УДК 004.056

**ҮЛКЕН ДЕРЕКТЕРДІҢ ҚАУІПСІЗДІГІ**

**Жұмабекова Айдана Төлеуқызы**

*zhumabekova2702@gmail.com*

әл-Фараби атындағы Қазақ Ұлттық университеті, Ақпараттық технологиялар факультетінің докторанты

Ғылыми жетекші - Дуйсебекова Куланда Сейтбековна

Алматы, Қазақстан

**Аңдатпа:** Үлкен деректер соңғы жылдары қызу зерттеу тақырыбына айналды. Үлкен деректер технологияларының пайда болуы деректердің қауіпсіздігі мен құпиялылығы үшін жаңа қиындықтар тудырады. Үлкен деректердің қауіпсіздігі мен құпиялығын қамтамасыз ету үшін қолданылатын технологиялық шешімдер талданады және олардың қазіргі жағдайы талданады. Бұл зерттеуде біз бірінші кезекте үлкен деректердің қауіпсіздігі мен құпиялылығына қатысты мәселелерді, қауіпсіздік технологияларын қарастырамыз.

**Түйінді сөздер**: үлкен деректер, үлкен деректердің қауіпсіздігі, үлкен деректердің құпиялығы, гомоморфты шифрлау

І. Кіріспе.

Қазіргі уақытта желінің және ақпараттың дамуы мәліметтердің қарқынды өсуіне алып келеді. Әртүрлі тәсілдерден алынған деректердің экспоненциалды өсуімен үлкен деректер көптеген домендерде маңызды рөл атқарады, соның ішінде бизнес, іздеу жүйелері, білім беру және т.б. Өкінішке орай, үлкен деректердің дамуы көптеген қиындықтарға да тап болып отыр, себебі қауіпсіздік пен құпиялылық тәуекелдері маңызды мәселелердің бірі ретінде танылды. Шын мәнінде, пайдаланушылар деректердің қауіпсіздігін сақтау және өңдеу үшін криптографиялық технологиялар мен сенімді есептеу орталарын қолдана алады. Алайда, ірі компаниялар үлкен деректердің өндірушілері мен менеджерлері болып табылады, сондықтан тек техникалық құралдардың көмегімен үлкен деректердің құпиялылығы мен қауіпсіздігін сақтау өте қиын.

Бұл зерттеуде біз алдымен үлкен деректердің өмірлік циклын қарастырамыз және үлкен деректердің өмірлік циклінің әртүрлі кезеңдеріндегі қауіпсіздік мәселелерін қарастырамыз. Үлкен деректердің құпиялығы мен қауіпсіздігін зерттеп, сонымен қатар деректер қауіпсіздігін қамтамасыз ету әдістеріне зерттеу жүргіземіз.

ІІ. Үлкен деректердің инфрақұрылымы

Көлемі, жылдамдығы, түрлілігі бойынша әртүрлі көлемдегі үлкен деректерді өңдеу үшін және әртүрлі көздерден өте жоғары жылдамдықпен келетін үлкен көлемдегі деректерді өңдеу үшін тиімді жүйелерді дамытуымыз керек. Үлкен мәліметтер өзінің өмірлік циклі барысында бірнеше кезеңдерден өтуі керек, төмендегі 1-суретте көрсетілгендей:

көптеген дереккөздерден үлкен деректер жасау

үлкен деректерді өңдеу

үлкен мәліметтер қоймасы

1-сурет. Үлкен деректердің өмірлік циклін иллюстрациялау

Үлкен деректердің өмірлік циклі. Деректер генерациясы: деректер әртүрлі таратылған көздерден жасалуы мүмкін. Соңғы жылдары адамдар мен машиналар жасаған мәліметтер саны күрт өсті. Мысалы, веб-сайт күн сайын 2,5 квинтиллион байт деректерді шығарады, ал дүниежүзілік деректердің 90 пайызы соңғы бірнеше жылда жасалған. Әдетте үлкен, әр түрлі және күрделі мәліметтер жасалады. Сондықтан дәстүрлі жүйелермен жұмыс істеу қиын. Құрылған деректер, әдетте, бизнес, интернет, зерттеу және т.б. сияқты белгілі бір салаға қатысты болады.

Деректерді сақтау. Бұл фаза ауқымды мәліметтер жиынтығын сақтау мен басқаруды білдіреді. Сақтау жүйесі екі бөлімнен тұрады: аппараттық инфрақұрылым және деректерді басқару. Аппараттық инфрақұрылым дегеніміз ақпараттық-коммуникациялық технологиялар ресурстарын әр түрлі тапсырмалар үшін пайдалану. Ал деректерді басқару дегеніміз ауқымды мәліметтер жиынтығын басқаруға, сұрауға арналған аппараттық инфрақұрылымның жоғарғы жағында орналасқан программалық жасақтама. Сонымен қатар, ол сақталған деректерді өзара әрекеттесуге және талдауға арналған бірнеше интерфейстерді қамтамасыз етуі керек.

Мәліметтерді өңдеу. Деректерді өңдеу кезеңі негізінен мәліметтерді жинау, мәліметтерді тарату, алдын-ала өңдеу және пайдалы ақпаратты іздеу процесіне жатады. Деректерді жинау кезеңінде мәліметтер арнайы деректерді жинау технологиясының көмегімен белгілі бір өндіріс ортасынан жиналады. Деректерді тасымалдау кезеңінде бастапқы деректерді белгілі бір өндіріс ортасынан жинап алғаннан кейін бізге аналитикалық қосымшалардың әр түрлі типтері үшін мәліметтерді тиісті қоймаға жіберу үшін жылдамдығы жоғары механизм қажет. Сонымен, алдын-ала өңдеу кезеңі деректердің мағынасыз және артық бөліктерін жоюға бағытталған, осылайша сақтау орны көбірек болады [1].

Деректерді талдау саласындағы дамып келе жатқан зерттеулерді алты техникалық бағытқа бөлуге болады: құрылымдық деректерді талдау, мәтіндік талдау, мультимедиялық талдау, веб-аналитика, желілік аналитика және мобильді аналитика.

ІІІ. Үлкен деректердің құпиялылығы пен қауіпсіздігі

Үлкен деректер тұрғысынан құпиялылық пен қауіпсіздік маңызды мәселе болып табылады. Ақпараттың құпиялылығы – бұл жеке ақпараттың жиналуы мен пайдаланылуын біраз бақылауға құқылы. Ақпараттық құпиялылық – бұл адамның немесе топтың өздері туралы ақпаратты басқа адамдарға белгілі болуына жол бермеу қабілеті, тек олар осы ақпаратты беретіндерден басқа. Пайдаланушылардың жеке өміріне қатысты маңызды мәселелердің бірі – интернет арқылы тарату кезінде жеке ақпаратты анықтау. Қауіпсіздік – бұл технологиялар мен процестер арқылы ақпаратты және ақпараттық активтерді қорғау тәжірибесі. Сонымен қатар, мыналардан үйрену: рұқсатсыз қол жеткізу, анықтау, бұзу, өзгерту, тексеру, жазу және жою.

Деректердің құпиялылығы жеке деректерді пайдалану мен басқаруға бағытталған, мысалы тұтынушылардың жеке ақпаратын жинау, бөлу және пайдалануды қамтамасыз ететін саясатты құру. Қауіпсіздік деректерді зиянды шабуылдардан және ұрланған деректерді пайда табу мақсатында дұрыс пайдаланбауға көбірек көңіл бөледі. Қауіпсіздік деректерді қорғау үшін маңызды болғанымен, құпиялылықты қамтамасыз ету жеткіліксіз. 1-кестеде жеке өмір мен қауіпсіздік арасындағы қосымша айырмашылыққа назар аударылған.

1 – кесте. Құпиялылық пен қауіпсіздік арасындағы айырмашылық

|  |  |  |
| --- | --- | --- |
| № | Құпиялылық | Қауіпсіздік |
| 1 | Құпиялылық - бұл қолданушы туралы ақпаратты дұрыс пайдалану. | Қауіпсіздік - бұл «құпиялылық, тұтастық және қол жетімділік» |
| 2 | Құпиялылық дегеніміз - адам туралы қандай ақпарат қайда кететінін шешу мүмкіндігі. | Қауіпсіздік шешімдердің орындалатынына сенімді болуға мүмкіндік береді.  |
| 3 | Құпиялылық мәселесі көбінесе тұтынушының өз ақпаратын басқа тараптан қорғау құқығына қатысты. | Қауіпсіздік құпиялылықты қамтамасыз ете алады. Көптеген қауіпсіздік жүйелерінің жалпы мақсаты - кәсіпорынды немесе агенттікті қорғау. |
| 4 | Нашар құпиялылық пен қауіпсіздіктің жақсы тәжірибелері болуы мүмкін. | Алайда деректерді қорғаудың жақсы бағдарламасынсыз құпиялылықтың жақсы тәжірибелеріне қол жеткізу қиын. |
| 5 | Мысалы, егер пайдаланушы XYZ-тен сатып алса және өнімді жіберу үшін төлем және мекен-жай ақпаратын ұсынса, олар пайдаланушының алдын-ала келісімінсіз үшінші тарапқа пайдаланушы туралы ақпаратты сата алмайды. | XYZ технологияның немесе желілік осалдықтардың әсерінен деректердің бұзылуына жол бермеу үшін әр түрлі әдістерді (шифрлау, брандмауэр) қолданады. |

IV.Үлкен деректер қауіпсіздігін қамтамасыз ету әдістері [2].

Ғылыми зерттеушілер үлкен деректердің қауіпсіздігі мен құпиялылығына қатысты мәселелерді шешудің түрлі әдістерін ұсынған.

*А. Деректердің құпиялылығын қорғау*

Мәліметтерді шифрлау технологиялары. Деректерді шифрлау – деректердің құпиялылығын қорғаудың маңызды құралы. Үлкен деректер жүйелерінің деректерді жылдам және тиімді түрде өңдеу қабілеті шифрлауға қажетті аппараттық және программалық қамтамасыз ету талаптарына жауап береді

а) Гомоморфты шифрлауды деректердің құпиялығын сақтау үшін пайдалануға мүмкіндік береді. Гомоморфты шифрлау ұғымын алғаш рет Р.Л. Ривест және оның әріптестері ұсынған. Бұл әдістің артықшылығы – шифрлық мәтіндерді тікелей, шифрды шешпестен және есептеу нәтижелеріне әсер етпей өңдеуге болады. 2-суретте бұлттағы гомоморфты шифрлаудың нақты мысалы келтірілген. Суреттен көріп отырғанымыздай, А және В мәтіндеріне гомографиялық шифрлау қолданылады және олар бұлтқа жіберіледі. Гомографиялық шифрлаудан кейін шифрленген мәтін шифры шешіліп, дұрыс нәтиже С-де жазылады.

Жалпы гомоморфты шифрлау шартты түрде екі түрге бөлінеді: жартылай гомоморфты шифрлау және толық гомоморфты шифрлау. Жартылай гомоморфты шифрлау схемалары тек қосу және көбейту сияқты қарапайым әрекеттерді қолдайды. Ал толық гомоморфты шифрлау схемасы ерікті көпмүшелерді есептеуді қолдайды. BGV, Bral2, TSZ және GSW1321 сияқты көптеген танымал толық гомоморфты шифрлау схемалары үлкен деректер қауіпсіздігі мен құпиялылығын қамтамасыз ету үшін пайдаланылды. Алайда, гомоморфты шифрлау схемаларында шуды бақылау қиын және бұлтты ортада тиімділігі төмен. Осылайша, гомоморфты шифрлау кейбір қолданбалы жүйелердің талаптарына сәйкес келмейді [3].



2-сурет Бұлттағы гомоморфты шифрлау

b) Қауіпсіз көпжақты есептеу схемасы алғаш рет A. Яо ұсынған. Бұл схема тараптарға функцияны жеке (жасырын) кірістерімен үлестірілген бұлт ортасында есептеуге мүмкіндік береді. Соңғы жылдары қауіпсіздік мәселелерін шешу үшін қауіпсіз көпжақты есептеу әдісіне негізделген жаңа схемалар ұсынылды.

А.Патра және оның әріптестері ұсынған қауіпсіз асинхронды көпжақты есептеу схемасы статистикалық тұрғыдан қауіпсіз және асинхронды жасырын деректермен алмасуды қамтамасыз етеді. Деректерді өзін-өзі қорғау схемасы А.Ю. Сархан мен С.Карр бұлттағы деректер иелеріне сыртқы пайдаланушылар жіберетін деректерді толық басқаруға мүмкіндік береді. Авторлар атрибутқа негізделген шифрлау, кілттерді басқаруға арналған RSA, деректерді өзін-өзі қорғауға арналған белсенді деректер пакеттері және кіруді басқаруды қамтамасыз ету үшін трафикті басқаруға арналған тәуелсіз мобильді агенттер сияқты төрт жетекші технологияларды біріктірді [5].

c) Атрибуттарға негізделген шифрлауды алғаш рет А.Сахай мен Б.Уотерс ұсынған. Бұл әдіс деректерге қауіпсіз қол жеткізу үшін ең қолайлы және танымал шифрлау әдісі болды. Жеке куәлікке негізделген шифрлаудан айырмашылығы, атрибуттарға негізделген шифрлауда деректер иелері атрибуттар жиынтығының көмегімен кілттерді де, шифрлық мәтінді де белгілейді. Содан кейін пайдаланушылар осы атрибуттар үшін заңды пайдаланушылардың авторизациясын растауы керек. Содан кейін мәліметтер кілт пен шифрленген мәтін атрибуттарына сәйкес жүктеледі және шифрланады.

Деректерді жасыру әдісі – құпиялылықтың тағы бір маңызды технологиясы. Бұл жағдайда ол зиянды түрде құпия деректерді алса да, түпнұсқа нақты деректерді ала алмайды, себебі кілт өрісінің мәні жасырылған.

*B) Қол жетімділікті басқару әдісі (қол жетімділікті басқару технологиясы)*

Қол жетімділікті басқару технологиясы – басқарылатын мәліметтермен алмасудың тиімді құралы. Алайда, үлкен деректер ортасында пайдаланушылар саны көп, ал авторизациялау қиын. Сондықтан, басқарылатын деректермен алмасуды жүзеге асыру үшін жаңа технологияны қолдану қажеттілігі туындайды. Пайдаланушылардың келісімін алуға, құқықтарды басқаруды жеңілдетуге және құпиялылықты сақтауға рұқсат алу кезіндегі пайдаланушылардың рөлін анықтайды. Бастапқыда қол жетімділікті басқару әдісі құқықтарын басқару жоғарыдан төменге бағытталған тәсіл болды. Үлкен деректер доменіне қатысты, кәсіпорынның рөлдік позициясына сәйкес, зерттеушілер пайдаланушы-объектілік қуат негізінде «төменнен жоғарыға» ауыса бастады. [4].

V. Қорытынды

Үлкен деректер көлемінің өсуіне байланысты оның қауіпсіздігі мен жеке өміріне қатысты мәселелер де арта түседі. Ақпараттық қауіпсіздік және үлкен деректер технологияларының құпиялылық тәуекелдері бұл технологияларды қолдану мен дамытуға кедергі келтіреді, олардың мүмкіндіктерін шектейді. Үлкен деректер қауіпсіздігіне үлкен мән берілуі керек, қауіпсіздік технологияларын зерттеу және дамыту қажет. Қауіпсіз шифрлау мен сенімді есептеу технологияларын үлестірілген сақтау, бөлшек сауда, платформаны тарату және басқа функциялар үшін әзірлеу қажет. Сонымен бірге деректердің қауіпсіздігінің үлкен стратегиялары мен сенімді қауіпсіздік жүйелерін әзірлеу қажеттілігі туындайды, өйткені үлкен деректер ашықтығы деректердің құпиялылығына қауіп төндіреді. Осылайша, үлкен деректер дамып келе жатқан технология болып табылады және оның қауіпсіздік тәуекелдеріне кепілдік берілмейді. Сондықтан қауіпсіздік технологияларының тиімділігін арттыру алдағы жылдардағы тенденциялардың бірі болып қала бермек.

**ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ:**

1. R, Bao, Z, Chen and M. S. Obaidat, “Challenges and techniques in Big data security and privacy: A review,” Security and Privacy, vol. 1, no. 4, 2018, pp. 1-8.
2. Fatima-Z. Benjelloun and A. L. Ayoub, “Big Data Security: Challenges, Recommendations and Solutionsç” Handbook of Research on Security Considerations in Cloud Computing, 2015, pp. 301-313.
3. R Alguliyev, Imamverdiyev Y. Big Data: Big promises for information security / Proceedings of the IEEE 8th International Conference on Application of Information and Communication Technologies (AICT), Astana, Kazakhstan 15-17 October, 2014, pp.216–219.
4. R. M. Əliquliyev, M. Ş. Hacırəhimova and A.S. Əliyeva, “Big data-nin aktual elmi-nəzəri problemləri,” İnformasiya cəmiyyəti problemləri, №2, 2016, səh. 37–49.
5. Д. Пудов, “Проблемы безопасности больших данных,” Открытые системы. СУБД, № 04, 2017, <https://www.osp.ru/os/2017/04/>