Multi-Bulud Sistemlərində Kibertəhlükəsizlik Problemləri

İlkin Əzizov
azizovilkin@hotmail.com

***Xülasə*— Bu məqalə son zamanlar bulud texnologiyaları sahəsində yeni yanaşma olan multi-bulud sistemlərinə həsr olunub. Multi-bulud sistemlərinin kiber-hücumlara qarşı dayanıqlığı və kiber-müdafiəsi metodlarına baxılır.**

Açar sözlər— bulud texnologiyaları, multi-bulud sistemi, informasiya təhlükəsizliyi, kibertəhlükəsizlik.

I. GİRİŞ

Bulud texnologiyaları son zamanlar verilənlərin emalı mərkəzləri (Data Centres, DC) üçün yeni bir dizayn modeli olaraq yaranmışdır. Axtarış, elekton məktub, sosial şəbəkələr və s. kimi imkanlara malik tətbiqlər təqdim edən servis provayderləri bu xidmətləri təklif edirlər. "Multi-bulud" anlayışı elmi araşdırmalarda "inter-bulud" və "buludların buludu" kimi də tanınır.

Bulud xidməti təklif edən provayderlər üçün informasiyanın gizliliyi və təhlükəsizliyi önəmli məsələdir. "Tək bulud" provayderlərində problemlə qarşılaşma riski, istifadəçiyə daha uyğun xidmət təklifi və tək buludda bədniyyətli kontekstlə qarşılaşma ehtimalı nəzərə alındığına görə, son zamanlar aktuallığını itirir.

Məqalədə multi-bulud sistemlərində kibertəhlükəsizlik problemləri və onların həllərinə yanaşmalar analiz edilir. Məqalənin strukturu aşağıdakı kimidir. Əvvəlcə multi-bulud şəbəkə topologiyası üzrə olan araşdırmalarda önə çıxan mövzulara toxunulur. Sonra bu sistemlərdə kibertəhlükəsizlik problemləri analiz edilir, kibertəhlükəsizliyin təmin edilməsi metodlarına, o cümlədən risklərin idarə edilməsinə yanaşmalar, multi-bulud sistemlərində identifikasiya və girişin idarə edilməsi metodlarına baxılır.

II. MULTİ-BULUD TOPOLOGİYASI

Multi-bulud topologiyası İnternet olaraq biliinən məlumat şəbəkəsinə bənzərdir və birlikdə işləyə bilmə imkanına sahibdir: "Bulud hesablamaları" dünyasında kontekst, məlumat saxlama və məlumat emalı multi-bulud kimi tanınan bulud şəbəkəsinin hər yerində yerləşə və birlikdə işləyə bilər.

WAN şəbəkəsinin topologiyasında istifadə edərək İnternet infrastrukturunun üzərinə modellənmişdir. Bunun üçün çeşidli provayderlərin yaranmasına ehtiyac yaranır. İlk olaraq Multi-bulud Kök provayder çoxluğu olaraq, multi-bulud hesablama qaynaqları üçün "Cloud Computing Resource Catalogs"-a ev sahibliyi edə biləcək və DNS kimi çalışma metoduna sahib olacağı düşünülür. Bulud özəlliklərindən (kök sistemlərin çoxaldılması (təkrarlanması) və iyerarxik olması) önəmli fərqi iyerarxik şəkildə çoxaldılmamasıdır. Miqyaslanması üçün köklərin "Peer-to-Peer" texnologiyasını istifadə edərək "yan-yana" və ya "yuxarıya doğru" çoxaldılması nəzərdə tutulmuşdur. P2P texnologiylarında olan "yan-yana" çoxaldılmada "Əsas düyün" çoxaldılarkən "yuxarıya doğru" çoxaldılmada bir-birinə bağlı düyün təkrarlanır.

Multi-bulud mübadiləsi, sıra ilə qaynaqlara bəzi seçimlər və məhdudiyyətlər tətbiq edərək Bulud qaynaqlarını bərabərləşdirmək üçün paylanmış qaynaq kataloq məlumatlarında istifadə edir. Bundan əlavə, mübadilələr uyğun sorğuların optimallaşdırılmış qaynaqlarını yüngülləşdirmək üçün DHT (Distributed Hash Table) yer paylaşımı metoduna görə "peer to peer" arası bir məlumat emalı prosesi düyünləri təmin edir. DHT yer paylaşımı düyünlərdəki məlumatları federativ Multi-bulud Köklərindən köçürür (çoxaldır).

"RDFPeers", "Piazza", "PIER" və "Distributed Overlay for Federation of Enterprise Buluds" kimi Semantik Peer-to-Peer əsaslı sistemlər üzərində çox sayda tədqiqat işləri aparılmışdır. Multi-bulud topologiyasındakı bütün elementlər Multi-bulud birlikdə işləyə bilməyə qoşulmaq üçün Multi-bulud protokollarını tətbiq edən bir İnternet marşrutlayıcısına analoji bəzi şəbəkə şlüzü özəlliklərinə sahibdir. Buna Multi-bulud Şəbəkə şlüzləri deyilir.

Sonrakı bölmədə multi-bulud sistemlərində qarşılaşılacaq problemlər müəyyən edilərək sinifləndirilmişdir.

III. MULTİ-BULUD SİSTEMLƏRİNDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİ

İnformasiya üçüncü bir tərəflə paylaşılacağından, bulud istifadəçiləri tək buludda etimad edilməyən bir bulud provayderindən qaçınmaq istəyirlər. Hesab kartı məlumatları və ya bədniyyəli kontekstdən qorunması kritik bir önəmə sahibdir. Məlumat bazasını böyük bir verilənlər mərkəzinə köçürülməsi, virtuallaşdırılma təhlükəsizlik boşluğu, giriş icazəsi boşluğu, üçüncü tərəflərdən girişi edilən məlumatlarla bağlı məxfilik və idarə edilmə problemləri, tamlıq, konfidensiallıq, məlumat itkisi və ya oğurluğu kimi bir çox kibertəhlükəsizlik problemlərini əhatə edir. Bulud xidmətlərinə etimadsızlıq faktorları kimi aşağıdakı problemləri müəyyən edir.

- ***Verilənlərin tamlığı***: Bulud təhlükəsizlik riskləri ilə bağlı ən önəmli mövzulardan biri də verilənlərin tamlığıdır. Buludda saxlanan verilənlər köçürülmə zamanı bulud köçürülmə işinə və ya bulud saxlama provayderinə zərər verə bilər.
- ***Məlumat müdaxiləsi:*** Bir bulud provayderi ilə baş verə biləcək təhlükəsizlik riskidir: Amazon bulud xidməti kimi bir şifrə və ya məlumat oğurluğu kimi müdaxiləyə məruz qalması.

DOI: 10.25045/NCSoftEng.2017.52

Bədniyyətli Amazon hesab şifrəsinə əldə edərək bütün hesabın bağlı olduğu servislərə və qaynaqlara giriş əldə edə bilər.

- ***Xidmətin əlyetərliyi***: Bulud xidmətlərində başqa bir problem isə xidmətin əlyetərliyidir. Amazon lisenziya müqaviləsində təklif etdiyi xidmətin istifadəsi mümkün olmadığı vaxtların olduğunu bildirir. Əgər istifadəçinin faylı bulud saxlama siyasətində problem yaradarsa, istifadəçinin veb xidməti hər hansı bir zamanda hər hansı bir səbəbdən ləğv edilə bilər.

Bu multi-bulud sistemlərində federasiyaya daxil olan buludların etimad indeksinin olması informasiyanın paylaşılmasında qarşıya çıxacaq təhlükəsizlik problemlərini minimuma endirmiş olur.

IV. TƏHLÜKƏSİZLİYİN TƏMİN EDİLMƏSİ METODLARI

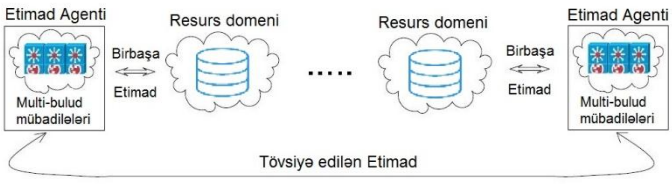
A. Etimad (Trust) modeli

Multi-bulud federativ birləşmiş buludlar mühitində təhlükəsizlik tədbirləri daha önəmli və mürəkkəbdir. Multi-bulud modeli məlumatların və gizliliyin qorunduğuna əmin olunduğu halda istifadəçilər tərəfindən qəbul edilir. Etimad heterogen bulud sistemlərində təhlükəsizlik üçün ən təməl yollardan biridir.

Hal-hazırda PKI (Public Key Infrastructure) əsaslı Etimad modeli sistemi ən çox istifadə olunur. PKİ Etimad modeli, bütün sistemi qoruma altına almaq üçün bir neçə kök düyünə bağlı olmalıdır. Kök düyünlərin etimad sertifikatları, mükəmməl qurulmuş CA (Certificate Authority) tərəfindən imzalanır.

Təməl olaraq, multi-bulud topologiyası PKI əsaslı Etimad modelinə qoşulur. PKI Etimad modelində Multi-bulud Kök sistemləri bir "Trust Authority" olaraq fəaliyyət göstərir. Etimad modeli infrastruktunda Etimad zənciri yaratmaq üçün CA tərəfindən verilən bir Sertifikat istifadə olunmalıdır [1]. Sertifikatları təqdim edən CA-lər, xüsusi formatları təmin etməlidir. Bu sahədə bəlli şirkətlər tərəfindən yoxlamalar aparılaraq və "Public Key Infrastructure" [2] olaraq bilinən ən yaxşı tətbiqlərə uyğun olmalıdır. Bu tələblər fərqli ölkələrdə fərqli tətbiq edilə bilər.

Multi-bulud topologiyası Multi-bulud Kök, statik PKI CA kökünə bənzər funksionallıq təmin edilməsi üçün yeniləmələr edilir. Digər tərəfdən, multi-bulud mübadiləçiləri, PKI sertifikat əsaslı Etimad modeli üzərinə laylı dinamik "Trust level" modelindən cavabdeh olacaqdır. Ümumi Etimad modeli, "Domain based Trust" modelindən daha çoxdur. Bulud provayderləri informasiya texnologiyaları sahəsini çeşidli Etimad sahələrinə bölür. Eyni domen altındakı düyünlər, ümumiyyətlə, bir-birlərini daha çox tanıdıqları üçün daha çox etimad edirlər (şəkil 1).



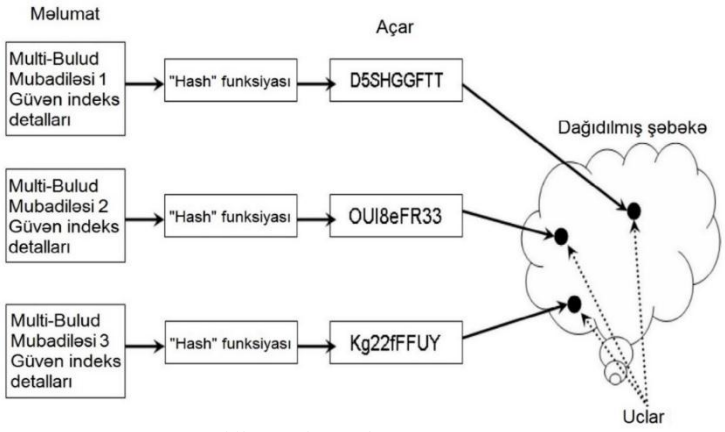
Şəkil 1. Multi-buludlarda Etimad idarəçiliyi modeli.

Bundan sonrakı başlıqda sistemin idarə edilməsində istifadə olunan DHT nəzəriyyəsinə baxılacaqdır.

B. Bağlantılarda DHT nəzəriyyəsi (Distributed Hash Table)

Multi-bulud mübadiləsi bir Etimad agenti olaraq, "DHT overlay" əsaslı yanaşma ilə peer-to-peer şəklində başqa bir bulud provayderinin (müvafiq Etimad agenti vasitəsilə) "Trust index"-ni tapır. "DHT overlay" sisteminin əsas ideyası bir açar aralığını uclara bərabərləşdirmək və bununla da hər ucun bu aralığın bəlli bir hissəsindən cavabdeh olması və heş açarları ucun hissəsinə aid olduğu məlumatı saxlamasıdır (şəkil 2). Bu cür sistemlərin üstünlüyü deterministik davranışları və uclar arasındakı yükü ədalətli balanslaşdırmasıdır. Bundan başqa, "location transparency"-də təmin edilir: sorğular məlumatın gerçək yerləşmə yerini bilmədən, hər hansı bir ucdan verilə bilər.

"DHT peer-to-peer overlay" modeli, şəbəkədəki cihazları təmsil edən məntiqi ucları, məlumat strukturunu təmsil edən bir açar aralığından gələn açarlarla əlaqələndirən, özünü idarə edə bilən, paylanmış bir giriş strukturudur. Hər bir uc ümumi açar aralığının bir hissəsinə cavabdehdir və qonşu uclara sorğuları göndərmək üçün əlavə yönləndirmə informasiyası saxlayır. Şəbəkəyə daxil olan cihazların sayı və paylaşılan məlumatın həcmi dəyişdikcə, uclar yönləndirmə cədvəllərini (routing table) dinamik və paylanmış bir şəkildə binar axtarış ağacı alqoritmi ilə effektiv şəkildə idarə edir.



Şəkil 2. Paylanmış heş cədvəli

Bundan sonrakı bölmədə multi-bulud sistemində istifadəçilərin girişlərinin idarə edilməsi üçün nəzərdə tutulan platformaların işləmə prinsiplərinə baxılacaqdır.

V. MULTİ-BULUD SİSTEMLƏRİNDƏ İDENTİFİKASİYA VƏ GİRİŞİN İDARƏ EDİLMƏSİ

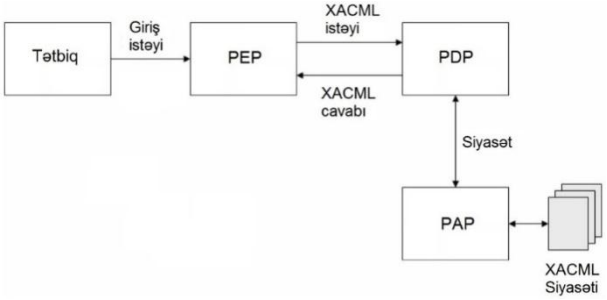
Multi-bulud sistemində identifikatorların idarə edilməsi üçün bir çox stantdarlar istifadə edilərək keyfiyyətli standartlar modeli ilə federativ identifikatorların idarə edilməsi dəstəklənir. Əhatəli İdentifikator İdarəetmə sistemləri tipik olaraq İstifadəçi qarşılanması və idarə edilməsi, identifikatorların identifikasiyası və səlahiyyətləndirmə və identifikasiya məlumatlarının inteqrasiyası – virtuallaşdırılması kimi xidmətləri təmin edir. Federativ identifikasiya modelində bulud provayderinin başqa bir bulud provayderi ilə təhlükəsiz şəkildə bağlantı qurması üçün, Etimad provayderi servisindən bir Etimad bildirişi istəyir. Etimad provayder servisi soruşulan

DOI: 10.25045/NCSoftEng.2017.52

bildirişlə birlikdə Etimad servisinin şifrəli sübut bildirişi olan gizli açarların iki nüxsəsini göndərir.

Multi-bulud mühitində geniş səlahiyyətləndirmə ilə bağlı XACML [12] girişə nəzarət və siyasətin tətbiqi üçün standart dil və metod təklif edir (şəkil 3). XACML (eXtensible Access Control Markup Language), OASIS-də standartlaşdırılan girişə nəzarət üçün XML əsaslı bir dildir. XACML həm girişə nəzarət siyasəti dili, həm də sorğu/cavab dilini açıqlayır. Sorğu/Cavab dili, müəyyən bir giriş sorğularının icazəli olub-olmadığını təsvir edir və bu sorğulara verilən cavabları açıqlayır. XACML çalışma ssenarisində bir mövzu (məsələn. insan-istifadəçi, işçi stansiya) müəyyən bir qaynaq üzərində bəzi işləri yerinə yetirmək istəyir. Mövzu, sorğunu qaynağı qoruyan subyektə (məs., fayl sistemi, poçt serveri, veb server) göndərir. Bu subyektə "Policy Enforcement Point (PEP)" deyilir.

PEP mövzunun, işləmin, qaynağın və digər əlaqəli məlumatların simvollarına əsasən bir sorğu formalaşdırır (XACML sorğu dilini istifadə edərək). PEP daha sonra bu tələbi, sorğunu incələyən, bu tələb üçün keçərli olan siyasətləri (XACML siyasət dilində yazılmış) alır və bu giriş üçün Siyasətləri dəyərləndirmək üçün XACML qaydalarına görə verilməsi lazım olub-olmadığını müəyyən edən ilk qərar nöqtəsinə – "Policy Decision Point (PDP)" göndərir. Bu cavab *XACML cavab dili ilə təsvir edilir, PEP-ə geri göndərilir və bununla da PEP, sorğu sahibinə giriş icazəsi verə və ya rədd edə bilir. Müəyyən edilmiş siyasəti almaq üçün "Policy Administration Point (PAP)"-dan istifadə edilir. PDP siyasətlərin yazıldığı və uyğun bir saxlancda saxlandığı PAP-i istifadə edir.



Şəkil 3. OASIS XACML emal mühiti

Multi-bulud sistemlərdə təhlükəsizliyin təmin edilməsi üçün bir neçə akademik araşdırma edilmişdir. Bu araşdırmaların nəticələrinə bundan sonrakı bölümdə baxılacaq.

VI. TƏHLÜKƏSİZLİK RİSKLƏRİNİN İDARƏ EDİLMƏSİNƏ YANAŞMALAR

Bulud saxlama yerindəki riski azaltmaq üçün müştərilərin buludda saxlanan məlumatlarını qorumaq üçün kriptoqrafik metodlardan istifadə edilir [3]. Heş funksiyası istifadə edərək lokal yaddaşa qısa bir heş almaq verilənlərin tamlığı üçün yaxşı bir həll metodudur. Bu şəkildə, serverlərin cavablarının autentikasiyası, lokal məlumatların saxlanması ilə müqayisə edilərək alınan məlumatın heşini yenidən hesablayaraq edilir . Əgər məlumatın həcmi böyükdürsə, bir heş agacı funksiyası həll yolu kimi seçilə bilər.

Cachin və qrupunun əvvəlki araşdırmalarında istifadəçinin məlumatlarını serverlər tərəfindən geri göndərilməsini doğrulamasına rəğmən, serverlərin bu sorğunu bilmədən cavablayacağını və məlumatların serverdə olub olmadığını, doğru formada saxlanıb-saxlanmadığını zəmanət verməməkdədir. Juels və Kaliski [4], Ateniese və qrupu [5] istifadəçilərin məlumatlarını geri qaytarılması üçün "Proofs of Retrievability (PORs)" və "Proofs of Data Possession (PDP)" protokollarını təqdim edirlər. Cachinet , bulud saxlanmasında məlumat tamlığını təmin edilməsi üçün və hər buludun tək nüxsəsini qoruyur. "Bizans xətaya dayanıqlı" (Byzantine-fault-tolerant) protokollarını çalışdırmaq üçün birdən çox bulud provayder istifadə etməyi tövsiyyə edilir [8]. Cachin bu yanaşmada yalnızca Amazon EC2-də təmin edilən bir xidmət kimi buludda saxlamanın, habelə "Byzantine Quorum Systems" [6] ilə "Byzantine Disk Paxos" [7] istifadə edərək tövsiyə etməkdədir. İstifadəçilərin atomik əməliyyatlarını təmin etmək və bir bulud xəta riskini ortadan qaldırmaq üçün en az dörd fərqli bulud istifadə edilir.

DEPSKY sistemində məlumatlar dörd kommersiya buludunda (Amazon S3, Windows Azure, Nirvanix və Rackspace) təkrarlanır. Məlumat tək bir bulud üzərindən keçirilmir (relay), bu səbəblə Kök bulud "vendor lock-in" probleminə səbəb olan problem önləmiş olur [9]. Bundan əlavə, DEPSKY sistemindəki hər bir buludun yarısı qədər məlumat saxlamaq, silinən kodları istifadə edilərək təmin edilir. Nəticə olaraq, bir provayderdən digərinə məlumat mübadiləsi daha az xərclə nəticələnir. DEPSKY sistemi tək bir bulud istifadəsi xərcinin 2 qatı olmaq üzərə dörd buludun (xərcin 4 qatı) istifadə xərcini azatmağı hədəfləyir. DEPSKY, sistemindəki oxuma və yazma əməliyyatlarını gerçəkləşdirmək üçün bir set Bizans nüvəsi sistemi protokolu istifadə edir bu səbəblədə, hər buludda əməliyyat aparmaq üçün 2 bağlantı gedişi edir. Bir neçə buludun istifadə edilməsi "Byzantine quorum systems" protokollarının ehtiyacı olan çeşidli lokasiyalar, idarəçilik, dizayn və tətbiq tələb edir. DepSky sistemində (saxlama buludu) serverlərdəki kodların çalışdırılması, bəzi kod icasına ehtiyac duyan digər Bizans protokollarının əksinə gərəkli deyildir [10]. Bu protokolları istifadəsindən sonra, DepSky sistemi hər buludda saxlanan məlumat miqdarını azaldaraq məlumat məxfiliyini qorumağı məqsədi güdür.

VII. MULTİ-BULUD SİSTEMLƏRİNDƏ MƏLUMAT BAZASI MODELİ

Multi-bulud məlumat bazası bulud texnologiyasında təhlükəsizliyi və gizliliyi təmin edir və multi-bulud xidmət provayderlərinə məxfi paylaşım alqoritmləri tətbiq edir. Bu mexanizmlər daha öncəki məlumat bazası təhlükəsizliyi araşdırmalarında istifadə edilmişdir [11]. Məlumat bazası istifadəçilərə video, şəkil vəya fayl kimi fərqli məlumat tipilərini saxlamaq üçün bir araya gətirmə, tam uyğun və aralıq sorğusu kimi fərqli məlumat bazası sorğuları olan istifadəçilərə icazə verən "Bulud məlumat bazası" təqdim edir. Təqdim edilən bu modelin məqsədi buludun içərisində bədniyyətlinin olması riskinin və bulud xidmətlərinin uğursuzluğunun qarşısını almaqdır.

C. Metodun analizi və tətbiqi

Senari. Bu modeldə VBİS (Verilənlər bazalarını idarəetmə sistemi) istifadəçinin etimad etmədiyi bulud provayderindən gizlətmək istədiyi məlumatı n paya və ya qrupa bölür.

DOI: 10.25045/NCSoftEng.2017.52

Məlumatları (məlumatların rəqəmsal verilənlər olduğu, məsələn, işçinin maaşı olduğu fərz edilir) 3 paya bölüb, bunları fərqli CSP-lərdə (Cryptographic Service Provider) saxladıqdan sonra, VBİS dərəcəsi ilə eyni səviyyədəki dərəcəylə WORKER cədvəlindəki funksiyanın sabit qismi olaraq gerçək maaş ilə hər işçinin maaşı üçün bir təsadüfi çoxhədli generasiya edir. Bu qiymətlər daha sonra fərqli CSP-də saxlanır. Bu ssenari üçün, n=3 və k=2 qiymətləri istifadə edilir. Bundan əlavə, VBİS gizli qiyməti yaratmaq üçün gizli məlumat olan X qiymətlərini (x1 = 3, x2 = 1, x3 = 2) istifadə edir. Maaşlar {1000, 2500, 2900, 3000 və 3200} üçün çoxhədli aşağıdakı kimi olacaqdır:

- Q1000 (x) = 100x +1000;
- Q2500 (x) = 5x +2500;
- Q2900 (x) = x +2900;
- Q3000 (x) = 2x +3000.

Çoxhədlilərdə x1 tətbiq edilərsə, 1000 maaşının dəyəri CSP1'də 1300, CSP2'də 1100 və CSP3-də 1200 olaraq tutulur. Bu vaxt, istifadəçinin sorğusu VBİS-ə gəlmiş olmalı və VBİS nəticələri CSP-dən əlaqəli payı almaq üçün sorğu yenidən yazılmalıdır. Daha sonra, VBİS, istifadəçiyə göndərmək üçün gizli qiyməti hesablayır. Rəqəmsal atribut məlumat növü gizli pay metodunda dəyərləndirilir.

NƏTİCƏ

Son saxlama modelindəki bir neçə payın təsirini analiz etmək üçün, statik məlumat həcmi 10 MB istifadə edilərək VBİS-də məlumat saxlamaq üçün test edildi. Şəkil 4-də göstərilən nəticələr məlumat saxlama prosedurunun zaman xərclərinin pay sayı ilə birlikdə artdığını göstərməkdədir. Zaman xərci artan sayıda pay ilə birlikdə artsa da, pay sayını artırmaq, etimadsız bulud provayderindən gələn məlumatların gizli dəyərinin təhlükəsizlik dərəcəsini artıracaqdır. Bunun səbəbi CSP-lərin daha çox, k məlumatların detallarını bilməsidir.

Şəkil 4. Məlumat saxlamanın zaman müqayisəsi (fərqli paylar)

Bulud texnologiyalarının fərdi və korparativ istifadəsinin artmasına baxmayaraq, bulud məlumat emalının təhlükəsizliyi, bulud texnologiyası mühitindəki ən böyük problem olaraq qəbul edilir. Müştərilər buluddakı bədniyyətli kontentlər səbəbilə özünəməxsus şəxsi məlumatları itirmək istəmirlər. Buna əlavə olaraq, xidmətin əlyetərliyinin pozulması son zamanlarda çox sayda müştərinin problemlə üzləşməsinə səbəb olur. Ayrıca, məlumat müdaxiləsi bulud texnologiysı istifadəçiləri üçün bir çox problemə yol açmaqdadır. Bu modelin və metodların tətbiqinin məqsədi Şamirin gizli məlumat paylaşımı alqoritminin tək bulud yerinə, multi-bulud provayderlərində istifadə edilməsidir. Bu modellərin və metodların məqsədi təhlükəsizlik risklərini azaltmaq və məlumat tamlığını, məlumat oğurluğu və xidmət əlyetərliyi ilə bağlı mövzuları özündə birləşdirir.

ƏDƏBİYYAT

[1] S.M. Habib, S. Ries, M. Muhlhauser, “Towards a trust management system for cloud computing,” Proc. of the IEEE 10th International Conference on.Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 933–939, 2011.

[2] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, “Internet X. 509 public key infrastructure certificate policy and certification practices framework.” 2003.

[3] A. Shraer, C. Cachin, A, Cidon, I. Keidar, Y. Michalevsky, D. Shaket, “Venus: Verification for untrusted cloud storage,” Proc. of the ACM Workshop on Cloud Computing Security. pp. 19–30, 2010.

[4] A. Juels, B.S. Kaliski (Jr), “PORs: Proofs of retrievability for large files,” Proceedings of the 14th ACM Conference on Computer and Communications Security, pp. 584–597, 2007..

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, “Provable data possession at untrusted stores,” Proc. of the 14th ACM Conference on Computer and Communications Security, pp. 598–609, 2007.

[6] D. Malkhi, M. Reiter, “Byzantine quorum systems,” Distributed Computing, Vol. 11, No. 4, pp. 203–213, 1998.

[7] I. Abraham, G. Chockler, I. Keidar, D. Malkhi, “Byzantine disk paxos: optimal resilience with byzantine shared memory,” Distributed Computing, Vol. 18, No. 5, pp. 387–408, 2006.

[8] P. Ramadevi, N. Siddaiah, “Cloud Computing protection for outsourced record in Cloud Computing,” International Journal of Innovative Technologies, Vol. 4, Issue 8, pp. 1303-1306, 2016.

[9] H. Abu-Libdeh, L. Princehouse, H. Weatherspoon, “RACS: a case for cloud storage diversity,” Proc. of the 1st ACM Symposium on Cloud Computing, pp. 229–240, 2010.

[10] C. Cachin, S. Tessaro, “Optimal resilience for erasure-coded Byzantine distributed storage,” International Conference on Dependable Systems and Networks (DSN), pp. 115–124, 2006.

[11] D. Agrawal, A.E. Abbadi, F. Emekci, A. Metwally, “Database management as a service: Challenges and opportunities,” IEEE 25th International Conference on Data Engineering (ICDE'09), pp. 1709–1716, 2009.

[12] R. Sinnema, E. Wilde, “RFC 7061: eXtensible Access Control Markup Language (XACML) XML Media Type.” 2013.

DOI: 10.25045/NCSoftEng.2017.52