

Supplementary Materials: Data-Extraction, Quality-Appraisal, and Eligibility-Audit Tables

for “Deep Learning for Proxy Zero-Day Intrusion Detection: A Systematic Review, Taxonomy, and Evaluation Framework”

Margaret Zita, Mujeeb Ur Rehman, Muhammad Kazim, Sohail Khalid,
Muhammad Abrar, Eerke Boiten

Online Resource 1 (Supplementary Material)

Article title: Deep Learning for Proxy Zero-Day Intrusion Detection: A Systematic Review, Taxonomy, and Evaluation Framework

Journal: *Artificial Intelligence Review* (Springer Nature)

Authors: Margaret Zita, Mujeeb Ur Rehman, Muhammad Kazim, Sohail Khalid, Muhammad Abrar, Eerke Boiten

Affiliations: Department of Computer Science and Informatics, De Montfort University, Leicester, UK; Department of Computer Science, University of Management and Technology, Lahore, Pakistan

Corresponding author: Mujeeb Ur Rehman, mujeeb.rehman@dmu.ac.uk

This document accompanies the main manuscript and provides the full data-extraction, quality-appraisal, and eligibility-audit record for the systematic review. It contains five tables:

- **Table S1** – Bibliographic and dataset information for the 37 studies in the corrected audited primary synthesis corpus.
- **Table S2** – Reported-performance extraction (accuracy/F1) for the 15 primary-corpus studies with an extractable, architecture-specific absolute value, including the source text, architecture/dataset tags, and correction notes used in Section 4 of the main manuscript.
- **Table S3** – Reporting and methodological credibility appraisal (author-constructed checklist; not PROBAST, ROBIS, or another validated instrument – see Section 3.5 of the main manuscript) for the 37 audited primary-corpus studies, with final per-domain and overall counts.
- **Table S4** – Venue-stage background/emerging evidence: 41 records (32 journal or proceedings records and 9 preprint/repository records), retained for transparency. Publisher, issuing-organization, or repository names are supplied where they could be identified; bibliographic identification alone does not establish eligibility for the primary synthesis.
- **Table S5** – Background/emerging evidence excluded at the post-hoc eligibility audit: 22 records that passed venue verification but did not meet this review’s own empirical primary-study criteria, each with its specific reason (Section 3.4 of the main manuscript).

Study IDs are immutable screening identifiers. The corrected venue audit moves B019 and B029 into Tables S1–S3 without renumbering them, while S034, S035, S041, S012, S014, and S032 move to Table S5. The letter prefix therefore records the original audit-sheet position rather than the final inclusion status. **Each row cites its source with a standard \cite{} key rather than a bracketed number**, because this supplementary document and the main manuscript compile independent bibliographies from the same `refs-air.bib` database; a bracketed number here would not reliably correspond to the same reference’s number in the main text (this discrepancy was identified and corrected during the audit that produced this revision). Where a study is also cited in the main manuscript’s running text (e.g., the studies in Table S5 that additionally appear in the main text’s Table 1 survey comparison), the citation key is identical in both documents, so the two can always be cross-matched by key even though the rendered numbering differs.

Corpus composition. Of the 100 studies that passed topical screening (Figure 5 of the main manuscript), the corrected audit retained 59 records in the DOI-verified venue set and 41 records as venue-stage background/emerging evidence (Table S4: 32 journal or proceedings records and 9 preprint/repository records). Publisher/issuer/repository identification in Table S4 is a bibliographic clarification only: it does not, by itself, establish peer-review status, domain fit, a qualifying proxy protocol, or empirical eligibility. The eligibility audit excludes 22 of the 59 venue-verified records (Table S5: 11 literature reviews/surveys, 8 outside the network-intrusion-detection domain, 2 comparative/conceptual records without a qualifying primary empirical DL evaluation, and 1 record lacking demonstrated empirical validation), leaving 37 studies in the corrected primary synthesis corpus (Tables S1–S3) and 63 background/emerging-evidence records overall. Table S2 reports 15 of the 37 primary-corpus studies with an extractable, architecture-specific absolute accuracy or F1 value; the remaining 22 are valid corpus members that do not contribute a quantitative data point. Table S3 is a reporting and methodological credibility appraisal, not a validated risk-of-bias instrument.

Table S1: Bibliographic and dataset information for the 37 studies in the corrected, audited primary synthesis corpus.

Study ID	Citation	Venue (publisher)	Year	Peer-review status	Dataset(s)	Architecture family
S001	Raja and Mahri (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The study utilizes the CIC-IDS2023 data set, which provides realistic zero-day attack simulations and a wide range of system. . .	RNN/LSTM
S002	Hussain et al. (2026)	Taylor & Francis	2026	Peer-reviewed journal	The study utilizes various benchmark datasets, specifically NSL-KDD, CICIDS2017, CIC-AndMal2017, as well as a specially created. . .	Reinforcement
S003	Uttarkar and Vanjale (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study includes benchmark intrusion detection datasets, specifically NSL-KDD and CICIDS2017 . - The type. . .	Federated
S005	Nair and Rani (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study consists of a large dataset of network traffic. - Specific characteristics regarding the size, time. . .	CNN
S006	Chhetry et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is the CICIoT2023 dataset, which consists of benign data distributed across IoT nodes. - The. . .	Federated
S007	Kara et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset utilized in this study is the CIC-IDS2017 dataset, developed by the Canadian Institute for Cyber-security, which. . .	Reinforcement
S008	Kaur and Kalsi (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset utilized in the study consists of the latest network traffic datasets.	Federated
S009	Rodríguez et al. (2022)	MDPI	2022	Peer-reviewed journal	Three specialized datasets were created for evaluating the proposed intrusion detection framework. - The datasets are. . .	Unspecified/other DL
S010	Babu et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is not reported.	Hybrid
S011	Cristiano et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is not specified.	Unspecified/other DL
S013	Mpatziakas et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset consists of weakly labeled traffic data used to model networks in the context of Zero-Day attack detection. - No. . .	Unspecified/other DL
S015	Ranpara et al. (2025)	IET	2025	Peer-reviewed journal	The study uses the NSL-KDD and UNSW-NB15 datasets for evaluation . - The datasets consist of network event data used to measure. . .	Unspecified/other DL (Bayesian/probabilistic)
S016	Saurabh et al. (2024)	IEEE	2024	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is the CICIoT2023 dataset, which is specifically designed for IoT security. - The type of data. . .	Hybrid
S017	Roshan and Zafar (2021)	IEEE	2021	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is CICIDS2017, which is noted as the latest dataset for evaluation purposes. - The dataset is. . .	Autoencoder

Continued on next page

Table S1 – continued from previous page

Study ID	Citation	Venue (publisher)	Year	Peer-review status	Dataset(s)	Architecture family
S018	Mansur (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The study utilizes benchmark datasets, specifically CICIDS2017 and UNSW-NB15, for evaluating the proposed ZeroDayGuard framework. . .	Unspecified/other DL
S020	Mchina et al. (2026)	MDPI	2026	Peer-reviewed journal	The dataset used in the study is the CSE-CIC-IDS2018 dataset, which allows for the evaluation of network intrusion detection. . .	Hybrid
S021	Nithyalakshmi and Muthukumaravel (2026)	IGI Global	2026	Peer-reviewed book chapter	The dataset used in the study is the Next-Gen Cyber Threat Dataset (NGCTD-2025) . - The dataset includes attacks from categories. . .	Hybrid
S022	Prabu et al. (2024)	IEEE	2024	Peer-reviewed (IEEE conference/journal)	The study utilizes the CICIDS2017 and UNSW-NB15 datasets for evaluating the proposed AI-based network intrusion detection system. . . .	Autoencoder
S023	Khan (2024)	IET	2024	Peer-reviewed journal	The dataset for the study includes a testbed environment used to evaluate the proposed DL-ZTNA system. - Key variables assessed. . .	Unspecified/other DL
S024	Arun et al. (2024)	IEEE	2024	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is not mentioned.	Unspecified/other DL
S025	Sarhan et al. (2023)	Springer	2023	Peer-reviewed	The study utilizes two NIDS data sets: UNSW-NB15 and NF-UNSW-NB15-v2, which are synthetic and created using virtual network. . .	Few-shot/Meta
S028	Perumal et al. (2024)	IAES	2024	Peer-reviewed journal	The study utilizes well-established IDS datasets, CICIDS2017 and CSECICIDS2018, for evaluating the model's efficacy . - These. . .	Unspecified/other DL
S030	Sunkara et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study comprises experiments conducted in various cyber-physical systems (CPS) environments, which. . .	Unspecified/other DL (Bayesian/probabilistic)
S031	Kumar et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is derived from experimental analyses of the Optimized Cloud Intrusion Detection Framework (OCIDF). . . .	Ensemble/Classical-ML hybrid
S033	Zhang et al. (2023)	IEEE	2023	Peer-reviewed (IEEE conference/journal)	The dataset used in the study is the N-BaIoT, which is an open dataset . - Evaluations were conducted on this dataset to. . .	Federated
S036	Thatha et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset used in the study includes benchmark datasets like NSL-KDD, CICIDS2017, and UNSW-NB15. - NSL-KDD removes the. . .	Unspecified/other DL
S044	Nagarjun and Rajkumar (2025)	Nature Portfolio	2025	Peer-reviewed journal	The KDD99 dataset consists of 4.9 million records on network events labelled across 22 attack types, providing a foundation for. . .	Hybrid (multi-task study)

Continued on next page

Table S1 – continued from previous page

Study ID	Citation	Venue (publisher)	Year	Peer-review status	Dataset(s)	Architecture family
S045	Wang et al. (2025)	PLOS	2025	Peer-reviewed journal	The dataset used in the study includes the UNSW-NB15 and CICIDS2017 datasets, which are utilized for binary classification of . . .	Hybrid
S046	Basim et al. (2025)	IAES	2025	Peer-reviewed journal	The dataset consists of nine synthetic datasets generated for experiments within two security domains: network traffic and access. . .	Unspecified/other DL
S048	Malathi et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The dataset consists of a large-scale database with 1.2 million labeled events . - Data sources include network traffic logs, . . .	Hybrid
S049	Kinger and Rupa (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The study does not provide any specific information about the dataset used, including its source, type, size, timeframe, or key. . .	Few-shot/Meta
S050	Al-Jamali et al. (2025)	IET	2025	Peer-reviewed journal	The dataset used in the study is the CIC IoT Dataset 2023, which contains both malicious and the most recent attack patterns in. . .	CNN
S052	Saheed and Chukwuere (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The study evaluated Anomaly-Agent using the Edge-IIoTset (IIoT-specific) and CIC-IoT2023 (general IoT) datasets. - The. . .	Unspecified/other DL (LLM-agent)
S055	Prajwalasimha et al. (2025)	IEEE	2025	Peer-reviewed (IEEE conference/journal)	The study utilizes benchmark cybersecurity datasets, specifically CICIDS2017, BoT-IoT, and ToN-IoT . - These datasets are. . .	Federated
S056	Naeem et al. (2025)	PLOS	2025	Peer-reviewed journal	The dataset comprised 2000 episodes, with 1000 episodes used for training the model and another 1000 episodes for forecasting. - . . .	Reinforcement
B019	Soltani et al. (2023)	Elsevier	2023	Peer-reviewed journal	The study evaluates the DOC++ open-set recognition and adaptation framework on CIC-IDS2017 and CSE-CIC-IDS2018, including unknown-sample detection, clustering, expert-assisted labelling, and model updating.	Unspecified/other DL (open-set recognition)
B029	Hindy et al. (2020)	MDPI	2020	Peer-reviewed journal	The study evaluates an autoencoder-based zero-day NIDS using CICIDS2017 and NSL-KDD and compares it with a one-class SVM baseline.	Autoencoder

Architecture-coding method (Table S1, rightmost column): for the 15 studies in Table S2, architecture family is coded directly from each study’s full extracted source text. For the remaining 22 studies, architecture family is coded from the study’s title using a documented keyword rule (Federated: “federated”; Reinforcement: “reinforcement”/“DRL”/“Q-learning”; Few-shot/Meta: “few-shot”/“prototypical”/“meta-learning”/“zero-shot”; Transformer: “transformer”; GNN: “graph neural”/“GNN”; Autoencoder: “autoencoder”; CNN: “CNN”/“convolutional”/“DNN” absent other matches; RNN/LSTM: “LSTM”/“RNN”/“recurrent”; Ensemble/Classical-ML hybrid: “ensemble”/“stacking”/“multi-classifier”/“voting”; Hybrid: explicit “hybrid”/“fusion” wording or two or more of the preceding tags co-occurring; otherwise Unspecified/other DL). Both coding methods agree on every study where they could be cross-checked. This method has real limits: a title-only scan cannot detect an architecture the title does not name, so the 13-study “Unspecified/other DL” total in Table 11 of the main manuscript should be read as an upper bound on true architectural diversity rather than a claim that these 13 studies use no identifiable deep-learning method.

Table S2: Reported-performance extraction for the 15 audited primary-corpus studies with an extractable, architecture-specific absolute accuracy or F1 value, used in Section 4 (Tables 11–12 and Figure 6) of the main manuscript. Bold bracketed text marks a value-extraction correction or a final scope note for a multi-task or boundary-case study, resolved as described in each note.

Study ID	Citation	Architecture (coded)	Accuracy (%)	F1 (%)	Source-text extract used for extraction
S001	Raja and Mahri (2025)	RNN/LSTM	98.7	97.1	The proposed model achieves 98.7% accuracy, 97.4% precision, 96.9% recall, and an F1-score of 97.1% in detecting zero-day attacks . - The approach utilizes a Long Short-Term Memory (LSTM) network combined with attention mechanisms to model temporal. . . [Corrected: the pre-audit table entered the 97.4% precision figure in the accuracy column; 98.7% is the value the source text itself labels “accuracy”.]
S007	Kara et al. (2025)	Reinforcement (RL)	94.0	–	Decision Tree (DT) and Random Forest (RF) models achieve the highest accuracy in detecting known attacks, with RF reaching 99% accuracy, while Deep Q-Learning (DQL) shows a 94% accuracy but excels in identifying unknown threats like zero-day attacks - The. . . [Corrected: the pre-audit table reported RF’s 99% (a classical-ML baseline on known attacks) as the study’s headline DL value and coded the architecture as Ensemble/Classical-ML hybrid; 94% is DQL’s own, zero-day-proxy-relevant, deep-learning result, and the architecture is reclassified to Reinforcement (RL) accordingly.]
S010	Babu et al. (2025)	Hybrid (Autoencoder+RNN/LSTM+CNN)	97.0	–	A hybrid deep learning approach integrating Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks achieves detection accuracy above 97% in intrusion detection . - The system reports fewer false positives compared to conventional. . .
S015	Ranpara et al. (2025)	Unspecified/Other DL	96.2	–	A novel Bayesian Probabilistic Network (BPN) Framework was proposed for proactive zero-day attack detection, focusing on modeling dependencies between network events and real-time anomaly detection . - The framework integrates a hybrid detection mechanism. . . [Final decision: retained. The study is coded “Unspecified/other DL” rather than a named neural-network family because a Bayesian probabilistic network is a graphical/probabilistic model rather than a conventional deep neural architecture; it is kept in the corpus because it meets this review’s empirical, network-intrusion-detection, proxy-evaluation criteria (Section 3.3), and its dataset and reported accuracy are independently verifiable.]
S017	Roshan and Zafar (2021)	Autoencoder	99.3	–	The proposed Intrusion Detection System effectively detects Zero-day and unknown cyber-attacks using an autoencoder model. - The threshold plays a crucial role in achieving good recall for detecting Zero-day cyber-attacks, indicating that a single threshold. . .
S020	Mchina et al. (2026)	Hybrid (Autoencoder+CNN)	97.5	–	The proposed decision-level adaptive intrusion-detection framework combines hierarchical CNN-based closed-set classification with autoencoder-based zero-day detection in a cascade architecture, achieving strong closed-set performance with 98.98% accuracy and. . .
S021	Nithyalakshmi and Muthukumaravel (2026)	Hybrid (Autoencoder+Ensemble/Classical-ML-hybrid)	99.1	–	The proposed IDS model integrates XGBoost feature selection and Autoencoder-based anomaly detection, achieving a 99.1% detection accuracy . - The model reduces computational load by 20.5% and decreases false positive incidents by 20% . - Detection rates. . .

Continued on next page

Table S2 – continued from previous page

Study ID	Citation	Architecture (coded)	Accuracy (%)	F1 (%)	Source-text extract used for extraction
S022	Prabu et al. (2024)	Autoencoder	98.0	–	A novel AI-based network intrusion detection system (NIDS) is introduced to tackle data imbalance and enhance detection performance for zero-day attacks. - The study proposes an autoencoder with both basic and deep architectural implementations for improved...
S030	Sunkara et al. (2025)	Unspecified/Other DL	96.1	–	The presented method implements a probabilistic deep learning framework through Bayesian neural networks and graph attention networks to detect anomalies across distributed CPS nodes . - The detection excellence of this approach was ascertained through...
S031	Kumar et al. (2025)	Ensemble/Classical-ML-hybrid	94.0	94.0	OCIDF improves detection performance of cloud systems in terms of accuracy, adaptability, and efficiency, achieving 96% accuracy, 94% precision, 93% recall, and 93.5% F1-score . - The framework exhibits a high throughput of 3200 instances per second and...
S044	Nagarjun and Rajkumar (2025)	Hybrid (Transformer+GNN+Autoencoder)	99.1	98.2	Integration of Ethereum Blockchain with deep learning methods enhances cloud security by addressing diverse security challenges including data migration security, real-time intrusion detection, and threat response . - Blockchain-Aware Federated Learning for... [Final decision: retained. This is a multi-task study (blockchain security, fraud prevention, and intrusion detection are evaluated together); the reported 99.1%/98.2% figure is this study’s own headline value for its intrusion-detection component specifically, so it is kept as this study’s contributing data point, with the multi-task scope disclosed here for transparency rather than treated as a reason to exclude an otherwise-eligible record.]
S048	Malathi et al. (2025)	Hybrid (RNN/LSTM+CNN)	97.3	–	The proposed intelligent cybersecurity system achieves a 97.3% accuracy, 96.1 precision, 95.4 recall, and 0.99 AUC score . - The false positive rate is reduced to 2.1% . - The adaptive retraining mechanism enhances resistance to new zero-day attacks, making...
S049	Kinger and Rupa (2025)	Few-shot/Meta	84.0	–	An enhanced Intrusion Detection System (IDS) framework integrates Prototypical Network-based Meta-learning with Mahalanobis Distance-based Outlier Detection, enabling accurate classification with minimal labeled data . - The model successfully identified...
S052	Saheed and Chukwuere (2025)	Unspecified/Other DL	–	64.0	Anomaly-Agent is a novel LLM-powered explainable anomaly detection framework that successfully addresses zero-day threats in IoT/IIoT edge environments - The framework achieved accuracies of 0.96 and 0.89 on the Edge-IIoTset and CIC-IoT2023 datasets,...
B029	Hindy et al. (2020)	Autoencoder	92.96	–	The proposed autoencoder reports overall NSL-KDD accuracies of 91.84%, 92.96%, and 91.84% at thresholds 0.30, 0.25, and 0.20, respectively, and evaluates zero-day detection on CICIDS2017 and NSL-KDD. [Added after full-text verification: 92.96% is the highest explicitly reported overall NSL-KDD accuracy for the proposed autoencoder; CICIDS2017 results are primarily class- and threshold-specific and are not collapsed into an unsupported single overall value.]

Excluded from the 15-study quantitative subset (footnote): S002 (Hussain et al. (2026)) reported “91.7% accuracy” for its closed-set evaluation and an “83.4% detection rate” specifically for previously unseen (proxy zero-day) attacks; because these are different metric definitions and neither provides an unambiguous proxy-zero-day accuracy value under this table’s extraction rule, S002 is retained in the primary corpus but excluded from the quantitative subset. S012 (Okey et al. (2025)), together with S029, S038, S051, and S053, is excluded from the quantitative subset because the final eligibility audit (Table S5) removed the underlying study from the primary corpus; S012 was excluded as a device-identification study outside the NIDS domain.

Table S3: Reporting and methodological credibility appraisal for the 37 studies in the final audited primary synthesis corpus (author-constructed checklist; not PROBAST, ROBIS, AMSTAR 2, or another validated risk-of-bias instrument). D1: participants/dataset reporting; D2: predictors/architecture reporting; D3: outcome/metric reporting; D4: analysis/venue verification. Domain scoring rules and final aggregate counts are given in the note below.

Study ID	Citation	D1 Participants	D2 Predictors	D3 Outcome	D4 Analysis	Overall
S001	Raja and Mahri (2025)	Low	Low	Low	Low	Low
S002	Hussain et al. (2026)	Low	Low	Some concerns	Low	Some concerns
S003	Uttarkar and Vanjale (2025)	Low	Low	Some concerns	Low	Some concerns
S005	Nair and Rani (2025)	Low	Low	Some concerns	Low	Some concerns
S006	Chhetry et al. (2025)	Low	Low	Some concerns	Low	Some concerns
S007	Kara et al. (2025)	Low	Low	Low	Low	Low
S008	Kaur and Kalsi (2025)	Low	Low	Some concerns	Low	Some concerns
S009	Rodríguez et al. (2022)	Low	Some concerns	Some concerns	Low	Some concerns
S010	Babu et al. (2025)	High	Low	Low	Low	High
S011	Cristiano et al. (2025)	High	Some concerns	Some concerns	Low	High
S013	Mpatziakas et al. (2025)	Low	Some concerns	Some concerns	Low	Some concerns
S015	Ranpara et al. (2025)	Low	Some concerns	Low	Low	Some concerns
S016	Saurabh et al. (2024)	Low	Low	Some concerns	Low	Some concerns
S017	Roshan and Zafar (2021)	Low	Low	Low	Low	Low
S018	Mansur (2025)	Low	Some concerns	Some concerns	Low	Some concerns
S020	Mchina et al. (2026)	Low	Low	Low	Low	Low
S021	Nithyalakshmi and Muthukumaravel (2026)	Low	Low	Low	Low	Low
S022	Prabu et al. (2024)	Low	Low	Low	Low	Low
S023	Khan (2024)	Low	Some concerns	Some concerns	Low	Some concerns
S024	Arun et al. (2024)	High	Some concerns	Some concerns	Low	High
S025	Sarhan et al. (2023)	Low	Low	Some concerns	Low	Some concerns
S028	Perumal et al. (2024)	Low	Some concerns	Some concerns	Low	Some concerns
S030	Sunkara et al. (2025)	Low	Some concerns	Low	Low	Some concerns
S031	Kumar et al. (2025)	Low	Low	Low	Low	Low
S033	Zhang et al. (2023)	Low	Low	Some concerns	Low	Some concerns
S036	Thatha et al. (2025)	Low	Some concerns	Some concerns	Low	Some concerns

Continued on next page

Table S3 – continued from previous page

Study ID	Citation	D1 Participants	D2 Predictors	D3 Outcome	D4 Analysis	Overall
S044	Nagarjun and Rajkumar (2025)	Low	Low	Low	Low	Low
S045	Wang et al. (2025)	Low	Low	Some concerns	Low	Some concerns
S046	Basim et al. (2025)	Low	Some concerns	Some concerns	Low	Some concerns
S048	Malathi et al. (2025)	Low	Low	Low	Low	Low
S049	Kinger and Rupa (2025)	High	Low	Low	Low	High
S050	Al-Jamali et al. (2025)	Low	Low	Some concerns	Low	Some concerns
S052	Saheed and Chukwuere (2025)	Low	Some concerns	Low	Low	Some concerns
S055	Prajwalasimha et al. (2025)	Low	Low	Some concerns	Low	Some concerns
S056	Naeem et al. (2025)	Low	Low	Some concerns	Low	Some concerns
B019	Soltani et al. (2023)	Low	Some concerns	Some concerns	Low	Some concerns
B029	Hindy et al. (2020)	Low	Low	Low	Low	Low

Domain scoring rules (applied uniformly, not per-study judgement calls):

- **D1 (Participants/dataset):** *Low* if the study names a specific dataset; *High* if no dataset is named in the extracted text.
- **D2 (Predictors/architecture):** *Low* if the study’s architecture could be classified into a specific family (CNN, RNN/LSTM, Transformer, GNN, Autoencoder, Federated, Few-shot/Meta, Ensemble, Reinforcement, or Hybrid); *Some concerns* if the architecture could only be coded as “Unspecified/other DL”.
- **D3 (Outcome/metric reporting):** *Low* if an absolute accuracy or F1 value meeting the extraction rule could be confirmed (Section 4.2 of the main manuscript); *Some concerns* if no such value could be confirmed (the study may still report other metrics, e.g., AUC, latency, or only relative improvement).
- **D4 (Analysis/venue verification):** *Low* for all 37 audited primary-corpus studies by construction, since only DOI-verified peer-reviewed sources that also passed the post-hoc eligibility audit are retained in this corpus (Section 3.4 of the main manuscript).
- **Overall:** *Low* if all four domains are Low; *High* if any domain is High; *Some concerns* otherwise.

This is a transparent, rule-based coding applied uniformly by the extraction script rather than an independent expert consensus judgement per study, and it screens for *reporting completeness* rather than genuine methodological safeguards against bias (e.g., it does not verify absence of test-set leakage or independence between training and proxy-evaluation splits – see Section 3.5 of the main manuscript). Across the 37 studies in the corrected final audited primary corpus, the per-domain distribution is: D1, 33 low / 4 high; D2, 24 low / 13 some concerns; D3, 15 low / 22 some concerns; D4, 37 low. Combining domains, the overall screen is low for 10 studies, some concerns for 23 studies, and high for 4 studies; an unreported dataset (D1) is the sole driver of every high overall rating.

Table S4: Venue-stage background/emerging evidence: 41 records retained outside the primary synthesis corpus (32 journal or proceedings records and 9 preprint/repository records). Publisher, issuing-organization, or repository names were identified from DOI metadata, ISSN records, repository records, or official journal/publisher pages. Publisher identification is bibliographic only and does not establish peer-review, domain, proxy-protocol, or empirical eligibility.

ID	Reference	Publisher, issuer, or repository (identified)	Year	Dataset(s)	Key findings (as reported)
B001	Singh (2024)	Auricle Global Society of Education and Research	2024	The dataset utilized in this study is the CICIDS2018 dataset, which includes diverse modern attack...	A deep learning framework for anomaly detection using the CICIDS2018 dataset was developed, exhibiting high accuracy levels. - The hybrid CNN-LSTM...
B002	Archana et al. (2026)	Engineering Research Hub	2026	The paper does not mention a dataset.	An artificial intelligence-driven framework is proposed to identify, anticipate, and mitigate emerging zero-day threats. - The framework utilizes...
B003	Peppes et al. (2025)	Preprints.org	2025	The dataset includes synthetic data generated from malware images and tabular zero-day attack...	The paper presents a novel unified threat detection pipeline that integrates advanced machine learning and deep learning techniques, combining...
B004	Wei (2025)	Computer Science Bulletin	2025	The dataset comprises 12,847 binary samples from real-world applications. - The data collected is...	An adaptive multi-scale feature extraction framework for detecting zero-day vulnerabilities in binary code is proposed, integrating deep learning...
B005	Wahed (2025)	Editorial Salud, Ciencia y Tecnologia	2025	The dataset used in the study is not mentioned.	AI-enhanced threat intelligence significantly improves the detection of zero-day attacks compared to traditional methods. - The framework reduces...
B006	Ramavath et al. (2025)	TechRxiv	2025	Dataset is not mentioned	The novel multi-modal deep learning framework significantly improves the detection of advanced persistent threats. - Traditional signature-based...
B007	Anwer et al. (2026)	Tech Science Press	2026	The study utilizes three publicly available datasets: kit-sune, Bot-IoT, and UNSW-NB15, achieving...	A Federated Learning (FL) framework is proposed to enhance cyber threat detection in IoT networks, addressing limitations in traditional Machine...
B008	J (2024)	ESRGroups	2024	The paper does not mention a dataset.	A data-driven framework employing predictive analytics and machine learning techniques enhances threat detection and incident response in cloud...
B009	Laila et al. (2026)	Growing Science	2026	Experimental evaluation using diverse attack datasets demonstrates superior performance. - Specific...	A novel deep learning-driven, multilayer intrusion detection and prevention framework is proposed, integrating network-based IDS/IPS, host-based...
B010	Nebhnani and Agrawal (2025)	Academic Science Publications and Distributions	2025	The dataset used in the study is the KDD99 benchmark dataset, which is evaluated to assess the...	ProEn-XAI achieves a remarkable accuracy of 99.78% on the KDD99 benchmark dataset. - The model reports macro and weighted F1-scores of 0.9971 and...
B011	Patil et al. (2025)	PUBETA Single Member P.C.	2025	The dataset used in the study consists of raw network traffic data, which is utilized to predict...	INCEPT is a modular, multi-pronged deep-learning framework designed to predict cyberattacks in detail from raw network traffic data, integrating five...
B012	Njoku et al. (2025)	Research and Scientific Innovation Society (RSIS International)	2025	The dataset used in the study consists of benign and malicious Flash samples, which are described...	A novel deep learning-based approach utilizing a hybrid CNN-LSTM model is proposed for effective detection of zero-day Flash malware. - The model...
B013	Akshaya and Vathi (2025)	AIRCC Publishing Corporation	2025	The empirical evaluation was performed on two publicly available benchmark datasets. - The datasets...	A hybrid deep learning framework using four models significantly improves the prediction and detection of Zero-Day Attacks (ZDAs). - The models...
B014	Jones and Omar (2024)	Universitas Komputer Indonesia	2024	The dataset comprises standard datasets used for evaluating the GEADD method in detecting zero-day...	The GPT-2 Enhanced Attack Detection and Defense (GEADD) method integrates the GPT-2 model with metaheuristic optimization techniques to enhance...

Continued on next page

Table S4 – continued from previous page

ID	Reference	Publisher, issuer, or repository (identified)	Year	Dataset(s)	Key findings (as reported)
B015	Sheluhin et al. (2025)	Society for Radioelectronics Engineering	2025	The paper does not provide specific details about a dataset used in the study. - Information about...	Zero-day attacks exploit unknown vulnerabilities, posing significant challenges for traditional machine learning methods that rely on labeled...
B016	Roopak et al. (2024)	Authorea	2024	The dataset used in the study is the CIC-DDoS2019 datasets. - The dataset includes data related to...	An unsupervised Intrusion Detection System (IDS) for detecting zero-day DDoS attacks in IoT networks is proposed, which operates without prior...
B017	Sarhan et al. (2023)	Research Square	2022	The study utilizes two NIDS data sets: UNSW-NB15 and NF-UNSW-NB15-v2, which are synthetic and...	A novel zero-shot learning (ZSL) methodology has been proposed to evaluate the performance of machine learning-based network intrusion detection...
B018	R et al. (2026)	Engineering Research Hub	2026	The dataset used in the study is the NSL-KDD dataset, which is specifically utilized for evaluating...	A Dual-Phase Learning Approach is proposed for effective intrusion detection, focusing on zero-day attack identification using the NSL-KDD dataset ...
B020	Bagiro et al. (2025)	IJCESN / Iskender Akkurt	2025	The dataset used in the study is a benchmark dataset pertaining to cybersecurity . - Specific...	Deep learning techniques significantly improve the accuracy of threat detection and enhance the automation of threat response in cybersecurity - AI...
B021	Schneider et al. (2025)	PT Antis International Publisher	2025	The dataset evaluated includes benchmark datasets and real-world deployment scenarios, although...	An AI-powered cybersecurity threat detection system was designed that utilizes deep learning and behavioral analysis for identifying and mitigating...
B022	V (2026)	PSG CARE, PSG College of Technology	2026	The dataset used in the study is a publicly available network traffic dataset of the logistics...	A deep learning-based approach utilizing a hybrid Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) network is...
B023	Kunduru (2024)	Unicorn Publications	2024	The dataset used in the study comprises network traffic and system logs collected in real time from...	A hybrid model combining Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks achieves a 98.7% detection rate for cyber...
B024	Xu et al. (2025)	arXiv	2025	The dataset used in the study consists of publicly available benchmark datasets related to...	Deep learning techniques have significantly enhanced the generalizability of intrusion detection systems (IDS) by allowing them to learn underlying...
B025	Murali (2025)	International Journal for Research in Applied Science and Engineering Technology	2025	The dataset is not mentioned.	AI-driven Intrusion Detection Systems (IDS) enhance detection capabilities by learning complex patterns from network traffic . - The review discusses...
B026	Nayak (2026)	arXiv	2026	The dataset used in the study is the ToN IoT benchmark, which is evaluated chronologically. -...	ThreatFormer-IDS is proposed as a Transformer-based framework for robust intrusion detection in IoT and industrial networks, achieving AUC-ROC of...
B027	Lin (2025)	EWA Publishing (Eliwise Academy)	2025	The dataset used in the study is not reported.	Low disclosure rates and the strong destructive force of zero-day attacks threaten security and privacy . - A systematic study of AI-based...
B028	Gambo et al. (2026)	Scientific Research Publishing	2026	The dataset used in the study is not reported.	Local Area Networks (LANs) face vulnerabilities from various sophisticated cyber threats, highlighting the inadequacy of traditional defenses. - The...
B030	Bandarupalli (2024)	Research Square	2024	The CIC-IDS-2017 dataset includes CSV files containing network traffic data that captures various...	A Deep Neural Network (DNN) model is proposed for anomaly-based Intrusion Detection Systems (IDS) to effectively detect and classify various attack...
B031	Jamshidi et al. (2026)	arXiv	2026	The dataset comprises feature representations derived from various attack categories, with the...	A semantics-driven federated IDS framework is introduced, utilizing language-derived semantic supervision to enable open-set and zero-shot intrusion...

Continued on next page

Table S4 – continued from previous page

ID	Reference	Publisher, issuer, or repository (identified)	Year	Dataset(s)	Key findings (as reported)
B032	Oluwadare and Elsayed (2023)	FLAIRS / University of Florida Libraries	2023	The dataset is not mentioned.	Machine Learning based Intrusion Detection Systems (IDS) are challenged by the evolving nature of network attacks, particularly Zero-day attacks,...
B033	Jotangiyai et al. (2025)	International Journal of Scientific Research in Engineering and Management	2025	The study used the CSE-CIC-IDS2018 Dataset for implementation and evaluation . - This dataset...	Machine learning techniques, specifically random forest, demonstrate superior performance in detecting and blocking zero-day cyber-attacks compared...
B034	Nandiraju et al. (2025)	SCIENCEDOMAIN International	2025	The dataset used in the study is the UNSW-NB15 dataset, which reflects real-world and comprehensive...	The study shows that a Convolutional Neural Network (CNN) model achieved the highest accuracy of 93.8% in detecting zero-day attacks in network...
B035	Osman (2025)	Academic Publications	2025	The dataset consists of threat intelligence data from three sources: CVE/NVD vulnerability...	An innovative ensemble machine learning system was developed for detecting zero-day attacks by integrating threat intelligence data from multiple...
B036	Kinekar (2026)	International Journal for Research in Applied Science and Engineering Technology	2026	The study utilizes the NSL-KDD dataset, which focuses on network intrusion detection and consists...	The proposed study integrates six classical machine learning models with a Quantum Machine Learning (QML) model for cyberattack prediction, achieving...
B037	Ibraheem and Toshio (2024)	Universitas Pendidikan Indonesia	2024	The dataset used in the study is the CSE-CIC-IDS2018 Dataset, which was utilized for the execution...	Random forest outperforms other machine learning algorithms in terms of detection rates and accuracy for zero-day cyber-attacks . - The ability of...
B038	Swathi et al. (2025)	Sky Research Publication and Journals	2025	The study utilizes the NSL-KDD and CICIDS2017 datasets for model evaluation. - Both datasets...	A deep neural network (DNN) architecture was designed to enhance intrusion detection in cloud environments, achieving high detection accuracy of...
B039	Khan and Riaz (2026)	IJ Publication (IJEDR)	2026	The dataset used in the study includes the CICDDoS2019 and InSDN datasets, focusing on network flow...	An adaptive ensemble learning framework combining Random Forest, Gradient Boosting, and eXtreme Gradient Boosting classifiers effectively detects...
B040	Jibunoh et al. (2026)	arXiv	2026	The paper does not mention any specific dataset used in the study.	Zero-day attacks primarily arise from the exploitation of undisclosed vulnerabilities rather than novel attack behaviors . - Memory-corruption...
B041	Ahmed and Dabag (2025)	Northern Technical University	2025	The dataset analyzed consists of 50 peer-reviewed literatures published between 2015 and 2025,...	Structured Query Language Injection (SQLi) poses significant threats to web applications, prompting the adoption of Machine Learning (ML) and Deep...
B042	Dr C Nagesh and Y Venkatalakshmi (2026)	Shivkrupa Publications	2026	The experimental evaluation utilized benchmark cybersecurity datasets, demonstrating improved...	The AI-Driven Zero Trust Intrusion Detection Framework (AZT-IDF) integrates federated learning and self-supervised learning, enabling adaptive and...
B043	Aljarrah et al. (2026)	International Academic Press	2026	The dataset used in the study includes large-scale datasets such as EMBER 2018, which contains 800K...	A novel cross-attention feature fusion architecture is proposed, integrated with explainable artificial intelligence (XAI) techniques for zero-day...

Table S4 verification note. Publisher, issuing-organization, and repository names were checked against DOI landing-page metadata, ISSN records, repository records, or official journal/publisher pages. This correction replaces the previous unresolved-publisher placeholder with an identified issuing organization where evidence was available. It is a bibliographic clarification, not an endorsement of the venue and not an automatic reclassification into the primary corpus. Any reclassification would require complete reapplication of the review’s peer-review, domain, proxy-protocol, and empirical-eligibility criteria and corresponding updates to the PRISMA counts and main manuscript.

Table S5: Background/emerging evidence excluded at the post-hoc eligibility audit: 22 records that passed corrected DOI-based venue verification but did not meet this review’s empirical primary-study inclusion criteria on re-examination. Each record is retained in the bibliography and, where applicable, cited as background or comparative literature.

Study ID	Citation	Exclusion category	Specific reason
S004	Deldar and Abadi (2023)	Literature review/survey	Not an empirical primary study: a taxonomic survey of DL techniques for zero-day malware detection and classification, ACM Computing Surveys.
S019	Zhang and Maple (2023)	Literature review/survey	Not an empirical primary study: a review of deep reinforcement learning-based intrusion detection in IoT systems.
S026	Papalkar and Alvi (2023)	Literature review/survey	Not an empirical primary study: a review of unknown-attack detection with deep learning techniques (edited book chapter).
S027	Lal and Ashok (2026)	Literature review/survey	Not an empirical primary study: a comprehensive survey of DL-based network intrusion detection methods, evolution, and research perspectives.
S029	Won et al. (2023)	Domain mismatch	Addresses synthetic zero-day <i>malware-image</i> generation via GAN (PlausMal-GAN) rather than network-traffic intrusion detection; outside this review’s network-intrusion-detection scope.
S037	Li and Zhao (2024)	Domain mismatch	Addresses IoT malware detection via fine-grained power <i>side-channel</i> analysis (hardware telemetry), not network-flow monitoring; outside this review’s network-intrusion-detection scope.
S038	Siam et al. (2026)	Literature review/survey	Not an empirical primary study: an exploratory review of AI-powered models for zero-day attack detection, Expert Systems.
S039	Nair and Mhavan (2023)	Literature review/survey	Not an empirical primary study: a survey of intrusion detection systems for combating zero-day vulnerabilities (already correctly cited as prior work in Table 1 of the main manuscript).
S040	Houda et al. (2024)	Domain mismatch	Addresses physical-layer <i>jamming-attack</i> mitigation in O-RAN wireless networks, a distinct wireless-security problem, not network intrusion detection.
S042	Tayyab et al. (2022)	Literature review/survey	Not an empirical primary study: a survey of recent trends in deep-learning-based malware detection, Journal of Cybersecurity and Privacy.
S043	Kritika (2024)	Literature review/survey	Not an empirical primary study: a literature review of phishing URL detection using deep learning techniques (topically adjacent, not network intrusion detection).
S047	B et al. (2025)	Literature review/survey	Not an empirical primary study: a comprehensive review of machine learning in cybersecurity.
S051	Mahida (2026)	Domain mismatch	Addresses financial- <i>fraud</i> detection using a DRL zero-trust framework, not network intrusion detection.
S053	Ali et al. (2022)	Comparative/benchmarking study	Comparative evaluation of existing AI-based techniques for zero-day attack detection across multiple prior studies; its headline accuracy figure could not be confidently attributed to a single, novel, primary-empirical DL system.
S054	Mote and Arabagatte (2025)	Literature review/survey	Not an empirical primary study: a survey of detection and mitigation strategies for zero-day attacks with case studies.
S057	Manjula and Saravanakumar (2025)	Literature review/survey	Not an empirical primary study: a survey of machine learning and deep learning approaches for zero-day attack detection in cloud security (already correctly cited as prior work in Table 1 of the main manuscript).
S034	Zahoor et al. (2022)	Domain mismatch	Empirical deep-learning ransomware detection using host-level API, registry, file, directory, string, and process behaviour rather than network traffic or network-flow intrusion detection; outside the review’s NIDS scope.
S035	Anwer et al. (2022)	Comparative/conceptual study	The supplied paper record discusses and compares soft-computing and federated-learning solutions but does not establish a qualifying implemented primary DL system with a dataset-based proxy protocol and quantitative results.

Continued on next page

Table S5 – continued from previous page

Study ID	Citation	Exclusion category	Specific reason
S041	Naithani et al. (2024)	No demonstrated empirical validation	The supplied paper record proposes an integrated cloud-DDoS framework and mentions deep learning and honey-pot data collection, but does not report a verified implementation, explicit proxy protocol, dataset experiment, or quantitative performance result.
S012	Okey et al. (2025)	Outside network-intrusion-detection domain	Full-text verification confirmed the task is zero-day <i>device</i> identification and fingerprinting in IoT settings, i.e. recognising previously unseen devices rather than unknown network attacks; outside the review's NIDS scope.
S014	Wahid et al. (2025)	Outside network-intrusion-detection domain	The STACK-ED architecture is an endpoint threat-detection stack evaluated on a combined host-oriented dataset; although empirically substantive, the target task is endpoint rather than network-traffic intrusion detection.
S032	Elijah et al. (2025)	Outside network-intrusion-detection domain	The framework detects zero-day browser exploits from behavioural monitoring and system logs rather than network-flow traffic; outside the review's NIDS scope.

Summary: 11 records are literature reviews/surveys; 8 are outside the network-intrusion-detection domain; 2 are comparative/conceptual records without a qualifying primary empirical DL evaluation; and 1 lacks demonstrated empirical validation in the supplied record. Combined with Table S4 (41 records retained as venue-stage background/emerging evidence), the full background/emerging-evidence set comprises 63 records, and the corrected audited primary synthesis corpus comprises 37 records (Tables S1–S3), summing to the original 100 topically screened studies (Figure 5 of the main manuscript).

References

- Ahmed, S. S. and Dabag, M. L. A. (2025). Machine learning and deep learning approaches for sql injection detection: A review. *Ntu Journal of Engineering and Technology*.
- Akshaya, S. and Vathi, P. (2025). Enhancing cyber defense against zero-day attacks using ensemble neural networks. *International Journal of Computer Networks and Communications*.
- Ali, S., Rehman, S. U., Imran, A., Adeem, G., Iqbal, Z., and Kim, K.-I. (2022). Comparative evaluation of ai-based techniques for zero-day attacks detection. *Electronics*, 11(23):3934.
- Aljarrah, N., Shehadeh, H. H., Obeidat, R. A., and Tawfik, M. (2026). Cross-attention feature fusion for interpretable zero-day malware detection. *Statistics, Optimization and Information Computing*.
- Al-Jamali, N. A. S., Zaroor, A. R., and Al-Raweshidy, H. S. (2025). An effective technique of zero-day attack detection in the internet of things network based on the conventional spike neural network learning method. *Iet Networks*.
- Anwer, M., Ahmed, G., Abdelhaq, M., Alsaqour, R., Hussain, S., and Akhunzada, A. (2026). Towards decentralized iot security: Optimized detection of zero-day multi-class cyber-attacks using deep federated learning. *Computers, Materials and Continua*.
- Anwer, M., Ahmed, G., Akhunzada, A., Hussain, S., and Khan, M. (2022). Comparative analysis of soft computing approaches of zero-day-attack detection. In *2022 International Conference on Emerging Trends in Smart Technologies (ICETST)*. IEEE.
- Archana, P., Kumaravel, S., and Devi, K. G. (2026). Artificial intelligence-based zero-day attack detection and proactive mitigation strategies: A literature review. *International Research Journal on Advanced Engineering Hub (Irjaeh)*.
- Arun, A., Nair, A. S., and Sreedevi, A. G. (2024). Zero day attack detection and simulation through deep learning techniques. In *2024 14th International Conference on Cloud Computing, Data Science and Engineering (Confluence)*. IEEE.
- B, S. C., G, P. K., K, A. B. M., Aswathy, A. A., and Gracia, C. D. (2025). Machine learning in cyber security: A comprehensive review. In *2025 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)*. IEEE.
- Babu, K. S., Meghana, G., Divya, D., Divya, G. K., Rao, C. M., Vandana, D., and Moturi, S. (2025). A custom deep learning framework for identifying security threats in digitally connected systems. In *Proceedings of the 2025 IEEE ICAICIT Conference*. IEEE.
- Bagiro, A., Azad, M., Karim, S. R. I., Chu, T. S., Khan, H., and Suha, S. H. (2025). The role of artificial intelligence in cybersecurity: A deep learning approach to securing digital infrastructure. *International Journal of Computational and Experimental Science and Engineering*.
- Bandarupalli, G. (2024). Efficient deep neural network for intrusion detection using cic-ids-2017 dataset. *Research Square*.
- Basim, I., Makhlof, A. M., and Fakhfakh, A. (2025). Advanced cloud security framework based on zero trust architecture and adaptive deep learning for next-generation systems. *Indonesian Journal of Electrical Engineering and Computer Science*.
- Chhetry, B., Matam, R., and Barbhuiya, F. A. (2025). A federated learning framework for zero-day intrusion detection in iot environments. In *Proceedings of the 2025 IEEE ICSIT Conference*. IEEE.
- Cristiano, G. M., D’Antonio, S., Giglio, J., and Mazzeo, G. (2025). Implementation and experimental evaluation of defense techniques against adversarial attacks. In *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE.
- Deldar, F. and Abadi, M. (2023). Deep learning for zero-day malware detection and classification: A survey. *ACM Computing Surveys*, 56(2):1–37.
- Dr C Nagesh, D. V. S. and Y Venkatalakshmi, C. B. (2026). Reinforcing zero-trust security with ai: Federated and self-supervised learning for adaptive intrusion detection. *International Journal of Advanced Research in Science Communication and Technology*.
- Elijah, T. D., Walee, N. A., and Shalan, A. M. (2025). Ai-based detection of zero-day exploits: A framework. In *Proceedings of the 2025 IEEE ICICIS Conference*. IEEE.
- Gambo, M., Riddle, K., Abiona, O., and Onime, C. (2026). Mitigating cybersecurity risks in lan environments using ai techniques. *Int’l J. of Communications, Network and System Sciences*.
- Hindy, H., Atkinson, R., Tachtatzis, C., Colin, J.-N., Bayne, E., and Bellekens, X. (2020). Utilising deep learning techniques for effective zero-day attack detection. *Electronics*, 9(10).

- Houda, Z. A. E., Moudoud, H., and Brik, B. (2024). Federated deep reinforcement learning for efficient jamming attack mitigation in o-ran. *Ieee Transactions on Vehicular Technology*.
- Hussain, S., Kalpana, V., Raghavendran, V., Gangatharan, N., Mouleswararao, B., and K, V. R. (2026). Machine learning-based zero-day attack detection using deep reinforcement learning. *Information Security Journal*.
- Ibraheem, I. O. and Tosho, A. U. (2024). Zero day attack vulnerabilities: mitigation using machine learning for performance evaluation. *Journal of Computers for Society*.
- J, R. V. (2024). Data-driven framework for cloud storage security optimization: Leveraging predictive analytics and machine learning to enhance threat detection and incident response. *Journal of Electrical Systems*.
- Jamshidi, S., Wahab, O. A., Khomh, F., and Nafi, K. W. (2026). Tri-llm cooperative federated zero-shot intrusion detection with semantic disagreement and trust-aware aggregation. *Arxiv (Cornell University)*.
- Jibunoh, N., Khanchi, S., and Makanju, A. (2026). Zero day attacks: Novel behaviour or novel vulnerability? arXiv preprint. Preprint; not peer reviewed.
- Jones, R. and Omar, M. (2024). Revolutionizing cybersecurity: The gpt-2 enhanced attack detection and defense (geadd) method for zero-day threats. *International Journal of Informatics, Information System and Computer Engineering*.
- Jotangiyai, V., Khara, B. S., Hareshkumar, R. H., Daruwala, Z. D., and Kanani, Y. D. (2025). Ai for zero-day threat prediction and mitigation. *International Journal of Scientific Research in Engineering and Management*.
- Kara, A. O., Kara, M., and Boyaci, A. (2025). A comparative analysis of machine learning and deep reinforcement learning approaches for adaptive intrusion detection. *Ieee Access*.
- Kaur, S. and Kalsi, J. S. (2025). Federated learning with blockchain for zero-day attack detection in cybersecurity. In *Proceedings of the 2025 IEEE SMART Conference*. IEEE.
- Khan, M. (2024). Safeguarding iot networks against ddos attacks using deep learning based zero trust network access. *Electronics Letters*.
- Khan, M. I. and Riaz, N. (2026). Adaptive ensemble learning framework for zero day ddos attack detection in software defined networks using multi dimensional feature correlation. *International Journal of Engineering Development and Research*.
- Kinekar, N. (2026). Quantum machine learning for cyberattack prediction. *International Journal for Research in Applied Science and Engineering Technology*.
- Kinger, S. and Rupa, D. (2025). Adaptive intrusion detection using prototypical networks and statistical outlier detection. In *Proceedings of the 2025 IEEE ICCUBE Conference*. IEEE.
- Kritika, E. (2024). A comprehensive literature review on phishing url detection using deep learning techniques. *Journal of Cyber Security Technology*.
- Kumar, S. S., Indumathi, K., Rakshitha, R., Bhatt, N., Anitha, C., and Balamuralitharan, S. (2025). Optimized cloud intrusion detection framework leveraging multi-classifier security algorithms. In *Proceedings of the 2025 IEEE ICTBIG Conference*. IEEE.
- Kunduru, G. R. (2024). Deep learning-enabled data security and intrusion detection in azure and aws cloud systems. *International Journal of Engineering Research and Science & Technology*.
- Laila, D. A., Obeidat, I. M., Amin, M., Alqutaish, A., Obeidat, M., and Aldhyani, T. H. H. (2026). Deep learning-driven multi-layer intrusion detection and prevention framework for resilient defense against adaptive evasion techniques in modern networks. *International Journal of Data and Network Science*.
- Lal, P. S. and Ashok, A. (2026). Deep learning-based network intrusion detection systems: A comprehensive survey of methods, evolution, and research perspectives. In *2026 7th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*. IEEE.
- Li, Z. and Zhao, D. (2024). Zerod-fender: A resource-aware iot malware detection engine via fine-grained side-channel analysis. *Acm Transactions on Design Automation of Electronic Systems*.
- Lin, X. (2025). A survey of ai-based zero-day attack detection methods. *Applied and Computational Engineering*.
- Mahida, A. (2026). An intellectual zero trust security framework using deep reinforcement learning for predictive threat mitigation in ai-based fraud detection systems. *Ieee Access*.
- Malathi, P., G, M., Shinde, P., Amudha, A., Sohal, J., and Gupta, T. (2025). Intelligent cybersecurity frameworks using deep learning for advanced threat prediction. In *Proceedings of the 2025 IEEE SISIMPACT Conference*. IEEE.
- Manjula, L. and Saravanakumar, E. (2025). Zero-day attack detection in cloud security: A survey of machine learning and deep learning approaches. In *2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pages 2055–2062. IEEE.

- Mansur, T. A. (2025). Zero-day guard: Self-supervised temporal correlation framework for zero-day threat detection in cloud platforms. In *Proceedings of the 2025 IEEE ICINVENTS Conference*. IEEE.
- Mchina, J. P., Mduma, N., and Sinde, R. S. (2026). Adaptive decision-level intrusion detection for known and zero-day attacks. *Network*.
- Mote, M. S. A. and Arabagatte, D. S. (2025). Survey on detection and mitigation strategies for zero-day attacks: An extensive analysis of current developments and case studies. In *First International Conference on Computer, Computation and Communication (IC3C-2025)*. River Publishers.
- Mpatziakas, A., Lalas, A., Drosou, A., Chatzidiamantis, N., and Tzovaras, D. (2025). An ai-driven unsupervised mechanism for zero-day attack detection and mitigation in b5g networks. In *2025 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*. IEEE.
- Murali, A. (2025). Ai-driven: Network intrusion detection systems. *International Journal for Research in Applied Science and Engineering Technology*.
- Naeem, M. R., Amin, R., Farhan, M., Alsubaei, F. S., Alsolami, E., and Zakaria, M. D. (2025). Cyber security enhancements with reinforcement learning: A zero-day vulnerability identification perspective. *Plos One*.
- Nagarjun, A. V. and Rajkumar, S. (2025). Quantum deep learning-enhanced ethereum blockchain for cloud security: intrusion detection, fraud prevention, and secure data migration. *Scientific Reports*.
- Nair, D. and Mhavan, N. (2023). Augmenting cybersecurity: a survey of intrusion detection systems in combating zero-day vulnerabilities. In *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy*, pages 129–153. Emerald Publishing Limited.
- Nair, S. G. and Rani, A. J. M. (2025). Zero day attack prediction using improved deep neural network. In *Proceedings of the 2025 IEEE RMKMATE Conference*. IEEE.
- Naithani, A., Singh, S. N., and Sharma, P. K. (2024). Zero-day vigilance: Proposing a machine learning framework for ddos detection in cloud computing. In *2024 International Conference on Artificial Intelligence and Emerging Technology (Global AI Summit)*. IEEE.
- Nandiraju, S. K. K., Chundru, S. K., Tyagadurgam, M. S. V., Gangineni, V. N., Pabbineedi, S., and Kakani, A. B. (2025). Enhancing cybersecurity: Zero-day attack detection in network traffic with deep learning model. *Asian Journal of Research in Computer Science*.
- Nayak, S. (2026). Threatformer-ids: Robust transformer intrusion detection with zero-day generalization and explainable attribution. *Arxiv (Cornell University)*.
- Nebhnani, N. and Agrawal, D. S. (2025). Proen-xai: A high-precision ids model for zero-day attack detection using hybrid deep learning and shap-line interpretability. *International Journal of Environmental Sciences(Ind)*.
- Nithyalakshmi, N. and Muthukumaravel, A. (2026). Ai-driven intrusion detection leveraging xgboost and autoencoder-based deep learning for cyber threat analysis. In *AI-Driven Sustainable and Secure Smart Infrastructure Systems*, pages 215–239. IGI Global.
- Njoku, D. O., Amalagu, C. S., Mbanefo, B. C., Odoemene, E. C., Adedero, C., and Jibiri, J. E. (2025). Deep learning for zero-day flash malware detection: Prospective and challenges. *International Journal of Research and Innovation in Applied Science*.
- Okey, O. D., Dadkhah, S., Rodríguez, D. Z., and Kleinschmidt, J. H. (2025). Zero-day device identification for iot security through optimized incremental learning and drift adaptation. In *Proceedings of the 2025 IEEE SIoT Conference*. IEEE.
- Oluwadare, S. and Elsayed, Z. (2023). A survey of unsupervised learning algorithms for zero-day attacks in intrusion detection systems. *The International Flairs Conference Proceedings*.
- Osman, A. A. (2025). Zero-day attack prediction using ensemble machine learning with threat intelligence data. *International Journal of Applied Mathematics*.
- Papalkar, R. R. and Alvi, A. S. (2023). Review of unknown attack detection with deep learning techniques. In *Artificial Intelligence, Blockchain, Computing and Security Volume 1*. CRC Press.
- Patil, G., Sapkal, A., and Ingale, V. S. (2025). Designing an improved cyberattack prediction model using context-aware behavioral modeling analysis. *Engineering, Technology and Applied Science Research*.
- Peppes, N., Daskalakis, E., Alexakis, T., and Adamopoulou, E. (2025). A multimodal framework for advanced cybersecurity threat detection using gan-driven data synthesis. *Preprints.Org*.
- Perumal, R., Karuppiyah, T., Panneerselvam, U., Annamalai, V., and Kaliyaperumal, P. (2024). Enhancing network security using unsupervised learning approach to combat zero-day attack. *Indonesian Journal of Electrical Engineering and Computer Science*.
- Prabu, K., A, V., Radhakrishnan, R., P, R., Thenmozhi, E., and Ramesh, S. P. (2024). Enhancing cloud security with ai-driven anomaly detection for zero-day threats. In *Proceedings of the 2024 IEEE ICAC2N Conference*. IEEE.

- Prajwalasimha, S. N., Pimpalkar, A., Shelke, N., Saini, D. K. J. B., Kumar, G. H., and Sindhu, A. (2025). Federated adversarial learning for scalable and robust zero-day cyber threat detection in iot networks. In *Proceedings of the 2025 IEEE ICICI Conference*. IEEE.
- R, R., M, S., T, N. S., and Archana, P. (2026). Dual-phase learning approach for zero-day intrusion detection using nsl-kdd. *International Research Journal on Advanced Engineering Hub (Irjaeh)*.
- Raja, M. C. and Mahri, M. M. B. A. (2025). Behavioral anomaly detection in big data streams: An attention-enhanced lstm approach for privacy-aware zero-day attack detection. In *Proceedings of the 2025 IEEE ICIDCA Conference*. IEEE.
- Ramavath, S. K., Mittal, A., and Gudur, V. (2025). Deep learning embeddings for zero-day cyber threat detection: A multi-modal framework for network flow and siem data analysis. TechRxiv preprint. Preprint; not peer reviewed.
- Ranpara, R., Hirpara, J., Doshi, M., and Shah, D. (2025). A novel bayesian-inspired framework for proactive detection and mitigation of zero-day attacks in distributed network architectures. *Iet Conference Proceedings*.
- Rodríguez, E., Valls, P., Otero, B., Costa, J. J., Verdú, J., Pajuelo, M. A., and Canal, R. (2022). Transfer-learning-based intrusion detection framework in iot networks. *Sensors*.
- Roopak, M., Parkinson, S., Tian, G. Y., Ran, Y., Khan, S., and Chandrasekaran, B. (2024). An unsupervised approach for the detection of zero-day ddos attacks in iot networks. Authorea preprint. Preprint; not peer reviewed.
- Roshan, K. and Zafar, A. (2021). An optimized auto-encoder based approach for detecting zero-day cyber-attacks in computer network. In *2021 5th International Conference on Information Systems and Computer Networks (ISCON)*, pages 1–6.
- Saheed, Y. K. and Chukwuere, J. E. (2025). Autonomous llm agent: A memory-augmented, edge-optimized shap explanations with zero-day attack resilience in iot/industrial iot networks. *Ieee Internet of Things Journal*.
- Sarhan, M., Layeghy, S., Gallagher, M., and Portmann, M. (2023). From zero-shot machine learning to zero-day attack detection. *International Journal of Information Security*, 22(4):947–959.
- Saurabh, K., Singh, U., Mishra, A., Vyas, R., and Vyas, O. (2024). Zero-shot based hybrid neural network system for enhancing zero-day attack detection. In *2024 IEEE 21st India Council International Conference (INDICON)*, pages 1–6. IEEE.
- Schneider, L., Fischer, H., and Becker, J. (2025). Design of ai-powered cybersecurity threat detection systems to protect business networks and digital infrastructure from emerging cyber risks. *International Journal of Business Law and Political Science*.
- Sheluhin, O., Rybakov, S., and Zvezhinsky, S. (2025). Detection of zero-day cyber attacks and zero-day malware using machine learning methods. *Radioengineering*.
- Siam, A. A., Faruqui, N., Azad, A., and Moni, M. A. (2026). Securing the unseen: A comprehensive exploration review of ai-powered models for zero-day attack detection. *Expert Systems*.
- Singh, G. (2024). Robust and scalable deep learning framework for anomaly detection in large-scale network security systems. *International Journal of Intelligent Systems and Applications in Engineering*.
- Soltani, M., Ousat, B., Jafari Siavoshani, M., and Jahangir, A. H. (2023). An adaptable deep learning-based intrusion detection system to zero-day attacks. *Journal of Information Security and Applications*, 76:103516.
- Sunkara, K. C., Mittal, T., Sripada, N. K., K, B. H., Tlajiya, F., and Thakur, V. S. (2025). Probabilistic deep learning algorithmic model for robust anomaly detection in decentralized networked cyber-physical systems. In *2025 3rd International Conference on Data Science and Information System (ICDSIS)*. IEEE.
- Swathi, B., Balaram, A., Kiran, A., and Thrimurthulu, V. (2025). Enhancing intrusion detection using deep neural networks in cloud environments. *International Journal for Multidisciplinary Research*.
- Tayyab, U.-E.-H., Khan, F. B., Durad, M. H., Khan, A., and Lee, Y. S. (2022). A survey of the recent trends in deep learning based malware detection. *Journal of Cybersecurity and Privacy*.
- Thatha, V. N., Reddy, B. V., Venkat, M. K., Reddy, P. P. K., Reddy, A. B., and Reddy, S. N. (2025). Machine learning and transfer learning approaches for handling known and zero day cyber attacks in intrusion detection system. In *Proceedings of the 2025 IEEE ICACRS Conference*. IEEE.
- Uttarkar, A. R. and Vanjale, S. (2025). A novel convolutional-sequential xgb neural model for zero-day attack detection in federated learning. In *Proceedings of the 2025 IEEE WorldS4 Conference*. IEEE.
- V, V. (2026). An attention-enhanced cnn–bilstm framework for zero-day exploit detection in network traffic. *International Journal of Research in Science and Technology*.
- Wahed, M. A. (2025). Ai-enhanced threat intelligence for proactive zero-day attack detection. *Gamification and Augmented Reality*.
- Wahid, A. R., Anggreani, D., Hayat, M. A. M., Rahman, A. A., and Faisal, M. (2025). Stacking architecture-endpoint detection: a hybrid multi layered architecture for endpoint threat detection. *International Journal of Advances in Applied Sciences*.

- Wang, J., Huang, N., Zhang, H., Liu, L., Fu, Q., Cao, K., Guo, X., and Jung, H. (2025). Self-learning model fusion for network anomaly detection: A hybrid cnn-lstm-transformer framework. *Plos One*.
- Wei, S. (2025). Adaptive multi-scale feature extraction for zero-day vulnerability detection in system binaries. *Computer Science Bulletin*.
- Won, D.-O., Jang, Y.-N., and Lee, S.-W. (2023). Plausmal-gan: Plausible malware training based on generative adversarial networks for analogous zero-day malware detection. *Ieee Transactions on Emerging Topics in Computing*.
- Xu, Z., Wu, Y., Wang, S., Gao, J., Qiu, T., Wang, Z., Wan, H., and Zhao, X. (2025). Deep learning-based intrusion detection systems: A survey. *Arriv (Cornell University)*.
- Zahoora, U., Khan, A., Rajarajan, M., Khan, S. H., Asam, M., and Jamal, T. (2022). Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive pareto ensemble classifier. *Scientific Reports*.
- Zhang, H. and Maple, C. (2023). Deep reinforcement learning-based intrusion detection in iot system: a review. *Iet Conference Proceedings*.
- Zhang, J., Liang, S., Ye, F., Hu, R. Q., and Qian, Y. (2023). Towards detection of zero-day botnet attack in iot networks using federated learning. In *2023 IEEE International Conference on Communications (ICC)*. IEEE.