ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный университет
имени аль-Фараби

NEWS

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

1 (341)

JANUARY – MARCH 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физика және информатика сериясы» ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын усынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физика и информационные технологии» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series physico-mathematical.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1, Number 341 (2022), 77–87 https://doi.org/10.32014/2022.2518-1726.119

ИРСТИ 28.23.37
УДК 004.75

Ж.М. Ташенова[1*], Э.Н. Нурлыбаева[2], Ж.К. Абдугулова[3], Ш.А. Аманжолова[4]

[1,3]Л. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан;
[2]Т.Қ. Жүргенев атындағы Қазақ Ұлттық өнер академиясы, Алматы, Қазақстан;
[4]Құрманғазы атындағы Қазақ ұлттық консерваториясы, Алматы, Қазақстан.
E-mail: zhuldyz_tm@mail.ru

БҰЛТТЫҚ ЖҮЙЕДЕГІ ҚАУІПСІЗДІК ЖӘНЕ ШИФРЛАУ ӘДІСТЕРІ

Аннотация. Бұл мақалада бұлтты жүйедегі қауіпсіздік және шифрлау әдістері қарастырылады. Бұлтты есептеулер жылдам технологиялы, бір жағынан қолдануға арналған көптеген қолданбалар жайлы айтылады және де, екінші жағынан, құпиялылықты бұзу, деректердің тұтастығын бұзу және деректердің қол жетімді еместігі сияқты ортақ кеңістіктегі қауіпсіздікке қатысты түрлі қауіптері қарастырылады. Бұл мақалада, бұлтқа жүктелместен бұрын файлды шифрлайтын жақтары ұсынылады. AES (Advanced Encryption Standard) - бұл ең қауіпсіз шифрлау алгоритмдерінің бірі және AES көмегімен шифрланған мәліметтерге көптеген шабуылдар сәтті бола бермейді. Бұл ұсыныс бұлттағы деректерге төнетін қауіптердің көпшілігін шешеді. Сондай-ақ, құрылым пайдаланушының деректеріне шынайы және рұқсатты қол жетімділікті қамтамасыз ету үшін кіру идентификаторы мен құпия сөзді пайдалануды ұсынады. Сонымен қатар, бұлтты есептеу қауіпсіз қолданылуы, қолданушыға таңғажайып артықшылықтар берілуі және қауіпсіздікке төнетін жалғыз кемшіліктері айтылады. Cloud Computing пайдаланушыларға компьютерлер кластерлері мен торларын құру арқылы әр түрлі қызметтерді ұсынады. Мұның басты мақсаты - қолданушының бәрін өздігінен ұстау жүктемесін азайту үшін виртуалды түрде қызмет көрсету. Бұл сонымен қатар құрылғыларға, ақпараттарға немесе бағдарламалық қамтамасыз етудің ортақ қорымен қамтамасыз ететін, бір рет пайдалану үшін ақы төлеуге негізделген веб-есептеулерге қатысты. Қосымшаларды басқару үшін жергілікті серверлердің немесе меншікті құрылғылардың орнына адамдар бұлттың есептеу ресурстарының ортақ моделін пайдаланады. Бұлтты есептеу жүйелері Интернетке негізделген әртүрлі деректерді сақтау мен қызметтерді ұсынады. Бұлтты есептеулердің клиенттердің әр түрлі қажеттіліктеріне негізделген төрт қызмет түрін ұсынады және сол қызметтер қарастырылған. Бұлттық жүйедегі қауіпсіздікке қатысты аспектілер айтылады. Қолданыстағы қауіпсіздік модельдері қарастырылады. Файлды бұлттық жүйеге жүктеудің дерек-сызбасы, оның қадамдары рет-ретімен айтылған.

Түйін сөздер: бұлт, шифрлеу, қауіпсіздік, бұлтты қызметтер, бұлтты есептеу, AES, обфускация.

Ж.М. Ташенова[1*], Э.Н. Нурлыбаева[2] , Ж.К. Абдугулова[3], Ш.А. Аманжолова[4]

[1,3]Евразийский национальный университет имени Л.Н. Гумилева, Нур-Султан, Казахстан;
[2]Казахская национальная академия искусств имени Т.К. Жургенова, Алматы, Казахстан;
[4]Казахская национальная консерватория имени Курмангазы, Алматы, Казахстан.
E-mail: zhuldyz_tm@mail.ru

МЕТОДЫ БЕЗОПАСНОСТИ И ШИФРОВАНИЯ В ОБЛАЧНОЙ СИСТЕМЕ

Аннотация. В статье обсуждаются методы безопасности и шифрования в облаке. Облачные вычисления – это быстро развивающееся приложение с несколькими приложениями, которое устраняет различные угрозы безопасности в общем пространстве, такие как нарушения

конфиденциальности, нарушения целостности данных и недоступность данных. В этой статье дано описание, как зашифровать файл перед его загрузкой в облако. Aes (advanced encryption standard) – один из самых безопасных алгоритмов шифрования, и многие атаки на данные, зашифрованные с помощью aes, не всегда успешны. Эта рекомендация устраняет большинство угроз облачным данным. Структура также рекомендует использовать логин и пароль для обеспечения аутентичного и доступного доступа к пользовательским данным. В нем также упоминается, что облачные вычисления можно использовать безопасно, что дает пользователю удивительные преимущества и что это единственная угроза безопасности. Облачные вычисления предоставляют пользователям множество услуг за счет создания компьютерных кластеров и сетей. Основная цель этого – предоставить виртуальную услугу, чтобы снизить нагрузку на самообслуживание всех пользователей. Это также относится к веб-расчетам с оплатой за просмотр, которые обеспечивают общее резервное копирование устройств, информации или программного обеспечения. Вместо локальных серверов или проприетарных устройств для управления приложениями люди используют общую модель облачных вычислительных ресурсов. Системы облачных вычислений предлагают различные хранилища данных и услуги в интернете. Облачные вычисления предлагают четыре типа услуг, основанных на различных потребностях клиентов, и эти услуги предоставляются. Аспекты, связанные с безопасностью в облачной системе. Рассмотрены существующие модели безопасности. Схема загрузки файла в облачную систему, последовательно описаны ее действия.

Ключевые слова: облако, шифрование, безопасность, облачные сервисы, облачные вычисления, AES, обфускация.

Zh. Tashenova[1*], E. Nurlybaeva[2], Zh. Abdugulova[3], Sh. Amanzholova[4]

[1,3]L.N. Gumilyov Eurasian National University, Department of Information technology, Nur-Sultan, Kazakhstan;
[2]Kazakh National Academy of Arts named after T. Zhurgenov, Almaty, Kazakhstan;
[4]Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan.
E-mail: zhuldyz_tm@mail.ru

CLOUD SECURITY AND ENCRYPTION METHODS

Abstract. This article discusses methods of security and encryption in the cloud. Cloud computing is a rapidly evolving application with several applications, which eliminates various threats of security in the public space, such as violations of confidentiality, violations of integrity and integrity. This article describes how to encrypt a file before uploading it to the cloud. Aes (advanced encryption standard) is one of the most secure encryption algorithms, and many attacks on data, encrypted with the help of aes, are not always successful. This recommendation eliminates most of the threat of cloud data. The structure also recommends using a login and password to secure authentic and accessible data to the user. It also mentions that cloud computations can be used safely, which gives the user an amazing advantage and that it is the only threat of safety. Cloud computations provide multiple services to users at the expense of creating computer clusters and networks. The main purpose of this is to provide a virtual service to reduce the load on self-service of all users. This also applies to web calculations with a fee for viewing, which provide a general backup of the device, information or software support. Instead of local servers or proprietary devices for managing applications, people use a common model of cloud computing resources. Cloud computing systems offer different types of data storage and services on the Internet. Cloud deductions offer four types of services based on different customer needs, and these services are provided. Aspects related to security in the cloud system. Existing safety models are considered. The file download scheme in the cloud system, followed by the description of its actions.

Key words: cloud, encryption, security, cloud services, cloud computing, AES, diffusion.

Кіріспе. Қазір күн сайын әркім осы сандық әлеммен бір-бірімен байланысты және бұл ақпараттық технологияның өсуінің басты себебі. Мұның басты факторы - кез-келген жерден және кез-келген уақытта қол жетімді пайдаланушы үшін қолайлы орта. Интернет әр түрлі адамдарға, мысалы бизнесмендерге, зерттеушілерге, студенттерге және т.б. өз мақсаттарын жүзеге асырудың көптеген нұсқаларын ұсына отырып, жұмыстарды аяқтауға мүмкіндік береді.

Көптеген пайдаланушылар өздерін интернетпен байланыстырады және IT-инфрақұрылымды күнделікті қажеттіліктерге сай пайдаланады. Интернетке деген сұраныс артқан сайын, Интернет арқылы бағдарламалық жасақтама, платформа, мәліметтер базасы, сақтау қызметі және т.б. сияқты қызметтер де біртіндеп артып келеді. Бұл жерде бұлтты есептеудің маңызды терминдері пайда болады, ол желі арқылы өз пайдаланушыларына көптеген қызметтерді ұсынады. Қамтамасыз еткендей «Өзің төле, өйткені төле» негізгі қолданушысы үлкен пайда көре алады осы қызметті арзан бағамен пайдалану арқылы.

«Бұлт» - бұл есептеу ресурстарын виртуалды жинау үшін қолданылатын термин. Бұлтты есептеулерді қолданатын тұтынушыларға көптеген артықшылықтар ұсынылады: бағдарламалық қосымшалардың үлкен жиынтығы, шексіз сақтау мүмкіндігі, найзағай жылдам өңдейтін қуатқа қол жетімділік және бүкіл әлем бойынша ақпаратты оңай бөлісу мүмкіндігі. Пайдаланушы осы артықшылықтардың барлығын Интернетке кірген кез-келген уақытта өз браузері арқылы ала алады. 90-жылдардың басында үлкен банкоматтар желісі «бұлт» деп аталды. Бұл термин тағы да он екі жыл бұрын Amazon веб-қызметтерінің пайда болуымен пайда болды. Бұлтты есептеу тұтынушылар мен корпоративті құрылымдарға бұлт ұсынатын барлық қосымшаларды орнатудың қосымша күшінсіз пайдалануға мүмкіндік береді, сонымен қатар Интернетке кіру мүмкіндігі бар кез-келген компьютерден жеке файлдарға қол жеткізуді ұсынады. [1]

Бұлтты есептеу - бұл бағдарламалық жасақтаманың, аппараттық құралдардың, өңдеудің және сақтаудың күрделі инфрақұрылымы, олардың барлығы қызмет ретінде қол жетімді. Ол барлық пайдаланушылар үшін қол жетімді болатын қашықтан басқарылатын қосымшалардан тұрады («бұлтта» деп аталады). Бұл технология көптеген суперкомпьютерлердің санына қол жеткізуге мүмкіндік береді және олардың нәтижелері бүкіл әлем бойынша көптеген жерлерде қосылған, осылайша секундына ондаған триллиондармен жылдамдықты ұсынады.

Бұлт тұтынушыларға үнемділік пен жылдамдықты уәде етеді. Бұлт технологиясын қолдана отырып, компания негізгі технология компоненттерінің кеңеюі мен қысқаруына іскери өмірдің жоғары және төмен деңгейіне қол жеткізуге болатын қосымшаларды жылдам қолдана алады. Бұған виртуализация және торды толтыру сияқты бұлт қосқыштардың көмегімен қосымшаларды жұмыс уақытында ең қолайлы инфрақұрылымға динамикалық түрде орналастыруға мүмкіндік береді. Айта кету керек, бұл жағымды көрінсе де, сенімділік, портативтілік, құпиялылық және қауіпсіздік мәселелері бар.

Бұлтты есептеу есептеуіш және желілік қызметтердің жаңа түрлеріне мүмкіндік береді ресурстар Интернет арқылы Интернетте қол жетімді. Ең танымал қызметтерінің бірі бұлтты есептеу - бұл аутсорсинг.

Бұлт - бұл Интернетке негізделген есептеу технологиясы, онда бағдарламалық жасақтама, платформа, сақтау және ақпарат сияқты ортақ ресурстар тұтынушыларға сұраныс бойынша ұсынылады. Cloud Computing - инфрақұрылымдарды, бағдарламалық қамтамасыздандыруды, қосымшаларды және бизнес-процестерді қамтитын ресурстарды бөлуге арналған есептеу алаңы. Cloud Computing - есептеу ресурстарының виртуалды пулы. Ол Интернет арқылы пайдаланушыларға бассейндегі есептеу ресурстарын ұсынады. Бұлтты есептеу дамып келе жатқан есептеу парадигмасы ретінде жаппай пайдаланушылар арасында сақтау, есептеу және қызметтерді мөлдір түрде бөлуге бағытталған. Бұлтты есептеуіш жүйелер пайдаланушылардың деректерінің құпиялығын қорғауда айтарлықтай шектеулер тудырады. Пайдаланушылардың құпия деректері шифрланбаған түрде үшінші тараптардың провайдерлері басқаратын және басқаратын қашықтағы машиналарға ұсынылатындықтан, қызмет провайдерлері пайдаланушылардың құпия деректерін рұқсатсыз жария етудің қауіптері өте жоғары болуы мүмкін. Пайдаланушылардың деректерін сыртқы шабуылдаушылардан қорғаудың көптеген әдістері бар. Анықтама қызмет провайдерлерінен пайдаланушылардың деректерінің құпиялығын қорғауға арналған және қызмет жеткізушілері бұлт есептеу жүйелерінде деректерді өңдеу және сақтау кезінде пайдаланушылардың құпия деректерін жинай алмауын қамтамасыз етеді. Бұлтты есептеу жүйелері Интернетке негізделген әртүрлі деректерді сақтау мен қызметтерді ұсынады.

Материалдар мен әдістер. Бұлттық есептеудегі «бұлт» термині - бұл байланыс желісі немесе есептеу инфрақұрылымымен біріктірілген желі. Бұлтты есептеу жүйесіне бағдарламалық қамтамасыздандыруды, аппаратураны, өңдеуді және т.б. қамтамасыз ететін желі арқылы қол жеткізіледі. Пайдаланушыға сұраныс туындаған кезде. Cloud Computing - бұл Интернет арқылы пайдаланушыларға пул ұсынатын есептеу ресурстарының виртуалды пулы.

Cloud Computing пайдаланушыларға компьютерлер кластерлері мен торларын құру арқылы әр түрлі қызметтерді ұсынады. Мұның басты мақсаты - қолданушының бәрін өздігінен ұстау жүктемесін азайту үшін виртуалды түрде қызмет көрсету. Бұл сонымен қатар құрылғыларға, ақпараттарға немесе бағдарламалық қамтамасыз етудің ортақ қорымен қамтамасыз ететін, бір рет пайдалану үшін ақы төлеуге негізделген веб-есептеулерге қатысты. Қосымшаларды басқару үшін жергілікті серверлердің немесе меншікті құрылғылардың орнына адамдар бұлттың есептеу ресурстарының ортақ моделін пайдаланады. [2]

Бұлтты есептеу пайдаланушының өзінің виртуалды инфрақұрылымы бар ортаны қамтамасыз етеді, оны қолдана отырып, олар географиялық шекараға тәуелді емес тапсырмаларды орындай алады. Икемді орта мен арзанырақ болғандықтан, адамдар бұлтты қызметтерді пайдалануға қызығушылық танытады, бұл Платформамен, бағдарламалық жасақтамамен немесе инфрақұрылыммен байланысты болуы мүмкін. Cloud-ті қолдану негізінде үш орналастыру моделі бар: Public Cloud, Private Cloud және Hybrid Cloud.

Бұлтты есептеу өзінің қолданушыларына көптеген артықшылықтар береді, бірақ қараңғы жағынан ол тұтастық немесе сақтаудың дұрыстығы, қол жетімділік, құпиялылық және басқа да көптеген мәселелерден зардап шегеді. Бұл мәселелер пайдаланушылар үшін бұлтты ортаға бейімделуді қиындатады. Бұлтты пайдаланушылардың бұлтты қызмет провайдерлеріне сенімін орнату үшін осы бағытта көптеген зерттеулер қажет.

Бұлтты қызметтер. Бұлт төмендегі суретте көрсетілгендей клиенттердің әр түрлі қажеттіліктеріне негізделген төрт қызмет түрін ұсынады.

Software-as-a-Service (SaaS): бағдарламалық жасақтама ретінде қызмет ретінде бұлтты қызмет провайдерлері әртүрлі бағдарламалық қамтамасыз етуді ұсынады. Бұл біздің жұмыс станциямызды сақтауды жақсартады. Саас жеткізушісі бағдарламалық жасақтама, желілік кеңістік және деректер орталығы сияқты ең жақсы бағдарламалық инфрақұрылыммен қамтамасыз етеді. SaaS мысалдары мыналарды қамтиды: Salesforce.com, Google Apps.

Қызмет ретінде платформа (PaaS): бұл пайдаланушының үй-жайына жүктеместен бағдарламалық жасақтаманы пайдалануға және оған қол жеткізуге немесе оны кез-келген пайдаланушы үшін, оны әзірлеуші немесе кез-келген пайдаланушы үшін жергілікті машинада орнатудың қажеті жоқ. Ол көп жүйелі жүйелер үшін платформалық интеграцияның жоғары деңгейін қамтамасыз етеді. Пайдаланушылар желіні, серверлерді, операциялық жүйелерді және сақтауды басқара алмаған кезде, Платформаны Қызмет ретінде таңдайды. 1-суретте көрсетілген PaaS-тің кейбір мысалдары - Force.com, Google App Engine және Microsoft Azure.[3]

1-сурет. Бұлтты қызметтер

Қызмет ретінде инфрақұрылым (IaaS): IAAS - бұл көптеген физикалық ресурстарды желі арқылы бөлісу. IAAS-тың негізгі мақсаты - қосымшалар мен ОЖ арқылы серверге, сақтау мен желіге жылдам қол жетімділікті қамтамасыз ету. Осылайша, ол Бағдарламалық жасақтама интерфейсін (API) қолдана отырып, талап етілетін қарапайым инфрақұрылымды ұсынады.Пайдаланушыға бұлтты инфрақұрылымдағы негізгі жабдықты басқару қажет емес, ол серверді, қосымшаны және ОЖ-ны басқара алады. IaaS-тің кейбір мысалдары Amazon Elastic Cloud Computing (EC2) т.б.

Қызмет ретінде мәліметтер базасы (DaaS): DaaS пайдаланушыларға маңызды құжаттар мен басқа ақпаратты сақтау туралы. Бұл сонымен қатар тиісті ақпаратты алу үшін менікі болуы мүмкін көптеген файлдарды сақтау бойынша қызметтерді ұсынады. Деректер базасы сонымен қатар пайдаланушылардың жеке ақпараттары, тіркелгі деректері және т.б. сияқты ақпаратты сақтайтын қызметтердің маңызды бөлігі болып табылады.[4]

Зерттеу нәтижесі. Cloud модельдердің үш түрін ұсынады: барлығына ашық жалпыға қол жетімді бұлт; Жеке бұлтқа тек жеке меншік аймақтың пайдаланушысы ғана рұқсат етіледі; Мемлекеттік және жеке бұлт ұсынатын қызметтердің екі түрінің де ымыралық тапсырмасын орындайтын гибридті бұлт.

Орналастырудың төрт моделі бар, олар төменде көрсетілген:

Жеке бұлт:

Бұл құрылым қызметкерлерінің ішінен пайдаланатын кез келген бір ұйымға арналған. Жалпы, бұлтты инфрақұрылымды ұйым өзі басқарады немесе кез келген үшінші тараптың көмегін ала алады.

Жалпы бұлт:

Бұлтты қызметтерді ұсынатын ұйым, кез-келген жерден қол жеткізе алатын және пайдаланғаны үшін ақы төлейтін көпшілікке қол жетімді платформаны ұсынады.

Қоғамдық бұлт:

Бұл бірнеше қауымдастықтар қолданатын бұлт жүйесі, онда барлық мүшелер осы инфрақұрылымға тең қол жетімді.

Гибридті бұлт:

Клиентке тиімді қызмет көрсететін жоғарыда аталған екі немесе одан да көп бұлтты модельдер гибридті инфрақұрылым жасайды, мұнда өнердің бір бөлігі көпшілік үшін шектелуі мүмкін, ал кейбір бөліктері барлығына қол жетімді.

Бұлтты қызметтің өмірлік циклы:

Бұлт үшін қызмет ету мерзімі келесі суретте көрсетілген кезеңдерден тұрады:

Сұранымды тұжырымдау: Пайдаланушы сұралған Cloud қызметіне арналған SLA функционалды және функционалды емес талаптарын анықтайды.

Табу және мониторинг: кандидаттардың қызметтерін ұсынады және олардың бақыланатын SLA өлшеуіштері мен бағалық ақпаратты әр түрлі деректер қоймаларында сақтайды.

Сәйкестік: талапкердің есептеу және сақтау ресурстарына SLA талаптарын сәйкестендіру арқылы сұралған қызметті ұсыну үшін қолайлы бұлттарды таңдайды.

Орналастыру: таңдалған провайдерлерге қызмет көрсету компоненттерін орналастырады.

Орындалуы: қызмет орындалады және оның күйі үнемі бақыланады жұмыс уақыты.

Тоқтату: қызметті пайдаланушының өтініші бойынша тоқтатуға болады. (мысалы, SLA бірнеше рет бұзылған жағдайда).

Бұлттық есептеудің артықшылықтары:

Шығын тиімділігі - бұлтты есептеу - бағдарламалық жасақтама, платформа және инфрақұрылым қызметтерін пайдаланудың ең жақсы және арзан әдісі. Ол «барған сайын төлеу» қағидасына негізделген, сондықтан оған қосымша ақша төлеудің қажеті жоқ.

Дерлік шектеусіз сақтау - бұлтты сақтаудың сыйымдылығы шектеусіз, сондықтан деректерді сақтау үшін ешқандай шектеулер жоқ. [5]

Сақтық көшірме жасау және қалпына келтіру - бұлтты есептеулерде оны қалпына келтіру және қалпына келтіру оңай.

Бағдарламалық жасақтаманы автоматты түрде интеграциялау - бұлтты компьютерлік бағдарламамен интеграциялау әдетте автоматты түрде пайда болатын нәрсе. Сондықтан қолданушыны қосымшаны өз қажеттіліктеріне сәйкес баптауға қосымша күш жұмсамау керек.

Ақпаратқа оңай қол жеткізу - бұлтта, пайдаланушы тіркелгеннен кейін, кез келген жерден өзінің деректерін қолдана алады және орналасқан жерді шектемейді.

Бұлтты есептеудің кемшіліктері:

Бұлтты есептеулерде кейбір шектеулер бар, олар төменде келтірілген.

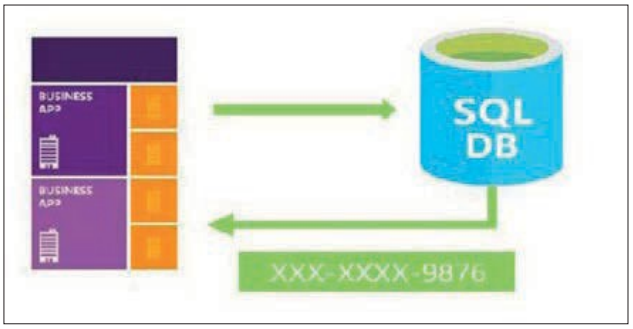
Техникалық мәселелер - желіге қосылудың техникалық мәселесі.

Бұлттық есептеудегі басты мәселе - бұлттық қауіпсіздік. Бұлтты есептеулерде көптеген пайдаланушылар бұлтты сақтауды пайдалана алады. Сонымен, пайдаланушылар аутентификация, құпиялылық және тұтастық тұрғысынан қауіпсіздікке қатысты мәселелерге тап болуы мүмкін.

Мүмкін үзілістер-бұлтты есептеу шағын бизнесті олардың Интернетке қосылу сенімділігіне тәуелді етеді. [6]

Деректер қауіпсіздігінің мақсаты құпия ақпаратты бөгде адамдардан және уәкілетті тұлғалардан жасыру болып табылады. Деректерді қорғаудың бұл саласы соңғы уақыт аралығында деректерді беру жылдамдығының ұлғаюына байланысты көбірек назар аударды.

Деректер обфускациясы



2- сурет. Обфускация

Обфускацияны қолдана отырып, қолданушы деректерінің көрінісі өзгереді. Жалпыға бірдей түсінікті және (әдетте) төмен шығындар әдісі пайдаланылып, мәліметтерді берілмеген күйде сақтауға мүмкіндік береді. Обфускация процесі жалпылама түрде 2-суретте бейнеленген.

Обфусация дегеніміз - хабарды түсінуді қиындататын, әдетте шатастыратын және анық емес тілде сөйлесудің мағынасын жасыру. [7]

Обфускация әдістері

Деректерді толтыру әдістерін бірқатар критерийлер бойынша жіктеуге болады:

Пайдалылық - бұл өзгертілгеннен кейін алынған мәліметтер қаншалықты пайдалы екендігі туралы өлшеу.

Потенциал - анықталмаған мәліметтер туралы түсінік алу үшін рұқсат етілмеген қолданушыдан талап етілетін білім, күш және уақыт өлшемдері.

Төзімділік - шабуылдаушыға егжей-тегжейін ашпайтын бағдарламаны жасау қаншалықты қиын екенін өлшейді. Автоматты толқынсыздыққа қарсы тұрақтылық қараңғы құрылымның қауіпсіздігін арттырады.

Құны - әзірлеу / тестілеу бағдарламасын орындау үшін алдыңғы екі әдісті қолданатын бағдарламаны құруға кететін уақытты өлшейді. үлкен жадты немесе көп уақытты қажет ететін әдіс үлкен шығынды талап етеді.

Кесте 1

Обфускация әдістері

Обфускация әдісінің беріктігі: домен	**Әдістер**	**Потенциал**	**Төзімділік**	**Құны**
Трансформация	Код	Орташа	Бір бағытты	Тегін
Трансформация	Дерек	Жоғары	Екі бағытты	Арзан
Трансформация	Басқару	Орташа	Жартылай бір бағытты	Қымбат

Бағдарламалық жасақтама жасаушы қол жетімді зияткерлік меншікті техникалық қорғаудың әртүрлі нысандары бар. Ал обфускация түрлерін 3-суреттегі сызбадан көре аласыз.[8]

3 - сурет. Обфускация түрлері

Жоғарыда келтірілген критерийлерге сүйеніп, тұндырудың кейбір пайдалы әдістері төменде келтірілген:

Символдық белгілер: тұжырымның бөлігі болып табылатын таңбалардыретке келтіріп, түпнұсқалық құндылықтар бұрмаланған сияқты.

Қайталанатын кейіпкерлер маскировкасы: бірінші таңбалардың кейбіреулері «*» -ге ауыстырылады, ал кейбіреулері сол қалпында көрсетілген.

Сандық өзгеріс: сандық мән кейбір басқа сандық мәндермен өзгертіледі.

Кодтау: мәнді көрсету үшін кейіпкерлердің бірнеше сериялары таңдалады.

Бұлттық жүйедегі қауіпсіздікке қатысты аспектілер. Қолданыстағы қауіпсіздік модельдері. Компаниялар бұлтқа тез қарай жылжуда, өйткені олар нарықтағы ең жақсы ресурстарды қолдана алады және сонымен бірге өз операцияларының құнын күрт төмендетеді. Бұлтқа көбірек ақпарат түскен сайын, қауіпсіздік мәселелері де дами бастады.

Деректерді бұзу қауіпсіздіктің ең үлкен мәселесі болып табылады. Білікті хакер клиенттің қосымшасына оңай кіріп, клиенттің құпия мәліметтеріне кіре алады. [9]

Тиімсіз және дұрыс емес API мен интерфейс оңай мақсатқа айналады. Бұлтты қызметтерді ұсынатын IT компаниялары үшінші тарап компанияларына API интерфейсін өзгертуге және өздерінің функционалдығын енгізуге мүмкіндік береді, бұл өз кезегінде бұл компанияларға бұлттың ішкі құрылымын түсінуге мүмкіндік береді.

Қызметтен бас тарту (DoS) сонымен қатар пайдаланушыға ішінара немесе қол жетімділік берілген кезде үлкен қауіп болып табылады. Қазір компаниялар тәулік бойы бұлтты қолданады және DoS қолданушы үшін де, провайдер үшін де қымбаттау әкелуі мүмкін.

Қосылымды тыңдау дегеніміз, хакердің сіздің жеке деректеріңізге кіру үшін сіздің желідегі әрекеттеріңізді қарап шығуы және белгілі бір трансляцияны көбейту / қайталауы дегенді білдіреді. Бұл сонымен бірге қолданушының заңсыз немесе қалаусыз сайттарға апаруы мүмкін.

Деректердің жоғалуы - бұл басқа мәселе. Зиянкес хакер деректерді немесе табиғи немесе қолдан жасалған кез келген деректерді жоя алады. Мұндай жағдайларда дербес көшірменің болуы үлкен артықшылық болып табылады. Қызмет көрсетушінің абайсыздығы деректердің жоғалуына әкелуі мүмкін.

Әр түрлі бұлт қызметтерінің үйлесімділігі де мәселе болып табылады. Егер пайдаланушы бір бұлттан екіншісіне ауысуды шешсе, үйлесімділік деректердің жоғалмауын қамтамасыз етеді. [10]

Бұлтты бұрыс мақсаттарда да қолдануға болады, яғни бұлтты теріс пайдалану. Бұлтта жаңа технологиялардың болуына байланысты оны стандартты компьютерде жасауға болмайтын жоғары есептеулер үшін қолдануға болады.

Бұлтты технологияларды жеткіліксіз түсіну қауіптің белгісіз деңгейіне әкелуі мүмкін. Компаниялар бұлтқа көшеді, өйткені бұл шығындарды едәуір төмендетуді қамтамасыз етеді, бірақ егер аудару қажет болмаса, фондық оқыту, туындаған мәселелер одан да көп болуы мүмкін.

Деректерді зиянды мақсаттарда қолдана алатын қазіргі немесе бұрынғы қызметкер, мердігер және т.б. түрінде ішкі ұрлық.

Шифрлау кілттерін қауіпсіз сақтау да проблема болып табылады. Жақсартылған қауіпсіздік үшін шифрлауды қолдансаңыз да, кілтті қауіпсіз сақтау мәселеге айналады. Кілттің иесі кім болуы керек? Пайдаланушы жауап ретінде көрінеді, бірақ ол қаншалықты мұқият және ұқыпты болса, ол деректердің қауіпсіздігін шешеді.

Бұлт қауіпсіздігіне қатысты түрлі қауіптерді келесі бағыттар бойынша жіктеңіз:

Қол жетімділік: бұлтты сервистердің мақсаты кез-келген жерде, кез келген уақытта пайдаланушыға ақпарат беру. Веб-қызмет бұлты қолданушыға кез-келген жерден кез-келген жерден қол жеткізуге мүмкіндік береді және бұл оны ұсынатын барлық қызметтерге қолданылады. Клиент деректердің қай жерде сақталатынын білуі керек. Клиент бұлтты қызметке жүгінетін жағдайда деректерді жою үшін провайдер деректерді жою керек. Бұлтты қызмет провайдері ешқандай ақпаратты жасырмауы керек.

Басқару: бұлтта жүйені басқару және оны пайдалану маңызды. Қызмет көрсетушінің кез-келген мүшесіне көрінетін деректер мөлшерін бақылау керек. Деректердің көрінуі бақылау деңгейін анықтайды.

Сәйкестік: тиісті органдар бұлттағы деректердің сақталуын реттейтін заңдарды анықтауы керек, өйткені бұлттар әлемнің көптеген юрисдикцияларын кесіп өтуі мүмкін. Егер деректердің бір бөлігі басқа елде сақталса және онда билік сұрайтын құпия мәліметтер болса, онда ережелер осы мәліметтерге қолданылады ма?

Деректердің тұтастығы: қарапайым түрдегі деректердің тұтастығы деректердің сақталуын және пайдаланушының рұқсатынсыз ешқандай өзгертулер жасалмайтындығын білдіреді. Бұлтта деректердің тұтастығы басты талап болып табылады. [11]

Аудит: Бұл бұлтта болып жатқан әрекеттерді қарапайым тексеруді білдіреді. Тексеру механизмінің болуы бұзушылықтардың алдын алуға көмектесу үшін журналды, оқиғалар тізімін және т.б. жүргізе алады.

Құпиялылықты бұзу: бұлтты қызмет жеткізушісі қауіпсіздікті бұзу туралы өз пайдаланушыларына хабарлауы керек. Пайдаланушы өз кеңістігінде не болып жатқанын білуге құқылы. Қызмет провайдері мұны қалай қадағалайды?

Құпиялылық: Бұл пайдаланушының деректерінің құпия сақталуын қамтамасыз етеді. Құпиялылық - бұл пайдаланушылардың қарапайым ойында сұрақтар туғызатын бұлтты сақтаудың бір аспектісі. Бұлт қоғамдық желі болып табылады және көбірек қауіптерге ұшырайды, сондықтан құпиялылық өте маңызды.

Бұлттық жүйедегі шифрлау әдістері және архитектурасы. Бұнда файлдарды шифрлау арқылы қорғауды қамтитын жақтауды ұсынамын. Құрылғыда орналасқан файл құпия сөзге негізделген AES алгоритмі арқылы шифрланады. Пайдаланушы кез-келген жүктелген шифрланған файлдарды жүктей алады және оны жүйеде оқи алады.

AES-тің артықшылықтары көп. AES кез-келген шабуылға сезімтал емес, бірақ Brute Force шабуылына ұшырайды. Алайда, Brute Force шабуылы тіпті супер компьютер үшін де оңай емес. Себебі, AES алгоритмінде қолданылатын шифрлау кілтінің мөлшері 128, 192 немесе 256 бит тәрізді, нәтижесінде миллиардтаған өзгерістер мен комбинациялар пайда болады. AES сонымен қатар RSA сияқты дәстүрлі алгоритмдерге қарағанда әлдеқайда жылдам. Осылайша, бұлтты деректерді қорғауға тамаша таңдау жасайды.

Ұсынылған жүйе тұрақты интернет байланысы болған кезде ғана жұмыс жасайтындығын атап өту керек. Файлды бұлттық жүйеге жүктеудің дерек-сызбасы 4-суретте көрсетілген.

Файлды жүктеу процесінің қадамдары төменде түсіндірілген:

Пайдаланушының аты мен құпия сөзін қабылдаңыз. Егер пайдаланушы аутентификацияланған болса, бұлтпен байланыс орнатыңыз. Басқа жағдайда, аутентификация қателігін көрсетіңіз

Пайдаланушыдан бұлтқа жүктелетін файлды таңдауын сұраңыз

Пайдаланушыдан шифрлау процесі үшін құпия сөзді енгізуді сұраңыз

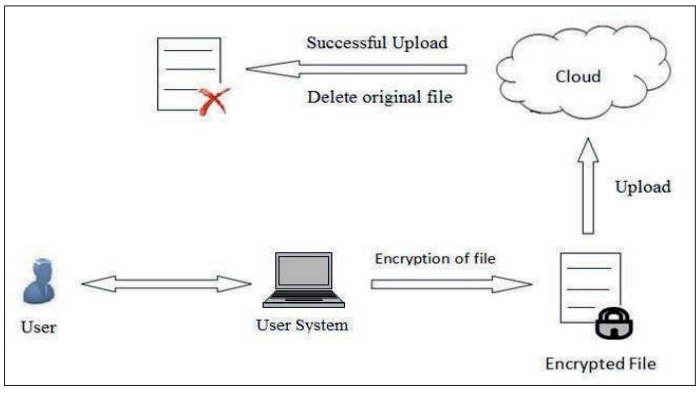
Осы құпия сөзді сақтаңыз және осы құпия сөзден кілт жасаңыз

Шифрлау алгоритмін қолданыңыз

Файлды бұлтқа жүктеңіз

Пайдаланушыдан оны жүктегеннен кейін оны жойғысы келетін-келмейтінін сұраңыз. Егер пайдаланушы жою опциясын таңдаса, файлды жойыңыз

Бұлтпен байланысты ажыратыңыз



4 - сурет. Файлды бұлттық жүйеге жүктеу

1-қадам - пайдаланушының аутентификациясы. Біз ұсынған әдістеме пайдаланушының мәліметтеріне кез-келген шабуылдың алдын алуға бағытталған. Сол қадамға апаратын алғашқы қадам - аутентификация. Жүйе пайдаланушының аты мен құпия сөзін қабылдайды. Екеуі тексерілгеннен кейін, пайдаланушыға оның файлдарына қол жетімділік беріледі. [12]

Пайдаланушы аты мен құпия сөзді енгізгеннен кейін оның жарамдылығын тексеріңіз. Егер

енгізілген аты мен құпия сөзі дұрыс болса, жүйе бұлтпен байланыс орнатады. Егер енгізілген ат пен құпия сөз дұрыс болмаса, жүйе қатені көрсетеді және қолданушыны қабылдамайды.

Келесі қадамдар пайдаланушының түпнұсқалығы расталған және бұлтпен жұмыс байланысы орнатылған жағдайда жұмыс істейді.

Жүктелетін файлды таңдау 2-қадамда жасалды. Пайдаланушы қазір қолданыстағы машинаның жадында кез-келген мәтіндік файлды таңдай алады.

Жүктелетін файл таңдалғаннан кейін 3-қадамға өтіңіз. Бұл қадам пайдаланушыны шифрлау процесі үшін құпия сөз сұрайды. Пайдаланушыға құпия сөз ретінде ұзақ фразаларды пайдалану ұсынылады. Бұл құпия сөз кілтті құру үшін қолданылады. Бұл ұрпақтың егжей-тегжейлері келесі қадамда сипатталған.

4-қадам - бұл жүйе үшін өте маңызды қадам. Бұл қадамда шифрлау процесінің кілті жасалады. AES - бұл симметриялы кілт алгоритмі, яғни шифрлау үшін мәліметтерді де шифрлау үшін қолданылатын кілт қолданылады. Бұл кілт құпия сөзден кілт генераторы функциясының көмегімен жасалады. Бізге PBKDF2 (құпия сөзге негізделген кілт құру функциясы 2) қолдануды ұсынамыз. PBKDF2 итерацияны мыңдаған ретпен қолданады. Бұл қосымша есептеу құпия сөзді бұзуды қиындатады. Бұл процесс кілтті созу деп аталады. AES алгоритмінде қолданылатын кілттерге белгілі шабуылға сезімтал болмаса да, құпия сөзді Brute-power шабуылына ұшырату мүмкіндігі бар екенін атап өту керек. Сондықтан, пайдаланушыға кілтті жасау үшін ұзақ фразаларды пайдалану ұсынылады.

Осылайша, бұл қадамда жүйе енгізілгеннен кейін құпия сөзді сақтайды және шифрлау үшін кездейсоқ кілтті жасайды.

5-қадам - шифрлау қадамы. Бұл қадамда шифрлау мәтінін құру үшін қарапайым мәтінге біздің шифрлау алгоритміміз, яғни AES алгоритмі қолданылады. Жоғарыда айтылғандай, AES кез-келген белгілі шабуылдарға ұшырамайды. Сонымен, қолданушы оның деректері бұлт қауіпсіздігіне қатысты түрлі қауіптерден сенімді екеніне сенімді бола алады. Пайдаланушының деректері екі есе сенімді, өйткені бір адам деректерге тек кірген пайдаланушы аты мен құпия сөзі ғана жарамды және екеуі де, егер пайдаланушының логин құпия сөзіне шабуыл жасалса да, жүктелген файл шифрланған, шифрланған жағдайда ғана шешіледі. пайдаланушы шифрлау процесінде енгізген құпия сөзді енгізеді.

Бұл құпиялылықты қамтамасыз етеді. Сондай-ақ, жүктелген деректер шифрланғандықтан, шифр мәтініне ешқандай өзгертулер енгізуге болмайды. Бұл мәліметтердің тұтастығын қамтамасыз етеді.

Шифр мәтіні жасалғаннан кейін, шифрланған файлды бұлтқа жүктеңіз. Бұл сіздің процестің алтыншы қадамы.

Жетінші қадам - қарапайым мәтіндік файлды машинаның жадынан алып тастауға қатысты. Пайдаланушыға бұлтқа жүктелгеннен кейін түпнұсқа файлды жою мүмкіндігі беріледі. Егер пайдаланушы мұны қаламаса, бастапқы файлды сақтаудың екінші нұсқасын таңдай алады. Түпнұсқа файлды жоюды ұсынамыз. Бұл машинада сақталған қарапайым мәтіндік файлға рұқсатсыз кірудің болмауын қамтамасыз етеді.

Егер пайдаланушы жою опциясын таңдаса, жүйе компьютерден түпнұсқа файлды жояды.

Шифр мәтіндік файлы бұлтқа сәтті жүктелгеннен кейін және пайдаланушының жүктелетін файлдары болмаған кезде, жүйе пайдаланушы тіркелгісінен шығып, бұлтпен орнатылған байланысты ажыратады.

Талқылау. Файлды желіден жүктеу. Файлдарды жүктеу процесінің қадамдары түсіндірілген:

1-қадам файлды жүктеудің 1-қадамымен бірдей. Пайдаланушының жеке басы осы қадамда аутентификацияланған.

Екінші қадамда пайдаланушының бұлтқа жүктеген файлдарының жиыны көрсетіледі. Пайдаланушыдан тізімнен файлдардың біреуін таңдау сұралады.

3-қадамда пайдаланушыдан құпия сөзді енгізу сұралады, ол файлды шифрлау кезінде енгізген. Осы енгізілген құпия сөздің дұрыстығын тексеру 4-қадамда жүзеге асырылады. Пайдаланушы жүктеген шифрланған мәтіндік файл шифрланған кезде құпия сөз шифрланған кезде енгізілген құпия сөзбен бірдей болған жағдайда ғана шифрленіп, жүктеледі. Бұл құпия сөздің шифрлау процесінде сақталуының себебі сақталған құпия сөз енгізілген құпия сөзді растау үшін пайдаланылады. Жоғарыда айтылғандай, AES алгоритмі - симметриялы кілт алгоритмі. Сондықтан, деректерді шифрлау және шифрын ашу үшін оған бірдей кілт керек. Кілтті генерациялау үшін кілт генераторының қызметіне бірдей құпия сөз енгізілген жағдайда ғана мүмкін болады.

Енгізілген құпия сөз расталғаннан кейін кілт генераторы функциясының көмегімен шифрлау

кілтін құру үшін құпия сөзді қолданыңыз. Егер құпия сөз расталмаса, қате туралы хабарды көрсетіңіз және құпия сөзді қабылдамаңыз.

5-қадамда, құрылған кілтті пайдаланып, жүктелген шифр мәтінін шифрлау үшін AES алгоритмін қолданыңыз.

Шифрланған қарапайым мәтінді пайдаланушы машинасының жадына сақтаңыз. Бұл 6-қадамда жасалады.

7-қадамда пайдаланушыдан бұлтқа жүктелген шифрлы мәтіндік файлды жойғысы келетін-келмейтіні сұралады. Егер пайдаланушы мұны таңдаса, файлдан шифрланған файлды жойыңыз.

Пайдаланушы бұлттан басқа файлдарды жүктегісі келмесе, пайдаланушы тіркелгісінен шығып, бұлтпен орнатылған қосылымды ажыратыңыз. Бұл жүктеу процесінің соңғы сатысы.

1 Пайдаланушының аты мен құпия сөзін қабылдаңыз

Егер пайдаланушы аутентификацияланған болса, бұлтпен байланыс орнатыңыз

Басқа жағдайда, аутентификация қателігін көрсетіңіз

2 Пайдаланушыдан жүктелетін файлды таңдауын сұраңыз

3 Пайдаланушыдан шифрды шешуге арналған құпия сөзді енгізуді сұраңыз

4 Осы құпия сөздің дұрыстығын тексеріңіз

Егер енгізілген құпия сөз дұрыс болса, кілт жасаңыз

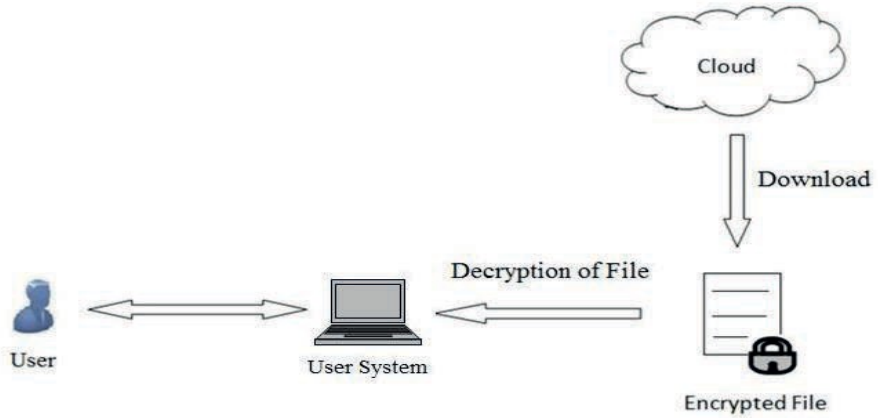
Басқа жағдайда қате туралы хабарды көрсетіңіз және құпия сөзді қабылдамаңыз

5 Шифрлау алгоритмін қолданыңыз.

Файлды бұлттан жүктеңіз. Жүктеу процесінің дерек-сызбасын 5-суреттен байқай аласыз.

7 Пайдаланушыдан жүктелген шифрланған файлды жойғысы келетіндігін сұраңыз. Егер пайдаланушы жою опциясын таңдаса, шифрланған файлды бұлттан жойыңыз

8 Бұлтпен байланысты ажыратыңыз



5 – сурет. Файлды бұлттық жүйеден жүктеу

Қорытынды. Бұлтты есептеу - бұл кез-келген адам жоғалуы мүмкін құбылыс. Бірақ кез-келген басқа технологиялар сияқты, бұлтты есептеу де қос қылыш болып табылады. Бір жағынан найзағай жылдам технологиясы, қолдануға арналған көптеген қолданбалар, шектеусіз көрінетін сақтау орны бар. Екінші жағынан, құпиялылықты бұзу, деректердің тұтастығын бұзу және деректердің қол жетімді еместігі сияқты ортақ кеңістіктегі қауіпсіздікке қатысты түрлі қауіптер жатыр. Бұл мақалада, біз бұлтқа жүктелместен бұрын файлды шифрлайтын жақтауды ұсындық. AES (Advanced Encryption Standard) - бұл ең қауіпсіз шифрлау алгоритмдерінің бірі және AES көмегімен шифрланған мәліметтерге көптеген шабуылдар сәтті бола бермейді. Бұл ұсыныс бұлттағы деректерге төнетін қауіптердің көпшілігін шешеді. Сондай-ақ, біздің құрылым пайдаланушының деректеріне шынайы және рұқсатты қол жетімділікті қамтамасыз ету үшін кіру идентификаторы мен құпия сөзді пайдалануды ұсынады. Осылайша, бұлтты есептеу қауіпсіз қолданылса, қолданушыға таңғажайып артықшылықтар береді және қауіпсіздікке төнетін жалғыз кемшілігін жеңеді.

Information about the authors:

Tashenova Zhuldyz – PhD, L.N. Gumilyov Eurasian National University, Department of Information technology, Nur-Sultan, Kazakhstan. E-mail: zhuldyz_tm@mail.ru, ORCID: 0000-0003-3051-1605;

Nurlybaeva Elmira – PhD, Kazakh National Academy of Arts named after T. Zhurgenov, Almaty, Kazakhstan. E-mail: nuremuk@mail.ru, ORCID: 0000-0002-0479-7542;

Abdugulova Zhanat – PhD, L. N. Gumilyov Eurasian National University, Department of Information technology, Nur-Sultan, Kazakhstan. E-mail: janat_6767@mail.ru, ORCID: 0000-0001-7462-4623;

Amanzholova Sh – assoc.professor, Kurmangazy Kazakh National Conservatory, Almaty, Kazakhstan. E-mail: schirin75@ mail.ru, ORCID: 0000-0002-6674-2766.

ӘДЕБИЕТТЕР

[1] Е. Гребнева. Облачные сервисы: взгляд из России. – М.: С News, 2011. – 282с.

[2] Николас Карр. Великий переход: что готовит революция облачных технологий» 2014. – 272 с.

[3] С. Сейдаметова, С.Н. Сейтвелиева. Облачные сервисы в образовании. -Симферополь, 2012 - 206с.

[4] Модели облачных технологий. – Режим доступа: http://wiki.vspu.ru/workroom/adb91/index.

[5] Облачные вычисления (Материал из Википедии – свободной энциклопедии) - Режим доступа: https://ru.wikipedia.org/wiki/Облачные_вычисления.

[6] Что такое облачные сервисы, и какие бывают облачные технологии, а также их применение – Режим доступа: http://sd-company.su/article/cloud/service.

[7] http://www.bourabai.kz/mmt/cloud.htm.

[8] Клементьев И.П. Устинов В.А. Введение в облачные вычисления. – УГУ, 2009.

[9] Широкова Е.А. Облачные технологии - Уфа: Лето, 2011.

[10] http://bigital.ru/oblachnye-texnologii-budushhee-i-perspektivy.

[11] Облачные сервисы: взгляд из России. Под ред. Е. Гребнева. – М.: С News, 2011. – 282с. -Режим доступа: http://expo itsecurity.ru/upload/iblock/909/CloudTechnology.pdf.

[12] Облачные сервисы для библиотек и образования И. Билан// «Университетская книга» №10, 2011.

REFRENCES

[1] E. Grebneva. Cloud services: a look from Russia. – M.: CNews, 2011. – 282p.

[2] Nicholas Carr. The great transition: what is preparing a revolution in cloud technologies» 2014. - 272 p.

[3] S. Seydametova, S.N. Seitveliev. Cloud services in education. -Simferopol, 2012 - 206p.

[4] Models of cloud technologies. - Access mode: http://wiki.vspu.ru/workroom/adb91/index.

[5] Cloud calculations (Material from Wikipedia - free encyclopedia) - Access mode: https://ru.wikipedia.org/wiki/Oblachnye_chychisleniya.

[6] What are the cloud services, and what are the cloud technologies, and also their application - Access mode: http://sd-company.su/article/cloud/service.

[7] http://www.bourabai.kz/mmt/cloud.htm.

[8] Klementiev I.P. Ustinov V.A. Introduction to cloud computing. - UGU, 2009.

[9] Shirokova E.A.Cloud technologies - Ufa: Summer, 2011.

[10] http://bigital.ru/oblachnye-texnologii-budushhee-i-perspektivy.

[11] Cloud services: a look from Russia. Under the editor. E. Grebneva. - M.: CNews, 2011. - 282p. - Access mode: http: // expo itsecurity.ru/upload/iblock/909/CloudTechnology.pdf.

[12] Cloud services for library and education I. Bilan // “University Book” №10, 2011.

СОДЕРЖАНИЕ

ИНФОРМАТИКА

ФИЗИКА

МАЗМҰНЫ

ИНФОРМАТИКА

ФИЗИКА

CONTENTS

COMPUTER SCIENCE

PHYSICS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 10.03.2022.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,0 п.л. Тираж 300. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19