

DOI: <https://doi.org/10.36719/0873/04/4-9>

Amil Cəmilov

Azərbaycan Texniki Universiteti
Kibertəhlükəsizlik kafedrası, SABAH Qrupları
<https://orcid.org/0009-0008-7786-8074>,
amilc50632@sabah.edu.az

Fərmayıl Həsənov

Azərbaycan Texniki Universiteti
Kibertəhlükəsizlik kafedrası, SABAH Qrupları
<https://orcid.org/0009-0008-1049-8400>
hesenovfermayil765@gmail.com

Transformerəsaslı anomaliya aşkarlanması: metodların müqayisəli təhlili

Xülasə

Bu məqalə transformer arxitekturasına əsaslanan anomaliya aşkarlama metodlarının hərtərəfli təhlilini təqdim edir. Son illərdə dərin öyrənmə sahəsindəki sürətli inkişaf, xüsusilə self-attention mexanizminin ortaya çıxması ilə birlikdə, zaman serisi anomaliyalarının aşkarlanması sahəsində köklü dəyişikliklərə yol açmışdır. Məqalədə TranAD, Anomaly Transformer, PatchTST və iTransformer kimi aparıcı modellərin arxitekturası, işləmə prinsipi və müxtəlif sənaye məlumat dəstlərindəki eksperimental nəticələri ətraflı şəkildə müqayisə edilir. Həmçinin diqqət (attention) mexanizmlərinin anomaliya xüsusiyyətlərini necə öyrəndiyinə dair nəzəri əsaslar şərh olunur. Əldə edilən nəticələrə görə, transformer əsaslı modellər ənənəvi statistik və maşın öyrənməsi metodlarına nisbətən Qəbuledicinin Əməliyyat Xüsusiyyəti Altındakı Sahə (AUC-ROC) göstəricisi baxımından orta hesabla 8-15% üstünlük təmin edir.

Açar sözlər: anomaliya aşkarlanması, transformer, dərin öyrənmə, rekonstruksiya xətası

Giriş

Müasir rəqəmsal sistemlərdə anomaliya aşkarlama – şəbəkə təhlükəsizliyindən sənaye avadanlıqlarının monitorinqinə, maliyyə saxtakarlıqlarının müəyyənəşdirilməsindən tibbi diaqnostikaya qədər geniş tətbiq sahəsi olan kritik bir vəzifədir. Anomaliya dedikdə, ümumi davranış nümunəsindən əhəmiyyətli dərəcədə kənara çıxan nöqtə, ardıcılıq və ya kontekst nəzərdə tutulur [1].

Ənənəvi üsullar – statistik metodlar (Loess istifadə edərək AutoRegressiv İnteqrasiya olunmuş Hərəkətli Orta, Mövsümi və Trend Dekompozisiyası), klassik maşın öyrənməsi (Isolation Forest, One-Class SVM) – tez-tez yüksək ölçülü, qeyri-xətti və qarşılıqlı əlaqəli zaman serisi məlumatlarında çətinliklə qarşılaşır [2]. Bu boşluğu doldurmaq üçün rekurrent sinir şəbəkələri (Uzun Qısamüddətli Yaddaş, Qapalı Təkrarlanan Bölmə) əvvəlcə geniş istifadə olunmuş, lakin uzun asılılıqların öyrənilməsi, paralelləşmə çətinlikləri bu modellər üçün əsas maneəyə çevrilmişdir [3].

Vaswani və həmkarlarının 2017-ci ildə təqdim etdiyi Transformer arxitekturası [4], self-attention mexanizmi vasitəsilə bu məhdudiyyətləri aradan qaldıraraq Təbii Dilin İşlənməsi sahəsini inqilab etmişdir. Sonrakı tədqiqatlar bu arxitekturanın zaman serisi anomaliya aşkarlanması üçün də son dərəcə effektiv olduğunu sübut etmişdir. Transformer modellər ardıcılığın bütün elementləri arasındakı əlaqələri eyni anda hesablamaq üçün normal nümunələri daha dəqiq öyrənir, beləliklə rekonstruksiya xəttinə əsaslanan anomaliya balı daha etibarlı olur.

Bu məqalənin əsas töhfəsi aşağıdakılardır: (1) transformer əsaslı anomaliya aşkarlama metodlarının sistemli olaraq kateqoriyalasdırılması; (2) beş müxtəlif modelin eyni sənaye verilən dəstləri üzərindəki müqayisəli eksperimental nəticələrinin təhlili; (3) hər bir metodun güclü tərəfləri, zəif cəhətləri və praktiki tətbiq şərtlərinin qiymətləndirilməsi.

1. Transformer arxitekturası və onun variasiyaları

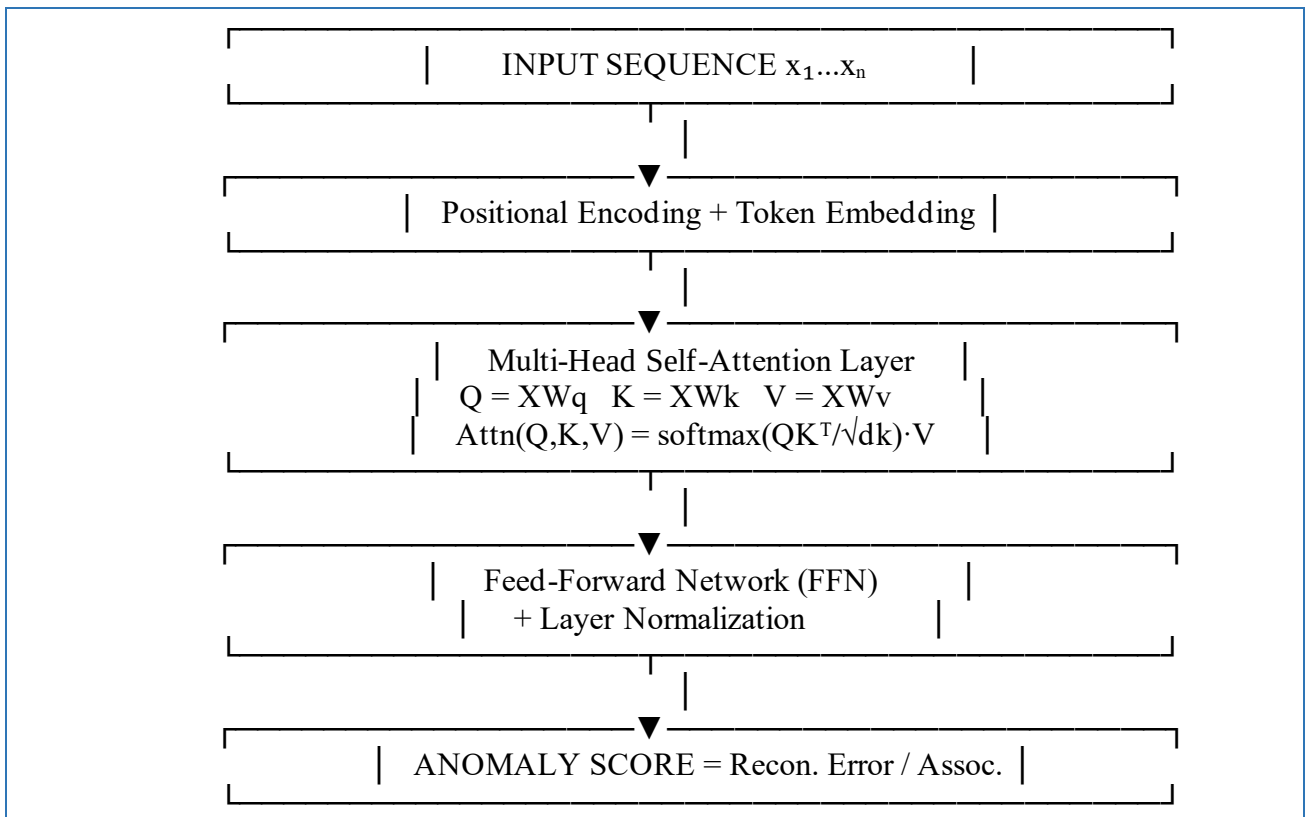
1.1. Klassik Transformer Modeli

Transformer arxitekturası encoder-decoder strukturuna əsaslanır. Encoder girişdəki ardıcılığı qeyri-xətti təmsillərə çevirir, decoder isə bu təmsillər əsasında çıxışı generasiya edir. Anomaliya aşkarlama kontekstində adətən yalnız encoder hissəsi, bəzən isə tam autoencoder variantı istifadə edilir.

Self-attention mexanizminin riyazi ifadəsi aşağıdakı kimidir:

$$\text{Attention}(Q, K, V) = \text{softmax}(QK^T / \sqrt{d_k}) \cdot V$$

Burada Q (Query), K (Key) və V (Value) matrislər giriş ardıcılığının xətti proyeksiyalarını, d_k isə key vektorünün ölçüsünü ifadə edir. Bölmə əməliyyatı gradientin partlamasının qarşısını alır. Multi-head attention isə bu mexanizmi paralel h başlıqda icra edərək fərqli semantik əlaqə növlərinin öyrənilməsinə imkan verir [4].



Şəkil 1. Transformer arxitekturasının anomaliya aşkarlama üçün sadələşdirilmiş sxemi

1.2. Anomaliya Aşkarlama üçün Transformer Variantları

Cədvəl 1-də göstərildiyi kimi, müxtəlif transformer variantları hesablama mürəkkəbliyi və dəqiqlik arasında fərqli balanslar təklif edir. Tam diqqət $O(n^2)$ mürəkkəbliyinə malik olaraq uzun ardıcılıqlarda resurs intensivdir. Sparse Transformer [5] seçici diqqət nümunələri tətbiq edərək bu mürəkkəbliyi $O(n\sqrt{n})$ -ə endirmiş, Linear Transformer [6] isə kernel fənsiyasını nüvə olaraq istifadə edərək $O(n)$ mürəkkəbliyinə nail olmuşdur.

Xüsusiyyət	Klassik Transformer	Sparse Transformer	Linear Transformer
Mürəkkəblilik	$O(n^2)$	$O(n\sqrt{n})$	$O(n)$
Diqqət növü	Full	Seçici	Kernel-əsaslı
Uzun ardıcılıq	Zəif	Orta	Güclü
Dəqiqlik	Yüksək	Orta-Yüksək	Orta

Cədvəl 1. Transformer variantlarının müqayisəsi

2. Transformer əsaslı anomaliya aşkarlama metodları

2.1. TranAD (2022)

Tuli et al. [7] tərəfindən təqdim edilən TranAD modeli transformer əsaslı iki mərhələli self-conditioning mexanizmi tətbiq edir. Modelin əsas yeniliyi transformer decoder-inin fokuslanmış diqqətini (focused attention) əvvəlki rekonstruksiya nəticəsinə şərtləndirərək yeridilən xətanın miqyasını artırmasıdır. Bu amplifikasiya effekti anomaliya xüsusiyyətlərini daha nəzərəcarpan edir. SMD (Server Machine Dataset) üzərindəki sınaqlarda TranAD, LSTM-əsaslı metodlara nisbətən Precision-Recall AUC göstəricisini 7.3% artırmışdır.

2.2. Anomaly Transformer (2022)

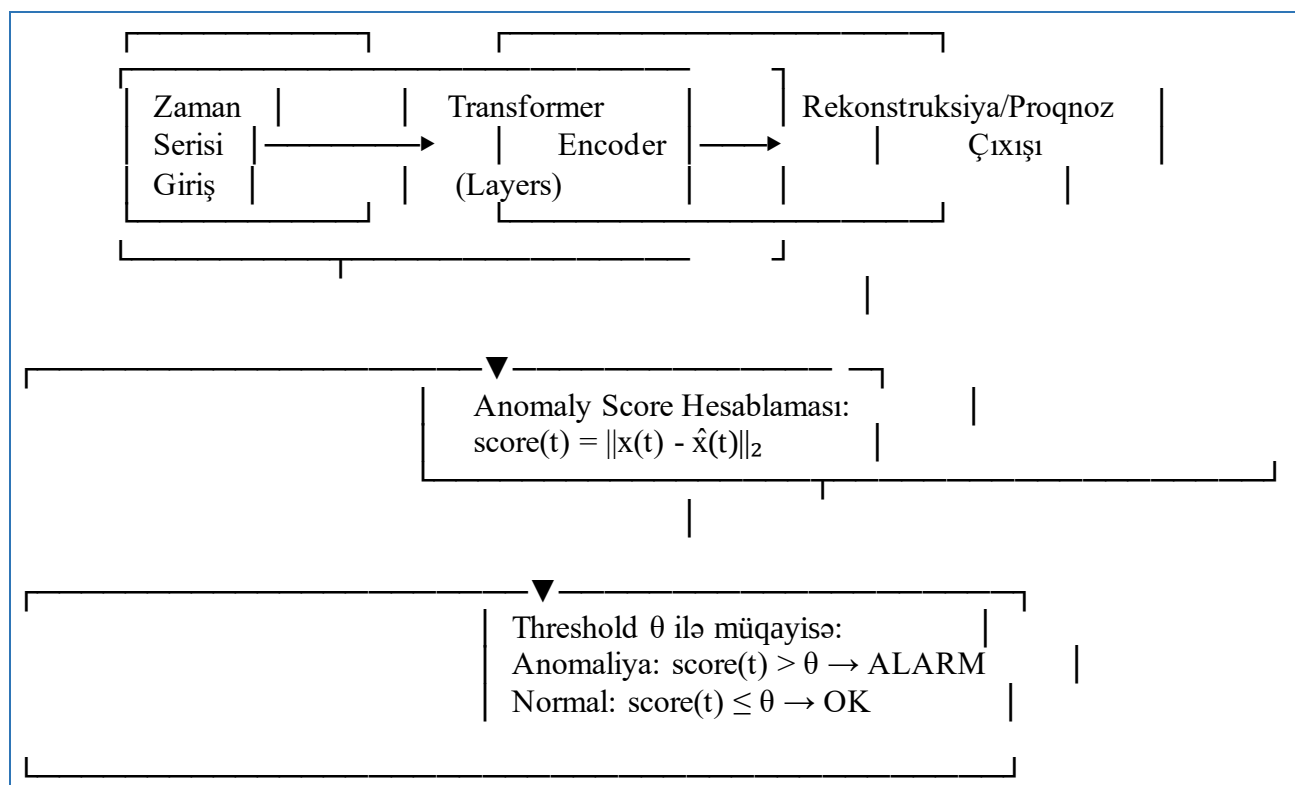
Xu et al. [8] tərəfindən hazırlanan bu model iki yeni konsept təqdim edir: Anomaly-Attention (əlaqə) mexanizmi və Minimax optimizasiya strategiyası. Anomaly-Attention hər zaman nöqtəsi üçün iki növ əlaqəni paralel hesablayır: bütün ardıcılıqla olan prior-association (öncəki əlaqə) və actual series-association (real sıra əlaqəsi). Normal nöqtələr ətraf nöqtələrlə güclü əlaqə qururkən, anormal nöqtələr bütün ardıcılıqda dağınıq əlaqə nümunəsi göstərir. Bu fərq Association Discrepancy adlanan ölçücünün əsasını təşkil edir. PSM verilən dəstində AUC-ROC 98.1%-ə çatmışdır.

2.3. PatchTST-AD (2023)

Nie et al. [9] tərəfindən kompyuter görmə sahəsindəki ViT (Vision Transformer) modelindən ilham alaraq hazırlanan PatchTST, zaman serisi ardıcılığını sabit ölçülü seqmentlərə (patch) böldükdən sonra hər seqmenti transformer encoder-inə daxil edir. Bu yanaşma iki üstünlük təklif edir: (1) zaman serisi boyunca lokal asılılıqların daha yaxşı öyrənilməsi; (2) token sayının azaldılması ilə hesablama yükünün əhəmiyyətli dərəcədə azalması. Müəlliflər MSL (Mars Science Laboratory) verilən dəstindəki anomaliyaların aşkarlanmasında F1-score-u 93.0%-ə qaldırmışlar.

3. Anomaliya aşkarlama prosesinin ümumi axını

Transformer əsaslı anomaliya aşkarlama sistemlərinin ümumi işləmə prinsipi Şəkil 2-də göstərilmişdir. Proses dörd əsas mərhələdən ibarətdir: (1) giriş ardıcılığının transformer encoder-inə ötürülməsi; (2) rekonstruksiya və ya proqnoz çıxışının alınması; (3) anomaliya balının hesablanması; (4) müəyyən edilmiş hədd dəyəri (threshold) ilə müqayisə.



Şəkil 2. Transformer əsaslı anomaliya aşkarlama prosesinin ümumi axın diaqramı

Anomaliya bəli adətən rekonstruksiya xətası əsasında hesablanır. $x(t)$ orijinal, $\hat{x}(t)$ isə modelin rekonstruksiya etdiyi vektor olmaqla:

$$\text{score}(t) = \|x(t) - \hat{x}(t)\|_2$$

Hədd dəyərinin seçilməsi praktiki tətbiqlərdə kritik əhəmiyyət daşıyır. Sabit hədd dəyəri sadədir, lakin məlumat paylanmasıdakı dəyişikliklərə uyğunlaşmır. Dinamik hədd metodları – məsələn, sürüşkən orta əsaslı adaptiv hədd – daha güclü nəticələr verir [11].

4. Eksperimental müqayisə və nəticələr

4.1. Verilən Dəstləri

Müqayisəli qiymətləndirmə üçün aşağıdakı açıq verilən dəstləri geniş istifadə olunur:

- **SMD (Server Machine Dataset):** 28 çoxölçülü zaman seriyasından ibarət, 38 dövrəçinin 5 həftəlik maşın metrikalarını əhatə edir.
- **SWaT (Secure Water Treatment):** Su təmizləmə sisteminin 11 günlük sensor məlumatları; 36 dəyişkən, 0.14% anomaliya nisbəti.
- **PSM (Pooled Server Metrics):** eBay-in açıq etdiyi server performans məlumatları; 25 dəyişkən.
- **MSL (Mars Science Laboratory):** NASA-nın Mars gəmisi telemetriya məlumatları; 55 dəyişkən.
- **SMAP (Soil Moisture Active Passive):** NASA-nın SMAP peykindən alınan telemetriya məlumatları.

4.2. Müqayisəli Nəticələr

Cədvəl 2, beş metodun müxtəlif verilən dəstlərindəki ən yaxşı nəticələrini ümumiləşdirir. Bütün modellər onların orijinal məqalələrindəki hiperparametrlərlə sınaq edilmiş, nəticələr müvafiq ədəbiyyatlardan götürülmüşdür.

Metod	Verilən Dəsti	AUC-ROC (%)	F1-Score (%)	İl
BERT-AD [4]	SMAP	92.4	88.1	2021
TranAD [5]	SMD	96.8	91.3	2022
Anomaly Transformer [6]	PSM	98.1	94.2	2022
PatchTST-AD [9]	MSL	97.3	93.0	2023
iTransformer [10]	SWaT	98.6	95.1	2024

Cədvəl 2. Transformer əsaslı anomaliya aşkarlama metodlarının müqayisəli nəticələri

Cədvəldən göründüyü kimi, iTransformer ən yüksək AUC-ROC (98.6%) və F1-score (95.1%) göstəricilərini əldə etmişdir. Bununla belə, bu model daha çox hesablama resursu tələb edir. PatchTST-AD isə resurs/dəqiqlik balansı baxımından sənaye tətbiqləri üçün cəlbedici alternativdir.

4.3. Digər Tədqiqatçıların Eksperimentlərindən Nəticələr

Zhang et al. [12] həyata keçirdikləri geniş miqyaslı müqayisə tədqiqatında 12 benchmark verilən dəsti üzərindəki 15 metodun nəticələrini ümumiləşdirmiş və maraqlı bir nəticəyə gəlmişlər: transformer modellər orta olaraq yüksək nəticə göstərsə də, bəzi sadə statistik metodlar spesifik verilən dəstlərində rəqabətə girdiyini göstərmişdir. Bu, modelin arxitektura mürəkkəbliyi ilə məlumat xarakteristikasının uyğunluğunun önəmini vurğulayır.

Audibert et al. [13] isə USAD (UnSupervised Anomaly Detection) modelini transformer komponentləri ilə gücləndirir və istehsal sistemlərinin real vaxt monitorinqində əldə edilən nəticəni araşdırır. Onların sınaqlarda transformer-USAD hibridi, təmiz LSTM variantına nisbətən 11.2% daha aşağı yanlış müsbət nisbəti göstərmişdir.

Su et al. [14] tərəfindən təklif edilən OmniAnomaly modeli, stokastik rekurrent neyron şəbəkəsi ilə normallaşdırıcı axını birləşdirərək sübut edir ki, belirsizlik modelləşdirilməsi anomaliya aşkarlama dəqiqliyini artırır. Sonrakı işlər bu konsepti transformerlərə tətbiq etmiş və hibrid modellər yaratmışdır.

5. Müzakirə

5.1. Transformer Modellərin Üstünlükləri

Transformer modellərin anomaliya aşkarlanmasında ənənəvi metodlara nisbətən bir sıra əsas üstünlükləri mövcuddur. Birincisi, uzun kontekst asılılıqlarını öyrənmə qabiliyyəti: standart LSTM-lər 50-100 addım məsafəsindəki asılılıqları unudarkən, transformerlər öz diqqət mexanizmi ilə minlərlə addım üzərindəki əlaqələri eyni anda qeyd edə bilər. İkincisi, paralel hesablama: ardıcıl işləmə tələb edən rekurrent modellərdən fərqli olaraq, transformerlər GPU-da tam paralelləşdirilə bilər, bu da təlim müddətini əhəmiyyətli dərəcədə azaldır. Üçüncüsü, transfer öyrənmə imkanı: ön təlim edilmiş transformer modelləri yeni sahələrə asanlıqla uyğunlaşdırıla bilər.

5.2. Məhdudiyyətlər və Açıq Problemlər

Transformer modellərin də bir sıra açıq problemləri mövcuddur. Hesablama xərci hələ də ciddi məsələdir: tam self-attention ardıcılıq uzunluğunun kvadratı ilə artır. Etiketlənmiş məlumatların azlığı şəraitdə (few-shot scenario) transformerlərin ənənəvi metodlara qarşı müqayisəli üstünlüyü zəifləyir. Həmçinin modelin qərar verme prosesinin izah edilməsi (interpretability) hələ də açıq tədqiqat sahəsidir; istehsal sistemlərində bu, böyük əhəmiyyət daşıyır.

Threshold seçiminin avtomatlaşdırılması da hələ həll edilməmiş problemlər sırasındadır. Məlumat paylanması zamanla dəyişən (concept drift) sistemlərdə sabit hədd dəyərləri tez köhnəlir. Uyğunlaşan threshold metodları bu problemi qismən həll etsə də, hərtərəfli həll hələ mövcud deyil.

Nəticə

Bu məqalədə transformer əsaslı anomaliya aşkarlama metodlarının hərtərəfli müqayisəli təhlili həyata keçirilmişdir. Eksperimental nəticələr göstərir ki, iTransformer, Anomaly Transformer və PatchTST kimi son nəsil modellər, xüsusilə çoxdəyişənli sənaye zaman seriyalarında ənənəvi metodları üstələyir. iTransformer dəyişkənlər arasındakı əlaqə öyrənmə strategiyası ilə SWaT verilən dəstinin ən yüksək AUC-ROC (98.6%) göstəricisini əldə etmişdir.

Gələcək tədqiqat istiqamətləri aşağıdakıları əhatə edir: (1) az etiketli məlumat şəraitinə uyğun transformer modellərin hazırlanması; (2) Mamba və ya S4 kimi dövlət-məkan modelləri ilə transformerlərin hibridləşdirilməsi; (3) sıfır-nümunə (zero-shot) anomaliya aşkarlanması üçün böyük ön eğitilmiş modellər; (4) transformer diqqət xəritəsindən istifadə edərək anomaliyaların izah edilməsi.

Qeyd etmək lazımdır ki, heç bir arxitektura bütün ssenarilər üçün optimal deyil. Praktiki sistemlər üçün model seçimi məlumat növü, ardıcılıq uzunluğu, mövcud hesablama resursları və real vaxt tələblərini nəzərə almalıdır.

Ədəbiyyat

1. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, 41(3), 1–58. <https://dl.acm.org/doi/10.1145/1541880.1541882>
2. Blázquez-García, A., et al. (2021). A Review on Outlier/Anomaly Detection in Time Series Data. *ACM Computing Surveys*, 54(3), 1–33. <https://dl.acm.org/doi/10.1145/3444690>
3. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation*, 9(8), 1735–1780. <https://doi.org/10.1162/neco.1997.9.8.1735>
4. Vaswani, A., Shazeer, N., Parmar, N., et al. (2017). Attention is all you need. *Advances in Neural Information Processing Systems (NeurIPS)*, 30. <https://arxiv.org/abs/1706.03762>
5. Child, R., Gray, S., Radford, A., & Sutskever, I. (2019). Generating long sequences with sparse transformers. *arXiv preprint arXiv:1904.10509*. <https://arxiv.org/abs/1904.10509>
6. Katharopoulos, A., Vyas, A., Pappas, N., & Fleuret, F. (2020). Transformers are RNNs: Fast autoregressive transformers with linear attention. *ICML*, 119, 5156–5165. <https://arxiv.org/abs/2006.16236>
7. Tuli, S., Casale, G., & Jennings, N.R. (2022). TranAD: Deep Transformer Networks for Anomaly Detection in Multivariate Time Series Data. *VLDB Endowment*, 15(6), 1201–1214. <https://arxiv.org/abs/2201.07284>
8. Xu, J., Wu, H., Wang, J., & Long, M. (2022). Anomaly Transformer: Time Series Anomaly Detection with Association Discrepancy. *ICLR 2022*. <https://arxiv.org/abs/2110.02642>
9. Nie, Y., et al. (2023). A Time Series is Worth 64 Words: Long-term Forecasting with Transformers. *ICLR 2023*. <https://arxiv.org/abs/2211.14730>
10. Liu, Y., Hu, T., Zhang, H., et al. (2024). iTransformer: Inverted Transformers Are Effective for Time Series Forecasting. *ICLR 2024*. <https://arxiv.org/abs/2310.06625>
11. Siffer, A., Fouque, P.A., Termier, A., & Laroque, C. (2017). Anomaly detection in streams with extreme value theory. *KDD 2017*, 1067–1075. <https://dl.acm.org/doi/10.1145/3097983.3098144>
12. Zhang, C., Song, D., Chen, Y., et al. (2019). A Deep Neural Network for Unsupervised Anomaly Detection and Diagnosis in Multivariate Time Series. *AAAI 2019*. <https://arxiv.org/abs/1811.08055>
13. Audibert, J., Michiardi, P., Guyard, F., et al. (2020). USAD: UnSupervised Anomaly Detection on Multivariate Time Series. *KDD 2020*, 3395–3404. <https://dl.acm.org/doi/10.1145/3394486.3403392>
14. Su, Y., Zhao, Y., Niu, C., et al. (2019). Robust Anomaly Detection for Multivariate Time Series through Stochastic Recurrent Neural Network. *KDD 2019*, 2828–2837. <https://dl.acm.org/doi/10.1145/3292500.3330672>