Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 17 No. 1, March 2026 - www.cisdijournal.net

Systematic Literature Review of Intrusion Detection and Classification in Edge Computing: Types, Challenges, Solutions, Limitations and Research Directions

Ojeniyi, J.A. Kigbu, A.P. Ahmad, S. Isah, A. O., Noel, M. D. & Subairu, S. O.
Department of Cyber Security Science
Federal University of Technology
Minna, Niger State, Nigeria
E-mails: Ojeniyija@futminna.edu.ng, alaka.kigbu@gmail.com, ahmads@futminna.edu.ng, ao.isah@futminna.edu.ng moses.noel@futminna.edu.ng, sikiru.subairu@st.futminna.edu.ng

ABSTRACT

This study presents a systematic literature review of intrusion detection and classification method for edge computing environment. Following PRISMA guided procedure, appropriate studies were identified from 2019 to 2026 through structured search method across relevant digital libraries, followed by thorough inclusion and exclusion screening. This review covered intrusion detection system (IDS) types and deployment structure. It also examined machine learning and deep learning method, feature engineering method, dataset, performance measures, and implementation. The review shows that host-based and anomaly-based intrusion detection system (IDS) lead in edge deployment. They track behaviors in detail and use few computing resources. Lightweight machine learning model like decision trees, random forests, and ensemble classifier are widely adopted, while Deep learning model often run into problems from limited resources. The review draws on this result to highlight key research gaps. It suggests paths ahead that focus on lightweight and federated detection system, standard test dataset, and low resource adaptive learning. It serves as a full guide for researchers and practitioners. Aim to build strong, scalable, and smart intrusion detection systems for safe edge computing environment.

Keywords: Intrusion Detection System, Edge Computing Security, Cybersecurity, Anomaly Detection, Machine Learning, Deep Learning, Internet of Things

CISDI Journal Reference Format
Ojeniyi, J.A. Kigbu, A.P. Ahmad, S. Isah, A. O., Noel, M. D. & Subairu, S.O. (2026): Systematic Literature Review of Intrusion Detection and Classification in Edge Computing: Types, Challenges, Solutions, Limitations and Research Directions. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 17 No 1, Pp 41-54.
Available online at www.isteams.net/cisdijournal. dx.doi.org/10.22624/AIMS/CISDI/V17N1P3

1. BACKGROUND TO THE STUDY

The design of edge computing is key to developing a system that supports latency-sensitive applications by allowing computing and data processing to take place near the source of the data generation. This creates new vulnerabilities in security because of the number of attack vectors that can occur over the ranges involved(Song et al., 2025). Many different types of devices will be involved in edge computing; therefore, edge environments will require a comprehensive Intrusion Detection System (IDS) to provide an intrusion detection capability.

The development of IDS tools has evolved since their introduction to include such capabilities as signature-based detection to anomaly detection to hybrid detection. Machine Learning (ML) and Deep Learning (DL) technologies are increasingly being used to detect previously known threats and unknown threats(Satilmis et al., 2024). Intrusion Detection Systems (IDS) are critical component of cybersecurity today by continuously monitoring network activity and host activity and detecting any potentially harmful activities and/or unauthorized access to systems(Nie et al., 2022). Prior to the implementation of IDS tools, they were designed based on fixed and central locations of assets(Kaushik et al., 2025). Consequently, IDS tools that rely on these types of architectures have proven to be ineffective when dealing with cloud, IoT, and Edge computing's dynamic, distributed, and elastic infrastructures because there are multiple virtualized and heterogeneous resources across which traffic flows (Ogab et al., 2025).

The availability of Edge Computing services has introduced new security risks; they share resources among many users and can scale rapidly(Chowdhury et al., 2026). However, they provide limited visibility into their internal operations which, in turn, impedes on monitoring and delays the discovery of attacks; machine learning (ML) offers a viable solution(Almalawi et al., 2025). ML will provide the means for developing standalone intrusion detection systems (IDS) that can scale and adapt to edge environments (Mahanipour & Khamfroush, 2024). These would be required to learn the normal behaviour of users and to subsequently detect advanced persistent and novel threats(Al-Ghuwairi et al., 2023).

Recent studies are integrating ML and DL within distributed and hybrid formats, and proving to substantially increase detection rates for resource poor environments(Huma et al., 2025). The current review will compile the most relevant research to date on intrusion detection within an edge computing environment; it will consider the different types of IDS, the challenges and constraints faced, potential solutions to these issues, the limitations of existing IDS solutions, and the possible future direction of IDS in edge computing, all via an established strict systematic literature review(SLR) approach(Araujo & Vieira, 2025).

2. RELATED WORKS

According to Nasim, Pranav and Dutta (2025), their study on the changes in architecture needed for virtualization through cloud-based intrusion detection system, feature a systematic review of existing literature in the area of Intrusion Detection System (IDS) for cloud computing with some very key findings. The authors indicate that the traditional signature-based intrusion detection system would find it difficult to cope with the rapidly changing virtual environment and therefore, advocate the use of either anomaly detection based or hybrid anomaly detection/machine learning based approach to provide flexibility and scalability to the system(Nasim et al., 2025). This study therefore provide means for implementing and assessing the use of machine learning in IDS, as it creates a benchmark for use across multiple studies.

Araujo and Vieira (2025) conducted a survey of existing IDS that included significant advances in the use of machine learning and deep learning technologies for intrusion detection. They found that some of the most common machine learning-based classifier (Decision Trees, Random Forests, Support Vector Machine, and Neural Network) performed better than traditional rule-based system for accurately detecting intrusion.

However, the authors also noted one downside to using this model; to build deep learning model takes a significant amount of computing resources and can have relatively long training time, which limits their use in many types of low-resource environment. As a result, this has implication for developing lightweight intrusion detection algorithm which can be deployed at the edge of network(Araujo & Vieira, 2025).

The research reviewed by Babu and Bagubali (2025) considered an investigation into federated intrusion detection system (IDS) specifically within the context of the Internet of Medical Things (IoMT). This also encompassed distributed learning across edge devices without sharing raw data(Babu & Bagubali, 2025). By addressing scalability and privacy improvement through Federated Learning technique; however, they identified some of the additional considerations for using federated learning such as communication costs, differences between devices, and potential model poisoning(Hozouri et al., 2025). All of these considerations can provide clarity into the advantages and disadvantages of using federated learning in developing distributed intelligent system.

According to Rahamathulla & Ramaiah (2025), optimization processes today have advanced the performance of machine learning model (MLM) algorithm. The authors present an improved firefly algorithm to optimize hyperparameters of MLM classifier. The firefly algorithm also improves the performance of anomaly detection in highly resource-constrained environment such as Edge IoT network. The results of their experiments have demonstrated higher accuracy and faster convergence time compared to traditional metaheuristic algorithm. Such automatic tuning of hyperparameter makes using MLM technique on very limited resource Edge IoT node more practicable than it used to be (Rahamathulla & Ramaiah, 2025).

3. METHODOLOGY

This review uses a (PRISMA) based technique that ensure clear stages, transparency, and planned evidence summary. The stages include forming research question, and cover search strategy design, selection studies, extraction of data, and checking quality. PRISMA offers a checklist for vital items to account, and provides a flow diagram as well. To map out the review method: selection studies, search results, and screening. Figure 1 illustrate the outcome.

3.1 Search Strategy

The search followed standard SLR approach that searched key academic databases as followed: ScienceDirect, ACM Digital Library, IEEE, and SpringerLink. This generated appropriate IDS studies. Combination of the following keywords were used: “intrusion detection system,” “edge computing,” “machine learning,” “deep learning,” “anomaly detection,” and “hybrid IDS.” These terms covered basic and smart approaches.

3.1.1 Inclusion Criteria

The inclusion/exclusion criteria for fitting studies according to the following measures are:

1. The proposed or evaluated IDS must be for edge or virtualized environments.
2. The study must have used either ML, DL, or intelligent classification techniques.
3. The study must report some form of evaluation metrics and/or data sets for their IDS.
4. The study must be a peer reviewed journal or conference paper.

The above rules are consistent with the criteria for selecting studies identified in previous IDS SLR.

3.1.2 Exclusion Criteria

Excluded studies:

1. Studies without experimental proof are not included in the review.
2. Exclusion criteria include studies that do not relate to intrusion detection.
3. Also, non-academic papers as well as duplicates are removed.

These procedures ensure that the results will be appropriate; thus, the methodology will be reliable.

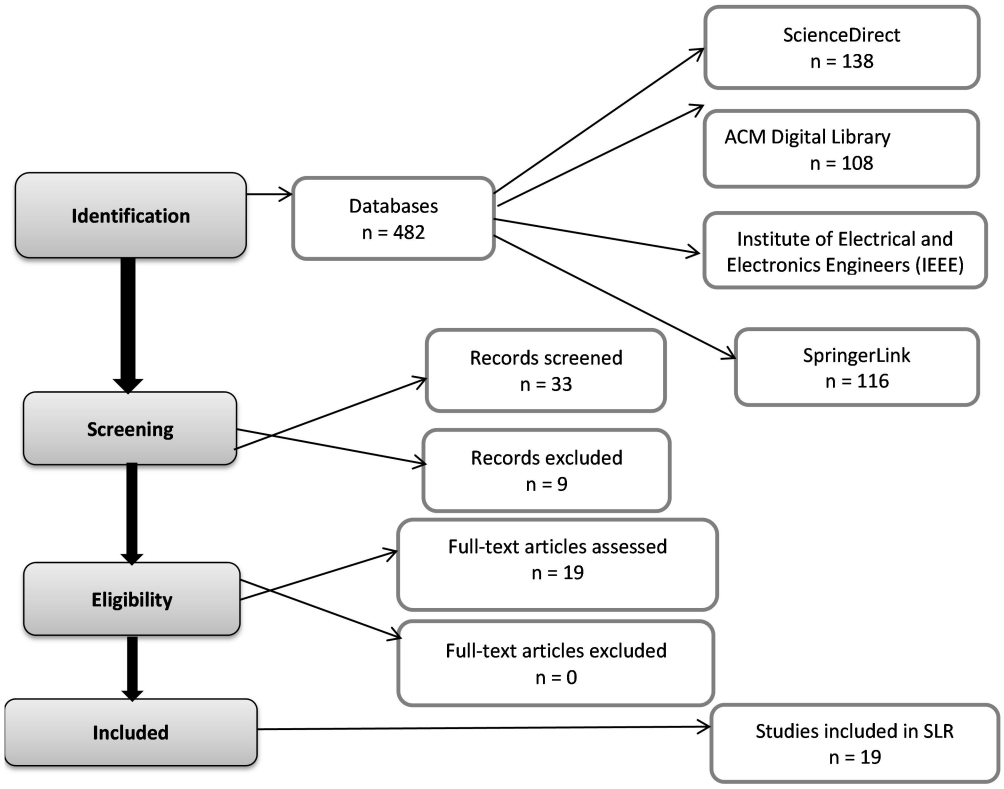

Fig 1: Outcome of the SLR Using PRISMA Flowchart

3.2 Research Question

This literature review established research questions (RQ) pertaining to the intrusion detection and classification methods for edge computing. It organized these questions based on limitations, design constraints, and future challenges evident in the selected studies. These gaps have resulted in the establishment of the following research questions from identified gaps and trends:

1. RQ: What types and designs of intrusion detection system (IDS) are currently being implemented in edge computing environment?
2. RQ: What type of classifying and/or spotting algorithm, whether machine learning or deep learning, provide the most effective means of identifying and classifying an intrusion within an edge computing environment?
3. RQ: What dataset and feature set have been utilized to test IDS at the edge, how did those dataset and feature set compare, and what impact did they have on the findings of this study?

4. RQ: What key issues have been identified that hinder the creation and continued development of strong IDS for use in edge computing?
5. RQ: What solutions provide to address resource and scale limitations in IDS at the edge?

3.3 Digital Libraries Selection

Several high-quality academic sources were chosen. They cover a wide range of subject and engineering field. Past IDS studies and cloud/edge security reviews often use these sources.

Table 3.1: Digital Libraries Used for the Literature Retrieval

DIGITAL LIBRARY	RATIONALE	COVERAGE TYPE	USAGE JUSTIFICATION	REF
SCIENCEDIRECT (ELSEVIER)	Major publisher of IDS/cloud/edge security research	Journals + conferences	Many selected IDS/cloud surveys originate here	(Nasim et al., 2025)
IEEE XPLORE	Networking, IoT, edge computing venues	Conferences + journals	Core source for IDS and distributed systems	(Dini et al., 2023)
SPRINGERLINK	Security + ML research	Journals/books	Hosts systematic reviews and IDS advances	(Memon, 2022)
ACM DIGITAL LIBRARY	Systems, containers, cloud-native security	Conferences	Relevant for edge/container IDS works	(Q. Deng et al., 2026)

Multiple sources cut sampling bias and boost reproducibility, and systematic Intrusion Detection system (IDS) review this principle(Rehman et al., 2025).

Table 3.2: Search Strings Used

ID	Boolean Search String
S1	("intrusion detection system" OR IDS OR "anomaly detection") AND ("edge computing" OR "fog computing" OR "distributed edge")
S2	("intrusion detection" OR IDS) AND ("cloud computing" OR IoT OR IIoT OR IoMT) AND ("machine learning" OR "deep learning")
S3	("host-based intrusion detection" OR HIDS OR "system call") AND (edge OR container OR microservice)
S4	("federated learning" OR distributed learning) AND ("intrusion detection" OR IDS)
S5	("ensemble" OR hybrid OR optimization OR metaheuristic) AND ("intrusion detection system") AND (edge OR IoT)
S6	("survey" OR "systematic literature review") AND ("intrusion detection") AND (cloud OR edge OR IoT)

Final Boolean search strings linked keywords from the three main parts. Truncation and wildcards came into play where each database allowed them.

These strings capture:
Architecture types (host/network/distributed), intelligent techniques (ML/DL/ensemble/FL), and deployment contexts (edge/cloud/IoT). This multi-string approach mirror strategies used in previous Intrusion Detection System (IDS) SLR method to maximize recall and coverage.

4. RESULTS AND DISCUSSION

4.1 Types of Intrusion Detection System (IDS) in Edge Computing

According to Thakkar & Lohiya (2023), intrusion detection system (IDS) in edge environment adopts different types of system(Thakkar & Lohiya, 2023).

For example:

1. Host-based Intrusion Detection System (IDS) based on an analysis of individual host and their system call.
2. Network-based Intrusion Detection System (IDS) monitor network traffic flow.
3. Distributed Intrusion Detection System (IDS) distributed over multiple nodes.
4. Hybrid Intrusion Detection System (IDS) employ both machine and deep learning.

Host-based intrusion detection system looking at system call tracing will work particularly well for edge services as they allow for close monitoring of the computer behavior (Pundir et al., 2020). Distributed Intrusion Detection System (IDS) design enhance scalability and therefore, are better suited to multi-tenant structure or node physically distributed from each other (Rahman et al., 2025).

4.2 Challenges in Edge Intrusion detection system (IDS)

Edge environment faces these key challenges(Makris et al., 2025):

1. Limited resources
2. Poor visibility.
3. Scalability needs.
4. Advanced adaptive attacks

Machine learning model act differently in various settings, demanding careful model selection and appropriate data representations(Grzesik & Mrozek, 2024).

4.3 Proposed Solutions

Researchers propose:

1. Lightweight machine learning classifier.
2. Graph method shape system call view
3. Sliding windows spot detection
4. Feature engineering pair with dimensionality reduction.
5. Hybrid model blend with ensemble learning

Graph-based encoding of system call keeps context link intact. This helps spot anomalies better. While sliding window post processing raises attack detection rate. It also lower false alarm(P. Deng & Huang, 2025).

4.4 Limitations

Even with improvement several limitations remain:

1. Model overfit to particular dataset.
2. Evaluation covers few machines learning model.
3. Deep model demand high computing power.
4. Generalization struggle across varied node.

Additionally, lack of standard dataset and evaluation metrics makes fair comparison difficult(Cao et al., 2024).

4.5 Research Directions

Future work should focus on:

1. Lightweight and machine learning for devices with limited resources.
2. Federated and distributed learning on edge node.
3. Reliable system call or graph models
4. Hybrid and multimodal detection method.
5. Uniform benchmark and reproducible result

These guidelines seek adaptive, scalable, and reliable intrusion detection system (IDS) for next-generation edge computing settings(Bhupesh et al., 2019).

4.6 Comparative Analysis Table

Tabel 4.1: IDS Approaches vs Edge and Cloud Deployment Features

STUDY / CONTEXT	DEPLOYMENT LEVEL	TECHNIQUE	FEATURE TYPE	CLASSIFIER / MODEL	KEY STRENGTHS	KEY LIMITATIONS	REF
CONTAINERIZED SERVICES IDS	Edge / containers	Host-based monitoring	System calls	DT, RF, Isolation Forest	Lightweight, low overhead, suitable for edge nodes	Model sensitivity to workload variation	(Araujo & Vieira, 2025)
GRAPH-BASED HIDS	Edge / host	System-call graphs + sliding window	Graph sequences	ML classifiers	High detection rate, reduced false alarms	Complexity of graph construction	(P. Deng & Huang, 2025)
ENSEMBLE IDS	Edge-IoT	Hybrid learning	Engineered features	E-Tree + DNN + RF	Improved accuracy via ensemble diversity	Increased training complexity	(Nasim et al., 2025)

FEDERATED IDS SURVEYED	Distributed edge / IoMT	Federated learning	Distributed local features	FL-based models	Privacy-preserving collaborative detection	Poisoning and heterogeneity issues	(Hassan et al., 2025)
STUDY / CONTEXT	DEPLOYMENT LEVEL	TECHNIQUE	FEATURE TYPE	CLASSIFIER / MODEL	KEY STRENGTHS	KEY LIMITATIONS	REF
CLOUD-IOT IDS	Cloud-assisted edge	Multi-feature extraction	Statistical + traffic features	MFE-ELM	Fast training, low weights for cloud nodes	Dataset dependency	(Lin et al., 2023)
IOT IDS	Edge IIoT	Hyperparameter optimization	Network features	ML + Enhanced Firefly Algorithm tuning	Higher accuracy with reduced overhead	Metaheuristic tuning cost	(Bakır & Ceviz, 2024)
IDS SURVEY	Cloud/Edge/IoT	Multiple ML/DL	Mixed	LR, SVM, RF, DL	Comprehensive taxonomy and benchmarks	Lack of standardization	(Naghib et al., 2025)

Tabel 4.2: Comparing Dataset from Different Studies

STUDY	DATASET(S) USED	DATASET TYPE	PURPOSE	NOTES	REF
CLOUD IOT IDS	Classical intrusion detection benchmark dataset	Network traffic	Training/testing	Used for preprocessing, feature engineering, model validation	(Lin et al., 2023)
IOT IDS (FIREFLY OPTIMIZED)	Edge-IIoT dataset	Industrial IoT traffic	Multi-class attack detection	Class imbalance handled using SMOTE	(Rahamathulla & Ramaiah, 2025)
CONTAINER/EDGE IDS	System-call traces	Host behavior	Anomaly detection	Suitable for microservices/containers	(Araujo & Vieira, 2025)
GRAPH HIDS	System calls sequence logs	Host	Graph-based anomaly modeling	Sliding window improves accuracy	(P. Deng & Huang, 2025)
IOMT IDS SURVEY	Multiple IoMT security datasets (reviewed)	Medical/healthcare traffic	Comparative evaluation	Highlights dataset gaps and need for standardization	(Hassan et al., 2025)
CLOUD/EDGE IDS SLR	Various public IDS datasets	Mixed	Taxonomy & evaluation	Notes heterogeneity and lack of unified benchmarks	(Naghib et al., 2025)

Tabel 4.3: Method Effectiveness Summary

CATEGORY	COMMON ALGORITHMS	EDGE SUITABILITY	EVIDENCE
SIGNATURE-BASED	Rules/pattern matching	Low (poor zero-day detection)	(Nasim et al., 2025)
ANOMALY-BASED	RF, DT, SVM, IF	High (lightweight)	(Araujo & Vieira, 2025)
DEEP LEARNING	DNN/LSTM	Moderate–Low (resource heavy)	(Hassan et al., 2025)
ENSEMBLE	Hybrid stacking	High accuracy	(Jacob & Sultana Habibullah, 2024)
FEDERATED LEARNING	Distributed training	High privacy + scalability	(Fenanir & Semchedine, 2023)
OPTIMIZATION/METAHEURISTIC	Firefly tuning	Improves performance	(Rahamathulla & Ramaiah, 2025)

Tabel 4.4: Studies Summary Table

AUTHOR	YEAR	METHOD	DATASET / FEATURES	KEY FINDINGS	REF
RAHAMATHULLA & RAMAIAH	2025	Enhanced Firefly Algorithm (metaheuristic tuning for ML IDS)	Edge-IIoT dataset + SMOTE	Hyperparameter optimization improves convergence, accuracy, and efficiency for edge IIoT	(Rahamathulla & Ramaiah, 2025)
ARAUJO & VIEIRA	2025	Host-based IDS with system-call features + DT/RF/Isolation Forest	System-call traces	Lightweight detection with low runtime overhead suitable for containers/edge	(Araujo & Vieira, 2025)
DENG & HUANG	2025	Graph-based system-call modeling + sliding window ML	System-call graphs	Context-preserving representation improves detection and reduces false alarms	P Deng & Huang (2025)
MAHADIK S, PAWAR P, & MUTHALAGU R	2024	Ensemble (Enhanced Tree + DNN + RF)	IoT-edge traffic features	Ensemble diversity increases robustness and classification performance	(Mahadik et al., 2024)
SPADACCINO P & FRANCECA CUOMO	2022	Multi-Feature Extraction + Extreme Learning Machine (MFE-ELM)	Network intrusion dataset	Fast training and lightweight inference for distributed/cloud-edge nodes	(P. Spadaccino & Francesca Cuomo, 2022)
NADELLA G	2024	Federated Learning IDS taxonomy	Multiple IoMT datasets	Collaborative privacy-preserving learning; challenges include poisoning and heterogeneity	(Nadella, 2024)

AUTHOR	YEAR	METHOD	DATASET / FEATURES	KEY FINDINGS	REF
GHUWAIRI, SHARRAB & ALGAMI	2023	Taxonomy of cloud IDS techniques	Multiple IDS benchmarks	Classified host/network/distributed IDS; ML required for scalability	(Al-Ghuwairi et al., 2023)
SPADACCINO	2024	ML/DL taxonomy (LR, SVM, RF, DL, hybrid)	Various public datasets	ML/DL outperform signatures but incur computational overhead	(P. C. F. Spadaccino, 2024)
WEN F, OHNO H, & SAMPALLI S	2024	Systematic review of IoMT IDS	Healthcare/medical traffic datasets	Dataset gaps and need for standardization/explainability identified	(Wen et al., 2024)
ALBIN J, &ADAM N	2023	Behavioral anomaly detection	Runtime/service logs	Limited visibility necessitates host-level monitoring at edge	(Albin & Adam, 2023)
ELSEDIMY, ELHADIDY & ABOHASHINE	2024	Hybrid signature + anomaly IDS	Mixed host/network features	Reduced false positives and improved generalization	(Elsedimy et al., 2024)
ALGAMI A, ACARER T, & AHMAD Z	2024	ML-based IDS integrated with edge security framework	Edge traffic features	Combines detection and isolation of intruders near data source	(Algarni et al., 2024)
KONG L, TAN J, & DAS S	2023	Survey of edge-driven IoT security designs	Multiple IoT-edge case studies	Highlights distributed attack surfaces and need for edge IDS	(Kong et al., 2023)
ZHIMIN & JUN	2024	ML-based IDS for next-gen networks	Wireless traffic traces	Demonstrates need for scalable detection in high-throughput networks	(Zhimin & Jun, 2024)
(ALI S, LI Q, & YOUSAFZAI	2024	Multi-teacher knowledge distillation	Network intrusion dataset	Lightweight student models retain high accuracy with lower cost	(Ali et al., 2024)
TEKIN N, ACAR A & GUNGOR V	2023	Soft computing + ML optimization	IoT traffic dataset	Improved detection accuracy via heuristic optimization	(Tekin et al., 2023)
WEN F, OHNO H, & SAMPALLI S	2024	Systematic review of HIDS	Multiple host logs/system calls	Confirms HIDS effectiveness for behavioral anomaly detection	(Wen et al., 2024)
(IOT JAVEED D, SAEED M, & TAHIR M	2023	ML/DL IDS for IoT networks	Various IoT datasets	Discusses trade-off between accuracy and energy/resource usage	(Javeed et al., 2023)
ALBIN J, & ADAM N	2023	Edge-computing-driven IoT architecture + security	Distributed IoT testbeds	Edge reduces latency but requires local security mechanisms	(Albin & Adam, 2023)

5. CONCLUSION

In this systematic literature review, we present the state of the art of intrusion detection and classification for computing environment. Findings shows that conventional intrusion detection system (IDS) do not scale to distributed and dynamic environment. This has led to the need for machine learning (ML) and deep learning (DL) based, distributed detection, and hybrid solution. Host based monitoring of system calls, lightweight classifier, and graph-based representation are promising. These enable effective detection despite limited resources. Challenges in scaling, system variety, data quality, and model generalization remain. Future work is required. Progress in clear explanation, distributed processing, and adaptive learning will define the next edge intrusion detection system (IDS) solution. These will offer robust protection in real time security.

REFERENCES

Albin, J., & Adam, N. (2023). *Bachelor Degree Project Edge Computing Security for IoT-A Systematic Literature Review*.

Algarni, A., Acarer, T., & Ahmad, Z. (2024). An Edge Computing-Based Preventive Framework With Machine Learning- Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications. *IEEE Access*, *12*, 53646–53663. https://doi.org/10.1109/ACCESS.2024.3387529

Al-Ghuwairi, A. R., Sharrab, Y., Al-Fraihat, D., AlElaimat, M., Alsarhan, A., & Algarni, A. (2023). Intrusion detection in cloud computing based on time series anomalies utilizing machine learning. *Journal of Cloud Computing*, *12*(1). https://doi.org/10.1186/s13677-023-00491-x

Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: a survey. In *Ad Hoc Networks* (Vol. 152). Elsevier B.V. https://doi.org/10.1016/j.adhoc.2023.103320

Almalawi, A., Hassan, S., Fahad, A., & Khan, A. I. (2025). Edge computing optimization: an enhanced algorithm for efficient caching and latency reduction. *Egyptian Informatics Journal*, *31*. https://doi.org/10.1016/j.eij.2025.100781

Araujo, I., & Vieira, M. (2025). Enhancing intrusion detection in containerized services: Assessing machine learning models and an advanced representation for system call data. *Computers and Security*, *154*. https://doi.org/10.1016/j.cose.2025.104438

Babu, A., & Bagubali, A. (2025). Federated Learning With Sailfish-Optimized Ensemble Models for Anomaly Detection in IoT Edge Computing Environment. *IEEE Access*, *13*, 53171–53187. https://doi.org/10.1109/ACCESS.2025.3554301

Bakır, H., & Ceviz, Ö. (2024). Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithm-based Hyperparameter Tuning and Hybrid Feature Selection. *Arabian Journal for Science and Engineering*, *49*(9), 13025–13043. https://doi.org/10.1007/s13369-024-08949-z

Bhupesh, P., Abha, T., & Rishabh, S. (2019). *2019 - EDGE COMPUTING EVOLUTION CHALLENGES AND FUTURE DIRECTIONS*.

Cao, L., Huo, T., Li, S., Zhang, X., Chen, Y., Lin, G., Wu, F., Ling, Y., Zhou, Y., & Xie, Q. (2024). Cost optimization in edge computing: a survey. *Artificial Intelligence Review*, *57*(11). https://doi.org/10.1007/s10462-024-10947-4

Chowdhury, A. P., Nur, F. N., Islam, A. H. M. S., Alam, K., Karim, A., & Shah, M. A. (2026). FLEX-IDS: A secure and explainable federated intrusion detection framework for Edge-of-Things

environments under adversarial conditions. *Computers and Electrical Engineering*, *129*. https://doi.org/10.1016/j.compeleceng.2025.110827

Deng, P., & Huang, Y. (2025). Edge-featured multi-hop attention graph neural network for intrusion detection system. *Computers and Security*, *148*. https://doi.org/10.1016/j.cose.2024.104132

Deng, Q., Goudarzi, M., Shaghaghi, A., Sarvi, M., & Buyya, R. (2026). A secure framework for containerized IoT applications in integrated edge–cloud computing environments. *Future Generation Computer Systems*, *174*. https://doi.org/10.1016/j.future.2025.108010

Dini, P., Elhanashi, A., Begni, A., Saponara, S., Zheng, Q., & Gasmi, K. (2023). Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity. In *Applied Sciences (Switzerland)* (Vol. 13, Number 13). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/app13137507

Elsedimy, E. I., Elhadidy, H., & Abohashish, S. M. M. (2024). A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. *Cluster Computing*, *27*(7), 9917–9935. https://doi.org/10.1007/s10586-024-04458-8

Fenanir, S., & Semchedine, F. (2023). Smart Intrusion Detection in IoT Edge Computing Using Federated Learning. *Revue d'Intelligence Artificielle*, *37*(5), 1133–1145. https://doi.org/10.18280/ria.370505

Grzesik, P., & Mrozek, D. (2024). Combining Machine Learning and Edge Computing: Opportunities, Challenges, Platforms, Frameworks, and Use Cases. In *Electronics (Switzerland)* (Vol. 13, Number 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13030640

Hassan, S. R., Tanveer, M. U., Prajapat, S., & Shabaz, M. (2025). A comprehensive survey on intrusion detection in internet of medical things: Datasets, federated learning, blockchain, and future research directions. *ICT Express*, *11*(6), 1291–1310. https://doi.org/10.1016/j.icte.2025.11.005

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges. *Discover Artificial Intelligence*, *5*(1). https://doi.org/10.1007/s44163-025-00578-1

Huma, Z. e, Jan, S. U., Ahmad, J., Buchanan, W., & Pitropakis, N. (2025). Adversarial Machine Learning in IoT Security: A Comprehensive Survey. *ACM Computing Surveys*. https://doi.org/10.1145/3785665

Jacob, S. L., & Sultana Habibullah, P. (2024). A Systematic Analysis and Review on Intrusion Detection Systems Using Machine Learning and Deep Learning Algorithms. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewjcce42023249

Javeed, D., Saeed, M. S., Ahmad, I., Kumar, P., Jolfaei, A., & Tahir, M. (2023). An Intelligent Intrusion Detection System for Smart Consumer Electronics Network. *IEEE Transactions on Consumer Electronics*, *69*(4), 906–913. https://doi.org/10.1109/TCE.2023.3277856

Kaushik, S., Bhardwaj, A., Almogren, A., Bharany, S., Altameem, A., Rehman, A. U., Hussen, S., & Hamam, H. (2025). Robust machine learning based Intrusion detection system using simple statistical techniques in feature selection. *Scientific Reports*, *15*(1), 3970. https://doi.org/10.1038/s41598-025-88286-9

Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., Zeng, P., Khan, M., & Das, S. K. (2023). Edge-computing-driven Internet of Things: A Survey. *ACM Computing Surveys*, *55*(8). https://doi.org/10.1145/3555308

Lin, H., Xue, Q., Feng, J., & Bai, D. (2023). Internet of things intrusion detection model and algorithm based on cloud computing and multi-feature extraction extreme learning machine. *Digital*

Communications and Networks, 9(1), 111–124. https://doi.org/10.1016/j.dcan.2022.09.021

Mahadik, S. S., Pawar, P. M., & Muthalagu, R. (2024). Edge-Federated Learning-Based Intelligent Intrusion Detection System for Heterogeneous Internet of Things. *IEEE Access*, *12*, 81736–81757. https://doi.org/10.1109/ACCESS.2024.3410046

Mahanipour, A., & Khamfroush, H. (2024). *Enhancing IoT Security: A Novel Feature Engineering Approach for ML-Based Intrusion Detection Systems*. http://arxiv.org/abs/2404.19114

Makris, I., Karampasi, A., Radoglou-Grammatikis, P., Episkopos, N., Iturbe, E., Rios, E., Piperigkos, N., Lalos, A., Xenakis, C., Lagkas, T., Argyriou, V., & Sarigiannidis, P. (2025). A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions. In *Computer Science Review* (Vol. 56). Elsevier Ireland Ltd. https://doi.org/10.1016/j.cosrev.2024.100717

Memon, S. (2022). Host-based intrusion detection system using Support Vector Machine. *Quaid-e-Awam University Research Journal of Engineering, Science & Technology*, *20*(1), 44–54. https://doi.org/10.52584/qrj.2001.07

Nadella, G. S. (2024). Advancing Edge Computing with Federated Deep Learning: Strategies and Challenges. *International Journal for Research in Applied Science and Engineering Technology*, *12*(4), 3422–3434. https://doi.org/10.22214/ijraset.2024.60602

Naghib, A., Gharehchopogh, F. S., & Zamanifar, A. (2025). A comprehensive and systematic literature review on intrusion detection systems in the internet of medical things: current status, challenges, and opportunities. *Artificial Intelligence Review*, *58*(4). https://doi.org/10.1007/s10462-024-11101-w

Nasim, S. S., Pranav, P., & Dutta, S. (2025). A systematic literature review on intrusion detection techniques in cloud computing. In *Discover Computing* (Vol. 28, Number 1). Springer Science and Business Media B.V. https://doi.org/10.1007/s10791-025-09641-y

Nie, L., Wu, Y., Wang, X., Guo, L., Wang, G., Gao, X., & Li, S. (2022). Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach. *IEEE Transactions on Computational Social Systems*, *9*(1), 134–145. https://doi.org/10.1109/TCSS.2021.3063538

Ogab, M., Zaidi, S., Bourouis, A., & Calafate, C. T. (2025). Intrusion Detection Systems for the Internet of Drones Security Using Multi-Teacher Knowledge Distillation. *IEEE Access*, *13*, 210134–210152. https://doi.org/10.1109/ACCESS.2025.3642632

Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J. P. C., & Park, Y. (2020). Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges. In *IEEE Access* (Vol. 8, pp. 3343–3363). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2019.2962829

Rahamathulla, M. Y., & Ramaiah, M. (2025). Optimizing anomaly detection models for edge IIoT with an enhanced firefly algorithm-based hyperparameter tuning strategy. *Results in Engineering*, *27*. https://doi.org/10.1016/j.rineng.2025.105843

Rahman, M. M., Shakil, S. Al, & Mustakim, M. R. (2025). A survey on intrusion detection system in IoT networks. In *Cyber Security and Applications* (Vol. 3). KeAi Communications Co. https://doi.org/10.1016/j.csa.2024.100082

Rehman, H. M. R. U., Liaquat, S., Gul, M. J., Jhandir, M. Z., Gavilanes, D., Vergara, M. M., & Ashraf, I. (2025). A systematic literature study of machine learning techniques based intrusion detection: datasets, models, challenges, and future directions. *Journal of Big Data*, *12*(1). https://doi.org/10.1186/s40537-025-01323-2

Satilmis, H., Akleylek, S., & Tok, Z. Y. (2024). A Systematic Literature Review on Host-Based Intrusion Detection Systems. *IEEE Access*, *12*, 27237–27266. https://doi.org/10.1109/ACCESS.2024.3367004

Song, W., Zhu, X., Ren, S., Tan, W., & Peng, Y. (2025). A hybrid blockchain and machine learning approach for intrusion detection system in Industrial Internet of Things. *Alexandria Engineering Journal*, *127*, 619–627. https://doi.org/10.1016/j.aej.2025.05.030

Spadaccino, P. C. F. (2024). *INTRUSION DETECTION SYSTEMS FOR IOT: OPPORTUNITIES AND CHALLENGES OFFERED BY EDGE COMPUTING AND MACHINE LEARNING*.

Spadaccino, P., & Francesca Cuomo. (2022). *INTRUSION DETECTION SYSTEMS FOR IOT: OPPORTUNITIES AND CHALLENGES OFFERED BY EDGE COMPUTING AND MACHINE LEARNING*.

Tekin, N., Acar, A., Aris, A., Uluagac, A. S., & Gungor, V. C. (2023). Energy consumption of on-device machine learning models for IoT intrusion detection. *Internet of Things (Netherlands)*, *21*. https://doi.org/10.1016/j.iot.2022.100670

Thakkar, A., & Lohiya, R. (2023). A Review on Challenges and Future Research Directions for Machine Learning-Based Intrusion Detection System. *Archives of Computational Methods in Engineering*, *30*(7), 4245–4269. https://doi.org/10.1007/s11831-023-09943-8

Wen, F. E. I., Ohno, H., & Sampalli, S. (2024). A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions. *ACM Computing Surveys*, *56*(5). https://doi.org/10.1145/3625094

Zhimin, L., & Jun, W. (2024). Intrusion Detection in Wireless Sensor Networks Based on IPSO-SVM Algorithm. *Journal of Cyber Security and Mobility*, *13*(4), 803–822. https://doi.org/10.13052/jcsm2245-1439.13410