RESEARCH FOCUS
xalqaro ilmiy jurnali
hamkorligida

DOI
10.66073/ReFocus-Conf/0910064

QR-kod maqolaning DOI sahifasini ochadi

SAHIFALAR
342–345

TIL
O'zbek (kirill)

IQTIBOS UCHUN
Арзиева Жамила Тилеубаевна, Юлдашева Равшаной Алламбергеновна, Куралбаева Райхон. Булутли ҳисоблаш тизимларини криптографик ҳимоялаш усуллари // «O'zbekiston olima ayollarining mamlakat taraqqiyotiga qo'shayotgan hissasi» mavzusidagi xalqaro ilmiy-amaliy konferensiya materiallari (Nukus, 2026-yil 9–10-oktyabr). – Nukus, 2026. – B. 342–345. – DOI: https://doi.org/10.66073/ReFocus-Conf/0910064

БУЛУТЛИ ҲИСОБЛАШ ТИЗИМЛАРИНИ КРИПТОГРАФИК ҲИМОЯЛАШ УСУЛЛАРИ

Арзиева Жамила Тилеубаевна
Юлдашева Равшаной Алламбергеновна
Куралбаева Райхон
Бердақ номидаги Қорақалпоқ давлат университети

Аннотация: Ушбу мақолада булутли ҳисоблаш тизимларида сақланаётган ва қайта ишланаётган маълумотларнинг махфийлиги ҳамда бутунлигини таъминлашнинг замонавий криптографик усуллари таҳлил қилинган. Учинчи томон провайдерларига (Cloud Service Provider – CSP) тўлиқ ишонч мавжуд бўлмаган муҳитда маълумотларни муҳофаза қилиш муаммолари кўриб чиқилган. Тадқиқотда Гомоморф шифрлаш (Homomorphic Encryption), Атрибутларга асосланган шифрлаш (CP-ABE), Қидирувга имкон берувчи шифрлаш (SSE) усулларининг функционал имкониятлари ва таққослама таҳлили келтирилган.

Калит сўзлар: булутли ҳисоблаш, криптография, гомоморф шифрлаш, CP-ABE, SSE, дедупликация, маълумотлар махфийлиги.

Булутли ҳисоблаш технологиялари (Cloud Computing) ресурсларни марказлаштириш, унумдорликни ошириш ва харажатларни тежаш имконияти сабабли замонавий ахборот-коммуникация инфратузилмасининг асосига айланди. Бироқ, ташкилотлар ва фойдаланувчиларнинг махфий маълумотлари локал серверлардан масофавий булутли платформаларга (AWS, Azure, Google Cloud) ўтказилганда ахборот хавфсизлиги бўйича жиддий таҳдидлар юзага келади.

Булут тизимларидаги марказий муаммо шундаки, булутли хизмат кўрсатувчи провайдер (CSP) кўп ҳолларда "ҳалол, лекин қизиқувчан" (Honest-but-Curious) деб таснифланади. Яъни, провайдер инфратузилма ишини тўғри таъминлайди, аммо сақланаётган ва қайта ишланаётган маълумотларни ўрганишга ҳаракат қилиши ёки инсайдерлик ҳужумларига учраши мумкин.

Анъанавий симметрик ва асимметрик шифрлаш алгоритмлари (AES, RSA) маълумотларни узатишда (Data-in-Transit) ва сақлашда (Data-at-Rest) самарали ҳимоя қилади. Лекин, булутли серверда маълумот устида ҳисоб-китобларни бажариш учун уни оператив хотирада дешифрлаш талаб этилади. Бу эса маълумотларнинг ҳимояланишига олиб келади. Ушбу муаммони ҳал этиш учун булутли тизимларда маълумотларни шифрланган ҳолида қайта ишлаш ва кириш ҳуқуқларини криптографик бошқариш усулларини жорий этиш талаб этилади.

Булутли ҳисоблаш тизимларини (Cloud Computing) криптографик ҳимоялаш усуллари маълумотларнинг махфийлиги, бутунлиги ва ахборотга фақат ваколатли

фойдаланувчилар киришини таъминлашнинг энг ишончли воситаси ҳисобланади. Булутли муҳитда маълумотлар ташқи серверларда (магазин ва ишлаш зоналарида) сақлангани сабабли, анъанавий хавфсизлик усуллари етарли бўлмайди.

Қуйида булутли тизимларда қўлланиладиган асосий криптографик ҳимоялаш усуллари, уларнинг ишлаш принциплари ва афзалликлари келтирилган.

Булутли тизимларни криптографик ҳимоялашнинг асосий усуллари – булутли муҳит спецификасидан келиб чиқиб, замонавий криптография бир нечта махсус усулларни таклиф этади:

1-жадвал. Булутли криптографиянинг асосий усуллари

Криптографик усул	**Асосий вазифаси ва ишлаш принципи**	**Таснифи/ Турлари**	**Афзалликлари**
Гомоморф шифрлаш *(Homomorphic Encryption)*	Булутда сақланаётган маълумотларни дешифрламасдан (очмасдан) улар устида математик ва мантиқий ҳисоб-китобларни бажариш.	• PHE (Partially Homomorphic) • SHE (Somewhat Homomorphic) • FHE (Fully Homomorphic)	Булут провайдери аслида қандай маълумотни қайта ишлаётганини кўрмайди, бу эса абсолют махфийликни таъминлайди.
Атрибутларга асосланган шифрлаш *(CP-ABE)*	Фойдаланувчининг роли, бўлими ва лавозими каби атрибутлари асосида мураккаб ва мослашувчан кириш назоратини амалга ошириш.	•CP-ABE (Ciphertext-Policy) •KP-ABE (Key-Policy)	Кўп фойдаланувчили булутли муҳитда ҳужжатларга кириш ҳуқуқларини марказлашмаган ҳолда хавфсиз бошқариш имконини беради.
Қидирувга имкон берувчи шифрлаш *(SSE / PEKS)*	Булутда сақланаётган шифрланган ҳужжатлар ва индекслар ичидан калит сўз (keyword) бўйича қидирув ўтказиш.	• SSE (Symmetric Searchable) •PEKS (Public-Key Searchable)	Очиқ матн ва қидирув сўровларини булут провайдерига ошкор қилмасдан керакли файлларни тезкор топиш имконини беради.

1. Гомоморф шифрлаш (Homomorphic Encryption – HE)

Булутли криптографиядаги энг истиқболли ва муҳим усуллардан биридир. У булутли серверга шифрланган маълумотларни дешифрламасдан (очмасдан) улар устида арифметик ёки мантиқий амалларни бажариш имконини беради.

⁻ Қисман гомоморф шифрлаш (Partially Homomorphic – PHE): Фақат битта амални (ё фақат қўшиш — *Paillier*, ёки фақат кўпайтириш — *RSA*) шифрланган ҳолда бажаради.

DOI 10.66073/ReFocus-Conf/0910064

⁻ Деярли тўлиқ гомоморф шифрлаш (Somewhat Homomorphic – SHE): Чекланган миқдордаги қўшиш ва кўпайтириш амалларини бажаради.

⁻ Тўлиқ гомоморф шифрлаш (Fully Homomorphic – FHE): Исталган мураккабликдаги ҳисоб-китобларни ва алгоритмларни шифрланган манбада дешифрлашсиз бажариш имконини беради (*Gentry*, *BGV/BFV схемалари*).

Афзаллиги: Булут провайдери (CSP) фойдаланувчининг реал маълумотларини умуман кўрмайди, лекин топшириқни тўлиқ бажариб беради.

2. Атрибутларга асосланган шифрлаш (Attribute-Based Encryption – ABE)

Булутли муҳитда кўп фойдаланувчили кириш назоратини (Access Control) криптографик бошқариш механизми.

⁻ CP-ABE (Ciphertext-Policy ABE): Шифрлаш сиёсати (масалан, "Шифокор" AND ("Кардиолог" OR "Реаниматолог")) бевосита шифрланган маълумотнинг ўзига сингдирилади. Фойдаланувчининг атрибутлари ушбу қоидага мос келсагина маълумот дешифрланади.

⁻ KP-ABE (Key-Policy ABE): Шифрлаш сиёсати фойдаланувчининг калитига бириктирилади, маълумот эса шунчаки атрибутлар тўплами билан шифрланади.

Афзаллиги: Булутли файл хотираларида кириш ҳуқуқларини мослашувчан, марказлашмаган ҳолда бошқариш имконини беради.

3. Қидирувга имкон берувчи шифрлаш (Searchable Encryption – SE)

Фойдаланувчи булутда сақланаётган шифрланган файллар ичидан маълум бир калит сўзни (keyword) файлларни дешифрламасдан ва булутга очиқ сўзни ошкор қилмасдан қидириб топиш имконини беради.

⁻ Симметрик қидирувга эга шифрлаш (SSE): Жадал қидирув учун ягона махфий калитдан ва шифрланган индекслардан фойдаланади.

⁻ Очиқ калитли қидирув (PEKS): Очиқ калит ёрдамида файлларни шифрлаш ва фақат тегишли махфий калит эгасига қидирув сўровларини (*Trapdoor*) юбориш имконини беради.

Булутли ҳисоблаш тизимларида маълумотларни криптографик ҳимоялаш анъанавий шифрлаш чегараларидан чиқиб, шифрланган муҳитда ҳисоб-китобларни бажариш ва кириш ҳуқуқларига мослашувчан бошқариш босқичига ўтди.

Ушбу мақолада булутли ҳисоблаш тизимларида (Cloud Computing) сақланаётган ва қайта ишланаётган маълумотларнинг махфийлиги, бутунлиги ҳамда хавфсизлигини таъминлашнинг замонавий криптографик усуллари, математик моделлари ва алгоритмлари атрофлича таҳлил қилинди. Олинган илмий ва амалий натижалар асосида қуйидаги асосий хулосаларга келинди:

✓ Гомоморф шифрлашнинг ўрни: Гомоморф шифрлаш (HE) алгоритмлари (хусусан, *Paillier* ва *FHE* схемалари) булутли серверларга маълумотларни дешифрламасдан улар устида мураккаб математик ва мантиқий амалларни бажариш имконини беради. Бу эса учинчи томонга очиқ маълумотларни ошкор қилмасдан, мукаммал конфиденциалликни таъминлайди.

✓ Мослашувчан кириш назорати ва қидирув: Атрибутларга асосланган шифрлаш (CP-ABE) кўп фойдаланувчили булутли муҳитда кириш сиёсатини

DOI 10.66073/ReFocus-Conf/0910064

тўғридан-тўғри шифрланган матннинг ўзига сингдириш орқали ҳуқуқларни марказлашмаган ҳолда хавфсиз бошқариш имконини беради. Шифрланган қидирув (SSE) алгоритмлари эса булутдаги шифрланган файллар ичидан калит сўзлар бўйича тезкор ва хавфсиз қидирув ўтказишни таъминлайди.

✓ Гибрид модель зарурати: Ҳозирги босқичда Тўлиқ Гомоморф Шифрлашнинг (FHE) юқори ҳисоблаш ресурслари талаб қилишини ҳисобга олган ҳолда, реал булутли платформаларда гибрид криптографик архитектурани (сақлаш учун *AES-256*, кириш назорати учун *CP-ABE*, статистик ҳисоб-китоблар учун *PHE/Paillier* ва қидирув учун *SSE*) қўллаш энг оптимал ва амалий самарали ечимдир.

Фойдаланилган адабиётлар

1. Гафуров, А. А., & Каримов, М. М. (2022). Ахборот хавфсизлиги ва киберхавфсизлик асослари. Дарслик. Тошкент: "Муҳаммад ал-Хоразмий номидаги ТАТУ", 340 б.

2. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st annual ACM symposium on Theory of computing (STOC '09) (pp. 169–178).

3. Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In Eurocrypt '99 (pp. 223–238). Springer.

4. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy (SP '07) (pp. 321–334).

5. Қодиров, Б. Р., & Ахмедов, Ш. Т. (2023). Булутли технологияларда маълумотларни муҳофаза қилишнинг криптографик усуллари. Муҳаммад ал-Хоразмий номидаги ТАТУ хабарлари, 3(67), 112–119.

6. Arzieva J., Avazov K., Sevinov J., ...Vafoev B., Cho Y.I. «Secure Communication in Wireless Sensor Networks Using Ascon Lightweight Cryptography» Computers Materials and Continua. 89(2)., 2026.

DOI 10.66073/ReFocus-Conf/0910064