Supplementary Information

Deployable AI for IoT/IIoT Security: A Systematic Review of Labeling, Transfer, Resource, and Explainability Constraints

Anass Rharif[1,*], Ziad Charafi[1], Mounia Zaydi[2], Sofia Belkhala[1], and Yassine Maleh[1]

[1]Laboratory LaSTI, ENSAK, Sultan Moulay Slimane University, Khouribga, 54000, Morocco
[2]ICL, Junia, Université Catholique de Lille, LITL, Lille, 59000, France
[*]anass.rharif@usms.ac.ma

Supplementary Information overview

This Supplementary Information file provides the methodological audit trail, search documentation, screening evidence, extraction codebook, quality-assessment framework, extended descriptive results, reproducibility index, supporting figures, and complete corpus reference list for the systematic literature review. It is organized to help reviewers trace how records were identified, screened, appraised, coded, and synthesized into deployment-oriented conclusions.

Supplementary item map

Reviewer note. This map gives reviewers a quick orientation before reading the detailed Supplementary Information. It identifies what each item contributes and whether the item primarily supports reproducibility, corpus definition, descriptive synthesis, or deployment-oriented interpretation.

Supplementary item map.

Item	Description
Supplementary Note 1	Review protocol: documents the pre-screening objective, scope, databases, screening process, quality rubric, and extraction strategy.
Supplementary Table S1A–S1B	Critical comparison of prior surveys: separates scope/method coverage from strengths, limitations, and the added value of this SLR.
Supplementary Table S2A–S2B	Search log: summarizes retrieval counts and preserves the Boolean logic used across the six databases.
Supplementary Table S3A–S3B	Citation chaining and manual checks: explains the additional retrieval route used to reduce indexing and terminology bias.
Supplementary Table S4	Inclusion and exclusion criteria: defines the eligibility boundary of the final corpus.
Supplementary Tables S5–S6	PRISMA screening evidence: reports the numerical screening trail and full-text exclusion reasons.
Supplementary Tables S7–S10	Quality assessment and extraction infrastructure: provides the appraisal rubric, quality-score structure, extraction codebook, and included-study registry fields.
Supplementary Tables S11–S14	Evidence distribution: reports AI-family distribution, security-task distribution, matrix reproducibility logic, and the highest-density AI/task intersections.
Supplementary Tables S15–S16	Dataset comparability: explains benchmark properties and cross-dataset comparison risks affecting performance interpretation.
Supplementary Tables S17–S19	Study-level coding schemas: documents evaluation-protocol, operational-metric, and secondary-tag variables to be completed in the machine-readable workbook.
Supplementary Table S20	Reproducibility package index: maps each supplementary component to the PDF or spreadsheet location.
Supplementary Figs. S1–S2	Supporting visual syntheses: show the SLR structure and AI-family profiles under deployment constraints.
Supplementary Reference List	References cited in the Supplementary Information, including methodological references, representative prior surveys, and reviewed studies; the machine-readable included-study registry is provided in Supplementary Data S1.

Supplementary Note 1. Review protocol

Reviewer note. This note records the protocol components that governed the review before screening. It allows reviewers to verify that the search window, corpus boundary, screening logic, extraction variables, quality assessment approach, and synthesis strategy were defined consistently and applied transparently.

The review protocol was defined before screening. It specified the review objective, time window, study type, databases, screening process, quality assessment rubric, extraction schema, and synthesis strategy. The protocol was used to preserve transparency, reduce selection bias, and support traceability from search to final synthesis.

Protocol summary supporting Supplementary Note 1.

Element	Protocol item
Review objective	Deployment-oriented systematic literature review of AI for IoT/IIoT security
Review period	January 2021 to November 2025
Study type	Peer-reviewed Q1/Q2 journal articles
Databases	IEEE Xplore; ACM Digital Library; Scopus; Web of Science; ScienceDirect; SpringerLink
Screening process	Title/abstract screening; full-text screening; consensus process
Quality assessment	Eight-criterion rubric scored from 0 to 2 per criterion
Extraction strategy	AI family; security task; dataset; evaluation protocol; metrics; deployment constraints

Supplementary Table S1. Critical comparison of representative prior surveys

Reviewer note. This item positions the present review against representative prior surveys. To improve readability and avoid compressed landscape pages, the comparison is split into two aligned tables: S1A summarizes method and scope coverage, while S1B records strengths, limitations, and the specific positioning value of each survey.

The comparison documents how representative prior surveys differ from the present deployment-oriented SLR. The purpose is not to devalue earlier surveys, but to show why a cross-task, evidence-quality, and deployability-centered synthesis is needed.

Supplementary Table S1A. Scope and methodological coverage of representative prior surveys.

Ref.	Method style	Back-ground	Application domain	Tech-niques	Chal-lenges	Future direction
(2)	Comprehensive survey and taxonomy	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
(24)	XAI-focused survey	*Yes*	*Partial*	*Yes*	*Yes*	*Yes*
(16)	Taxonomy and structured survey	*Yes*	*Partial*	*Yes*	*Yes*	*Yes*
(27)	Broad SLR with mixed scope	*Yes*	*Yes*	*Partial*	*Yes*	*Yes*
(13)	Task-centric survey	*Yes*	*Partial*	*Yes*	*Yes*	*Yes*
(15)	Comparative survey on FL IDS	*Yes*	*Partial*	*Partial*	*Yes*	*Yes*
(20)	Domain-centric review	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
(28)	Domain/task SLR	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
(23)	Task-centric review with performance analysis	*Partial*	*Partial*	*Yes*	*Yes*	*Yes*
(26)	Updated anomaly review	*Yes*	*Partial*	*Yes*	*Yes*	*Yes*
(31)	IDS review	*Yes*	*Partial*	*Yes*	*Yes*	*Yes*
(25)	Task-centric review	*Partial*	*Partial*	*Yes*	*Yes*	*Yes*
(32)	Systematic mapping study	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
(22)	Architecture-centric review	*Yes*	*Yes*	*Partial*	*Yes*	*Yes*
This SLR	PRISMA-guided SLR and cross-RQ synthesis	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*

Supplementary Table S1B. Critical synthesis of representative prior surveys.

Ref.	Strengths	Limitations	Relevance to the present SLR
(2)	Strong coverage of 6G/edge threats, datasets, and defenses; useful dataset orientation	6G/edge framing can underrepresent non-6G brownfield IoT; limited cross-task synthesis beyond IDS/anomaly	Useful for edge/6G security; not a unified AI-for-IoT-security SLR
(24)	Clear XAI taxonomy; covers trust and analyst usability	Primarily IDS/XAI; limited malware, authentication, privacy analytics, and response coverage	Deep on XAI for IoT IDS; not broad AI security coverage
(16)	Strong placement taxonomy across edge/fog/cloud and IDS categories	IDS-dominant; limited system integration, governance, and cross-task comparison	Good IDS map; weak end-to-end IoT security architecture view
(27)	Broad threat and application context; useful landscape view	AI depth is uneven; evaluation practices and deployability are not deeply assessed	Good macro view; limited AI technique and evidence-rigor depth
(13)	Solid overview of ML/DL anomaly detectors; notes drift and resource issues	Mostly anomaly detection; limited cross-domain evidence and standardized evaluation critique	Useful anomaly survey; not a full IoT security SLR

Continued on next page

Ref.	Strengths	Limitations	Relevance to the present SLR
(15)	Strong on FL threat model, communication overhead, and poisoning risks	Narrow to FL IDS; limited coverage of authentication, malware, and broader privacy analytics	Strong FL IDS slice; not a unified AI security landscape
(20)	Good healthcare threat context and risk mitigation lens	Domain specificity reduces generalizability; limited cross-domain technique comparison	Strong for IoMT; less applicable to general IoT/IIoT breadth
(28)	Concrete smart-home context and behavior-modeling focus	Smart-home scope; limited to anomaly detection approaches	Deep for smart homes; not cross-sector IoT/IIoT synthesis
(23)	Good comparison of unsupervised methods for multivariate sensor anomaly detection	Time-series anomaly niche; limited security tasks beyond anomaly detection	Valuable niche review; not comprehensive IoT security
(26)	Modern trends such as zero-day detection, drift, and scalable learning	Still anomaly-centric; limited authentication, trust, malware, privacy, and response coverage	Strong anomaly update; limited breadth across tasks
(31)	Broad IDS algorithm coverage and practical pros/cons	Evaluation rigor, deployment, and governance treatment often shallow; IDS only	Good IDS reference; limited system-level guidance
(25)	Covers modern models such as GNN, GAN, and ensembles	Limited cross-task and cross-domain synthesis	Good network anomaly snapshot; not comprehensive IoT security
(32)	Structured mapping across domains and highlights underexplored sectors	Mapping depth can be shallow per technique; focus remains anomaly detection	Strong map; limited deep evidence synthesis
(22)	Useful architecture view for dense IoT	6G framing; less empirical comparison and broader IoT/IIoT representativeness	Good architecture overview; limited evidence consolidation
This SLR	Unified evidence across AI families and IoT/IIoT security tasks; explicit evaluation critique and deployment constraints; includes XAI as adoption enabler	Depends on available published evidence; limited access to proprietary industrial datasets; reporting heterogeneity constrains meta-analysis	Positions AI for IoT/IIoT security as a deployable capability requiring governance, robustness, efficiency, and auditability

Supplementary Table S2. Database-specific Boolean search strings and retrieval results

Reviewer note. This item provides the exact search log needed to reproduce database retrieval. To preserve readability, retrieval metadata are separated from the Boolean syntax. The Boolean expression is intentionally reported in full because small syntax changes can materially affect retrieval.

The search strategy combined three groups of terms: IoT/IIoT context terms, security objective terms, and AI technique terms. Database-specific syntax was adapted to each source while preserving the same conceptual search logic.

Supplementary Table S2A. Database retrieval metadata and record counts.

Database	Fields searched	Filters	Search date	Records
IEEE Xplore	Metadata, abstract, index terms	Journal, English, 2021–2025	15/11/2025	210
ACM Digital Library	Title, abstract, keywords	Journal, English, 2021–2025	15/11/2025	135
Scopus	Title, abstract, keywords	Article, English, 2021–2025	16/11/2025	315
Web of Science	Topic	Article, English, 2021–2025	16/11/2025	260
ScienceDirect	Title, abstract, keywords	Research article, English, 2021–2025	17/11/2025	190
SpringerLink	Title, abstract, keywords	Article, English, 2021–2025	17/11/2025	140
Total	–	–	–	**1,250**

Supplementary Table S2B. Database-specific Boolean search strings.

Database	Search string / syntax adaptation
IEEE Xplore	(("Internet of Things" OR IoT OR "Industrial Internet of Things" OR IIoT) AND (security OR cybersecurity OR "intrusion detection" OR "anomaly detection" OR malware OR botnet OR DDoS OR authentication OR privacy OR "attack detection") AND ("artificial intelligence" OR "machine learning" OR "deep learning" OR "federated learning" OR "reinforcement learning" OR "adversarial learning" OR "self-supervised learning" OR "explainable AI"))
ACM Digital Library	Same conceptual Boolean expression as IEEE Xplore; adapted to title, abstract, and keyword fields.
Scopus	TITLE-ABS-KEY(("Internet of Things" OR IoT OR "Industrial Internet of Things" OR IIoT) AND (security OR cybersecurity OR "intrusion detection" OR "anomaly detection" OR malware OR botnet OR DDoS OR authentication OR privacy OR "attack detection") AND ("artificial intelligence" OR "machine learning" OR "deep learning" OR "federated learning" OR "reinforcement learning" OR "adversarial learning" OR "self-supervised learning" OR "explainable AI"))
Web of Science	TS=(("Internet of Things" OR IoT OR "Industrial Internet of Things" OR IIoT) AND (security OR cybersecurity OR "intrusion detection" OR "anomaly detection" OR malware OR botnet OR DDoS OR authentication OR privacy OR "attack detection") AND ("artificial intelligence" OR "machine learning" OR "deep learning" OR "federated learning" OR "reinforcement learning" OR "adversarial learning" OR "self-supervised learning" OR "explainable AI"))
ScienceDirect	Same conceptual Boolean expression as IEEE Xplore; adapted to title, abstract, and keyword search fields with research-article and date filters.
SpringerLink	Same conceptual Boolean expression as IEEE Xplore; adapted to title, abstract, and keyword search fields with article, English-language, and date filters.

Supplementary Table S3. Citation chaining and manual journal checks

Reviewer note. This item documents supplementary retrieval beyond database searching. It shows how citation chaining and manual journal checks reduced the risk of missing relevant studies because of terminology variation, indexing gaps, or fragmented publication practices.

Citation chaining and manual checks were added to reduce the risk of missing relevant studies due to indexing limitations, terminology variation, or fragmented publication practices.

Supplementary Table S3A. Citation chaining and manual journal checks.

Source type	Number of records	Method	Notes
Backward citation chaining	76	References of included or relevant papers	Same eligibility criteria applied
Forward citation chaining	84	Citation tracking	Same eligibility criteria applied
Manual journal checks	40	Relevant journals in IoT, cybersecurity, AI, and network security	Same eligibility criteria applied
Total	**200**	Additional records	Added before deduplication

Supplementary Table S3B. Journal/platform-level manual checks.

Journal/platform checked	Date checked	Search/browse method	Records retrieved	Records retained
IEEE Internet of Things Journal	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
IEEE Transactions on Dependable and Secure Computing	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
IEEE Transactions on Information Forensics and Security	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
Computer Networks	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
Future Generation Computer Systems	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
Journal of Network and Computer Applications	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
Internet of Things	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total
Cluster Computing / Soft Computing / Applied Soft Computing	November 2025	Manual issue/search browse using review terms	Not separately frequency-coded in the supplied evidence	Included in manual-journal-check total

Supplementary Table S4. Inclusion and exclusion criteria

Reviewer note. This table defines the eligibility boundary of the corpus. It supports auditability by showing the inclusion rule, corresponding exclusion condition, and rationale used during screening.

Supplementary Table S4. Inclusion and exclusion criteria.

ID	Inclusion criterion	Exclusion criterion	Rationale
IC1	Peer-reviewed Q1/Q2 journal article	Conference paper, workshop paper, editorial, book chapter, thesis, white paper, or non-peer-reviewed preprint	Corpus-boundary criterion

Continued on next page

ID	Inclusion criterion	Exclusion criterion	Rationale
IC2	Published between January 2021 and November 2025	Published outside the selected period	Scope consistency
IC3	Explicit IoT or IIoT security context	Generic network security without clear IoT/IIoT specificity	Domain relevance
IC4	Uses AI, ML, DL, FL, RL, adversarial learning, XAI, self-supervised learning, graph learning, or hybrid AI	Non-AI or purely rule-based security method	Technical relevance
IC5	Addresses a security objective such as IDS, anomaly detection, malware or botnet detection, DDoS detection, authentication, privacy-preserving analytics, or adaptive response	AI for non-security IoT analytics such as energy optimization, traffic prediction, or predictive maintenance only	Alignment with review questions
IC6	Provides empirical evaluation using datasets, testbeds, simulations, trace replay, or real deployment evidence	Conceptual, theoretical, or architecture-only article without evaluation	Evidence synthesis
IC7	Reports sufficient methodological detail, including dataset, model, metrics, and evaluation protocol	Insufficient methodological detail for extraction or appraisal	Reproducibility

Supplementary Table S5. PRISMA screening summary

Reviewer note. This table gives the numerical screening audit trail that complements the PRISMA flow figure in the main manuscript. It allows reviewers to verify the transition from records identified to the final included corpus.

Supplementary Table S5. PRISMA screening summary.

Stage	Number	Description
Records identified from databases	1,250	Six databases: IEEE Xplore, ACM Digital Library, Scopus, Web of Science, ScienceDirect, and SpringerLink
Additional records	200	Citation chaining and manual checks
Total records identified	1,450	Before deduplication
Duplicates removed	300	DOI, title, author, and year matching
Records screened	1,150	Title and abstract screening
Records excluded	850	Outside scope or basic criteria not met
Full-text reports assessed	300	Eligibility assessment
Full-text reports excluded	146	Excluded after full-text review
Studies included	**154**	Final corpus

Supplementary Table S6. Full-text exclusion reasons

Reviewer note. This table disaggregates the 146 full-text exclusions. It strengthens the transparency of the eligibility stage by showing why articles assessed in full text were not retained.

Supplementary Table S6. Full-text exclusion reasons.

Exclusion reason	Number	Explanation
No explicit IoT/IIoT context	32	Generic network security
No AI or ML method	21	Non-AI method
No security objective	18	Non-security IoT analytics

Exclusion reason	Number	Explanation
No empirical evaluation	24	Conceptual/theoretical only
Insufficient methodological detail	19	Dataset/model/metrics/protocol missing
Conference-only or non-journal article	14	Publication type excluded
Duplicate or overlapping version	11	Journal version retained
Non-English publication	7	Language criterion
Total	**146**	Full-text exclusions

Supplementary Table S7. Quality assessment rubric

Reviewer note. This item explains how study quality was appraised and how the score distribution was used for evidence weighting. The rubric emphasizes methodological transparency, evaluation rigor, and deployment relevance rather than performance claims alone.

Quality assessment was based on eight criteria scored from 0 to 2. The maximum score was 16. Quality bands were used for evidence weighting.

Supplementary Table S7A. Quality assessment rubric.

Criterion	Score 0	Score 1	Score 2
Problem definition	Unclear or generic	Partially clear	Clear and security-specific
Dataset transparency	Missing or unclear	Partial dataset information	Complete dataset and preprocessing details
Evaluation protocol	Weak, unclear, or leakage-prone	Standard random split or cross-validation	Time-aware, scenario-aware, device-aware, or cross-domain validation
Baselines	Absent or weak	Limited baselines	Strong and task-relevant baselines
Metric reporting	Single metric only	Multiple standard metrics	Includes operational metrics such as FPR, latency, memory, energy, throughput, drift, or calibration
Reproducibility	Low	Partial	High methodological transparency
Limitations	Absent	Generic limitations	Explicit and evidence-based limitations
Deployability evidence	Absent	Discussed only	Measured or experimentally evaluated

Supplementary Table S7B. Quality assessment score distribution across the 154 studies.

Quality band	Score range	Number of studies	Interpretation
High	12–16	62	Higher interpretive weight in synthesis
Medium	8–11	73	Moderate interpretive weight; conclusions interpreted with caution
Low	0–7	19	Low interpretive weight for strong claims
Total	–	**154**	Full included corpus

Supplementary Table S9. Data extraction schema

Reviewer note. This codebook defines the extraction variables used to connect individual studies to the review questions. It also supports reproducibility by documenting how bibliographic, technical, dataset, evaluation, and deployment-constraint variables were captured.

Supplementary Table S9. Data extraction schema.

Category	Extracted variables	Purpose
Bibliographic data	Authors, year, journal, publisher, ranking, article type	Corpus description
Security task	IDS, anomaly detection, DDoS detection, malware/botnet detection, authentication, privacy-preserving analytics, adaptive response, other	RQ1/RQ2
AI family	Classical ML, DL, FL, RL, XAI, graph learning, generative models, quantum ML, hybrid and related approaches	Technical synthesis
Dataset	Dataset name, IoT-native status, data type, attack types, device type, traffic format	Dataset analysis
Evaluation protocol	Random split, cross-validation, predefined split, time-aware split, scenario-disjoint split, device-disjoint split, cross-dataset validation, real deployment or pilot	RQ3
Metrics	Accuracy, precision, recall, F1, FPR, AUC, latency, memory, energy, throughput, communication overhead, drift, explainability usefulness	Operational evidence
Deployment constraints	Labeling burden, transfer/domain shift, resource and real-time feasibility, explainability/auditability	RQ4
Quality assessment	Criterion scores, total score, quality band	Evidence weighting
Limitations	Reported limitations and inferred methodological or deployment risks	Critical synthesis

Supplementary Table S11. Distribution of studies by primary AI family

Reviewer note. This table summarizes the primary AI family assigned to each included study. It supports the main Results by showing where evidence is concentrated and where AI-family evidence remains relatively limited.

Supplementary Table S11. Distribution of studies by primary AI family.

AI family	Number of studies	Percentage	Interpretation
Classical machine learning	61	39.6%	Largest group; mainly detection and classification, often feature-based and lightweight
Deep learning	22	14.3%	Strong in IDS and anomaly detection; often label- and compute-intensive
Federated, split, or swarm learning	24	15.6%	Distributed and privacy-preserving security analytics
Reinforcement learning	3	1.9%	Limited evidence; mainly adaptive decision-making
Graph or knowledge-graph models	7	4.5%	Emerging for relational and coordinated threat analysis
Generative models	4	2.6%	Limited evidence for augmentation, rare attacks, and robustness
Quantum machine learning	4	2.6%	Exploratory; limited operational validation
Explainable AI	6	3.9%	Trust and interpretability; often not operationally validated
Optimization, metaheuristics, fuzzy, rule-based, or immune approaches	12	7.8%	Feature selection and lightweight optimization
Privacy, blockchain, or differential privacy	6	3.9%	Privacy and trust mechanisms

Continued on next page

AI family	Number of studies	Percentage	Interpretation
Edge, TinyML, programmable switches, or knowledge distillation	5	3.2%	Constrained or edge-oriented deployment settings
Total	**154**	**100.0%**	Full corpus

Supplementary Table S12. Distribution of studies by primary IoT/IIoT security task

Reviewer note. This table summarizes the primary security task assigned to each included study. It helps reviewers see the evidence balance across IDS, anomaly detection, encrypted traffic analysis, CPS/ICS protection, robustness, and other task areas.

Supplementary Table S12. Distribution of studies by primary IoT/IIoT security task.

Security task	Number of studies	Percentage	Interpretation
Intrusion detection / IDS / NIDS	48	31.2%	Largest task area
Anomaly detection	28	18.2%	Second largest area; unknown behavior or attacks
DoS / DDoS detection	7	4.5%	Moderate benchmark-driven area
Malware / botnet detection	6	3.9%	Focused but limited
Authentication / device identification	2	1.3%	Underexplored despite operational importance
Insider threat detection	2	1.3%	Very limited evidence
Encrypted traffic classification / threat detection	11	7.1%	Moderate evidence area
CPS / ICS / SCADA protection	10	6.5%	Important industrial and cyber-physical settings
Threat hunting / response	4	2.6%	Emerging but limited
Root-cause / localization	3	1.9%	Underexplored
Adversarial robustness / backdoor defense	7	4.5%	Moderate but important for trustworthy AI
General security / other / unspecified	26	16.9%	Broad multi-task security analytics
Total	**154**	**100.0%**	Full corpus

Supplementary Table S13. AI-family-by-security-task matrix

Reviewer note. This item specifies how the full AI-family-by-security-task matrix should be reproduced from the study-level extraction sheet. It prevents overinterpretation by requiring row totals to match Supplementary Table S11 and column totals to match Supplementary Table S12.

The full AI-family-by-security-task matrix should be generated from the study-level extraction sheet using the mutually exclusive primary AI family and primary security task fields. Row totals must match Supplementary Table S11, column totals must match Supplementary Table S12, and selected high-density cells must match Supplementary Table S14.

Supplementary Table S13. AI-family-by-security-task matrix submission status and reproducibility logic.

Item	Description
AI family / task matrix	Status in this submission package
Full matrix values	To be generated directly from the coded extraction sheet using primary AI family and primary security task fields

Item	Description
Available in PDF	Row totals in Supplementary Table S11, column totals in Supplementary Table S12, and highest-density cells in Supplementary Table S14
Reviewer traceability	The accompanying Supplementary Data workbook contains the matrix-ready schema and columns required to reproduce the matrix from study-level coding
Integrity control	No unverified cell-level counts are reported where study-level matrix coding is not present in the supplied evidence

Supplementary Table S14. Selected highest-density AI-family-by-security-task combinations

Reviewer note. This table gives the most visible intersections between AI-family coding and security-task coding. It supports the heatmap interpretation in the main manuscript while keeping the complete reproducibility logic in Supplementary Table S13.

Supplementary Table S14. Selected highest-density AI-family-by-security-task combinations.

AI family	Security task	Number of studies	Percentage
Classical machine learning	Intrusion detection / IDS / NIDS	17	11.0%
Classical machine learning	Anomaly detection	12	7.8%
Deep learning	Intrusion detection / IDS / NIDS	12	7.8%
Classical machine learning	Encrypted traffic classification / threat detection	7	4.5%
Classical machine learning	CPS / ICS / SCADA protection	7	4.5%
Classical machine learning	General security / other / unspecified	7	4.5%
Optimization/metaheuristics/fuzzy/rule-based/immune approaches	Intrusion detection / IDS / NIDS	7	4.5%
Federated, split, or swarm learning	Anomaly detection	6	3.9%

Supplementary Table S15. Dataset overview and comparability-relevant properties

Reviewer note. This table summarizes benchmark datasets frequently used in IoT/IDS evidence and highlights why performance values across papers are not directly comparable without considering domain, data type, realism, scale, attack coverage, and preprocessing choices.

Supplementary Table S15. Dataset overview and comparability-relevant properties.

Dataset	Domain	Data type	Realism	Size	Attack coverage
IoT-23	IoT malware/botnet traffic	Network flows / packet-derived features	IoT-specific malicious and benign scenarios	Medium	IoT malware, botnet, C&C, benign traffic
CIC-IDS2017	General IDS enterprise network	Network flows	Controlled but broad IDS benchmark	Large	Brute force, DoS/DDoS, web attacks, botnet, infiltration
CSE-CIC-IDS2018	General IDS cloud/enterprise network	Network flows	Larger controlled IDS benchmark	Very large	Brute force, DoS/DDoS, botnet, infiltration, web attacks
NSL-KDD	Legacy network intrusion benchmark	Connection records	Legacy benchmark; lower realism for modern IoT	Small / medium	DoS, Probe, R2L, U2R

Supplementary Table S16. Cross-dataset comparison dimensions for representative IoT/IDS benchmarks

Reviewer note. This table compares datasets on the dimensions that most strongly affect cross-paper comparability: realism, label granularity, reproducibility artifacts, best-suited task, and comparability risk.

Supplementary Table S16. Cross-dataset comparison dimensions for representative IoT/IDS benchmarks.

Dimension	IoT-23	CIC-IDS2017	CSE-CIC-IDS2018	NSL-KDD
Primary realism	IoT-oriented malware and botnet scenarios	Controlled enterprise IDS traffic	Large controlled enterprise/cloud IDS traffic	Legacy network intrusion setting
Label granularity	Benign/malicious and attack labels depending on processed version	Flow-level labels	Flow-level labels	Attack class labels
Reproducibility artifacts	Public dataset and derived flow versions	Public dataset with documented scenarios	Public dataset with documented attack days	Public processed dataset
Best suited task	IoT malware/botnet and IoT anomaly detection	IDS/NIDS benchmarking	IDS/NIDS benchmarking at larger scale	Baseline method comparison only
Main comparability risk	Scenario and preprocessing differences	Synthetic/controlled traffic may not match deployment	Scale and preprocessing choices affect comparability	Outdated traffic and attacks; weak IoT representativeness

Supplementary Table S17. Evaluation protocol coding

Reviewer note. This item defines the evaluation-protocol variables used to judge methodological realism. It distinguishes conventional random or cross-validation designs from stronger time-aware, scenario-disjoint, device-disjoint, cross-dataset, or real-deployment validation designs.

The fields below should be populated at study level in the accompanying Supplementary Data workbook when full coding is available. They are not interpreted as a corpus-level frequency distribution unless every included study has been coded consistently.

Supplementary Table S17. Evaluation protocol coding fields.

Field	Reviewer-facing purpose
Study ID	Links each protocol entry to the included-study registry.
Evaluation protocol	Captures the stated validation design used by the article.
Random split; cross-validation; predefined split	Records conventional evaluation designs that may be useful but can overestimate deployability if leakage or distribution overlap is present.
Time-aware split; scenario-disjoint; device-disjoint	Captures stronger evidence of temporal, scenario, and device generalization.
Cross-dataset validation	Records whether transfer/generalization was tested across independent datasets.
Real deployment/pilot	Identifies the strongest form of operational evidence.
Notes	Preserves methodological caveats that are not captured by binary fields.

Supplementary Table S18. Operational metric coding

Reviewer note. This item defines the operational metrics used to assess whether reported models are plausible for deployment, not only accurate in offline benchmarks. It separates conventional classification metrics from latency, memory, energy, throughput, communication overhead, drift, and explainability-usefulness indicators.

Supplementary Table S18. Operational metric coding fields.

Metric group	Fields and interpretation
Classification performance	Accuracy; precision; recall; F1; AUC; FPR. These metrics describe detection quality but do not alone establish deployability.
Resource and timing evidence	Latency; memory; energy; throughput. These fields document whether the approach can run within IoT/IIoT operational constraints.
Distributed-learning evidence	Communication overhead and coordination cost, especially for federated, split, swarm, or edge-learning approaches.
Robustness and drift	Drift, transfer degradation, adversarial robustness, or backdoor resistance where reported.
Explainability usefulness	Whether explanations were evaluated for analyst utility, decision support, auditability, or trust, rather than only generated visually.
Notes	Free-text field for metric definitions, dataset-specific caveats, or missing operational reporting.

Supplementary Table S19. Secondary AI-family and security-task tags

Reviewer note. This item documents how hybrid and multi-task papers should be handled without distorting the primary frequency counts. The main synthesis uses one primary AI family and one primary security task per study, while secondary tags preserve additional technical or task information.

Supplementary Table S19. Secondary AI-family and security-task tag fields.

Field	Purpose
Study ID	Links each secondary-tag entry to the included-study registry.
Primary AI family	Mutually exclusive field used for primary distribution counts.
Secondary AI family tags	Preserves hybrid techniques such as FL+XAI, DL+GAN, graph+DL, blockchain+FL, or optimization+ML.
Primary security task	Mutually exclusive field used for task distribution counts.
Secondary security task tags	Preserves multi-task coverage such as IDS plus DDoS detection, anomaly detection plus root-cause analysis, or malware plus robustness.
Notes	Explains ambiguous coding decisions or strong secondary claims.

Supplementary Table S20. Reproducibility package index

Reviewer note. This index tells reviewers where each supplementary item is located and which files support reproducibility. It separates readable PDF content from machine-readable spreadsheet material that is better handled as Supplementary Data.

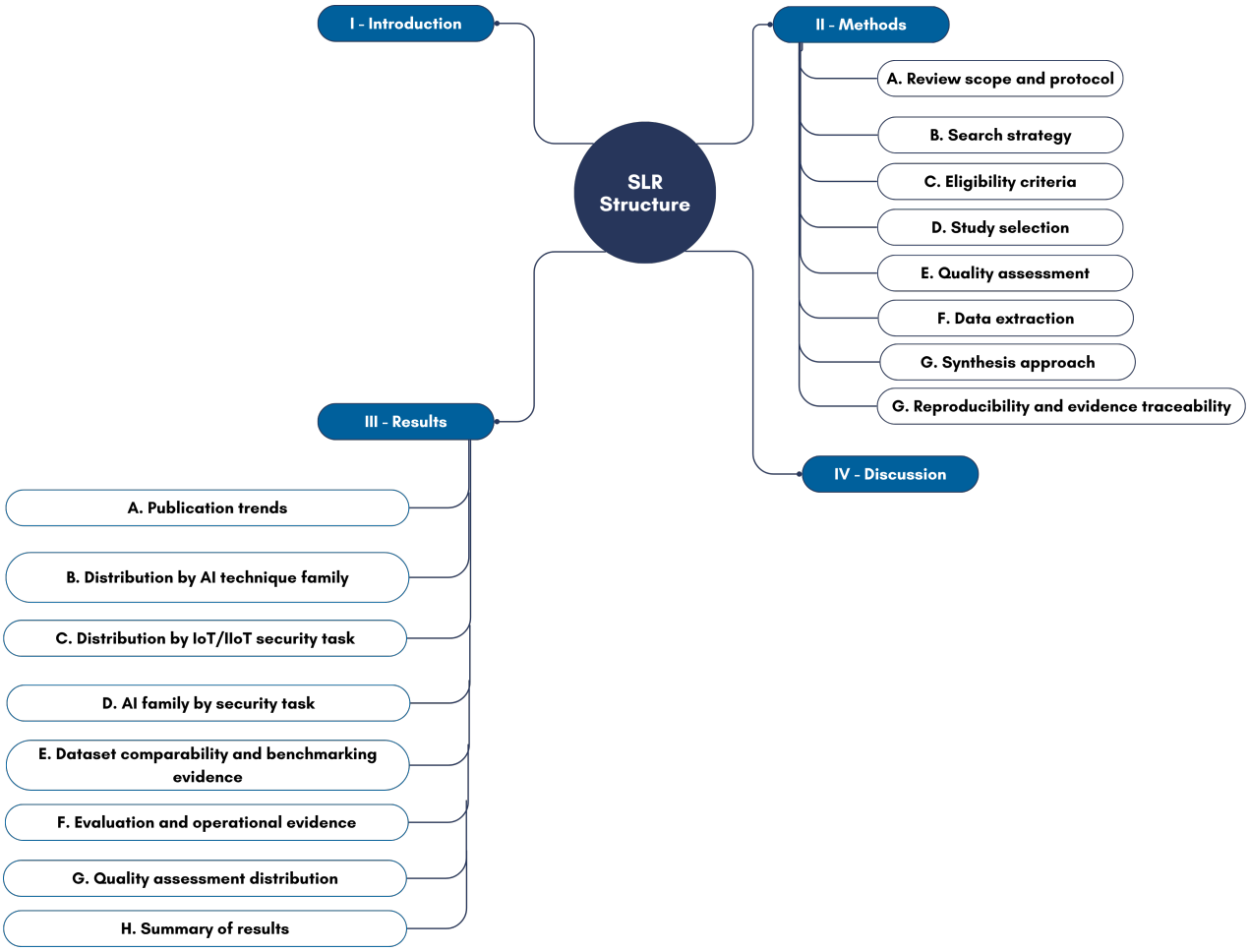
Supplementary Table S20. Reproducibility package index.

File / table	Description	Format
Supplementary Information PDF	Narrative supplementary file containing the protocol, item map, search log, screening evidence, quality rubric, extraction schema, extended distributions, dataset comparability tables, supporting figures, and supplementary references.	PDF
Supplementary Tables S1–S7	Prior-survey positioning, search and screening documentation, inclusion/exclusion criteria, full-text exclusion reasons, and quality-assessment rubric.	PDF tables

File / table	Description	Format
Supplementary Tables S8–S10	Study-level quality-score structure, extraction codebook, and included-study registry fields. The complete row-level data should be supplied in Supplementary Data S1.	PDF summary + XLSX
Supplementary Tables S11–S16	AI-family distribution, security-task distribution, AI-family/security-task reproducibility logic, highest-density intersections, and dataset comparability evidence.	PDF tables
Supplementary Tables S17–S19	Study-level coding fields for evaluation protocol, operational metrics, and secondary AI-family/security-task tags.	PDF summary + XLSX
Supplementary Data S1	Machine-readable workbook containing search log, screening decisions, full-text exclusions, included-study registry, quality scores, extraction sheet, AI-family/task matrix, evaluation-protocol coding, and operational-metric coding.	XLSX
Supplementary Figs. S1–S2	Supporting visual syntheses covering the SLR structure and AI-family profiles under deployment constraints.	PDF figures + PNG files
Supplementary Reference List	References supporting the review and corpus traceability, including methodological references, representative prior surveys, and reviewed studies.	PDF list

Supplementary Fig. S1. Structure of the systematic literature review

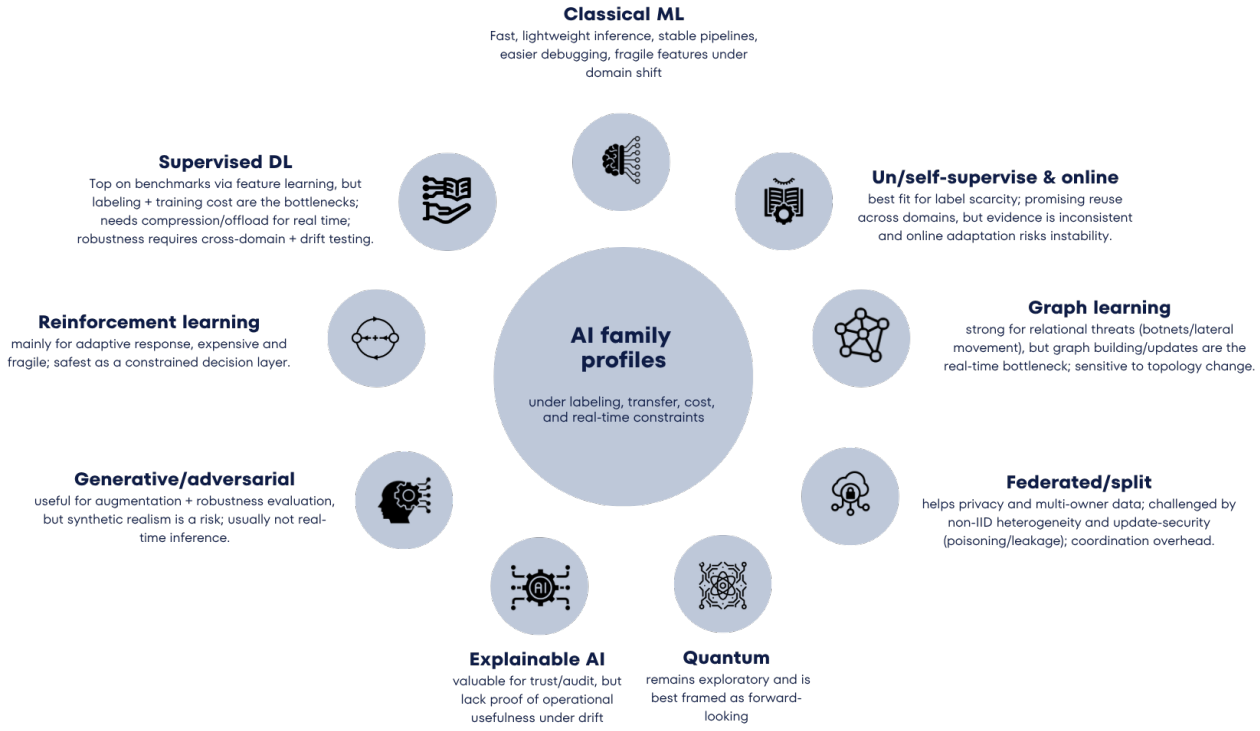
Reviewer note. This figure gives reviewers a visual overview of the review workflow. It links database searching, citation chaining, deduplication, screening, eligibility assessment, extraction, quality appraisal, and synthesis into one traceable methodological structure.



Supplementary Fig. S1. Structure of the systematic literature review, showing how the search, screening, extraction, quality assessment, and synthesis stages are connected.

Supplementary Fig. S2. AI-family profiles under deployment constraints

Reviewer note. This figure provides a qualitative synthesis of how major AI families relate to labeling burden, transfer, resource and real-time feasibility, robustness, explainability, privacy, and governance constraints. It should be read as a synthesis aid rather than a quantitative ranking.



Supplementary Fig. S2. AI-family profiles under deployment constraints. The figure summarizes how major AI families relate to labeling burden, transfer, resource and real-time feasibility, robustness, explainability, privacy, and governance constraints. It is intended as a qualitative synthesis aid rather than a quantitative ranking of model families.

Supplementary Reference List. References supporting the review and full corpus traceability

Reviewer note. This list reports the sources cited in the Supplementary Information, including methodological references, representative prior surveys, and reviewed studies used in the systematic literature review. It supports transparency while avoiding confusion between background/methodological references and the machine-readable included-study registry.

This reference list reports the sources cited in the Supplementary Information, including methodological references, representative prior surveys, and reviewed studies used in the systematic literature review. The complete included-study registry, with study identifiers, bibliographic metadata, AI-family coding, security-task coding, dataset information, quality scores, and extraction variables, is provided separately in Supplementary Data S1.

References

1. El Azzaoui, A., Salim, M. M. & Park, J. H. Secure and reliable big data based decision making using quantum approach in IIoT systems. *Sensors* **23**, 4852, https://doi.org/10.3390/s23104852 (2023).
2. Ferrag, M. A. *et al.* Edge learning for 6G enabled Internet of Things: A comprehensive survey of vulnerabilities, datasets, and defenses. *IEEE Commun. Surv. Tutor.* **25**, 2654–2713, https://doi.org/10.1109/COMST.2023.3317242 (2023).
3. Khan, A. A. *et al.* Artificial intelligence, Internet of Things, and blockchain empowering future vehicular developments: A comprehensive multi-hierarchical lifecycle review. *Hum.-Centric Comput. Inf. Sci.* **15**, 13, https://doi.org/10.22967/HCIS.2025.15.013 (2025).
4. Park, J. H. *et al.* A comprehensive survey on blockchain for secure IoT-enabled smart city beyond 5G: Approaches, processes, challenges, and opportunities. *Hum.-Centric Comput. Inf. Sci.* **13**, 51, https://doi.org/10.22967/HCIS.2023.13.051 (2023).
5. Bhanu, B. S. *et al.* IoT integrated edge platform for secure industrial application with deep learning. *Hum.-Centric Comput. Inf. Sci.* **13**, 19, https://doi.org/10.22967/HCIS.2023.13.019 (2023).
6. Park, J. H. *et al.* PoAh enabled federated learning architecture for DDoS attack detection in IoT networks. *Hum.-Centric Comput. Inf. Sci.* **14**, 3, https://doi.org/10.22967/HCIS.2024.14.003 (2024).
7. Li, Q. *et al.* A novel intrusion detection method for imbalanced datasets. *Hum.-Centric Comput. Inf. Sci.* **15**, 19, https://doi.org/10.22967/HCIS.2025.15.019 (2025).
8. Hdaib, M. *et al.* Quantum deep learning-based anomaly detection for enhanced network security. *Quantum Mach. Intell.* **6**, 26, https://doi.org/10.1007/s42484-024-00163-2 (2024).
9. Tychola, K. A. *et al.* Quantum machine learning: An overview. *Electronics* **12**, 2379, https://doi.org/10.3390/electronics12112379 (2023).
10. Oh, H. & Park, D. K. Quantum support vector data description for anomaly detection. *Mach. Learn. Sci. Technol.* **5**, 035052, https://doi.org/10.1088/2632-2153/ad6be8 (2024).
11. Kitchenham, B. & Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. Keele University and Durham University Joint Report, EBSE-2007-01 (2007).
12. Moher, D. *et al.* Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Med.* **6**, e1000097, https://doi.org/10.1371/journal.pmed.1000097 (2009).
13. Al-amri, R. *et al.* A review of machine learning and deep learning techniques for anomaly detection in IoT data. *Appl. Sci.* **11**, 5320, https://doi.org/10.3390/app11125320 (2021).
14. Zhao, J. *et al.* A review of computer vision methods in network security. *IEEE Commun. Surv. Tutor.* **23**, 1838–1878, https://doi.org/10.1109/COMST.2021.3086475 (2021).
15. Fedorchenko, E. *et al.* Comparative review of the intrusion detection systems based on federated learning: Advantages and open challenges. *Algorithms* **15**, 247, https://doi.org/10.3390/a15070247 (2022).
16. Jamalipour, A. & Murali, S. A taxonomy of machine learning-based intrusion detection systems for the Internet of Things: A survey. *IEEE Internet Things J.* **9**, 9444–9466, https://doi.org/10.1109/JIOT.2021.3126811 (2022).
17. Ferrag, M. A., Shu, L., Friha, O. & Yang, X. Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA J. Autom. Sin.* **9**, 407–436, https://doi.org/10.1109/JAS.2021.1004344 (2022).

18. Yang, M. & Zhang, J. Data anomaly detection in the Internet of Things: A review of current trends and research challenges. *Int. J. Adv. Comput. Sci. Appl.* **14**, https://doi.org/10.14569/IJACSA.2023.0140901 (2023).

19. Zehra, S. *et al.* Machine learning-based anomaly detection in NFV: A comprehensive survey. *Sensors* **23**, 5340, https://doi.org/10.3390/s23115340 (2023).

20. Khatun, M. A. *et al.* Machine learning for healthcare IoT security: A review and risk mitigation. *IEEE Access* **11**, 145869–145896, https://doi.org/10.1109/ACCESS.2023.3346320 (2023).

21. Bansal, K. & Singhrova, A. Review on intrusion detection system for IoT/IIoT brief study. *Multimed. Tools Appl.* **83**, 23083–23108, https://doi.org/10.1007/s11042-023-16395-6 (2024).

22. Alotaibi, A. & Barnawi, A. Securing massive IoT in 6G: Recent solutions, architectures, future directions. *Internet Things* **22**, 100715, https://doi.org/10.1016/j.iot.2023.100715 (2023).

23. Belay, M. A. *et al.* Unsupervised anomaly detection for IoT-based multivariate time series: Existing solutions, performance analysis and future directions. *Sensors* **23**, 2844, https://doi.org/10.3390/s23052844 (2023).

24. Moustafa, N. *et al.* Explainable intrusion detection for cyber defences in the Internet of Things: Opportunities and solutions. *IEEE Commun. Surv. Tutor.* **25**, 1775–1807, https://doi.org/10.1109/COMST.2023.3280465 (2023).

25. Rafique, S. H. *et al.* Machine learning and deep learning techniques for Internet of Things network anomaly detection: Current research trends. *Sensors* **24**, 1968, https://doi.org/10.3390/s24061968 (2024).

26. Adhikari, D. *et al.* Recent advances in anomaly detection in Internet of Things: Status, challenges, and perspectives. *Comput. Sci. Rev.* **54**, 100665, https://doi.org/10.1016/j.cosrev.2024.100665 (2024).

27. Mishra, N. & Pandya, S. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access* **9**, 59353–59377, https://doi.org/10.1109/ACCESS.2021.3070853 (2021).

28. Araya, J. I. I. & Rifà-Pous, H. Anomaly-based cyberattacks detection for smart homes: A systematic literature review. *Internet Things* **22**, 100792, https://doi.org/10.1016/j.iot.2023.100792 (2023).

29. Jeffrey, N. *et al.* A review of anomaly detection strategies to detect threats to cyber-physical systems. *Electronics* **12**, 3283, https://doi.org/10.3390/electronics12153283 (2023).

30. Isong, B. *et al.* Insights into modern intrusion detection strategies for Internet of Things ecosystems. *Electronics* **13**, 2370, https://doi.org/10.3390/electronics13122370 (2024).

31. Kikissagbe, B. R. & Adda, M. Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. *Electronics* **13**, 3601, https://doi.org/10.3390/electronics13183601 (2024).

32. Trilles, S. *et al.* Anomaly detection based on artificial intelligence of things: A systematic literature mapping. *Internet Things* **25**, 101063, https://doi.org/10.1016/j.iot.2024.101063 (2024).

33. Wu, W. *et al.* Deep transfer learning techniques in intrusion detection system Internet of vehicles: A state-of-the-art review. *Comput. Mater. Continua* **80**, 2785–2813, https://doi.org/10.32604/cmc.2024.053037 (2024).

34. Cruz, M. A. A. D. *et al.* Detecting compromised IoT devices through XGBoost. *IEEE Trans. Intell. Transp. Syst.* **24**, 15392–15399, https://doi.org/10.1109/TITS.2022.3187252 (2023).

35. Balta, E. C. *et al.* Digital twin-based cyber attack detection framework for cyber-physical manufacturing systems. *IEEE Trans. Autom. Sci. Eng.* **21**, 1695–1712, https://doi.org/10.1109/TASE.2023.3243147 (2024).

36. Yu, J. *et al.* CONGO^2: Scalable online anomaly detection and localization in power electronics networks. *IEEE Internet Things J.* **9**, 13862–13875, https://doi.org/10.1109/JIOT.2022.3143123 (2022).

37. Azeri, N. *et al.* A distributed intelligence framework for enhancing resilience and data privacy in dynamic cyber-physical systems. *Clust. Comput.* **27**, 6289–6304, https://doi.org/10.1007/s10586-024-04349-y (2024).

38. Sharmeen, S. *et al.* An advanced boundary protection control for the smart water network using semisupervised and deep learning approaches. *IEEE Internet Things J.* **9**, 7298–7310, https://doi.org/10.1109/JIOT.2021.3138372 (2022).

39. Khan, I. A. *et al.* A context-aware zero-trust-based hybrid approach to IoT-based self-driving vehicles security. *Ad Hoc Netw.* **167**, 103694, https://doi.org/10.1016/j.adhoc.2024.103694 (2025).

40. Huertas Celdrán, A. *et al.* Privacy-preserving and syscall-based intrusion detection system for IoT spectrum sensors affected by data falsification attacks. *IEEE Internet Things J.* **10**, 8408–8415, https://doi.org/10.1109/JIOT.2023.3261989 (2023).

41. Rosero-Montalvo, P. D. *et al.* Hybrid anomaly detection model on trusted IoT devices. *IEEE Internet Things J.* **10**, 10959–10969, https://doi.org/10.1109/JIOT.2023.3243037 (2023).

42. Abououf, M. *et al.* Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. *IEEE Internet Things J.* **11**, 3446–3457, https://doi.org/10.1109/JIOT.2023.3296809 (2024).

43. Kayan, H. *et al.* CASPER: Context-aware IoT anomaly detection system for industrial robotic arms. *ACM Trans. Internet Things* **5**, 1–36, https://doi.org/10.1145/3670414 (2024).

44. Jahangir, H. *et al.* A deep learning-based solution for securing the power grid against load-altering threats by IoT-enabled devices. *IEEE Internet Things J.* **10**, 10687–10697, https://doi.org/10.1109/JIOT.2023.3240289 (2023).

45. Xu, X. *et al.* Internet of Things for emotion care: Advances, applications, and challenges. *Cogn. Comput.* **16**, 2812–2832, https://doi.org/10.1007/s12559-024-10327-8 (2024).

46. Li, R. *et al.* ADRIoT: An edge-assisted anomaly detection framework against IoT-based network attacks. *IEEE Internet Things J.* **9**, 10576–10587, https://doi.org/10.1109/JIOT.2021.3122148 (2022).

47. Fu, C. *et al.* Frequency-domain feature-based robust malicious traffic detection. *IEEE/ACM Trans. Netw.* **31**, 452–467, https://doi.org/10.1109/TNET.2022.3195871 (2023).

48. Shukla, P. *et al.* EIoT-DDoS: Embedded classification approach for IoT traffic-based DDoS attacks. *Clust. Comput.* **27**, 1471–1490, https://doi.org/10.1007/s10586-023-04027-5 (2024).

49. Hussan, M. I. T. *et al.* DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. *Clust. Comput.* **27**, 4469–4490, https://doi.org/10.1007/s10586-023-04187-4 (2024).

50. Mothukuri, V. *et al.* Federated learning-based anomaly detection for IoT security attacks. *IEEE Internet Things J.* **9**, 2545–2554, https://doi.org/10.1109/JIOT.2021.3077803 (2022).

51. Kumar, A. *et al.* Machine learning-based early detection of IoT botnets using network-edge traffic. *Comput. Secur.* **117**, 102693, https://doi.org/10.1016/j.cose.2022.102693 (2022).

52. Soltani, N. *et al.* Robust intrusion detection for network communication on the Internet of Things: A hybrid machine learning approach. *Clust. Comput.* **27**, 9975–9991, https://doi.org/10.1007/s10586-024-04483-7 (2024).

53. Wang, Z. *et al.* A deep residual SConv1D-attention intrusion detection model for industrial Internet of Things. *Clust. Comput.* **28**, 116, https://doi.org/10.1007/s10586-024-04786-9 (2025).

54. Karacayılmaz, G. & Artuner, H. A novel approach detection for IIoT attacks via artificial intelligence. *Clust. Comput.* **27**, 10467–10485, https://doi.org/10.1007/s10586-024-04529-w (2024).

55. Cai, J. *et al.* CapBad: Content-agnostic, payload-based anomaly detector for industrial control protocols. *IEEE Internet Things J.* **9**, 12542–12554, https://doi.org/10.1109/JIOT.2021.3138534 (2022).

56. Fan, C. *et al.* Auto-updating intrusion detection system for vehicular network: A deep learning approach based on cloud-edge-vehicle collaboration. *IEEE Trans. Veh. Technol.* **73**, 15372–15384, https://doi.org/10.1109/TVT.2024.3399219 (2024).

57. Ahakonye, L. A. C. *et al.* SCADA intrusion detection scheme exploiting the fusion of modified decision tree and Chi-square feature selection. *Internet Things* **21**, 100676, https://doi.org/10.1016/j.iot.2022.100676 (2023).

58. Li, R. *et al.* SeIoT: Detecting anomalous semantics in smart homes via knowledge graph. *IEEE Trans. Inf. Forensics Secur.* **19**, 7005–7018, https://doi.org/10.1109/TIFS.2024.3375000 (2024).

59. Mishra, A. K. & Paliwal, S. Mitigating cyber threats through integration of feature selection and stacking ensemble learning: The LGBM and random forest intrusion detection perspective. *Clust. Comput.* **26**, 2339–2350, https://doi.org/10.1007/s10586-022-03735-8 (2023).

60. Truong, V. T. & Le, L. B. MetaCIDS: Privacy-preserving collaborative intrusion detection for metaverse based on blockchain and online federated learning. *IEEE Open J. Comput. Soc.* **4**, 253–266, https://doi.org/10.1109/OJCS.2023.3312299 (2023).

61. Verma, P. *et al.* Zero-day guardian: A dual-model-enabled federated learning framework for handling zero-day attacks in 5G-enabled IIoT. *IEEE Trans. Consum. Electron.* **70**, 3856–3866, https://doi.org/10.1109/TCE.2023.3335385 (2024).

62. Yazdinejad, A. *et al.* Block Hunter: Federated learning for cyber threat hunting in blockchain-based IIoT networks. *IEEE Trans. Ind. Inform.* **18**, 8356–8366, https://doi.org/10.1109/TII.2022.3168011 (2022).

63. Cui, L. *et al.* Boosting accuracy of differentially private federated learning in industrial IoT with sparse responses. *IEEE Trans. Ind. Inform.* **19**, 910–920, https://doi.org/10.1109/TII.2022.3161517 (2023).

64. Pan, Z. *et al.* One-shot backdoor removal for federated learning. *IEEE Internet Things J.* **11**, 37718–37730, https://doi.org/10.1109/JIOT.2024.3438150 (2024).

65. Xu, X. *et al.* SAFE: Synergic data filtering for federated learning in cloud-edge computing. *IEEE Trans. Ind. Inform.* **19**, 1655–1665, https://doi.org/10.1109/TII.2022.3195896 (2023).

66. Samriya, J. K. *et al.* Adversarial ML-based secured cloud architecture for consumer Internet of Things of smart healthcare. *IEEE Trans. Consum. Electron.* **70**, 2058–2065, https://doi.org/10.1109/TCE.2023.3341696 (2024).

67. Sánchez-Sánchez, P. M. *et al.* Robust federated learning for execution-time-based device model identification under label-flipping attack. *Clust. Comput.* **27**, 313–324, https://doi.org/10.1007/s10586-022-03949-w (2024).

68. Sánchez, P. M. *et al.* Studying the robustness of anti-adversarial federated learning models detecting cyberattacks in IoT spectrum sensors. *IEEE Trans. Dependable Secure Comput.* **21**, 573–584, https://doi.org/10.1109/TDSC.2022.3204535 (2024).

69. Liu, Y. *et al.* Swarm learning and knowledge distillation empowered self-driving detection against threat behavior for intelligent IoT. *IEEE Trans. Mob. Comput.* **23**, 7117–7134, https://doi.org/10.1109/TMC.2023.3330514 (2024).

70. Purohit, R. M. *et al.* FedBlocks: Federated learning and blockchain-based privacy-preserved pioneering framework for IoT healthcare using IPFS in web 3.0 era. *Clust. Comput.* **28**, 139, https://doi.org/10.1007/s10586-024-04738-3 (2025).

71. Esmaeili, B. *et al.* A GNN-based adversarial Internet of Things malware detection framework for critical infrastructure: Studying gafgyt, mirai, and tsunami campaigns. *IEEE Internet Things J.* **11**, 26826–26836, https://doi.org/10.1109/JIOT.2023.3298663 (2024).

72. Nguyen, H. & Kashef, R. TS-IDS: Traffic-aware self-supervised learning for IoT network intrusion detection. *Knowl.-Based Syst.* **279**, 110966, https://doi.org/10.1016/j.knosys.2023.110966 (2023).

73. Fu, C. *et al.* Flow interaction graph analysis: Unknown encrypted malicious traffic detection. *IEEE/ACM Trans. Netw.* **32**, 2972–2987, https://doi.org/10.1109/TNET.2024.3370851 (2024).

74. Sarkar, N. *et al.* A better and fast cloud intrusion detection system using improved squirrel search algorithm and modified deep belief network. *Clust. Comput.* **27**, 1699–1718, https://doi.org/10.1007/s10586-023-04037-3 (2024).

75. Sivasakthi, D. A. *et al.* HybridRobustNet: Enhancing detection of hybrid attacks in IoT networks through advanced learning approach. *Clust. Comput.* **27**, 5005–5019, https://doi.org/10.1007/s10586-023-04248-8 (2024).

76. Jayalaxmi, P. L. S. *et al.* MADESANT: Malware detection and severity analysis in industrial environments. *Clust. Comput.* **27**, 11347–11367, https://doi.org/10.1007/s10586-024-04527-y (2024).

77. Babbar, H. & Rani, S. FRHIDS: Federated learning recommender hybrid intrusion detection system model in software-defined networking for consumer devices. *IEEE Trans. Consum. Electron.* **70**, 2492–2499, https://doi.org/10.1109/TCE.2023.3329151 (2024).

78. Yang, L. *et al.* MTH-IDS: A multitiered hybrid intrusion detection system for Internet of vehicles. *IEEE Internet Things J.* **9**, 616–632, https://doi.org/10.1109/JIOT.2021.3084796 (2022).

79. Mittal, K. & Khurana Batra, P. Graph ensemble fusion for enhanced IoT intrusion detection: Leveraging GCN and deep learning. *Clust. Comput.* **27**, 10525–10552, https://doi.org/10.1007/s10586-024-04404-8 (2024).

80. Asri, T. M. *et al.* Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction. *J. Big Data* **11**, 33, https://doi.org/10.1186/s40537-024-00886-w (2024).

81. Hazman, C. *et al.* Enhanced IDS with deep learning for IoT-based smart cities security. *Tsinghua Sci. Technol.* **29**, 929–947, https://doi.org/10.26599/TST.2024.9010019 (2024).

82. Kim, D. J. *et al.* A novel split learning-based consumer electronics network traffic anomaly detection framework for smart city environment. *IEEE Trans. Consum. Electron.* **70**, 4197–4204, https://doi.org/10.1109/TCE.2024.3356410 (2024).

83. Zeghida, H. *et al.* Enhancing IoT cyber-attacks intrusion detection through GAN-based data augmentation and hybrid deep learning models for MQTT network protocol cyber-attacks. *Clust. Comput.* **28**, 58, https://doi.org/10.1007/s10586-024-04750-7 (2025).

84. Zhang, J. *et al.* Federated learning for distributed IIoT intrusion detection using transfer approaches. *IEEE Trans. Ind. Inform.* **19**, 8159–8169, https://doi.org/10.1109/TII.2022.3216575 (2023).

85. Abid, A. *et al.* Real-time data fusion for intrusion detection in industrial control systems based on cloud computing and big data techniques. *Clust. Comput.* **27**, 2217–2238, https://doi.org/10.1007/s10586-023-04087-7 (2024).

86. Bajpai, A. *et al.* A novel methodology for anomaly detection in smart home networks via fractional stochastic gradient descent. *Comput. Electr. Eng.* **119**, 109604, https://doi.org/10.1016/j.compeleceng.2024.109604 (2024).

87. Eljialy, A. E. M. *et al.* Novel framework for an intrusion detection system using multiple feature selection methods based on deep learning. *Tsinghua Sci. Technol.* **29**, 948–958, https://doi.org/10.26599/TST.2023.9010032 (2024).

88. Shukla, P. *et al.* SDDA-IoT: Storm-based distributed detection approach for IoT network traffic-based DDoS attacks. *Clust. Comput.* **27**, 6397–6424, https://doi.org/10.1007/s10586-023-04230-7 (2024).

89. Ahmadi Assalemi, G. *et al.* Super learner ensemble for anomaly detection and cyber risk quantification in industrial control systems. *IEEE Internet Things J.* **9**, 13279–13297, https://doi.org/10.1109/JIOT.2022.3144127 (2022).

90. Jemili, F. *et al.* Intrusion detection based on ensemble learning for big data classification. *Clust. Comput.* **27**, 3771–3798, https://doi.org/10.1007/s10586-023-04149-w (2024).

91. Chohra, A. *et al.* Chameleon: Optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection. *Comput. Secur.* **117**, 102684, https://doi.org/10.1016/j.cose.2022.102684 (2022).

92. Alwaisi, Z. *et al.* Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention. *Internet Things* **28**, 101398, https://doi.org/10.1016/j.iot.2024.101398 (2024).

93. Aurangzeb, S. *et al.* Cybersecurity for autonomous vehicles against malware attacks in smart cities. *Clust. Comput.* **27**, 3363–3378, https://doi.org/10.1007/s10586-023-04074-y (2024).

94. Khan, S. *et al.* Hybrid computing framework security in dynamic offloading for IoT-enabled smart home system. *PeerJ Comput. Sci.* **10**, e2211, https://doi.org/10.7717/peerj-cs.2211 (2024).

95. Sharma, S. *et al.* PULSE: Proactive uncovering of latent severe anomalous events in IIoT using LSTM-RF model. *Clust. Comput.* **27**, 13749–13762, https://doi.org/10.1007/s10586-024-04653-7 (2024).

96. Zheng, C. *et al.* IIsy: Hybrid in-network classification using programmable switches. *IEEE/ACM Trans. Netw.* **32**, 2555–2570, https://doi.org/10.1109/TNET.2024.3383952 (2024).

97. Farfoura, M. E. *et al.* A lightweight machine learning methods for malware classification. *Clust. Comput.* **28**, 1, https://doi.org/10.1007/s10586-024-04665-3 (2025).

98. Zukaib, U. *et al.* Meta-IDS: Meta-learning-based smart intrusion detection system for Internet of Medical Things network. *IEEE Internet Things J.* **11**, 23080–23095, https://doi.org/10.1109/JIOT.2024.3369777 (2024).

99. Toony, A. A. *et al.* MULTI-BLOCK: A novel ML-based intrusion detection framework for SDN-enabled IoT networks using new pyramidal structure. *Internet Things* **26**, 101231, https://doi.org/10.1016/j.iot.2024.101231 (2024).

100. Xie, G. *et al.* Empowering in-network classification in programmable switches by binary decision tree and knowledge distillation. *IEEE/ACM Trans. Netw.* **32**, 382–395, https://doi.org/10.1109/TNET.2023.3287091 (2024).

101. Ahakonye, L. A. C. *et al.* Agnostic CH-DT technique for SCADA network high-dimensional data-aware intrusion detection system. *IEEE Internet Things J.* **10**, 10344–10356, https://doi.org/10.1109/JIOT.2023.3237797 (2023).

102. Örs, F. K. & Levi, A. Data-driven intrusion detection for 6LoWPAN-based IoT systems. *Ad Hoc Netw.* **143**, 103120, https://doi.org/10.1016/j.adhoc.2023.103120 (2023).

103. Amaouche, S. *et al.* IDS-XGbFS: A smart intrusion detection system using XGBoost with recent feature selection for VANET safety. *Clust. Comput.* **27**, 3521–3535, https://doi.org/10.1007/s10586-023-04157-w (2024).

104. Hazman, C. *et al.* A smart model integrating LSTM and XGBoost for improving IoT-enabled smart cities security. *Clust. Comput.* **28**, 70, https://doi.org/10.1007/s10586-024-04780-1 (2025).

105. Hazman, C. *et al.* lIDS-SIoEL: Intrusion detection framework for IoT-based smart environments security using ensemble learning. *Clust. Comput.* **26**, 4069–4083, https://doi.org/10.1007/s10586-022-03810-0 (2023).

106. Alhowaide, A. *et al.* Towards the design of real-time autonomous IoT NIDS. *Clust. Comput.* **26**, 2489–2502, https://doi.org/10.1007/s10586-021-03231-5 (2023).

107. Ilango, H. S. *et al.* A FeedForward-convolutional neural network to detect low-rate DoS in IoT. *Eng. Appl. Artif. Intell.* **114**, 105059, https://doi.org/10.1016/j.engappai.2022.105059 (2022).

108. Shukla, R. M. & Sengupta, S. A novel machine learning pipeline to detect malicious anomalies for the Internet of Things. *Internet Things* **20**, 100603, https://doi.org/10.1016/j.iot.2022.100603 (2022).

109. Malathi, D. S. & Begum, S. R. Enhancing trustworthiness among IoT network nodes with ensemble deep learning-based cyber attack detection. *Expert Syst. Appl.* **255**, 124528, https://doi.org/10.1016/j.eswa.2024.124528 (2024).

110. Qiao, H. *et al.* Concept drift analysis by dynamic residual projection for effectively detecting botnet cyber attacks in IoT scenarios. *IEEE Trans. Ind. Inform.* **18**, 3692–3701, https://doi.org/10.1109/TII.2021.3108464 (2022).

111. Belhadi, A. *et al.* Group intrusion detection in the Internet of Things using a hybrid recurrent neural network. *Clust. Comput.* **26**, 1147–1158, https://doi.org/10.1007/s10586-022-03779-w (2023).

112. Abid, Y. A. *et al.* Multilevel deep neural network approach for enhanced distributed denial-of-service attack detection and classification in software-defined Internet of Things networks. *IEEE Internet Things J.* **11**, 24715–24725, https://doi.org/10.1109/JIOT.2024.3376578 (2024).

113. Chander, N. & Upendra Kumar, M. Enhanced pelican optimization algorithm with ensemble-based anomaly detection in industrial Internet of Things environment. *Clust. Comput.* **27**, 6491–6509, https://doi.org/10.1007/s10586-024-04303-y (2024).

114. Bensaid, R. *et al.* Securing fog-assisted IoT smart homes: A federated learning-based intrusion detection approach. *Clust. Comput.* **28**, 50, https://doi.org/10.1007/s10586-024-04711-0 (2025).

115. Zareh Farkhady, R. *et al.* 3DLBS-BCHO: A three-dimensional deep learning approach based on branch splitter and binary chimp optimization for intrusion detection in IoT. *Clust. Comput.* **28**, 83, https://doi.org/10.1007/s10586-024-04768-x (2025).

116. Dou, S. *et al.* Anomaly detection in event-triggered traffic time series via similarity learning. *IEEE Trans. Dependable Secure Comput.*, https://doi.org/10.1109/TDSC.2024.3418906 (2024).

117. Khan, I. A. *et al.* DFF-SC4N: A deep federated defence framework for protecting supply chain 4.0 networks. *IEEE Trans. Ind. Inform.* **19**, 3300–3309, https://doi.org/10.1109/TII.2021.3108811 (2023).

118. Xie, S. *et al.* Anomaly detection for multivariate time series in IoT using discrete wavelet decomposition and dual graph attention networks. *Comput. Secur.* **146**, 104075, https://doi.org/10.1016/j.cose.2024.104075 (2024).

119. Oseni, A. *et al.* An explainable deep learning framework for resilient intrusion detection in IoT-enabled transportation networks. *IEEE Trans. Intell. Transp. Syst.* **24**, 1000–1014, https://doi.org/10.1109/TITS.2022.3188671 (2023).

120. Cui, L. *et al.* Security and privacy enhanced federated learning for anomaly detection in IoT infrastructures. *IEEE Trans. Ind. Inform.* **18**, 3492–3500, https://doi.org/10.1109/TII.2021.3107783 (2022).

121. Wang, Z. *et al.* A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning. *Expert Syst. Appl.* **206**, 117671, https://doi.org/10.1016/j.eswa.2022.117671 (2022).

122. Nguyen, X. H. & Le, K. H. Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model. *Internet Things* **23**, 100851, https://doi.org/10.1016/j.iot.2023.100851 (2023).

123. Praveena Anjelin, D. & Ganesh Kumar, S. An effective classification using enhanced elephant herding optimization with convolution neural network for intrusion detection in IoMT architecture. *Clust. Comput.* **27**, 12341–12359, https://doi.org/10.1007/s10586-024-04512-5 (2024).

124. Al-Fawa'reh, M. *et al.* MalBoT-DRL: Malware botnet detection using deep reinforcement learning in IoT networks. *IEEE Internet Things J.* **11**, 9610–9629, https://doi.org/10.1109/JIOT.2023.3324053 (2024).

125. Nazir, A. *et al.* Enhancing IoT security: A collaborative framework integrating federated learning, dense neural networks, and blockchain. *Clust. Comput.* **27**, 8367–8392, https://doi.org/10.1007/s10586-024-04436-0 (2024).

126. Ayantayo, A. *et al.* Network intrusion detection using feature fusion with deep learning. *J. Big Data* **10**, 167, https://doi.org/10.1186/s40537-023-00834-0 (2023).

127. Abdel Wahab, O. Intrusion detection in the IoT under data and concept drifts: Online deep learning approach. *IEEE Internet Things J.* **9**, 19706–19716, https://doi.org/10.1109/JIOT.2022.3167005 (2022).

128. Muhammad, G. *et al.* Stacked autoencoder-based intrusion detection system to combat financial fraudulent. *IEEE Internet Things J.* **10**, 2071–2078, https://doi.org/10.1109/JIOT.2021.3041184 (2023).

129. Nakıp, M. & Gelenbe, E. Online self-supervised deep learning for intrusion detection systems. *IEEE Trans. Inf. Forensics Secur.* **19**, 5668–5683, https://doi.org/10.1109/TIFS.2024.3402148 (2024).

130. Alshahrani, H. *et al.* Energy-aware routing with optimal deep learning-based anomaly detection in 6G IoT networks. *Sustain. Energy Technol. Assess.* **60**, 103494, https://doi.org/10.1016/j.seta.2023.103494 (2023).

131. Hilal, A. M. *et al.* Deep learning-enabled class imbalance with sand piper optimization-based intrusion detection for secure cyber-physical systems. *Clust. Comput.* **26**, 2085–2098, https://doi.org/10.1007/s10586-022-03628-w (2023).

132. Dhanalaxmi, B. *et al.* OptFBFN: IoT threat mitigation in software-defined networks based on fuzzy approach. *Clust. Comput.* **27**, 12943–12963, https://doi.org/10.1007/s10586-024-04616-y (2024).

133. Maseno, E. M. & Wang, Z. Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection. *J. Big Data* **11**, 24, https://doi.org/10.1186/s40537-024-00887-9 (2024).

134. Vu, L. *et al.* Learning latent representation for IoT anomaly detection. *IEEE Trans. Cybern.* **52**, 3769–3782, https://doi.org/10.1109/TCYB.2021.3013416 (2022).

135. Das, S. *et al.* AIDPS: Adaptive intrusion detection and prevention system for underwater acoustic sensor networks. *IEEE/ACM Trans. Netw.* **32**, 1080–1095, https://doi.org/10.1109/TNET.2023.3313156 (2024).

136. Elsedimy, E. I. *et al.* A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. *Clust. Comput.* **27**, 9917–9935, https://doi.org/10.1007/s10586-024-04458-8 (2024).

137. Gyamfi, E. & Jurcut, A. D. Novel online network intrusion detection system for industrial IoT based on OI-SVDD and AS-ELM. *IEEE Internet Things J.* **10**, 3827–3839, https://doi.org/10.1109/JIOT.2022.3172393 (2023).

138. Gorzalczany, M. B. & Rudzinski, F. Intrusion detection in Internet of Things with MQTT protocol: An accurate and interpretable genetic fuzzy rule-based solution. *IEEE Internet Things J.* **9**, 24843–24855, https://doi.org/10.1109/JIOT.2022.3194837 (2022).

139. Costa, G. *et al.* Rule-based detection of anomalous patterns in device behavior for explainable IoT security. *IEEE Trans. Serv. Comput.* **16**, 4514–4525, https://doi.org/10.1109/TSC.2023.3327822 (2023).

140. Sáez de Cámara, X. *et al.* Clustered federated learning architecture for network anomaly detection in large-scale heterogeneous IoT networks. *Comput. Secur.* **131**, 103299, https://doi.org/10.1016/j.cose.2023.103299 (2023).

141. Asad, M. & Otoum, S. BPPFL: A blockchain-based framework for privacy-preserving federated learning. *Clust. Comput.* **28**, 126, https://doi.org/10.1007/s10586-024-04834-4 (2025).

142. Pourahmadi, V. *et al.* Spotting anomalies at the edge: Outlier exposure-based cross-silo federated learning for DDoS detection. *IEEE Trans. Dependable Secure Comput.* **20**, 4002–4015, https://doi.org/10.1109/TDSC.2022.3224896 (2023).

143. Siddiqui, M. A. *et al.* Anomaly detection framework for IoT-enabled appliances using machine learning. *Clust. Comput.* **27**, 9811–9835, https://doi.org/10.1007/s10586-024-04461-z (2024).

144. Fan, J. *et al.* Score-VAE: Root cause analysis for federated learning-based IoT anomaly detection. *IEEE Internet Things J.* **11**, 1041–1053, https://doi.org/10.1109/JIOT.2023.3289814 (2024).

145. Yang, K. *et al.* Stacked one-class broad learning system for intrusion detection in industry 4.0. *IEEE Trans. Ind. Inform.* **19**, 251–260, https://doi.org/10.1109/TII.2022.3157727 (2023).

146. Yu, S. *et al.* Deep Q-network-based open-set intrusion detection solution for industrial Internet of Things. *IEEE Internet Things J.* **11**, 12536–12550, https://doi.org/10.1109/JIOT.2023.3333903 (2024).

147. Amiri-Zarandi, M. *et al.* A federated and explainable approach for insider threat detection in IoT. *Internet Things* **24**, 100965, https://doi.org/10.1016/j.iot.2023.100965 (2023).

148. Feng, Y. *et al.* A collaborative stealthy DDoS detection method based on reinforcement learning at the edge of Internet of Things. *IEEE Internet Things J.* **10**, 17934–17948, https://doi.org/10.1109/JIOT.2023.3279615 (2023).

149. Zheng, T. *et al.* Enhancing TinyML-based container escape detectors with syscall semantic association in UAVs networks. *IEEE Internet Things J.* **11**, 21158–21169, https://doi.org/10.1109/JIOT.2024.3361452 (2024).

150. Nguyen, T. A. *et al.* Federated PCA on Grassmann manifold for IoT anomaly detection. *IEEE/ACM Trans. Netw.* **32**, 4456–4471, https://doi.org/10.1109/TNET.2024.3423780 (2024).

151. Wu, T. *et al.* Multiview ensemble learning-based robust graph convolutional networks against adversarial attacks. *IEEE Internet Things J.* **11**, 27700–27714, https://doi.org/10.1109/JIOT.2024.3400056 (2024).

152. Nguyen, D. D. N. *et al.* Toward IoT node authentication mechanism in next-generation networks. *IEEE Internet Things J.* **10**, 13333–13341, https://doi.org/10.1109/JIOT.2023.3262822 (2023).

153. Duan, C. *et al.* IoTa: Fine-grained traffic monitoring for IoT devices via fully packet-level models. *IEEE Trans. Dependable Secure Comput.* **21**, 3931–3947, https://doi.org/10.1109/TDSC.2023.3340563 (2024).

154. Ma, M. *et al.* An adaptive detection framework based on artificial immune for IoT intrusion detection system. *Appl. Soft Comput.* **166**, 112152, https://doi.org/10.1016/j.asoc.2024.112152 (2024).