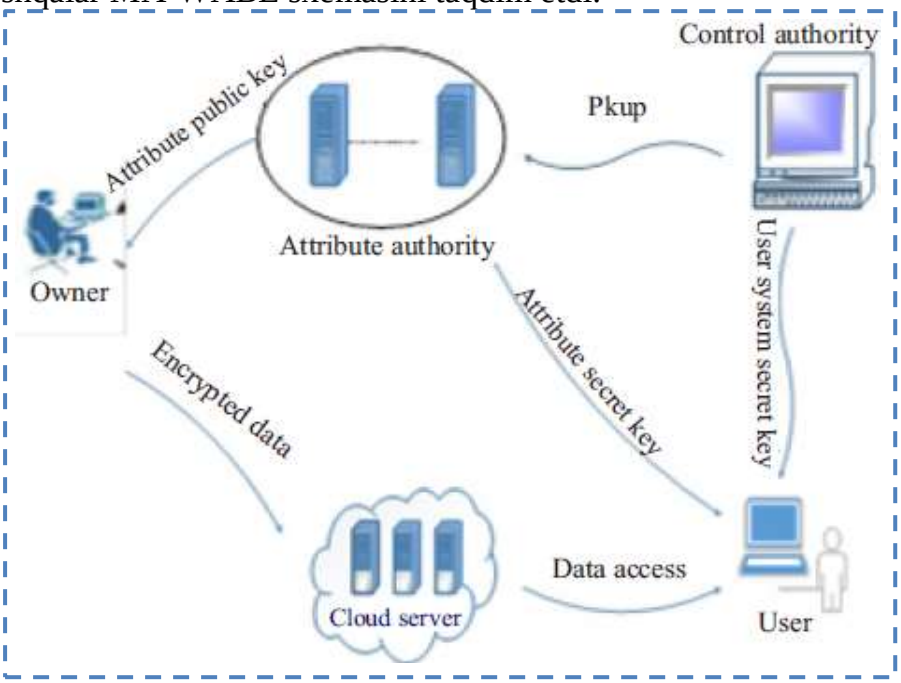
4-algoritm
1. Setup (1^{λ}, U) -> PK, MK (1^{λ} = xavfsizlik parametri, U = atribut) 2. Encrypt (M, S^0, PK) -> CT (CT talab qilingan atribut S^0 bilan bog‘liq) 3. KeyGen (MK, A) -> SK (A – talab qilingan ruxsat tuzilmasi va SK uni o‘z ichiga oladi) 4. Decrypt (CT, SK) -> M
Agar, SK dagi ruxsat tuzilmasini, talab etilgan atributlar majmui S qanoatlantirsa

Deshifrlashda, talab qilinadigan atributlar majmuasi talab qilingan ruxsat tuzilmasini qanoatlantirishi shart.

KP-WABE dagi cheklovlar quyidagilar:

- Manba kimlar ma`lumotni deshifrlay olishini belgilay olmaydi.
- Bir nechta vakolatli organlar tomonidan berilgan atributlarni boshqarish qiyin.

Multi-Authority-based Weighted Attribute-Based Encryption (MA-WABE). Mavjud ABE shifrlash usullarining ko‘pchiligi maxfiy va ochiq kalitlarni boshqarish uchun yagona vakolatga ega. Ko‘pgina hollarda foydalanuvchilarning ko‘plab vakolatlari uchun atributlari bo‘ladi va ma`lumot egalari boshqa vakolatga ega bo‘lgan foydalanuvchilar bilan ma`lumotlarni almashadilar. Ushbu muammoni hal qilish uchun turli “multi-authority attribute-based access control” sxemalari joriy qilindi. Yang va Jia Cloudda ma`lumotlarni saqlash uchun “multi-authority attribute-based access control” tizimni joriy etdi. Wang va boshqalar MA-WABE sxemasini taqdim etdi.



1.6-rasm. Multi-authority-based access control tizimi modeli

Tizim 20-rasmda keltirilgani kabi beshta asosiy ob’ektdan tashkil topgan:

- Cloudga yuklashdan oldin ma`lumotlarni shifrlovchi ma`lumot egasi;
- Cloud server, ma`lumotlarni saqlash uchun;
- Darajasiga qarab foydalanuvchilarning atributlarini berish, yangilash va bekor qilish uchun Atributlar markazi;
- Har bir foydalanuvchi uchun global foydalanuvchi identifikatori va Atributlar markaziga ochiq kalitni belgilaydigan Markaziy boshqaruv;
- Foydalanuvchilar (ma`lumotdan foydalanuvchilar).

MA-WABE ruxsatlarni nazoratlashni va ko‘p vakolatli xavfsizlikni ta`minlaydi.

1.1-jadval

Algoritm-lar	Ruxsatlarni nazoratlash	Hisob-lash	Foy-larni bekor qilish samaradorligi	Samrador-lik	To‘qna-shuvga bardoshlilik
ABE	Past	O‘rtac	O‘rtacha	O‘rtacha	O‘rtachada

		ha			n pastroq
KP-ABE	Past	O‘rtacha	Past	O‘rtacha	O‘rtacha
EKP-ABE	KP-ABE dan yaxshiroq	O‘rtacha	O‘rtacha	KP-ABE dan yuqoriroq	O‘rtachadan yuqori
CP-ABE	O‘rtacha	O‘rtacha	Past	O‘rtacha	Yaxshi
CP-ASBE	CP-ABE dan yuqoriroq	CP-ABE dan pastroq	O‘rtachadan yuqori	CP-ABE dan yaxshiroq	Yaxshi
HABE	Yuqori	Past	O‘rtacha	O‘rtacha dan yuqori	Yaxshi
HASBE	Yuqori	Past	O‘rtachadan yuqori	Yuqori	Yaxshi
CP-WABE	Juda yuqori	Yuqori	O‘rtachadan yuqori	Yuqori	Yaxshi
KP-WABE	Juda yuqori	Past	O‘rtachadan yuqori	Yuqori	Yaxshi
MA-WABE	Juda yuqori	Past	Juda yuqori	Juda yuqori	Juda yaxshi

Umumiy holda shuni aytish mumkinki, ABE Cloud computinda ruxsatlarni nazoratlash uchun keng ishlatiladigan shifrlash usulidir. ABE ning asosiy ustunligi shundan iboratki, u foydalanuvchilarga kuchli shifrlash imkoniyatini beradi. Cloudda foydalanish uchun ruxsatlarni nazoratlash, moslashuvchanlik va samaradorlik mezonlari asosida WABE tizimi boshqa tizimlardan yaxshiroq.

Xulosa:

Bulutli texnologiyalar tez sur'atlar bilan rivojlanib, foydalanuvchilarga ma’lumotlarni masofadan saqlash va boshqarishning keng imkoniyatlarini taqdim etmoqda. Ammo ma’lumotlarning xavfsizligini ta'minlash bulutli muhitda eng muhim va dolzarb masalalardan biri hisoblanadi. Ushbu maqolada ma’lumotlarni himoyalash uchun qo'llaniladigan zamonaviy kriptografik algoritmlar tahlil qilinib, ularning samaradorligi, xavfsizlik darajasi va bulutli tizimlardagi qo'llanilish imkoniyatlari ko'rib chiqildi.

Tahlillar shuni ko'rsatdiki, simmetrik kriptografik algoritmlar, masalan, AES, ma’lumotlarni shifrlash va shifrdan chiqarishda yuqori tezlikka ega bo'lib, katta hajmdagi ma’lumotlarni himoyalash uchun samarali vosita hisoblanadi. Assimetrik algoritmlar, masalan, RSA va ECC, yuqori xavfsizlikni ta'minlashda muhim rol o'ynaydi, ammo ular resurs talabchanligi sababli ma’lumotlarni katta hajmda shifrlash uchun kamroq qo'llaniladi. Shu sababli, bulutli muhitda ma’lumotlarni himoyalashda simmetrik va assimetrik usullarni birgalikda qo'llash – eng samarali yondashuv hisoblanadi.

Maqolada shuningdek, bulutli tizimlarda kriptografik algoritmlarni tanlashda hisobga olinishi kerak bo'lgan asosiy omillar, jumladan, ishlash samaradorligi, xavfsizlik darajasi, hisoblash xarajatlari va zaifliklar batafsil ko'rib chiqildi.

Natijalar shuni ko'rsatadiki, ma’lumotlarni himoyalashda muvozanatni ta'minlash uchun algoritmlarni tizimning ehtiyojlariga va resurslariga mos ravishda tanlash zarur. Ma’lumotlarni shifrlash va boshqarish jarayonida zamonaviy kriptografik yondashuvlardan foydalanish foydalanuvchilarning maxfiyligi va ma’lumotlar yaxlitligini ta'minlashga yordam beradi.

Ushbu maqola tadqiqotchilar, dasturiy ta'minot ishlab chiquvchilar va axborot xavfsizligi bo'yicha mutaxassislar uchun foydali bo'lib, bulutli texnologiyalarning xavfsizligini ta'minlash borasida muhim ilmiy va amaliy tavsiyalarni taqdim etadi. Maqolada keltirilgan xulosalar bulutli tizimlar xavfsizligini oshirishda samarali yondashuvlarni ishlab chiqishga asos bo'lib xizmat qiladi.

ADABIYOTLAR RO‘YXATI:

1. Harris T. Cloud Computing-An Overview, Whitepaper // Torry Harris Business Solutions. – 2010.
2. Wikipedia, “Cloud computing”, Reference Link https://en.wikipedia.org/wiki/Cloud_computing.
3. Puthal D. et al. Cloud computing features, issues, and challenges: a big picture //Computational Intelligence and Networks (CINE), International Conference. – IEEE, 2015. – C. 116-123.
4. Armbrust M. et al. A view of cloud computing //Communications of the ACM. – 2010. – T. 53. – №. 4. – C. 50-58.
5. Vishwanath K. V., Nagappan N. Characterizing cloud computing hardware reliability //Proceedings of the 1st ACM symposium on Cloud computing. – ACM, 2010. – C. 193-204.
6. Diversity Limited, Rackspace Hosting, “Understanding The Cloud Computing Stack SaaS, PaaS, IaaS”, 2011.
7. Infrastructure-as-a-Service Builder’s Guide. v1.0.2 – Q4 2009. Copyright 2009-2010, Cloudscaling (a business of neoTactics, Inc).