ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

ИНТЕРНЕТ ЗАТТАРЫ (IOT) ЖҮЙЕЛЕРІНДЕГІ ҚАУІПСІЗДІК ПЕН ҚҰПИЯЛЫЛЫҚТЫ ЖАҚСАРТУ ҮШІН ГОМОМОРФТЫ ШИФРЛАУ АЛГОРИТМІН ҚОЛДАНУ

Мырзакул Гулжан Нурматуллақызы
myrzakul0103@mail.ru
"Ақпараттық қауіпсіздік жүйелері" мамандығының 4 курс студенті
Л. Н. Гумилев атындағы Еуразия Ұлттық Университеті, Астана қ., Қазақстан
Ғылыми жетекшісі- Токкулиева А.К.

Тақырып өзектілігі: Күнделікті өмірде сымсыз ақылды сағаттардан бастап үлкен өнеркәсіптік жүйелерге дейін интернет заттары (IoT) тұрмысымыздың ажырамас бөлігіне айналып барады. Жыл сайын интернет заттары (IoT) қарқынды даму үстінде, миллиардтаған қосылған құрылғылар үлкен көлемдегі деректерді шығарып отырады. Бұл дегеніміз құпия деректердің барлығы қауіпсіздік шараларының керектігін талап етеді. Яғни жеке деректер мен құпия ақпараттардың ағып кетуі немесе бұрмалануы олардың қауіпсіздігін жақсарту керектігін айқындайды.

Көптеген IoT құрылғылары әрқашан дерлік кибершабуылдарға төтеп бере алмай, зиянды әрекеттерге осал болып келеді. Дәл осы сәтте гомоморфты шифрлау алгоритмдерін қолдану IoT жүйелеріндегі ақпаратты қорғаудың перспективалы тәсілдерінің бірі болып көрінеді. Гомоморфты шифрлау шифрланған деректердің мазмұнын ашпай-ақ операцияларды орындауға мүмкіндік береді.Ақпараттың құпиялылығын сақтай отырып жұмыс жасауда көмегін тигізеді.

Интернет заттары (IoT) және оның қауіпсіздігі

"Заттар интернеті" (IoT) термині соңғы бірнеше жылда танымал "технологиялық шу" терминдерінің бірі ретінде пайда болды. Қазіргі технологиялық әлемде IoT тез өсуіне байланысты технология туралы пікірталастарда ерекше орын алады. Заттар интернеті физикалық құрылғылардың, көлік құралдарының, тұрмыстық техниканың және электроникамен, бағдарламалық жасақтамамен, датчиктермен және деректерді жинауға және бөлісуге мүмкіндік беретін желілік қосылыммен жабдықталған басқа заттардың желісін білдіреді. Ақпараттық технологиялар бұл құрылғыларға бір-бірімен және қоршаған ортамен өзара әрекеттесуге мүмкіндік береді және интеллектуалды жүйелер мен қызметтерді құруға мүмкіндік береді.

Интернет заттарының кейбір мысалдарына мыналар жатады (1-сурет):

1 сурет Интернет заттары (IoT)

* Термостаттар, жарықтандыру жүйелері және қауіпсіздік жүйелері сияқты ақылды үй құрылғылары.

* Фитнес-трекерлер мен ақылды сағаттар сияқты киілетін құрылғылар.

* Пациенттерді бақылау жүйелері және киюге болатын медициналық құрылғылар сияқты денсаулық сақтау құрылғылары.

* Болжамды техникалық қызмет көрсету жүйелері және жеткізілім тізбегін басқару жүйелері сияқты өнеркәсіптік жүйелер.

* Қосылған автомобильдер мен автономды көліктер сияқты көлік жүйелері.

Интернет заттарының қауіпсіздігі (IoT) маңызды рөл атқарады, өйткені бұл саладағы құрылғылар сезімтал деректерді өңдейді және жібереді. IoT-тегі қауіпсіздік кепілдігі бірнеше маңызды аспектілерді қамтиды.

Микроконтроллер-бұл электронды құрылғыларды басқару үшін жиі қолданылатын шағын компьютер. Ол көбінесе IoT (IoT) қосымшаларында қолданылады, өйткені ол арзан, қуатты аз пайдаланады және әртүрлі құрылғыларға оңай ене алады.

Ең алдымен, аутентификация мен авторизация маңызды, сондықтан жүйеге тек уәкілетті құрылғылар ғана қол жеткізе алады. Бірегей идентификаторлар немесе сертификаттар сияқты күшті аутентификация әдістерін пайдалану негізгі элемент болып табылады.

Деректерді шифрлау деректерді тасымалдау жолында да (мысалы, TLS протоколдарын пайдалану) және деректерді құрылғыда және бұлтта сақтау үшін маңызды. Физикалық қауіпсіздік сонымен қатар рұқсатсыз кіруден және физикалық шабуылдардан қорғауды талап ететін рөл атқарады.

Осалдықтарды жою үшін бағдарламалық жасақтаманы үнемі жаңартып отыру қажет. Қол жеткізуді басқару, құқықтарды бақылау және ауытқуларды бақылау рұқсатсыз кірудің алдын алуға және ықтимал қауіптерді жылдам анықтауға көмектеседі.

DDoS және сыртқы шабуылдарды қоса алғанда, әртүрлі шабуылдардан қорғау да қауіпсіздіктің маңызды құрамдас бөлігі болып табылады. ISO/IEC 27001 сияқты реттеуші органдардың стандарттары мен талаптарын сақтау IoT-ке қауіпсіз тәсілді толықтырады.

IoT саласының күрделілігін ескере отырып, әзірлеушілерді, өндірушілерді және соңғы пайдаланушыларды осы экожүйедегі қауіпсіздікті қамтамасыз ету бойынша бірлескен күш-жігерге тарту маңызды

IoT қауіпсіздігіндегі гомоморфты шифрлаудың рөлі

Гомоморфты шифрлау-шифрланған деректермен операцияларды шифрды ашпай орындауға мүмкіндік беретін шифрлау әдісі. Кез келген операцияларды орындамас бұрын деректерді шифрлау қажет дәстүрлі шифрлаудан айырмашылығы, гомоморфты шифрлау шифрланған деректердің құпиялылығын сақтай отырып, олардың үстінен есептеулер жүргізуге мүмкіндік береді.

Гомоморфты шифрлаудың жалпы формуласы келесідей ұсынылуы мүмкін:

E-шифрлау функциясы,

D-шифрды ашу функциясы,

M-бастапқы хабарламалар кеңістігі,

C-шифрлық мәтін кеңістігі,

K-кілт кеңістігі,

$\odot$ - M кеңістігіндегі операция,

$\oplus$ - C кеңістігіндегі қосу операциясы.

Содан кейін гомоморфты шифрлау әдетте келесі қасиетті орындауды қамтиды:

$$D\big(K, E(K, m_1) \odot E(K, m_2)\big) = m_1 \oplus m_2$$

Бұл теңдеу екі шифрланған хабарламадағы операция нәтижесінің шифрын ашу бастапқы хабарламаларға қосу операциясына (немесе басқа қолдау көрсетілетін операцияға) тең екенін білдіреді.

IoT желісінде гомоморфты шифрлауды қолдану

1. Тасымалдаудағы деректерді қорғау: Гомоморфты шифрлау желі арқылы тасымалдау кезінде IoT деректерін қорғауға мүмкіндік береді. Деректер жіберілмес бұрын құрылғыда шифрлануы мүмкін және оны тек соңғы алушы ғана шеше алады.

2. Жадтағы деректерді қорғау: IoT құрылғылары жадтан ақпарат алуға шабуыл жасауы мүмкін. Гомоморфты шифрлау деректерді құрылғының жадында шифрланған түрде сақтауға мүмкіндік береді, бұл оны рұқсатсыз қол жетімсіз етеді.

3. Шифрланған деректерді есептеу: Гомоморфты шифрлау шифрланған деректерді есептеуге мүмкіндік береді, бұл әсіресе IoT-те маңызды, мұнда құпия ақпаратты ашпай-ақ үлкен көлемдегі деректерді өңдеу қажет.

4. Шабуылдар мен ағып кетулерден қорғау:

Деректердің ағып кетуіне жол бермеу: Гомоморфты шифрлау деректердің ағып кету қаупін азайтуы мүмкін, өйткені жүйе бұзылған жағдайда да деректер шифрланған күйінде қалады және оларды тиісті кілттерсіз пайдалану мүмкін емес.

Қиындықтар мен перспективалар

Гомоморфты шифрлау IoT-те қауіпсіздік пен құпиялылықты жақсартудың перспективалы шешімдерін ұсынғанымен, ол есептеу күрделілігі және өнімділіктің үстеме шығындары сияқты қиындықтарға тап болады. Алайда, криптографиялық технологиялар мен аппараттық шешімдердің дамуымен бұл проблемалар IoT желісінде гомоморфты шифрлауды қолданудың жаңа мүмкіндіктерін ашу арқылы шешіледі деп күтілуде.

Гомоморфты шифрлау схемасын қалай жүзеге асыруға болады?

Гомоморфты шифрлау схемасын енгізу уақытты қажет етеді. Іске асырудың ең жақсы әдісі сіздің компанияңыздың саласы, оның мөлшері және сіздің деректеріңіздің құпиялылық деңгейі сияқты факторларға байланысты. Мысалы, медициналық ақпарат HIPAA сәйкестігінің қатаң ережелеріне сәйкес қорғалуы керек болғандықтан, интенсивті шифрлау технологиясын медициналық салаға енгізу зияткерлік меншікті қорғағысы келетін өндірушіге қарағанда ұзағырақ уақыт алады.

Дегенмен, сақтау керек деректердің түрі мен мөлшеріне қарамастан орындалуы керек бірнеше негізгі қадамдар бар. Бұл қадамдар келесі компоненттерді таңдауды қамтиды:

шифрланған мәтінді түрлендірудің дұрыс алгоритмі, деректерді шифрлауға және шифрын ашуға арналған ең жақсы кілттер, бұлтқа негізделген провайдер, ол сіздің барлық қауіпсіздік тапсырмаларыңызды жақсы орындайды және сіздің талаптарыңызға сәйкес келеді.

Шифрлау схемасын енгізгеннен кейін оны жеделдету жолдарын іздеуге болады. Кейбір сарапшылар 5G қауіпсіздігі туралы алаңдаушылық білдірсе де, бүкіл әлемде көбірек желілер салынуда. Өнімділік гомоморфты шифрлаудың бір кедергісі болғандықтан, жоғары жылдамдықты 5G желілері бұл кедергіні жеңуге үміт береді.

Қорытынды

Гомоморфты шифрлауды қолдану интернет заттарының қауіпсіздігі мен құпиялылығын жақсартудың қуатты құралы болып табылады. Бұл тәсіл деректерді олардың өмірлік циклінің барлық кезеңдерінде - беруден өңдеуге дейін қорғауға мүмкіндік береді, қауіпсіз және сенімді IoT шешімдерін дамытудың жаңа перспективаларын ашады.

Пайдаланылған әдебиеттер тізімі

1. Gubbi, Jayavardhana, et al. "Internet of Things (IoT): A vision, architectural elements, and future directions." Future generation computer systems 29.7 (2013): 1645-1660.

2.Gentry, Craig. "Fully homomorphic encryption using ideal lattices." Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009.

3.Brakerski, Zvika, and Vinod Vaikuntanathan. "Efficient fully homomorphic encryption from (standard) LWE." SIAM Journal on Computing 43.2 (2014): 831-871.

4.Smart, Nigel P. "Fully homomorphic encryption with relatively small key and ciphertext sizes." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2010.