BULUTLI HISOBLASH TIZIMLARIDA MA’LUMOTLAR XAVFSIZLIGINI TA’MINLASHDA FOYDALANILADIGAN KRIPTOGRAFIK ALGORITMLAR TAHLILI

PhD, dotsent **B.K. Yusupov, c**
O‘zbekiston Respublikasi Mudofaa vazirligi Axborot-kommunikatsiya texnologiyalari va aloqa harbiy instituti

Annotatsiya. *Ushbu maqola bulutli hisoblashning turli afzalliklari va asosiy xavfsizlik muammolarini muhokama qiladi, shuningdek, turli kriptografik shifrlash algoritmlarini tahlil qiladi. Bundan tashqari, bulutli hisoblashda qo‘llanilayotgan shifrlash algoritmlarining samaradorligi taqqoslanib Gamomorfik shifrlash algortimi taklif etilgan.*

Kalit so‘zlar: *Provayder, Google, AES, DES, RSA, Gomomorfik, kriptografiya, konfidensiyal.*

Annotation. *This article discusses the various benefits and key security issues of cloud computing, as well as analyzes various cryptographic encryption algorithms. In addition, the efficiency of the encryption algorithms used in cloud computing is compared and the Hamomorphic encryption algorithm is proposed.*

Keywords: *Provider, Google, AES, DES, RSA, Homomorphic, cryptography, confidential*

Аннотация. *В этой статье обсуждаются различные преимущества и ключевые проблемы безопасности облачных вычислений, а также анализируются различные алгоритмы криптографического шифрования. Кроме того, сравнивается эффективность алгоритмов шифрования, используемых в облачных вычислениях, и предлагается хамоморфный алгоритм шифрования.*

Ключевые слова: *провайдер, Google, AES, DES, RSA, гомоморфный, криптография, конфиденциальный.*

XXI-asrga kelib Internet va tarmoq xizmatlari soni va sifati kun sayin ortib borboqda. 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. Ushbu texnologiya har qanday vaqtda axborot texnologiyalari talablarini qondirishi mumkin. U ijara yoki ijara asosida bulutda iste’molchi ilovalarini saqlashi, yaratishi, boshqarishi, ishga tushirish imokiniyatini yaratadi. Virtualizatsiya orqali bir nechta iste’molchilarga xizmat sifatida resurslarni

taqdim etadi. Ushbu texnologiya ko‘plab axborot texnologiyalari tashkilotlariga ulkan iqtisodiy to‘siqlarsiz biznesni boshlashga yordam beradi va asta-sekin sanoatdagi yetakchi tashkilotga aylanishini ta’minlaydi. Tashkilotlarning kattaligidan qat’iy nazar, ob’yektlarga xizmat ko‘rsatishi mumkin.

Ushbu xizmatlar hisoblash texnologiyasi sohasiga yangilik sifatida kirib keldi. Bulutli hisoblash - bu tez sozlanishi mumkin bo‘lgan hisoblash resurslarining umumiy bazasi bo‘lib, tarmoqqa qulay, talab bo‘yicha kirishni ta’minlash uchun model. Bunda foydalanish minimal boshqaruv harakati yoki xizmat ko‘rsatuvchi provayderning o‘zaro ta’siri bilan ta’minlanadi va chiqariladi [1]. Turli xil bulutli xizmat ko‘rsatuvchi provayderlar Amazon, Google, IBM, Microsoft va Salesforce.com xizmatlar uchun o‘zlarining bulutli infratuzilmasini taklif qiladi.

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.

Bunday Kriptografik algoritmlarga AES, DES, RSA, Gomomorfik shifrlash usul va algoritmlari misol bo‘la oladi. Bu algoritmlar tomonidan bajariladigan ikkita funksiya bajarib, ular ma’lumotni shifrlash va shifrlangan ma’lumotni ochishdan iboratdir.

Ushbu eng keng tarqalgan va ishonchli shifrlash algoritmlarining afzalliklari tahlilini ko‘rib chiqaylik.

DES (Data Encryption Standard) - bu Milliy standartlar va texnologiyalar instituti (NIST) tomonidan nashr etilgan simmetrik blokli shifrdir. U shifrlash va deshifrlash uchun bitta kalitdan (maxfiy kalit) foydalanadi. U 56 bitli kalit bilan 64 bitli ma’lumotlar bloklarida ishlaydi va Raundlar uchun kalit hajmi 48 bitga teng bo‘ladi.

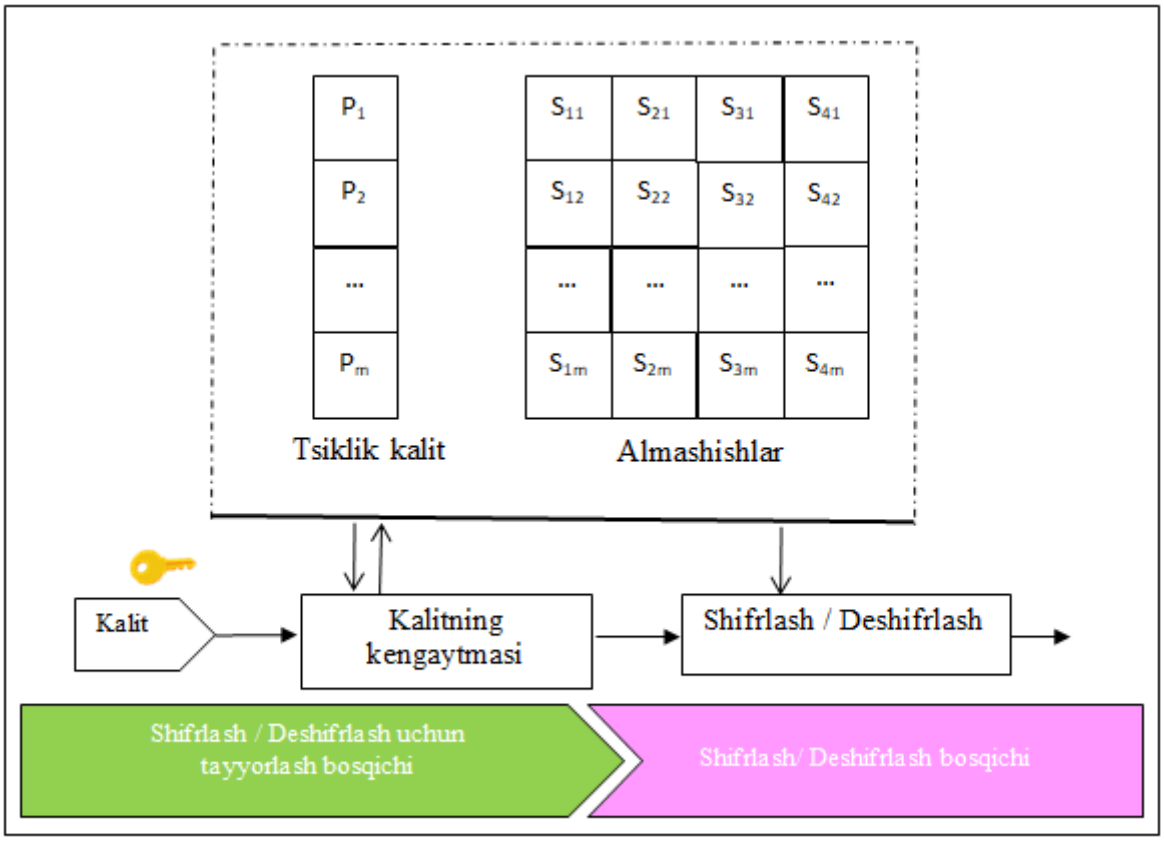
Butun ochiq matn 64 bitli bloklarga ajratiladi. Bu jarayonda agar zarurat paydo bo‘lsa, oxirgi blok ham to‘ldiriladi.

DES algoritmi ikkita almashtirishdan (P-boxes) va o‘n oltita Feistel raundidan iborat bo’lib, ushbu jarayonni uch bosqichga bo‘lish mumkin:

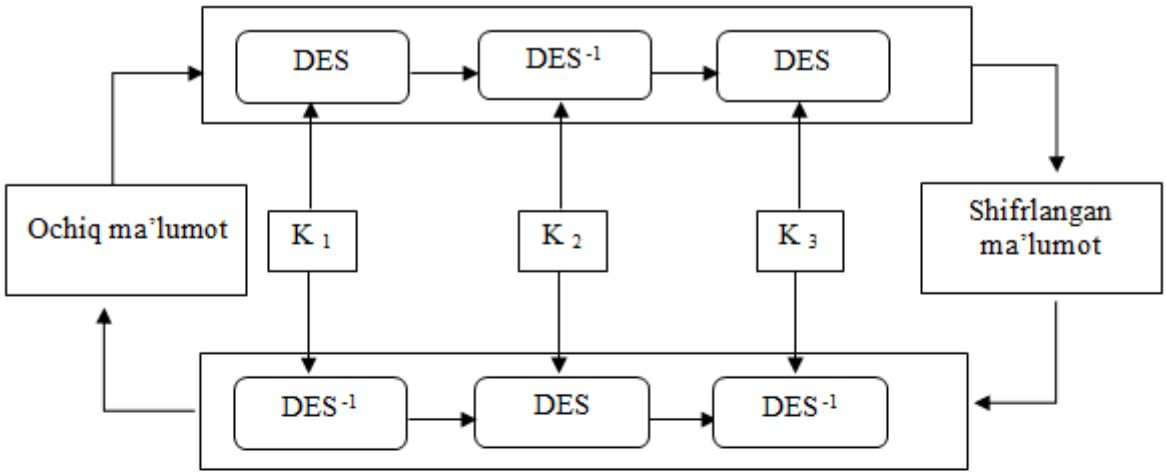
1. Dastlabki almashtirish 64 bitli ochiq matnning bitlarini qayta tartibga soladi. U hech qanday kalitlardan foydalanmaydi, oldindan belgilangan shaklda ishlaydi.

2. Ikkinchi bosqichda 16 ta Feistel raundlari mavjud. Har bir tur oldindan belgilangan algoritmga muvofiq ishlab chiqarilgan 64-bitli chiqishni ishlab chiqarish uchun ochiq matn bitlariga taalluqli boshqa 48-bitli raund kalitdan foydalanadi. Raund kalit generatori 56 bitli shifrlangan kalitdan o‘n oltita 48 bitli kalitni hosil qiladi.

3. Nihoyat, oxirgi bosqich yakuniy almashtirishni amalga oshiriladi. Dastlabki almashtirishning teskari ishlashi va chiqish 64 bitli shifrlangan matn hosil bo‘ladi.

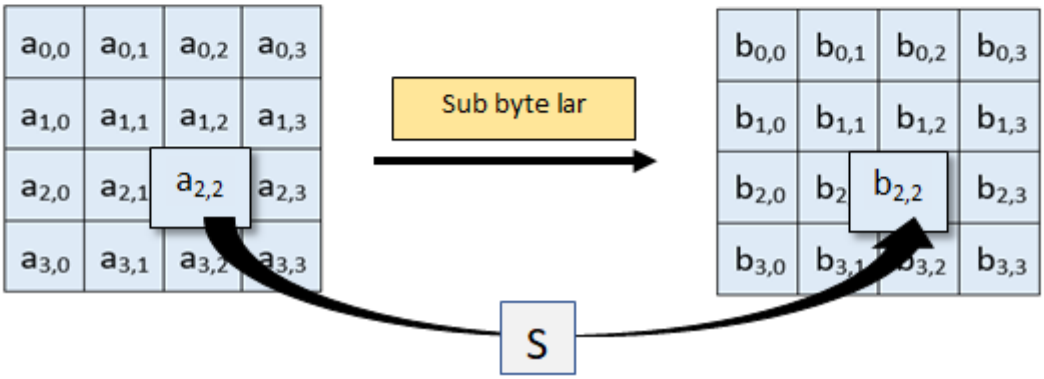


1- rasm. Ma'lumotlarni DES algoritmida shifrlash va deshifrlashning matritsali ko'rinishi



2- rasm. Ma’lumotlarni DES algoritmida shifrlash va ochishning sxematik ko‘rinishi

AES ***(Advanced Encryption Standard)*** - bu Milliy standartlar va texnologiyalar instituti (NIST) tomonidan nashr etilgan simmetrik blokli shifr. Eng ko‘p qabul qilingan simmetrik shifrlash AES hisoblanadi. U baytlar bo‘yicha hisoblashni amalga oshiradi, 128 bit ochiq matn blokini 16 bayt deb hisoblaydi. Ushbu 16 bayt matritsa sifatida ishlov berish uchun to‘rtta ustun va to‘rt qatorga joylashtirilgan.



3-rasm. AES shifrlash algoritmining ishlash tamoyili

U almashtirishlar yordamida butun ma’lumotlar blokida ishlaydi. AES shifrlash uchun ishlatiladigan kalit o‘lchami shifrlash jarayonida foydalaniladigan transformatsiyalar sonini belgilaydi [4,5].

Mumkin bo‘lgan kalitlar va roundlar soni quyidagilar:

- 10 round uchun 128-bit kalit.
- 12 round uchun 192-bit kalit.
- 14 round uchun 256-bit kalit.

DESga nisbatan AESning asosiy afzalliklari quyidagicha:

1. Ma’lumotlar blokining uzunligi 128 bit.
2. Versiyaga qarab kalit uzunligi 128/192/256 bit.
3. Aksariyat protsessorlar AES ni qo‘llab-quvvatlashni o‘z ichiga olgan.
4. O‘rniga qo‘yish va o‘rin almashtirishlardan foydalaniladi.
5. Mumkin bo‘lgan kalitlar: 2128 , 2192 va 2256 [6]

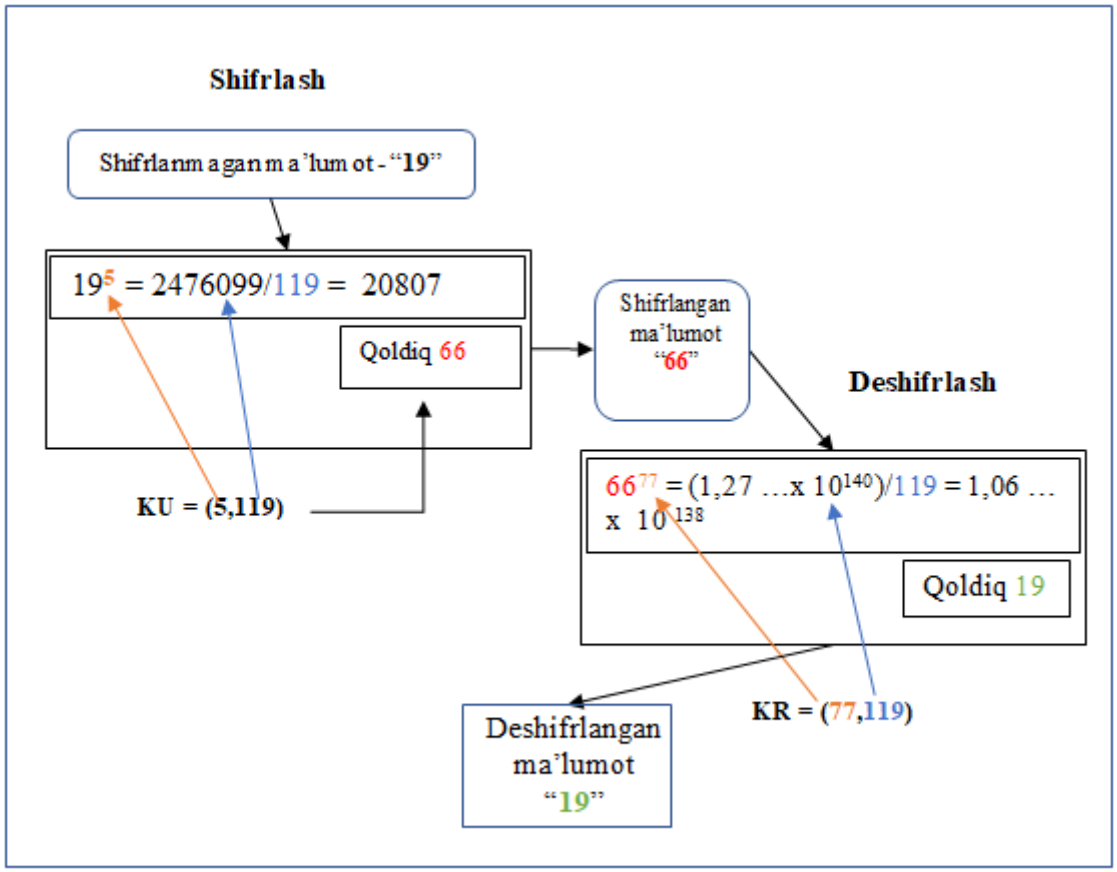
6. DESga qaraganda xavfsizroq.
7. Eng ko‘p qabul qilingan simmetrik shifrlash algoritmi

RSA (Rivest-Shamir-Adleman) – 1977 yilda Ron Rivest, Adi Shamir va Len Adlemen tomonidan ishlab chiqilgan ochiq kalitli shifrdir. Bu eng mashhur assimmetrik shifrlash algoritmidir. Ushbu algoritm turli xil ma’lumotlar bloklari hajmidan foydalanadi. U shifrlash va deshifrlash uchun assimmetrik kalitlarga ega.

Umumiy va shaxsiy kalitlarni yaratish uchun ikkita tub sondan foydalanadi. Ushbu ikki xil kalit shifrlash va shifrni ochish uchun ishlatiladi. Bu algoritmni keng ma’noda uch bosqichga bo‘lish mumkin: ikkita tub sondan foydalangan holda kalitlarni yaratish, shifrlash va deshifrlash.

RSA bugungi kunda yuzlab dasturiy mahsulotlarda qo‘llaniladi va kalit almashinuvi, raqamli imzolar yoki kichik ma’lumotlar bloklarini shifrlash uchun ishlatilishi mumkin[7]. Bu algoritm asosan ochiq aloqa kanalida xavfsiz aloqa va autentifikatsiya qilish uchun qo‘llanilib kelinmoqda.

RSA algoritmining ishlashini DES bilan solishtirganda, agar biz kalitni loyihalash uchun p & q (tub sonlar) ning kichik qiymatlaridan foydalansak, shifrlash jarayoni juda zaiflashadi va ma’lumotlarni tasodifiy ehtimollik nazariyasi hujumlari yordamida shifrni buzish orqali ochiq matnga ega bo‘lish mumkin. Boshqa tomondan, agar katta p & q uzunliklari tanlansa, u ko‘proq vaqt sarflaydi va DES [7] bilan solishtirganda ishlash yomonlashadi. RSA shifrlash algoritmlarining ishlash tezligi simmetrik algoritmlarga nisbatan sekin ishlaydi.



4-rasm. RSA shifrlash algoritmining ishlash tamoyili

Kalitlar quyidagicha hisoblanadi:

1. Ikkita oddiy son tanlanadi: p=7 va q = 17.
2. Xisoblanadi n = pq = 7*17 = 119
3. Xisoblanadi f(n) = (p-1)(q-1) = 96
4. f(n) dan kichik va o‘zaro tub bo‘lgan son tanlanadi. Hozirgi holatda f(n) = 96 ga teng va shartni qanoatlantiruvchi son bu – 5.
5. Shunday d son tanlanadiki, de=1 (mod 96) va d < 96. O‘z navbatida bunga mos qiymat d=77 ga teng bo‘ladi. Ya’ni 77*5 = 385=4*96+1
6. Natijada ochiq kalit sifatida KU = {5,119} olinsa, shaxsiy kalit sifatida KR = {77,119} ga ega bo‘linadi.

Ochiq kalit ma’lumotlarni shifrlash uchun, shaxsiy kalit esa uni ochish uchun ishlatiladi. RSA keng qo‘llaniladi, lekin Internet orqali o‘tadigan haqiqiy ma’lumotlarni shifrlash uchun emas. Buning o‘rniga, u kalitlarni boshqa algoritm bilan shifrlash uchun ishlatiladi, ayniqsa shaxsiy kalitingizni baham ko‘rishingiz kerak bo‘lganda. Ma’lum qilinishicha, 768-bitli RSA kaliti buzilgan, ammo hozirda RSA kalitlarining aksariyati 2048-bit va 4096-bit. Bu shifrlash uchun xavfsizroq qiladi, lekin u juda sekin.

Gomomorfik algoritm. Bu shifrlangan ma’lumotlar (shifrlangan matn) ustidan ajoyib hisoblash imkoniyatini beruvchi va shifrlangan natijani qaytaradigan shifrlash algoritmidir. Ushbu algoritm xavfsizlik va maxfiylik bilan bog‘liq ko‘plab muammolarni

hal qilishi mumkin. Ushbu algoritmda mijoz va provayder saytida sodir bo‘ladigan shifrlash va deshifrlash shifrlangan ma’lumotlar asosida ishlaydi.

Bu mijoz va xizmat ko‘rsatuvchi provayder o‘rtasida ma’lumotlarni uzatishda tahdidni hal qilishi mumkin, u xizmat ko‘rsatuvchi provayderdan ochiq matnni yashiradi, provayder faqat shifrlangan matnda ishlaydi.

Gomomorf shifrlash shifrlangan ma’lumotlarda dastlabki ma’lumotlardan foydalanmasdan murakkab matematik operatsiyalarni bajarishga imkon beradi. X1 va X2 ochiq matnlari hamda tegishli Y1 va Y2 shifrlangan matnlar uchun gomomorf shifrlash sxemasi P1 G P2 dan foydalanmasdan X1 G X2 ni Y1 va Y2 dan hisoblash imkonini beradi. Kriptotizim multiplikativ yoki qo‘shimchali Gomomorf bo‘lib, u ko‘paytirilishi mumkin bo‘lgan operatsiyaga qarab ko‘paytiriladi [7]. Gomomorfik kriptotizimlar boshqa kriptotizimlar kabi maxfiylik darajasini ta’minlaydi, shu bilan birga ma’lumotlar bilan operatsiyalarni ma’lumotlarni deshifrlamasdan bajarishga imkon beradi.

Mijoz va server o‘rtasidagi to‘liq maxfiylik hech qanday kamaymagan funksionalliksiz amalga oshiriladi. Bunday tizimlar deyarli hamma narsaga qo‘llanilishi mumkin masalan, hisoblash, ovoz berish, bank, bulutli hisoblash va boshqalarda.

Bulutli hisoblash ko‘plab afzalliklarni taqdim etsada, bulutli hisoblash ham ko‘p muammolarga duch keladi. An’anaviy tarmoqdan bulutli tarmoqga o‘tishda kompaniyalar ushbu tizimning afzalliklari va muammolaridan xabardor bo‘lishlari kerak.

Ushbu muammolarni tahlil qilganda, ma’lumotlar xavfsizligi bulutli hisoblashdagi eng dolzarb masaladir. Ko‘plab tadqiqotlarning natijalariga ko‘ra texnik mutaxasislarning 70% dan ortig‘i xavfsizlik va ma’lumotlar maxfiyligi muammolari sababli bulutli xizmatlardan foydalanmasligining asosiy sababi deb hisoblaydi [2].

Aksariyat tashkilotlar ushbu xavfsizlik masalasini diqqat bilan kuzatib boradilar va bulutli makonga o‘tishga shoshilmaydilar. Bu bulutli hisoblashning yetuklik darajasining yetishmasligining asosiy sababidir. Xavfsizlik muammolarining ba’zilari quyida muhokama qilinadi.

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.

Konfidensiallikning umumiy yechimi Shifrlash algoritmlari bo‘lib, buning uchun asosan simmetrik va assimetrik algoritmlardan foydalaniladi. Ma’lumotlarning konfidensialligini ta’minlashning yechimi shifrlash bo‘lsada, bu bilan bog‘liq ko‘plab savollar tug‘iladi:

1. Shifrlash va deshifrlash qayerda amalga oshirilmoqda (mijoz tomoni yoki bulut tomoni).

2. Shifrlangan ma’lumotlarni qanday qidirish kerak.

3. Mijozdan bulutga ma’lumotlarni uzatishda qanday tahdidlar mavjud?

4. Xizmat ko‘rsatuvchi provayder tomonidan ma’lumotlardan noto‘g‘ri foydalanish.

5. Xizmat ko‘rsatuvchi provayder tomonidan kalitdan har qanday noto‘gri foydalanish.

6. Va shu kabi savollar.

Ma’lumotlar bulutdan hayot siklining oxirida olib tashlanishi, xotira qayta formatlanishi yoki qayta ishlanishi kerak. Ma’lumot saqlagich vositalarini qayta formatlash avval yozilgan ma’lumotlarni saqlash vositalaridan olib tashlamaydi, lekin keyinchalik unga kirish yoki qayta tiklash ham mumkin. Axborot vositalarini qayta ishlash uchun aniq standart yo‘q. Ushbu ma’lumotlarni qayta ishlash bulutdan apparat resurslarini chiqarishni qiyinlashtiradi. Aksariyat foydalanuvchilar ajratilgan resurslar va saqlash joylari haqida bilishmaydi, Ushbu muammo tufayli foydalanuvchilar bitta xizmat ko‘rsatuvchi provayderga bog‘langan. Ma’lumotlarning saqlanishiga qarshi kurashish uchun turli usullar ishlab chiqilgan.

Xulosa

Bulutli hisoblash - bu axborot texnologiyalari sohasidagi dunyoda yangi avlod texnologiyasi. Uning ko‘plab afzalliklari bor, ammo bu texnologiyada ba’zi muammolar hali ham mavjud.

Xavfsizlik bu texnologiyada eng qiyin masala. Ushbu maqolada xavfsizlik muammosini hal qilish uchun turli xil shifrlash algoritmlari muhokama qilindi, shifrlashning afzalliklari va kamchiliklari ko‘rib chiqildi.

Bu yerda gomomorfik shirflash algoritmi bulutli hisoblash muhitida ochiq tarmoqdagi qimmatli ma’lumotlarni ishonchli himoya qilish uchun eng mos algoritm degan xulosaga kelindi.

Shifrlangan ma’lumotlar ustida operatsiyalarni bajarish uchun gomomorf algoritm RSA, DES va AES kabi algoritmlarga qaraganda yuqori xavfsizlikni ta’minlaydi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

[1]. Foster, I. T., Zhao, Y., Raicu, I., & Lu, S. (2009). Cloud Computing and Grid Computing 360- Degree Compared CoRR. abs/0901.01

[2]. Gartener: Seven cloud-computing security risks. InfoWorld.2008-07-02. http://www.infoworld.com/d/security-central/gartener-seven-cloud- computing-security-risks-853.

[3]. Data Remanence, https://en.wikipedia.org/wiki/Data_remanence.

[4]. Vijay Kumar, “Brief Review on Cloud Computing”, International Journal of Computer Science and Mobile Computing, vol. 5, September 2016.

[5]. Rijndael.Advanced Encryption Standard (AES). FIPS. November 23, 2001. http://csrc.nist.gov/publications/fips/fips197/fips197.pdf

[6]. Shraddha Soni, Himani Agrawal , Dr. (Mrs.) Monisha Sharma, “Analysis and Comparison between AES and DES Cryptographic Algorithm”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012

[7]. 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