Bulud Sistemlərində Kiberkriminalistika Yanaşması ilə Kibercinayətlərin Aşkarlanması Modeli

Rəşid Ələkbərov[1], Oqtay Ələkbərov[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*rashid.alakberov@gmail.com*, [2]*oqtayalakbarov@yahoo.com*

Xülasə — **Müasir informasiya texnologiyalarının inkişafı bulud hesablama sistemlərinin geniş yayılmasına səbəb olmuşdur. Bulud texnologiyaları məlumatların saxlanılması, emalı və paylaşılması üçün effektiv və çevik imkanlar yaradır. Lakin bu texnologiyaların geniş tətbiqi kibercinayətkarlıq risklərinin də artmasına gətirib çıxarmışdır. Bulud mühitində məlumatların uzaq serverlərdə saxlanılması və çoxsaylı istifadəçilər tərəfindən istifadə olunması təhlükəsizlik baxımından yeni problemlər yaradır. Məqalədə bulud sistemlərində kibercinayətkarlıq fəaliyyətinin xüsusiyyətləri, təhlükəsizlik problemləri və rəqəmsal kriminalistika metodları araşdırılır. Eyni zamanda bulud kriminalistikasının əsas mərhələləri, sübutların toplanması üsulları və kibercinayətlərin araşdırılmasında istifadə oluna biləcək metod təklif edilmişdir.**

Açar sözlər — ***bulud texnologiyaları, kibercinayətkarlıq, rəqəmsal kriminalistika, bulud kriminalistikası, kibertəhlükəsizlik.***

I. GİRİŞ

Bulud texnologiyaları istifadəçilərə məlumatları uzaq serverlərdə saxlamağa, müxtəlif proqram təminatından internet vasitəsilə istifadə etməyə və hesablama resurslarını daha səmərəli şəkildə idarə etməyə imkan verir. Lakin bu üstünlüklərlə yanaşı, bulud mühitində məlumatların uzaq serverlərdə saxlanılması və çoxsaylı istifadəçilər tərəfindən paylaşılması kibertəhlükəsizlik baxımından yeni risklər yaradır. Xüsusilə məlumatların mərkəzləşdirilmiş şəkildə saxlanılması və şəbəkə üzərindən idarə olunması kibercinayətkarlar üçün bu sistemlərə hücum etmək baxımından geniş imkanlar açır.

Müasir dövrdə dövlət qurumları, özəl şirkətlər və fərdi istifadəçilər böyük həcmdə məlumatları bulud platformalarında saxlayırlar. Bu isə kibercinayətkarlıq hallarının artmasına və məlumat sızması kimi təhlükələrin daha geniş yayılmasına səbəb olmuşdur. Son illərdə baş verən kibertəhlükəsizlik insidentləri göstərir ki, bulud mühitində təhlükəsizlik problemləri yalnız texniki deyil, həm də ciddi iqtisadi və hüquqi nəticələrə səbəb ola bilər. Eyni zamanda, bulud sistemlərində məlumatların paylanmış struktura malik olması və müxtəlif coğrafi regionlarda yerləşməsi kibercinayətlərin araşdırılmasını daha mürəkkəb edir. Bu mühitdə rəqəmsal sübutların toplanması, qorunması və analiz edilməsi xüsusi yanaşmalar tələb edir. Bu baxımdan, bulud sistemlərində kibercinayətkarlıq fəaliyyətinin araşdırılması və rəqəmsal kriminalistika metodlarının inkişaf etdirilməsi müasir kibertəhlükəsizlik sahəsində həm elmi, həm də praktiki baxımdan aktual və vacib hesab olunur.

II. ƏLAQƏLİ İŞLƏR

Məqalə [1] də bulud kriminalistikasında rast gəlinən əsas texniki problemlər, xüsusilə multi-tenant mühitdə sübutların ayrılması, məlumatların yerləşdiyi yurisdiksiyaların müxtəlifliyi və bulud provayderlərindən asılılıq kimi məsələlər təhlil edilmiş və mövcud həllər müqayisəli şəkildə qiymətləndirilmişdir.

Məqalə [2] də bulud kriminalistikasının mövcud problemləri, sübutların əldə olunması çətinlikləri, serverlərin fiziki müsadirəsinin mümkün olmaması və hüquqi məhdudiyyətlər sistemli şəkildə analiz edilmiş və açıq tədqiqat problemləri müəyyən edilmişdir. Məqalə [3] də bulud mühitində kibercinayətlərin araşdırılması üçün etibarlı üçüncü tərəf (TTP) modelinə əsaslanan forensik çərçivə təqdim edilmiş və sübutların hüquqi etibarlılığının təmin olunması məsələləri araşdırılmışdır. Tədqiqat [4] də bulud sistemlərində DDoS hücumlarının araşdırılması üçün forensik çərçivə hazırlanmış, sübutların toplanması və xidmət provayderlərindən asılılığın azaldılması yolları təklif edilmişdir. Məqalə [5] də bulud kriminalistikasının metodologiyası, istifadə olunan forensik alətlər və bu sahənin gələcək inkişaf istiqamətləri geniş şəkildə təhlil edilmişdir. Bu işdə [6] da bulud mühitində kibercinayət ssenariləri, hücum mənbəyinin müəyyən edilməsi üsulları və effektiv istintaq modellərinin qurulması məsələləri araşdırılmışdır. Məqalə [7] də süni intellekt və maşın öyrənməsi metodlarının bulud kriminalistikasında anomaliyaların aşkarlanması və sübutların avtomatlaşdırılmış analizi üçün tətbiqi araşdırılmışdır. Tədqiqat [8] də bulud və IoT mühitində rəqəmsal sübutların toplanması, API əsaslı məlumat əldə etmə və müasir kriminalistik yanaşmaları araşdırılır. Bu işdə [9] da bulud yaddaş xidmətlərində saxlanılan məlumatların, sinxronizasiya artefaktlarının və loq fayllarının kriminalistik analiz üsulları təqdim edilmişdir.

III. BULUD SİSTEMLƏRİNDƏ KİBERCİNAYƏTKARLIQ PROBLEMLƏRİ

Bulud texnologiyalarının geniş tətbiqi ilə yanaşı kibercinayətkarlıq fəaliyyətinin artması bu mühitdə bir sıra ciddi problemlərin yaranmasına səbəb olmuşdur. Bulud sistemlərinin paylanmış strukturu, çoxistifadəçili mühiti və uzaqdan idarə olunması təhlükəsizlik baxımından əlavə risklər yaradır. Bu problemlər həm texniki, həm də hüquqi aspektləri əhatə edir və kibercinayətlərin aşkar olunmasını və araşdırılmasını çətinləşdirir. Bulud sistemlərində kibercinayətkarlığında meydana çıxan problemlər aşağıda göstərilmişdir:

- Məlumatların məxfiliyi və təhlükəsizliyi-Bulud sistemlərində məlumatlar uzaq serverlərdə saxlanıldığı üçün icazəsiz giriş və məlumat sızması riski artır. Zəif şifrələmə və təhlükəsizlik mexanizmləri bu riski daha

DOI: 10.25045/forensic.gov.2026.15

da gücləndirir.

- Autentifikasiya və giriş nəzarəti problemləri - Zəif parollar və çoxfaktorlu autentifikasiyanın olmaması kibercinayətkarların sistemə daxil olmasını asanlaşdırır. Bu da istifadəçi hesablarının ələ keçirilməsi ilə nəticələnə bilər.
- Paylanmış arxitektura və hüquqi problemləri-Məlumatların müxtəlif ölkələrdə yerləşməsi hüquqi çətinliklər yaradır. Bu vəziyyət kibercinayətlərin araşdırılmasını və hüquqi məsuliyyətin müəyyən edilməsini çətinləşdirir.
- Rəqəmsal sübutların toplanması və qorunması-Bulud mühitində məlumatların tez dəyişməsi və silinməsi sübutların toplanmasını çətinləşdirir. Fiziki çıxışın olmaması kriminalistik araşdırmaları daha mürəkkəb edir.
- Çoxistifadəçi (Multi-tenant) mühitində təhlükəsizlik riskləri-Eyni infrastrukturun bir neçə istifadəçi tərəfindən paylaşılması məlumat sızması riskini artırır. Sistem zəifliklərı digər istifadəçilərin məlumatlarına çıxışa səbəb ola bilər.
- Kibercinayətlərin aşkarlanmasının çətinliyi-Böyük həcmli məlumatlar içərisində şübhəli fəaliyyətlərin aşkar edilməsi çətindir. Bu səbəbdən avtomatlaşdırılmış analiz və anomaliya aşkarlama metodlarından istifadə olunur

Bu problemlərin həlli məqsədilə müasir təhlükəsizlik texnologiyaları və rəqəmsal kriminalistika metodlarından geniş şəkildə istifadə olunur.

Rəqəmsal kriminalistika informasiya sistemlərində baş verən cinayət hadisələrinin araşdırılması üçün istifadə olunan metod və texnologiyaların məcmusudur. Bu sahənin əsas məqsədi rəqəmsal sübutların toplanması və analiz edilməsidir.

Rəqəmsal kriminalistika aşağıdakı mərhələlərdən ibarətdir:

- hadisənin aşkar edilməsi
- sübutların toplanması
- sübutların qorunması
- analiz
- nəticələrin sənədləşdirilməsi
- qərarın verilməsi

Bulud kriminalistikası bulud mühitində baş verən kibercinayətlərin aşkar edilməsi, araşdırılması və rəqəmsal sübutların toplanması ilə məşğul olan rəqəmsal kriminalistikanın bir sahəsidir. Bulud texnologiyalarının geniş tətbiqi nəticəsində məlumatların böyük hissəsi uzaq serverlərdə saxlanılır və bu da kibercinayətlərin araşdırılmasını daha mürəkkəb edir. Bu kontekstdə bulud kriminalistikası hadisələrin səbəbini müəyyən etmək, hücumların izlərini izləmək və sübutları sistemli şəkildə analiz etmək üçün istifadə olunur.Bulud kriminalistikası çərçivəsində şübhəli fəaliyyətlərin aşkarlanması loq fayllarının analizi, şəbəkə trafikinin monitorinqi, istifadəçi davranışlarının qiymətləndirilməsi, rəqəmsal sübutların toplanması və qorunması, həmçinin virtual maşın və yaddaş kriminalistikası kimi metodların tətbiqi əsasında həyata keçirilir.

Bulud kriminalistikası vasitəsilə şübhəli fəaliyyətlərin müəyyən edilməsi:

- Loq fayllarının analizi - Bulud mühitində baş verən əməliyyatlar loq fayllarında qeyd olunur. Bu loglar vasitəsilə istifadəçi girişləri, sistem fəaliyyətləri və şübhəli əməliyyatlar araşdırılır.
- Şəbəkə trafikinin monitorinqi - Şəbəkə üzərindən ötürülən məlumatlar analiz edilərək qeyri-adi trafik axını, şübhəli əlaqələr və potensial hücumlar müəyyən edilir.
- İstifadəçi davranışlarının analizi - İstifadəçi fəaliyyətləri izlənilir və normal davranışdan kənara çıxan hallar anomaliya kimi qiymətləndirilərək şübhəli fəaliyyətlərin aşkarlanmasına imkan verir.
- Rəqəmsal sübutların toplanması - Şübhəli fəaliyyətlərlə əlaqəli loglar, fayllar və digər rəqəmsal məlumatlar toplanır və sübut kimi analiz olunur.
- Sübutların qorunması və təhlili - Toplanan rəqəmsal sübutlar dəyişdirilmədən saxlanılır və kriminalistik metodlarla analiz edilərək hadisənin mahiyyəti və səbəbləri müəyyən edilir.
- Virtual maşınların analizi - Bulud mühitində istifadə olunan virtual maşınlar (VM) araşdırılaraq onların disk görüntüləri, konfiqurasiyası və fəaliyyət tarixçəsi analiz edilir. Bu, hücumun izlərini və sistemə müdaxilə üsullarını müəyyən etməyə kömək edir.
- Yaddaş kriminalistikası - Virtual maşınların operativ yaddaşı (RAM) analiz edilərək aktiv proseslər, işləyən proqramlar və müvəqqəti məlumatlar araşdırılır. Bu yanaşma xüsusilə silinmiş və ya diskdə saxlanılmayan məlumatların bərpası üçün istifadə olunur.

IV. BULUD MÜHİTİNDƏ KİBERCİNAYƏTLƏRİN AŞKARLANMASI MODELİ

Bulud mühitində yerləşən informasiya sistemində istifadəçi hesabı vasitəsilə icazəsiz giriş və məlumatların oğurlanması və ya silinməsi hadisəsi qeydə alınmışdır. İstifadəçi bu əməliyyatları yerinə yetirmədiyini bildirir və hadisənin hansı üsulla həyata keçirildiyi, sistemə girişin necə əldə edildiyi və əməliyyatların hansı subyekt tərəfindən (qanuni istifadəçi, administrator və ya kənar hücumçu) icra olunduğu ilkin mərhələdə məlum deyil.

Kiberkriminalistikanın əsas məqsədi mövcud rəqəmsal sübutlar əsasında hadisənin baş vermə mexanizmini rekonstruksiya etmək, hücumun xronologiyasını qurmaq və fəaliyyətin real icraçısını müəyyən etməkdir. Bu məqsədlə sistemdə saxlanılan müxtəlif mənbələrdən əldə edilən məlumatlar kompleks şəkildə təhlil olunur. Autentifikasiya və giriş loqları istifadəçi hesabına hansı zaman intervalında və hansı üsulla daxil olunduğunu müəyyən etməyə imkan verir. IP ünvanları və şəbəkə məlumatları sistemə qoşulan mənbələrin coğrafi və texniki mənşəyini müəyyən etmək üçün istifadə olunur.İstifadəçi fəaliyyətləri və davranış göstəriciləri adi istifadə modelindən kənara çıxan davranışların, yəni istifadəçinin normal fəaliyyətindən fərqlənən anomaliyaların aşkarlanmasına kömək edir Sistem daxilində icra olunmuş əməliyyatların analizi isə hansı məlumatların əldə edildiyini,

dəyişdirildiyini və ya silindiyini müəyyən etməyə imkan yaradır. Toplanmış bu göstəricilər riyazi modeldə çoxölçülü müşahidə vektoru kimi təqdim olunur və normal davranış profili ilə müqayisə edilir. Müqayisə nəticəsində hadisənin anomaliya olub-olmaması qiymətləndirilir, hücumun mümkün mexanizmi müəyyən edilir və fəaliyyətin ehtimal olunan icraçısı barədə əsaslandırılmış qərar verilir. Beləliklə, təklif edilən model rəqəmsal sübutların sistemli analizinə, hadisənin tam mənzərəsinin bərpasına və gələcəkdə oxşar hücumların qarşısının alınmasına xidmət edir.

Modeldə anomaliyanın qiymətləndirilməsi üçün aşağıdakı əsas göstəricilər müəyyən edilib:

- A — uğursuz giriş cəhdlərinin intensivliyi(sayı).
- B — giriş mənbələrinin (müxtəlif IP ünvanlarının sayı) qeyri-adiliyi.
- C — istifadəçi davranışında anomaliyalar.
- D — sistem daxilində şübhəli əməliyyatlar.

w1, w2, w3, w4 — hər göstəricinin əhəmiyyətini ifadə edən çəkilər.

Bulud mühitində kiberkriminalistika məqsədilə istifadəçi fəaliyyətlərinin statistik təhlilinə əsaslanan qərarvermə modeli.

4.1. Parametrlərin (göstəricilərin) 0–1 intervalında normallaşdırılması

Bu müxtəlif göstəricilərin müqayisə oluna bilməsi və vahid skorda birləşdirilməsi üçün bütün parametrlər 0–1 intervalına normallaşdırılır. Bunun üçün min–max normallaşdırma üsulundan istifadə edilir:

$$x_i^{norm}(k) = (x_i(k) - x_i^{min}) / (x_i^{max} - x_i^{min}), \quad i \in \{A, B, C, D\}, \quad k=1,\ldots,n$$

Burada *i* göstəricinin indeksidir, yəni A, B, C və D parametrlərindən hansı üçün hesablamanın aparıldığını göstərir. *k* müşahidənin və ya zaman intervalının indeksidir, yəni vektorda *k*-ci müşahidə nöqtəsi üçün normallaşdırılmış qiyməti göstərir. Burada x_i (k)göstəricinin cari qiymətini (real ölçü), x_i^{min} və x_i^{max} isə müvafiq göstəricinin müşahidə olunan minimal və maksimal qiymətlərini ifadə edir, normallaşdırmadan sonra bütün parametrlər [0,1] intervalına gətirilir və modeldə müqayisə edilə bilən vahid ölçü şkalasında istifadə olunur.

4.2. Modeldə istifadə olunan göstəricilər vektoru. Bu vektor normallaşdırılmış parametrlər əsasında belə yazıla bilər:

$$X^{(k)} = (A^{(k)}, B^{(k)}, C^{(k)}, D^{(k)}), \quad k=1,\ldots,n$$

Beləliklə, bütün göstəricilər vahid şkalaya gətirilmiş olur və modeldə müqayisə edilə bilən formada istifadə olunur.

4.3. Normal davranışın formalaşması. *n* sayda normal müşahidə götürülür və aşağıdakı şəkildə təqdim edilir:

$$X^{(1)}, X^{(2)}, \ldots, X^{(n)}$$

Hər bir $X^{(k)}$ vektoru sistemin normal davranışını xarakterizə edən göstəriciləri əks etdiri

4.4. Hər bir göstərici (A, B, C, D) üzrə orta qiymət normal müşahidələr əsasında hesablanır:

$$\mu_i = \frac{1}{n}\sum_{k=1}^{n} x_i^{(k)}, \quad i \in \{A,B,C,D\}$$

Hər bir göstərici üzrə orta qiymət normal müşahidələr əsasında hesablanır.

4.5. Hər bir göstərici (A, B, C, D) üzrə dispersiya və standart kənarlaşma normal müşahidələr əsasında hesablanır:

Dispersiya:

$$\sigma^2_i = \frac{1}{n}\sum_{k=1}^{n} (x_i^{(k)} - \mu_i)^2, \quad i \in \{A,B,C,D\}$$

Standart kənarlaşma:

$$\sigma_i = \sqrt{\sigma_i^2}, \quad i \in \{A,B,C,D\}$$

4.6. Çəkilərin hesablanması. Hər bir parametrin təsir dərəcəsini müəyyən et mək üçün çəkilər istifadə olunur.

$$w_i = (1/\sigma_i) / \sum_{i=1}^{4} \frac{1}{\sigma i}, \text{ hardakı } , \sum_{i=1}^{4} w_i = 1$$

4.7. Normal müşahidələrin qiymətinin hesablanması. hər bir müşahidə üçün bütün göstəricilər çəkilər əsasında hesablanır

$$S_k = \sum_{i=1}^{4} w_i \cdot x_i^{(k)}$$

4.8. Normal müşahidələrin qiymətlərinin statistikası. Orta (μR) və standart (σR) kənarlaşmanin hesablanması:

$$\mu_R = \frac{1}{n}\sum_{k=1}^{n} S_k,$$

$$\sigma_R = \sqrt{\frac{1}{n}\sum_{k=1}^{n} (S_k - \mu_R)2}$$

4.9. Həddnormal davranışın statistikasına əsaslanaraq müəyyən edilir və hadisənin anomaliya olub-olmadığını qiymətləndirməyə imkan verir:

Anomaliyaların aşkar edilməsi üçün həddqiyməti müəyyən edilir.

$$S_{th} = \mu_R + s * \sigma_R, \quad k \in [2,3]$$

burada, μ_R və σ_R — normal müşahidələrin orta və standart kənarlaşmasıdır. s isə statistik təcrübəyə əsasən seçilən əmsaldır və adətən 2–3 intervalında götürülür: s=2 olduqda model daha həssas olur və daha çox anomaliya aşkarlaya bilir, s=3 olduqda isə meyar daha sərt olur və yalnız əhəmiyyətli anomaliyalar seçilir.

4.10. Hadisə vektoru. Hadisə baş verib və onun qiymətləndirilməsi. Hadisə baş verdikdə, onun göstəriciləri normal davranışın formalaşdırılması qaydası ilə qiymətləndirilir (S_{event}) və əldə olunan nəticə normal davranışın şablon qiyməti (Sth) ilə müqayisə edilir.

$$X^{event} = (A', B', C', D')$$

burada, A′,B′,C′,D′ — hadisə zamanı müşahidə olunan normallaşdırılmış göstəricilərdir.

4.11. Hadisənin qiyməti (S_{event}) bütün göstəricilər üzrə çəkilər tətbiq edilməklə hesablanır və hadisənin normal

davranışdan nə qədər fərqləndiyini ölçmək üçün istifadə olunur: Hadisə vektoru, normal davranış vektoru X(k) ilə müqayisə edilərək anomaliyaların aşkarlanmasında istifadə olunur.

$$S_{event} = \sum_{i=1}^{4} w_i \cdot x_i^{event}$$

4.12. Hesablanmış hadisə qiyməti (S_{event}) normal davranış üçün müəyyən edilmiş normal həddi qiyməti (Sth) ilə müqayisə edilərək hadisənin tipi müəyyən olunur.Hadisənin qiyməti (Sevent) bütün göstəricilər üzrə çəkilər tətbiq edilməklə hesablanır və hadisənin normal davranışdan nə qədər fərqləndiyini ölçmək üçün istifadə olunur:

Hesablanmış qiymətləndirmə əsasında hadisənin tipi müəyyən olunur.

$$S_{event} \geq S_{th} \Rightarrow \text{Anomaliya}$$
$$S_{event} < S_{th} \Rightarrow \text{Normal}$$

Anomaliya təsdiqləndikdən sonra hadisənin icraçısını müəyyən etmək üçün müşahidə olunan göstəricilər istifadəçinin normal davranış profili ilə müqayisə edilir. Hadisə zamanı hesablanmış S_{event} qiyməti ilə S_{th} həddi müqayisə olunur:

$| S_{event} - \mu_R | \leq S_{th} \Rightarrow$hadisə istifadəçi tərəfindən törədilib,

$| S_{event} - \mu_R | > S_{th}$ h⇒hadisə kənar hucümçu (haker) tərəfindən törədilib

Beləliklə, model həm anomaliyanın mövcudluğunu, həm də hadisənin ehtimal olunan icraçısını sistemli şəkildə müəyyən etməyə imkan verir.

Təklif edilən riyazi modelin əsas məqsədi hadisənin yalnız normal və ya anomaliya olmasını müəyyən etmək deyil, artıq baş vermiş anomaliya əsasında hadisənin real icraçısını müəyyənləşdirməkdir. Alınmış nəticələr (giriş cəhdləri, IP mənbələrinin qeyri-adiliyi, istifadəçi davranışındakı əmsallar (sapmalar), sistem daxilində icra olunan əməliyyatlar və s.) kiberkriminalist tərəfindən təhlil olunur və istintaq prosesində düzgün interpretasiya edilərək hadisənin normal və ya anomaliya olduğu müəyyənləşdirilir. Model istifadəçinin normal davranışı ilə hadisə zamanı müşahidə olunan davranış arasındakı fərqi ölçməklə hadisənin istifadəçi tərəfindən, yoxsa kənar şəxs (haker) tərəfindən törədildiyi barədə qərarın qəbuluna kömək edir.

NƏTİCƏ

Təklif edilən riyazi model bulud mühitində kibercinayətlərin aşkarlanması üçün istifadəçi fəaliyyətinin statistik təhlilinə əsaslanan anomaliya aşkarlama yanaşmasıdır. Model normallaşdırılmış parametrlər və çəkilər vasitəsilə istifadəçi davranışının normal profilini müəyyən edir və hadisələr zamanı müşahidə olunan göstəriciləri müqayisə edərək icazəsiz girişləri, potensial hücumları və qeyri-adi fəaliyyətləri aşkar etməyə imkan verir. Aparılan tədqiqat göstərir ki, bu yanaşma müxtəlif göstəricilərin normallaşdırılması, çəkilərin hesablanması və hədd qiymətinin müəyyən edilməsi əsasında hadisələrin avtomatlaşdırılmış şəkildə normal və ya anomaliya kimi qiymətləndirilməsini effektiv şəkildə həyata keçirir. Əldə olunan nəticələrin kiberkriminalist tərəfindən interpretasiyası hadisənin istifadəçi fəaliyyəti və ya kənar müdaxilə ilə bağlı olub-olmamasını, həmçinin kibercinayətlərin potensial subyektlərini müəyyənləşdirməyə imkan verir.

ƏDƏBİYYAT

[1] G. Grispos, T. Storer, and W. B. Glisson, "Cloud forensics: Technical challenges, solutions and comparative analysis," Digital Investigation, vol. 13, pp. 38–57, Jun. 2015.

[2] S. Zawoad and R. Hasan, "Cloud forensics: A meta-study of challenges, approaches, and open problems," IEEE Security & Privacy, vol. 11, no. 6, pp. 35–43, 2013.

[3] S. K. A. Manoj and L. Bhaskari, "Cloud forensics – A framework for investigating cyber attacks in cloud environment," Procedia Computer Science, vol. 85, pp. 149–154, 2016.

[4] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," Computers & Electrical Engineering, vol. 60, pp. 193–205, May 2017.

[5] B. Cinar and J. P. Bharadiya, "Cloud computing forensics: Challenges and future perspectives," Asian Journal of Research in Computer Science, vol. 16, no. 1, pp. 37–42, 2023.

[6] S. S. Akter and M. S. Rahman, "Cloud forensic: Issues, challenges and solution models," arXiv preprint arXiv:2303.06313, 2023.

[7] M. T. P. Mukti and N. Hanif, "Artificial intelligence in cloud forensics: Automating evidence acquisition and anomaly detection in distributed environments," FORSEC: Forensics & Security Journal, vol. 1, no. 1, pp. 26–33, 2024, DOI: 10.55677/forsec.v1i1.3.

[8] M. D. Prakasiwi, "Cloud and IoT forensics for strengthening cybercrime investigation: Acquisition challenges and analytical frameworks," FORSEC: Forensics & Security Journal, vol. 1, no. 1, pp. 9–17, 2024,

[9] Y.-Y. Teing, A. Dehghantanha, and K.-K. R. Choo, "CloudMe forensics: A case of big-data investigation," Future Generation Computer Systems, vol. 79, pp. 950–961, Feb. 2018, DOI: 10.1016/j.future.2017.02.038.

A Model for Detecting Cybercrimes in Cloud Systems Using a Cyberforensics Approach

Rashid Alakbarov[1], Ogtay Alakbarov[2]

[1,2]Institute of Information Technology, Baku, Azerbaijan

[1]rashid.alakberov@gmail.com, [2]oqtayalakbarov@yahoo.com

Abstract- The development of modern information technologies has led to the widespread adoption of cloud computing systems. Cloud technologies provide efficient and flexible capabilities for data storage, processing, and sharing. However, the extensive use of these technologies has also increased the risks of cybercrime. The storage of data on remote servers and its use by multiple users in cloud environments introduce new security challenges. This article examines the characteristics of cybercriminal activities in cloud systems, associated security issues, and digital forensic methods. At the same time, the main stages of cloud forensics, methods of evidence collection, and an approach used in the investigation of cybercrimes are proposed.

Keywords- cloud technologies; cybercrime; digital forensics; cloud forensics; cybersecurity.