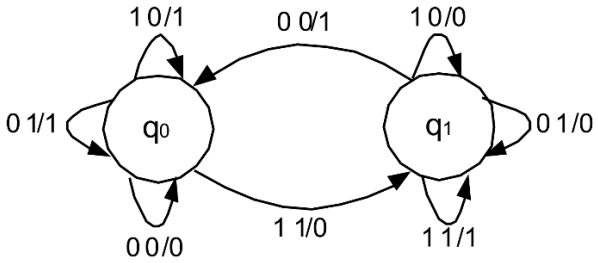
Абстрактылы автоматтың қолданылу мысалы.

Екілік санау жүйесіндегі тізбектердің сумматоры. Автоматтың екі күйі бар: q_0 –көшіру бар (цифрларды қосу кезінде алдыңғы разрядтан келген бірлік көшіруді есепке алмаймыз);

q_1 –көшіру жоқ (көшіру бірлігін есепке алу қажет).



9-сурет Бір разрядты екілік санау жүйесіндегі тізбектердің сумматорының графы

Қорытынды. Ақпараттық технологиялардың дамуы автоматтар теориясын цифрлық электрониканың аппараттық құралдарын модельдеу шеңберінен тысқары алып, оны қазіргі теориялық информатиканың іргелі негіздеріне дейін кеңейтті. Бүгінгі таңда автоматтар теориясында жасалған абстракциялар мен модельдер формальды грамматика теориясы, математикалық лингвистика, логикалық модельдер теориясы, математикалық логика, кодтау теориясы және басқалары сияқты ғылыми пәндерге қажет. Абстрактылы автоматтарды дискретті ақпарат түрлендіруші ретінде қарастыруға болатындықтан, оны криптографияда қолдануға болады. Жүргізіліп жатқан зерттеулер дәл криптографиялық түрлендірулерде машиналарды пайдалануға бағытталған.

Қолданылған әдебиеттер тізімі

1. Минский М. Вычисления и автоматы. – М.: Мир, 1971. - 364 б.
2. Карпов Ю. Г. Теория автоматов. – СПб.: Питер, 2002. - 206 б.
3. Романов В. Ф. Лекции по теории автоматов. – Владимир, 2009. – 1-бөлім.

ОӘЖ 004.056

БҰЛТТЫ ЕСЕПТЕУЛЕРДЕ ДЕРЕКТЕРДІ ҚОРҒАУ ҮШІН ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ

Омарова Жания Жанатовна
zhaniya.omarova@bk.ru
Л.Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің магистранты
Нұр-Сұлтан, Қазақстан
Ғылыми жетекшісі – А.К. Сексенбаева

Бұлттық есептеулер әртүрлі есептеулер мен есептерді қамтамасыз ету үшін бірлесіп қолданылатын компьютерлер тобын қамтиды. Бұлтты есептеулер – соңғы бірнеше жылдағы ең маңызды IT-парадигмаларының бірі. Негізгі артықшылықтардың бірі – IT технологиясы компаниялары үшін, уақыт пен шығынды азайту. Бұлттық есептеулер компаниялар мен ұйымдарға жалпы сақтау және есептеу ресурстарын пайдалануға мүмкіндік береді. Бұл өз инфрақұрылымын дамытуға және пайдалануға қарағанда тиімді. Бұлтты есептеулер ұйымдар мен компанияларға икемді, қауіпсіз және экономикалық тиімді IT-инфрақұрылымы болуға мүмкіндік береді. Оны ұйымдар мен үйлерге орталықтандырылған басқарылатын, тиімді және үнемді энергия көзіне қосылуға мүмкіндік беретін ұлттық электр желілерімен салыстыруға болады. Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle және Novell сияқты негізгі корпорациялар бұлтты есептеулерге инвестиция салып, жеке тұлғалар мен компаниялар үшін бірқатар бұлтты шешімдерді ұсынады.

Бұлтты есептеулер қоғамдық бұлт, жеке бұлт, гибридті бұлт және қауымдастық бұлты қамтиды. Қызметтерді ұсыну модельдері SaaS (қызмет ретінде бағдарламалық қамтамасыз ету), PaaS (қызмет ретінде платформа) және IaaS (қызмет ретінде инфрақұрылым) ретінде жіктелуі мүмкін. Бұлттық есептеулерді әдетте екі тәсілмен жіктеуге болады: бұлттық есептеулердің орналасқан жері бойынша және ұсынылған қызмет түрлері бойынша. Бұлт орналасуы бойынша бұлтты есептеулер әдетте мыналарға бөлінеді: жария бұлт (онда есептеу инфрақұрылымы бұлт жеткізушісі орналасқан); жеке бұлт (есептеу инфрақұрылымы белгілі бір ұйымға тағайындалған және басқа ұйымдармен бірлесіп пайдаланылмайтын); гибридті бұлт (жеке және жария бұлттарды бірге пайдалану); және қауымдастық бұлты (ол бір қауымдастық ұйымдары арасында АТ инфрақұрылымын бірлесіп пайдалануды көздейді). Егер классификация ұсынылатын қызметтердің түріне негізделген болса, онда бұлт былайша жіктеледі: IaaS (Инфрақұрылым қызмет ретінде), PaaS (платформа қызмет ретінде) және бағдарламалық жасақтама қызмет ретінде (SaaS) [1].

Бұлттық есептеулер электрондық түрде деректерді өңдеу және берудің жаңа технологиясы ретінде қазіргі уақытта іс жүзінде әрбір компьютерлік жүйеде қолданылады. Ол шабуылдардың алуан түрлері үшін ашық желілік инфрақұрылымда жұмыс істейді. DDoS (қызмет көрсетуден бас тарту) - қолданылатын ең танымал шабуылдардың бірі. Syn cookies, сондай-ақ бұлтты технологиямен байланысты пайдаланушылардың серверге қол жеткізуін шектеу қызмет көрсетудегі бөлінген бас тартуды тоқтату шаралары ретінде пайдаланылуы мүмкін.

Бұлтты есептеу технологиясына шабуыл жасаудың басқа түрі – бұл man in the middle. Secure Socket Layer (SSL) – бұл шабуылдарды еңсеру үшін қауіпсіздік техникасы. Егер бұл қауіпсіздік әдісі дұрыс орнатылмаса, клиент пен сервердің аутентификациясы бұлтты технология пайдаланушыларын ортасында адамнан қорғау үшін тиісті түрде жұмыс істемеуі мүмкін.

Бұлттық есептеулерді пайдалану кезінде деректерді қорғау қауіпсіздігі мәселелері тиісті түрде шешілуі және барынша азайтылуы тиіс. Біз бұлтты есептеулерді пайдаланғанда, біз алдымызда жоқ қатты дискілер мен процессорларда біздің бағдарламалық жасақтаманы іске қосамыз. Сондықтан пайдаланушылар осы технологияны пайдаланған кезде қауіпсіздік мәселелеріне көп күмән тудырады. Осылайша, бұлтты технологияларда шабуылдардың көптеген түрлері болуы мүмкін. Жоғарыда аталғандардан басқа, белгілі шабуылдардың көпшілігіне фишинг, IP-спуфинг, хабарламаларды түрлендіру, трафикті талдау, IP-порттар және т. б. кіреді. Бұлттық есептеулер жабдықтаушыларынан алынатын деректерді қорғау үшін қауіпсіздікті қамтамасыз етудің көптеген әдістері бар және олардың барлығы аутентификацияны, құпиялылықты, кіруді бақылауды және авторландыруды қамтамасыз етеді.

Бұлт есептеулеріндегі Аутентификация

Бұлттық есептеулердегі Аутентификация тиісті заңды немесе жеке тұлғаның бұлттық технология жеткізушісінен берілген деректерге қол жеткізуіне кепілдік береді. Аутентификация бұлтты есептеулерде қамтамасыз етілген кезде, бұлтта сақталған ақпаратқа қол жеткізу кезінде пайдаланушының жеке басын бұлт қызметі провайдеріне дәлелдейді. Бұлттардың көпшілік және жеке түрлері RSA көмегімен аутентификация үшін әр түрлі конструкцияларды пайдаланады. RSA криптожүйесі екі факторлы аутентификация, білім негізінде аутентификация және адаптивті аутентификация сияқты аутентификацияның түрлі үлгілерін қабылдайды. AWS (Amazon Web Services) виртуалды жеке бұлтты қоса алғанда, веб-сервер мен браузер арасында құпия ақпаратты беруге шоғырланады.

Бұлт есептеулерін пайдаланғанда, кейбір сыртқы веб-сайттағы қажетті IP мекенжайларының аутентификациясын қосу үшін прокси серверді баптауға болады. Прокси серверінің URL мекенжайы тек сенімді сайттарға кіруге мүмкіндік береді.

Сондықтан бұлттық технология деректерін қорғау үшін келесі аутентификация механизмдері жиі қолданылады: білім негізінде аутентификация, екі факторлы аутентификация, адаптивті аутентификация, көп факторлы аутентификация және бір пароль

бойынша аутентификация. Білім негізінде аутентификация, екіфакторлы аутентификация және адаптивті аутентификация RSA көмегімен қосылған және олардың артықшылықтары шығындарды азайту мен қауіпсіздікті арттырудан тұрады

Көп факторлы аутентификация бұлтта деректерді қорғау үшін AWS қолданылады. Осы аутентификация механизмінің артықшылықтары ол идентификация мен қолжетімділікті басқаруға мүмкіндік береді. Бұлтта деректерді қорғауды қамтамасыз ету үшін Facebook-тен бірегей аутентификация паролі қолданылады. Мұндай аутентификация механизмінің артықшылығы ол honeypot шабуылынан және сөздікке шабуылдан қорғауды қамтамасыз етеді.

Бұлтты есептеулердегі құпиялылық

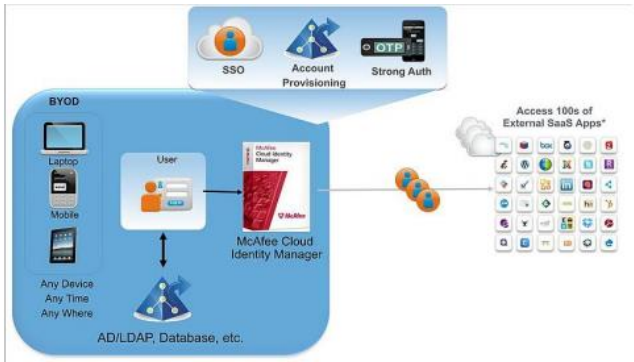
Құпиялылық бұлттағы пайдаланушылардың деректерін қорғаудың маңызды тетіктерінің бірі болып табылады. Бұл деректер бұлтта сақталғанға дейін шифрланған мәтіндегі ашық мәтінді шифрлауды қамтиды. Бұл әдіс пайдаланушы деректерін қорғайды, тіпті бұлт қызметінің провайдерлері бұлтта сақталған мазмұнды өзгерте немесе оқи алмайды.

Бұл қорғаныс түрін Dell data protection and encryption компаниясы ұсынады, онда пайдаланушылардың деректері оларды сыртқы дискіде немесе тасымалдаушыда сақтағанда қорғалады. Шифрлау бағдарламалық және аппараттық қамтамасыз ету арқылы жүзеге асырылуы мүмкін. Мұндай қорғаныс түрінің үлкен артықшылығы-бұл пайдаланушыларға Dell деректерді қорғау және шифрлау саясаттарын қолдану туралы алаңдатудың қажеті жоқ. Dell, сондай-ақ, деректерге қатынайтын пайдаланушыларды басқару үшін мөлдір файлдарды шифрлауды пайдаланады.

Құпиялылықты, сондай-ақ vendor Online Tech компаниясы қамтамасыз етеді, ол бұлттық есептеулерде шифрлау әдістерін (мысалы, дискіні толық шифрлау) пайдалана отырып, қатты дискіде сақталған деректерді жүктеудің бүкіл процессінде шифрлайды. Барлық дискті шифрлау, сондай-ақ белгілі AES (Advanced Encryption Standard) алгоритмі арқылы деректерді шифрлау үшін қолданылады. Бұлттық есептеу технологиясын пайдаланатын құрылғы жоғалған немесе ұрланған болса, жоғалған немесе ұрланған құрылғыдағы деректерді қорғайтын bit locker құпия сөзі де бар.

Бұлт есептеулеріне қатынауды бақылау

Бұлттық есептеулерде деректерді қорғауды қамтамасыз ету үшін қатынауды бақылау өте маңызды қауіпсіздік тетігі болып табылады. Бұл тек авторизацияланған пайдаланушылардың бұлтта сақталған сұралған деректерге қол жеткізуіне кепілдік береді. Бұлт есептеулеріне қатынауды тиісті бақылауды қамтамасыз ететін қауіпсіздікті қамтамасыз етудің әртүрлі әдістері бар. Басып кіруді, брандмауэрлерді анықтау жүйелері, сондай-ақ міндеттерді бөлу түрлі желілік және бұлтты деңгейлерде іске асырылуы мүмкін. Брандмауэр бұлт желісі арқылы тек сүзілген мазмұнды өткізуге мүмкіндік береді. Брандмауэр әдетте пайдаланушы орнатқан белгілі бір қауіпсіздік саясатына сәйкес реттеледі. Брандмауэр әдетте қосымша деректер қауіпсіздігін қамтамасыз ететін демилитаризацияланған аймақтарға жатады.



Сур. 1 Бұлтты есептеу үшін McAfee ұсынған бұлтты идентификациялау менеджері

McAfee-бұлт есептеулеріне қатынауды бақылауды қамтамасыз ететін жеткізуші. Ол McAfee Single Sign On, McAfee Web Gateway және McAfee one time password сияқты

қатынауды бақылаудың түрлі әдістерін ұсынады. Мұндай қауіпсіздікті қамтамасыз ету әдістері саясатты басқаруға және деректердің жоғалуын болдырмауға мүмкіндік береді. (Сур. 1) Fujitsu-бұл виртуалды жүйені басқару және басқарудың орталықтандырылған авторизациясы сияқты әр түрлі авторландыру әдістерімен қатынауды бақылауды ұсынатын тағы бір жеткізуші. Бұл қауіпсіздік әдістері интернет аралық сценарийлер мен инъекциялық шабуылдарды болдырмау үшін тиімді.

Бұлттық есептеулерде Авторизация

Бұлттық есептеулерде авторизациялану пайдаланушылар үшін маңызды, себебі олар бұлттық қызметке кірген кезде, олардың сәйкестігін дәлелдеуге мүмкіндік береді. Осылайша, авторизациялану әдетте аутентификациядан кейін қолданылады. Oracle Database Vault – бұлтта авторизациялауды жүзеге асыруға мүмкіндік беретін қауіпсіздік техникасының үлгісі. Бұл қауіпсіздік әдісі Oracle жеткізушісімен ұсынылады. Әр түрлі әкімшілік қолданушылардан берілген қосымшалар осы авторизация әдісі арқылы қорғалған. Авторлар [2] құпиялылық саясатын дербес орнатуға мүмкіндік бере отырып, пайдаланушылардың құпиялылығын қорғайтын саясат негізінде авторизациялау әдісін пайдаланады. Осылайша, пайдаланушылар өз деректерін рұқсатсыз қол жеткізуден тиімді қорғайды. Бұлтта авторландыру қызмет жеткізушілердің саясатын корпоративтік каталогтармен және әртүрлі саясаттармен біріктіретін VMware компаниясымен ұсынылады. Сертификаттар немесе жұмсақ белгілер соңғы пайдаланушыларды қауіпсіз авторизациялау үшін пайдаланылады. Oasis Cloud authorization рұқсаттарды басқаруға негізделген қауіпсіздік әдістерін пайдалануға мүмкіндік береді. Пайдаланушы журналдары пайдаланушылардың орналасқан жері мен пайдаланушылардан пайдаланылатын құрылғылар туралы ақпаратты беретін осы әдіс арқылы қолдау көрсетеді.

Қорытынды

Бұл жұмыстың негізгі мақсаты бұлтты есептеулерде деректерді қорғау қауіпсіздігін қамтамасыз ету әдістерін талдау және бағалау болды. Осы мақсатта біз бұлтты есептеу жабдықтаушыларынан қабылданған деректерді қорғау үшін қауіпсіздікті қамтамасыз етудің аса маңызды әдістерін талдап, бағаладық. Біз оларды қауіпсіздік тетіктеріне сәйкес төрт бөлім бойынша топтастырдық: аутентификация, құпиялылық, кіруді бақылау және авторизация.

Сонымен, біз бұлтты технологиялар саласындағы негізгі сұрақтарға табысты жауап бердік, немесе деректерді қорғауда бұлтты есептеулерге сену керектігін айтты. Егер аутентификацияны, құпиялылықты, кіруді бақылауды және авторизациялауды қамтамасыз ететін барлық ұсынылған шараларды ескерсе, бұлттық есептеулерге деректерді қорғау саласындағы сенуге болады.

Біз сондай-ақ бұлттағы деректердің тиісті қауіпсіздігін қамтамасыз ету үшін терең ескерілуі тиіс қауіпсіздік мәселелеріне назар аударды. Біз бұлтта деректерді қорғауға қатысты маңызды қауіпсіздік шараларын ескеруді ұсындық.

Қолданылған әдебиеттер тізімі

1. L. Badger, T. Grance, R. Patt-Corner and J. Voas, “Cloud computing synopsis and recommendations (draft), nist special publication 800-146”, Recommendations of the National Institute of Standards and Technology, Tech. Rep. (2011).
2. D. W. Chadwick and K. Fatema, “A privacy preserving authorisation system for the cloud”, Journal of Computer and System Sciences, 78(5), (2012), 1359-1373.
3. M. Hange, “Security Recommendations for Cloud Computing Providers”, Federal Office for Information Security (2011).
4. Синиченко С. О безопасности облачных сервисов. -Директора по безопасности, декабрь 2009.