Research Report on

Evolutionary Mixture-of-Typicalities IDS for high-throughput IoT streams

Full search query: I want to find research on anomaly-based intrusion detection systems (IDS) for IoT that use evolutionary clustering approaches—especially mixture of typicalities—within high-throughput, cloud-based stream architectures (like Kafka). I am interested in both conceptual/theoretical models and empirical implementations. Highly relevant works address real-time data streams, adaptive models for concept drift and class imbalance, computational efficiency for edge deployment, and benchmarks against classical IDS under metrics like accuracy, false positive rate, latency, and scalability

Summary

No paper in this literature set directly implements a Mixture of Typicalities (MoT)-based evolutionary clustering anomaly IDS for IoT within a high-throughput streaming architecture (Kafka/Spark) addressing real drift, class imbalance, and edge constraints; the closest approach is [1], which uses Bayesian possibilistic clustering with online adaptation, but without full joint typicality-membership optimization or true stream/cloud deployment.

Main Findings Relative to Search Criteria

1. Mixture of Typicalities and Evolutionary Clustering

- **No references** implement the Mixture of Typicalities (MoT) framework in the sense of joint optimization of membership and typicality for clustering in streaming IoT IDS.
- [1] uses an online Bayesian possibilistic clustering module, providing some robustness to outliers and drift, but typicality is not jointly optimized with membership as in MoT, and it lacks explicit streaming/cloud infrastructure.
- All other papers ([2,3,4,5,6,7,8,9,10]) rely on standard or incremental clustering/classification without MoT or focus on fuzzy/possibilistic approaches only loosely related to the joint objective of MoT.

2. Streaming/Cloud-Based High-Throughput Architectures

- Several works ([2,3,5,6,7,8,10]) implement or benchmark their IDS in genuine streaming environments, leveraging Apache Kafka and Spark (or similar distributed data stream frameworks).
  - [6,7,8,10] indicate strong focus on scalability, throughput, and latency in distributed IDS, but do **not** use evolutionary or typicality-based clustering (favoring incremental trees, KMeans, or hybrid ML pipelines).

3. IoT-Specific Evaluation and Datasets

- [1] and [5] use real IoT data sources; [2,3,4] include IoT-specific datasets (Bot-IoT, IoT-23, NF-ToN-IoT-v2, etc.), although only [1] and [5] are explicit about true device/protocol heterogeneity and streaming ground truth.
- Many other studies repurpose general IDS datasets (NSL-KDD, UNSW-NB15), which may have limited IoT diversity.

4. Concept Drift and Class Imbalance

- **Concept drift adaptation** is addressed in [1,2,3,4,9]:
  - [1]: Adaptive possibilistic clustering and online fuzzy ensemble adjust to drift.
  - [2,3,4]: Explicit drift detectors and retraining for DDoS/malware streaming IDS.
  - [9]: Black-box adaptation and explanation in streaming AIoT.
- **Class imbalance mitigation** is largely unaddressed (no reference uses the MoT objective or minority reweighting at the clustering level). Most works rely on post-hoc resampling or mention imbalance as a challenge.

5. Computational Efficiency and Edge/Resource Constraints

- Edge or low-resource deployment claims are largely unquantified.
  - [5] emphasizes a fog/edge context but provides no concrete CPU, RAM, or energy usage results.
  - Others focus on cloud/cluster resource scaling ([2,6,8,10]) with attention to throughput but not lightweight, IoT-embedded constraints.

6. Benchmarking (Accuracy, FPR, Latency, Scalability, and Classical IDS)

- [1] compares against traditional/ML competitors for accuracy and stability, but not real-time classical IDS (e.g., Snort) in streaming cloud setups.
- [6,7,8,10] provide accuracy, F1, and throughput under substantial streaming loads, but omit advanced clustering, drift, or typicality mechanisms.
- Benchmarks versus signature-based IDS in a streaming/IoT/cloud context are rare.

Gaps and Research Opportunities

- **No work unifies MoT, evolutionary clustering, streaming cloud deployment, IoT heterogeneity, and edge efficiency.**
  - [1] advances streaming fuzzy clustering and ensemble adaptation, but does not implement MoT or a cloud-scale pipeline.
  - Most stream/edge/cloud IDS ([2,3,5,6,7,8,9,10]) do not use fuzzy or typicality-based clustering.
- **Concept drift adaptation is now a research norm; integration with advanced clustering (MoT) is not.**
- **Edge metrics (CPU/RAM/energy) and class imbalance mitigation in high-throughput IoT IDS remain critically under-explored.**

Recommended Resources for Further Study

- **Closest conceptual match:** [1] – for fuzzy/possibilistic online clustering and streaming IoT IDS, though without MoT or streaming cloud architecture.
- **Strong streaming implementation and drift detection (standard ML):** [2,3,6,7,8,10].
- **Best real-time distributed IDS pipeline with throughput benchmarks:** [8].
- **State-of-the-art concept drift adaptation (non-clustering):** [9].
- **IoT-specific testbeds/pipelines without advanced clustering:** [5].

References

See [1,2,3,4,5,6,7,8,9,10] as mapped in the original list.

Categories

Comprehensive Comparison of Anomaly-Based IDS for IoT using Evolutionary Clustering and Stream Architectures

Overview of the Comparative Dimensions

For your advanced topic, the comparison is structured on axes central to anomaly-based IDS in IoT with evolutionary clustering/typicalities, in streaming/cloud contexts, explicitly addressing:

- **Clustering Approach** (Evolutionary/Incremental, MoT, other fuzzy/possibilistic methods)
- **Mixture of Typicalities or Related Typicality Framework**
- **Streaming/Cloud Architecture Used**
- **IoT-Specific Evaluation** (true IoT workloads, edge hardware, protocol diversity)
- **Concept Drift Adaptation**
- **Class Imbalance Handling**
- **Computational Efficiency & Edge-Relevant Metrics**
- **Empirical Benchmarks** (Against classical IDS, streaming metrics: latency, throughput, scalability)

Summary Table: Core Aspects Across Major Papers

Ref	Clustering Approach	Typicality/MoT	Streaming Arch.	IoT-Specific?	Concept Drift	Imbalance	Comp. Efficiency	Benchmarking	Notes
[1]	Bayesian possibilistic clustering +		Online module (no explicit		Adaptive clustering,	Not explicit		Versus traditionals; accuracy/ro-	Closest to typicality-based

	fuzzy ensemble	Possibilistic (not joint MoT)	Kafka/Flink/Spark)	Eval. on real IoT traffic	online fuzzy ensemble		Not quantified for edge	bustness focus	online clustering in IoT; lacks explicit MoT, stream backend, or edge metrics
[2]	Unsupervised adaptive clustering	No (unspecified drift detector)	Online, big data pipeline, scalable	Datasets indicate IoT DDoS	Explicit drift detection	Not explicit	Scalable pipeline, no edge metrics	Emphasizes real-time DDoS, throughput, scalability	Focus on pipeline scalability and concept drift, but not fuzzy or typicality clustering
[3]	Not clustering (focus on classifiers & drift detectors)	No	Spark + Kafka, true streaming	NSL-KDD, IoT-23	6 drift detectors compared	No	Not edge-quantified	Accuracy and drift-detection rates	Good cloud/streaming setup, but not clustering/typicality
[4]	Incremental density-based clustering	No (density/nearest neighbor/thresholding)	Streaming (Python simulation)	NSL-KDD, UNSW-NB15	Handles concept drift	No explicit	Not for edge; rates (FPR/acc)	Accuracy, FPR (vs. prior cluster methods)	Real-time clustering, but not typicality/MoT, nor full IoT stack
[5]	ML classifiers (not clustering; several ML methods)	No	Fog/Edge + Spark	NF-ToN-IoT-v2 (real IoT events)	Not explicit	Not explicit	Not specified	ML classifier accuracy	Emphasis on edge/fog system, but not evolutionary/typicality clustering
[6]	Incremental decision trees (Hoeffding VFDT), deep DL	No	Kafka, big-data streaming arch	Real-world (unspecified), not IoT explicit	Adaptive online learning	Not explicit	Streaming efficiency, not edge	Throughput, acc., F1, responsiveness	DL/trees, not clustering nor typicality
[7]	K-Means + KNN, unsup+sup hybrid	No	Kafka + Spark	NetFlow, high-volume traffic	Not explicit	No	Not for edge	Descriptive stats, not full streaming metrics	Useful full pipeline, not cluster/typicality
[8]	ML classifiers (Spark MLlib ensemble), not clustering	No	Kafka + Spark + Hadoop	DDoS focus; general net. flows	Not explicit	Not explicit	Scalable/distributed	Streaming F1/accuracy	DDoS-specific, high-throughput framework
[9]	Black-box anomaly detector; DA/SHAP-driven retrain	No	Streaming setting, not explicit on Kafka/Flink	AIoT emphasis	Explicit: drift detection/adaptation/retraining	No explicit	No quantified edge metrics	Adaptability, false positives	Emphasis on adaptation, not clustering or typicality
[10]	MLlib classifiers (not clustering)	No	Kafka + Spark	No explicit IoT eval	Not explicit	Not explicit	Throughput, not edge	Streaming accuracy, efficiency	Emphasizes scalable IDS pipeline

Narrative Analysis by Key Dimension

1. Evolutionary Clustering and Typicality/MoT Use

- **Closest to Desired MoT**: Only [1] applies a soft/fuzzy approach with an online possibilistic (but not mixture-of-typicalities) clustering module; typicality (belief) is present, but not jointly optimized with membership as in MoT.
- **Pure Evolutionary Clustering**: [4] presents incremental (cluster) adaptation with density thresholding–but does not use fuzzy/typicality or possibilistic extensions.
- **Rest**: Most (e.g., [2,3,5,6,7,8,10]) employ either classifiers or batch-trained clustering; their streaming early detection relies on online learning or micro-batching rather than on incremental centroid updating with fading/micro-clusters.

2. Streaming/Cloud Architectures

- **Kafka/Spark Used Explicitly**: [2,3,5,6,7,8,10] embody real streaming pipeline elements (Kafka ingestion, Spark/Flink for analytics), from “exactly-once” streaming to large distributed settings.
  - [3,8,10] provide strongest coupling to real cloud-scale stream processing.
  - [6] for incremental learning and [7] blend Kafka with standard big-data ML tools.
- **Simulation Only**: [4,1] are implemented in local Python/online frameworks—less relevant to true production-grade stream settings.

3. IoT Context and Datasets

- **Strongest IoT Relevance**: [1] (real IoT system traffic), [5] (NF-ToN-IoT-v2 from actual IoT sources), [2,3] (although using NSL-KDD/IoT-23: mixed edge/IoT, not always strongly heterogeneous).
- **Most Others**: DDoS focus or NSL-KDD/UNSW (used in [4])—not always involving highly heterogeneous, resource-constrained IoT protocols.

4. Concept Drift & Class Imbalance Handling

- **Concept Drift**
  - **Addressed Explicitly**: [1] (fully incremental/fuzzy ensemble), [2] (online retraining under unsupervised drift detection), [3] (six drift detectors compared in streaming context), [4] (on-the-fly clustering updates).
  - **Not Explicit**: [5,6,7,8,10]—some use standard updates or periodic retraining, not sophisticated drift adaptation.
- **Class Imbalance**
  - **Only [1]** describes robust unfamiliar pattern detection/cluster emergence; **none** describe oversampling/minority reweighting at the MoT-objective or centroid level.

5. Computational Efficiency/Edge Deployment

- **Edge/Resource-Aware**: [5] is “Fog” oriented, but does not present quantified CPU/memory results.
- **Most Others** focus on cloud/cluster throughput ([2,3,6,7,8,10]), with streaming throughput but lacking low-power or embedded-deployment numbers.
- **[1]**: Online, but missing actual edge benchmarks or model-compression results.

6. Benchmarks (Latency, FPR, Classical IDS, Scalability)

- **Comprehensive Streaming Benchmarks**: [3,6,7,8,10] all provide streaming accuracy, >10^4 events/sec, and sometimes F1/FPR. [8,10] especially emphasize throughput and low latency.
- **Classical IDS comparison**: [1] reports comparison to “numerous competitors” (not clearly naming Snort/Suricata), typically academic ML baselines.
- **Scalability (Horizontal)**: Stressed in [2,6,8,10] via distributed cluster implementation (Kafka/Spark).
- **Latency, FPR Quantification**: [4] (7.9% FPR on NSL-KDD), [6] (latency optim, throughput), [7,8,10] focus on throughput/latency but sometimes omit explicit latency budget.

Expert Summary Table: Alignment with Search Criteria

Paper(s)	Evolutionary/Incremental Clustering	MoT/Typicality	IoT Streaming Arch. (Kafka/Spark)	Concept Drift	Imbalance	Edge Metrics	Streaming Benchmarks
[1]		HP(ossibilistic)	~ (Online, not Kafka/Spark)		(Partial)		(Some, not full)
[2,3]	(No, classifier)		(Kafka/Spark)				
[4]			~ (Simulated streaming)				Partial
[5]			(Spark/Fog)			(Edge-oriented)	Partial
[6,7,8,10]			(Kafka/Spark)	(No/incidental)			
[9]			(No explicit Kafka)				

Color legend

- = Addressed
- ~ = Partially addressed

- = Not addressed
- ⧧ Related but not strict MoT/typicality

Key Takeaways for Domain Experts

- **No paper in this set directly implements a Mixture of Typicalities (MoT) clustering model within a Kafka/Spark-based streaming pipeline for IoT intrusion detection.**
  - [1] comes closest: online fuzzy/possibilistic methods, but not joint membership-typicality MoT.
- **Streaming architectures are robustly adopted** ([2,3,5,6,7,8,10]), but the combination with evolutionary clustering (not just online classifiers) is rare.
- **Concept drift is increasingly addressed** (esp. [1,2,3,4,9]), yet integration with true online fuzzy-typicality models and rigorous class imbalance mitigation is largely absent.
- **Benchmarks are cloud/throughput focused**; explicit comparisons to traditional signature-based IDS in a streaming context are rare.
- **Edge/IoT deployment constraints are not well studied in terms of quantifiable resource metrics**, except for Fog-contextual mentions ([5]); most papers focus on scalability for cloud/distributed nodes.
- **IoT traffic and datasets are sometimes present** ([1,2,3,5]), but heterogeneity (protocols/devices) and ground-truth alignment for streaming benchmarks remain spotty.

Conclusion: Gaps and Unique Contributions

- **Almost no intersection** of MoT theory, evolutionary clustering, Kafka-scale streaming, and IoT/edge benchmarking exists in these papers. [1] is the most conceptually relevant for online typicality-based clustering, but lacks both explicit MoT and scalable streaming/cloud deployment.
- **Streaming IDS research in IoT leans towards online classifiers or batch-updated clustering**, with fuzzy/possibilistic methods underrepresented in large-scale cloud pipelines.
- **Future work should unify MoT (or similar robust fuzzy clustering) with real streaming architectures, true IoT workloads, and end-to-end performance metrics including edge and cloud deployment.**

References

See numerical citations above ([1,2,3,4,5,6,7,8,9,10]).

Timeline

Timeline and Development of Anomaly-based IDS for IoT with Evolutionary Clustering and Stream Architectures

1. Early Evolutionary and Fuzzy/Typicality-Based Approaches (pre-2022)

- **Fuzzy and possibilistic clustering in IDS:**
  - Before the recent focus on full Mixture-of-Typicalities (MoT) and large-scale cloud-based deployment, researchers explored online fuzzy/possibilistic clusterers to provide better robustness to outliers and imbalanced classes.
  - These methods typically aimed for greater adaptability and resilience compared to classic k-means or signature-based IDS, but were mostly limited to batch or small-scale online environments.

2. First Wave: Online/Evolutionary Clustering with Fuzzy/Possibilistic Approaches (2022–2023)

- **[1] (2022, Fangqi Li et al., IEEE Trans. Fuzzy Syst.)**
  - **Significance:** Incorporates a full Bayesian possibilistic clustering module and ensemble fuzzy classifiers for online IoT IDS.
  - **Advances:** Dynamic cluster identification, adapts to traffic distribution shifts, ensemble backend for stability and drift adaptation.
  - **Limitations:** Uses possibilistic clustering (related to MoT but not a true MoT joint membership-typicality optimizer).
  -

Impact: Set a foundation for streaming fuzzy clustering models in online IoT environments, with advances in cluster adaptation and robustness to evolving streams.

- **Distributed streaming anomaly detection (2022–2023):**
  - Several works pivoted toward integration with distributed stream platforms, e.g., Spark Streaming and Kafka, to handle the velocity and scale characteristic of IoT data ([5,7,8,10]).

3. Big Data and Real-Time Stream Architectures Become Central (2021–2025)

- **Kafka/Spark-based scalable IDS frameworks:**
  - Studies such as [5,6,7,8,10] demonstrate the uptake of cloud-native tools (Kafka for ingest, Spark for processing) as core platforms for real-time IDS.
  - **Emphasis:** Achieving high throughput, reproducibility, and low-latency threat detection in realistic settings, rather than simulation-only environments.
  - **Methods:** Most adopted classical or incremental ML (k-means, KNN, VFDT), but rarely combined with advanced cluster-typicality or fully evolutionary cluster adaptation.
  - **Milestone:** [8] (2022) stands out for its real-time Spark-Kafka integration with streaming DDoS detection, though it does not use MoT or evolutionary cluster adaptation mechanisms.
  - **Latest:** [6,10] (2025) underscore a continuing trend toward very-high-throughput platforms, emphasizing scalability, and adaptive incremental learning, but without deep typicality models.

4. Concept Drift and Class Imbalance: Acknowledgement and Partial Solutions (2022–2024)

- **Stream-specific drift and adaptation:**
  - Researchers recognize and directly tackle concept drift ([2,3,4,9]), with explicit discussion of online drift detectors (KS-test, DDM, ADWIN, etc.) and mechanisms for retraining or adaptive update on distribution shift.
  - **Empirical evaluation:** Some works such as [3] and [4] evaluate various drift detectors in high-velocity IoT traffic streams, sometimes using realistic streaming pipelines (e.g., [3] with Spark and Kafka).
  - **Coverage:** Class imbalance is sometimes addressed, but often via straightforward resampling or threshold adjustment, not via integration with cluster-typicality objectives.
- **Trend:** Recent studies move toward automatic drift handling and balancing, but seldom within a MoT optimization.

5. Mixture of Typicalities and Joint Membership-Typicality Optimization: Still Emerging

- **Absence of fully MoT-based online IDS in high-throughput IoT streams:**
  - While possibilistic/fuzzy clustering is leveraged ([1]), no paper in this batch demonstrates a real-time evolutionary clustering IDS for IoT using the full MoT framework (jointly optimizing memberships and typicalities per the MoT objective), especially not in a heavily cloud-native streaming platform.
  - Outlier management and typicality-based anomaly scoring—a signature of MoT—remain rarely implemented in distributed/realtime IoT-ready IDS from this literature set.
  - **Implication:** The field shows a preparatory evolution—from offline/possibilistic clustering to distributed, scalable platforms, with mounting attention to drift and imbalance—yet full realization of MoT in these contexts is, as of this literature, essentially an open challenge.

6. Edge Deployment and Resource Efficiency: A Growing Consideration

- **Edge/Hierarchical focus:** Only occasional, often in future work or as conceptual statements (e.g., [6]).
- **Metrics Trend:** Reporting is improving—some more recent papers record latency, F1, throughput ([6,7,8,10]), but detailed edge-resource benchmarks (CPU, RAM, energy, real ARM/MCU targets) are rare.

Key Trends and Patterns

- **Integration of cloud-native streaming tools (Kafka, Spark, Flink) for IDS is now standard**: Initially adopted mainly for batch or offline studies, recent works increasingly implement and benchmark in real distributed streaming environments ([5,6,7,8,10]).
- **Incremental/online clustering is common, but state-of-the-art MoT evolutionary clustering remains rare**: Most clustering-based IDS still employ simpler or batch-mode fuzzy/possibilistic clusterers ([1,4]) or classic online clustering (k-means variants), not the full MoT joint optimization.
- **Explicit handling of concept drift and imbalance is recognized as essential**: Recent works directly compare and benchmark drift adaptation strategies ([2,3,4,9]).
- **Clear movement toward empirical benchmarking under realistic streaming loads**: Fluid event rates, latency and throughput metrics, and big data pipeline orchestration are now often included ([6,7,8,10]).
-

Scarcity of detailed resource/edge deployment analysis: While edge suitability is highlighted as a need, detailed evaluation on embedded platforms is rare; usually, this is deferred to future work or assumed on the basis of algorithmic "lightweightness."

Major Contributors and Collaborative Clusters

- **No clear repeated clusters of authors or research groups emerge with a dominating thread through this corpus**:
  - Most impactful works (e.g., [1,8]) appear to be led by separate research teams.
  - Some overlap in citations exists ([2] referencing [8]), but there is no obvious sustained multi-year effort by a single group fully spanning evolutionary clustering, MoT, and high-throughput stream IDS in IoT.
- **Individual contributions highlight different facets:**
  - *Fangqi Li et al.* ([1]): pushed Bayesian possibilistic clustering and fuzzy ensembles online, focusing on flexibility and drift adaptation, evaluated on real IoT datasets.
  - *Patil and Kumar et al.* ([8]): innovated in high-throughput, distributed IDS architectures but did not address typicality/MoT-style clustering.
- **Synergy across subfields (fuzzy clustering, spark streaming, concept drift)** is more common than deep convergence: Most advances combine technologies but have not synthesized all of them into the target approach (evolutionary MoT in high-throughput IoT stream IDS).

Summary Table: Milestones and Gaps

Period	Key Milestone	Papers	MoT Used	Drift/Imbalance	High-throughput Stream	Empirical Benchmarking	Edge focus
Pre-2022	Fuzzy/possibilistic clustering	---	Some variants	Not explicit	No	Accuracy only	No
2022	Bayesian possibilistic online	[1]	No (close)	Yes	Partial	Yes	Limited
2021–2024	Distributed big-data pipelines	[5,7,8,10]	No	Sometimes	Yes	Improving	Limited
2022–2024	Drift/imbalance solutions	[2,3,4,9]	No	Yes	Sometimes	Yes	Rare
2025	Scalable streaming + VFDT	[6,10]	No	Implicit	Yes	Yes	Some

---

Conclusions and Future Implications

- **Mixture-of-Typicalities (MoT) in streaming IoT IDS is barely explored** within realistic, high-throughput cloud/edge frameworks as of 2024. Solutions so far emphasize one or two facets (fuzzy clustering, stream adaptation, cloud scalability), **not all combined**.
- **Next milestone for the field:** A work that unites
  - full evolutionary MoT clustering,
  - real-time drift/imbalance handling,
  - and deployment/evaluation within Kafka/Flink/Spark in large-scale IoT settings,
  - including edge-computing benchmarks,
  - and classical IDS/ML baselines under rich metrics,
    will both fill a research gap and address the most pressing open challenges identified in this literature.
- **Research is moving in this direction,** with active attention to adaptive streaming, unsupervised anomaly detection, scalability, and interpretability, but full convergence is yet to be achieved.

References:
[1,2,3,4,5,6,7,8,9,10] (as per supplied list; see above for mapping).

Foundational Work

Which papers form the foundational references on this topic?

The below table shows the resources that are most often cited by the relevant papers on this topic. This is measured by the **reference rate**, which is the fraction of relevant papers that cite a resource. Use this table to determine the most important core papers to be familiar with if you want to deeply understand this topic. Some of these core papers may not be directly relevant to the topic, but provide important context.

Ref.	Reference Rate	Title	Cited By These Relevant Papers
[11]	0.09	Intrusion Detection in the IoT Under Data and Concept Drifts: Online Deep Learning Approach	[2, 16, 17, 21]
[16]	0.08	ADTCD: An Adaptive Anomaly Detection Approach Toward Concept Drift in IoT	[2, 9]
[141]	0.06	Anomaly detection model based on data stream clustering	[4]
[35]	0.04	Practical Application of Machine Learning based Online Intrusion Detection to Internet of Things Networks	[11]
[104]	0.04	Securing Fog-to-Things Environment Using Intrusion Detection System Based On Ensemble Learning	[11]
[119]	0.04	Learning under Concept Drift: A Review	[2, 11, 17]
[142]	0.04	Intrusion detection systems in the Internet of things: A comprehensive investigation	[11]
[143]	0.04	Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things	[11]
[144]	0.04	A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security	[11]
[145]	0.04	A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework	[11]
[1]	0.04	Online Intrusion Detection for Internet of Things Systems With Full Bayesian Possibilistic Clustering and Ensembled Fuzzy Classifiers	[23, 40]
[146]	0.04	Principal Component Analysis	[11]
[7]	0.03	An ML Based Anomaly Detection System in real-time data streams	[22]
[2]	N/A	UASDAC: An Unsupervised Adaptive Scalable DDoS Attack Classification in Large-Scale IoT Network Under Concept Drift	[3]
[3]	0.00	Adaptive Real-Time Malware Detection for IoT Traffic Streams: A Comparative Study of Concept Drift Detection Techniques	N/A
[4]	0.00	A clustering-based method for outlier detection under concept drift	N/A
[5]	0.00	Design of A Distributed Intrusion Detection System for Streaming Data in IoT Environments	N/A
[6]	0.00	Streaming-Based Intrusion Detection with Big Data and Online Learning Algorithms	N/A
[8]	0.00	SSK-DDoS: distributed stream processing framework based classification system for DDoS attacks	[2]
[9]	0.00	Addressing Concept Drift in IoT Anomaly Detection: Drift Detection, Interpretation, and Adaptation	N/A

Adjacent Work

Which papers cite the same foundational papers as relevant papers?

Use this table to discover related papers on adjacent topics, to gain a broader understanding of the field and help generate ideas for useful new research directions.

Ref.	Adjacency score	Title	References These Foundational Papers
[17]	0.05	Intrusion detection in the IoT data streams using concept drift localization	[11]
[40]	0.04	ADCL: Toward an Adaptive Network Intrusion Detection System Using Collaborative Learning in IoT Networks	[1, 11]
[54]	0.04	Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems	[11, 16]
[180]	0.03	A Novel Multi Wavelet Oriented Auto Encoder for Intrusion Detection in IoT System	[11]
[182]	0.03	Strategic Network Attack Prevention System Leveraging Sophisticated Query-Based Network Attention Algorithm (QNAA) and Self-Perpetuating Generative Adversarial Network (SPF-GAN) Techniques for Optimal Detection	[11]
[184]	0.03	CDDA-MD: An efficient malicious traffic detection method based on concept drift detection and adaptation technique	[11]
[185]	0.03	Deep learning-driven methods for network-based intrusion detection systems: A systematic review	[11]
[186]	0.03	Boosting incremental intrusion detection system with adversarial samples	[11]
[188]	0.03	ASAP: Automatic Synthesis of Attack Prototypes, an online-learning, end-to-end approach	[11]
[189]	0.03	Intrusion detection based on concept drift detection and online incremental learning	[11]
[198]	0.03	AOC-IDS: Autonomous Online Framework with Contrastive Learning for Intrusion Detection	[11]
[140]	0.03	Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study	[11]
[136]	0.03	The analysis of the internet of things database query and optimization using deep learning network model	[11]
[135]	0.03	A Deep Autoencoder Based Outlier Detection Model for Intrusion Detection Systems in Wireless Sensor Networks	[11]
[134]	0.03	A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions	[11]
[130]	0.03	Privacy-Preserving Attribute-Based Access Control Scheme With Intrusion Detection and Policy Hiding for Data Sharing in VANET	[11]
[128]	0.03	Modeling Intrusion Detection for the Landscape Design Software Procreate from Data Layer	[11]
[123]	0.03	A systematic review of metaheuristics-based and machine learning-driven intrusion detection systems in IoT	[11]
[120]	0.03	Design of Intrusion Detection and Response Mechanism for Power Grid SCADA Based on Improved LSTM and FNN	[11]
[117]	0.03	Deep learning for cyber threat detection in IoT networks: A review	[11]

References

[1] Online Intrusion Detection for Internet of Things Systems With Full Bayesian Possibilistic Clustering and Ensembled Fuzzy Classifiers
Fangqi Li, ..., and Weiping Ding. IEEE Transactions on Fuzzy Systems, 2022. 11 citations.
46% Topic Match
Proposes an online IDS for IoT using full Bayesian possibilistic clustering and ensemble fuzzy classifiers.
Combines a streaming-capable Bayesian fuzzy clustering module (auto cluster number) with drift-adaptive, ensemble fuzzy decision trees.
Addresses real IoT datasets, drift adaptation, accuracy, and benchmarking, but does not explicitly use the Mixture-of-Typicalities framework or cloud/Kafka stream architectures.

[2] UASDAC: An Unsupervised Adaptive Scalable DDoS Attack Classification in Large-Scale IoT Network Under Concept Drift
Saravanan Selvam and Uma Maheswari Balasubramanian. IEEE Access, 2024. 2 citations.
39% Topic Match
Proposes an adaptive, scalable IDS for real-time IoT DDoS detection.
Implements an unsupervised drift detector within a big data streaming pipeline to classify DDoS/benign IoT traffic and handle concept drift.
Focuses on scalability and adaptive retraining; does not mention evolutionary clustering or Mixture-of-Typicalities, and lacks explicit edge deployment or classic IDS benchmarking details.

[3] Adaptive Real-Time Malware Detection for IoT Traffic Streams: A Comparative Study of Concept Drift Detection Techniques
D. Bharani, ..., and S. Saravanan. 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), 2024. 0 citations.
33% Topic Match
Proposes a real-time adaptive malware detection system for IoT streams.
Implements and benchmarks six concept drift detection techniques within a Spark/Kafka streaming pipeline, evaluating on NSL-KDD and IoT-23 datasets.
Does not mention evolutionary clustering or Mixture of Typicalities; focuses on concept drift in real-time streaming but lacks details on fuzzy/typicality-based IDS or specific edge deployment metrics.

[4] A clustering-based method for outlier detection under concept drift
Mahjabeen Tahir, ..., and K. A. Kasmiran. Mehran University Research Journal of Engineering and Technology, 2024. 0 citations.
30% Topic Match
Proposes a clustering-based streaming anomaly detection method with drift adaptation.
Uses incremental updates and density thresholds to identify outliers in network data streams, buffering to reduce false positives.
Evaluated only on generic network datasets (NSL-KDD/UNSWNB-15), not IoT; no mention of Mixture-of-Typicalities, cloud-streaming frameworks, or edge deployment metrics.

[5] Design of A Distributed Intrusion Detection System for Streaming Data in IoT Environments
Souad Atbib, ..., and H. Chaoui. 2023 9th International Conference on Optimization and Applications (ICOA), 2023. 0 citations.
27% Topic Match
Proposes a streaming IDS architecture for IoT using Spark.
Implements multiple machine learning algorithms on streaming IoT data (NF-ToN-IoT-v2) within a fog/cloud (Spark) environment.
Does not mention evolutionary clustering or Mixture of Typicalities; streaming setup is relevant, but model type and drift/imbalance handling may be outside target scope.

[6] Streaming-Based Intrusion Detection with Big Data and Online Learning Algorithms
Amro Saleh, ..., and Mouhammd Alkasassbeh. 2025 International Conference on New Trends in Computing Sciences (ICTCS), 2025. 0 citations.
24% Topic Match
Proposes a Kafka-based streaming IDS using deep learning and online VFDT.
Achieves adaptability, accuracy, and scalability on real-world high-throughput data streams, with per-event incremental updates.
Does not use evolutionary clustering or Mixture-of-Typicalities; focuses on VFDT and standard streaming ML, not fuzzy/typicality or IoT-specific edge deployment.

[7] An ML Based Anomaly Detection System in real-time data streams
Javier Jose Diaz Rivera, ..., and Wang-Cheol Song. 2021 International Conference on Computational Science and Computational Intelligence (CSCI), 2021. 6 citations.
22% Topic Match
Proposes a real-time anomaly detection system for network streams.
Implements Kafka-based NetFlow ingestion, Spark processing, and anomaly detection using k-means and KNN.
Uses classical clustering (no evolutionary or typicality/MoT), unclear IoT/edge focus, lacks explicit concept drift/imbalance and cloud-stream benchmarks.

[8] SSK-DDoS: distributed stream processing framework based classification system for DDoS attacks
N. Patil, ..., and Krishan Kumar. Cluster Computing, 2022. 30 citations.
19% Topic Match
Proposes a real-time DDoS classification system using Spark Streaming and Kafka.
Implements distributed MLlib classifiers on streaming IoT/network data ingested via Kafka to classify multiple DDoS attack types.
Focuses on batch-trained classification, not anomaly-based or evolutionary clustering; lacks Mixture-of-Typicalities, concept drift handling, or edge deployment metrics.

[9] Addressing Concept Drift in IoT Anomaly Detection: Drift Detection, Interpretation, and Adaptation
Lijuan Xu, ..., and Chuan Chen. IEEE Transactions on Sustainable Computing, 2024. 5 citations.
17% Topic Match
Proposes a framework for concept drift detection and adaptation in IoT anomaly detection.
Integrates drift detection, SHAP-based interpretation, and selective model retraining to handle shifting data distributions in unsupervised IoT streams.
Addresses concept drift and reduces false positives on multiple IoT datasets, but does not mention evolutionary clustering, Mixture of Typicalities, or streaming/cloud infrastructure specifics.

[10] Distributed Intrusion Detection System using Kafka and Spark Streaming
Kotyada Mohan, ..., and Karthik Ullas. 2025 International Conference on Visual Analytics and Data Visualization (ICVADV), 2025. 0 citations.
16% Topic Match
Proposes a scalable IDS using Kafka and Spark Streaming.
Uses Kafka for real-time ingestion and Spark MLlib for parallelized classification of network traffic.
Does not mention anomaly-based, evolutionary clustering, or mixture-of-typicalities; focus is on streaming infrastructure, not novel adaptive clustering for IoT or drift/imbalance handling.

[11] Intrusion Detection in the IoT Under Data and Concept Drifts: Online Deep Learning Approach
Omar Abdel Wahab. IEEE Internet of Things Journal, 2022. 83 citations.
14% Topic Match

Abstract: Although the existing machine learning-based intrusion detection systems in the Internet of Things (IoT) usually perform well in static environments, they struggle to preserve their performance over time, in dynamic environments. Yet, the IoT is a highly dynamic and heterogeneous environment, leading to what is known as data drift and concept drift. Data drift is a phenomenon which embodies the change that happens in the relationships among the independent features, which is mainly due to changes in the data quality over time. Concept drift is a phenomenon which depicts the change in the relationships between input and output data in...

[12] Knox: Lightweight Machine Learning Approaches for Automated Detection of Botnet Attacks
Shritik Raj, ..., and Ch. Venkata Rami Reddy. ICST Transactions on Scalable Information Systems, 2023. 2 citations.
12% Topic Match

Abstract: With an advancement in technology, the Internet of Things (IoT) has penetrated various domains such as smart buildings, intelligent transportation systems, healthcare, smart parking, air quality monitoring, water contamination identification, and supply chain owing to its ubiquitous nature. IoT devices periodically collect the data and send it to the gateway or server for pre-processing. However, the security offered in the IoT devices or gateways are still in a nascent stage. An Intrusion Detection System (IDS) meant for detecting the cyber threats on IoT should intercept most threats with minimum latency and yet be lightweight in nature. IoT devices also have...

[13] Streamlined Data Pipeline for Real-Time Threat Detection and Model Inference
Rajkanwar Singh, ..., and Sunil Kumar Singh. 2025 17th International Conference on COMmunication Systems and NETworks (COMSNETS), 2025. 0 citations.
11% Topic Match

Abstract: Real-time threat detection in streaming data is crucial yet challenging due to varying data volumes and speeds. This paper presents an architecture designed to manage large-scale, high-speed data streams using deep learning and machine learning models. The system utilizes Apache Kafka for high-throughput data transfer and a publish-subscribe model to facilitate continuous threat detection. Various machine learning techniques, including XGBoost, Random Forest, and LightGBM, are evaluated to identify the best model for classification. The ExtraTrees model achieves exceptional performance with accuracy, precision, recall, and F1 score all reaching 99% using the SensorNetGuard dataset within this architecture. The PyFlink framework, with...

[14] A Stream Learning Intrusion Detection System for Concept Drifting Network Traffic
Pedro Horchulhack, ..., and Martin Andreoni Lopez. 2022 6th Cyber Security in Networking Conference (CSNet), 2022. 5 citations.
10% Topic Match

Abstract: Network-based intrusion detection is a widely explored topic in the literature. Yet, despite the promising reported results, designed schemes are rarely used in production environments. Apart from evolving as time passes, the behavior of network traffic varies significantly, rendering proposed schemes unreliable for real-world application. This paper proposes a new stream learning intrusion detection aiming for feasible model updates, implemented in three phases. First, intrusion detection is performed through a stream learning classifier, enabling incremental model updates to be performed. Second, new network traffic behavior is identified through a one-class learner. Third, identified new network traffic is incrementally incorporated into...

[15] Network intrusion detection in big datasets using Spark environment and incremental learning
Abdelwahed Elmoutaoukkil, ..., and Marouane Chriss. IAES International Journal of Artificial Intelligence (IJ-AI), 2024. 1 citations.
9% Topic Match

Abstract: Internet of things (IoT) systems have experienced significant growth in data traffic, resulting in security and real-time processing issues. Intrusion detection systems (IDS) are currently an indispensable tool for self-protection against various attacks. However, IoT systems face serious challenges due to the functional diversity of attacks, resulting in detection methods with machine learning (ML) and limited static models generated by the linear discriminant analysis (LDA) algorithm. The process entails adjusting the model parameters in real time as new data arrives. This paper proposes a new method of an IDS based on the LDA algorithm with the incremental model. The model...

[16] ADTCD: An Adaptive Anomaly Detection Approach Toward Concept Drift in IoT
Lijuan Xu, ..., and Xin Li. IEEE Internet of Things Journal, 2023. 21 citations.
8% Topic Match

Abstract: The data collected by sensors is streaming data in the Internet of Things (IoT). Although existing deep-learning-based anomaly detection methods generally perform well on static data, they struggle to respond timely to streaming data after distribution changes. However, streaming data suffers from conceptual drift due to the highly dynamic nature of IoT. In network security, concept drift-oriented anomaly detection is a crucial task, because it can adjust the model to adapt to the latest data, and detect attacks in time. Existing streaming anomaly detection methods are confronted with some challenges, including the latency of model updates, the uneven importance of...

[17] Intrusion detection in the IoT data streams using concept drift localization
Renjie Chu, ..., and Quanxi Feng. AIMS Mathematics, 2023. 1 citations.
7% Topic Match

Abstract: With the widespread application of smart devices, the security of internet of things (IoT) systems faces entirely new challenges. The IoT data stream operates in a non-stationary, dynamic environment, making it prone to concept drift. This paper focused on addressing the issue of concept drift in data streams, with a key emphasis on introducing an innovative drift detection method-ensemble multiple non-parametric concept localization detectors, abbreviated as EMNCD. EMNCD employs an ensemble of non-parametric statistical methods, including the Kolmogorov-Smirnov, Wilcoxon rank sum and Mann-Kendall tests. By comparing sample distributions within a sliding window, EMNCD accurately detects concept drift, achieving precise localization...

[18] Anomalous Network Packet Detection Using Data Stream Mining
Zachary Miller, ..., and Wei-Gang Hu. J. Information Security, 2011. 21 citations.
6% Topic Match

Abstract: In recent years, significant research has been devoted to the development of Intrusion Detection Systems (IDS) able to detect anomalous computer network traffic indicative of malicious activity. While signature-based IDS have proven effective in discovering known attacks, anomaly-based IDS hold the even greater promise of being able to automatically detect previously undocumented threats. Traditional IDS are generally trained in batch mode, and therefore cannot adapt to evolving network data streams in real time. To resolve this limitation, data stream mining techniques can be utilized to create a new type of IDS able to dynamically model a stream of network traffic....

[19] Extending Isolation Forest for Anomaly Detection in Big Data via K-Means
Md Tahmid Rahman Laskar, ..., and Lei Liu. ACM Transactions on Cyber-Physical Systems (TCPS), 2021. 44 citations.
6% Topic Match

Abstract: Industrial Information Technology infrastructures are often vulnerable to cyberattacks. To ensure security to the computer systems in an industrial environment, it is required to build effective intrusion detection systems to monitor the cyber-physical systems (e.g., computer networks) in the industry for malicious activities. This article aims to build such intrusion detection systems to protect the computer networks from cyberattacks. More specifically, we propose a novel unsupervised machine learning approach that combines the K-Means algorithm with the Isolation Forest for anomaly detection in industrial big data scenarios. Since our objective is to build the intrusion detection system for the big data...

[20] PWPAE: An Ensemble Framework for Concept Drift Adaptation in IoT Data Streams
Li Yang, ..., and A. Shami. 2021 IEEE Global Communications Conference (GLOBECOM), 2021. 55 citations.
5% Topic Match

Abstract: As the number of Internet of Things (IoT) devices and systems have surged, IoT data analytics techniques have been developed to detect malicious cyber-attacks and secure IoT systems; however, concept drift issues often occur in IoT data analytics, as IoT data is often dynamic data streams that change over time, causing model degradation and attack detection failure. This is because traditional data analytics models are static models that cannot adapt to data distribution changes. In this paper, we propose a Performance Weighted Probability Averaging Ensemble (PWPAE) framework for drift adaptive IoT anomaly detection through IoT data stream analytics. Experiments on...

[21] Enhancing IoT Intrusion Detection System Performance with the Diversity Measure as a Novel Drift Detection Method
O. A. Mahdi, ..., and Ansam Khraisat. 2023 9th International Conference on Information Technology Trends (ITT), 2023. 6 citations.
5% Topic Match

Abstract: The emergence of the Internet of Things (IoT) has revolutionized various sectors, such as healthcare, intelligent homes, agriculture, transportation, and manufacturing. Nevertheless, the rapid growth of IoT networks has introduced new security challenges, making them susceptible to a variety of attacks. In response, machine learning-driven intrusion detection approaches have been developed, which analyze IoT devices' behavior and communication patterns to detect and counteract suspicious activities. While these approaches exhibit high accuracy and low false alarm rates in static contexts, their performance stability in dynamic, evolving environments is yet to be determined. Model drift, the decline in a machine learning model's...

[22] Real-Time Visualization and Detection of Malicious Network Flows in IoT Devices using a Scalable Stream Processing Pipeline
S. Saravanan, ..., and Kanagasundaram K. 2024 Eighth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2024. 0 citations.
5% Topic Match

Abstract: The continuous adoption of Internet of Things (IoT) devices has established notable security risks. In recent times, IoT devices are often targeted by malicious actors as IoT devices are limited with processing and memory resources. The detection of malicious network flows in real-time is necessary to maintain the security of IoT networks. This paper addresses the challenge by presenting a scalable stream processing pipeline that identifies malicious and non-malicious flows from IoT devices in real-time. The proposed system utilizes NFStream to generate network flows from device packets. The generated network flows are then published to a Kafka topic and consumed...

[23] Online Machine Learning-based Anomaly Detection in Internet of Things Applications
M. Rashid, ..., and Santoso Wibowo. 2023 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2023. 0 citations.
4% Topic Match

Abstract: With the ever-increasing usage of Internet of Things (IoT) applications in every aspect of our lives, protecting IoT networks from security threats has become a significant challenge. Machine learning techniques are widely used to detect anomalous behavior in networks. However, most of the existing machine learning techniques train a model on a whole batch of data at a time. This is not suitable for many IoT networks where new data is constantly arriving in a stream. To address this issue, we propose an online Machine Learning (ML) model that processes a data stream element simultaneously, keeps learning, and does not...

[24] Network attack classification framework based on Autoencoder model and online stream analysis technology
Nguyen Viet Hung, ..., and Ngo Thanh Tung. Journal of Science and Technology on Information security, 2023. 1 citations.
4% Topic Match

Abstract: Abstract— To deal with diverse and constantly changing forms of cyberattacks, machine learning methods have been researched and applied extensively in network data processing for positive results in network attack detection. However, machine learning models require extensive computational resources and their application to handle significant real-time data flow monitoring problems still needs improvement. In this paper, we research and propose a network attack detection framework using a 2-stage classification algorithm with an Autoencoder model, integrating online stream processing technology based on Apache Kafka and Spark technology. The results show that the proposed framework has high efficiency in detecting network attacks...

[25] Edge Intelligence (EI)-Enabled HTTP Anomaly Detection Framework for the Internet of Things (IoT)
Yufei An, ..., and Victor C.M. Leung. IEEE Internet of Things Journal, 2021. 41 citations.
3% Topic Match

Abstract: In recent years, with the rapid development of the Internet of Things (IoT), various applications based on IoT have become more and more popular in industrial and living sectors. However, the hypertext transfer protocol (HTTP) as a popular application protocol used in various IoT applications faces a variety of security vulnerabilities. This article proposes a novel HTTP anomaly detection framework based on edge intelligence (EI) for IoT. In this framework, both clustering and classification methods are used to quickly and accurately detect anomalies in the HTTP traffic for IoT. Unlike the existing works relying on a centralized server to perform...

[26] Adaptive Clustering-based Malicious Traffic Classification at the Network Edge
A. Diallo and P. Patras. IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, 2021. 49 citations.
3% Topic Match

Abstract: The rapid uptake of digital services and Internet of Things (IoT) technology gives rise to unprecedented numbers and diversification of cyber attacks, with which commonly-used rule-based Network Intrusion Detection Systems (NIDSs) are struggling to cope. Therefore, Artificial Intelligence (AI) is being exploited as second line of defense, since this methodology helps in extracting non-obvious patterns from network traffic and subsequently in detecting more confidently new types of threats. Cybersecurity is however an arms race and intelligent solutions face renewed challenges as attacks evolve while network traffic volumes surge. In this paper, we propose Adaptive Clustering-based Intrusion Detection (Acid), a novel...

[27] Enhancing IoT Network Security with Concept Drift-Aware Unsupervised Threat Detection
V. Agate, ..., and Giuseppe Lo Re. 2024 IEEE Symposium on Computers and Communications (ISCC), 2024. 1 citations.
3% Topic Match

Abstract: The dynamic characteristics of Internet of Things (IoT) systems create major challenges for threat detection systems that rely on machine learning models. Over time, shifts in the statistical distribution of data can lead to drastic performance degradation. This phenomenon is known as concept drift. When this problem occurs, traditional static systems require human intervention to manually retrain, leaving the network vulnerable in the meantime. In this paper, we propose an unsupervised system for online detection of anomalous traffic generated by malware-infected IoT devices. The proposed multi-tier system explicitly accounts for concept drift, automatically retraining only when necessary. We thoroughly tested...

[28] Distributed intrusion detection system in the cloud environment based on Apache Kafka and Apache Spark
Mohamed Ouhssini, ..., and Elhafed Agherrabi. 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS), 2021. 4 citations.
3% Topic Match

Abstract: After, the emergence of cloud computing (CC), it's gained more attraction to be used for organizations and users. CC allows to migrate the computing power to the internet services. That makes cloud system target of attackers to disrupt services or data breaching. Many existing works try to deal with security issues in cloud computing systems, but it is still suffering against new updated attacks. Therefore, it's necessary to develop new IDS able to detect attacks with high performance. In this paper, we present a distributed IDS based on big data tools and machine learing algorithms to detect attacks in the...

[29] A Few-Shot and Anti-Forgetting Network Intrusion Detection System based on Online Meta Learning
Zhen Wang, ..., and Hongxiang Wang. GLOBECOM 2024 - 2024 IEEE Global Communications Conference, 2024. 2 citations.
2% Topic Match

Abstract: In the actual Internet of Things (IoT) environment, the proportion of abnormal behavior is much lower than that of normal behavior, and abnormal samples are often scarce, so it is a significant challenge to train efficient network intrusion detection systems using limited labeled samples. Meanwhile, intrusion detection systems based on online learning are prone to catastrophic forgetting, which greatly reduces the performance of online models. Previous research has not comprehensively addressed these two issues. Therefore, this paper proposes a few-shot and anti-forgetting network intrusion detection system based on online meta-learning. The system uses meta-learning as the basic algorithm to efficiently...

[30] Design of A Distributed Intrusion Detection System for Streaming Data in IoT Environments
Souad Atbib, ..., and H. Chaoui. 2023 9th International Conference on Optimization and Applications (ICOA), 2023. 3 citations.
2% Topic Match

Abstract: Nowadays, IoT devices produce a large amount of streaming data that requires real-time analysis to ensure its security. Traditional security solutions are no longer sufficient to counter recent IoT attacks and to analyze the huge amount of data. In recent years, intrusion detection systems have been the subject of much research to evaluate their performance in detecting intrusions in IoT, especially since they are based on Artificial Intelligence and allow real-time intrusion detection. In this paper, we present the architecture of an intrusion detection system for streaming data analysis. We implemented our IDS in a Fog computing architecture and developed...

[31] A Dual-Tier Adaptive One-Class Classification IDS for Emerging Cyberthreats
Md. Ashraf Uddin, ..., and Md. Alamin Talukder. ArXiv, 2024. 8 citations.
2% Topic Match

Abstract: In today's digital age, our dependence on IoT (Internet of Things) and IIoT (Industrial IoT) systems has grown immensely, which facilitates sensitive activities such as banking transactions and personal, enterprise data, and legal document exchanges. Cyberattackers consistently exploit weak security measures

and tools. The Network Intrusion Detection System (IDS) acts as a primary tool against such cyber threats. However, machine learning-based IDSs, when trained on specific attack patterns, often misclassify new emerging cyberattacks. Further, the limited availability of attack instances for training a supervised learner and the ever-evolving nature of cyber threats further complicate the matter. This emphasizes the need...

[32] Clust-IT: clustering-based intrusion detection in IoT environments
Robert P. Markiewicz and D. Sgandurra. Proceedings of the 15th International Conference on Availability, Reliability and Security, 2020. 6 citations.
2% Topic Match

Abstract: Low-powered and resource-constrained devices are forming a greater part of our smart networks. For this reason, they have recently been the target of various cyber-attacks. However, these devices often cannot implement traditional intrusion detection systems (IDS), or they can not produce or store the audit trails needed for inspection. Therefore, it is often necessary to adapt existing IDS systems and malware detection approaches to cope with these constraints. We explore the application of unsupervised learning techniques, specifically clustering, to develop a novel IDS for networks composed of low-powered devices. We describe our solution, called Clust-IT (Clustering of IoT), to manage...

[33] A Real-Time Network Intrusion Detection Based on Transformer-LSTM Model
Jeevan G, ..., and Jayana H S. 2024 Fourth International Conference on Multimedia Processing, Communication & Information Technology (MPCIT), 2024. 0 citations.
2% Topic Match

Abstract: This paper introduces a novel approach to network intrusion detection by leveraging the advanced capabilities of deep learning. Traditional intrusion detection systems (IDS) often rely on rule-based mechanisms or require human intervention for feature selection, which limits their effectiveness against sophis-ticated and evolving cyber threats. To address these challenges, this paper focuses on the development of an innovative deep learning model that combines Transformer and Long Short-Term Memory (LSTM) architectures, aiming to enhance the accuracy and automation of intrusion detection tasks. The uniqueness of our approach lies in the integration of the proposed deep learning model with Apache Kafka, a...

[34] Enhanced Intrusion Detection with Data Stream Classification and Concept Drift Guided by the Incremental Learning Genetic Programming Combiner
Methaq A. Shyaa, ..., and José I. Santamaría. Sensors (Basel, Switzerland), 2023. 13 citations.
2% Topic Match

Abstract: Concept drift (CD) in data streaming scenarios such as networking intrusion detection systems (IDS) refers to the change in the statistical distribution of the data over time. There are five principal variants related to CD: incremental, gradual, recurrent, sudden, and blip. Genetic programming combiner (GPC) classification is an effective core candidate for data stream classification for IDS. However, its basic structure relies on the usage of traditional static machine learning models that receive onetime training, limiting its ability to handle CD. To address this issue, we propose an extended variant of the GPC using three main components. First, we replace...

[35] Practical Application of Machine Learning based Online Intrusion Detection to Internet of Things Networks
Christopher Nixon, ..., and Mohamed Hassan. 2019 IEEE Global Conference on Internet of Things (GCIoT), 2019. 19 citations.
2% Topic Match

Abstract: Internet of Things (IoT) devices participate in an open and distributed perception layer, with vulnerability to cyber attacks becoming a key concern for data privacy and service availability. The perception layer provides a unique challenge for intrusion detection where resources are constrained and networks are distributed. An additional challenge is that IoT networks are a continuous non-stationary data stream that, due to their variable nature, are likely to experience concept drift. This research aimed to review the practical applications of online machine learning methods for IoT network intrusion detection, to answer the question if a resource efficient architecture can be...

[36] Attack-adaptive network intrusion detection systems for IoT networks through class incremental learning
Francesco Cerasuolo, ..., and Antonio Pescapé. Comput. Networks, 2025. 0 citations.
1% Topic Match

No summary or abstract available

[37] Adaptive intrusion detection in IoT: combining batch and incremental learning for enhanced security
N. W. Abderrahim and Amina Benosman. Engineering Research Express, 2025. 0 citations.
1% Topic Match

Abstract: The Internet of Things (IoT) has become an integral part of everyday life, and plays a significant role in various sectors by enabling device-to-device communication without human intervention. However, the constant connectivity of these devices to the Internet exposes them to numerous cyberattacks, potentially leading to data breaches, device malfunctions, and unauthorized network access. The diverse range of threats targeting IoT systems highlights the need for robust security solutions, such as machine learning-based intrusion detection systems, which have attracted growing research interest. This study proposes a novel adaptive approach for intrusion detection in IoT environments by combining batch and incremental...

[38] MemStream: Memory-Based Streaming Anomaly Detection
Siddharth Bhatia, ..., and Bryan Hooi. Proceedings of the ACM Web Conference 2022, 2021. 18 citations.
1% Topic Match

Abstract: Given a stream of entries over time in a multi-dimensional data setting where concept drift is present, how can we detect anomalous activities? Most of the existing unsupervised anomaly detection approaches seek to detect anomalous events in an offline fashion and require a large amount of data for training. This is not practical in real-life scenarios where we receive the data in a streaming manner and do not know the size of the stream beforehand. Thus, we need a data-efficient method that can detect and adapt to changing data trends, or concept drift, in an online manner. In this work,...

[39] GBDT-IL: Incremental Learning of Gradient Boosting Decision Trees to Detect Botnets in Internet of Things
Ruidong Chen, ..., and Erfan Zhao. Sensors (Basel, Switzerland), 2024. 5 citations.
1% Topic Match

Abstract: The rapid development of the Internet of Things (IoT) has brought many conveniences to our daily life. However, it has also introduced various security risks that need to be addressed. The proliferation of IoT botnets is one of these risks. Most of researchers have had some success in IoT botnet detection using artificial intelligence (AI). However, they have not considered the impact of dynamic network data streams on the models in real-world environments. Over time, existing detection models struggle to cope with evolving botnets. To address this challenge, we propose an incremental learning approach based on Gradient Boosting Decision Trees...

[40] ADCL: Toward an Adaptive Network Intrusion Detection System Using Collaborative Learning in IoT Networks
Zuchao Ma, ..., and Wenjuan Li. IEEE Internet of Things Journal, 2023. 8 citations.
1% Topic Match

Abstract: With the widespread of cyber attacks, network intrusion detection system (NIDS) is becoming an important and essential tool to protect Internet of Things (IoT) environments. However, it is well known that the NIDS performance depends heavily on the effectiveness of the detection model, which can be influenced significantly by the learning mechanism and the available training data. Many existing studies try to mitigate the above challenges, but few of them consider the adaptability and the cost of deploying an NIDS, the integrity of the learning process, the capacity of model based on concrete traffic samples at the same time. To...

[41] Anomaly Detection of Network Streams via Dense Subgraph Discovery
Hao Yan, ..., and Sheng Chen. 2021 International Conference on Computer Communications and Networks (ICCCN), 2021. 7 citations.
1% Topic Match

Abstract: We consider cyber security as one of the most significant technical challenges in current times. One of the main tasks is to detect anomalous patterns in the network streams as soon as they appear. In order to solve the above problem, previous propositions use statistical or machine learning-based methods to detect anomalous patterns in the network streams. However, these solutions incur significant low efficiency and precision due to the frequent recomputation of the results from scratch and unreasonable assumptions. In graph theory, dense subgraphs can be used to model the anomalous patterns if we abstract the network streams as a...

[42] TNN-IDS: Transformer neural network-based intrusion detection system for MQTT-enabled IoT Networks
Safi Ullah, ..., and M. Ch. Comput. Networks, 2023. 32 citations.

1% Topic Match

No summary or abstract available

[43] Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection
Wajdi Alhakami, ..., and N. Bouguila. IEEE Access, 2019. 92 citations.
1% Topic Match

Abstract: Anomaly-based intrusion detection systems (IDSs) have been deployed to monitor network activity and to protect systems and the Internet of Things (IoT) devices from attacks (or intrusions). The problem with these systems is that they generate a huge amount of inappropriate false alarms whenever abnormal activities are detected and they are not too flexible for a complex environment. The high-level rate of the generated false alarms reduces the performance of IDS against cyber-attacks and makes the tasks of the security analyst particularly difficult and the management of intrusion detection process computationally expensive. We study here one of the challenging aspects...

[44] Intrusion Detection based on Incremental Learning
Islem Chouchen and Farah Jemili. 2023 International Conference on Cyberworlds (CW), 2023. 0 citations.
1% Topic Match

Abstract: Machine learning and deep learning have become essential in enhancing the performance of intrusion detection systems. While existing research on intrusion detection systems utilizing data mining and machine learning has shown effectiveness, it typically involves training static batch classifiers that identify intrusions without considering the time-varying characteristics of the regular data stream. This paper aims to propose an ensemble adaptive approach for online intrusion detection using stream-oriented learning, which can effectively adapt to concept drift in real-world environments. The technique involves the utilization of an ensemble Adaptive Random Forest classifier and Support Vector Regression (SVR) with the ADWIN change detector...

[45] A comparative study on online machine learning techniques for network traffic streams analysis
A. Shahraki, ..., and A. Jurcut. Comput. Networks, 2022. 68 citations.
1% Topic Match

No summary or abstract available

[46] A Fuzzy Intrusion Detection System for Identifying Cyber-Attacks on IoT Networks
A. L. Cristiani, ..., and H. Camargo. 2020 IEEE Latin-American Conference on Communications (LATINCOM), 2020. 7 citations.
1% Topic Match

Abstract: The Internet of Things (IoT) is increasingly present in our daily activities, connecting the most varied types of physical devices present around us to the internet. IoT is the basis for smart cities, e-health, precision agriculture, among others. With this growth, the number of cyber-attacks against these types of devices and services has also increased. Each type of attack has its specific characteristics that allow its identification and prevention through machine learning techniques. However, classic machine learning techniques may have their performance compromised due to the non-stationary characteristics of these environments, together with the search for different types of vulnerabilities...

[47] HEDVA: Harnessing HTTP Traffic for Enhanced Detection of Vulnerability Attacks in IoT Networks
Xukai Zhou, ..., and Wei Lou. GLOBECOM 2024 - 2024 IEEE Global Communications Conference, 2024. 0 citations.
1% Topic Match

Abstract: The widespread adoption of Internet of Things (IoT) devices has led to increasingly complex and varied cyber-threats. Traditional defense mechanisms are often inadequate in countering these evolving threats, as attackers continuously develop new strategies. In response, this paper introduces a rapid threat detection method designed to automatically pinpoint vulnerability attacks on IoT devices amidst vast internet traffic. Our approach incorporates a multilevel clustering method, significantly accelerating the identification of malicious behaviors. Additionally, we develop a reliable assessment criterion for recognizing when a detection model becomes outdated due to the dynamic nature of network environments. This criterion is underpinned by a...

[48] Towards achieving lightweight intrusion detection systems in Internet of Things, the role of incremental machine learning: A systematic literature review
P. Agbedanu, ..., and Destiny Kwabla Amenyedzi. F1000Research, 2022. 2 citations.
1% Topic Match

Abstract: While the benefits of IoT cannot be overstated, its computational constraints make it challenging to deploy security methodologies that have been deployed in traditional computing systems. The benefits and computational constraints have made IoT systems attractive to cyber-attacks. One way to mitigate these attacks is to detect them. In this study, a Systematic Literature Review (SLR) has been conducted to analyze the role of incremental machine learning in achieving lightweight intrusion detection for IoT systems. The study analyzed existing incremental machine learning approaches used in designing intrusion detection systems for IoT ecosystems, emphasizing the incremental methods used in detecting intrusions,...

[49] Streamlining IoT Malware Detection:A Pipeline Based Approach
G. Naresh, ..., and M. A. Kumar. 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2024. 0 citations.
1% Topic Match

Abstract: Internet of Things (IoT) malware detection has become a significant cybersecurity challenge due to the expansion of the threat landscape brought about by the proliferation of IoT devices. IoT malware is growing more complex and dynamic every day, making traditional signature-based detection techniques ineffective against it. By using large-scale data generated by IoT devices to identify patterns and anomalies, machine learning (ML) techniques present a promising way to detect IoT malware. The process of developing effective machine learning models to identify malware for Internet of Things, however, can be difficult and time-consuming owing to the requirementfor meticulous preprocessing,feature engineering, model...

[50] A hybrid deep learning-based intrusion detection system for IoT networks.
Noor Wali Khan, ..., and Jawad Ahmad. Mathematical biosciences and engineering : MBE, 2023. 34 citations.
1% Topic Match

Abstract: The Internet of Things (IoT) is a rapidly evolving technology with a wide range of potential applications, but the security of IoT networks remains a major concern. The existing system needs improvement in detecting intrusions in IoT networks. Several researchers have focused on intrusion detection systems (IDS) that address only one layer of the three-layered IoT architecture, which limits their effectiveness in detecting attacks across the entire network. To address these limitations, this paper proposes an intelligent IDS for IoT networks based on deep learning algorithms. The proposed model consists of a recurrent neural network and gated recurrent units (RNN-GRU),...

[51] CADeSH: Collaborative Anomaly Detection for Smart Homes
Yair Meidan, ..., and A. Shabtai. IEEE Internet of Things Journal, 2023. 9 citations.
1% Topic Match

Abstract: Although home Internet of Things (IoT) devices are typically plain and task oriented, the context of their daily use may affect their traffic patterns. That is, a given IoT device will probably not generate the exact same traffic data when operated by different people in different environments and when connected to different networks with different topologies and communication components. For this reason, anomaly-based intrusion detection systems tend to suffer from a high false positive rate (FPR). To overcome this, we propose a two-step collaborative anomaly detection method which first uses an autoencoder to differentiate frequent (“benign”) and infrequent (possibly “malicious”)...

[52] Comparative Study between Big Data Analysis Techniques in Intrusion Detection
Mounir Hafsa and Farah Jemili. Big Data Cogn. Comput., 2018. 33 citations.
1% Topic Match

Abstract: Cybersecurity ventures expect that cyber-attack damage costs will rise to $11.5 billion in 2019 and that a business will fall victim to a cyber-attack every 14 seconds. Notice here that the time frame for such an event is seconds. With petabytes of data generated each day, this is a challenging task for traditional intrusion detection systems (IDSs). Protecting sensitive information is a major concern for both businesses and governments. Therefore, the need for a real-time, large-scale and effective IDS is a must. In this work, we present a cloud-based, fault tolerant, scalable and distributed IDS that uses Apache Spark Structured...

[53] Concept Drift Analysis by Dynamic Residual Projection for Effectively Detecting Botnet Cyber-Attacks in IoT Scenarios

Hanli Qiao, ..., and J. Blech. IEEE Transactions on Industrial Informatics, 2021. 24 citations.
1% Topic Match

Abstract: IoT devices typically stream data such as sensor values to other devices including cloud-based services. Analyzing these streams for cyber-attacks is a challenging task. This is due to the infinite nature of stream-based datatypes. Analyzing streams can require additional real-time processing and computational performance capabilities. In this article, we focus on how concept drifts affect Botnet cyber-attack detection in IoT scenarios. To reveal the result, we incorporate the concept drift analysis to detect cyber-attacks on the Bot-IoT dataset, which consists of legitimate and simulated IoT network traffics, together with various types of attacks. We designed subdatasets of the Bot-IoT to...

[54] Evolving cybersecurity frontiers: A comprehensive survey on concept drift and feature dynamics aware machine and deep learning in intrusion detection systems
Methaq A. Shyaa, ..., and Laith H. Alzubaidi. Eng. Appl. Artif. Intell., 2024. 20 citations.
1% Topic Match

No summary or abstract available

[55] Concept Drift Detection and Adaptation in IoT Data Stream Analytics
Aleksandra I. Stojnev Ili and D. Stojanovi 2023 16th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS), 2023. 1 citations.
1% Topic Match

Abstract: Dynamic nature of the IoT data can often cause machine learning model degradation, which can lead to analysis and actions failures. In order to address this challenge, it is of utmost importance to detect drifts in the data that can cause unwanted behavior of the system, and to update models accordingly. This paper gives an overview of different methods for addressing concept drift detection and adaptation, demonstration of some of the methods using open source libraries, and a design for a component for smart adaptive system for streaming data analysis that uses presented techniques to ensure high model performance.

[56] Design and Implementation of an Intelligent IoT Platform Based on Information Technology
Yanhua Zhong. 2024 International Conference on Computing, Robotics and System Sciences (ICRSS), 2024. 0 citations.
1% Topic Match

Abstract: With the development of the Internet of Things (IoT) technology, various intelligent devices generate massive heterogeneous data, posing higher requirements for real-time processing and efficient analysis of the data. Achieving accurate clustering and anomaly detection of dynamic data has become a critical issue in enhancing the intelligence level of IoT platforms. To address this challenge, this study proposes a solution based on an optimized K-means algorithm and deploys it in a smart community environment to improve the system's real-time response and data processing capabilities. Experimental results demonstrate that the algorithm performs excellently in data clustering and anomaly detection. The average...

[57] Performance Analysis of Online Machine Learning Frameworks for Anomaly Detection in IoT Data Streams
Santosh Kumar Ray and Seba Susan. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2024. 0 citations.
1% Topic Match

Abstract: With the rapid progress of technology, the Internet of Things (IoT) is vital in connecting real-time data sources. These sources generate a substantial volume of streaming data through various applications. When dealing with streaming data, there can be a significant amount of abnormal data, referred to as anomalies, which are completely unknown and can negatively affect the system's performance. In this context, unsupervised anomaly detection methods are expected to perform better than supervised methods. In this paper, we evaluate the performance scores of nine unsupervised anomaly detection models belonging to two recently introduced online machine learning frameworks: River and Python...

[58] Robust Distributed Intrusion Detection System for Edge of Things
Wassila Lalouani and M. Younis. 2021 IEEE Global Communications Conference (GLOBECOM), 2021. 7 citations.
1% Topic Match

Abstract: The edge computing paradigm has been adopted in many Internet-of-Things (IoT) applications to improve responsiveness and conserve communication resources. However, such high agility and efficiency come with increased cyber threats. Intrusion detection systems (IDS) have been the primary means for guarding networked computing assets against hacking attempts. The popular design methodology for IDS relies on the application of machine learning (ML) techniques that use intelligence data to classify malicious activities. However, in the realm of IoT, insufficient data is available to build IDS; hence a distributed intrusion system with continual data collection is primordial to refine the detection model. Such...

[59] Leveraging AI for Real-Time Anomaly Detection in IoT Data Streams
R. G. Gokila, ..., and Natayan L. 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC), 2024. 0 citations.
0% Topic Match

Abstract: The proliferation of Internet of Things (IoT) sensors has resulted in the generation of vast volumes of data, which necessitates the implementation of an efficient real-time anomaly detection protocol. This is necessary in order to ensure the reliability and safety of the system. This paper presents a novel AI-driven framework for real-time anomaly detection in Internet of Things data streams. The purpose of this framework is to address the high velocity, volume, and variety of data that is generated by Internet of Things devices. The solution that has been proposed makes use of cutting-edge machine learning techniques, such as ensemble...

[60] FlowSpotter: Intelligent IoT Threat Detection via Imaging Network Flows
Shuaishuai Tan, ..., and Mohsen Guizani. IEEE Network, 2024. 1 citations.
0% Topic Match

Abstract: With the prevalence of Internet of Things (IoT) technologies, the huge growth of IoT devices has also brought attention of cyber attackers. IoT botnets are rapidly spreading and evolving worldwide, causing serious risks to users and data. Machine learning (ML) has shown its effectiveness on threat detection. However, existing feature encoding and learning methods are unsuitable for resource constrained edge devices like the IoT gateway. In this paper, we propose a lightweight threat detection scheme called FlowSpotter. The flow imaging mechanism requires less feature extraction but preserves more spatial and temporal information. A lite convolution neural network architecture based on...

[61] Novel Intrusion Detection Strategies With Optimal Hyper Parameters for Industrial Internet of Things Based on Stochastic Games and Double Deep Q-Networks
Shou-jian Yu, ..., and Shigen Shen. IEEE Internet of Things Journal, 2024. 10 citations.
0% Topic Match

Abstract: The Industrial Internet of Things (IIoT) has experienced rapid growth in recent years, with an increasing number of interconnected devices, thereby expanding the attack surface. Effectively detecting intrusions is crucial for safeguarding the IIoT systems from malicious attacks. However, due to the dynamic and complex nature of the IIoT environment, designing an intrusion detection strategy that balances accuracy and efficiency remains a significant challenge. In this article, we propose a novel intrusion detection strategy based on the stochastic games and deep reinforcement learning (DRL) for detecting attacks effectively while balancing detection accuracy and efficiency in the IIoT. We model the...

[62] Intrusion detection for internet of things security: a hidden Markov model based on fuzzy rough set
Yuanting Wang and Guoliang Wu. Unknown journal, 2024. 0 citations.
0% Topic Match

Abstract: Internet of Things (IoT) devices are vulnerable to various cyber-attacks. Therefore, it is significantly crucial to design an effective intrusion detection system (IDS) for IoT security. However, IoT devices have limited resources such as computing resources needing to handle a great of data, which further increases the difficulty of precise intrusion detection. Moreover, most IDSs lack transparency. This study develops a feature selection-based hidden Markov model (HMM) for intrusion detection. We first establish a modified approach based on a fuzzy rough set for feature selection to select optimal features so that the computational burden can be reduced. Furthermore, an interpretable...

[63] Network Intrusion Detection for Modern Smart Grids Based on Adaptive Online Incremental Learning
Qiuyu Lu, ..., and Jin Wang. IEEE Transactions on Smart Grid, 2025. 0 citations.

0% Topic Match

Abstract: New and evolving cyber attacks against smart grids are emerging. This necessitates that the network intrusion detection systems (IDSs) have online learning ability. However, most existing methods struggle to handle new and evolving attacks while retaining old attack knowledge, and many of them employ deep models requiring long update periods. Therefore, we propose an IDS based on adaptive online incremental learning (AdaOIL-IDS). 1) A class-correlated broad learning system (CC-BLS) is proposed for intrusion detection. A weighted CC-factor derived from intra- and inter-class correlations is introduced in CC-BLS to improve classification accuracy. CC-incremental learnings are designed to quickly add new inputs...

[64] An Efficient Feature Extraction Method for Attack Classification in IoT Networks
P. H. Do, ..., and R. Kirichek. 2021 13th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2021. 7 citations.
0% Topic Match

Abstract: Numerous attacks on the Internet of Things (IoTs) necessitate detection and prevention technologies, such as Intrusion Detection Systems (IDSs). Anomaly detection is a time-consuming and challenging task in intrusion detection systems. It requires the development of a robust classifier model capable of intelligently detecting multiple types of attacks. When different input features are provided, IDS' detection performance will fluctuate substantially. Additionally, the volume of network traffic and its multidimensional characteristics will result in a lengthy classification process. In this paper, we focus on data preprocessing and propose another feature extraction method for classifying attacks in IoT networks. Additionally, we also...

[65] An Intelligent Two-Layer Intrusion Detection System for the Internet of Things
M. Alani and A. Awad. IEEE Transactions on Industrial Informatics, 2023. 34 citations.
0% Topic Match

Abstract: The Internet of Things (IoT) has become an enabler paradigm for different applications, such as healthcare, education, agriculture, smart homes, and recently, enterprise systems. Significant advances in IoT networks have been hindered by security vulnerabilities and threats, which, if not addressed, can negatively impact the deployment and operation of IoT-enabled systems. This article addresses IoT security and presents an intelligent two-layer intrusion detection system for IoT. The system's intelligence is driven by machine learning techniques for intrusion detection, with the two-layer architecture handling flow-based and packet-based features. By selecting significant features, the time overhead is minimized without affecting detection accuracy....

[66] Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques
Ahlem Abid, ..., and O. Korbaa. Cluster Computing, 2023. 26 citations.
0% Topic Match

No summary or abstract available

[67] A Lightweight Concept Drift Detection and Adaptation Framework for IoT Data Streams
Li Yang and A. Shami. IEEE Internet of Things Magazine, 2021. 108 citations.
0% Topic Match

Abstract: In recent years, with the increasing popularity of “Smart Technology”, the number of Internet of Things (IoT) devices and systems have surged significantly. Various IoT services and functionalities are based on the analytics of IoT streaming data. However, IoT data analytics faces concept drift challenges due to the dynamic nature of IoT systems and the ever-changing patterns of IoT data streams. In this article, we propose an adaptive IoT streaming data analytics framework for anomaly detection use cases based on optimized LightGBM and concept drift adaptation. A novel drift adaptation method named Optimized Adaptive and Sliding Windowing (OASW) is proposed...

[68] TrustBlkSys: A Trusted and Blockchained Cybersecure System for IIoT
Geetanjali Rathee, ..., and Mohamed Lahby. IEEE Transactions on Industrial Informatics, 2023. 15 citations.
0% Topic Match

Abstract: Industrial Internet of Things (IIoT) has emerged as a new paradigm in the era of smart systems where interactions and transmission of messages among various entities in an industrial ecosystem are done autonomously. This includes manufacturing of products, shipment process, storage of records, and counting the data, to name a few. However, the involvement of multiple cyber threats that accompany the smart devices may lead the organizations on a heavy risk of profits. Even though the number of cybersecurity approaches have been proposed to ensure a secure and efficient communication mechanism in IIoT systems, the identification of cybersecurity issues in...

[69] Advancements in Intrusion Detection Systems for Internet of Things Using Machine Learning
Shahid Ul Haq and A. Abbas. 2022 5th International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT), 2022. 3 citations.
0% Topic Match

Abstract: Advancement in technology leads to connecting different types of devices or things to the Internet and enables the formation of a special kind of network called the Internet of Things (IoT). Intrusion detection in an IoT is a challenging task due to its unique characteristics. Machine learning schemes possess the potential to improve intrusion detection systems in case of an IoT. In this paper, we present a survey of advancements in research on the use of machine learning approaches for intrusion detection in an IoT. Our focus is on architectures, schemes, and the types of machine learning approaches used for...

[70] An Energy-Efficient Intrusion Detection Offloading Based on DNN for Edge Computing
João A. Simioni, ..., and Everton de Matos. IEEE Internet of Things Journal, 2025. 0 citations.
0% Topic Match

Abstract: To improve the accuracy of deep neural networks (DNNs) applied to network intrusion detection systems (NIDS) researchers often increase the complexity of their designed model. Given the processing limitations of resource-constrained devices, researchers have proposed offloading the NIDS task to the cloud. However, simultaneously ensuring energy efficiency and detection accuracy remains a challenge. This article proposes a DNN-based NIDS through early exits that operate following an energy-efficient edge-computing architecture implemented twofold. First, we propose a DNN-based NIDS employing multiobjective optimization for efficient inference and computation offloading. It is designed to perform the classification task at the edge device and configured...

[71] Hybrid Learning Approach of Combining Cluster-Based Partitioning and Hidden Markov Model for IoT Intrusion Detection
Sulaiman Alhaidari and M. Zohdy. Proceedings of the 2019 3rd International Conference on Information System and Data Mining, 2019. 5 citations.
0% Topic Match

Abstract: Internet of Things (IoT) is a global network that connects various types of objects "things" via internet. It becomes a core technology for various applications and more and more embedded within our daily lives and businesses. As the technology grows and evolves a number of issues will arise and be focused on in IoT, Security is one of the central issues in IoT in the last decade. However, most of today's IoT intrusion detection systems suffer from high false alarms rate with moderate accuracy and detection rates when it's not able to detect all types of IoT intrusions correctly. To...

[72] Revisiting streaming anomaly detection: benchmark and evaluation
Yang Cao, ..., and Kai Ming Ting. Artif. Intell. Rev., 2024. 1 citations.
0% Topic Match

Abstract: Anomaly detection in streaming data is an important task for many real-world applications, such as network security, fraud detection, and system monitoring. However, streaming data often exhibit concept drift, which means that the data distribution changes over time. This poses a significant challenge for many anomaly detection algorithms, as they need to adapt to the evolving data to maintain high detection accuracy. Existing streaming anomaly detection algorithms lack a unified evaluation framework that validly assesses their performance and robustness under different types of concept drifts and anomalies. In this paper, we conduct a systematic technical review of the state-of-the-art methods...

[73] Network Traffic Anomaly Detection based on Apache Spark
P. H. Pwint and T. Shwe. 2019 International Conference on Advanced Information Technologies (ICAIT), 2019. 8 citations.
0% Topic Match

Abstract: With the growing amount of internet and IoT traffic across the network, network anomaly detection system has become a popular and useful strategy to detect anomalies, attacks and intrusions. With machine learning technique, network traffic anomalies can be detected with reasonable prediction accuracy. However, most of the previous work has been focused on detecting anomalies using traditional machine learning environment. Because of ever increasing amount of data

and high speed networks, traditional machine learning environment becomes infeasible to cope with the current condition. In this paper, we investigate the feasibility of the applying one of the big data technologies, Apache...

[74] Trust-Augmented Deep Reinforcement Learning for Federated Learning Client Selection
Gaith Rjoub, ..., and A. Bataineh. Information Systems Frontiers, 2022. 30 citations.
0% Topic Match

Abstract: In the context of distributed machine learning, the concept of federated learning (FL) has emerged as a solution to the privacy concerns that users have about sharing their own data with a third-party server. FL allows a group of users (often referred to as clients) to locally train a single machine learning model on their devices without sharing their raw data. One of the main challenges in FL is how to select the most appropriate clients to participate in the training of a certain task. In this paper, we address this challenge and propose a trust-based deep reinforcement learning approach...

[75] ROAST-IoT: A Novel Range-Optimized Attention Convolutional Scattered Technique for Intrusion Detection in IoT Networks
Mahalingam Anandaraj, ..., and Qaisar Abbas. Sensors (Basel, Switzerland), 2023. 10 citations.
0% Topic Match

Abstract: The Internet of Things (IoT) has significantly benefited several businesses, but because of the volume and complexity of IoT systems, there are also new security issues. Intrusion detection systems (IDSs) guarantee both the security posture and defense against intrusions of IoT devices. IoT systems have recently utilized machine learning (ML) techniques widely for IDSs. The primary deficiencies in existing IoT security frameworks are their inadequate intrusion detection capabilities, significant latency, and prolonged processing time, leading to undesirable delays. To address these issues, this work proposes a novel range-optimized attention convolutional scattered technique (ROAST-IoT) to protect IoT networks from modern threats...

[76] Sustaining the Effectiveness of IoT-Driven Intrusion Detection over Time: Defeating Concept and Data Drifts
Omar Abdul Wahab. Unknown journal, 2021. 3 citations.
0% Topic Match

Abstract: This paper addresses the challenge of sustaining the intrusion detection effectiveness of machine learning-based intrusion detection systems in the Internet of Things (IoT) in the presence of concept and data drifts. Data drift is a phenomenon which embodies the change that happens in the relationships among the independent features, which is mainly due to changes in the data quality over time. Concept drift is a phenomenon which depicts the change in the relationships between input and output data in the machine learning model over time. To address data drifts, we first propose a series of data preparation steps that help...

[77] RADAR: Reactive Concept Drift Management with Robust Variational Inference for Evolving IoT Data Streams
Abdullah Alsaedi, ..., and Z. Tari. 2023 IEEE 39th International Conference on Data Engineering (ICDE), 2023. 3 citations.
0% Topic Match

Abstract: The accuracy and performance of Machine Learning (ML) models can gradually or even suddenly degrade when the underlying statistical distribution of data streams changes over time; this is known as concept drift. This phenomenon could adversely affect the IoT data management and analysis landscape that relies intensely on data-driven cognitive technologies. Therefore, concept drift should be detected immediately, which is challenging due to the increasing number of dimensional features and lack of ground truth. Its adaptive countermeasures also become difficult to design when data streams are being generated frequently and require latency-sensitive responses. The uncertainty and time dependencies characteristics of...

[78] Intursion detection in iot networks using feature selection and svm classificastion
Maryam Ali Hussein Al-Balhawi and G. Cansever. 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022. 2 citations.
0% Topic Match

Abstract: The steady growth in the number of devices connected to the Internet has attracted cyber criminals looking for vulnerabilities in computer networks and systems. The objective of this paper is to develop a model to identify DDoS, Infiltration, Web and Brute force attacks on computer networks, using Machine Learning (ML) techniques, increasing the accuracy, sensitivity, precision and measurement values. -F in relation to existing work.

[79] Adaptive Model Pooling for Online Deep Anomaly Detection from a Complex Evolving Data Stream
Susik Yoon, ..., and Byung Suk Lee. Proceedings of the 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2022. 25 citations.
0% Topic Match

Abstract: Online anomaly detection from a data stream is critical for the safety and security of many applications but is facing severe challenges due to complex and evolving data streams from IoT devices and cloud-based infrastructures. Unfortunately, existing approaches fall too short for these challenges; online anomaly detection methods bear the burden of handling the complexity while offline deep anomaly detection methods suffer from the evolving data distribution. This paper presents a framework for online deep anomaly detection, ARCUS, which can be instantiated with any autoencoder-based deep anomaly detection methods. It handles the complex and evolving data streams using an adaptive...

[80] Building a large scale Intrusion Detection System using Big Data technologies
Pablo Panero, ..., and Ioan Cristian Schuszter. Proceedings of International Symposium on Grids and Clouds 2018 in conjunction with Frontiers in Computational Drug Discovery — PoS(ISGC 2018 & FCDD), 2018. 2 citations.
0% Topic Match

Abstract: Computer security threats have always been a major concern and continue to increase in frequency and complexity. The nature and techniques of the attacks evolve rapidly over time, making their detection more difficult. Therefore the means and tools used to deal with them need to evolve at the same pace if not faster. In this paper the implementation of an Intrusion Detection System (IDS) both at the Network (NIDS) and Host (HIDS) level, used at CERN, is presented. The system is currently processing in real time approximately one TB of data per day, with the final goal of coping with...

[81] Impact analysis of real and virtual concept drifts on the predictive performance of classifiers
Rashmi Benni, ..., and Karibasappa Kg. Unknown journal, 2023. 3 citations.
0% Topic Match

No summary or abstract available

[82] Intrusion Detection System for IoT Based on Modified Random Forest Algorithm
O. Z. Akif, ..., and S. K. Subramaniam. Iraqi Journal for Computer Science and Mathematics, 2025. 0 citations.
0% Topic Match

Abstract: An intrusion detection system (IDS) is key to having a comprehensive cybersecurity solution against any attack, and arti cial intelligence techniques have been combined with all the features of the IoT to improve security. In response to this, in this research, an IDS technique driven by a modi ed random forest algorithm has been formulated to improve the system for IoT. To this end, the target is made as one-hot encoding, bootstrapping with less redundancy, adding a hybrid features selection method into the random forest algorithm, and modifying the ranking stage in the random forest algorithm. Furthermore, three datasets have been used...

[83] Adaptive Intrusion Detection Systems: Class Incremental Learning for IoT Emerging Threats
Francesco Cerasuolo, ..., and A. Pescapé. 2023 IEEE International Conference on Big Data (BigData), 2023. 8 citations.
0% Topic Match

Abstract: In the evolving landscape of Internet of Things (IoT) security, the need for continuous adaptation of defenses is critical. Class Incremental Learning (CIL) can provide a viable solution by enabling Machine Learning (ML) and Deep Learning (DL) models to (i) learn and adapt to new attack types (0-day attacks), (ii) retain their ability to detect known threats, (iii) safeguard computational efficiency (i.e. no full re-training). In IoT security, where novel attacks frequently emerge, CIL offers an effective tool to enhance Intrusion Detection Systems (IDS) and secure network environments. In this study, we explore how CIL approaches empower DL-based...

[84] A Comparative Analysis of Traditional and Deep Learning-Based Anomaly Detection Methods for Streaming Data
Mohsin Munir, ..., and Sheraz Ahmed. 2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA), 2019. 36 citations.
0% Topic Match

Abstract: With the Internet of Things (IoT) devices becoming an integral part of human life, the need for robust anomaly detection in streaming data has also been elevated. Dozens of distance-based, density-based, kernel-based, and cluster-based algorithms have been proposed in the area of anomaly detection. Recently, because of the robustness of the deep neural networks (DNN), different deep learning-based anomaly detection methods have also been proposed. With all these rapid developments, there exists a small number of comparative studies for anomaly detection methods. Even in those studies, the comparison is done only in typical anomaly detection settings without taking the streaming...

[85] Drift Detection and Model Update using Unsupervised AutoML in IoT
Mohamed Khalafalla Hassan and I. Y. Alshareef. WSEAS TRANSACTIONS ON COMPUTERS, 2023. 0 citations.
0% Topic Match

Abstract: This paper addresses the challenges of concept drift on the Internet of Things (IoT) environments and evaluates a machine-learning model's performance under varying data drift conditions using unsupervised Automatic Machine Learning (AutoML) anomaly detection techniques. By implementing a dynamic learning framework and employing advanced analytics, the study showcases the resilience of the proposed methodology against evolving data patterns. The results demonstrate the model's robust predictive capabilities, even in high drift scenarios, underscoring the importance of adaptive models in maintaining effective IoT security measures. The achieved improvement percentages can reach 46% for the F1 score.

[86] Federated Anomaly Detection on System Logs for the Internet of Things: A Customizable and Communication-Efficient Approach
Beibei Li, ..., and Jin Yang. IEEE Transactions on Network and Service Management, 2022. 28 citations.
0% Topic Match

Abstract: Runtime log-based anomaly detection is one of several key building blocks in ensuring system security, as well as post-incident forensic investigations. However, existing log-based anomaly detection approaches that are implemented on large-scale Internet of Things (IoT) systems generally upload local data from edge devices to a centralized (cloud) server for processing and analysis. Such a workflow incurs significant communication and computation overheads, with potential privacy implications. Hence, in this paper, we propose a customizable and communication-efficient federated anomaly detection scheme (hereafter referred to as FedLog), designed to facilitate the identification of abnormal log patterns in large-scale IoT systems. Specifically, we...

[87] DLA-ABIDS:Deep Learning Approach for Anomaly Based Intrusion Detection System
Imen Ben Ahmed, ..., and Khalil Ben Kalboussi. 2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), 2023. 1 citations.
0% Topic Match

Abstract: Nowadays, with the proliferation of the number of IoT devices, management and security of data are becoming crucial tasks. Intrusion detection systems (IDS) monitor network traffic for any unusual activity and send out alerts when it detects anomalies. The often-used intrusion detection systems are built on a variety of machine learning algorithms that allow the automation of detection on a scale that has never been achieved before. However, due to the massive size of traffic data and the nature of zero-day attacks, it is difficult to discover potential threats exploiting security vulnerabilities, which makes the detection process complicated. As a...

[88] mLBOA-DML: modified butterfly optimized deep metric learning for enhancing accuracy in intrusion detection system
V. Prabhakaran and Ashokkumar Kulandasamy. Journal of Reliable Intelligent Environments, 2023. 7 citations.
0% Topic Match

No summary or abstract available

[89] An IoT Intrusion Detection System Based on TON IoT Network Dataset
Ge Guo, ..., and Kewei Hu. 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC), 2023. 14 citations.
0% Topic Match

Abstract: As the Internet of Things (IoT) rapidly proliferate in the world, new attacks exploiting the weaknesses of the unfledged IoT technologies are emerging constantly. An Intrusion Detection System (IDS) is a powerful tool to defend IoT systems against security threats by monitoring abnormal activities on networks. As an effective approach to detecting malicious behaviors, Machine Learning (ML) has gained substantial interest from researchers. An ML-based IDS framework for IoT systems is proposed in this study and ten learning methods are applied for performance evaluation based on a recently published dataset, the TON_ IoT network dataset. Experimental results show that the...

[90] A hybrid deep learning classifier and Optimized Key Windowing approach for drift detection and adaption
Dharani Kumar Talapula, ..., and Manoj Kumar. Decision Analytics Journal, 2023. 9 citations.
0% Topic Match

No summary or abstract available

[91] RTASM: An AI-Driven Real-Time Adaptive Streaming Model for Zero-Latency Big Data Processing
Ravi Chourasia. International Journal of Advanced Research in Science, Communication and Technology, 2025. 0 citations.
0% Topic Match

Abstract: The exponential growth of real-time data from financial transactions, IoT devices, social media, and industrial applications has intensified the need for high-speed, intelligent, and fault-tolerant streaming architectures. Traditional batch-processing and micro-batch systems, such as Apache Kafka with Spark Streaming, struggle with high latency, static resource allocation, and reactive fault recovery mechanisms, making them inadequate for modern data-driven enterprises. To address these challenges, we propose the Real-Time Adaptive Streaming Model (RTASM)—an AI-driven, ultra-low-latency streaming framework that integrates Apache Kafka, Hadoop, and AI-powered dynamic optimization. RTASM introduces several groundbreaking innovations, including AI-Optimized Workload Balancing, Predictive Caching & Query Optimization, Self-Healing Disaster Recovery,...

[92] Deep Learning-Based Intrusion Detection for IoT Networks
Mengmeng Ge, ..., and A. Robles-Kelly. 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), 2019. 172 citations.
0% Topic Match

Abstract: Internet of Things (IoT) has an immense potential for a plethora of applications ranging from healthcare automation to defence networks and the power grid. The security of an IoT network is essentially paramount to the security of the underlying computing and communication infrastructure. However, due to constrained resources and limited computational capabilities, IoT networks are prone to various attacks. Thus, safeguarding the IoT network from adversarial attacks is of vital importance and can be realised through planning and deployment of effective security controls; one such control being an intrusion detection system. In this paper, we present a novel intrusion detection...

[93] A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data
Redhwan Al-amri, ..., and A. A. Alkahtani. Applied Sciences, 2021. 124 citations.
0% Topic Match

Abstract: Anomaly detection has gained considerable attention in the past couple of years. Emerging technologies, such as the Internet of Things (IoT), are known to be among the most critical sources of data streams that produce massive amounts of data continuously from numerous applications. Examining these collected data to detect suspicious events can reduce functional threats and avoid unseen issues that cause downtime in the applications. Due to the dynamic nature of the data stream characteristics, many unresolved problems persist. In the existing literature, methods have been designed and developed to evaluate certain anomalous behaviors in IoT data stream sources. However,...

[94] Mix-CL: Semi-Supervised Continual Learning for Network Intrusion Detection
Bingxin Tian, ..., and Jiuchun Ren. 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), 2024. 0 citations.
0% Topic Match

Abstract: We present an approach to address the evolving and complex challenges of network security in contemporary network environments. Our proposed framework integrates continual learning and semi-supervised learning techniques tailored for network traffic intrusion detection. We begin by assessing the effectiveness of conventional continual learning methods, such as LwF, ER, iCaRL, and DER, when faced with limited supervised data. Then we proposed Mix-CL, a semi-supervised continual learning strategy based on MixMatch. Experimental results demonstrate the efficacy of our approach in scenarios where supervision is scarce, yielding robust and efficient models for continual learning. This research offers a novel insight and methodology...

[95] An Online Intrusion Detection Method using Adaptive Multi-Level Classifier Network and PCA-Guided Model Reuse Mechanism
Haizhaoyang Huang and Hongpo Zhang. Proceedings of the 2025 4th International Conference on Cryptography, Network Security and Communication Technology, 2025. 0 citations.
0% Topic Match

Abstract: The network era caused the network security concerns to escalate dramatically, and network intrusion detection is shown as an important technology to guarantee network security. During the past few years, artificial intelligence technology has improved remarkably, and also involve advances from various studies, which started to adapt deep learning with intrusion detection models and obtained some salient detection results. However, the Internet is a developing environment, concept drift will unavoidably be produced which may result in model degeneration. Meanwhile, to tackle these difficulties, we propose an online adaptive intrusion detection method and the key point is a model reuse mechanism...

[96] Detecting the cyber-physical-social cooperated APTs in high-DER-penetrated smart grids: Threats, current work and challenges
Qiuyu Lu, ..., and Jianbo Luo. Comput. Networks, 2024. 5 citations.
0% Topic Match

No summary or abstract available

[97] AESMOTE: Adversarial Reinforcement Learning With SMOTE for Anomaly Detection
Xiangyu Ma and Wei Shi. IEEE Transactions on Network Science and Engineering, 2020. 88 citations.
0% Topic Match

Abstract: Intrusion Detection Systems (IDSs) play a vital role in securing today's Data-Centric Networks. In a dynamic environment such as the Internet of Things (IoT), which is vulnerable to various types of attacks, fast and robust solutions are in demand to handle fast-changing threats and thus the ever-increasing difficulty of detection. In this paper, we present a novel framework for the detection of anomalies, which, in particular, supports intrusion detection. The anomaly-detection framework we propose combines reinforcement learning with class-imbalance techniques. Our goal is not only to exploit the auto-learning ability of the reinforcement-learning loop but also to address the dataset...

[98] An efficient IDS using FIS to detect DDoS in IoT networks
Trong-Minh Hoang, ..., and Nam-Hoang Nguyen. 2022 9th NAFOSTED Conference on Information and Computer Science (NICS), 2022. 0 citations.
0% Topic Match

Abstract: The growing Internet of Things (IoT) applications of today have brought numerous benefits to our lives. In addition, cyber-attacks are growing as a result of increasingly sophisticated and violent attacks. Detection systems that serve as security protection against emerging attacks are also being developed using machine learning techniques. However, many additional challenges continue to emerge as demand for Intrusion Detection System (IDS) deployment at the edge network, where resource-constrained devices exist, continues to increase. These devices require a database with a high level of accuracy for attack detection. This research provides a Fuzzy-based IDS for detecting DDOS attacks with over...

[99] From Pixels to Insights: Image Datasets for AI/ML in Software-Defined Networking
Pranav Pant, ..., and L. Vashishtha. 2023 OITS International Conference on Information Technology (OCIT), 2023. 0 citations.
0% Topic Match

Abstract: In the modern landscape of pervasive digital data, the need for robust intrusion detection systems (IDS) has become paramount to safeguard networks from malicious activities. This research explores the synergistic integration of big data analytics and AI/ML techniques, with a focus on leveraging Apache Spark as a platform for intrusion detection. The study delves into the core principles underlying intelligent IDS systems enhanced by AI, leading to heightened accuracy and adaptability in countering dynamic cyber threats. The research introduces an innovative SDN DDoS attack image dataset, refined to optimize machine learning and deep learning models for IDS. Through novel image...

[100] Dimensionality reduction for detection of anomalies in the IoT traffic data
Dominik Olszewski, ..., and W. Graniszewski. Future Gener. Comput. Syst., 2023. 12 citations.
0% Topic Match

No summary or abstract available

[101] AI-Driven Anomaly Detection Framework for Improving IoT System Reliability
Sameh A. Salem, ..., and Samar M. Nour. 2024 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), 2024. 0 citations.
0% Topic Match

Abstract: Nowadays, Internet of Things (IoT) become progressively a fundamental part of our life. It revolutionizes various industries by enabling seamless connectivity between devices as well as it increases automation and efficiency. However, the reliability of IoT systems is often compromised due to the complexity and scale of these networks. It makes them vulnerable to failures and security breaches. To mitigate this problem, anomaly detection using artificial Intelligence (AI) in IoT can be a promising candidate to help data identifies unusual patterns that could indicate system faults or threats. In this paper, AI-Driven Anomaly Detection Framework for Enhancing IoT Security is...

[102] IoT-based Smart Home Security System with Machine Learning Models
Selman H1zal, ..., and Devrim AkgünAcademic Platform Journal of Engineering and Smart Systems, 2024. 2 citations.
0% Topic Match

Abstract: The Internet of Things (IoT) has various applications in practice, such as smart homes and buildings, traffic management, industrial management, and smart farming. On the other hand, security issues are raised by the growing use of IoT applications. Researchers develop machine learning models that focus on better classification accuracy and decreasing model response time to solve this security problem. In this study, we made a comparative evaluation of machine learning algorithms for intrusion detection systems on IoT networks using the DS2oS dataset. The dataset was first processed to feature extraction using the info gain attribute evaluation feature extraction approach. The...

[103] Industrial control system intrusion detection method based on belief rule base with gradient descent
Jinyuan Li, ..., and Wei Zhang. Comput. Secur., 2025. 0 citations.
0% Topic Match

No summary or abstract available

[104] Securing Fog-to-Things Environment Using Intrusion Detection System Based On Ensemble Learning
Poulmanogo Illy, ..., and S. Garg. 2019 IEEE Wireless Communications and Networking Conference (WCNC), 2019. 75 citations.
0% Topic Match

Abstract: The growing interest in the Internet of Things (IoT) applications is associated with an augmented volume of security threats. In this vein, the Intrusion detection systems (IDS) have emerged as a viable solution for the detection and prevention of malicious activities. Unlike the signature-based detection approaches, machine learning-based solutions are a promising means for detecting unknown attacks. However, the machine learning models need to be accurate enough to reduce the number of false alarms. More importantly, they need to be trained and evaluated on realistic datasets such that their efficacy can be validated on real-time deployments. Many solutions proposed in...

[105] A Data Sampling and Two-Stage Convolution Neural Network for IoT Devices Identification
Trong Binh Hoang, ..., and Nguyen Quang Uy. 2022 RIVF International Conference on Computing and Communication Technologies (RIVF), 2022. 1 citations.
0% Topic Match

Abstract: The rapid development of Internet of Things (IoT) enables emerging user services and applications to improve life quality. However, the presence of rogue IoT devices can result in the vulnerabilities that hurt users. In order to address this threat, organizations often apply security policies in which only the connection of white-listed IoT devices is permitted. To obtain that goal, organizations must be able to identify the IoT devices connected to their networks and, more specifically, to identify connected IoT devices that are not in the white-list (unknown devices). However, for new/unknown devices, it is often difficult to collect enough data...

[106] A Lightweight Intrusion Detection System for Internet of Things: Clustering and Monte Carlo Cross-Entropy Approach

Abdulmohsen Almalawi. Sensors (Basel, Switzerland), 2025. 0 citations.
0% Topic Match

Abstract: Our modern lives are increasingly shaped by the Internet of Things (IoT), as IoT devices monitor and manage everything from our homes to our workplaces, becoming an essential part of health systems and daily infrastructure. However, this rapid growth in IoT has introduced significant security challenges, leading to increased vulnerability to cyber attacks. To address these challenges, machine learning-based intrusion detection systems (IDSs)—traditionally considered a primary line of defense—have been deployed to monitor and detect malicious activities in IoT networks. Despite this, these IDS solutions often struggle with the inherent resource constraints of IoT devices, including limited computational power and...

[107] KRF-AD: Innovating anomaly detection with KDE-KL and random forest fusion
Aarthi Gopalakrishnan, ..., and W. A. Banu. Intelligent Decision Technologies, 2024. 1 citations.
0% Topic Match

Abstract: Anomaly detection in Intrusion Detection System (IDS) data refers to the process of identifying and flagging unusual or abnormal behavior within a network or system. In the context of IoT, anomaly detection helps in identifying any abnormal or unexpected behavior in the data generated by connected devices. Existing methods often struggle with accurately detecting anomalies amidst massive data volumes and diverse attack patterns. This paper proposes a novel approach, KDE-KL Anomaly Detection with Random Forest Integration (KRF-AD), which combines Kernel Density Estimation (KDE) and Kullback-Leibler (KL) divergence with Random Forest (RF) for effective anomaly detection. Additionally, Random Forest (RF) integration...

[108] A Scalable, Lightweight AI-Driven Security Framework for IoT Ecosystems: Optimization and Game Theory Approaches
K. Chaganti. IEEE Access, 2025. 0 citations.
0% Topic Match

Abstract: The rapid growth of IoT has introduced significant security challenges, particularly in scalability, real-time threat detection, and resource management. Traditional security models struggle with an increasing number of interconnected devices, often reacting to threats rather than proactively mitigating them. This study proposes a three-layer security framework that combines artificial intelligence-based intrusion detection, blockchain for decentralized trust management, and edge computing for efficient resource utilization. Machine learning enhances anomaly detection, blockchain ensures secure data integrity, and edge computing reduces latency. Optimization techniques improve the detection accuracy from 94.2% to 94.78%, reduce the response time by 14.98%, and optimize the energy consumption...

[109] Machine Learning-Assisted Intrusion Detection for Enhancing Internet of Things Security
Mona Esmaeili, ..., and Hadi Jabbari Saray. ArXiv, 2024. 4 citations.
0% Topic Match

Abstract: Attacks against the Internet of Things (IoT) are rising as devices, applications, and interactions become more networked and integrated. The increase in cyber-attacks that target IoT networks poses a considerable vulnerability and threat to the privacy, security, functionality, and availability of critical systems, which leads to operational disruptions, financial losses, identity thefts, and data breaches. To efficiently secure IoT devices, real-time detection of intrusion systems is critical, especially those using machine learning to identify threats and mitigate risks and vulnerabilities. This paper investigates the latest research on machine learning-based intrusion detection strategies for IoT security, concentrating on real-time responsiveness, detection...

[110] A novel unsupervised framework for time series data anomaly detection via spectrum decomposition
Tianyang Lei, ..., and Jichao Li. Knowl. Based Syst., 2023. 17 citations.
0% Topic Match

No summary or abstract available

[111] Concept drift detection with False Positive rate for multi-label classification in IoT data stream
Pingfan Wang, ..., and Gerhard Fehringer. 2020 International Conference on UK-China Emerging Technologies (UCET), 2020. 6 citations.
0% Topic Match

Abstract: Machine learning, as a significant component of the Industrial Internet of Things (IIoT), has been widely applied in many fields. The continuously generated data from the various sensors are collected and stored, this is also known as a data stream. However, the non-stationary phenomenon in data stream, concept drift, is important to be detected immediately for the operation of the IoT system. Therefore, the detection method for concept drift is needed to alert the requirement to maintain or replace some components in advance, so as to avoid or mitigate the risk of malfunction of the IoT system. The majority of...

[112] Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning
M. Ferrag, ..., and H. Janicke. IEEE Access, 2022. 463 citations.
0% Topic Match

Abstract: In this paper, we propose a new comprehensive realistic cyber security dataset of IoT and IIoT applications, called Edge-IIoTset, which can be used by machine learning-based intrusion detection systems in two different modes, namely, centralized and federated learning. Specifically, the dataset has been generated using a purpose-built IoT/IIoT testbed with a large representative set of devices, sensors, protocols and cloud/edge configurations. The IoT data are generated from various IoT devices (more than 10 types) such as Low-cost digital sensors for sensing temperature and humidity, Ultrasonic sensor, Water level detection sensor, pH Sensor Meter, Soil Moisture sensor, Heart Rate Sensor, Flame...

[113] Intrusion Detection System for High Volume and High Velocity Packet Streams: A Clustering Approach
D. Sitaram, ..., and Rishika Todi. International journal of innovation, management and technology, 2013. 5 citations.
0% Topic Match

Abstract: Abstract—The success of any Intrusion Detection System lies in its ability to quickly adapt to new threats in near real time and further prevent new attacks. This implies extremely efficient machine learning algorithms in the backend, which in turn may use clustering algorithms capable of distinguishing between normal and anomalous network traffic. This work is a first step towards proposing such an IDS, which is built on clustering-based machine learning. The authors evaluate different clustering algorithms using a network packet trace and provide results, which help in evaluating these algorithms. The work-in-progress section of the paper visualizes the IDS...

[114] Intrusion Detection for Unmanned Aerial Vehicles Security: A Tiny Machine Learning Model
Yixuan Wu, ..., and Li Zheng. IEEE Internet of Things Journal, 2024. 8 citations.
0% Topic Match

Abstract: Unmanned aerial vehicles (UAVs) are vulnerable to network attacks. Designing an effective intrusion detection system (IDS) for UAVs is crucial. However, UAVs have limited computing resources and need to deal with massive amounts of network data, which further increases the difficulty of detection. Moreover, most existing IDSs have large parameters. In this study, we develop a tiny machine learning-based IDS to solve the above issue. We first establish an improved fuzzy rough set (FRS) model based on adaptive neighborhoods. Then, using the proposed FRS model, we employ a feature selection (FS) method to select optimal features and reduce the overall...

[115] Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends
Saida Hafsa Rafique, ..., and Thangavel Murugan. Sensors (Basel, Switzerland), 2024. 47 citations.
0% Topic Match

Abstract: With its exponential growth, the Internet of Things (IoT) has produced unprecedented levels of connectivity and data. Anomaly detection is a security feature that identifies instances in which system behavior deviates from the expected norm, facilitating the prompt identification and resolution of anomalies. When AI and the IoT are combined, anomaly detection becomes more effective, enhancing the reliability, efficacy, and integrity of IoT systems. AI-based anomaly detection systems are capable of identifying a wide range of threats in IoT environments, including brute force, buffer overflow, injection, replay attacks, DDos attack, SQL injection, and back-door exploits. Intelligent Intrusion Detection Systems (IDSs)...

[116] Deep Clustering Based Latent Representation for IoT Malware Detection
Huu Noi Nguyen, ..., and V. Cao. 2023 12th International Conference on Control, Automation and Information Sciences (ICCAIS), 2023. 0 citations.
0% Topic Match

Abstract: The Internet of Things with a billion connected devices can generate a huge amount of data daily. This poses challenges to security tasks (i.e. identifying IoT malware). Our previous studies used analytic techniques to reduce the data size and extract valuable information. Currently, clustering is a key technique for many data-driven applications, and it has been widely studied with different distance functions and algorithms. One research direction is to use representation learning for

clustering. This research proposes a combination of Deep Clustering AutoEncoder (DCAE) with anomaly detection algorithms for an end-to-end anomaly detection framework. The DCAE maps the data from...

[117] Deep learning for cyber threat detection in IoT networks: A review
Alyazia Aldhaheri, ..., and A. Battah. Internet of Things and Cyber-Physical Systems, 2023. 57 citations.
0% Topic Match
No summary or abstract available

[118] A novel approach to IoT security for intrusion detection system using ensemble network and heuristic-assisted feature fusion
Atul B. Kathole, ..., and Ankur Goyal. Journal of Discrete Mathematical Sciences and Cryptography, 2024. 1 citations.
0% Topic Match
Abstract: The area of “Internet of Things (IoT)” has gained popularity recently as a method for developing intelligent models. Security and privacy are regarded as the two main issues in every real-world IoT application. The security risks posed by IoT-enabled devices are serious threats to the development of the smart industry. Thus, to reduce the security dangers that emanate from IoT devices and give birth to numerous security concerns, Intrusion Detection Systems (IDSs) specifically tailored for the IoT sectors are important. Conventional intrusion detection systems (IDSs) are unsuitable for use in standard Internet of Things (IoT) networks for a variety of...

[119] Learning under Concept Drift: A Review
Jie Lu, ..., and Guangquan Zhang. IEEE Transactions on Knowledge and Data Engineering, 2019. 1295 citations.
0% Topic Match
Abstract: Concept drift describes unforeseeable changes in the underlying distribution of streaming data over time. Concept drift research involves the development of methodologies and techniques for drift detection, understanding, and adaptation. Data analysis has revealed that machine learning in a concept drift environment will result in poor learning results if the drift is not addressed. To help researchers identify which research topics are significant and how to apply related techniques in data analysis tasks, it is necessary that a high quality, instructive review of current research developments and trends in the concept drift field is conducted. In addition, due to the...

[120] Design of Intrusion Detection and Response Mechanism for Power Grid SCADA Based on Improved LSTM and FNN
Yu Huang and Liangyuan Su. IEEE Access, 2024. 3 citations.
0% Topic Match
Abstract: The current behavior pattern extraction methods in intrusion detection systems cannot fully extract information. To improve the accuracy of such systems, the study first uses sequence feature construction algorithms to explicitly represent sequence feature information. Afterwards, an intrusion detection system is designed that combines long short-term memory networks and feed-forward neural networks to remember sequence information and adjust output dimensions, thereby mapping the results to classification labels. According to the simulation comparison results, the designed system had a significantly higher packet capture rate per second compared with the other three intrusion detection systems. When the intrusion rates were 10% and...

[121] Isolation-Based Anomaly Detection
Fei Tony Liu, ..., and Zhi-Hua Zhou. ACM Trans. Knowl. Discov. Data, 2012. 1663 citations.
0% Topic Match
No summary or abstract available

[122] A pdf-Free Change Detection Test Based on Density Difference Estimation
Li Bu, ..., and Dongbin Zhao. IEEE transactions on neural networks and learning systems, 2018. 71 citations.
0% Topic Match
Abstract: The ability to detect online changes in stationarity or time variance in a data stream is a hot research topic with striking implications. In this paper, we propose a novel probability density function-free change detection test, which is based on the least squares density-difference estimation method and operates online on multidimensional inputs. The test does not require any assumption about the underlying data distribution, and is able to operate immediately after having been configured by adopting a reservoir sampling mechanism. Thresholds requested to detect a change are automatically derived once a false positive rate is set by the application designer....

[123] A systematic review of metaheuristics-based and machine learning-driven intrusion detection systems in IoT
Mohammad Shamim Ahsan, ..., and Swakkhar Shatabda. Swarm and Evolutionary Computation, 2025. 0 citations.
0% Topic Match
No summary or abstract available

[124] Online Machine Learning from Non-stationary Data Streams in the Presence of Concept Drift and Class Imbalance: A Systematic Review
A. S. Palli, ..., and Mazni Omar. Journal of Information and Communication Technology, 2024. 9 citations.
0% Topic Match
Abstract: In IoT environment applications generate continuous non-stationary data streams with in-built problems of concept drift and class imbalance which cause classifier performance degradation. The imbalanced data affects the classifier during concept detection and concept adaptation. In general, for concept detection, a separate mechanism is added in parallel with the classifier to detect the concept drift called a drift detector. For concept adaptation, the classifier updates itself or trains a new classifier to replace the older one. In case, the data stream faces a class imbalance issue, the classifier may not properly adapt to the latest concept. In this survey, we...

[125] A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems
E. Benkhelifa, ..., and W. Hamouda. IEEE Communications Surveys & Tutorials, 2018. 159 citations.
0% Topic Match
No summary or abstract available

[126] A Clustering Strategy for Enhanced FL-Based Intrusion Detection in IoT Networks
Jacopo Talpini, ..., and Marco Savi. ArXiv, 2023. 5 citations.
0% Topic Match
Abstract: The Internet of Things (IoT) is growing rapidly and so the need of ensuring protection against cybersecurity attacks to IoT devices. In this scenario, Intrusion Detection Systems (IDSs) play a crucial role and data-driven IDSs based on machine learning (ML) have recently attracted more and more interest by the research community. While conventional ML-based IDSs are based on a centralized architecture where IoT devices share their data with a central server for model training, we propose a novel approach that is based on federated learning (FL). However, conventional FL is ineffective in the considered scenario, due to the high statistical...

[127] Isolation Forest
Fei Tony Liu, ..., and Zhi-Hua Zhou. 2008 Eighth IEEE International Conference on Data Mining, 2008. 4704 citations.
0% Topic Match
No summary or abstract available

[128] Modeling Intrusion Detection for the Landscape Design Software Procreate from Data Layer
Xiang Zhao and Lushan Shi. 2024 Second International Conference on Inventive Computing and Informatics (ICICI), 2024. 0 citations.
0% Topic Match
Abstract: In today's digital landscape, network security faces escalating challenges with the proliferation of cyber threats. Intrusion detection is a central defense mechanism against these threats, requiring constant innovation and refinement. This study presents a novel approach to modeling intrusion detection specifically tailored to Procreate, a landscape design software, with a focus on the data layer. Leveraging machine learning and deep learning techniques, proposed methodology encompasses comprehensive steps including feature selection, data processing, and model implementation. Through experimentation and comparison with the traditional methods, the proposed model demonstrates superior performance in terms of accuracy, error rate, recall rate, precision, F-measure, AUC,...

[129] Efficient Learning-driven Anomaly Detection and Classification for IoT-based Monitoring Systems

Mayura Tapkire. Journal of Electrical Systems, 2024. 1 citations.
0% Topic Match

Abstract: The Internet of Things (IoT) has revolutionized data collection and analysis from diverse sources. IoT-based monitoring systems are now widespread in manufacturing, healthcare, and smart cities. These systems gather vast amounts of data from sensors and devices, enabling the detection of anomalies and patterns. The IoT has become an integral part of our lives, transforming various industries by enabling seamless connectivity between devices and increasing automation and efficiency. However, the reliability of IoT systems is often compromised due to the complexity and scale of these networks, making them vulnerable to failures and security breaches. To mitigate this problem, anomaly detection...

[130] Privacy-Preserving Attribute-Based Access Control Scheme With Intrusion Detection and Policy Hiding for Data Sharing in VANET
Zhihua Wang, ..., and Wei Song. IEEE Internet of Things Journal, 2024. 2 citations.
0% Topic Match

Abstract: Vehicle ad-hoc network (VANET) plays an important role in improving traffic management and driving safety. Data sharing in VANET can be achieved using such communications as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Cloud (V2C). However, due to the openness of VANET, if an adversary can access shared data without authorization, it will seriously threaten vehicle safety and user privacy, and bring great challenges to data sharing. Therefore, it is necessary to establish an efficient access control scheme for secure data sharing in cloud-assisted VANET. Attribute-based encryption (ABE) can achieve fine-grained access control. However, the traditional access control schemes for VANET rarely...

[131] Future Industrial Production Work Designusing Clustering Approach: Transitioning to Cyber Physical Systems
Kanika Gupta, ..., and Anishkumar Dhablia. 2023 International Conference on Data Science and Network Security (ICDSNS), 2023. 0 citations.
0% Topic Match

Abstract: The proliferation of Internet of Things (IoT) devices and infrastructure has prompted the development of several IoT data analytics methods for detecting hostile cyberattacks and keeping IoT infrastructure safe. The intrinsic instability of IoT data, however, may cause concept drift concerns in IoT data analytics, which in turn can cause model deterioration and the inability to detect assaults. This is due to the fact that static models used in conventional data analytics cannot accommodate for shifts in the distribution of data. In a smart factory, industrial equipment is outfitted with thousands of interconnected devices or sensors that collect and transmit...

[132] Hybrid Machine Learning Models for Intrusion Detection in IoT: Leveraging a Real-World IoT Dataset
Md Ahnaf Akif, ..., and Imadeldin Mahgoub. ArXiv, 2025. 0 citations.
0% Topic Match

Abstract: The rapid growth of the Internet of Things (IoT) has revolutionized industries, enabling unprecedented connectivity and functionality. However, this expansion also increases vulnerabilities, exposing IoT networks to increasingly sophisticated cyberattacks. Intrusion Detection Systems (IDS) are crucial for mitigating these threats, and recent advancements in Machine Learning (ML) offer promising avenues for improvement. This research explores a hybrid approach, combining several standalone ML models such as Random Forest (RF), XGBoost, K-Nearest Neighbors (KNN), and AdaBoost, in a voting-based hybrid classifier for effective IoT intrusion detection. This ensemble method leverages the strengths of individual algorithms to enhance accuracy and address challenges related...

[133] A survey of outlier detection in high dimensional data streams
Imen Souiden, ..., and Zaki Brahmi. Comput. Sci. Rev., 2022. 58 citations.
0% Topic Match

No summary or abstract available

[134] A Survey on IoT Intrusion Detection: Federated Learning, Game Theory, Social Psychology, and Explainable AI as Future Directions
Sarhad Arisdakessian, ..., and M. Guizani. IEEE Internet of Things Journal, 2023. 101 citations.
0% Topic Match

Abstract: In the past several years, the world has witnessed an acute surge in the production and usage of smart devices which are referred to as the Internet of Things (IoT). These devices interact with each other as well as with their surrounding environments to sense, gather and process data of various kinds. Such devices are now part of our everyday's life and are being actively used in several verticals, such as transportation, healthcare, and smart homes. IoT devices, which usually are resource-constrained, often need to communicate with other devices, such as fog nodes and/or cloud computing servers to accomplish certain...

[135] A Deep Autoencoder Based Outlier Detection Model for Intrusion Detection Systems in Wireless Sensor Networks
Shourya Shukla, ..., and Shalini Singh. 2025 3rd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT), 2025. 0 citations.
0% Topic Match

Abstract: With advancements in Wireless Sensor Network technologies, a large inflow of data is observed in the networks. Security threats have been rising in the recent years. These frequent security threats have created an urgency to upgrade the Intrusion Detection Systems to highly complex methods. Hence, increasing the computation overhead on the energy limited WSN nodes. These nodes sometimes undergo data or network anomalies while transmitting or receiving packets, creating outliers. In order to remove the outlier, a Hybrid Convolutional Neural Network, Fully Connected Network based Autoencoder has been proposed. The proposed algorithm successfully mitigated more than 31,000 outlier instances. Further,...

[136] The analysis of the internet of things database query and optimization using deep learning network model
Xiaowen Ma. PLOS ONE, 2024. 0 citations.
0% Topic Match

Abstract: To explore the application effect of the deep learning (DL) network model in the Internet of Things (IoT) database query and optimization. This study first analyzes the architecture of IoT database queries, then explores the DL network model, and finally optimizes the DL network model through optimization strategies. The advantages of the optimized model in this study are verified through experiments. Experimental results show that the optimized model has higher efficiency than other models in the model training and parameter optimization stages. Especially when the data volume is 2000, the model training time and parameter optimization time of the optimized...

[137] Deep Learning Based Intrusion Detection System for Network Security in IoT System
Jennifer E Joseph, ..., and Onyinyechukwu Prisca Onyeanisi. International Journal of Education, Management, and Technology, 2025. 0 citations.
0% Topic Match

Abstract: The Internet of Things (IoT) has grown rapidly, leading to unparalleled connectivity and vast amounts of data. Anomaly detection plays a crucial role in identifying unusual behavior that deviates from the system's normal operation, enabling the swift detection and resolution of these anomalies. The integration of artificial intelligence (AI) with IoT significantly improves the effectiveness of anomaly detection, enhancing the performance, dependability, and security of IoT systems. AI-powered anomaly detection methods can recognize a wide array of threats within IoT environments, such as brute force attacks, buffer overflows, injection attacks, replay attacks, Distributed Denial of Service (DDoS) attacks, SQL injection,...

[138] Leveraging Machine Learning Techniques in Intrusion Detection Systems for Internet of Things
Saeid Jamshidi, ..., and Foutse Khomh. ArXiv, 2025. 0 citations.
0% Topic Match

Abstract: As the Internet of Things (IoT) continues to expand, ensuring the security of connected devices has become increasingly critical. Traditional Intrusion Detection Systems (IDS) often fall short in managing the dynamic and large-scale nature of IoT networks. This paper explores how Machine Learning (ML) and Deep Learning (DL) techniques can significantly enhance IDS performance in IoT environments. We provide a thorough overview of various IDS deployment strategies and categorize the types of intrusions common in IoT systems. A range of ML methods -- including Support Vector Machines, Naive Bayes, K-Nearest Neighbors, Decision Trees, and Random Forests -- are examined alongside...

[139] Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey
Afrah Gueriani, ..., and A. Mazari. 2023 2nd International Conference on Electronics, Energy and Measurement (IC2EM), 2023. 17 citations.
0% Topic Match

Abstract: The rise of new complex attacks scenarios in Internet of things (IoT) environments necessitate more advanced and intelligent cyber defense techniques such as various Intrusion Detection Systems (IDSs) which are responsible for detecting and mitigating malicious activities in IoT networks without human intervention. To address this issue, deep reinforcement learning (DRL) has been proposed in recent years, to automatically tackle intrusions/attacks. In this paper, a comprehensive

survey of DRL-based IDS on IoT is presented. Furthermore, in this survey, the state-of-the-art DRL-based IDS methods have been classified into five categories including wireless sensor network (WSN), deep Q-network (QP), healthcare, hybrid, and...

[140] Leveraging AI for Intrusion Detection in IoT Ecosystems: A Comprehensive Study
Shashi Bhushan Sharma and Amit Kumar Bairwa. IEEE Access, 2025. 0 citations.
0% Topic Match

Abstract: The widespread adoption of Internet of Things (IoT) devices has brought about unprecedented connectivity and convenience, but it has also ushered in new security challenges. As IoT systems become integral parts of various domains, protecting them from malicious intrusions is crucial. This paper thoroughly examines how Artificial Intelligence (AI) techniques are applied to develop practical Intrusion Detection Systems (IDS) specifically designed for IoT environments. The examination comprehensively analyzes current state-of-the-art AI methodologies utilized in IoT-based IDS, including machine learning, deep learning, and anomaly detection algorithms. The paper delves into IoT systems' distinctive characteristics and vulnerabilities that demand specialized intrusion detection...

[141] Anomaly detection model based on data stream clustering
Chunyong Yin, ..., and Jin Wang. Cluster Computing, 2017. 30 citations.
Not measured Topic Match

No summary or abstract available

[142] Intrusion detection systems in the Internet of things: A comprehensive investigation
Somayye Hajiheidari, ..., and Nima Jafari Navimipour. Comput. Networks, 2019. 176 citations.
Not measured Topic Match

No summary or abstract available

[143] Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things
Geethapriya Thamilarasu and Shiven Chawla. Sensors (Basel, Switzerland), 2019. 220 citations.
Not measured Topic Match

Abstract: Cyber-attacks on the Internet of Things (IoT) are growing at an alarming rate as devices, applications, and communication networks are becoming increasingly connected and integrated. When attacks on IoT networks go undetected for longer periods, it affects availability of critical systems for end users, increases the number of data breaches and identity theft, drives up the costs and impacts the revenue. It is imperative to detect attacks on IoT systems in near real time to provide effective security and defense. In this paper, we develop an intelligent intrusion-detection system tailored to the IoT environment. Specifically, we use a deep-learning algorithm...

[144] A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security
M. Al-garadi, ..., and M. Guizani. IEEE Communications Surveys & Tutorials, 2018. 830 citations.
Not measured Topic Match

Abstract: The Internet of Things (IoT) integrates billions of smart devices that can communicate with one another with minimal human intervention. IoT is one of the fastest developing fields in the history of computing, with an estimated 50 billion devices by the end of 2020. However, the crosscutting nature of IoT systems and the multidisciplinary components involved in the deployment of such systems have introduced new security challenges. Implementing security measures, such as encryption, authentication, access control, network and application security for IoT devices and their inherent vulnerabilities is ineffective. Therefore, existing security methods should be enhanced to effectively secure the...

[145] A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework
Nickolaos Koroniotis, ..., and E. Sitnikova. Future Gener. Comput. Syst., 2020. 158 citations.
Not measured Topic Match

No summary or abstract available

[146] Principal Component Analysis
I. Jolliffe. Technometrics, 2003. 27691 citations.
Not measured Topic Match

Abstract: Principal component analysis is one of the most important and powerful methods in chemometrics as well as in a wealth of other areas. This paper provides a description of how to understand, use, and interpret principal component analysis. The paper focuses on the use of principal component analysis in typical chemometric areas but the results are generally applicable.

[147] Advances in Knowledge Discovery and Data Mining: 9th Pacific-Asia Conference, PAKDD 2005, Hanoi, Vietnam, May 18-20, 2005, Proceedings
T. Ho, ..., and Huan Liu. Unknown journal, 1997. 2 citations.
Not measured Topic Match

No summary or abstract available

[148] A Deep Learning Approach for Real-Time Application-Level Anomaly Detection in IoT Data Streaming
Mahsa Raeiszadeh, ..., and R. Mini. 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC), 2023. 1 citations.
Not measured Topic Match

Abstract: The growth of streaming data originating from Internet of Things (IoT)-based Industry 4.0 opens doors to real-time analytics of time-sensitive services. However, this ever-increasing amount of data inevitably leads to anomalies, resulting in considerable risks for time-sensitive applications. Thus, real-time detection of anomalies is critical to prevent impending failures and resolve them in time. Given that the problem is to detect application-level anomalies in real time, we develop a deep learning-based technique, which integrates time-series data inference with a Long-Short Term Memory (LSTM)-based prediction model. Our proposed method relies on a novel metric called Sequence Inconsistency Distance (SID), which determines...

[149] VEAD: Variance profile Exploitation for Anomaly Detection in real-time IoT data streaming
K. T. Le, ..., and Hyunseung Choo. Internet Things, 2023. 3 citations.
Not measured Topic Match

No summary or abstract available

[150] Real-Time Adaptive Anomaly Detection in Industrial IoT Environments
Mahsa Raeiszadeh, ..., and Raquel A. F. Mini. IEEE Transactions on Network and Service Management, 2024. 1 citations.
Not measured Topic Match

Abstract: To ensure reliability and service availability, next-generation networks are expected to rely on automated anomaly detection systems powered by advanced machine learning methods with the capability of handling multi-dimensional data. Such multi-dimensional, heterogeneous data occurs mostly in today's Industrial Internet of Things (IIoT), where real-time detection of anomalies is critical to prevent impending failures and resolve them in a timely manner. However, existing anomaly detection methods often fall short of effectively coping with the complexity and dynamism of multi-dimensional data streams in IIoT. In this paper, we propose an adaptive method for detecting anomalies in IIoT streaming data utilizing a...

[151] Low-Latency Dimensional Expansion and Anomaly Detection Empowered Secure IoT Network
Wenhao Shao, ..., and N. Crespi. IEEE Transactions on Network and Service Management, 2023. 4 citations.
Not measured Topic Match

Abstract: The Internet of Things (IoT) consists of a myriad of smart devices and offers tremendous innovation opportunities in industry, homes, and businesses to enhance the productivity and the quality of life. However, ecosystem of infrastructures and the services associated with IoT devices have introduced a new set of vulnerabilities and threats, resulting in abnormal values of information collected by sensors, jeopardizing system security. To secure sensor networks, it must be possible to detect such anomalies or sequences of patterns in IoT devices that significantly deviate from normal behavior. To perform this task, this paper proposes a real-time streaming anomaly detection...

[152] Examining a generic streaming architecture for smart manufacturing's Big data processing in Anomaly detection: A review and a proposal
Milton Samadder, ..., and Alok Kumar Roy. International Journal of Experimental Research and Review, 2023. 3 citations.

Not measured Topic Match

Abstract: The smart manufacturing industry has witnessed a rapid increase in data generation due to the integration of sensors, IoT devices, and other advanced technologies. With this huge amount of data, the need for efficient data processing methods becomes critical for identifying anomalies in real-time. With the rise of Industry 4.0 practices, digitally enabled manufacturing units are shifting their focus towards Smart Manufacturing paradigm for better productivity, throughput and increased business volume. Traditionally digital manufacturing units have considered different AI approaches like Neural Network, Statistical Methods, Deep Learning etc. to detect and predict anomalies in their production lines. But with the...

[153] Real-Time Deep Anomaly Detection Framework for Multivariate Time-Series Data in Industrial IoT
Hussain Nizam, ..., and Xiaopeng Hu. IEEE Sensors Journal, 2022. 85 citations.
Not measured Topic Match

Abstract: The data produced by millions of connected devices and smart sensors in the Industrial Internet of Things (IIoT) is highly dynamic, large-scale, heterogeneous, and time-stamped. These time-stamped data are the core of IIoT automation and have the potential to affect industrial processes intensely. It poses significant challenges to effectively detect anomalies from time-series data and deliver actionable insights in real time to drive improvements to industrial processes. In most practical applications, where data are used to make automated decisions, real-time anomaly detection is critical. With this focus, in this article, we advise a hybrid end-to-end deep anomaly detection (DAD) framework...

[154] Leveraging Semisupervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication
Yongliang Cheng, ..., and Yi Liu. IEEE Internet of Things Journal, 2021. 54 citations.
Not measured Topic Match

Abstract: The rapid development of the Internet of Things (IoT) accumulates a large number of communication records, which are utilized for anomaly detection in IoT communication. However, only a small part of these records can be labeled, which increases the difficulty in anomaly detection. This article proposes a semisupervised hierarchical stacking temporal convolutional network (HS-TCN), which is the first semisupervised model for anomaly detection in IoT communication, and it can train unlabeled data based on a small number of labeled data. Furthermore, HS-TCN fully considers the features of streaming data in IoT communication and can weed out uncertain records. Finally, the...

[155] Enhanced Anomaly Detection in IoT Through Transformer-Based Adversarial Perturbations Model
Saher Zia, ..., and Afnan Alhazmi. Electronics, 2025. 0 citations.
Not measured Topic Match

Abstract: Ensuring data security in IoT systems requires effective anomaly detection, particularly in multivariate time series data generated by sensor networks. This study introduces a transformer-based method to detect anomalies by capturing complex temporal patterns and long-range dependencies. The model adapts to diverse anomaly types across datasets, leveraging adversarial perturbations to enhance robustness and accuracy. Integration of the Streaming Peaks Over Threshold (SPOT) mechanism further improves thresholding. Experiments on MSL, SMD, NAB, and SWaT datasets validate the model's effectiveness, demonstrating its competitive performance in strengthening IoT systems and ensuring data security in dynamic environments.

[156] Detecting Anomaly in IoT Devices using Multi-Threaded Autonomous Anomaly Detection
Muhammad Yunus Iqbal Basheer, ..., and Sharifalillah Nordin. 2021 4th International Symposium on Agents, Multi-Agent Systems and Robotics (ISAMSR), 2021. 3 citations.
Not measured Topic Match

Abstract: In this paper, we proposed a multi-threaded anomaly detection algorithm that works autonomously and without any prior assumption in streaming data. The proposed algorithm was upgraded from the autonomous anomaly detection (AAD) algorithm. The difference is we change the AAD algorithm from working offline to online by using IoT devices. Furthermore, to make it fast, we change the algorithm to process asynchronously. Before this, the AAD algorithm works in offline and worked in synchronous processing. Although AAD was altered to receive online data from IoT devices, the algorithm performance is still slow. Hence, this paper aims to prove that multi-threaded...

[157] RADAR: A Robust Behavioral Anomaly Detection for IoT Devices in Enterprise Networks (CMU-CyLab-19-003)
Tian-jiao Yu, ..., and S. Seshan. Unknown journal, 2021. 4 citations.
Not measured Topic Match

Abstract: IoT devices deployed inside enterprise networks (e.g., routers, storage appliances, cameras) are emerging security threats for enterprises. It is impractical for security administrators to address IoT threats with existing enterprise or smart home security techniques, e.g., host-based or mobile-based detection are not applicable, network firewall rules are too coarse-grained, signature-based detection fails with zero-day attacks, and existing anomaly detection mechanisms are ineffective for IoT devices (e.g., cannot detect IoT backdoor access) as they are proposed for computer activities (e.g., email spear phishing). Fortunately, we observe that unlike generalpurpose computing devices, the normal behavior of an IoT device is limited (e.g.,...

[158] A secure IoT architecture for streaming data analysis and anomaly detection
S. Clémençon, ..., and Mariona Roca. Unknown journal, 2018. 0 citations.
Not measured Topic Match

No summary or abstract available

[159] HS-TCN: A Semi-supervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT
Yongliang Cheng, ..., and Yi Liu. 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC), 2019. 23 citations.
Not measured Topic Match

Abstract: The rapid development of Internet of Things (IoT) accumulates lots of communication data. Not being processed in time, these massive data increase the difficulty of anomaly detection for smart service. Furthermore, labeling all communication data is unpractical. Therefore, it is necessary to accomplish some feasible ways which can incorporate unlabeled data effectively. In recent years, Temporal Convolutional Network (TCN) has been proposed to solve sequence problems and got better performance compared to Recurrent Neural Network (RNN) in most cases. This paper proposes a semi-supervised hierarchical stacking TCN for the first time, which concentrates on the anomaly detection of the communication...

[160] Anomaly Detection over Streaming Data: Indy500 Case Study
Chathura Widanage, ..., and J. Koskey. 2019 IEEE 12th International Conference on Cloud Computing (CLOUD), 2019. 11 citations.
Not measured Topic Match

Abstract: Sports racing is attracting billions of audiences each year. It is powered and transformed by the latest data analysis technologies, from race car design, driving skill improvements to audience engagement on social media. However, most of the data processing are off-line and retrospective analysis. The emerging real-time data analysis from the Internet of Things (IoT) result in fast data streams generated from distributed sensors. Applying advanced Machine Learning/Artificial Intelligence over such data streams to discover new information, predict future insights and make control decision is a crucial process. In this paper, we start by articulating racing car big data characteristics...

[161] (POSTER) Unsupervised and Condition Invariant Anomaly Detection for The Constrained Edge
Chandrakanth R. Kancharla, ..., and H. Hallez. 2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), 2023. 0 citations.
Not measured Topic Match

Abstract: Deep Learning models in the context of retrofitting are significantly constrained by the impracticality of data collection. Acquiring faulty, labelled and heterogeneous data is difficult and expensive. While the non-availability of faulty and labelled data mandates the usage of unsupervised anomaly detection methods, the lack of heterogeneity in the gathered samples forces these models to be generalizable. On the other hand, if the intended model implementation platform is a micro-controller, these deep data-driven models further exacerbate the issue of model selection. Most of the existing unsupervised anomaly detection techniques neglect the distribution shift in streaming data. Additionally, they fall short...

[162] Adaptive Cluster Tendency Visualization and Anomaly Detection for Streaming Data
Dheeraj Kumar, ..., and J. Gubbi. ACM Transactions on Knowledge Discovery from Data (TKDD), 2016. 31 citations.
Not measured Topic Match

No summary or abstract available

[163] LSTM-AE for Anomaly Detection on Multivariate Telemetry Data
Anes Abdennebi, ..., and Oktay Gungor. 2023 IEEE/ACIS 21st International Conference on Software Engineering Research, Management and Applications (SERA), 2023. 0 citations.
Not measured Topic Match

Abstract: Organizations and companies that collect data generated by sales, transactions, client/server communications, IoT nodes, devices, engines, or any other data generating/exchanging source, need to analyze this data to reveal insights about the running activities on their systems. Since streaming data has multivariate variables bearing dependencies among each other that extend temporally (to previous time steps).Long-Short Term Memory (LSTM) is a variant of the Recurrent Neural Networks capable of learning long-term dependencies using previous timesteps of sequence-shape data. The LSTM model is a valid option to apply to our data for offline anomaly detection and help foresee future system incidents. Anything...

[164] Anomaly and Degradation Detection Using Subspace Tracking in Streaming Data
Kyungduck Cha, ..., and Zohreh Asgharzadeh. 2020 IEEE International Conference on Big Data (Big Data), 2020. 1 citations.
Not measured Topic Match

Abstract: In our increasingly connected digital world, many sensors are connected to each other. Each sensor provides several features and data from those features. As a result, the data sets created from Internet of Things (IoT) applications can consist of hundreds or even thousands of dimensions. Even though the dimensionality is high in these data sets, the actual rank is mostly low because of the high correlations between these dimensions. As a result, subspace analysis and subspace tracking are useful methods of capturing low-dimensional structures from high-frequency, high-dimensional data. In streaming data, a substantial change in the subspace can indicate an...

[165] A systematic review of machine learning and deep learning techniques for anomaly detection in data mining
Mahjabeen Tahir, ..., and Khairul Azhar Kasmiran. International Journal of Computers and Applications, 2025. 4 citations.
Not measured Topic Match

Abstract: The growing use of the internet has increased the threat of cyberattacks. Anomaly detection systems are vital for protecting networks by spotting irregular activities. Various studies investigated anomaly detection techniques without a systematic approach. So far, the existing reviews mainly concerned time series and data streaming methods almost neglected the growing interest in graph-based data mining techniques which are vital in social networks, finance, and IoT domains. Following PRISMA guidelines, this systematic review examines anomaly detection methods applied to time series, data streaming, and graph-based data from 2018 to 2023. A total of 34 papers were selected from four key...

[166] Scalable Anomaly Detection with Machine Learning: Techniques for Managing High-Dimensional Data Streams
Saugat Nayak. Journal of Engineering Research and Reports, 2025. 0 citations.
Not measured Topic Match

Abstract: The increase in big data values from industries, especially in Analytics, Risk, and Management Information systems, offers a great catchment and, at the same time, books with a lot of potential hurdles. This paper provides the conceptual basis for combining unsupervised and deep learning for real-time anomaly detection in high feature-space trajectories and offers practical applications for several industries. Autoencoders, Isolation Forests, and RNNs are tested for their performance and compared with the PCA in finance, manufacturing, healthcare, and cybersecurity applications. Other benefits are measured in specifics, such as cutting fraud detection mistakes by 25% and increasing the effectiveness of...

[167] ADDAI: Anomaly Detection using Distributed AI
Maede Zolanvari, ..., and R. Jain. 2021 IEEE International Conference on Networking, Sensing and Control (ICNSC), 2021. 8 citations.
Not measured Topic Match

Abstract: When dealing with the Internet of Things (IoT), especially industrial IoT (IIoT), two manifest challenges leap to mind. First is the massive amount of data streaming to and from IoT devices, and second is the fast pace at which these systems must operate. Distributed computing in the form of edge/cloud structure is a popular technique to overcome these two challenges. In this paper, we propose ADDAI (Anomaly Detection using Distributed AI) that can easily span out geographically to cover a large number of IoT sources. Due to its distributed nature, it guarantees critical IIoT requirements such as high speed, robustness...

[168] A Hybrid Deep Learning-Based Model for Anomaly Detection in Cloud Datacenter Networks
S. Garg, ..., and R. Ranjan. IEEE Transactions on Network and Service Management, 2019. 202 citations.
Not measured Topic Match

Abstract: With the emergence of the Internet-of-Things (IoT) and seamless Internet connectivity, the need to process streaming data on real-time basis has become essential. However, the existing data stream management systems are not efficient in analyzing the network log big data for real-time anomaly detection. Further, the existing anomaly detection approaches are not proficient because they cannot be applied to networks, are computationally complex, and suffer from high false positives. Thus, in this paper a hybrid data processing model for network anomaly detection is proposed that leverages grey wolf optimization (GWO) and convolutional neural network (CNN). To enhance the capabilities of...

[169] ReRe: A Lightweight Real-Time Ready-to-Go Anomaly Detection Approach for Time Series
Ming-Chang Lee, ..., and Ernst Gunnar Gran. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020. 32 citations.
Not measured Topic Match

Abstract: Anomaly detection is an active research topic in many different fields such as intrusion detection, network monitoring, system health monitoring, IoT healthcare, etc. However, many existing anomaly detection approaches require either human intervention or domain knowledge, and may suffer from high computation complexity, consequently hindering their applicability in real-world scenarios. Therefore, a lightweight and ready-to-go approach that is able to detect anomalies in real-time is highly sought-after. Such an approach could be easily and immediately applied to perform time series anomaly detection on any commodity machine. The approach could provide timely anomaly alerts and by that enable appropriate countermeasures to...

[170] Real-Time Anomaly Detection Using Facebook Prophet
T. Nithish, ..., and S. Totad. Int. J. Nat. Comput. Res., 2021. 3 citations.
Not measured Topic Match

Abstract: With sensors percolating through everyday living, it may be toted that there is an enormous increase in the availability of real-time streaming and time series data. We also see an exponential increase in number of industry applications with sensors driven by IoT and connected with data sources that change over time. This time-series data presents many technical challenges, opportunities, and threats to industries. Thus, streaming analytics to model an unsupervised machine learning system for detecting unusual/anomalous behavior in real-time must be prominently addressed. In this paper, the authors propose a real-time abnormality detection model using a Facebook prophet that addresses...

[171] Privacy-preserving Real-time Anomaly Detection Using Edge Computing
Shagufta Mehnaz and E. Bertino. 2020 IEEE 36th International Conference on Data Engineering (ICDE), 2020. 25 citations.
Not measured Topic Match

Abstract: Anomaly detection on data collected by devices, such as sensors and IoT objects, is inevitable for many critical systems, e.g., an anomaly in the data of a patient's health monitoring device may indicate a medical emergency situation. Because of the resource-constrained nature of these devices, data collected by such devices are usually off-loaded to the cloud/edge for storage and/or further analysis. However, to ensure data privacy it is critical that the data be transferred to and managed by the cloud/edge in an encrypted form which necessitates efficient processing of such encrypted data for real-time anomaly detection. Motivated by the simultaneous...

[172] Track Before Detect: A Novel Approach For Unsupervised Anomaly Detection In Time Series
Ralph Bou Nader, ..., and R. Haque. 2021 IEEE International Conference on Smart Data Services (SMDS), 2021. 0 citations.
Not measured Topic Match

Abstract: The need for robust unsupervised anomaly detection techniques in streaming data increases rapidly in today's era of smart devices. Many existing anomaly detection methods have difficulties to detect anomalies in streaming data since most of them are designed to use all features of the data which are not applicable in a streaming context such as IoT. To address this problem, we present a novel unsupervised anomaly detection approach (Track Before Detect) for time series data. Track Before Detect (TBD) is capable of detecting a wide range of anomalies such as point anomalies and collective anomalies. In addition, it can differentiate...

[173] Perspective on efficiency enhancements in processing streaming data in industrial IoT networks
Julia Rosenberger, ..., and Dieter Schramm. 2021 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), 2021. 2 citations.
Not measured Topic Match

Abstract: Both data compression and anomaly detection are very deeply studied areas for the last decades and gain significance for the Internet of Things (IoT), especially industrial IoT (IIoT). Due to the advantages like fewer latency and security aspects, edge computing is often preferred to cloud solutions. While the amount of data as well as the demand for edge data processing increases, resources like bandwidth, computational performance, memory and, in case of Wireless Sensor Networks (WSN), also energy are still limited. This leads primarily to a trade-off between maximum data reduction, information extraction and minimal computational effort. Often, both data compression...

[174] Visual Structural Assessment and Anomaly Detection for High-Velocity Data Streams
Punit Rathore, ..., and M. Palaniswami. IEEE Transactions on Cybernetics, 2020. 9 citations.
Not measured Topic Match

Abstract: The widespread use of Internet-of-Things (IoT) technologies, smartphones, and social media services generates huge amounts of data streaming at high velocity. Automatic interpretation of these rapidly arriving data streams is required for the timely detection of interesting events that usually emerge in the form of clusters. This article proposes a new relative of the visual assessment of the cluster tendency (VAT) model, which produces a record of structural evolution in the data stream by building a cluster heat map of the entire processing history in the stream. The existing VAT-based algorithms for streaming data, called inc-VAT/inc-iVAT and dec-VAT/dec-iVAT, are not...

[175] Fast Anomaly Detection in Multiple Multi-Dimensional Data Streams
Hongyu Sun, ..., and Feifei Chen. 2019 IEEE International Conference on Big Data (Big Data), 2019. 19 citations.
Not measured Topic Match

Abstract: Multiple multi-dimensional data streams are ubiquitous in the modern world, such as IoT applications, GIS applications and social networks. Detecting anomalies in such data streams in real-time is an important and challenging task. It is able to provide valuable information from data and then assists decision-making. However, exiting approaches for anomaly detection in multi-dimensional data streams have not properly considered the correlations among multiple multi-dimensional streams. Moreover, for multi-dimensional streaming data, online detection speed is often an important concern. In this paper, we propose a fast yet effective anomaly detection approach in multiple multi-dimensional data streams. This is based on...

[176] Distributed contextual anomaly detection from big event streams
Bakhtiar Amen. Unknown journal, 2018. 1 citations.
Not measured Topic Match

No summary or abstract available

[177] Aqua-stream: an IoT based smart water management system for sustainable living
Sri Ramya Siraparapu and S. Azad. Indonesian Journal of Electrical Engineering and Computer Science, 2024. 2 citations.
Not measured Topic Match

Abstract: Aqua-stream, an innovative internet of things (IoT) enabled water management system, utilizes the power of long short-term memory (LSTM) networks, a sophisticated time-series forecasting machine learning technique with Kafka. Aqua-stream seamlessly integrates LSTM within the Kafka streaming architecture for efficient real-time data processing, ensuring quick responses to emerging water management needs. LSTM is employed for real-time anomaly detection, dynamically analyzing streaming data to prevent leaks through automated shut-off valves. The system's comprehensive dashboard utilizes LSTM insights for live water quality analysis; adaptive scheduling based on individual preferences and personalized recommendations, enhancing cost-effective water management. This streamlined approach extends to the...

[178] Multi-scale Anomaly Detection with Wavelets
J. Coughlin and Gianluigi Perrone. Proceedings of the International Conference on Big Data and Internet of Thing, 2017. 2 citations.
Not measured Topic Match

No summary or abstract available

[179] IOT-based Smart Surveillance Robotic Car using HC05
Nutakki Rajeswari, ..., and Kusuma Pavanchand. 2024 International Conference on Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA), 2024. 0 citations.
Not measured Topic Match

No summary or abstract available

[180] A Novel Multi Wavelet Oriented Auto Encoder for Intrusion Detection in IoT System
Kuruba Madhusudhan and Aravind Kumar Madam. Transactions on Emerging Telecommunications Technologies, 2025. 0 citations.
Not measured Topic Match

Abstract: IoT devices become more integrated into daily life, they are increasingly vulnerable to cyberattacks, compromising user confidentiality. Although existing intrusion detection techniques for IoT systems have been developed, they often fail to accurately classify attacks. This paper presents a novel approach for detecting intrusions in IoT devices by combining advanced feature extraction and deep learning techniques. The proposed method first pre processes dataset images to enhance data quality by filtering out irrelevant information. A unique Aquila Optimized Convolutional Neural Network (AO CNN) is then applied to extract optimal features. The proposed AO CNN incorporates an optimization technique called Aquila Optimizer that fine tunes the...

[182] Strategic Network Attack Prevention System Leveraging Sophisticated Query-Based Network Attention Algorithm (QNAA) and Self-Perpetuating Generative Adversarial Network (SPF-GAN) Techniques for Optimal Detection
Tahani Albalawi, ..., and F. Albalwy. Electronics, 2025. 0 citations.
Not measured Topic Match

Abstract: Network attack detection is a critical issue in complex networks at present, one which becomes even more challenging as the network complexity grows and new threats emerge. Existing security models may encounter problems such as low accuracy, a high number of false positives, and the inability to learn new attacks, especially jamming attacks, where the attacker floods a communication channel with noise. Hence, an adaptive and resilient approach is required. This study presents two novel approaches—the Query-Based Network Attention Algorithm (QNAA) and the Self-Perpetuating Generative Adversarial Network (SPF-GAN) —to enhance performance and flexibility. The QNAA integrates attention mechanisms that allow...

[184] CDDA-MD: An efficient malicious traffic detection method based on concept drift detection and adaptation technique
Saihua Cai, ..., and Wuhao Guo. Comput. Secur., 2025. 3 citations.
Not measured Topic Match

No summary or abstract available

[185] Deep learning-driven methods for network-based intrusion detection systems: A systematic review
Ramya Chinnasamy, ..., and Jaehyuk Cho. ICT Express, 2025. 4 citations.
Not measured Topic Match

No summary or abstract available

[186] Boosting incremental intrusion detection system with adversarial samples
Xiaodong Wu, ..., and Kai Liu. Expert Syst. Appl., 2025. 0 citations.
Not measured Topic Match

No summary or abstract available

[188] ASAP: Automatic Synthesis of Attack Prototypes, an online-learning, end-to-end approach
Jesús Fernando Cevallos Moreno, ..., and A. Coen-Porisini. Comput. Networks, 2024. 1 citations.
Not measured Topic Match

No summary or abstract available

[189] Intrusion detection based on concept drift detection and online incremental learning
Farah Jemili, ..., and O. Korbaa. Int. J. Pervasive Comput. Commun., 2024. 2 citations.
Not measured Topic Match

Abstract: Purpose The primary purpose of this paper is to introduce the drift detection method-online random forest (DDM-ORF) model for intrusion detection, combining DDM for detecting concept drift and ORF for incremental learning. The paper addresses the challenges of dynamic and nonstationary data, offering a solution that continuously adapts to changes in the data distribution. The goal is to provide effective intrusion detection in real-world scenarios, demonstrated through comprehensive experiments and evaluations using Apache Spark. Design/methodology/approach The paper uses an experimental approach to evaluate the DDM-ORF model. The design involves assessing classification performance metrics, including accuracy, precision, recall and F-measure. The...

[198] AOC-IDS: Autonomous Online Framework with Contrastive Learning for Intrusion Detection
Xinchen Zhang, ..., and Shuang-Hua Yang. IEEE INFOCOM 2024 - IEEE Conference on Computer Communications, 2024. 3 citations.
Not measured Topic Match

Abstract: The rapid expansion of the Internet of Things (IoT) has raised increasing concern about targeted cyber attacks. Previous research primarily focused on static Intrusion Detection Systems (IDSs), which employ offline training to safeguard IoT systems. However, such static IDSs struggle with real-world scenarios where IoT system behaviors and attack strategies can undergo rapid evolution, necessitating dynamic and adaptable IDSs. In response to this challenge, we propose AOC-IDS, a novel online IDS that features an autonomous anomaly detection module (ADM) and a labor-free online framework for continual adaptation. In order to enhance data comprehension, the ADM employs an Autoencoder (AE) with...