Bulud Hesablama Mühitində Ağıllı Nəqliyyat Sistemlərinin Kibertəhlükəsizliyi Problemləri və Həlli Yolları

Rəşid Ələkbərov[1], Məmməd Həmidov[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*rashid.alakberov@gmail.com*, [2]*hemidov8326@gmail.com*

***Xülasə*— Ağıllı nəqliyyat sistemləri müasir şəhərlərdə nəqliyyat axınlarının optimallaşdırılması, yol təhlükəsizliyinin artırılması və infrastrukturun səmərəli idarə olunması baxımından mühüm rol oynayır. Bu sistemlər müxtəlif sensorlar, IoT qurğuları və şəbəkə texnologiyaları vasitəsilə böyük həcmli məlumat toplayaraq toplanmış məlumatların saxlanılması və emalı üçün bulud hesablama mühitindən istifadə edir. Lakin bulud əsaslı arxitektura məlumatların məxfiliyi, bütövlüyü və əlçatanlığı ilə bağlı ciddi kibertəhlükəsizlik riskləri yaradır. Məqalədə bulud mühitində fəaliyyət göstərən ANS üçün konseptual model təqdim olunur, əsas kibertəhlükəsizlik problemləri təhlil olunur və onların aradan qaldırılması üçün müasir metod və yanaşmalar təklif olunur.**

Açar sözlər*— *ağıllı nəqliyyat sistemləri; bulud hesablama; kibertəhlükəsizlik; əşyaların interneti; məlumat təhlükəsizliyi.

I. GIRIŞ

Ağıllı nəqliyyat sistemləri (ANS) müasir şəhərlərdə nəqliyyat axınlarını real-vaxt rejimində izləməyə, yol-nəqliyyat hadisələrini azaltmağa və infrastrukturun səmərəli idarə olunmasına imkan verir. Bu sistemlər sensorlar, IoT qurğuları, V2X kommunikasiya texnologiyaları və bulud hesablama platformaları vasitəsilə böyük həcmli məlumatları toplayır, emal edir və nəqliyyatın idarə olunmasına dair qərarların qəbulunu dəstəkləyir. Lakin bu üstünlüklərlə yanaşı, ANS-in bulud əsaslı arxitekturada fəaliyyət göstərməsi və məlumatların şəbəkə üzərindən ötürülməsi kibertəhlükəsizlik baxımından yeni risklər yaradır. Xüsusilə məlumatların mərkəzləşdirilmiş şəkildə saxlanılması və IoT cihazlarının zəif təhlükəsizlik mexanizmlərinə malik olması kibercinayətkarların bu sistemlərə hücum imkanlarını artırır.

Müasir dövrdə dünyanın bir çox ölkəsində dövlət qurumları və özəl şirkətlər ağıllı şəhər layihələri çərçivəsində ANS-i geniş tətbiq edir və bu sistemlər vasitəsilə böyük həcmdə məlumat toplanır. Bu isə nəqliyyat infrastrukturuna yönəlmiş kiberhücumların artmasına və məlumat bütövlüyünün pozulması kimi təhlükələrin daha geniş yayılmasına səbəb olmuşdur. Son illərdə qeydə alınmış kibertəhlükəsizlik insidentləri göstərir ki, ANS-də təhlükəsizlik problemləri yalnız texniki deyil, həm də ictimai təhlükəsizlik və iqtisadi nəticələrə səbəb ola bilər [1]. Eyni zamanda, bulud əsaslı ANS-in çoxsəviyyəli struktura malik olması və müxtəlif komponentlərin paylanmış şəkildə işləməsi təhlükəsizlik risklərinin aşkarlanmasını daha mürəkkəb edir. Bu mühitdə şəbəkə trafikində anomaliyaların aşkarlanması, məlumatların qorunması və hücumların qarşısının alınması xüsusi yanaşmalar tələb edir. Bu baxımdan, bulud əsaslı ANS-də kibertəhlükəsizlik risklərinin aşkarlanması modelinin işlənib hazırlanması müasir kibertəhlükəsizlik sahəsində həm elmi, həm də praktiki baxımdan aktual və vacib istiqamətlərdən biri hesab olunur.

II. ƏLAQƏLI İŞLƏR

Ağıllı nəqliyyat sistemləri üçün süni intellekt əsaslı təhlükəsiz IoT çərçivəsi təqdim edilmiş, avtentifikasiya və nəqliyyat idarəetmə proseslərinin vahid strukturda birləşdirilməsi tədqiq olunmuşdur [2].

Bulud mühitinə əsaslanan xarici hücumların aşkarlanması üçün təsadüfi meşə alqoritmi və əlamət mühəndisliyi birləşdirərək yüksək dəqiqlikli müdaxilə aşkarlama modeli işlənmişdir [3]. Proqramla müəyyən edilmiş şəbəkə (SDN) mühitində DDoS hücumlarının kənar hesablama ilə birgə dərin öyrənmə metodları vasitəsilə erkən aşkarlanması və qarşısının alınması üçün hibrid yanaşma təklif edilmişdir [4].

Ağıllı şəhərlərdə kiberhücumlara, xüsusilə zərərli proqram hücumlarına qarşı müdafiə üçün avtonom nəqliyyat vasitələrinin kibertəhlükəsizliyinə dair hərtərəfli araşdırma aparılmış, effektiv həll yolları müzakirə edilmişdir [5]. Ağıllı nəqliyyat sistemlərinin idarəetməsində məlumat bütövlüyünü təmin etmək üçün blokçeyn texnologiyasından istifadə imkanları, o cümlədən tətbiqetmə problemləri və perspektivlər sistemli şəkildə araşdırılmışdır [6].

Müstəqil nəqliyyat vasitələri üçün mərkəzləşdirilməmiş məlumat bütövlüyü protokolunun blokçeyn əsasında qurulması təklif edilmiş, belə protokolun kibercinayətlərin qarşısının alınmasındakı rolu nümayiş etdirilmişdir [7].

Kooperativ adaptiv sürücülük idarəetməsinin təhlükəsizliyinin blokçeyn inteqrasiyalı çoxagentli dərin gücləndirilmiş öyrənmə ilə yüksəldilməsi üçün innovativ yanaşma işlənib hazırlanmışdır [8].

III. BULUD HESABLAMA MÜHITINDƏ AĞILLI NƏQLIYYAT SISTEMLƏRININ KONSEPTUAL MODELI

Bulud hesablama mühitində ağıllı nəqliyyat sistemlərinin konseptual modeli, məlumat toplama, şəbəkə və kommunikasiya, həmçinin bulud emalı və qərarvermə

DOI: 10.25045/forensic.gov.2026.53

səviyyələrindən ibarət üçqatlı strukturda sistemin iş prinsiplərini və kibertəhlükəsizlik aspektlərini əhatə edir [9].

A. IoT və kənar hesablama qatında məlumat toplanması

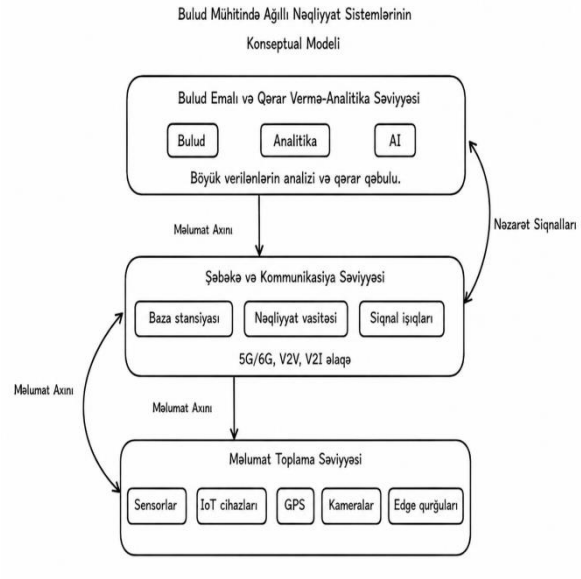
Ağıllı nəqliyyat sistemlərinin fəaliyyətinin başlanğıc nöqtəsi məlumat toplama səviyyəsidir. Bu səviyyə real fiziki mühitdə yerləşən sensorlar, kameralar, GPS modulları, radar və digər IoT qurğuları vasitəsilə yol və nəqliyyat haqqında məlumatların fasiləsiz şəkildə toplanmasını təmin edir. Yol infrastrukturu üzərində quraşdırılmış sensorlar nəqliyyat sıxlığı, avtomobillərin sürəti, hava şəraiti və yolun vəziyyəti kimi göstəriciləri ölçür. Eyni zamanda nəqliyyat vasitələrinin özündə yerləşən cihazlar avtomobilin hərəkəti, mövqeyi və texniki vəziyyəti barədə telemetriya məlumatlarını ötürür. Bu səviyyədə məlumatlar ilkin olaraq kənar hesablama (Edge Computing) texnologiyası vasitəsilə lokal şəkildə emal edilir. Kənar hesablama texnologiyasının əsas məqsədi böyük həcmli xam məlumatların bilavasitə bulud serverlərinə ötürülməsinin qarşısını almaq və şəbəkə üzərindəki yükü azaltmaqdan ibarətdir. Bu mərhələdə lazımsız, təkrarlanan və ya səhv məlumatlar filtrasiya olunur, yalnız faydalı və strukturlaşdırılmış məlumatlar növbəti səviyyəyə ötürülür. Beləliklə, sistemdə gecikmələr azalır və məlumatların ötürülməsi daha səmərəli həyata keçirilir. Bu səviyyə həm də fövqəladə halların ilkin aşkarlanmasında mühüm rol oynayır. Məsələn, qəza baş verdikdə və ya yol bağlandıqda sensorlar bu hadisəni dərhal müəyyən edir və məlumat növbəti səviyyəyə göndərilir.

B. Şəbəkə və kommunikasiya səviyyəsinin iş prinsipi (Şəbəkə layı)

Şəbəkə və kommunikasiya səviyyəsi məlumat toplama və bulud emalı səviyyələri arasında körpü rolunu oynayır. Bu səviyyənin əsas funksiyası müxtəlif mənbələrdən toplanan məlumatların təhlükəsiz, sürətli və fasiləsiz şəkildə ötürülməsini təmin etməkdir. Məlumatların ötürülməsi üçün 5G/6G mobil rabitə texnologiyaları, simsiz şəbəkələr və V2X (Vehicle-to-Everything) kommunikasiya protokolları istifadə olunur. Bu səviyyədə avtomobillər bir-biri ilə (V2V), avtomobillər yol infrastrukturu ilə (V2I) və avtomobillər bulud sistemi ilə qarşılıqlı əlaqə yaradır. Bu əlaqə sayəsində nəqliyyat vasitələri yol vəziyyəti barədə real-vaxt məlumatları alır və ötürür. Məsələn, bir avtomobil qəza və ya tıxac barədə məlumatı digər nəqliyyat vasitələrinə ötürə bilər. Şəbəkə səviyyəsinin digər mühüm funksiyası məlumatların təhlükəsizliyinin təmin edilməsidir. Bu məqsədlə məlumatların şifrələnməsi, autentifikasiya mexanizmləri və şəbəkə trafikinə nəzarət texnologiyaları tətbiq edilir. Eyni zamanda məlumat ötürülməsi zamanı gecikmələrin minimuma endirilməsi və yüksək xidmət keyfiyyətinin qorunması bu səviyyənin əsas prioritetlərindəndir.

C. Bulud emalı və qərarvermə səviyyəsinin iş prinsipi (Bulud hesablama layı)

Bulud emalı və analitika səviyyəsi ağıllı nəqliyyat sisteminin əsas idarəetmə və qərarvermə mərkəzi hesab olunur. Bu səviyyəyə daxil olan məlumatlar böyük verilənlər texnologiyaları vasitəsilə saxlanılır, emal edilir və analiz olunur. Bulud mühitinin yüksək hesablama gücü və miqyaslana bilmə imkanları sayəsində milyonlarla sensor və cihazdan gələn məlumatlar real-vaxt rejimində işlənə bilir. Bu səviyyədə süni intellekt və maşın öyrənməsi alqoritmləri tətbiq edilərək nəqliyyat axınlarının proqnozlaşdırılması həyata keçirilir. Sistem tarixi və cari məlumatları analiz edərək tıxacların yaranma ehtimalını əvvəlcədən müəyyən edə, optimal marşrutlar təklif edə və nəqliyyatın ümumi səmərəliliyini artıra bilir. Bulud səviyyəsində qəbul edilən qərarlar idarəetmə siqnalları şəklində aşağı səviyyələrə göndərilir. Məsələn, işıqforların iş rejimi dəyişdirilir, alternativ marşrutlar sürücülərə təqdim olunur və fövqəladə hallara operativ reaksiya verilir. Bundan əlavə, idarəetmə mərkəzləri üçün hesabatlar hazırlanır və şəhər nəqliyyatının strateji planlaşdırılması həyata keçirilir. Beləliklə, bu səviyyə bütün sistemin "idarəetmə-beyni" rolunu oynayaraq məlumatları qərara çevirir və nəqliyyat sisteminin effektiv idarə olunmasını təmin edir (Şəkil 1).



Şəkil 1. Bulud hesablama mühitində ağıllı nəqliyyat sistemlərinin konseptual modeli

IV. BULUD MÜHİTİNDƏ ANS-DƏ KİBERTƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

ANS bulud əsaslı arxitektura üzərində işlədiyi üçün sistemin hər səviyyəsi xüsusi kibertəhlükəsizlik riskləri ilə üzləşir. Konseptual modeldə üç əsas səviyyə – Məlumat toplama (Əşyaların İnterneti və Kənar hesablama layı), Şəbəkə və kommunikasiya (Şəbəkə layı) və Bulud emalı və qərarvermə (Bulud hesablama layı) – hər biri özünəməxsus zəiflik və təhlükəsizlik problemlərinə malikdir [10].

D. Məlumat toplama səviyyəsində (I səviyyə) kibertəhlükəsizlik məsələləri

Məlumat toplama səviyyəsi ANS-in ən həssas səviyyəsidir, çünki burada fiziki mühitdən birbaşa məlumat toplanır. Əsas risklər:

- IoT cihazlarının zəifliyi: Sensorlar, kameralar və GPS modulları kifayət qədər güclü autentifikasiya və şifrələməyə malik olmaya bilər. Təcavüzkarlar bu

zəiflikdən istifadə edərək cihazlara daxil ola, məlumatları ələ keçirə və ya manipulyasiya edə bilərlər.

- Fiziki müdaxilə: Yol sensorları və kameralar açıq mühitdə yerləşdiyindən fiziki zədələnmə və ya sabotaj riski mövcuddur.
- Məlumat sızmaları: Toplanan məlumatlar, xüsusilə sürücülərin mövqeyi, marşrut və hərəkət nümunələri, şəxsi məxfiliyə ciddi təhdid yarada bilər.
- Zərərli proqram təminatı: IoT cihazlarına yönəlmiş zərərli proqram hücumları məlumatların səhv ötürülməsinə və ya cihazların işdən çıxmasına səbəb ola bilər.

E. Şəbəkə və kommunikasiya səviyyəsində (II səviyyə) kibertəhlükəsizlik məsələləri

Şəbəkə səviyyəsi məlumatın sensorlardan bulud mühitinə ötürülməsini təmin edir. Burada kibertəhlükəsizlik məsələləri daha çox verilənlərin ötürülməsi və rabitə təhlükəsizliyi ilə bağlıdır. Əsas risklər:

- Ortadakı Adam (MitM) hücumları: Təcavüzkarlar məlumat paketlərini şəbəkədən ələ keçirərək dəyişdirə və ya izləyə bilərlər.
- DDoS (paylanmış xidmətdən imtina) hücumları: Bulud və şəbəkə infrastrukturu DDoS hücumlarına qarşı həssasdır, bu da ANS xidmətlərinin dayanmasına səbəb ola bilər.
- Saxta məlumat yeridilməsi: Təcavüzkarlar sistemə yanlış məlumat daxil edərək yol idarəetmə qərarlarını poza bilərlər.
- Zəif şifrələmə və autentifikasiya: Şəbəkədə məlumatlar kifayət qədər güclü şifrələnməzsə və cihazlar düzgün autentifikasiya olunmazsa, məlumatların təhlükəsizliyi risk altına düşür.

F. Bulud emalı və qərarvermə səviyyəsində (III səviyyə) kibertəhlükəsizlik məsələləri

Bulud səviyyəsi ANS-in "idarəetmə-beyni" olduğundan burada baş verən kibertəhlükəsizlik məsələləri sistemin bütövlüyünü və etibarlılığını birbaşa təsir göstərir. Əsas risklər:

- Məlumat bütövlüyünün pozulması: Buluda daxil olan məlumatlar hakerlər tərəfindən dəyişdirilərsə, sistem səhv qərarlar qəbul edə bilər, məsələn, işıqforların yanlış idarəsi və ya yanlış marşrut tövsiyəsi.
- Hücumların avtomatlaşdırılmış aşkarlanmasının olmaması: Süni intellekt və analiz mexanizmləri olmadan kiberhücumların erkən mərhələdə aşkarlanması çətin olur.
- Çoxicarəçili mühit zəifliklər: Bulud platformasında bir neçə istifadəçi və sistemin paylaşılması hücum səthini artırır.
- Tətbiqi proqramlaşdırma interfeysi (Application Programming Interface, API) və bulud interfeyslərinin zəifliyi: Sistem komponentləri arasında interfeyslərin zəif təhlükəsizliyi hücumlara imkan yaradır.
- DDoS və xidmətin dayanması riski: Bulud səviyyəsində resursların həddindən artıq istifadəsi və ya hədəfli hücumlar sistemi qeyri-işlək hala gətirə bilər.

Beləliklə, sistemin hər bir səviyyəsində çoxsəviyyəli və kompleks təhlükəsizlik yanaşmalarının tətbiqi zəruri hesab olunur. Sözügedən yanaşmalar IoT cihazlarının mühafizəsini, şəbəkə trafikinin fasiləsiz monitorinqinin həyata keçirilməsini, məlumatların etibarlı şifrələnməsini, həmçinin bulud analitikası mərhələsində süni intellekt əsaslı təhlükəsizlik metodlarının tətbiqini əhatə etməlidir.

V. KİBERTƏHLÜKƏSİZLİK MƏSƏLƏLƏRİNİN HƏLLİ ÜÇÜN METODLAR

Bulud mühitində ANS-də baş verən kibertəhlükəsizlik problemlərinin həlli üçün bir neçə əsas metod və yanaşma istifadə olunur. Hər bir səviyyəyə uyğun metodlar aşağıdakı kimidir [10]:

- Şifrələmə: Sensorlardan toplanan məlumatların uçdan-uca şifrələnməsi ilə üçüncü tərəflərin məlumatları ələ keçirməsinin qarşısını almaq.
- Güclü autentifikasiya: IoT cihazların və sensorların sertifikat və ya çoxfaktorlu autentifikasiya ilə qorunması.
- Kənar hesablama vasitəsilə təhlükəsizlik: Lokal emal zamanı məlumatların filtrasiya edilməsi və yalnız lazımi məlumatların buluda ötürülməsi.
- Fiziki təhlükəsizlik tədbirləri: Sensor və kameraların zədələnməsinin qarşısını almaq üçün qoruyucu qutular və monitorinq sistemlərinin tətbiqi.
- Məlumatların şifrələnməsi: TLS/SSL protokolları və VŞŞ (Virtual Şəxsi Şəbəkə) ilə məlumatların şəbəkədə təhlükəsiz ötürülməsi.
- Müdaxilə Aşkarlama Sistemləri (MAS) və Müdaxilə Qarşısının Alınması Sistemləri (MQAS): Şəbəkədə anomaliyaların aşkarlanması və hücumların qarşısının alınması.
- DDoS qorunması: Trafik analizi və filtrasiya sistemləri, bulud xidmət provayderlərinin DDoS müdafiə xidmətləri.
- Saxta məlumat aşkarlanması: Süni intellekt və analitik alqoritmlərlə şəbəkəyə daxil olan anormal məlumatların təhlili.
- Süni intellekt əsaslı təhlükəsizlik sistemi: Süni intellekt və maşın öyrənməsi ilə anomaliyaların real-vaxt aşkarlanması və hücumların bloklanması.
- Blokçeyn texnologiyası: Məlumatların dəyişdirilməz və izlənilə bilən şəkildə saxlanması, məlumat bütövlüyünün qorunması.
- Çoxicarəçili (Multi-tenant) mühitin izolyasiyası: Bulud mühitində hər istifadəçi və sistemin müstəqil virtual mühitdə işləməsi, hücum səthinin azaldılması.
- Tətbiqi proqramlaşdırma interfeysi (Application Programming Interface, API) təhlükəsizliyi: Güclü autentifikasiya, rol əsaslı giriş nəzarəti və şifrələmə ilə

interfeyslərin qorunması.

- Ehtiyatlı (redundant) bulud arxitekturası: DDoS və xidmət dayanmasına qarşı çoxlu server və regionlardan istifadə.

VI. Şəbəkə Trafikində Anomaliyaların Aşkarlanması Üçün Riyazi Model

Bu model şəbəkə trafikində normal davranış sahəsini müəyyən etməyə və həmin sahədən kənara çıxan hadisələri anomaliya kimi aşkar etməyə xidmət edir. Modelin əsas ideyası normal müşahidələrin çoxölçülü fəzada bir mərkəz (sentroid) ətrafında toplandığını qəbul etmək və bu mərkəz ətrafında normal zona radiusu təyin etməkdir. Yeni daxil olan hadisə bu zona daxilində qalarsa normal, zonadan kənara çıxarsa anomaliya hesab olunur. Bu tədqiqatda şəbəkə trafikində anomaliyaların aşkarlanması məqsədilə mərkəz əsaslı şəbəkə trafiki anomaliya aşkarlama modulu (adaptiv mərkəzi radius modeli - AMRM) istifadə edilmişdir. Şəbəkə trafikində anomaliya aşkarlaması modeli aşağıdakı mərhələlərdən ibarətdir.

1. Şəbəkəyə daxil olan məlumat axını (trafik) vektor kimi təsvir edilir:

$$X = (x_1, x_2, x_3, \ldots, x_n)$$

burada:

- x_1 – paketlərin sayı (müəyyən zaman intervalında ötürülən paketlərin ümumi sayı).
- x_2 – baytların sayı (ötürülən ümumi məlumat həcmi).
- x_3 – trafik sürəti (axın zamanı paket və baytların ötürülmə sürəti).
- x_4 – axının müddəti (axının davam etdiyi ümumi zaman).

2. Parametrlərin normallaşdırılması (min–max üsulu)

$$x_i^{norm} = \left(\frac{x_i - x_i^{min}}{x_i^{max} - x_i^{min}}\right)$$

beləliklə, normallaşdırılmış trafik vektorunu aşağıdakı kimi yazırıq:

$$X^{norm} = (x_1^{norm}, x_2^{norm}, x_3^{norm}, x_4^{norm})$$

Bu addımdan sonra bütün parametrlər [0, 1] intervalında olur.

3. Normal trafikin mərkəzinin hesablanması: Normal trafikin N müşahidəsi götürülür, yəni:

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

Əvvəlcə hər 283 adius 283 n 283 üzrə müşahidələrin orta qiymətini (yəni hər parametrin mərkəzini) hesablayırıq:

$$c_j = \frac{1}{N}\sum_{k=1}^{N} x_j^{(k)}, \quad j = 1, \ldots, 4$$

Normal trafikin mərkəzi vektoru aşağıdakı kimi təyin olunur:

$$C = (c_1, c_2, c_3, c_4)$$

C vektoru hər bir parametrin mərkəzlərinin cəminin orta qiymətinə bərabər olur. Yəni, hər bir 283 adius 283 n 283 c_j həmin parametrin bütün müşahidələr üzrə orta qiymətidir və bu komponentlərdən əmələ gələn C 283adius283n ümumi normal davranış mərkəzini göstərir.

4. Normal radiusun müəyyən edilməsi sistemdə normal trafik davranışının sərhədlərini təyin etmək və anomaliyaları aşkar etmək üçün aparılır. Hər normal müşahidənin mərkəz nöqtəsi ilə məsafəsi Evklid məsafəsi üzrə hesablanır:

$$d_k = \|X_k^{norm} - C\|, \quad k = 1, \ldots, N$$

4 ölçülü Evklid məsafəsi isə aşağıdakı kimi ifadə olunur:

$$d_k = \sqrt{\left(x_1^{(k)norm} - c_1\right)^2 + \left(x_2^{(k)norm} - c_2\right)^2 + \left(x_3^{(k)norm} - c_3\right)^2 + \left(x_4^{(k)norm} - c_4\right)^2}$$

5. Normal müşahidələrin mərkəzdən orta məsafəsini müəyyən edərək normal zonanın əsas ölçüsünü qiymətləndirmək üçün məsafənin orta qiyməti ($\bar{d}$) aşağıdakı kimi hesablanır:

$$\bar{d} = \frac{1}{N}\sum_{k=1}^{N} d_k$$

Daha sonra məsafələrin dəyişkənliyini qiymətləndirmək və normal zonanın sərhədini dəqiqləşdirmək üçün məsafələrin standart sapması ($std(d_k)$) aşağıdakı kimi hesablanır:

$$std(d_k) = \sqrt{\frac{1}{N}\sum_{k=1}^{N}\left(d_k - \bar{d}\right)^2}$$

Normal davranışın sərhədini müəyyən etmək və anomaliyaların aşkarlanması üçün normal zonanın 283adius ® aşağıdakı kimi hesablanır:

$$R = \left(\frac{1}{N}\right) \cdot \sum_{k=1}^{N} d_k + \beta \cdot std(d_k), \beta \in [1, 2]$$

burada $\bar{d}$ müşahidələrin mərkəzdən orta məsafəsi, $std(d_k)$ bu məsafələrin standart sapmasıdır (kənara çıxma), β əmsalı normal zonanın sərhədini tənzimləyir və praktiki olaraq 1–2 arasında seçilərək həm həssaslığı, həm də səhv pozitiv riskini balanslaşdırır.

Yeni daxil olan trafik:

$$X_{new} = (x_1, x_2, x_3, x_4)$$

Yeni daxil olan hadisənin qiymətləri min–max ilə normallaşdırılır:

$$X_{new}^{norm} = (x_1^{norm}, x_2^{norm}, x_3^{norm}, x_4^{norm})$$

Yeni hadisənin (trafikin) qiymətləndirilməsi:

$$d_{new} = \|X_{new}^{norm} - C\|$$

6. Qərar qaydası. Şəbəkəyə daxil olan yeni trafikin normal davranış mərkəzindən Evklid məsafəsi d_{new} hesablanır və bu məsafə normal müşahidələr əsasında müəyyən edilmiş normal zonanın 283 adius R ilə müqayisə olunur. Müqayisənin nəticəsinə əsasən hadisənin normal trafikə aid olub-olmaması barədə qərar verilir, başqa sözlə, modelin əsas ideyası yeni müşahidənin (trafikin) normal davranış

zonasına düşüb-düşmədiyini məsafə meyarı ilə qiymətləndirməkdir:

$$d_{new} > R \rightarrow Anomaliya$$

$$d_{new} \leq R \rightarrow Normal\ trafik$$

NƏTİCƏ

Məqalədə bulud əsaslı ağıllı nəqliyyat sistemlərinin üçqatlı konseptual modeli təqdim edilmişdir. Model məlumat toplama, şəbəkə və kommunikasiya, həmçinin bulud emalı və qərarvermə səviyyələrini əhatə edir və hər səviyyədə mövcud kibertəhlükəsizlik risklərini təsvir edir. Təklif olunan yanaşmalar IoT cihazlarının qorunması, şəbəkə trafikinin monitorinqi, məlumatların şifrələnməsi və bulud səviyyəsində süni intellekt əsaslı təhlükəsizlik metodlarının tətbiqini əhatə edir. Bu, ANS-in təhlükəsiz və etibarlı fəaliyyətini təmin etmək üçün vacibdir. Məqalədə həmçinin çoxölçülü normal trafikin mərkəzinin hesablanması (sentroid) modeli vasitəsilə şəbəkə trafikində anomaliyaların aşkarlanması metodologiyası göstərilmişdir. Normal davranış mərkəzi və radiusu müəyyən edilərək, yeni daxil olan hadisələr real-vaxtda qiymətləndirilir. Bu yanaşma sistemin səmərəliliyini artırır, qərar qəbuletmə prosesinin operativliyini artırır və kibertəhlükəsizlik səviyyəsini yüksəldir.

ƏDƏBIYYAT

[1] K. Ashokkumar, B. Sam, R. Arshadprabhu, and Britto, "Cloud based intelligent transport system," Procedia Computer Science, vol. 50, pp. 58–63, 2015, doi: 10.1016/j.procs.2015.04.061.

[2] H. Karthikeyan and G. Usha, "A secured IoT-based intelligent transport system (IoT-ITS) framework based on cognitive science," Soft Computing, vol. 28, pp. 13929–13939, 2024, doi: 10.1007/s00500-023-08410-7.

[3] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and M. Bhatt, "Cloud-based intrusion detection approach using machine learning techniques," Big Data Mining and Analytics, vol. 6, no. 3, pp. 311–320, 2023, doi: 10.26599/BDMA.2022.9020038.

[4] H. Zhou, Y. Zheng, X. Jia, and J. Shu, "Collaborative prediction and detection of DDoS attacks in edge computing: A deep learning-based approach with distributed SDN," Computer Networks, vol. 225, art. 109642, 2023, doi: 10.1016/j.comnet.2023.109642.

[5] S. Aurangzeb, M. Aleem, M. T. Khan, H. Anwar, and M. S. Siddique, "Cybersecurity for autonomous vehicles against malware attacks in smart cities," Cluster Computing, vol. 27, no. 3, pp. 3363–3378, 2024, doi: 10.1007/s10586-023-04114-7.

[6] D. Das, S. Banerjee, W. Mansoor, and U. Biswas, "Blockchain for intelligent transportation systems: Applications, challenges, and opportunities," IEEE Internet of Things Journal, pp. 1–15, 2023, doi: 10.1109/JIOT.2023.3277923.

[7] J. Huang, F. Wu, and H. Zhang, "Blockchain-based decentralized data integrity protocol for autonomous vehicles," IEEE Access, vol. 11, pp. 7509–7522, 2023, doi: 10.1109/ACCESS.2023.3237915.

[8] G. Raja, K. Kottursamy, K. Dev, R. Narayanan, A. Raja, and K. B. V. Karthik, "Blockchain-integrated multiagent deep reinforcement learning for securing cooperative adaptive cruise control," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 3, pp. 2614–2625, 2022, doi: 10.1109/TITS.2022.3168486.

[9] T. Mecheva and N. Kakanakov, "Cybersecurity in intelligent transportation systems," Computers, vol. 9, no. 4, art. 83, pp. 1–12, 2020, doi: 10.3390/computers9040083.

[10] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," IEEE Access, vol. 9, pp. 9180–9208, 2021, doi: 10.1109/ACCESS.2021.3050038.

Cybersecurity Risk Detection Model at the Network Level of Cloud-Based Intelligent Transportation Systems

Rashid Alakbarov[1], Mammad Hamidov[2]

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

[1]rashid.alakberov@gmail.com, [2]hemidov8326@gmail.com

Abstract- Intelligent transportation systems (ITS) play an important role in modern cities in terms of optimizing traffic flows, improving road safety, and ensuring efficient management of infrastructure. These systems collect large volumes of data through various sensors, IoT devices, and network technologies, and use cloud computing for data storage and processing and processing. However, the cloud-based architecture creates serious cybersecurity risks related to the confidentiality, integrity, and availability of data. This paper presents a conceptual model for ITS operating in a cloud environment, analyzes the main security problems, and proposes modern methods and approaches for their elimination.

Keywords- intelligent transportation systems; cloud computing; cybersecurity; Internet of Things; data security