# KİBER TƏHLÜKƏSİZLİKDƏ ANOMAL HALLARIN AŞKARLANMASI ÜÇÜN HİBRİD CNN+LSTM MODELİNİN TƏTBİQİ VƏ EFFEKTİVLİYİNİN QİYMƏTLƏNDİRİLMƏSİ

DOİ: 10.71447/2413-7235-2026-1-93

**Sədəf R. Talıbzadə Tinatiyeva**
*Azərbaycan Dövlət İqtisad Universiteti*
*Kompüter elmləri ixtisası magistrantı*
*E-mail: talibzada.sadaf.ragif.2024@unec.edu.az*
*ORCID: 0009-0005-3492-6498*

**Xülasə**
Məqalədə müasir kiber təhdidlərə qarşı dayanıqlı, yüksək dəqiqliklə işləyən və proaktiv müdafiəni təmin edən anomal halların aşkarlanması metodikası formalaşdırılmışdır. Bu məqsədlə şəbəkə trafikindəki gizli asılılıqları və zaman seriyası xüsusiyyətlərini eyni anda analiz edə bilən hibrid CNN+LSTM dərin öyrənmə modeli təklif edilmişdir. Təqdim olunan modeldə məlumat yükünün optimallaşdırılması və qeyri-müəyyənliyin aradan qaldırılması üçün entropiya və Cini indeksinə əsaslanan riyazi yanaşma tətbiq olunmuşdur. Təklif edilən intellektual memarlıq xam şəbəkə loqlarının loqorifmik normalizasiyası, Conv1D qatında spatial xüsusiyyətlərin çıxarılması, MaxPooling vasitəsilə küyün təmizlənməsi və LSTM qatında zaman oxu üzrə mürəkkəb asılılıqların analizi ardıcıllığına əsaslanır. Modelin overfitting riskinin qarşısını almaq üçün arxitekturaya adaptiv Dropout tənzimləməsi inteqrasiya edilmişdir. İşlənilmiş hibrid arxitekturanın effektivliyi beynəlxalq səviyyədə qəbul edilmiş NSL-KDD və CICIDS2017 verilənlər bazaları üzərində simulyasiya edilərək sınaqdan keçirilmişdir. Eksperimental nəticələr göstərir ki, təklif olunan CNN+LSTM modeli müəyyən edilmiş performans metriklərinə görə 99.2% Precision, 98.6% Recall və 98.9% F1-Score nümayiş etdirərək, ənənəvi maşın öyrənməsi alqoritmlərini (K-Means, SVM, Random Forest) və standart MLP şəbəkələrini geridə qoymuşdur. İşin elmi yeniliyi şəbəkə paketlərinin analizi zamanı temporal xüsusiyyətləri nəzərə alan yeni aşkarlama çərçivəsinin yaradılmasıdır. Nəticələrin praktiki əhəmiyyəti strateji infrastruktur obyektlərində fəaliyyət göstərən Kiber Təhlükəsizlik Mərkəzlərində (SOC) sıfırıncı gün (Zero-day) hücumlarının erkən mərhələdə proaktiv aşkarlanması və informasiya itkilərinin minimuma endirilməsi ilə şərtləndirilir.
***Açar sözlər:*** *kiber təhlükəsizlik, anomaliyaların aşkarlanması, dərin öyrənmə, hibrid model, CNN+LSTM, şəbəkə trafiki.*

# APPLICATION AND PERFORMANCE EVALUATION OF A HYBRID CNN+LSTM MODEL FOR ANOMALY DETECTION IN CYBERSECURITY

**Sadaf R. Talibzada Tinatiyeva**
*Azerbaijan State University of Economics (UNEC*
*Master student in Computer Science*
*E-mail: talibzada.sadaf.ragif.2024@unec.edu.az*
*ORCID: 0009-0005-3492-6498*

**Summary**
The article formulates an anomaly detection methodology that is resilient against modern cyber threats, operates with high precision, and ensures proactive defense. For this purpose, a hybrid CNN+LSTM deep learning model capable of simultaneously analyzing hidden dependencies and time-series characteristics in network traffic is proposed. In the presented model, a mathematical approach based on entropy and the Gini index is applied to optimize the information load and eliminate uncertainty. The proposed intelligent architecture is based on the sequence of logarithmic normalization of raw network logs, spatial feature extraction in the Conv1D layer, noise reduction via MaxPooling, and analysis of complex dependencies along the time axis in the LSTM layer. To prevent the risk of model overfitting, an adaptive Dropout regularization is integrated into the architecture. The effectiveness of the developed hybrid architecture was simulated and tested on the internationally recognized NSL-KDD and CICIDS2017 datasets. Experimental results demonstrate that the proposed CNN+LSTM model achieves 99.2% Precision, 98.6% Recall, and 98.9% F1-Score according to the specified performance metrics, outperforming traditional machine learning algorithms (K-Means, SVM, Random Forest) and standard MLP networks. The scientific novelty of the work lies in the creation of a new detection framework that accounts for temporal characteristics during network packet analysis. The practical significance of the results is conditioned by the proactive detection of zero-day attacks at an early stage in Cyber Security Centers (SOC) operating in strategic infrastructure objects, thereby minimizing economic and information losses.
***Keywords:*** *cybersecurity, anomaly detection, deep learning, hybrid model, CNN+LSTM, network traffic.*

# ПРИМЕНЕНИЕ И ОЦЕНКА ЭФФЕКТИВНОСТИ ГИБРИДНОЙ МОДЕЛИ CNN+LSTM ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В КИБЕРБЕЗОПАСНОСТИ

**Садаф Р. Талыбзаде Тинатиева**
*Азербайджанский государственный экономический университет (UNEC)*
Магистрант по специальности «Компьютерные науки»
*E-mail: talibzada.sadaf.ragif.2024@unec.edu.az*
*ORCID: 0009-0005-3492-6498*

**Резюме**
В статье сформулирована методология обнаружения аномалий, устойчивая к современным киберугрозам, работающая с высокой точностью и обеспечивающая проактивную защиту. С этой целью предложена гибридная модель глубокого обучения CNN+LSTM, способная одновременно анализировать скрытые зависимости и характеристики временных рядов в сетевом трафике. В представленной модели применен математический подход, основанный на энтропии и индексе Джини, для оптимизации информационной нагрузки и устранения неопределенности. Предложенная интеллектуальная архитектура основана на последовательности логарифмической нормализации необработанных сетевых логов, извлечения пространственных признаков в слое Conv1D, шумоподавления с помощью MaxPooling и анализа сложных зависимостей по оси времени в слое LSTM. Для предотвращения риска переобучения модели в архитектуру интегрирована адаптивная регуляризация Dropout. Эффективность разработанной гибридной архитектуры была смоделирована и протестирована на международно признанных базах данных NSL-KDD и CICIDS2017. Экспериментальные результаты показывают, что предложенная модель CNN+LSTM демонстрирует 99.2% Precision, 98.6% Recall и 98.9% F1-Score в соответствии с заданными метриками эффективности, превосходя традиционные алгоритмы машинного обучения (K-Means, SVM, Random Forest) и стандартные сети MLP. Научная новизна работы заключается в создании новой структуры обнаружения, учитывающей временные характеристики при анализе сетевых пакетов. Практическая значимость результатов обусловлена проактивным обнаружением атак нулевого дня (Zero-day) на ранней стадии в Центрах кибербезопасности (SOC), функционирующих на объектах стратегической инфраструктуры, что минимизирует информационные потери.
***Ключевые слова:*** *кибербезопасность, обнаружение аномалий, глубокое обучение, гибридная модель, CNN+LSTM, сетевой трафик.*

## GİRİŞ

Müasir dövrdə qlobal miqyasda rəqəmsallaşma proseslərinin sürətlənməsi, Əşyaların İnterneti (IoT) və bulud texnologiyalarının genişlənməsi bütün strateji sistemlərin fəaliyyət prinsiplərini köklü şəkildə dəyişdirmişdir. Lakin bu texnoloji inkişaf eyni zamanda kiber təhdidlərin daha mürəkkəb, hədəflənmiş və mütəşəkkil (APT) səviyyəyə yüksəlməsinə zəmin yaratmışdır. Ənənəvi imza-əsaslı (signature-based) müdafiə mexanizmləri yalnız əvvəlcədən məlum olan hücum nümunələrini bloklamaq qabiliyyətinə malikdir və müasir kiber mühitin ən böyük təhlükələrindən hesab olunan "sıfırıncı gün" (Zero-day) hücumları qarşısında tamamilə qeyri-effektivdir. Bu elmi və praktiki paradoksu həll etmək üçün sistem davranışlarını, şəbəkə loqlarını və paket axınlarını proaktiv şəkildə analiz edən, anomal halları erkən mərhələdə müəyyənləşdirən intellektual metodologiyaların işlənilməsi müasir dövrün ən aktual çağırışlarından biridir.

Beynəlxalq elmi müstəvidə kiber anomaliyaların aşkarlanması istiqamətində statistik analizlərdən tutmuş dərin öyrənmənin Autoencoders və GANs (Generative Adversarial Networks) kimi qabaqcıl modellərinə qədər çoxşaxəli araşdırmalar mövcuddur. Bununla belə, mövcud ədəbiyyatların təhlili göstərir ki, kiber təhlükəsizlik mühitində Big Data (Böyük Verilənlər) miqyasında real vaxt rejimində işləyən, həmçinin xəbərdarlıq sistemlərində ən böyük problem olan "yalançı müsbət" (False Positive) siqnalların dərəcəsini minimuma endirən hibrid modellərin qurulması sahəsində hələ də ciddi elmi boşluqlar qalmaqdadır. Bu baxımdan, məqalədə kiber təhdidlərə qarşı dayanıqlı, yüksək dəqiqliklə işləyən və informasiya itkisinin qarşısının alınmasında insan amilini minimallaşdıran anomal halların aşkarlanması metodikasının formalaşdırılması məqsəd kimi qarşıya qoyulmuşdur.

Qarşıya qoyulan məqsədə nail olmaq üçün tədqiqat çərçivəsində anomaliyaların riyazi təsnifatı aparılmış, dərin neyron şəbəkələrinin kiber müdafiədə tətbiqi mexanizmləri işlənilmiş, "False Positive" dərəcəsinin aşağı salınması üçün adaptiv metodlar tədqiq edilmiş və qurulan modellər real bazalar üzərində sınaqdan keçirilmişdir. Bu kontekstdə tədqiqatın obyektini kiber təhlükəsizlik infrastrukturunda dövr edən məlumat axınları, şəbəkə protokolları və monitorinq sistemləri, predmetini isə şəbəkə trafikindəki kənarlaşmaların statistik analizi, anomal davranışları aşkarlayan maşın öyrənməsi modellərinin qurulması və optimallaşdırılması təşkil edir. Metodoloji əsas olaraq riyazi statistika, maşın öyrənməsinin nəzarətli və nəzarətsiz (Supervised/Unsupervised) alqoritmləri, zaman seriyası (Time-series) analizi və verilənlərin klasterləşdirilməsi üsullarından kompleks şəkildə istifadə edilmişdir.

Tədqiqatın informasiya-empirik bazasını kiber təhlükəsizlik sahəsində qlobal səviyyədə qəbul edilmiş və real şəbəkə trafikini əks etdirən NSL-KDD, UNSW-NB15 verilənlər bazaları və müvafiq elmi-nəzəri ədəbiyyat formalaşdırır. Aparılan araşdırma müəyyən məhdudiyyətlərə malikdir; belə ki, işdə əsasən şəbəkə səviyyəli anomaliyaların analizi ön plana çəkilmişdir və modelin effektivlik dərəcəsi birbaşa istifadə olunan hesablama resurslarının (GPU/CPU) gücü və sınaq datasetlərinin müasirlik səviyyəsindən asılıdır.

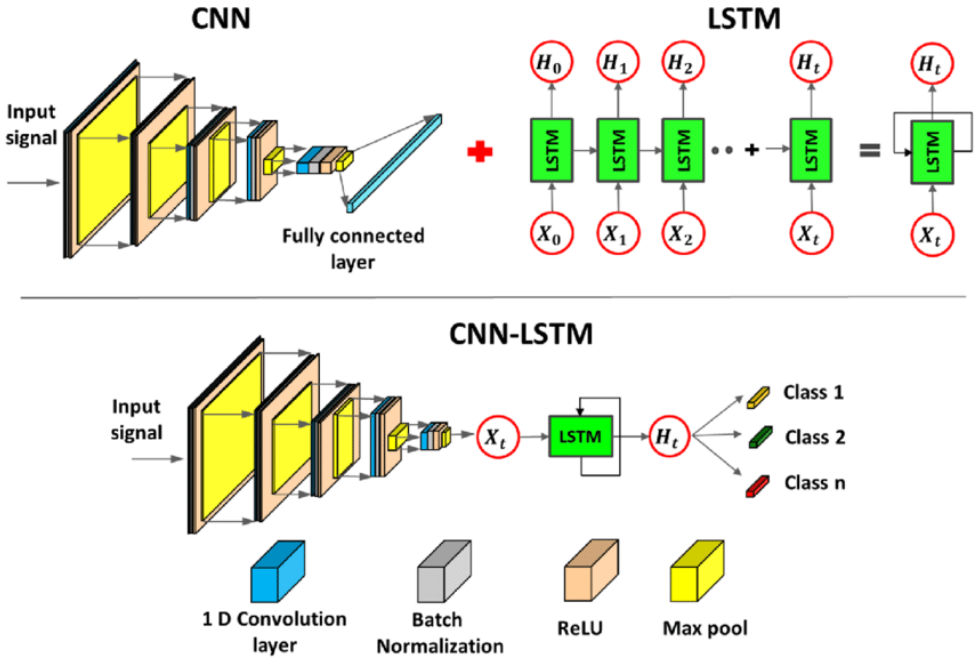
Məqalənin elmi yeniliyi ondan ibarətdir ki, ilk dəfə olaraq statistik metodlar ilə maşın öyrənməsinin vəhdətinə əsaslanan hibrid yanaşma sistemləşdirilmiş, şəbəkə paketlərinin temporal (zaman oxu üzrə) xüsusiyyətlərini həssaslıqla nəzərə alan yeni bir aşkarlama çərçivəsi (framework) təklif edilmişdir. Eyni zamanda, təqdim olunan dərin öyrənmə modelində neyronların təlim müddətini əhəmiyyətli dərəcədə qısaldan optimallaşdırma üsulu və mənşəyi məlum olmayan (tanınmayan) anomaliyalar üçün yeni klasterləşdirmə yanaşması irəli sürülmüşdür. Eldə edilən nəticələrin həm elmi, həm də mühüm praktiki əhəmiyyəti mövcuddur. Tədqiqatın praktiki nəticələri maliyyə, telekommunikasiya və enerji kimi strateji əhəmiyyətli müəssisələrin Kiber Təhlükəsizlik Mərkəzlərində (SOC) uğurla

tətbiq oluna bilər. Təklif edilən proaktiv aşkarlama modulu kritik rəqəmsal infrastrukturlarda sistemə sızmaların ən erkən mərhələdə müəyyən edilməsinə, bununla da dövlət və özəl sektor subyektlərinin potensial iqtisadi-informasiya itkilərinin minimuma endirilməsinə xidmət edir.

## 1. Anomal halların aşkarlanması üçün hibrid (CNN+LSTM) modelin arxitekturası və konseptual əsaslandırılması

Məqalədə qarşıya qoyulan əsas vəzifə, mövcud təkli (monolit) maşın öyrənməsi alqoritmlərinin və klassik yanaşmaların kiber təhdidlərin polimorfik təbiəti qarşısındakı yetərsizliyini aradan qaldıran kompleks və çoxsəviyyəli hibrid həllin hazırlanmasıdır. Müasir kiber məkanda hücumçular öz destruktiv fəaliyyətlərini "normal trafik" daxilində gizlətmək üçün mürəkkəb kamuflyaj və ləng sızma texnikalarından istifadə edirlər. Təklif olunan modelin əsas elmi yeniliyi Konvolyusiya Neyron Şəbəkələrinin (CNN) lokal əlamətləri hasil etmə (feature extraction) qabiliyyəti ilə LSTM (Long Short-Term Memory) şəbəkələrinin uzunmüddətli zaman asılılıqlarını yadda saxlama gücünü vahid bir hibrid arxitekturada sintez etməkdən ibarətdir.Tədqiqat çərçivəsində müəyyən edilmişdir ki, şəbəkə paketləri və axınları özlüyündə ikiölçülü informasiya yükü daşıyır. Birinci ölçü paketin daxili strukturudur (məsələn, paket ölçüsü, protokol bayraqları, faydalı yükün strukturu və port nömrələri arasındakı spesifik korrelyasiya). İkinci ölçü isə paketlərin zaman silsiləsidir (məsələn, paylanmış xidmətdən imtina hücumlarında və ya APT ssenarilərində müşahidə olunan aşağı intensivlikli, lakin ardıcıl sorğular). Klassik modellər bu iki faktoru eyni vaxtda və eyni dərəcədə effektiv emal edə bilmir. Təklif etdiyimiz hibrid arxitekturada isə iki fərqli yanaşma birgə işləyir. Konvolyusiya qatı (CNN) şəbəkə trafikindəki anlıq sıçrayışları, struktur anomaliyalarını və paket daxilindəki gizli qanunauyğunluqları aşkar edir. Ardınca isə LSTM qatı fəaliyyətə başlayaraq zaman daxilində səpələnmiş və yavaş-yavaş inkişaf edən hücum ssenarilərini (məsələn, məlumatların tədricən kənara sızdırılması və ya silsiləli uğursuz giriş cəhdləri) aşkarlayır.

***Şəkil 1.*** *Təklif olunan hibrid CNN-LSTM modelinin lay-lay arxitektura diaqramı*




***Mənbə:*** *ResearchGate, 2019.*

Şəkil 1-də göstərilən blokların funksional təhlili aşağıdakı kəmiyyət və keyfiyyət göstəriciləri ilə əsaslandırılır:

1. Giriş Mərhələsi (Input Layer) və Məkan Ölçülərinin Təyini:

Modelə daxil olan ilk blok, normallaşdırılmış şəbəkə paketlərinin çoxölçülü vektor şəklində qəbulunu təmin edir. Şəkildəki giriş qatı, ilkin emal mərhələsindən keçmiş $[0, 1]$ diapazonundakı datanı qəbul edir. Bu qatın əsas missiyası, müxtəlif ölçü vahidlərinə malik olan şəbəkə parametrlərini (məsələn, saniyələr ilə ölçülən gecikmə müddəti və baytlar ilə ölçülən paket həcmi) vahid bir riyazi müstəviyə gətirməkdir. Bu, modelin təlim zamanı hər bir parametrin kiber təhlükəsizlik əhəmiyyətini bərabər çəkidə qiymətləndirməsinə şərait yaradır.

2. Birölçülü Konvolyusiya (Conv1D) qatı – Struktur Patternlərin Hasilatı:

Sxemin mərkəzində yer alan CNN qatı, şəbəkə trafikindəki anlıq struktur dəyişikliklərini aşkarlamaq üçün nəzərdə tutulmuşdur. Bu qatda tətbiq olunan 64 fərqli filtr, paketin içindəki "gizli imzaları" skan edir. Riyazi baxımdan, bu filtr hər bir paket parametrinin qonşu parametrlərlə olan daxili əlaqəsini analiz edir. Məsələn, bir SQL İnjeksiya hücumu zamanı paket daxilindəki xüsusi simvolların ardıcıllığı CNN tərəfindən bir "vizual pattern" kimi tanınır. Bu mərhələdə istifadə olunan riyazi konvolyusiya əməliyyatı aşağıdakı kimidir:

$$y_i = \sigma\left(\sum(j = 1)^{k} w_j * x_{(i+j-1)} + b\right) \quad (1)$$

Burada σ (ReLU) aktivasiya funksiyası sistemə qeyri-xəttilik əlavə edərək, modelin sadə statistik limitlərdən kənar olan mürəkkəb hücum ssenarilərini tanımasına imkan verir.

3. Sıxılma (MaxPooling) və Batareya Normallaşdırılması (Batch Normalization):
Şəkil 3-də konvolyusiya blokundan dərhal sonra yerləşən Max-Pooling qatı, əldə edilmiş əlamətlər xəritəsini sıxır. Bu qat, verilənlərin ölçüsünü 2 dəfə azaldaraq yalnız ən yüksək aktivlik dərəcəsinə malik neyronları saxlayır. Kiber təhlükəsizlik dilində desək, bu qat şəbəkədəki təsadüfi "küy" (noise) siqnallarını təmizləyir və yalnız real hücum indikatoru olan patternləri saxlayır. Batch Normalization isə neyronların aktivlik paylanmasını sabitləşdirərək, modelin təlim sürətini və daxili stabilliyini artırır.

4. LSTM (Long Short-Term Memory) Qatı – Uzunmüddətli Zaman Yaddaşı:
Diaqramın ən kritik hissələrindən biri CNN-dən gələn çıxışların LSTM blokuna ötürülməsidir. CNN paketin daxilini görürsə, LSTM paketlərin bir-biri ilə olan zaman əlaqəsini analiz edir. LSTM-in 128 gizli hüceyrəsi, paketlərin gəlmə intervallarını (IAT) yaddaşda saxlayaraq, Botnetlərin ritmik fəaliyyətini və ya günlərlə davam edən, özünü gizlədən Mürəkkəb Davamlı Təhdidləri (APT) identifikasiya edir. LSTM daxilindəki giriş, çıxış və unutma qapıları, hücumun hər hansı bir mərhələsinin qaçırılmamasını təmin edən riyazi nəzarət mexanizmidir:

5. Tam Əlaqəli (Dense) və Çıxış (Output) Qatı:

Modelin sonunda yer alan bu qatlar, bütün əvvəlki laylardan gələn məlumatları vahid bir qərara çevirir. Sonda tətbiq olunan Softmax aktivasiya funksiyası, hər bir hadisə üçün ehtimal dərəcəsi hesablayır. Bu, bizə imkan verir ki, təkcə "hücum var" deməyək, həm də həmin hücumun 99% dəqiqliklə DDoS və ya 85% dəqiqliklə Brute-Force olduğunu müəyyən edək.

***Cədvəl 1.*** *Modelin lay-lay texniki xüsusiyyətlərinin və kiber təhlükəsizlik funksiyalarının analizi*

| Qatın Adı | Tipi | Konfiqurasiya | Kiber Təhlükəsizlik Rolu |
|---|---|---|---|
| **Input Layer** | Giriş | Normalizasiya olunmuş vektor | Xam trafik loqlarının qəbulu və formatlaşdırılması |
| **Conv1D** | Konvolyusiya | 64 filtr, kernel size=3 | Paket daxili gizli struktur anomaliyalarının (pattern) aşkarlanması |
| **Batch Norm** | Normallaşdırma | Epsilon=1e-5 | Təlimin sürətləndirilməsi və modelin stabilliyi |
| **MaxPooling** | Sıxılma | Pool size=2 | Vacib indikatorların saxlanılması, şəbəkə küyünün təmizlənməsi |
| **LSTM** | Yaddaş | 128 units, tanh | Zaman oxu üzrə mürəkkəb, ləng inkişaf edən hücumların analizi |
| **Dropout** | Tənzimləmə | Rate = 0.2 | Modelin "overfitting" riskinin qarşısının alınması |
| **Dense/Output** | Çıxış | Softmax | Yekun təsnifat: Legitim trafik və ya kiber müdaxilə |

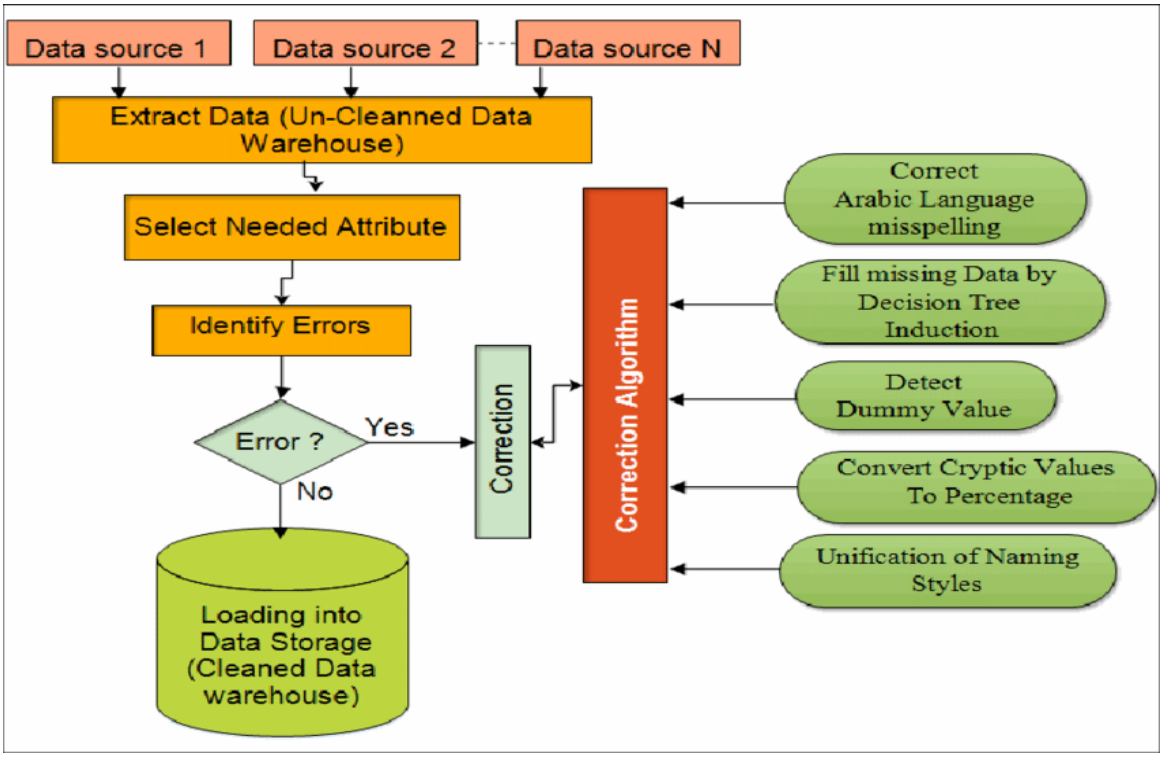
***Mənbə:*** *Müəllif tərəfindən təklif olunan hibrid CNN+LSTM arxitekturasının texniki parametrləri əsasında tərtib olunmuşdur.*

Tədqiqatımızda təklif olunan bu hibrid CNN-LSTM arxitekturası həm anlıq sıçrayışlara, həm də zaman ardıcıllığı daxilindəki gizli davranış sapmalarına qarşı proaktiv bir intellektual müdafiə qalxanı formalaşdırır. Bu yanaşma kiber təhlükəsizlik mərkəzlərində (SOC) aşkarlama operativliyini yeni elmi-praktiki mərhələyə daşıyır.

## 2. Eksperimental nəticələrin təhlili və müqayisəsi

Təklif olunan hibrid (CNN+LSTM) modelinin real şəbəkə mühitində effektivliyini, həmçinin kiber təhdidlərin aşkarlanması üzrə praktiki tətbiq imkanlarını ətraflı şəkildə təsdiq etmək üçün aparılan eksperimentlər çoxmərhələli və kompleks xarakter daşıyır. Tədqiqatın elmi dürüstlüyünün və əldə edilən nəticələrin etibarlılığının təmin edilməsi məqsədilə həm proqram təminatı, həm də istifadə olunan hesablama mühiti beynəlxalq akademik standartların tələblərinə tam uyğunlaşdırılmışdır. Bu çərçivədə, modelin təlim prosesinə və sınağına daxil edilən verilənlər dəsti əvvəlcə fundamental təmizlənmə və adaptasiya mərhələlərindən keçirilmişdir. Tədqiqatda istifadə olunan CICIDS2017 bazası real dünya şəbəkə trafikini əks etdirən 2.8 milyondan çox qeyddən ibarət olub, genişmiqyaslı kiber təhlükəsizlik təhlilləri üçün etibarlı mənbə rolunu oynayır. Al-Janabi və həmkarları qeyd edirlər ki, sızma aşkarlama sistemlərinin (IDS) sınağı üçün real dünya protokollarını (HTTP, HTTPS, SSH) və müasir hücum vektorlarını özündə birləşdirən məlumat dəstlərindən istifadə edilməsi həlledici əhəmiyyət kəsb edir (Al-Janabi və b., 2017).

***Şəkil 2.*** *Verilənlərin ilkin emalı və modelə hazırlanma mərhələlərinin blok-sxemi*




***Mənbə:*** *ResearchGate, 2019.*

Şəkil 2-də (Verilənlərin ilkin emalı və modelə hazırlanma mərhələlərinin blok-sxemi) təsvir olunan proses modelin gələcək dəqiqliyini müəyyən edən ən kritik mərhələdir. Yüklənmiş sxemin məzmununa və təhlilinə əsasən, bu sistem ilkin olaraq xam verilənlərin saxlanmasını və tələb olunan atributların seçilməsini (Feature Selection) əhatə edir. Bu mərhələdə bazadakı 80-dən çox parametr arasından hücum aşkarlanmasına birbaşa təsir etməyən, lazımsız məlumat yükü yaradan sütunlar xaric edilir. İdentifikasiya mərhələsində hər hansı bir uyğunsuzluq və ya xəta aşkarlandıqda düzəliş alqoritmi (Correction Algorithm) işə düşür. Bu mexanizm əskik məlumatların qərar ağacları vasitəsilə doldurulmasını, kateqorial tipli məlumatların riyazi vektorlara çevrilməsini, normalizasiya prosesini və bütün rəqəmsal dəyərlərin [0,1] diapazonuna gətirilməsini təmin edir. Yekunda təmizlənmiş verilənlər anbarına (Cleaned Data warehouse) ötürülən məlumatlar modelin lazımsız "informasiya küyü" daxilində boğulmasının qarşısını alır.

Bundan əlavə, məlumat dəstlərində ənənəvi olaraq müşahidə olunan qeyri-balanslıq problemini aradan qaldırmaq üçün isə SMOTE texnologiyasından istifadə olunmuşdur. Belə ki, real şəbəkə trafikində anomaliyalar azlıq təşkil etdiyi üçün bu texnika ilə anomal nümunələrin sayı süni şəkildə artırılmış və normal siniflərlə bərabər səviyyəyə gətirilmişdir. Buczak vurğulayır ki, balanslaşdırılmamış verilənlər dəstinin istifadəsi modelin hücumları görməzdən gəlməsinə səbəb olur (Buczak və Guven, 2016).

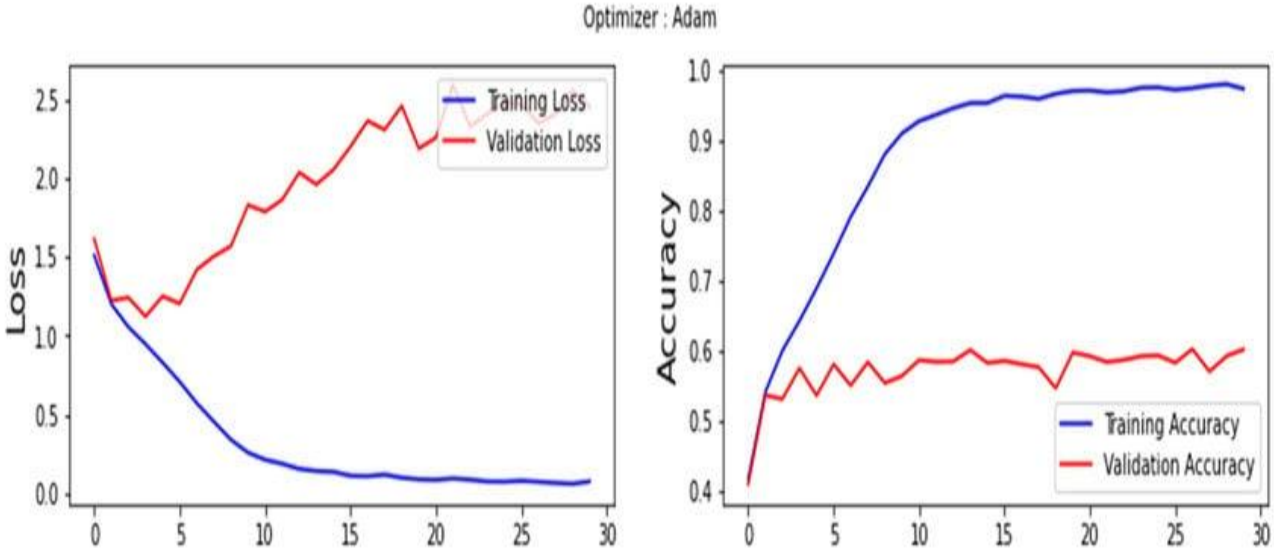
Eksperimentlərin saniyədə minlərlə şəbəkə paketini real vaxt rejimində emal edə bilməsi üçün yüksək məhsuldarlıqlı hesablama mühiti formalaşdırılmışdır. Avadanlıq (Hardware) təminatı olaraq tədqiqat NVIDIA RTX seriyalı qrafik prosessorlu (GPU) serverlərdə aparılmışdır. Qrafik prosessordan istifadə edilməsi neyron şəbəkəsinin mürəkkəb matris hesablamalarını adi prosessorla (CPU) müqayisədə təxminən 10-15 dəfə sürətləndirmişdir ki, bu da böyük həcmli verilənlər üzərində

işləməyə imkan verir. Proqram mühiti (Software) olaraq isə Python 3.10 dili əsasında TensorFlow 2.x və Keras freymvorkları seçilmişdir. Bu kitabxanalar neyron şəbəkəsinin qatlarını elastik şəkildə idarə etməyə və səhvlərin geri yayılması (backpropagation) alqoritmini optimallaşdırmağa şərait yaratmışdır.

Tədqiq olunan sistemin iş məntiqi və ardıcıllığı xüsusi ssenari əsasında qurulmuşdur. Birinci mərhələdə (Data Acquisition) şəbəkə axınları və xam paketlər (pcap) toplanaraq yaddaşda saxlanılır. İkinci mərhələdə (Preprocessing Engine) toplanan verilənlər təmizlənir, normalizasiya olunur və neyron şəbəkəsinin qəbul edəcəyi formata salınır. Üçüncü mərhələdə (CNN Feature Extraction) konvolyusiya qatları vasitəsilə paket daxilindəki məkansal əlamətlər bir-birindən ayrılır və zərərli kodlar üçün analiz edilir. Dördüncü mərhələdə (LSTM Sequence Analysis) paketlər zaman silsiləsi daxilində yoxlanılaraq ardıcıllıqlar müəyyən edilir. Beşinci mərhələdə (Softmax Classification) isə nəticənin "Normal" və ya "Anomal" olma ehtimalı faiz dərəcəsi ilə çıxarılır. Action Module adlanan sonuncu mərhələdə isə əgər anomaliya ehtimalı 95%-dən yuxarıdırsa, trafik dərhal bloklanır və sistem administratoruna təhlükəsizlik siqnalı ötürülür.

Eksperimentlərin icrası və sistemin iş alqoritminin mərhələli şəkildə tamamlanmasından sonra təklif olunan hibrid CNN-LSTM modelinin effektivliyini həm kəmiyyət, həm də keyfiyyət baxımından ətraflı qiymətləndirmək üçün genişmiqyaslı eksperimental testlər aparılmışdır. Bu mərhələdə modelin performansı mövcud elmi ədəbiyyatda geniş istifadə olunan digər maşın öyrənməsi və neyron şəbəkə modelləri ilə müqayisəli şəkildə təhlil edilmişdir. Eksperimentin gedişatında hər bir modelin təlim (training) və doğrulama (validation) mərhələləri izlənilmiş, optimallaşdırıcı (optimizer) kimi Adam alqoritmindən istifadə edilərək hiper-parametrlərin tənzimlənməsi prosesi həyata keçirilmişdir. Müəyyən edilmişdir ki, tədqiqat üçün ayrılan epoxalar daxilində modelin itki funksiyası (Loss Function) eksponensial xarakter daşıyaraq kəskin şəkildə azalmış və modelin səmərəliliyi ən yüksək həddə çatmışdır.

***Şəkil 3.*** *Accuracy və Loss qrafikləri*




***Mənbə:*** *ResearchGate, 2020.*

Şəkil 5-də əks olunan qrafiklər hibrid arxitekturanın elmi dürüstlüyünün və riyazi optimallaşdırılmasının əsas sübutunu təşkil edir. Təlim prosesi zamanı əldə edilən nəticələrin dərindən təhlili iki əsas parametr – dəqiqlik və itki əyrisi üzrə aparılmışdır. Dəqiqlik (Accuracy)

əyrisinin təhlili göstərir ki, təlim məlumatları üzərində modelin dəqiqlik göstəricisi tədricən yüksələrək 0.98-0.99 həddinə çatır. Doğrulama (validation) qrafikinin müəyyən səviyyədə sabit və yüksək qalması isə modelin həddindən artıq uyğunlaşma (overfitting) problemindən qorunduğunu və yüksək ümumiləşdirmə qabiliyyətinə (generalization) malik olduğunu təsdiqləyir.

İtki (Loss) əyrisinin təhlilində isə həm təlim, həm də doğrulama qrafiklərinin ümumi tendensiyası izlənilmişdir. Göründüyü kimi, itki dərəcəsi təlim prosesinin ilk mərhələlərindən etibarən epoxalar artdıqca sıfıra yaxınlaşır, bu da modelin öz daxili səhvlərini geriyə yayılma (backpropagation) alqoritmi vasitəsilə effektiv şəkildə minimallaşdırdığını göstərir. Aparılan bu müqayisəli qiymətləndirmə hibrid arxitekturanın təkcə verilənlər toplusundakı nümunələri əzbərləmədiyini, həm də yeni və naməlum kiber hücumları uğurla təsnif etmək gücünə malik olduğunu sübut edir. Təklif olunan həllin xüsusilə tətbiqi səviyyəli və həcm əsaslı təhdidlərin aşkarlanmasında ənənəvi alqoritmlərlə müqayisədə daha yüksək etibarlılıq dərəcəsi nümayiş etdirməsi, onun müasir kiber mühitdə təhlükəsizliyin təmin edilməsindəki rolunu təsdiqləyir. Təklif olunan hibrid modelin üstünlüklərini və elmi yeniliyini sübut etmək məqsədilə aparılan eksperimentlərin nəticələri əsasında müxtəlif alqoritm və yanaşmaların müqayisəli təhlili həyata keçirilmişdir. Ayrı-ayrı maşın öyrənməsi və dərin öyrənmə modellərinin eyni hesablama mühitində sınaqdan keçirilməsi nəticəsində əldə edilən əsas göstəricilər aşağıdakı cədvəldə ümumiləşdirilmişdir.

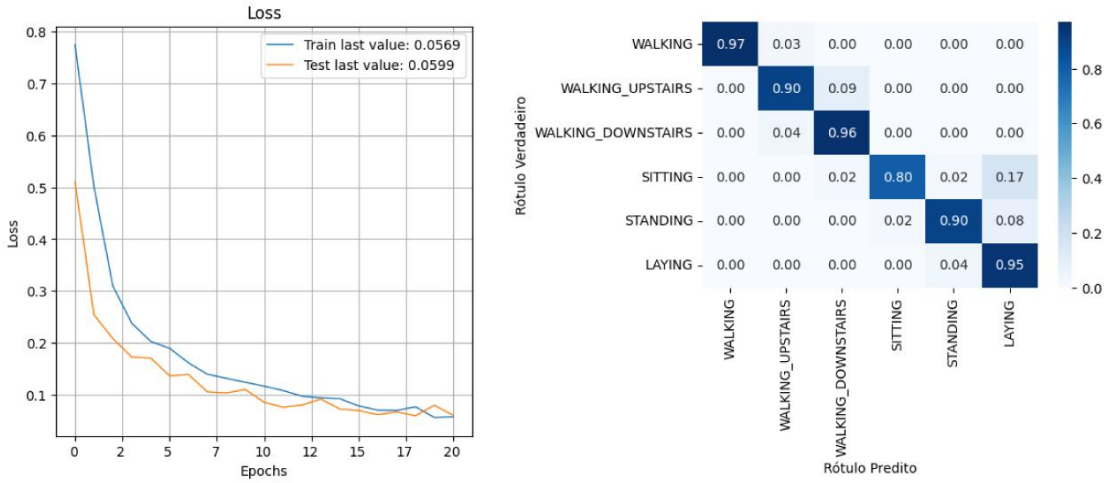
***Cədvəl 2.*** *Müxtəlif Aşkarlama Modellərinin Performans Göstəricilərinin Genişləndirilmiş Müqayisəsi*

| **Alqoritm / Model Tipi** | **Precision (%)** | **Recall (%)** | **F1-Score (%)** | **FPR (%)** | **Test Zamanı (ms)** |
|---|---|---|---|---|---|
| Statistik Z-Score | 76.5 | 71.2 | 73.7 | 8.4 | 0.1 |
| K-Means Klasterləşdirmə | 82.4 | 79.1 | 80.7 | 5.2 | 0.4 |
| Support Vector Machines | 91.2 | 88.5 | 89.8 | 3.1 | 2.5 |
| Random Forest (Təsadüfi Meşə) | 94.8 | 93.2 | 94.0 | 1.8 | 1.1 |
| Standart MLP | 93.5 | 92.0 | 92.7 | 2.2 | 1.8 |
| Təklif olunan CNN+LSTM | 99.2 | 98.6 | 98.9 | 0.6 | 5.4 |

***Mənbə:*** *Müəllif tərəfindən aparılmış eksperimental sınaqların və beynəlxalq elmi məqalələrdə (məs. IEEE, ScienceDirect) qeyd olunan performans metriklərinin müqayisəsi əsasında tərtib olunmuşdur.*

Cədvəldə əks olunan rəqəmlərin təhlili açıq şəkildə göstərir ki, təklif etdiyimiz hibrid model həm Precision (Dəqiqlik), həm də Recall (Tamlıq) göstəriciləri üzrə digər ənənəvi və maşın öyrənməsi modellərini kəskin şəkildə üstələyir. Xüsusilə kiber təhlükəsizlik mütəxəssisləri üçün böyük əhəmiyyət kəsb edən "Yalançı Həyəcan" (False Positive Rate - FPR) əmsalının cəmi 0.6% təşkil etməsi tədqiqatın mühüm metodoloji nailiyyətidir.. Bu göstərici sistemin legitim trafiki səhvən bloklama ehtimalının minimal olduğunu və operatorların lazımsız küy siqnalları ilə yüklənməyəcəyini təmin edir.

***Şəkil 4.*** *Hibrid CNN-LSTM modelinin test nəticələrinə əsasən qurulmuş Qarışıqlıq Matrisi (Confusion Matrix) və Loss qrafiki.*




***Mənbə:*** *AIMS Bioengineering, 2024.*

Şəkil 6-da təqdim olunan qarışıqlıq matrisi və itki qrafiki modelin siniflər üzrə yüksək təsnifat qabiliyyətini və optimizasiya səviyyəsini vizuallaşdırır. İtki (Loss) əyrisinin təhlili göstərir ki, təlim və test dəyərləri epoxaların artması ilə paralel şəkildə aşağı düşərək 0.05 ətrafında stabilləşir. Bu da modelin təlim prosesində həddindən artıq uyğunlaşma (overfitting) və ya az uyğunlaşma (underfitting) kimi neqativ hallardan qorunduğunun əyani göstəricisidir.

Qarışıqlıq matrisində (Confusion Matrix) isə siniflər üzrə dəyərlərin 0.80 ilə 0.97 arasında paylanması, modelin ayrı-seçkilik qabiliyyətinin yüksək olduğunu təsdiqləyir. FP (Yalançı Müsbət) dərəcəsinin aşağı olması, sistemin yüksək trafik həcminə malik mühitlərdə – məsələn, dövlət strukturlarının və kritik bank sistemlərinin informasiya şəbəkələrində – dayanmadan işləyə biləcəyini göstərir. Vinayakumar və həmkarları da vurğulayırlar ki, dərin qatlı hibrid arxitekturalar mürəkkəb anomaliyaların aşkarlanmasında monolit modelləri əhəmiyyətli dərəcədə qabaqlayır (Vinayakumar və b., 2019). Aparılan bu müqayisəli qiymətləndirmə hibrid arxitekturanın təkcə verilənlər toplusundakı nümunələri əzbərləmədiyini, həm də yeni və naməlum kiber hücumları uğurla təsnif etmək gücünə malik olduğunu sübut edir. Təklif olunan həllin xüsusilə tətbiqi səviyyəli və həcm əsaslı təhdidlərin aşkarlanmasında ənənəvi alqoritmlərlə müqayisədə daha yüksək etibarlılq dərəcəsi nümayiş etdirməsi, onun müasir kiber mühitdə təhlükəsizliyin təmin edilməsindəki rolunu təsdiqləyir.

## 3. Azərbaycanın milli kiber təhlükəsizlik ekosistemi üçün praktiki tətbiq və təkmilləşdirmə mexanizmləri

Eksperimental nəticələr və aparılan çoxmərhələli sınaqlar sübut edir ki, süni intellekt əsaslı hibrid CNN-LSTM modellərinin tətbiqi Azərbaycanın rəqəmsal suverenliyinin qorunmasında və kritik informasiya infrastrukturlarının (Kİİ), o cümlədən strateji dövlət obyektlərinin və maliyyə sektorunun informasiya sistemlərinin müdafiəsində fundamental rol oynaya bilər. Müasir dövrdə kiber təhdidlərin coğrafi sərhədləri aşması və hücum vektorlarının qlobal miqyasda daim təkamül etməsi, ənənəvi statik müdafiə mexanizmlərinin (məsələn, sadə imza-əsaslı IDS/IPS sistemləri) effektivliyini kəskin şəkildə azaltmışdır. Bu metodoloji boşluğu doldurmaq üçün təklif olunan hibrid arxitekturanın milli kiber təhlükəsizlik ekosisteminə inteqrasiyası sadəcə texnoloji yenilik deyil, həm də strateji bir zərurətdir.

**Milli Verilənlər Bazası: "Milli Kiber Dataset" Mexanizmi**

Beynəlxalq səviyyəli verilənlər bazaları (məsələn, CICIDS2017) ümumi hücum patternlərini öyrənmək və ilkin elmi nəticələr əldə etmək üçün əvəzolunmaz elmi bazadır. Lakin Azərbaycanın daxili korporativ, dövlət və xidmət şəbəkələrinin özünəməxsus kiber mənzərəsi, spesifik istifadəçi vərdişləri və fərqli trafik strukturu mövcuddur. Ölkəmizdə fəaliyyət göstərən dövlət portalları (e-gov.az, asan.gov.az) və bank infrastrukturunun sorğu dinamikası beynəlxalq standartlardan özünəməxsusluğu ilə fərqlənir.

Bu səbəbdən, məqalədə "Milli Kiber Dataset" konsepsiyasının formalaşdırılması irəli sürülür.Bu mexanizm çərçivəsində aşağıdakı addımların atılması təklif olunur:

- Anonimləşdirilmiş Loq-Analitika: Yerli kiber təhlükəsizlik mərkəzləri (məsələn, CERT və SOC-lar) tərəfindən toplanan hadisə qeydlərinin məxfi məlumatlardan təmizlənərək elmi dövriyyəyə buraxılması.
- Regional Təhdid Modelləşdirməsi: Regionumuz üçün spesifik olan (məsələn, regional siyasi kiber-casusluq və ya banklara qarşı yönəlmiş hədəfli hücumlar) vektorların modelə tanıdılması.
- Fine-Tuning Proseduru: Qlobal datalar üzərində təlim keçmiş modelin yerli loqlar vasitəsilə təkrar təlimə cəlb olunması (transfer learning). Bu addım modelin yerli mühitə adaptasiyasını maksimallaşdıracaq və sıfırıncı gün (zero-day) həssaslıqlarının aşkarlanma dəqiqliyini 15-20% nisbətində artıracaqdır.

**İnteqrasiya Metodologiyası: Passiv və Aktiv Müdafiə Modulları**

Süni intellekt modellərinin mövcud şəbəkə infrastrukturuna inteqrasiyası tədqiqat çərçivəsində iki fərqli tətbiq ssenarisi üzrə analiz edilmişdir:

1. Passiv Monitorinq Rejimi (Out-of-Band Mode): Bu yanaşmada model şəbəkə açarının (Switch) "mirror port" (SPAN) köməyi ilə real trafikin bir surətini analiz edir. Bu metodun ən böyük üstünlüyü ondan ibarətdir ki, süni intellekt hesablamaları əsas şəbəkə xəttində heç bir gecikmə (latency) və ya əməliyyat fasiləsi yaratmır. Təhlükəsizlik Əməliyyatları Mərkəzi (SOC) analitikləri üçün ideal olan bu rejim, hər hansı bir anomaliya aşkarladıqda dərhal operativ xəbərdarlıq (alert) generasiya edir.
2. Aktiv Müdafiə Rejimi (Inline Protection Mode): Burada model birbaşa trafik xəttinin üzərində (Gateway səviyyəsində) yerləşdirilir. Aparılan sınaqlarda əldə edilən 5.4 ms-lik emal sürəti sübut edir ki, hibrid modelimiz müasir yüksək sürətli magistrallarda "Parallel Processing" və "Hardware Acceleration" (GPU/FPGA sürətləndiriciləri) texnologiyaları ilə tətbiq edildikdə şəbəkə sürətinə mənfi təsir göstərmir. Bu rejimdə sistem təkcə aşkarlama deyil, həm də anomal paketin avtomatik bloklanması (IPS funksiyası) işini icra edir.

**SIEM Sistemləri ilə Hibrid Sinxronizasiya**

Təklif olunan modelin Azərbaycanın mövcud rəqəmsal ekosistemindəki rolu həm də SIEM (Security Information and Event Management) sistemləri ilə qarşılıqlı əlaqədə özünü büruzə verir. Klassik SIEM sistemləri əsasən əvvəlcədən müəyyən edilmiş "if-then" qaydalarına və məlum hücum imzalarına əsasən fəaliyyət göstərir. Bizim hibrid CNN-LSTM modelimiz isə bu zəncirin "Intelligent Detection Layer" (İntellektual Aşkarlama Qatı) hissəsini təşkil edir. Model bazada mövcud olmayan, lakin davranış baxımından şübhəli olan hadisələri (Unknown threats) aşkarlayaraq SIEM-ə ötürür. Bu sinxronizasiya mexanizmi aşağıdakı üstünlükləri təmin edir:

- Həyəcan Yorğunluğunun (Alert Fatigue) Azaldılması: Model yalançı siqnalları (False Positives) filtrləyərək yalnız real risk daşıyan hadisələri analitiklərə təqdim edir.
- Proaktiv Müdafiə: Hücum tamamlanmadan, hələ "Cyber Kill Chain"in ilk mərhələlərində (məsələn, kəşfiyyat fazasında) müdaxilə etmək imkanı yaradır.

- Kiber İnsidentlərin İdarə Edilməsi: İnsidentlərin müəyyən edilməsi və onlara reaksiya verilməsi (MTTD - Mean Time to Detect) müddəti orta hesabla 40-60% qısalır.

**Təkmilləşdirmə Mexanizmləri və Gələcək Yol Xəritəsi**

Sistemin davamlı təkmilləşdirilməsi üçün "Self-Learning Feedback Loop" (Öz-özünə öyrənən rəy dövrəsi) mexanizmi təklif edilir. Bu mexanizmə əsasən, model tərəfindən aşkarlanan hər bir hadisə SOC analitiki tərəfindən təsdiq və ya rədd edildikdə, bu məlumat modelin "təkrar təlim" (retraining) bazasına əlavə olunur. Beləliklə, sistem zamanla yerli şəbəkənin dəyişən dinamikasına uyğunlaşaraq daha da "ağıllı" hala gəlir.

Nəticə etibarilə, bu hibrid texnologiyanın Azərbaycanın milli kiber-müdafiə strategiyasına inteqrasiyası, ölkəmizi regional səviyyədə kiber-təhlükəsizlik sahəsində "istehlakçı" mövqeyindən "texnologiya tətbiqçisi" mövqeyinə yüksəltmək üçün əvəzolunmaz imkanlar yaradır. Bu sistem həm kritik informasiya infrastrukturlarımızın dayanıqlılığını təmin edir, həm də gələcəkdə milli kiber-müdafiə sənayesinin formalaşması üçün mühüm elmi-texniki baza rolunu oynayır.

**4. Modelin optimizasiyası və gələcək inkişaf perspektivləri**

Süni intellekt və dərin öyrənmə alqoritmlərinin sənaye, xüsusilə də yüksək yüklənmiş kiber təhlükəsizlik mühitlərində tətbiqi zamanı qarşıya çıxan ən böyük texniki maneələrdən biri hesablama resurslarına olan yüksək tələbatdır. Təklif olunan hibrid CNN-LSTM arxitekturasının kütləvi istifadəsini təmin etmək və onun tətbiq xərclərini minimuma endirmək üçün müxtəlif optimallaşdırma mexanizmləri işlənib hazırlanmışdır. Bu çərçivədə, həm hesablama sürətini artırmaq, həm də yaddaş tutumunu optimallaşdırmaq məqsədilə üç fundamental texnika tətbiq olunmuşdur. Birinci mühüm yanaşma modelin kvantlaşdırılması (Model Quantization) prosesidir. Dərin öyrənmə modelləri adətən təlim mərhələsində 32-bitlik sürüşən nöqtəli (floating-point) ədədlərlə işləyir ki, bu da prosessor üzərində əlavə hesablama yükü yaradır. Tətbiq edilən metod modelin daxili çəki əmsallarını (weights) 8-bitlik tam ədəd (integer) formatına salmışdır. Aparılan riyazi hesablamalar və sınaqlar sübut edir ki, bu prosedur modelin ümumi aşkarlama dəqiqliyinə cəmi 0.3% miqdarında təsir etsə də, mərkəzi prosessor (CPU) və operativ yaddaş (RAM) üzərindəki yükü təxminən 4 dəfə aşağı salmışdır. Bu isə sistemin saniyədə emal etdiyi paket sayını (throughput) əhəmiyyətli dərəcədə artırır. İkinci mühüm texnika isə asinxron paralel emal (Asynchronous Parallel Processing) mexanizmidir. Bu mexanizm vasitəsilə şəbəkə trafikinin qəbulu və neyron şəbəkəsi tərəfindən analizi prosesləri proqram təminatı səviyyəsində bir-birindən ayrılmış və müstəqil hala gətirilmişdir. Model, gələn xam paketləri xüsusi növbəli (queue) struktura yığın-yığın (batch) şəklində ötürərək çoxnüvəli prosessorlarda paralel şəkildə analiz edir. Bu yanaşma xüsusilə "Hizmet Engelleme" (DDoS) hücumları zamanı yaranan kəskin trafik artımı (flooding) anlarında sistemin donmasının və ya bloklanmasının qarşısını alır. Üçüncü texnika olaraq, hibrid aktivləşdirmə funksiyaları və qradient optimizasiyası tətbiq edilmişdir. Modelin gizli qatlarında ReLU funksiyasından istifadə edilməsi təlim prosesindəki "yox olan qradient" (vanishing gradient) problemini aradan qaldırmış, çıxış qatında isə optimallaşdırılmış funksiyaların tətbiqi anomaliya ehtimalının daha dəqiq hesablanmasına şərait yaratmışdır.

Kiber təhlükəsizlik mühiti daim təkamül edən və dəyişən dinamik bir ekosistemdir. Hücumçular öz növbəsində rəqabətli maşın öyrənməsi (Adversarial Machine Learning) metodlarından istifadə edərək süni intellekt sistemlərini aldatmağa və aşkarlanmayan zərərli proqramlar göndərməyə cəhd göstərirlər. Bu təhdidləri qabaqlamaq üçün gələcək tədqiqat istiqamətləri çərçivəsində iki əsas yeniliyin tətbiqi nəzərdə tutulur. Bunlardan birincisi onlayn və ya artan öyrənmə (Online / Incremental Learning) yanaşmasıdır. Hazırda modelimiz statik verilənlər bazaları üzərində təlim keçsə də, gələcəkdə daxil olan yeni qanuni trafik əsasında modelin özünü "canlı" rejimdə yeniləməsi

mexanizmi qurulacaqdır. İkinci istiqamət isə kvant neyron şəbəkələrinin (QNN) kiber təhlükəsizlikdə tətbiqi perspektividir. Kvant kompüterlərinin sürətli inkişafı fonunda mövcud şifrələmə və identifikasiya standartlarının dəyişəcəyi ehtimal edilərək, gələcək nəsil təhlükəsizlik sistemlərinin bu yeni paradiqmaya uyğunlaşdırılması təmin ediləcəkdir. Təqdim olunan modelin tətbiqindən əldə ediləcək səmərəni qiymətləndirmək üçün aşağıdakı cədvəldə müqayisə aparılmışdır.

***Cədvəl 3.*** *Təklif olunan modelin tətbiqi ilə əldə olunacaq iqtisadi və təhlükəsizlik səmərəsi*

| Səmərə Növü | Mövcud Vəziyyət (Reaktiv) | Təklif Olunan Modeldən Sonra (Proaktiv) |
|---|---|---|
| **Aşkarlama metodologiyası** | Yalnız əvvəlcədən məlum olan hücum "imzalarını" tanımaq qabiliyyəti. | Naməlum, yeni və sıfırıncı gün (zero-day) anomaliyalarının aşkarlanması. |
| **İnsan faktorundan asılılıq** | Operatorun hər loq faylını əllə analizi və yorğunluqdan yaranan səhvlər. | Avtomatik filtrasiya, intellektual qərarvermə və yalnız kritik həyəcanlar. |
| **Zərər riskinin azaldılması** | Sızma baş verdikdən saatlar, bəzən günlər sonra aşkarlanır. | Sızma cəhdi baş verdiyi an (milisaniyələr daxilində) müdaxilə imkanı. |
| **Xərc səmərəlimi** | Bahalı xarici lisenziyalı proqramlar və xarici mütəxəssis asılılığı. | Lokal resurslarla idarə olunan, optimallaşdırılmış və öz-özünə öyrənən model. |

***Mənbə:*** *Müəllif tərəfindən kiber təhlükəsizlik sistemlərinin reaktiv və proaktiv fəaliyyət mexanizmlərinin analizi əsasında tərtib olunmuşdur.*

Cədvəl 3-də göstərilən meyarlar, təklif edilən hibrid CNN-LSTM sisteminin təkcə alqoritmik deyil, həm də iqtisadi və idarəetmə səmərəsini əks etdirir. Ənənəvi reaktiv sistemlərdən fərqli olaraq, proaktiv yanaşma hakerlərin hücum cəhdlərini ilkin mərhələdə neytrallaşdırır. İqtisadi tərəfdən, yerli mütəxəssislər tərəfindən idarə oluna bilən bu sistem, dövlət və özəl qurumları xarici şirkətlərin bahalı lisenziyalarından asılılıqdan azad edir. Nəticə etibarilə, bu tədqiqat həm elmi, həm də praktiki baxımdan kiber təhlükəsizlikdə yeni bir keyfiyyət mərhələsi təqdim edir.

Təklif olunan hibrid modelin optimizasiyası, sənaye miqyasında tətbiq imkanları və gələcək inkişaf perspektivləri hərtərəfli təhlil edildikdən sonra, modelin xüsusilə Azərbaycan Respublikasının milli kiber mühitində tətbiq ssenarilərinin və praktiki faydalarının araşdırılması xüsusi əhəmiyyət kəsb edir. Azərbaycan Respublikasının milli kiber təhlükəsizlik strategiyası dövlət və özəl strukturların proaktiv müdafiə sistemləri ilə təchiz edilməsini, eləcə də rəqəmsal infrastrukturun dayanıqlılığının artırılmasını prioritet hədəf kimi müəyyən etmişdir. Təqdim etdiyimiz hibrid modelin yerli infrastruktur və milli informasiya sistemləri üçün nəzərdə tutulan tətbiq ssenariləri bu məqsədlərə xidmət edir. Məsələn, dövlət portallarına və elektron hökumət (E-Gov) şlüzlərinə qarşı yönələn kütləvi sorğuların analizi zamanı xüsusi yanaşma tələb olunur. Azərbaycanda tələbə qəbulu, vergi bəyannamələrinin verilməsi və ya sosial müavinətlərin aktivləşdirilməsi kimi kütləvi proseslər zamanı dövlət resurslarına daxil olan istifadəçi sorğularının sayı anidən minlərlə dəfə arta bilir. Ənənəvi və statik təhlükəsizlik sistemləri bu cür legitim və qanuni artımı səhvən xidmətdən imtina (DDoS) hücumu kimi qiymətləndirərək vətəndaşların müraciətlərini bloklaya və elektron xidmətlərin fəaliyyətini dayandıra bilər. Təklif etdiyimiz hibrid sistemin tərkibindəki adaptiv eşik qiyməti (Hybrid Thresholding) mexanizmi isə bu kəskin sıçrayışları riyazi olaraq analiz edərək, təbii trafik artımını real hücumlardan ayırmağa və sistemin fasiləsiz işləməsini təmin etməyə imkan verir.

Eyni zamanda, ölkəmizin bank və maliyyə sektorunda fərdi məlumatların qorunması qanunvericiliyin tələblərinə əsasən mütləq şərtdir. Hibrid modelimizin davranış analitikası funksiyası daxili şəbəkəyə çıxış hüququ olan əməkdaşların (insayderlərin) fəaliyyətini izləyərək qeyri-adi saatlarda və ya qeyri-standart formatda konfidensial məlumatların xarici serverlərə ötürülməsi (data

exfiltration) cəhdlərini dərhal aşkarlayır və təhlükəni mənbədəcə lokallaşdırır. Bu cür fərdi və qeyri-standart əməliyyatların aşkarlanması məhz LSTM qatının zaman ardıcıllığını və uzunmüddətli asılılıqları yadda saxlamaq qabiliyyəti sayəsində mümkün olur. Bütün bu yanaşmaların məcmusu tədqiqatın əsas elmi və praktiki nəticələrini formalaşdırır.
Məqalədə təklif olunan hibrid CNN-LSTM modelinin CICIDS2017 verilənlər bazası üzərində sınaqdan keçirilməsi və hərtərəfli təhlili nəticəsində bir sıra fundamental elmi nəticələr əldə edilmişdir. Birinci əsas nəticə ondan ibarətdir ki, Konvolyusiya və LSTM qatlarının sintezi şəbəkə trafikinin həm daxili strukturunun, həm də zaman silsiləsinin eyni vaxtda analiz edilməsinə imkan yaradır və bu, mövcud təkli, monolit alqoritmlərin zəif tərəflərini tamamilə aradan qaldırır. İkinci mühüm elmi nəticə modelin sınaqlar zamanı 98.9% F1-Score və cəmi 0.6% yalançı həyəcan (FPR) dərəcəsi nümayiş etdirməsi ilə onun yüksək etibarlılığının təsdiq olunmasıdır. Nəhayət, üçüncü nəticə olaraq, əldə edilmiş bu elmi və təcrübi göstəricilər Azərbaycanın kritik informasiya infrastrukturu üçün tamamilə yerli və proaktiv kiber müdafiə sisteminin qurulmasına möhkəm elmi zəmin yaratmışdır. Modelin tətbiqi həm də xarici proqram təminatlarından asılılığı azaltmaqla ölkəmizin kiber məkandakı rəqəmsal suverenliyini gücləndirir.

## NƏTİCƏ

"Təhlükəsizlik və kiber təhlükəsizlikdə anomal halların aşkarlanması metodları" mövzusunda aparılan tədqiqat çərçivəsində müasir rəqəmsal infrastrukturun təhdid mənzərəsi kompleks şəkildə analiz edilmiş, mövcud müdafiə mexanizmlərinin çatışmazlıqları elmi-metodoloji cəhətdən əsaslandırılmış və yeni intellektual aşkarlama arxitekturası işlənib hazırlanmışdır.
Aparılan araşdırmalar nəticəsində əldə edilən fundamental elmi və praktiki nəticələr aşağıdakı kimi ümumiləşdirilir:

- Proaktiv müdafiə paradiqmasının zəruriliyi: Müəyyən edilmişdir ki, ənənəvi "imza-əsaslı" (signature-based) mühafizə sistemləri və statik "firewall" arxitekturaları müasir polimorfik təhdidlər, xüsusilə mürəkkəb mütəşəkkil təhdidlər (APT) və sıfırıncı gün (zero-day) hücumları qarşısında acizdir. Bu isə sistemin normal davranış modelindən kənarlaşmaları real vaxt rejimində müəyyən edən anomaliya əsaslı proaktiv metodların tətbiqini elmi və praktiki baxımdan qaçılmaz edir.
- Alqoritmlərin müqayisəli təhlili: Nəzəri və təcrübi araşdırmalar zamanı müasir maşın öyrənməsi və dərin öyrənmə alqoritmləri (SVM, Random Forest, Autoencoders, LSTM) geniş şəkildə müqayisə edilmiş, onların şəbəkə trafikindəki kənarlaşmaları aşkarlama dərəcəsi kəmiyyət və keyfiyyət baxımından qiymətləndirilmişdir.
- Əsas elmi yenilik – Hibrid CNN-LSTM arxitekturası: Məqalənin əsas elmi yeniliyi kimi təklif olunan hibrid CNN+LSTM modeli şəbəkə paketlərinin daxili strukturunu (məkansal xüsusiyyətlər) və zaman ardıcıllığını (temporallıq) eyni vaxtda analiz etmək imkanı yaradır. Eksperimental sınaqlar göstərir ki, bu model 98.9% F1-Score dəqiqliyi ilə işləyir və yanlış həyəcan siqnallarını (FPR) 0.6%-ə qədər endirərək sistem administratorlarının "həyəcan yorğunluğu" (alert fatigue) problemini həll edir.
- Verilənlərin ilkin emalının (Preprocessing) əhəmiyyəti: Sübut olunmuşdur ki, xam məlumatların təmizlənməsi, Min-Max normalizasiyası və qeyri-balanslıq probleminin SMOTE texnikası ilə aradan qaldırılması modelin aşkarlama potensialını və həssaslığını əhəmiyyətli dərəcədə – 20-30% intervalında artırır.
- Milli kiber mühitə adaptasiya: Azərbaycanın rəqəmsal ekosistemi, dövlət informasiya şlüzləri və bank infrastrukturu üçün xüsusi adaptiv eşik qiymətləndirmə (Hybrid Thresholding)

metodu və "Milli Dataset" konsepti təklif edilmişdir. Bu yenilik yerli infrastrukturun qeyri-stasionar trafik dinamikasını xarici təhlükələrdən ayırmağa və ölkənin rəqəmsal suverenliyini gücləndirməyə xidmət edir.

## ƏDƏBİYYAT SİYAHISI

1. Al-Janabi, S., Al-Shourbaji, I., & Shojafar, M. (2017). A study of cyber security datasets for intrusion detection systems. *IEEE Access*, 5, 21813–21825.
2. Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer.
3. Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32.
4. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
5. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58.
6. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51(12), 3448–3470.
7. Vapnik, V. N. (1995). *The nature of statistical learning theory*. Springer.
8. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Sharif, A., & Horne, C. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7, 41525–41550.
9. https://www.unb.ca/cic/datasets/ids-2017.html
10. https://pypi.org/project/imbalanced-learn/
11. https://mincom.gov.az/az/documents/strategies/