

UDC 004.89

DOI 10.52171/2076-0515_2024_16_03_81_86

Big Data Analysys in Cyber Physical Systems

P.A. Abbasova

Azerbaijan Technology University (Sh.I. Khatai ave., 103, Ganja city, AZ2011, Azerbaijan)

For correspondence: Abbasova Parvin / e-mail: p.abbasova@atu.edu.az

Abstract

Big Data is a modern analytical trend that enables decision-making based on more data than ever before. Developments in mobile computing, communications, and mass storage architectures over the past decade have given rise to Big Data, an unprecedented amount of valuable information generated in various forms at high speeds. The ability to process this large volume of data in real-time using Big Data analytics tools brings many benefits that can be used in cyber threat analysis systems. This article describes Big Data for cyber-physical systems, real-time stream processing, modeling and behavioral learning for real-time control, current solutions and anticipated problems, and provides some guidelines for troubleshooting.

Keywords: Big Data, IoT, Cyber physical system, cyber attack.

Received 28.12.2023

Revised 19.09.2024

Accepted 23.09.2024

For citation:

P.A. Abbasova

[Big Data Analysys in Cyber Physical Systems]

Herald of the Azerbaijan Engineering Academy, 2024, vol. 16, № 3, pp. 81-86 (in Azerbaijani)

Kiberfiziki sistemlərdə Big Data analizi

P.Ə. Abbasova

Azərbaycan Texnologiya Universiteti (Ş.İ. Xətai pr., 103, Gəncə ş., AZ2011, Azərbaycan)

Xülasə

Big Data əvvəlkindən daha çox məlumat əsasında qərarlar qəbul etməyə imkan verən müasir analitik tendensiyadır. Son onillikdə mobil hesablama, rabitə və kütləvi saxlama arxitekturasındakı inkişafLAR yüksək sürətlə müxtəlif formalarda yaradılan misli görünməmiş miqdarda qiymətli məlumatı özündə cəmləşdirən Big Data-nı meydana gətirdi. Big Data-nın analitik alətlərindən istifadə etməklə bu böyük həcmdə məlumatı real vaxt rejimində emal etmək bacarığı kibertəhlükə analiz sistemlərində istifadə oluna biləcək bir çox fayda gətirir. Bu məqalə kiberfiziki sistemlər üçün Big Data, real vaxt rejimində nəzarət üçün real vaxt axınlarının işlənməsi, modelləşdirmə və davranışların öyrənilməsi, mövcud həlləri və gözlənilən problemləri təsvir edir, problemlərin həlli üçün bəzi təlimatlar təqdim edir.

Açar sözlər: Big Data, IoT, Kiberfiziki sistem, kiber hücum.

Анализ больших данных в киберфизических системах

П.А. Аббасова

Азербайджанский технологический университет (пр. Ш.И. Хатаи, 103, г. Гянджа, AZ2011, Азербайджан)

Аннотация

Большие данные – это современная аналитическая тенденция, которая позволяет принимать решения на основе большего количества данных, чем когда-либо прежде. Развитие мобильных вычислений, коммуникаций и архитектур хранения данных за последнее десятилетие породило большие данные – беспрецедентный объем ценной информации, генерируемой в различных формах на высоких скоростях. Возможность обрабатывать этот большой объем данных в режиме реального времени с помощью инструментов аналитики больших данных дает множество преимуществ, которые можно использовать в системах анализа киберугроз. В статье описываются большие данные для киберфизических систем, обработка потоков в реальном времени, моделирование и поведенческое обучение для управления в реальном времени, текущие решения и ожидаемые проблемы, а также приводятся некоторые рекомендации по устранению неполадок.

Ключевые слова: большие данные, IoT, киберфизическая система, кибератака.

Giriş

Dünya ətraf mühitin monitorinqi, mobil sağlamlıq sistemləri, intellektual nəqliyyat sistemləri və s. kimi müxtəlif sektorlarda yeni xidmətlər və tətbiqlər yaratmaqla dünyamızda inqilab edəcəyi gözlənilən kiberfiziki sistemlərin görünməmiş bir artımının şahidi olur.

İnformasiya və kommunikasiya texnologiyaları sektoru smartfonların, planşetlərin və video axınının geniş istifadəsi və yaxın gələcəkdə gözlənilən sensorların yerləşdirilməsinin əhəmiyyətli dərəcədə artması ilə əlaqədar məlumat trafikində əhəmiyyətli artım yaşayır. Məlumatların artım sürətinin nəzərəcarpacaq dərəcədə artıracağı gözlənilir.

Kiberfiziki sistemlərinin məlumatlarının toplanması, saxlanması, girişi, işlənməsi və təhlili ilə bağlı geniş icmal təqdim etməklə təqdim edirik. Digər sorğu sənədləri ilə müqayisədə, bu, Big Data üzrə ilk panoramik sorğudur. Burada bizim məqsədimiz müxtəlif kiberfiziki sistemlər aspektlərinin panoramik xülasəsini təqdim etməkdir. Bundan əlavə, kiberfiziki sistemlər onları zərərli hücumlardan və icazəsiz müdaxilədən qorumaq üçün kibertəhlükəsizliyi tələb edir ki, bu da şəbəkədə davamlı olaraq yaradılan çoxlu məlumatlarla problemə çevrilir.

Beləliklə, biz həmçinin kiberfiziki sistemlər böyük məlumatların saxlanması, girişi və analitikası üçün təklif olunan müxtəlif təhlükəsizlik həllərinin icmalını təqdim edirik.

Həmçinin kiberfiziki sistemlər kontekstində çağırışlara cavab verən böyük məlumatları müzakirə edirik.

Big Data istifadə sahələri

Big Data tətbiqləri təkcə texnologiyada deyil, bütün iş dünyasında faydalıdır [1]. Big Data-nın bəzi istifadə halları bunlardır:

✓ Məhsul haqqında qərar qəbul etmək:

Böyük məlumat Netflix və Amazon kimi şirkətlər tərəfindən qarşıdan gələn məhsul tendensiyalarına əsaslanan məhsullar hazırlamaq üçün istifadə olunur. İstehlakçıların istədikləri məhsulları istəməzdən əvvəl təxmin etmək üçün keçmiş məhsul performansından birləşdirilmiş məlumatlardan istifadə edə bilirlər. Onlar həmçinin hədəf müştərilərinə ən çox satmaq üçün optimal qiyməti müəyyən etmək üçün qiymət məlumatlarından istifadə edə bilirlər.

✓ **Sınaq:** Böyük verilənlər sistemdəki uğursuzluq nöqtələrini baş verməmişdən əvvəl tanımaq üçün milyonlarla səhv hesabatını, aparat spesifikasiyalarını, sensor oxunuşlarını və keçmiş dəyişiklikləri təhlil edə bilər. Bu, texniki xidmət qruplarına problemin və sistemdə baha başa gələn fasilələrin qarşısını almağa kömək edir.

✓ **Marketing:** Marketoloqlar gələcək reklam kampaniyalarını optimallaşdırmaq üçün əvvəlki marketing kampaniyalarından böyük məlumatları toplayırlar. Pərakəndə satıcılardan və onlayn reklamdan əldə edilən məlumatları birləşdirərək, böyük data müəyyən təsvir növləri, rəngləri və ya söz seçimi ilə reklamlara incə üstünlüklər tapmaqla strategiyaları dəqiqləşdirməyə kömək edə bilər.

✓ **Səhiyyə:** Tibb mütəxəssisləri dərmanların yan təsirlərini tapmaq və xəstəliyin erkən əlamətlərini aşkar etmək üçün böyük məlumatlardan istifadə edirlər. Məsələn, insanlara tez və xəbərdarlıq etmədən təsir edən yeni bir vəziyyətin olduğunu təsəvvür edin. Bununla belə, xəstələrin bir çoxu son illik müayinələrində baş ağrısından şikayət ediblər. Bu, böyük məlumatların təhlilindən istifadə edərək aydın korrelyasiya olaraq qeyd ediləcək, lakin zaman və məkan fərqləri səbəbindən insan gözü tərəfindən qaçırıla bilər.

✓ **Müştəri Təcrübəsi:** Böyük məlumatlar müştəri təcrübəsini və məhsulun qəbulunu qiymətləndirmək üçün işə salındıqdan sonra məhsul qrupları tərəfindən istifadə olunur [2]. Böyük məlumat sistemləri müştərilərin hansı problemlərinin olduğunu və məhsulun nə dərəcədə yaxşı qəbul edildiyini daha yaxşı göstərmək üçün sosial media qeydlərindən, onlayn rəylərdən və məhsul videolarına dair rəylərdən böyük məlumat dəstlərini təhlil edə bilər.

✓ **Maşın öyrənməsi:** Böyük verilənlər maşın öyrənməsi və süni intellekt texnologiyalarının mühüm hissəsinə çevrilib, çünki o, böyük məlumat ehtiyatı təklif edir [3]. ML mühəndisləri daha dəqiq və davamlı proqnozlaşdırma sistemləri yaratmaq üçün müxtəlif təlim məlumatları kimi böyük verilənlər dəstlərindən istifadə edirlər.

Milyardlarla qoşulmuş cihazın olduğu Əşyaların İnterneti (IoT) dövrü kiberhücumçuların istismarı üçün getdikcə daha geniş bir səth yaratdı ki, bu da həmin hücumların sürətli və dəqiq aşkarlanması zərurəti ilə nəticələndi. Son onillikdə mobil hesablama, rabitə və kütləvi saxlama arxitekturasındakı inkişafLAR yüksək sürətlə müxtəlif formalarda yaradılan misli görünməmiş miqdarda qiymətli məlumatı özündə cəmləşdirən böyük verilənlər fenomenini meydana gətirdi. Böyük verilənlərin analitik alətlərdən istifadə etməklə bu böyük həcmdə məlumatı real vaxt rejimində emal etmək bacarığı kibertəhlükə analiz sistemlərində istifadə oluna biləcək bir çox fayda gətirir. Şəbəkələrdən, kompüterlərdən, sensorlardan və bulud sistemlərindən toplanmış böyük məlumatlardan istifadə etməklə kibertəhlükə analitikləri və müdaxilənin aşkarlanması/qarşısının alınması sistemləri real vaxt rejimində faydalı məlumatları kəşf edə bilərlər. Bu məlumat yayılmaqda olan sistem zəifliklərini və hücumları aşkar etməyə

və buna uyğun olaraq təhlükəsizlik həlləri hazırlamağa kömək edə bilər.

Kiberfiziki sistemlər və Əşyaların İnterneti (IoT) kommunikasiyalarını, çoxlu mənbələrdən heterojen məlumat integrasiyasını, təhlükəsizlik, məxfilik və onun bulud hesablamalarına və Big Data platformalarına integrasiyasını əhatə edir. Big Datanın kiberfiziki sistemlər həllərinə integrasiyası bir sıra çətinliklər və imkanlar təqdim edir. Kiberfiziki sistemlər üçün Big Data oflayn və ya toplu emal əsasında ənənəvi həllər ilə uyğun deyil. Sənaye və kritik mühitlərdə real dünya ilə qarşılıqlı əlaqə real vaxt rejimində reaksiya tələb edir. Buna görə də, real vaxt ünsiyyətdən Big Data analitikasına qədər şaquli bir tələb olacaqdır.

Əşyaların İnterneti kiberfiziki sistemlər ilə bağlı cari tədqiqatlar əsasən ümumi obyektlərin fiziki dünyanı özləri görməsinə, eşitməsinə və qoxusuna və müşahidələrini bölüşmək üçün onları birləşdirməyə necə imkan yaratmağa yönəlib. Bu yazıda biz iddia edirik ki, yalnız bağlı olmaq kifayət deyil, bundan əlavə, ümumi obyektlər həm fiziki dünyanı özləri öyrənmək, düşünmək və anlamaq qabiliyyətinə malik olmalıdırlar [4].

Digər tərəfdən, Əşyaların İnterneti çoxlu sayda heterojen şəbəkəyə quraşdırılmış qurğular tərəfindən məskunlaşacaq. Əşyaların internetində böyük verilənlər analitikasının böyük əhəmiyyəti ilə bağlı demək olar ki, hər kəs arasında konsensus olsa da, bu günə qədər məhdud nəticələr, xüsusən də riyazi əsaslar əldə edilmişdir. Bu praktiki ehtiyaclar bizi dörd sinifdə qruplaşdırılan gələcək IoT-də böyük verilənlərin analitikası üçün effektiv alqoritmlərin inkişafı üzrə sisteməlik dərslər təklif etməyə sövq edir: heterojen məlumatların emalı; qeyri-xətti məlumatların emalı; yüksək ölçülü məlumatların emalı və s.

Təqdim olunan tədqiqatın potensial məhsuldar tədqiqat istiqamətində sadəcə kiçik addım kimi təklif olunduğunu düşünürük. Ümid edirik ki, bu məqalə, fənlərarası perspektivlərə, ağıllı resurs bölgüsü, avtomatik şəbəkə əməliyyatı və ağıllı xidmət təminatını təmin etmək üçün xüsusi IoT tətbiqləri üçün praktik və effektiv alqoritmlərin tədqiqi və inkişafına daha çox marağı stimullaşdıracaq [5].

Big Data bank, sığorta, pərakəndə satış, istehsal, təhsil və səhiyyə kimi bir çox sənayedə müştəri davranışlarını təhlil etmək, satış strategiyalarını müəyyənləşdirmək, məhsul inkişafı, proqnozlaşdırma, maşın öyrənmə və əməliyyat səmərəliliyini artırmaq üçün istifadə olunur. Müxtəlif mənbələrdən toplanan məlumatlar mənalı və işləndikdən sonra məlumatların bir-biri ilə əlaqələri araşdırılır [6, 7]. Daha sonra firma tərəfindən məlumatların istifadəsi məqsədindən asılı olaraq məlumatlara müxtəlif ssenarilər tətbiq oluna bilər. Big Data-dan səmərəli istifadə edən firmalar müştəri davranışlarını və əməliyyat proseslərini təhlil edərək bu rəylərə əsasən qərarlar qəbul edə bilərlər. Verilən qərarlar məlumatlara əsaslandığından, firmalar qərar qəbul etmə prosesini daha yaxşı idarə edərək strateji planlaşdırma həyata keçirə bilərlər. Beləliklə, həm əməliyyatlar, həm də müştəri tərəfi yoxlanılır və firmalar lazımi yerlərə vəsait qoyaraq xərclərini azalda bilərlər.

Big Data ilə xərclərin azaldılması, reklam strategiyalarının hazırlanması, işçi qüvvəsinə qənaət təmin olunur.

Nəticə

Big Datanın ölçüləri davamlı olaraq öz zirvəsinə çatır, çünki hazırda o, bir məlumat yaddaşında öz diapazonunu gigabaytdan terabayt sayına dəyişir. Bu məlumat partlayışının çox hissəsi quraşdırılmış sensorlar, ağıllı telefonlar və planşet, kompüterlər də daxil olmaqla şəbəkənin periferiyasında yerləşən cihazların kəskin artmasının nəticəsidir. Beləliklə, indi bir günün kiberfiziki sistemi böyük məlumatların idarə edilməsi mülkiyyəti ilə üzləşir və ondan əsas məlumatları əldə etmək həm də sürətlə artan resurslarla əsas problemdir. Böyük məlumatların doğruluğu, ölçüsü, dəqiqliyi, sərtliyi və təhlükəsizliyi ilə bağlı çoxlu sayda problemlər var. Bu problemlər məlumatların toplanması zamanı dərhal yüksəlir, burada bu məlumat sunamisi bizi bu cür qərar qəbul etməyə məcbur edir, hansı məlumatların saxlandığı və hansının atıldığı və bu məlumatların nümunəsinə uyğun olaraq necə saxlanacağı ilə bağlı praktiki olaraq mənasızdır.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılmasına tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **Lee, H. and Lee, S.**, “A Study on Security Event Detection in ESM Using Big Data and Deep Learning”, *International Journal of Internet, Broadcasting and Communication* Vol.13 No.3 42-49, 2021. *(in English)*
2. **Shetty, SD.** “Sentiment Analysis, Tweet Analysis and Visualization on Big Data Using Apache Spark and Hadoop”. *IOP Conf. Ser.: Mater. Sci. Eng.*, 2021. *(in English)*
3. **Oussous Ahmed, Benjelloun Fatima-Zahra, Lahcen Ayoub Ait, Belfkih Samir.** “Big data technologies: a survey”, *J. King Saud Univ.-Comput. Inf. Sci.* 30 (4), 431–448, 2018. *(in English)*

4. **Jagpreet K., Ramkumar K.R.** “The recent trends in cyber security: A review”, Journal of King Saud University - Computer and Information Sciences, 2021. *(in English)*
5. **Highnam K., Arulkumaran K., Hanif Z.D., and Jennings N.R.** “BETH Dataset: Real Cybersecurity Data for Anomaly Detection Research”, ICML In workshop on Uncertainty and Robustness in Deep Learning 2021 and Conference on Applied Machine Learning for Information Security (CAMLIS 2021), 2021. *(in English)*
6. **Muhammad A., Sagheer A., Khan M.A., Areej F., Muhammad Adnan K. and Sang Woong L.** “MapReduce Based Intelligent Model for Intrusion Detection Using Machine ECJSE 2022 (4) 1572-1582 Siber Güvenlik Amaçlı Büyük Veri Görselleştirme: BETH Veri Seti 1582 Learning Technique”, Journal of King Saud University - Computer and Information Sciences, 2021) *(in English)*
7. **Əsgərov T.K., Rəhimova N.Ə., Abdullayev V.H.** “Sənaye 4.0” platformasına əsaslanan kibernetik sistemlərin struktur layihələndirilməsi. *Azərbaycan Mühəndislik Akademiyasının Xəbərləri*, Cild 14, № 3, s. 87-95, 2022 *(in Azerbaijan)*