



DÖVLƏT İDARƏÇİLİYİNDƏ İNTELLEKTUAL SİSTEMLƏRİN TƏHLÜKƏSİZLİYİNDƏ NEYRON ŞƏBƏKƏLƏRİN TƏTBİQİ

NİCAT İLQAR OĞLU NƏSİROV

Azərbaycan Respublikasının Prezidenti Yanında Dövlət İdarəçilik Akademiyası
nicatnasirov17@gmail.com

Bildiyimiz kimi, müasir dövrdə intellektual sistemlər hər gün dayanmadan sürətli bir şəkildə inkişaf edir. Bu sistemlər artıq ağıllı ev alətlərindən tutmuş, ixtisaslaşmış robotlara, üz tanınma sistemlərinə qədər hər bir formada ola bilər. Dünya ölkələrində, eləcə də ölkəmizdə dövlət idarəçiliyinin diqqət mərkəzində olan ən əsas məsələlərdən biri də intellektual sistemlərin təhlükəsizliyinin düzgün qurulmasıdır. Neyron şəbəkələrin də bu sahədəki məqsədlərindən biri də məhz insanın müəyyən təsvirlərindən – barmaq izi, səs, sifət, göz bəbəyi və s. istifadə edərək ağıllı sistemlərdə təhlükəsizliyi 2 faktorlu identifikasiya və autentifikasiya forması ilə daha gücləndirməkdir. Bu sistemlərdə saxlanılan informasiyanın ölçüsü və keyfiyyəti çox önəmlidir. Verilənlər bazasının ölçüsü də burada mühüm rol oynayır. Bazaya əlavə edilmiş informasiyanın beynəlxalq standartlara cavab verməsi digər vacib şərtlərdəndir. Üz tanınma sistemi insanın üzündən istifadə edərək onun şəxsiyyətini müəyyən edə bilən və ya tanıyan süni intellekt əsasında qurulmuş intellektual sistemdir. Bu sistem istər verilmiş hər hansı şəkil ilə və yaxud da kamera vasitəsilə real vaxtda işləyə bilər. Üz aşkarlama və tanınma sistemi keyfiyyətli və səmərəli olduğundan dövlət idarəçiliyində, həmçinin bank, məktəb, universitet, hərbi, təhlükəsizlik, veb proqramlar, oyun və s. kimi sektorlarda da geniş istifadə olunur.[1] Məsələn, məktəblərdə və universitetlərdə davamiyyətin yoxlanılmasında istifadə oluna bilər. İnsanların təhlükəsizliyində və ölkədə geniş tətbiq olunur. Dövlət idarəçiliyində seçicilərin siyahısını yoxlamaq, siyahıyaalma, immiqrasiya prosesini aşkarlamaq, itkin düşənləri tapmaq kimi bir çox işləri yerinə yetirə bilər. Həmçinin, dövlət daxilində və xaricində cinayətkarların, oğruların tapılmasında əhəmiyyətli bir sistemdir. Təbii ki, hər bir sistemin mənfi cəhətləri olduğu kimi, üz tanınma sisteminin də müəyyən mənfi cəhətləri vardır. Bunlara yüksək qiymət, keyfiyyətli çəkilişə malik kameralar, böyük həcmli yaddaş aiddir. İntellektual sistemdə üz tanınma əməliyyatını həyata keçirmək üçün insanların biometrik məlumatları – üz quruluşu, fotosu, göz bəbəyi və s. öncədən hər hansı bir serverdə saxlanılır. Bu verilənlərin toplanması, yoxlanması və bazaya daxil edilməsi xüsusi işçi qrup və stansiyalar tərəfindən yerinə yetirilir və serverə göndərilir. Sonda isə sistemə daxil olmağa çalışan istənilən şəxsin biometrik məlumatlarını verilənlər bazasındakı məlumatlarla qarşılaşdıraraq onun kim olduğunu, hansı səlahiyyətlərə və rola sahib olduğunu təyin edir. Dövlət təhlükəsizlik orqanlarında, hüquq-mühafizə orqanlarında üz tanınma sistemindən istifadə edərkən məlumatların olduğu çoxlu sayda verilənlər bazası yaradılır. Oğruların, cinayətkarların üzləri bu bazalarda olan məlumatlarla



müqayisə edilərək kimlikləri tapılır. Son illərdə bu alqoritmlərdən geniş istifadə olunur. Biometrik məlumat sayılan uzun təsviri ilə identifikasiya olunan zaman kamera şəxsin üzünü aşkar edir, onu kodlaşdırır və bazayla əlaqə yaradıb üz tanınmanı həyata keçirir. Verilənlər bazasında uzun təsvirlərindən başqa həmin şəxs haqqında məlumat saxlanılır. 3 ölçülü modellər üz tanınmada mühüm rol oynayır və keyfiyyəti artırır.[4] Üz tanınma sisteminin əsasını neyron şəbəkələr təşkil edir. Neyron şəbəkələr bir-birilə əlaqəli olan neyronlardan ibarətdir. Bundan başqa süni neyron şəbəkələri (ANN) giriş qatı, bir və ya bir neçə gizli qatından və çıxış qatını göstərən qovşaqlardan ibarətdir. Hər bir neyron digəri ilə əlaqəlidir və əlaqəli çəki və həddə malikdir. Hər hansı qovşağın çıxışı müəyyən həddən artıq olarsa, həmin qovşaq aktivləşdirilir və məlumatı şəbəkənin növbəti qatına ötürür. Əks halda, heç bir məlumat şəbəkənin növbəti qatına ötürülmür. Neyronlar arasında əlaqə nöqtələri sinapslar adlanır. Siqnalların ötürülməsi elektrik yolu ilə və yaxud mediator vasitəsilə ionların bir qəfəsdən başqa qəfəsə keçməsi ilə baş verir. Neyronun emal elementi bir çox siqnal alır (həm digər neyronlardan, həm də xarici dünyadan giriş siqnalları kimi). Siqnallar bəzən qəbuledici sinapsda dəyişdirilir və ağırlıqlı girişlər emal elementində cəmlənir. Əgər o, həddi keçərsə, digər neyronlara giriş kimi (və ya xarici dünyaya çıxış kimi) gedir və proses təkrarlanır. Adətən çəkilər neyronlar arasında qarşılıqlı əlaqə gücünü təmsil edir. Aktivləşdirmə funksiyası nəzərdə tutulmuş problem üçün istənilən nəticəni əldə etmək üçün istifadə edilən ötürmə funksiyasıdır. Siqmoid funksiyası aktivləşdirmə funksiyası kimi istifadə edilə bilər. Bir neçə aktivləşdirmə funksiyaları var: xətti reqressiya, logistik reqressiya, şəxsiyyət funksiyası, bipolyar, ikili sigmoid, bipolyar sigmoid, hiperbolik tangens, sigmoidal hiperbolik və ReLU. Neyron şəbəkənin sinaptik əlaqələrinin çəkili öyrənmə prosesi ilə uyğunlaşır. Süni neyron şəbəkələri çox güclü hesablama tələb edir və bioloji neyron şəbəkələri ilə müqayisədə böyük miqdarda istilik buraxır. Neyron şəbəkələrdən artıq hər yerdə istifadə etmək mümkündür. Son vaxtlarda, terrorizmin artması ilə əlaqədar olaraq bir sıra yerlərdə - ictimai yerlərdə, ticarət mərkəzlərində, nəqliyyatda təhlükəsizlik təmin olunur.[2] Bunun üçün yüksək keyfiyyətli texnologiyalardan istifadə olunur. Yeni texnologiyalardan hətta insanın əl ilə yerinə yetirilməsi təhlükəli, riskli olan və ya mümkün olmayan işlərdə də istifadə olunur. Bu texnologiyalara şəxslərin üz tanınma sistemlərini, barmaq izi identifikatorlarını, göz skanerlərini, smart kartları və s. nümunə göstərmək olar. Üz tanınma sistemləri bir sıra şirkətlərdə də istifadə olunur. Şirkətdə işçilərə girişə icazə vermək üçün kamera və yaxud barmaq izi oxuma cihazı yerləşdirilir. İşçi məlumatları öncədən sistemə yazılır. Daha sonra hər daxil olma zamanı məlumatlar verilənlərlə yoxlanılır. Bu da icazəsiz daxil olmanın qarşısını alır və təhlükəsizliyi təmin edir. Başqa bir nümunəyə baxaq. Banklarda hər gün minlərlə kredit kartı əməliyyatı həyata keçirilir və saxta əməliyyatları müəyyən etmək üçün avtomatlaşdırılmış metod lazımdır. Neyron şəbəkə hər hansı şübhəli əməliyyatı dərhal qeyd edər, həmçinin müştəriləri, işçiləri xəbərdar edə və yaxud həmin bank kartını dərhal dondurmaq kimi tədbirləri görə bilər. Neyron şəbəkədən istifadə edilməsi müxtəlif hallarda istənilməyən hadisələrin (terrorçuluq, cinayətlərin və s.) qarşısının alınmasına və təhlükəsizliyin tam təmin olunmasına xidmət göstərəcək.[3] Neyron şəbəkələr insan beynini tam şəkildə əvəz edə bilməsələr də, bir çox məntiqi prosesləri yarada bilir və bir çox sənayelərə böyük imkanlar təqdim edir.



Ədəbiyyat

1. Yang, J.W. (2019) A brief analysis of computer network security precautions in the era of big data. Science and Technology Communication, no.2, pp.108-109.
2. Long, Z.H. (2019) Computer network information security and protection strategy in the era of big data. Management Informationization in China, no.3, pp.161-162.
3. Deng, Q.F. (2019) Computer network information security technology and its development trend. Electronic Technology and Software Engineering, no.24, pp.194-195.
4. Liu, W. (2018) Research on Optimizing Network Security Strategy Based on Big Data. Software, vol.39, no.9, pp.205-208.
5. Zhao, L. (2019) Research on computer network security protection strategy under the background of big data. Journal of Heihe University, vol.10, no.1, pp.217-218.
6. Wang, Q., Pan, C. (2017) Analysis of Network Complete Vulnerabilities and Preventive Measures in the Era of Big Data. Network Security Technology and Application, no.2, pp.77 + 79.
7. Bao, L.J. (2019) Application of Big Data-based Network Security Situation Awareness Platform in Private Network Field. Information Security Research, vol.5, no.2, pp.168-175.
8. Wang, B. (2019) Network security fuzzy risk assessment based on computer network technology. Foreign Electronic Measurement Technology, vol.38, no.5, pp.11-16.
9. Liu, Q., Cai, Z.P., Yin, J.P., et al. (2017) Research on the framework and methods of network security detection. Computer Engineering and Science, vol.39, no.12, pp.2224-2229