Şəhla Müslüm qızı HÜSEYNOVA
Qərbi Kaspi Universiteti, magistrant
E-mail: shlahuseynova72@gmail.com

BİG DATA TEXNOLOGİYALARINDAN İSTİFADƏDƏ ZƏRƏRVERİCİ PROQRAMLARDAN QORUNMA ÜSUL VƏ METODLARI

Xülasə

Məqalədə Big Data texnologiyalarından istifadə edərkən məlumatların sabitliyinin və məxfiliyin qorunması, məxfi məlumatların sızmasının qarşısının alınması və bununla bağlı risklərin qiymətləndirilməməsi problemləri təhlil edilir. "Klassik" təhlükəsizlik sistemlərindən istifadə etməklə böyük məlumat axınının işlənməsi üsulları təqdim olunur. İnformasiya təhlükəsizliyi məqsədləri üçün mövcud böyük verilənlər texnologiyalarının tətbiqi nəzərdən keçirilir. Göstərilir ki, böyük verilənlərlə işləyərkən kompüter şəbəkələrini qorumaq üçün təhlükəsiz məlumat ötürülməsinin müxtəlif üsullarına kompleks yanaşma lazımdır.

Açar sözlər- Big Data-böyük verilənlər texnologiyaları; məlumatların qorunması; məxfilik; icazəsiz giriş riski, kompüter şəbəkəsinin mühafizəsi, şifrələmə, böyük verilənlərin ötürülməsi

UOT: 004
JEL: M1; M2
DOI: https://doi.org/ 10.54414/EFYX4083

Giriş

Son illərdə informasiya texnologiyalarının sürətli inkişafı ilə bərabər, rəqəmsal dünyada təhlükəsizlik problemləri də artır. Müxtəlif sahələrdə yaranan böyük həcmdə məlumatların — *Big Data* — toplanması və emal edilməsi, həm yeni imkanlar, həm də yeni təhlükələr yaradır. Zərərverici proqramlar (malware), viruslar, troyanlar, spyware və digər kibertəhdidlər, xüsusilə böyük verilənlər bazalarına hücum edərək həm şəxsi, həm də korporativ məlumatların oğurlanmasına, sistemlərin sıradan çıxmasına və maliyyə itkilərinə səbəb olur.

Big Data texnologiyaları informasiya təhlükəsizliyi sahəsində yeni bir mərhələ açır. Çünki bu texnologiyalar çox böyük həcmlərdə olan müxtəlif formalı məlumatları sürətlə toplaya, saxlaya və təhlil edə bilir. Ənənəvi təhlükəsizlik metodları artıq bu miqyasda məlumat axınını nəzarətdə saxlamaq üçün kifayət etmir. Ona görə də müasir təhlükəsizlik sistemləri Big Data analitikası, süni intellekt (AI) və maşın öyrənməsi (ML) alqoritmlərinə əsaslanır. Bu yanaşma, zərərverici fəaliyyətləri əvvəlcədən aşkar etməyə, anomaliyalara reaksiya verməyə və real vaxtda təhlükəsizlik insidentlərini aradan qaldırmağa imkan yaradır.

Zərərverici proqramlardan qorunmaq üçün tətbiq edilən üsullar müxtəlifdir. Buraya şəbəkə təhlükəsizliyini təmin edən *IDS/IPS* sistemləri, hadisə və log analizləri üçün *SIEM* platformaları, məlumatların şifrələnməsi, süni intellektə əsaslanan anomaliya aşkarlama mexanizmləri və hətta blockchain texnologiyaları daxildir. Big Data, bu texnologiyaların effektivliyini artıraraq, milyonlarla hadisəni saniyələr ərzində təhlil etməyə imkan verir və beləliklə, zərərverici proqramların təsirini minimuma endirir.

Big Data-nın əsas xüsusiyyətləri adətən "5V" modeli ilə təsvir olunur. Bu parametrlər Big Data-nın fərqləndirici cəhətlərini izah edir:[1]

Həcm (Volume)

Big Data-nın ən əsas xüsusiyyəti məlumatların çox böyük həcmdə olmasıdır. Buraya sosial şəbəkələrdə paylaşılan məlumatlar, sensorlardan gələn datalar, videolar, şəkillər və digər nəhəng məlumat mənbələri daxildir. Müasir dövrdə bu

məlumatlar terabayt və ya petabayt səviyyəsində toplanır və saxlanılır.

Sürət (Velocity)

Big Data yalnız böyük deyil, həm də çox sürətlə yaranır və işlənir. Məsələn, bank əməliyyatları, sosial media postları və ya IoT cihazlarının göndərdiyi məlumatlar real vaxtda və davamlı şəkildə axır. Big Data sistemləri bu axını vaxtında emal edə bilməlidir.

Çeşid (Variety)

Big Data məlumatları çox müxtəlif formalarda olur:

Strukturlaşdırılmış (məsələn, verilənlər bazasındakı cədvəllər)

Strukturlaşdırılmamış (məsələn, videolar, şəkillər, e-maillər)

Yarı-strukturlaşdırılmış (məsələn, XML, JSON sənədləri)

Bu müxtəliflik Big Data-nı klassik verilənlər bazalarından fərqləndirir.

Dəqiqlik (Veracity)

Big Data mühitində məlumatların etibarlılığı böyük çətinlik yaradır, çünki məlumatlar çox vaxt natamam, səhv və ya ziddiyyətli olur. Bu səbəbdən, Big Data analitikləri məlumatların doğruluğunu yoxlayır və keyfiyyətini artırmaq üçün əlavə metodlar tətbiq edir.

Dəyər (Value)

Big Data-nın əsas məqsədi — bu böyük və müxtəlif məlumatlardan faydalı nəticələr əldə etməkdir. Dəyərsiz və işlənməyən məlumat fayda gətirmir. Big Data analitik alətləri bu məlumatlardan trendlər çıxarmaq, qərarları yaxşılaşdırmaq və biznes və ya elm sahəsində fayda yaratmaq üçün istifadə olunur.[3]

Böyük həcmli məlumatların yüksək sürətli təhlili məlumat axınlarının özləri ilə hesablama infrastrukturu arasında əlaqələndirilmiş qarşılıqlı əlaqəni tələb edir. Analitik sistem məlumat saxlanılmazdan əvvəl verilənlərdə hər hansı əhəmiyyətli anomaliya aşkar etməlidir ki, dərhal tədbir görülsün

Bıg datanın zərəverici fəaliyyətlərdən qorunması üsulları

Rəqəmsal transformasiya nəticəsində təşkilatlarda gündəlik olaraq petabaytlarla məlumat yaranır. Bu məlumatlar müştəri informasiyalarından tutmuş maliyyə əməliyyatlarına, sosial media fəaliyyətindən sensor məlumatlarına qədər müxtəlif mənbələrdən toplanır. Məhz bu geniş məlumat mənbələri kiberhücumçular üçün cazibədar hədəfə çevrilir. Zərərverici proqramlar bu məlumatlara sızaraq sistemlərə ciddi ziyan vura bilər. Məsələn, ransomware (fidyə proqramları) böyük təşkilatların məlumat bazalarını ələ keçirərək milyonlarla dollar tələb edir.

Big Data texnologiyaları isə bu məlumat axınını analiz edərək, normal davranış modellərini formalaşdırır və bundan kənara çıxan fəaliyyətləri (məsələn, anidən məlumatın kütləvi ötürülməsi) şübhəli kimi qeyd edir. Bununla, zərərverici proqramların erkən mərhələdə aşkar olunmasına şərait yaradır.

Sosial şəbəkələri bulud texnologiyaları ilə birləşdirərkən, məlumatların təhlükəsizliyini təmin etmək əhəmiyyətli bir məsələdir. Yüksək həcmli verilənlər, həmçinin daha çox riskə məruz qalır. Bu təhlükəsizlik riskləri və onların qarşısını almaq üçün nəzərə alınması vacib olan məsələlər aşağıdakılardır:

Məlumat Təhlükəsizliyi: Bulud sistemlərində verilənlər toplanaraq saxlanılır, buna görə də məlumatların şifrələnməsi və təhlükəsizlik tədbirləri kritik rol oynayır. Zəif təhlükəsizlik protokolları və səhv konfiqurasiya, verilənlərin icazəsiz şəxslər tərəfindən əldə olunmasına səbəb ola bilər. Məlumatın şifrələnməsi, etibarlı şəbəkə protokolları və çox faktorlu autentifikasiya ilə məlumat təhlükəsizliyinin təmin edilməsi vacibdir.

DDoS Hücumları (Paylanmış Xidmətdən İmtina Hücumları): Bulud mühitindəki Big Data infrastrukturuna qarşı DDoS hücumları çox böyük təhlükə yaradır. Bu cür hücumlar, xidmətin fasiləsizliyini pozur, serverlərə aşırı yük gətirərək normal iş rejimini dayandırır. DDoS hücumlarının qarşısını almaq üçün trafik izləmə, qorunma tədbirləri, hibrid bulud modellərindən istifadə və şəbəkə təhlükəsizliyinin gücləndirilməsi vacibdir.

Zərərli Proqramlar: Zərərli proqramlar (malware), Big Data sistemlərinə sızaraq məlumatları oğurlaya və ya silə bilər. Bu cür hücumlar, bulud xidmətlərinin zərərli kodlarla məhv edilməsinə səbəb ola bilər. Zərərli proqramlara qarşı qorunmaq üçün mütəmadi olaraq antivirus və təhlükəsizlik proqramlarının yenilənməsi, sistemlərdə təhlükəsizlik

boşluqlarının tapılması və bağlanması önəmlidir.

Zəif Autentifikasiya və Avtorizasiya: Məlumatların məxfiliyinin qorunması üçün yalnız icazə verilmiş şəxslərin bu məlumatlara giriş əldə etməsi lazımdır. Bulud xidmətləri, zəif autentifikasiya metodlarına sahib olduqda, hətta parol ilə qorunmuş məlumatlar belə asanlıqla sızdırıla bilər. Güclü parol siyasətləri, biometrik autentifikasiya və çox faktorlu identifikasiya ilə sistemlərin təhlükəsizliyi artırılmalıdır.

Big Data ilə işləyən zaman təhlükəsizlik məsələlərinin həllində bir neçə aspekti nəzərə almaq lazımdır. Birincisi, şəbəkənin özünün xarici təhlükələrdən qorunmasını təmin etmək lazımdır. İkincisi, şəbəkədə saxlanılan və ötürülən məlumatların qorunmasını təmin etmək lazımdır. Böyük verilənlər çox vaxt məxfi məlumatları özündə saxlayır və onların sızması ciddi nəticələrə səbəb ola bilər. Bu hallarda məlumatların qorunması üçün müxtəlif üsullardan istifadə olunur.

Məlumatların şifrələnməsi: Məlumatların şifrələnməsindən istifadə hətta icazəsiz giriş halında belə məlumatın məxfiliyini təmin etməyə kömək edir.

Şəbəkə fəaliyyətinin monitorinqi: Şəbəkə fəaliyyətinin müntəzəm monitorinqi anormal davranışı və potensial təhlükəsizlik insidentlərini tez müəyyən etməyə imkan verir.

Autentifikasiya və Avtorizasiya: Güclü autentifikasiya və avtorizasiya metodlarından istifadədə məlumatlara girişi yalnız səlahiyyəti olmayan istifadəçilər üçün məhdudlaşdırır.

Məlumatların surətlərin saxlanılması: Məlumatların müntəzəm surətinin çıxarılması fövqaladə hadisə zamanı məlumat itkisini minimuma endirməyə kömək edir.

Proqram təminatının yenilənməsi: Big Data proqramını və digər zəruri proqram sistemlərinin vaxtaşırı yenilənməsi kiberhücumların verə biləcəyi zərərlərin azaldılmasına səbəb olur.

Firewalldan istifadə . Bu üsul şəbəkədən keçən trafiki idarə edən və filtrləyən proqrama və ya aparat qurğusuna əsaslanır.

Virtual Private Networks (VPN)-dən istifadə - Bu üsulla şəbəkə iştirakçıları arasında təhlükəsiz kanal əlaqələrinin yaradılması vasitəsi ilə şəbəkəyə giriş qaydalarını təyin etməyə və şübhəli və ya zərərli trafiki blok etməyə imkan verir.

Antivirus proqram təminatından istifadə – viruslar, troyanlar, casus proqramlar və digər təhdidləri və zərərli proqramları aşkar etmək və aradan qaldırmaq üçün istifadə edilir.

İnformasiya təhlükəsizliyində big datadan istifadə texnologiyaları

Big Data təhlükəsizliyinin təmin edilməsi zamanı təhdidlərinin qarşısının alınması və aşkarlanması həm texniki, həm də elmi-nəzəri cəhətdən mürəkkəb məsələdir.

Big Data texnologiyalarına əsaslanan və informasiya təhlükəsizliyi problemlərini həll etmək üçün nəzərdə tutulan sistemlər bir neçə sahədə təkmilləşdirilmiş yanaşmalar və alqoritmlərdən istifadə edir. Bu sistemlər, böyük həcmdə məlumatların toplanması, saxlanması, təhlili və təhlükəsizliyin təmin edilməsi üçün müxtəlif metodlardan faydalanır. Aşağıda bu sahədə tətbiq olunan əsas sistemlərə baxaq:

Şəbəkə Təhlükəsizliyi Sistemləri:

Intrusion Detection Systems (IDS): Şəbəkəyə daxil olan məlumatların izlənməsi və anomaliyaların aşkar edilməsi üçün IDS-lər tətbiq olunur. Bu sistemlər, verilənlər bazasında baş verə biləcək qeyri-adi davranışları, zəiflikləri və şəbəkə hücumlarını real vaxtda izləyərək məlumatları qorumağa kömək edir.

Anomaly Detection: Bu alqoritmlər, böyük verilənlər toplusunda qeyri-adi davranışları aşkar edərək mümkün təhlükəsizlik boşluqları və hücumları təhlil edir. Çoxsaylı mənbələrdən toplanan məlumatlar üzərində işləyən bu alqoritmlər, adətən, statistik analiz, maşın öyrənməsi və süni intellekt metodlarından istifadə edir.

Şifrələmə və Məlumatların Qorunması:

Homomorphic Şifrələmə: Bu texnologiya, məlumatları şifrələyərkən onların üzərində əməliyyatlar aparmağa imkan verir. Bu cür şifrələmə, verilənlər bazasının təhlükəsizliyini qorumağa kömək edir, çünki verilənlər heç vaxt açıq halda işlənmir.

End-to-End Şifrələmə: Məlumatların ötürülməsi və saxlanması zamanı tam təhlükəsizlik təmin edən şifrələmə metodlarıdır. Bu yanaşma məlumatların yalnız göndərici və alıcı tərəfindən oxunmasını təmin edir.

Böyük Həcmli Məlumatların Təhlili və Maşın Öyrənməsi:

Məlumatların Analitikası və Vizualizasiyası: Bu yanaşmalar məlumatları daha asan təhlil etmək və qərar qəbul etməni sürətləndirmək məqsədilə istifadə edilir. Bu sistemlər, böyük verilənlər toplusunu vizual olaraq təqdim edir və hər hansı təhlükəsizlik riski və anomaliyaları aşkar etməyə kömək edir.

Maşın Öyrənməsi (ML): Məlumatların təhlili üçün maşın öyrənməsi modelləri geniş şəkildə tətbiq edilir. ML alqoritmləri, əvvəlki təhlükəsizlik hadisələrindən öyrənərək, yeni hücumları və anomaliyaları daha effektiv şəkildə təhlil edir və proqnozlaşdırır.

Hibrid Bulud Sistemləri və Verilənlər Bazasının Təhlükəsizliyi:

Hibrid Bulud İnfrastrukturunun Təhlükəsizliyi: Hibrid bulud yanaşması, məlumatların həm özəl, həm də ictimai buludda saxlanmasını və işlənməsini təmin edir. Bu yanaşma, məlumatların təhlükəsizliyini qorumağa kömək edərkən, eyni zamanda işin performansını optimallaşdırır.

Verilənlər Bazasının Şifrələnməsi və İcazələr: Böyük verilənlər bazasında, yalnız müəyyən istifadəçilərə məlumatlara giriş imkanı verilir və bu məlumatlar şifrələnir. Bu təhlükəsizlik tədbirləri verilənlərin itirilməsi və ya oğurlanmasının qarşısını alır.

Data Loss Prevention (DLP) Sistemləri:

DLP sistemləri, məlumatların itkisinə qarşı qoruma tədbirləri görür. Bu sistemlər, məlumatın oğurlanması və ya yanlış yerdə saxlanması risklərini azaldır. Sistemlər həm də məlumatın izlənməsi və nəzarət edilməsinə imkan verir.

Blockchain Texnologiyası:

Blockchain, Big Data təhlükəsizliyi üçün istifadə edilən başqa bir texnologiyadır. Blockchain, məlumatların dəyişdirilməzliyini və şəffaflığını təmin edərək, məlumatların təhlükəsizliyini artırır. Xüsusilə, məlumat mübadiləsi və autentifikasiyası sahələrində təhlükəsizlik problemlərinin həllinə kömək edir.

Süni İntellekt (AI) və Avtomatlaşdırılmış Təhlükəsizlik:

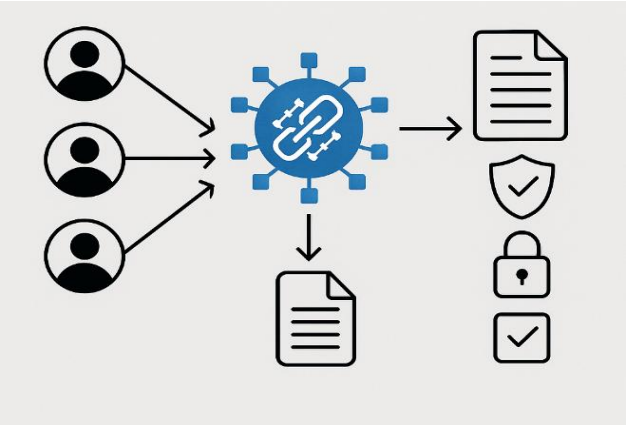
Süni İntellekt əsaslı Təhlükəsizlik Sistemləri: AI, böyük verilənlərə əsaslanan hücumları tanımaq və qarşısını almaq üçün real vaxtda qərarlar qəbul edir. Süni intellekt metodları, məlumat axınlarını təhlil edərək hücum ehtimallarını müəyyən edir və müdaxilə üçün avtomatik tədbirlər tətbiq edir.[7]

Bu sistemlər birləşərək, informasiya təhlükəsizliyinin qorunmasını təmin etmək və kiberhücumları öncədən aşkar etmək məqsədini güdür. Big Data-nın istifadəsi, bu prosesləri sürətləndirir və daha səmərəli edir

Nəticə

Beləliklə, böyük verilənlərlə işləyərkən kompüter şəbəkəsinin qorunması mürəkkəb və çoxşaxəli prosesdir. Bu, müxtəlif üsul və texnologiyalardan istifadəni, həmçinin təhdidlərin daimi monitorinqini və təhlilini tələb edir. Yalnız mühafizəyə kompleks yanaşma böyük verilənlərlə işləməyin etibarlılığını və təhlükəsizliyini təmin edə bilər.

Təklif olaraq - Blokzincir (Blockchain) əsaslı fayl inteqrasiya nəzarəti sistemi, məlumatların təhlükəsiz və şəffaf şəkildə idarə edilməsi üçün blokzincir texnologiyasından istifadə edən bir yanaşmadır. Bu sistem faylların saxlanması, paylanması və dəyişdirilməsi proseslərini mərkəzləşdirilməmiş bir şəbəkədə həyata keçirir. Blokzincir, hər bir əməliyyatı (məsələn, fayl yükləmə, silmə, və ya redaktə etmə) qeydə alır və həmin əməliyyatların hər biri bir blok olaraq zəncirlənir. Bu da sistemin şəffaflığını artırır, məlumat saxtakarlığını və icazəsiz dəyişiklikləri azaldır. Ayrıca, məlumatların təhlükəsizliyi təmin edilir, çünki hər bir əməliyyat kriptografik şəkildə qorunur.



Şəkil.1

Şəkil.1 Blockchain Əsaslı Fayl İnteqrasiya Nəzarəti Sisteminin işləmə prinsipini sadə şəkildə göstərir:

- Solda istifadəçilər (3 nəfər ikona bənzəyən fiqurlar) yerləşir. Bunlar sistemə daxil olub fayl əməliyyatları icra edən şəxslərdir.
- Mərkəzdə blokzincir şəbəkəsi təsvir olunub (mavi zəncir işarəsi ilə). Bura bütün əməliyyatların qeydə alındığı və idarə olunduğu mərkəzsizləşdirilmiş sistemdir.
- Sağ tərəfdə isə fayl, təhlükəsizlik simvolları (qalxan, kilid, yox işarəsi) göstərilir. Bu da faylın dəyişikliklərdən qorunduğunu, təhlükəsiz və təsdiq olunmuş olduğunu ifadə edir.
- Oxlar isə məlumat axını göstərir: istifadəçilər blokzincirə əməliyyat göndərir, blokzincir isə faylların təhlükəsiz inteqrasiyasını təmin edir.

Blokzincir əsaslı fayl inteqrasiya nəzarəti sistemi, müasir məlumat idarəçiliyində təhlükəsizlik, şəffaflıq və dəyişməzlik təmin edən güclü bir texnologiyadır. Bu sistem istifadəçi əməliyyatlarını kriptoqrafik şəkildə qoruyur, dəyişiklikləri blokzincirdə daimi olaraq qeyd edir və icazəsiz müdaxilələrin qarşısını alır. Şirkətlər, hökumətlər, tibb və təhsil sektorları üçün faylların düzgün və etibarlı inteqrasiyasını təmin edir. Gələcəkdə bu texnologiya daha geniş sahələrdə tətbiq ediləcək və rəqəmsal məlumatların idarə olunmasında standart həll halını alacaq.

ƏDƏBİYYAT SİYAHISI:

1. Big Data – Data Encryption in Big Data: [URL:https://www.encryptionconsulting.com/data-protection-in-big-data-using-encryption/.
2. IBM Security Intelligence with Big Data. http://www-03.ibm.com/security/solution/intelligence-big-data/
3. https://ru.wikipedia.org/wiki/DoS-атака
4. В. Коржов, “Большие Данные в службе безопасности,” 9,с.48-49 Открытые системы, 2013,№9, с 48-49
5. Kim, W., & Solomon, M. G. (2016). Fundamentals of Information Systems Security (2nd ed.). Jones & Bartlett Learning.
6. Pfleeger, S. L., & Pfleeger, C. P. (2012). Security in Computing (5th ed.). Pearson Education.
7. Bace, R. G., & Mell, P. (2001). Intrusion Detection Systems. Addison-Wesley.
8. Gartner, Inc. (2018). Magic Quadrant for Security Information and Event Management.
9. Liu, Z., & Zhang, G. (2017). "Big Data Security: Challenges, Methods and Applications". International Journal of Computer Science and Information Security (IJCSIS), 15(7), 98-110.
10. Jang, H., & Lee, Y. (2018). "Malware Detection and Prevention in Big Data Environments: A Survey". *Journal of Cybersecurity and Privacy*, 4(1), 67-83.

Shahla Muslim HUSEYNOVA
Master's student of Western Caspian University

METHODS AND METHODS OF PROTECTION FROM MALWARE USING BIG DATA TECHNOLOGIES

Summary.
The article analyzes the problems of protecting data stability and confidentiality, preventing the leakage of confidential information and underestimating the risks associated with this when using Big Data technologies. Methods of processing large data flows using "classical" security systems are presented. The application of existing big data technologies for information security purposes is considered. It is shown that in order to protect computer networks when working with big data, a comprehensive approach to various methods of secure data transmission is necessary.

Keywords. Big Data-big data technologies; data protection; confidentiality; unauthorized access risk, computer network security, encryption, big data transmission

Шахла Муслим ГУСЕЙНОВА
Западно-Каспийского университета, магистрант

МЕТОДЫ И СПОСОБЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИЙ BIG DATA

Резюме

В статье анализируются проблемы защиты стабильности и конфиденциальности данных, предотвращения утечки конфиденциальной информации, а также оценки связанных с этим рисков при использовании технологий Big Data. Представлены методы обработки больших потоков данных с использованием «классических» систем безопасности. Рассматривается возможность применения существующих технологий больших данных в целях обеспечения информационной безопасности. Показано, что защита компьютерных сетей при работе с большими данными требует комплексного подхода к различным методам безопасной передачи данных.

Ключевые слова - Большие данные; защита данных; конфиденциальность; риск несанкционированного доступа, безопасность компьютерных сетей, шифрование, передача больших данных

Daxil olub: 04.07.2025